

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ОҚУ АҒАРТУ МИНИСТРЛІГІ
Ы. АЛТЫНСАРИН АТЫНДАҒЫ ҰЛТТЫҚ БІЛІМ АКАДЕМИЯСЫ

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РЕСПУБЛИКИ КАЗАХСТАН
НАЦИОНАЛЬНАЯ АКАДЕМИЯ ОБРАЗОВАНИЯ ИМЕНИ Ы.
АЛТЫНСАРИНА



**БАЛАЛАРДЫҢ КИБЕРҚАУІПСІЗДІГІ, КИБЕРГИГИЕНАСЫ ЖӘНЕ
КИБЕРМӘДЕНИЕТІНЕ ҚАТЫСТЫ ЖАҒЫМДЫ ӘДЕТТЕРДІ
ҚАЛЫПТАСТЫРУ БОЙЫНША ӘДІСТЕМЕЛІК ҰСЫНЫМДАР**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ФОРМИРОВАНИЮ
ПОЛЕЗНЫХ ПРИВЫЧЕК В ОТНОШЕНИИ КИБЕРБЕЗОПАСНОСТИ,
КИБЕРГИГИЕНЫ И КИБЕРКУЛЬТУРЫ ДЕТЕЙ**

Астана 2023

Ы. Алтынсарин атындағы Ұлттық білім академиясы Ғылыми кеңесінің шешімімен баспаға ұсынылды (2023 жылғы 8 желтоқсандағы №9 хаттама)

Рекомендовано к печати решением Ученого совета Национальной академии образования им. Ы. Алтынсарина (протокол №9 от 8 декабря 2023 года)

Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша әдістемелік ұсынымдар – Астана: Ы.Алтынсарин атындағы Ұлттық білім академиясы, 2023. – 414бет

Методические рекомендации по формированию полезных привычек в отношении кибербезопасности, кибергигиены и киберкультуры детей – Астана: Национальная академия образования им. Ы. Алтынсарина, 2023. – 414 с

Цифрлық технологиялар қазіргі әлемнің ажырамас бөлігіне айналды және білім беруді табысты іске асыру үшін зор әлеуетке ие. Цифрлық әлемде білім алушылардың бойына киберқауіпсіздік, кибергигиена және кибермәдениет қасиеттерін қалыптастыру маңызды.

Әдістемелік ұсынымдамалар білім алушылардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты пайдалы әдеттерді қалыптастырудың кешенді тәсілін қамтиды. Ұсыныстар білім беру ұйымдарының директордың тәрбие жұмысы жөніндегі орынбасарларына, педагогтеріне, сынып жетекшілеріне арналған.

Цифровые технологии стали неотъемлемой частью современного мира и обладают огромным потенциалом для успешной реализации образования. В цифровом мире важно формировать у обучающихся свойства кибербезопасности, кибергигиены и киберкультуры.

Методические рекомендации включают комплексный подход к формированию полезных привычек в отношении кибербезопасности, кибергигиены и киберкультуры обучающихся. Рекомендации направлены заместителям директоров по воспитательной работе, педагогам, классным руководителям организаций образования.

© Ы.Алтынсарин атындағы
Ұлттық білім академиясы, 2023

© Национальная академия
образования им.Ы. Алтынсарина, 2023

КІРІСПЕ

Қазіргі әлем ақпараттық-коммуникациялық бағытта өте қарқынды даму процесінде. Адамдардың бір-бірімен қарым- қатынас орнатуы тек тікелей ғана емес, сонымен бірге Интернет арқылы да жүзеге асып жатады. Бұл процес білім алушылардың арасында да кеңінен етек алып, оларға қарқынды әсер етіп жатыр.

«Біз ұрпақ тәрбиесіне баса мән беріп, жастарды жақсылыққа жетелеуіміз керек. Бүгінгі интернет дәуірінде бұл оңай шаруа емес. Ашығын айтсақ, қазір жас ұрпақ әлеуметтік желі арқылы тәрбие алып жатыр. Баланы дұрыс бағытқа бұрып, жол көрсетіп отырмасақ, бұл – өте қауіпті үрдіс. Ғаламтор арқылы жат діни ағымдардың құрығына түскен жастар да бар. Ұрпақтың бойында жаман әдет болса, бұл – ең алдымен, үлкендердің кінәсі» деді Мемлекет басшысы Қасым-Жомарт Тоқаевтың Ұлттық құрылтайдың «Әділетті Қазақстан – Адал азамат» атты екінші отырысында сөйлеген сөзінде[1].

Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен Киберқауіпсіздік тұжырымдамасы қабылданды. Тұжырымдама электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғау, ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясатты іске асырудың негізгі бағыттарын белгілейді.

Қазақстан Республикасында ақпараттандыру мен байланыс саласындағы ақпараттық қауіпсіздікті, яғни киберқауіпсіздікті қамтамасыз ету бойынша шаралар жүйесінің ұйымдастыру – құқықтық және техникалық негіздері «Ұлттық қауіпсіздік туралы» Қазақстан Республикасының Заңына сәйкес ақпараттық қауіпсіздіктің және ақпараттық кеңістік пен байланыс инфрақұрылымының қауіпсіздігін қамтамасыз етудің құрамдас бөліктері ретінде заңнамалық түрде бекітілді [2].

Қазақстан Республикасының 2018 жылғы 2 шілдедегі № 169 «Балаларды денсаулығы мен дамуына зардабын тигізетін ақпараттан қорғау туралы» Заңында 4-ші «Ақпараттық өнімді таратуға қойылатын талаптар» тарауының 16 бабынның 3 тармағында интернет желісі арқылы таратылатын ақпараттық өнімді қоспағанда, балаларға тыйым салынған ақпаратты қамтитын ақпараттық өнімді кәмелетке толмағандарға таратуға жол берілмейді.

Балаларға тыйым салынған ақпаратты қамтитын ақпараттық өнімді кәмелетке толмағандарға Интернет желісі арқылы таратқан кезде балалардың ақпаратқа қол жеткізуін шектеудің әкімшілік, техникалық, бағдарламалық құралдары немесе өзге де тәсілдері қолданылады делінген [3].

Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы

Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар «Ақпараттандыру туралы» Қазақстан Республикасы Заңының 6-бабының 3) тармақшасына сәйкес

және ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы талаптарды айқындайды [4].

Ақпараттық және коммуникациялық, электрондық, цифрлық, компьютерлік және интернет-технологиялар осы дамудың маңызды құрамдас бөлігі болып табылады. Осы технологиялардың дамуы жылдам және үздіксіз өзгерістермен сипатталатын ортаны тудырады [5].

XX ғасырдың ортасын ақпараттық технологиялардың қалыптасуының, компьютерлер мен компьютерлік желілерді, мәліметтер базасын құрудың бастау кезеңі деп айтуға болады.

Ресей ғалымы В.А. Плешаковтың айтуынша, XX ғасырдың ортасынан XX ғасырдың 90-жылдарына дейін жалғасқан уақыт – төртінші ақпараттық революция кезеңі. Бесінші ақпараттық революция, ғалымның пікірінше, XX ғасырдың соңында бастау алады «... ол қазіргі адамзатқа өркениет эволюциясының сапалы жаңа кезеңіне – киберэволюцияға көшуге мүмкіндік беріп, бүкіл әлемдегі әлеуметтік құрылымдардың жаңа түбегейлі өзгерістерінің катализаторы болды» [6].

В. А. Плешаков киберкеңістік жеке тұлға психологиясымен тікелей байланысты. Адамдар киберкеңістікті өздерінің қарым-қатынасы мен мүдделерін көрсететін өзін-өзі көрсету ортасы ретінде жиі қолданады. Психоанализ тұрғысынан киберкеңістікті жеке адамның интрапсихикалық кеңістігі болып табылатын орта ретінде сипаттауға болады. Бүгінгі таңда киберкеңістік адам өмірінің ажырамас бөлігі, жеке тұлғаның киберкеңістікке интеграциялану дәрежесіне сәйкес оны тіпті алмастырады да (кибер немесе интернет-тәуелділік ретінде).

Осыған байланысты әлеуметтік нормалардың жиынтығын, цифрлық әлемде навигация дағдыларын, ақпаратты пайдалану мәдениетін және оған сыни көзқарасты қалыптастыру қажеттілігімен байланысты көптеген проблемалар туындайтыны мәлім.

Адам туғаннан бастап өмірінің соңына дейін әлеуметтенудің нақты әлеуетіне, сонымен қатар кибер әлеуметтену мүмкіндіктеріне ие.

Ғалым В.А. Плешаков Ол «адамның кибер әлеуметтендіруі жеке тұлғаның әлеуметтенуі ретінде – жеке тұлғаның өзін-өзі тану құрылымындағы сапалы өзгерістер процесі ретінде, сондай-ақ адамның қазіргі заманғы ақпараттық-коммуникациялық және компьютерлік технологияларды қолдану әсерінен және нәтижесінде пайда болатын жеке тұлғаның қажеттілік-мотивациялық сферасы ретінде», -деп анықтайды [7].

Кибер әлеуметтендіру процесінде адамда бірқатар жаңа, іс жүзінде киберологиялық күтулер мен мүдделер, мотивтер мен мақсаттар, қажеттіліктер мен көзқарастар, сондай-ақ киберкеңістікпен тікелей байланысты психологиялық және әлеуметтік белсенділік формалары пайда болады. Маслоу жасаған қажеттіліктер пирамидасына сүйене отырып, интернет қолданушылары өздерінің өзекті қажеттіліктерін қанағаттандыруды да, квази-қанағаттандыруды да (қиялды, нақты қанағаттандыру емес) табады деп болжауға болады. Ал ондай процесс бірнеше қиындықтарға әкелу мүмкін. Себебі әр тұлғаның

дамуында, оның сана сезімінде өзіндік ерекшеліктері бар.[8].

Қазіргі уақытта компьютерлік технологиялар біздің өмірімізге мықтап енді. Олар білім беру, жұмыс, қарым-қатынас және бос уақытты қоса алғанда, әртүрлі қызмет салаларында қолданылады. Балалар мен жасөспірімдер, халықтың ең белсенді және ізденімпаз бөлігі ретінде оларға цифрлық технологиялар ерекше, күшті әсер етуде.

Қоғамда балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетін сақтау мәселесі бүгінгі күнде өзекті болып отыр.

Дегенмен, компьютерлік технологияларды белсенді пайдалану қауіпсіздік, гигиена және мәдениетке байланысты бірқатар тәуекелдермен бірге жүреді.

Киберқауіпсіздік – бұл жеке тұлғаның, қоғамның және мемлекеттің ақпараттық кеңістікте туындайтын қауіптерден қорғау жағдайы.

Кибергигиена – бұл компьютерлік технологияны қауіпсіз және салауатты пайдалану бойынша ережелер мен нұсқаулардың жиынтығы.

Кибермәдениет – бұл ақпараттық кеңістіктегі адамдардың мінез-құлқын реттейтін нормалар мен құндылықтардың жиынтығы.

Киберқауіпсіздік, кибергигиена және кибермәдениет мәселелеріне жеткіліксіз назар аудару балалар мен жасөспірімдер үшін жағымсыз салдарға әкелуі мүмкін. Оларға:

Қауіпсіздік тәуекелдері: зиянды бағдарламалардың таралуы, фишингтік шабуылдар, кибербуллинг, Интернетке тәуелділік және басқалар.

Денсаулыққа тигізер қауіптер: көру қабілетінің, позаның, тірек-қимыл аппаратының бұзылуы, психикалық бұзылулардың дамуы және басқалар.

Мәдени даму үшін қауіптер: сауаттылық деңгейінің төмендеуі, қарым-қатынас мәдениеті, сыни ойлау және басқалар.

Сондықтан қазіргі уақытта қоғамдағы балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін сақтау маңызды міндет болып табылады.

Әдістемелік ұсынымдамалардың өзектілігі келесі факторларға байланысты:

- Балалар мен жасөспірімдердің компьютерлік технологияларды қолдануын кеңейту.

- Ақпараттық кеңістіктегі қауіпсіздік, гигиена және мәдениетке байланысты тәуекелдердің артуы.

- Балалар мен жасөспірімдерде компьютерлік технологияларды қауіпсіз және жауапты пайдалану мәдениетін қалыптастыру қажеттілігі.

Әдістемелік ұсынымдаманы зерттеудің мақсаты – қоғамдағы балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін сақтаудың негізгі бағыттары мен әдістерін анықтау.

Әдістемелік ұсынымдаманы зерттеуде мақсатқа жету үшін келесі міндеттерді шешу қажет:

- Киберқауіпсіздік, кибергигиена және кибермәдениеттің теориялық негіздерін зерттеу.

- Қоғамдағы балалардың киберқауіпсіздік, кибергигиена және кибермәдениет жағдайын талдау.

- Қоғамдағы балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін сақтау бойынша ұсыныстар әзірлеу.

Әдістемелік ұсынымдаманы зерттеу нысаны – қоғамдағы балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениеті.

Әдістемелік ұсынымдамада қоғамдағы балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін сақтаудың негізгі бағыттары мен әдістері ұсынылады.

Әдістемелік ұсынымдаманың бірінші «Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетінің ағымдағы жағдайын теориялық негіздеу және талдау» бөлімінде тақырыпқа сәйкес негізгі талаптар мен балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетін сақтаудың бағыттары ұсынылады.

Әдістемелік ұсынымдаманың екінші «Балалардың киберқауіпсіздігіне, кибергигиенасына және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша халықаралық және отандық тәжірибе» бөлімінде халықаралық және отандық тәжірибелер талданып, зерттеулер беріледі.

Әдістемелік ұсынымдаманың үшінші «Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша әдістемелік ұсынымдар» бөлімінде білім беру ұйымдарында білім алушылармен жүргізілетін іс-шаралар, тәрбие сағаттары және оқу процесінде ұйымдастырылатын пән сабақтарының жоспарлары, әлеуметтік жобалар мен акциялар сонымен қатар педагогтер мен ата-аналарға арналған кеңестер бойынша әдістемелік ұсынымдар ұсынылады.

1. Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетінің ағымдағы жағдайын теориялық негіздеу және талдау

Балаларға арналған Кибергигиена: жас ұрпақты интернеттегі қауіпсіздікке қалай үйрету керек?

Интернеттің және оған қосылған құрылғылардың кең таралуына байланысты қазіргі ұрпақ жас кезінен бастап әртүрлі желілік тәуекелдерге тап болды. Киберқауіптер — зиянды бағдарламалардан кибербуллингке дейін-балалардың ақпараттық, психологиялық және тіпті физикалық қауіпсіздігіне қауіп төндіруі мүмкін. Кибергигиена негіздерін оқыту күн тәртібінде жиі пайда болады және ол цифрлық салада жас ұрпақты қорғаудың маңызды шарты болып табылады.

Балалар үшін интернеттегі ең көп кездесетін қауіптер туралы және балалар мен жасөспірімдерге интернет кеңістігінде қауіпсіз болуды үйрету туралы ұсыныстар ұсынуға болады.

Негізгі қауіптер

Интернетке кіргеннен кейін балалар білімнің, ойын-сауықтың және қарым-қатынастың кең жүйесі мен желілік әлемнің қауіпті лабиринтіне еніп кетеді.

Интернет – бұл шексіз мүмкіндіктер орны және сонымен бірге жасырын қауіптер тәжірибесіз адамды оңай таң қалдыратын сала. Бұл жерде балалар киберқауіптерді жиі кездестіреді.

Зиянды бағдарламалар

Цифрлық ойын-сауық әлемі балаларды шексіз мүмкіндіктерімен қызықтырады. Дегенмен, ол сондай-ақ балалардың қызығушылығымен ойнайтын және оның соңы жиі қайғылы салдарға әкелетін қауіптерге әкеледі. Неғұрлым қызықты ойын тәжірибесін немесе премиум қолданбаларға тегін қол жеткізуді іздеу үшін балалар көбінесе «ойын режимдері» мен қарақшылық қолданбалардың алдамшы саласына түседі. Ойын режимдері – пайдаланушылар жасаған модификациялар жаңа кейіпкерлерді, деңгейлерді және ойын мүмкіндіктерін енгізеді, әдетте олар тегін қол жетімді, бұл оларды керемет қызықтырып, өзіне қарай тарта бастайды. Сол сияқты, қарақшылық қосымшалар балаларды ақылы қосымшалар мен ойындарды бір тиын жұмсамай-ақ, тегін пайдалануға шақырады. Бірақ цифрлық ойын-сауықтың астарында зиянды бағдарламалар жасырылған.

Зиянды бағдарлама (malware) әр түрлі формада болады: вирустар, трояндық бағдарламалар, төлем бағдарламалары және тыңшылық бағдарламалар, олардың әрқайсысы өздерінің жасырын мақсаттарын көздейді. Балалар осы жасырын қауіптерді жүктегенде, олар санасыз түрде өздерінің цифрлық өміріне көптеген ықтимал қауіпті тәуекелдерге тартады. Бұл тұзақтарға түсудің салдары әр түрлі болуы мүмкін. Зиянды бағдарламалар мен вирустар баланың құрылғысына үнсіз еніп, хакерлерге жеке ақпаратқа, отбасылық фотосуреттерге, тіпті мекен-жайлар мен байланыс деректері сияқты

құпия деректерге рұқсатсыз қол жеткізуге мүмкіндік береді. Кейбір зиянды бағдарламалар парольдер мен хабарламаларды қоса, әр пернені басуды үнсіз жазып, клавиатура ретінде жұмыс істей алады. Ол зиян жеке шығындармен ғана шектелмейді сонымен қатар құрылғыларға да таралады.

Зиянды бағдарламалар компьютерге немесе мобильді құрылғыға зиян келтіруі мүмкін бұл құрылғылардың бұзылуына немесе мүлдем істен шығуына әкеледі. Мұндай жағдайларда ата-аналар көбінесе құрылғыны қымбат жөндеуге немесе ауыстыруға ақы төлеу қажеттілігіне тап болады.

Фишинг және кибербуллинг

Сіз өзіңіздің сүйікті әлеуметтік желіңіздегі ескі досыңыздан хабарлама алдыңыз деп елестетіп көріңіз. Мұндай «достардың» хабарламалары қарапайым болып көрінуі және көбінесе ақша аудару, жеке ақпарат беру (несиелік карта нөмірлері немесе парольдер) сияқты зиянды веб-сайттарға жалған сілтемелерді қамтуы мүмкін. Бұл сізді «фишинг» деп аталатын опасыз схемаға итермелейтін алаяқтардың негізгі тактикасы.

Фишинг – бұл цифрлық алаяқтық, онда шабуылдаушылар танымал платформалар, танымал брендтер немесе тіпті сенімді адам ретінде көрінеді. Олардың мақсаты – жеке ақпаратты-тіркелгі деректерін немесе несие картасының деректерін хабарлауға мәжбүрлеу арқылы сеніміңізді басқару. Ықтимал тәуекелдер өте жоғары. Фишингтік шабуыл құрбандары өздерінің жеке деректерін ойданбастан жібереді, бұл жеке деректерді ұрлауға, қаржылық шығындарға немесе Интернеттегі шоттарды бұзуға әкелуі әбден мүмкін.

Бірақ бұл тек осымен ғана шектелмейді, өйткені кибербуллинг – адамдар интернет пен әлеуметтік желілерді қасақана қорқыту, қорлау немесе басқа адамдарға зиян келтіру үшін қолданатын онлайн-қатыгездіктің бір түрі.

Цифрлық кеңістіктің қараңғы бұрыштарында балаға нақты зиян келтіруге қабілетті анонимді пайдаланушылар жасырылған. Бұл субъектілердің мотивтері әртүрлі, бірақ олар аңғал пайдаланушыларды жасырын түрде қудалауға, қорқытуға немесе тіпті бопсалауға қабілетті және міндетті түрде солай жасайды. Олардың әрекеттері көбінесе құрбандарын нақты психологиялық жарақаттарға әкеледі. Балалар туралы ақпаратты олардың өміріне нақты қауіп төндіретіндердің қолына түсіруі алаңдатарлық жайт. Интернетте жеке ақпаратты шамадан тыс тарату олардың өмірі үшін де тәуекелдерді бірнеше есе арттырады. Шабуылдаушы бұл деректерді жинап, жәбірленушінің орналасқан жерін, оның қызығушылықтары мен күнделікті әдеттерін ашатын «мозаика» жасайды. Мұндай құпиялылықты бұзу қудалауға, жәбірлеуге және одан да жаман әрекеттерге жол ашады. Интернет қазіргі жастарға қарым-қатынас пен оқудың шексіз мүмкіндіктерін ұсынғанымен, оның бақыланбайтын кеңістігі де қауіп төндіреді. Кибергигиенаның негізгі дағдыларын үйрету арқылы жас интернет қолданушылар мүмкіндіктерді жасырын қауіптерден ажыратуды үйрене алады.

Негізгі кибергигиена

Кез келген ата-ана цифрлық дәуірде балаларды тәрбиелеу белгілі бір қиындықтарды тудыратынын біледі. Балаларды интернеттегі ақпарат пен

«достар әлемімен» таныстыру пайдалы болуы мүмкін болса да, әр экранның артында бақыланбайтын қауіптер бар. Жақсы гигиена физикалық денсаулықтың кепілі сияқты, кибергигиена цифрлық ортада қауіпсіздік пен әлауқатқа ықпал етеді. Кішкентай кезінен бастап балаларға негізгі қауіпсіздік дағдыларын үйрету оларға өмір бойы Интернетте қорғануға көмектеседі.

Ересектер мен балаларға ықтимал киберқауіптерден қорғану үшін беруге болатын кейбір кеңестер.

Зиянды бағдарламалар:

Бағдарламалық жасақтаманы жаңарту:

- амалдық жүйені және бағдарламалық жасақтаманы үнемі жаңартып отырыңыз, өйткені бұл жаңартулар көбінесе соңғы қауіптерден қорғайтын қауіпсіздік патчтарын қамтиды.

Сенімді орнату антивирустық бағдарлама:

- нақты уақыт режимінде зиянды бағдарламалардан қорғауды қамтамасыз ететін сенімді антивирустық бағдарламалық жасақтаманы қолданыңыз. Оның автоматты түрде жаңартуға және сканерлеуге орнатылғанына көз жеткізіңіз.

Файлдарды жүктеу кезінде абай болыңыз:

- қолданбаларды, файлдарды және бағдарламаларды тек қолданбалар дүкендері немесе ресми веб-сайттар сияқты ресми дереккөздерден жүктеп алыңыз.

- Бейтаныс сайттардан сақ болыңыз және күдікті сілтемелерге өтпеңіз.

Фишинг:

Жіберушінің түпнұсқалығын тексеру:

- балаларыңызға ешқашан сілтемелерді баспауға және белгісіз жіберушілердің хаттарында немесе хабарламаларында тіркемелерді ашпауға үйретіңіз.

- Әрекет жасамас бұрын жіберушінің заңдылығын тексеріңіз.

URL мекенжайын тексеру:

- сілтемені баспас бұрын, нақты URL мекенжайын көру үшін оның үстіне апарыңыз. Оның тағайындалған жерге сәйкес келетініне көз жеткізіңіз.

Көп факторлы аутентификацияны (MFA) пайдалану:

- мүмкіндігінше есептік жазбаларда көп факторлы аутентификацияны іске қосыңыз. Бұл екінші тексеру формасын қажет ететін қосымша қауіпсіздік деңгейін қамтамасыз етеді.

Электрондық пошта алаяқтықтары туралы хабардар болу:

- балаларыңызға шұғыл хабарламалар, күдікті сілтемелер немесе жеке ақпарат беру туралы өтініштер сияқты жалпы фишинг тактикасы туралы айтыңыз.

- Мұндай хабарламаларға жауап бермеу туралы ескертіңіз.

HTTPS шифрлауымен заңды сайттарды пайдалану.

- Бұл шифрлау деректерді ұстап қалудан қорғайды, ал күдікті жүктеулер мен сілтемелерден бас тарту зиянды бағдарламалардың

инфекциясын болдырмайды.

Кибербуллинг:

Ашық қарым-қатынас:

- балаларыңызбен тығыз байланыста болыңыз.

- Оларды Интернеттегі тәжірибелері туралы, соның ішінде кибербуллинг жағдайлары туралы айтуға шақырыңыз.

Әлеуметтік медиа шекараларын орнату:

- әлеуметтік желілерде өткізілетін уақытты шектеңіз және құпиялылықтың дұрыс параметрлерін қамтамасыз етіңіз. Әлеуметтік желілердегі құпиялылық параметрлерін дәл калибрлеу және жеке ақпаратты тек тексерілген достармен бөлісу алаяқтық пен қорлауды, жәбірлеуді болдырмайды.

Құжаттау және ескерту:

- егер сіздің балаңыз кибербуллингке тап болса, оған қорлайтын мазмұнды құжаттауға және оны платформаға, қажет болған жағдайда мектепке немесе құқық қорғау органдарына хабарлауға кеңес беріңіз.

Төзімділікті тәрбиелеу:

- балаларыңызға кибербуллингтің жиі жауап беретінін түсінуге көмектесіңіз. Оларды хат алмасуға, блоктауға немесе дыбысты өшіруге жол бермеуге шақырыңыз. Бірақ, сайып келгенде, ешқандай бұғаттау мен бақылау балалардың киберқауіпсіздігін қамтамасыз ете алмайды.

Бұл жерде ата-аналардың белсенді қатысуы мен білімі шешуші рөл атқарады. Сондай-ақ, ата-аналар этикалық нормалар мен балалардың қауіпсіздігін қамтамасыз етудің ең жақсы әдістерін көрсете отырып, желіде үлгі көрсетуі керек.

Салауатты отбасылық кибермәдениетті қалыптастыру уақыт пен ата-ананың назарын қажет етеді. Ата-аналар балаларды желілік тәуекелдерден толығымен қорғай алмаса да, олар сезімтал басшылықпен оларға интернетте қауіпсіз болуға мүмкіндік бере алады. Мектептер білім алушыларды цифрлық кеңістікте қауіпсіз навигацияға дайындауда басты рөлдердің біріде болуы керек. Кибергигиена мәселелерін оқу процесіне біріктіре отырып, педагогтер бастауыштан бастап білім алушыларға Интернетті пайдалану кезінде қауіп-қатер мен жауапкершілік туралы түсінік бере алады.

Білім алушылар үшін ғана емес, педагогтер мен ата-аналар үшін де арнайы оқу бағдарламасын немесе тіпті киберқауіпсіздік бойынша шағын дәрістерді енгізу желідегі қауіпсіздік негіздерін дәйекті түрде түсінуге, білімнің өзектілігін сақтауға және оларды мектептен тыс жерде таратуға мүмкіндік береді.

Оқу ортасында этикалық цифрлық мінез-құлық пен қауіпсіздікті сақтау бірдей маңызды. Тіпті оқу компьютерлерінде күшті парольдер мен SZI, қорғалған желілер және деректерге жауапкершілікпен қарау қажет. Ойластырылған білім беру саясаты мен өз үлгі-өнегесінің арқасында педагогтер білім алушыларға киберқауіпсіздікті қамтамасыз ету үшін қажетті білім мен

сыни ойлауды бере алады.

Қазіргі жастар цифрлық салада бұрын-соңды болмаған қауіптерге тап болуда. Вирустардан кибербулингке дейін бұл өте қауіпті және күрделі технологиялар. Бірақ кибергигиенаны үйрету арқылы біз балаларға интернетті қауіпсіз пайдалануға мүмкіндік бере аламыз.

Ерте жастан бастап қауіпсіз мінез-құлықтың негізгі әдеттерін үйрету, сыни ойлауды үйрету және үйде және мектепте қауіпсіз мінез-құлық үлгілерін бекіту арқылы біз балаларды желіде қорғауға көмектесе аламыз. Қырағылық пен бейімделу негізгі факторлар. Ата-аналар мен тәрбиешілер ретінде біз туындайтын қауіптерді қадағалап, оларға сәйкес өз стратегияларымызды әзірлеуіміз керек. Кешенді киберқауіпсіздік саясатын насихаттау виртуалды кеңістікке толық байсалдылықпен қарайтын адамдардың тұтас ұрпағын тәрбиелеуге мүмкіндік береді [9].

Киберқауіпсіздік

Киберқауіпсіздік – бұл жеке тұлғаның, қоғамның және мемлекеттің ақпараттық кеңістікте туындайтын қауіптерден қорғалу жағдайы. Ол келесі аспектілерді қамтиды:

Ақпараттық қауіпсіздік: ақпаратты рұқсатсыз кіруден, пайдаланудан, ашудан, бұғаттаудан, көшіруден, өзгертуден немесе жоюдан қорғау.

Инфрақұрылымдық қауіпсіздік: Ақпараттық жүйелер мен желілерді шабуылдардан, зақымданудан және істен шығудан қорғау.

Жеке қауіпсіздік: пайдаланушыларды кибербуллинг, Интернетке тәуелділік және т.б. сияқты қауіптерден қорғау.

Балалардың киберқауіпсіздігінің негізгі қауіптеріне мыналар жатады:

Зиянды бағдарламалардың таралуы: вирустар, трояндар, шпиондық бағдарламалар және басқалар.

Фишингтік шабуылдар: логиндер, парольдер, құпия сөздер немесе банктік карта нөмірлері сияқты құпия ақпаратты алдау әрекеттері.

Кибербуллинг: ақпараттық кеңістіктегі балаларды қудалау, қорқыту немесе қорлау.

Интернетке тәуелділік: компьютерлік технологияны қолдануға патологиялық тәуелділік.

Балаларды осы қауіптерден қорғау үшін келесі шараларды орындау қажет:

Балаларға киберқауіпсіздік негіздерін үйрету:

- Интернетте қауіпсіз жұмыс істеу ережелері, қауіптерді тану және олардың деректерін қорғау;
- Кибербуллинктің алдын алу бойынша бағдарламаларды іске асыру;
- Балалардың Интернетте сапалы ақпаратқа қол жеткізуін қамтамасыз ету.

Кибергигиена

Кибергигиена – бұл компьютерлік технологияны қауіпсіз және салауатты пайдалану бойынша ережелер мен нұсқаулардың жиынтығы.

Балалардың кибергигиенасы олардың денсаулығы мен әл-ауқатын сақтаудың маңызды факторы. Балалардың кибергигиенасы компьютерлік технологияны қолдану кезінде олардың денсаулығы мен қауіпсіздігін қорғауға бағытталған.

Ол келесі аспектілерді қамтиды:

Физикалық қауіпсіздік: денені көру қабілетінің бұзылуы, қалып, тірек-қимыл аппараты және т.б. сияқты компьютерлік технологияның теріс әсерінен қорғау.

Психологиялық қауіпсіздік: психиканы Интернетке тәуелділік, кибербуллинг және басқалар сияқты жағымсыз әсерлерден қорғау.

Ақпараттық қауіпсіздік: зиянды бағдарламалардан, фишингтік шабуылдардан және басқа қауіптерден қорғау.

Балаларға арналған кибергигиенаның негізгі ережелеріне мыналар жатады:

- Компьютерде үнемі үзіліс жасау;
- Компьютерде жұмыс істегенде дұрыс қалыпты отыру;
- Компьютерде өткізілетін уақытты шектеу,
- Монитордың зиянды сәулеленуінен көзді қорғау;
- Компьютерде жұмыс істегеннен кейін қол гигиенасын сақтау;
- Антивирустық бағдарламалық құралды орнату.

Балалардың кибергигиенасын қамтамасыз ету үшін келесі шараларды орындау қажет:

- Балаларға кибергигиена ережелерін үйрету.
- Балаларды эргономика талаптарына сәйкес келетін жиһазбен және жабдықтармен қамтамасыз ету.
- Балалардың компьютерде өткізетін уақытын шектеу.

Кибермәдениет

Кибермәдениет – бұл ақпараттық кеңістіктегі адамдардың мінез-құлқын реттейтін нормалар мен құндылықтардың жиынтығы. Балалардың кибермәдениеті олардың әлеуметтенуі мен жеке басын қалыптастырудың маңызды факторы.

Ол келесі аспектілерді қамтиды:

Пайдаланушылардың құқықтары мен міндеттері: басқа пайдаланушылардың құқықтары мен бостандықтарын сақтау, сондай-ақ ақпараттық кеңістікте өз міндеттерін орындау.

Қарым-қатынас этикасы: Интернеттегі этикалық қарым-қатынас ережелерін сақтау.

Ақпаратты тұтыну мәдениеті: Интернеттен алынған ақпаратқа сыни көзқарас.

Кибермәдениеттің негізгі құндылықтарына мыналар жатады:

- Басқа адамдарға құрмет. Ұлтына, жынысына, жасына, әлеуметтік мәртебесіне және басқа сипаттамаларына қарамастан басқа адамдарға деген құрмет;
- Нақты өмірдегі сияқты ақпараттық кеңістікте өз әрекеттері үшін жауапкершілік;

- Сыни тұрғыдан ойлау;
- Интернетте жағымды атмосфера құру;
- Интернет желісіндегі байланыс ережелерін, этикасы сақтау.

Балалардың кибермәдениетін қалыптастыру үшін келесі шараларды жүргізу қажет:

- Балаларға кибермәдениеттің құндылықтарын үйрету;
- Интернеттегі мінез-құлықтағы ересектердің мысалы;
- Интернеттегі балалардың қарым-қатынасы үшін қауіпсіз және жағымды орта құру.

Балалардың киберқауіпсіздік, кибергигиена және кибермәдениетінің қазіргі жағдайын талдау:

Қазіргі уақытта балалар мен жасөспірімдер өмірдің әртүрлі салаларында компьютерлік технологияны белсенді қолданады. Олар әлеуметтік желілерде сөйлеседі, компьютерлік ойындар ойнайды, бейнелер көреді және интернеттегі басқа әрекеттермен айналысады.

Бұл факт балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениеті назар аударуды қажет ететін маңызды және өзекті мәселелер екенін көрсетеді.

Балалардың киберқауіпсіздігі

Зерттеулер көрсеткендей, балалар мен жасөспірімдер киберқауіптерге қатысты халықтың ең осал тобы болып табылады. Олар көбінесе кибербуллингтің, Интернетке тәуелділіктің және басқа қауіптердің құрбаны болады.

Балаларға қатысты киберқауіптерге ықпал ететін негізгі факторлардың қатарына мыналар жатады:

- Балалар мен жасөспірімдердің киберқауіпсіздік туралы хабардарлығы.
- Ата-аналар мен басқа ересектердің бақылауының жеткіліксіз;
- Көбінесе танылмайтын киберқауіптердің күрделілігі;
- Балалардың кибергигиенасының сақалмауы;
- Ақпараттық кеңістіктегі қарым-қатынас мәдениетінің қалыптасуының төмен деңгейі.

Сонымен қатар балалар мен жасөспірімдердің кибергигиена ережелерін жиі елемейтіні байқалады. Бұл көру қабілетінің бұзылуы, тірек-қимыл аппараты және т.б. сияқты денсаулық мәселелеріне әкеледі.

Кибергигиенаның бұзылуына ықпал ететін негізгі факторларға мыналар жатады:

- Кибергигиена ережелерін білмеу;
- Ата-аналар мен басқа ересектердің балалардың кибергигиена ережелерін сақтауына жеткіліксіз назар аударуы;
- Компьютерлік технологияны ұзақ уақыт қолдану әдеті;
- Балалардың кибермәдениетінің болмауы;
- Зиянды бағдарламалар, фишингтік шабуылдар, кибербуллинг және

интернетке тәуелділік жағдайларының көбеюі.

Компьютерлік технологияны ұзақ уақыт қолданумен байланысты балалардың денсаулығының бұзылуы.

Ақпараттық кеңістіктегі байланыс мәдениетінің деградациясы.

Осы проблемаларды шешу үшін балалардың компьютерлік технологияларды пайдаланумен байланысты тәуекелдер туралы хабардарлығын арттыруға, олардың компьютерлік технологияларды пайдалану кезінде қауіпсіздігі мен денсаулығы үшін жауапкершілік сезімін қалыптастыруға, сондай-ақ ақпараттық кеңістікте қарым-қатынас мәдениетін дамытуға бағытталған іс-шаралар кешенін жүргізу қажет.

Балалар мен жасөспірімдер көбінесе ақпараттық кеңістіктегі адамдардың мінез-құлқын реттейтін нормалар мен құндылықтарды сақтамайды. Бұл қақтығыстарға, құқық бұзушылықтарға және басқа да жағымсыз салдарға әкеледі.

Кибермәдениеттің бұзылуына ықпал ететін негізгі факторларға мыналар жатады:

- Кибермәдениеттің нормалары мен құндылықтарын білмеу.
- Ата-аналар мен басқа ересектердің балалардағы кибермәдениетті тәрбиелеуге жеткіліксіз көңіл бөлуі.
- Интернеттегі дөрекі және агрессивті мінез-құлық әдеті.
- Балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін сақтау бойынша ұсыныстар

Балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін сақтау үшін келесі шараларды қабылдау қажет:

- Киберқауіпсіздік, кибергигиена және кибермәдениет саласында балалар мен жасөспірімдерге үздіксіз білім беру жүйесін құру;
- Балалардың компьютерлік технологияларды пайдалануына ата-аналар мен басқа ересектер тарапынан бақылауды күшейту;
- Балаларды киберқауіптерден қорғаудың тиімді тетіктерін әзірлеу және енгізу.

Бұл шаралар мемлекеттік, қоғамдық, білім беру және отбасылық деңгейлерде жүзеге асырылуы керек.

Балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін жақсарту бойынша ұсыныстар

Балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін арттыру үшін:

Мектеп бағдарламасына киберқауіпсіздік, кибергигиена және кибермәдениет мәселелерін тәрбие процесінде және оқу мазмұнына енгізу;

Балалардың компьютерлік технологияларды пайдаланумен байланысты тәуекелдер туралы хабардарлығын арттыруға, олардың компьютерлік технологияларды пайдалану кезінде қауіпсіздігі мен денсаулығы үшін жауапкершілік сезімін қалыптастыруға, сондай-ақ ақпараттық кеңістікте қарым-қатынас мәдениетін дамытуға бағытталған сыныптан тыс іс-шараларды өткізу;

Ата-аналармен бірлесіп балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін арттыруға бағытталған бағдарламаларды әзірлеу және практикаға енгізу.

Осы ұсыныстарды іске асыру балаларда компьютерлік технологияларды қауіпсіз және жауапты пайдалану мәдениетін қалыптастыруға мүмкіндік береді, бұл олардың қазіргі ақпараттық қоғамда табысты әлеуметтенуіне ықпал етеді.

Әдістемелік ұсынымдар:

Балалардың киберқауіпсіздігін, кибергигиенасын және кибермәдениетін арттыру бойынша ұсыныстарды іске асыру үшін келесі ұсынымдарды пайдалануға болады:

- Балаларға арналған киберқауіпсіздік, кибергигиена және кибермәдениет бойынша іс-шаралар, сынып сағаттары, сабақ жоспарлары, түрлі жоюалар мен акциялардың үлгілерін пайдалануға болады;

- Киберқауіпсіздік, кибергигиена және кибермәдениет мәселелеріне арналған мультфильмдер, бейнелер және басқа да медиа материалдар;

- Балалардың компьютерлік технологияларды қолданумен байланысты тәуекелдер туралы хабардарлығын арттыруға, олардың компьютерлік технологияларды пайдалану кезінде қауіпсіздігі мен денсаулығы үшін жауапкершілік сезімін қалыптастыруға, сондай-ақ ақпараттық кеңістікте қарым-қатынас мәдениетін дамытуға бағытталған ойындар мен жаттығулар.

Кибергигиена – компьютерлер мен басқа құрылғыларды пайдаланушылар өздерінің онлайн қауіпсіздігін арттыру және жүйенің жұмысын қамтамасыз ету үшін жасай алатын қадамдарды білдіреді. Кибергигиена жеке адамдар мен ұйымдарға ықтимал онлайн бұзылуларды жеңілдетуге көмектесетін қауіпсіздікке бағытталған ойлау мен әдеттерді қабылдауды білдіреді. Кибергигиенаның негізгі қағидасы – бұл күнделікті өмірдің бір бөлігіне айналады.

Кибергигиена дегеніміз не?

Кибергигиена – киберқауіпсіздік пен онлайн қауіпсіздік мәселелерінен озып кету үшін өзіңізді пайдалы киберқауіпсіздік әдеттерін қалыптастыруға үйрету. Кибергигиенаны кейде жеке гигиенамен салыстырады – бұл екеуі де денсаулық пен әл-ауқат үшін үнемі жүргізілетін сақтық шаралары.

Кибергигиена аппараттық және бағдарламалық жасақтаманың негізгі күйі мен қауіпсіздігін сақтауға бағытталған, оларды зиянды бағдарламалар сияқты қауіптерден қорғауға кепілдік береді. Үнемі қолданылатын кибергигиена деректерді сақтауға көмектеседі. Адам өмірінде қалыптастыратын жағымды дағдылар мен әдеттер сияқты, кибергигиена күнделікті дағдылануды және қайталауды қажет етеді.

Кибергигиенаға негізделген тәртіпті құру киберқылмыскерлердің шабуылын бұзудың немесе жеке ақпаратты ұрлаудың алдын алуына көмектеседі. Бұл сонымен қатар бағдарламалық жасақтама мен операциялық жүйелердегі соңғы өзгерістерден хабардар болуға көмектеседі.

Кибергигиена Covid-19 пандемиясынан кейін ерекше өзектілікке ие болды, өйткені бүкіл әлемде барлық адамдар қашықтан жұмыс істегеннен кейін киберқылмыстардың көбеюіне әкелді.

Жалпы кибергигиена мәселелері

Кибергигиена шешуге арналған кейбір мәселелерге мыналар жатады:

Қауіпсіздікті бұзу, соның ішінде хакерлердің қауіп-қатері, фишинг, зиянды бағдарламалар және вирустар.

Деректердің жоғалуы – сақтық көшірмесі жасалмаған қатты дискілер мен бұлтқа негізделген онлайн-қоймалар бұзуға, бүлінуге немесе деректердің жоғалуына әкелуі мүмкін басқа мәселелерге осал болуы мүмкін.

Ескірген бағдарламалық құрал құрылғыны онлайн шабуылдарға осал етеді.

Жаңартылмаған ескірген антивирустық бағдарламалық жасақтама сізді соңғы киберқауіптерден қорғауда тиімді болмайды.

Жақсы кибергигиенаны қалай қамтамасыз ете аласыз?

Жеке адамдар үшін кибергигиенаның екі маңызды аспектісі – күнделікті тәртіпті немесе әдеттерді қалыптастыру және дұрыс құралдарды пайдалану. Олардың әрқайсысын кезекпен қарастырайық.

- *Әдеттегі тәртіп немесе әдеттер:*

Кибергигиена – бұл бір реттік іс-шара емес, оны үнемі жасау керек. Автоматты еске салғыштарды орнату немесе әртүрлі тапсырмалар үшін күнтізбелерге күндер қосу арқылы әдеттер жасауға болады.

Бұған: антивирустық бағдарламалық жасақтаманы пайдаланып вирустарды тексеру, парольдерді өзгерту, қолданбаларды, бағдарламалық жасақтаманы және операциялық жүйелерді жаңарту және қатты дискіні тазарту кіруі мүмкін. Кибергигиенаны мұқият сақтағаннан кейін ғана ол жеке киберқауіпсіздік режимнің бір бөлігі болады.

- *Дұрыс құралдарды пайдалану:*

Оларға мыналар жатады:

Желілік брандмауэр – бұл рұқсат етілмеген пайдаланушылардың веб-сайттарға, электрондық пошта серверлеріне және Интернеттен кіруге болатын басқа ақпарат көздеріне кіруіне жол бермейді.

Деректерді жою бағдарламалық құралы – жаңа бағдарламалық құралды енгізгенде, аппараттық құралды қосқанда немесе жүйелік файлдарды өзгерткенде, жеке деректерді жоғалту қаупі бар. Деректерді тазалау бағдарламалық құралын пайдалану қажет емес деректерді жоюға және оны қатты дискіден толығымен өшіруге мүмкіндік береді.

Құпия сөз менеджері – сіз үнемі өзгертетін күшті, күрделі құпия сөздерді пайдалану интернет гигиенасының маңызды аспектісі болып табылады. Құпия сөз менеджерін пайдалану бірнеше құпия сөзді бақылауға көмектеседі.

Құрылғыларды автоматты түрде сканерлеуді жоспарлайтын және орындайтын, зиянды бағдарламалық құралды анықтайтын және жоятын,

сондай-ақ бірқатар онлайн қауіп-қатерлер мен қауіпсіздік бұзушылықтарынан қорғайтын жоғары сапалы антивирустық бағдарламалық құрал.

Кибергигиенаны сақтау цифрлық ортаны жақсы күйде ұстауға көмектеседі, себебі бұл бағдарламаларды жаңартып отыруға кепілдік береді. Ескірген бағдарламаларда хакерлер пайдалана алатын осалдықтар болуы мүмкін, яғни қауіпсіздік мәселелерін шешу үшін веб-қосымшалар, мобильді қосымшалар және операциялық жүйелер үнемі жаңартылып отыруы тиіс. Тұрақты жаңартуларда кемшіліктерді жою үшін бағдарламалық жасақтаманың жаңа түзетулері бар. Жабдықты жаңарту өнімділік мәселелерін болдырмауға көмектеседі.

Кәдімгі антивирустық тексеру проблемалар туындағанға дейін олардың алдын алуға көмектеседі. Тиісті қызмет көрсету кезінде цифрлық активтер тұрақты онлайн қауіптерден қорғалады. Бұл сонымен қатар файлдарды фрагменттерге бөлуден қорғайды, бұл деректердің жоғалуына әкеледі.

Адамдар кейде ескі компьютерлерді қалай қауіпсіз тастауға болатынын ойлайды. Егер сіз жұмыс үстелін, ноутбукты, планшетті немесе смартфонды сатсаңыз немесе одан құтылсаңыз, сіздің жеке немесе құпия деректеріңіз үшінші тұлғаларға берілмейтініне көз жеткізу маңызды. Жеке файлдарды немесе деректерді жою жеткіліксіз – қатты дискіні қайта пішімдеп, содан кейін толығымен өшіру керек. Бос қатты диск жеке ақпараттарды үшінші тұлғаларға берілмейтіндікті білдіреді.

Кибергигиенаны сақтау үшін:

- Жеке гигиена сияқты, оның тиімді болуы үшін кибергигиенаны үнемі қолдану керек екенін есте сақтау;
- Өзіңізді қорғағаныңызға көз жеткізу үшін осы кибергигиенаны тексеру тізімін пайдалану.

Тиісті кибергигиенаны қамтамасыз етуде нұсқауларды орындағаныңызға көз жеткізу үшін белсенді пайдалануға болатын жеке киберқауіпсіздік бақылау тізімі:

- Парольдердің сақталуын қамтамасыз ету;
- Әртүрлі есептік жазбалар үшін бірдей құпия сөзді пайдаланудан аулақ болу;
- Парольдерді үнемі өзгерту;
- Парольдердің ұзындығы кем дегенде 12 таңбадан (және одан да көп) тұруы;
- Парольдердің үлкен және кіші әріптер мен таңбалар мен сандардың тіркесімінен тұруы;

Парольдердің айқын болатындай нәрселерден – мысалы, реттік нөмірлерді («1234») немесе туған күні немесе аты-жөнің сияқты болжай алатын жеке ақпаратты пайдаланудан аулақ болу;

- Парольдерді жазудан немесе басқалармен бөлісуден аулақ болу;

Мен барлық құпия сөздерді бір қауіпсіз онлайн тіркелгіде жасауға, сақтауға және басқаруға көмектесетін құпия сөз менеджерін қолдану;

- Көп факторлы аутентификацияны қолдану;

- Электрондық пошта, әлеуметтік медиа немесе банктік қосымшалар сияқты барлық негізгі есептік жазбалар Google Authenticator немесе Authy сияқты қосымшалар арқылы көп факторлы аутентификациямен (MFA) қорғалған болуы.

Деректердің тұрақты сақтық көшірмесі

- Файлдарды қауіпсіз сақтау және оларды сыртқы қатты дискіде немесе бұлтта режимде маңызды файлдардың сақтық көшірмесін жасау арқылы деректердің жоғалуынан сақтау;

Құпиялылықты қамтамасыз ету

- Әлеуметтік желілерде үй мекенжайы, жеке фотосуреттер, телефон нөмірі немесе несие картасының нөмірлері сияқты жеке ақпаратты жарияламау;

- Әлеуметтік желілердегі құпиялылық параметрлерін қарап шығу және олардың жайлы сезінетін деңгейге қойылғанына көз жеткізу;

- Құпия жеке ақпаратты сұрайтын викториналардан, ойындардан немесе әлеуметтік желілердегі сауалнамалардан аулақ болу;

- Қолданатын барлық қосымшалар үшін қабылдайтын рұқсаттардан сақ болу;

- Компьютер мен телефонды құпия сөзбен немесе PIN кодымен құлыптау;

- Жалпыға Ортақ Wi-Fi желісін пайдалану кезінде жеке ақпаратты жарияламауға тырысу;

- Виртуалды жеке желіні немесе VPN-ді пайдалану, әсіресе Жалпыға Ортақ Wi-Fi -ды пайдалану;

- Жасаған барлық онлайн транзакциялар URL мекен-жайы <http://> емес, <https://>-ден басталатын қауіпсіз веб-сайт арқылы жүзеге асырылатындығына көз жеткізу және мекенжай жолағының сол жағында құлып белгішесін қою;

- Олардың қауіпсіздігін қамтамасыз ету үшін отбасыммен және достарыммен интернеттегі құпиялылық туралы ақпаратпен бөлісу;

- Қолданбаларды, бағдарламалық жасақтаманы және кіріктірілген бағдарламалық жасақтаманы жаңартып отыру

Қауіпсіздік ақауларын шешетін немесе түзететін соңғы нұсқаларды пайдалану үшін қолданбаларды, веб-шолғыштарды, операциялық жүйелерді және ендірілген Бағдарламалық құралды үнемі жаңартып отыру;

- Мүмкіндігінше бағдарламалық жасақтаманы автоматты түрде жаңартуды қамтамасыз ету үшін мүмкіндіктерді конфигурациялау;

- Керексіз, енді қолданбайтын қолданбаларды жою;

- Қосымшаларды тек беделді немесе ресми көздерден жүктеу;

Маршрутизаторларды қорғау

- үйдегі Wi-Fi үшін әдепкі атауды өзгерту;

- Маршрутизатордың пайдаланушы аты мен құпия сөзін өзгерту;

- Микробағдарламаны үнемі жаңартып отыру;

- Қашықтан қол жеткізуді, әмбебап қосылымды және Wi-Fi қорғанысымен орнатуды өшіру;

- Маршрутизаторым желі арқылы жіберілетін ақпараттың құпиялылығын қорғау үшін WPA2 немесе WPA3 шифрлауды қолдайтынына көз жеткізу;

Әлеуметтік инженерлік шабуылдардың алдын алу

- Күдікті сілтемелерге немесе сенімді емес сілтемелерге өтуден аулақ болу;
- Күдікті болып көрінетін электрондық хаттарды ашудан аулақ болу;
- Күтпеген электрондық пошталардан немесе мәтіндік хабарламалардан күдікті тіркемелерді жүктеуден аулақ болу;
- Тегін ақша, сыйлықтар немесе жеңілдіктер уәде ететін жарнамаларды баспау;

Желілік брандмауэрлерді пайдалану

- Зиянды бағдарламалық жасақтаманың компьютерге немесе желіге Интернет арқылы кіруіне жол бермеу үшін брандмауэрді қолдану;
- Брандмауэрдің дұрыс орнатылғанын тексеру;

Шифрлау құрылғылары

Ноутбуктер, планшеттер, смартфондар, алынбалы дискілер, сақтық көшірме таспалары және бұлтты сақтау сияқты құпия деректері бар құрылғылар мен басқа медианы шифрлау.

Қатты дискілерді тазалау

- Компьютерді, планшетті немесе смартфонды тастамас бұрын немесе сатпас бұрын, бөгде адамдардың кез келген жеке ақпаратқа қол жеткізуіне жол бермеу үшін қатты дискіні міндетті түрде тазалау.

Жоғары сапалы антивирустық қорғауды қамтамасыз ету

Компьютерлік вирустарды және басқа зиянды бағдарламалық жасақтаманы сканерлейтін және жоятын жоғары сапалы антивирустық бағдарламалық жасақтаманы қолдану;

- Антивирустық бағдарламалық жасақтаманы үнемі жаңартып отыру;

Қорытындылай келе, кибергигиена компьютерді немесе мобильді құрылғыны пайдалану кезінде жеке және қаржылық ақпараттардың қауіпсіздігін қамтамасыз ету үшін қорғаныс процедураларын әзірлеуді білдіреді. Күшті құпия сөздерді пайдалану және оларды үнемі өзгерту, бағдарламалық жасақтама мен операциялық жүйелерді жаңартып отыру, қатты дискілерді тазалау және Kaspersky Total Security сияқты кешенді антивирусты пайдалану киберқауіптерден бір қадам алда болуға көмектеседі.

Сонымен интернет біздің өміріміздің бір бөлігіне айналды. Біз бұған дейін Бүкіләлемдік ғаламторсыз қалай жүргенімізді елестете алмаймыз. Соңғы жылдары біз интернеттің және онда ұсынылатын қызметтердің өте қарқынды дамуын байқаймыз. Біз әлеуметтік желілерде сөйлесеміз, интернет-дүкендерде сауда жасаймыз, соңғы уақытта онлайн презентациялар мен вебинарларды жиі өткіземіз және оларға қатысамыз. Біз іс жүзінде онлайн режимінде өмір сүреміз. Бірақ біз желідегі деректердің қауіпсіздігі мен құпиялылығын жиі ұмытып кетеміз. Керекті ақпаратты әдеуметтік желіден іздеуге, сол жерден

табуға тырысамыз және іздегенімізді сол жерден табамыз да. Сондықтан көптеген адамдар, ұйымдар, компаниялар біз туралы ең көп ақпаратты жинауға тырысады. Мысалы: біздің әдеттеріміз, нені жақсы көретініміз, немен айналысатынымыз, не жейтініміз және не сатып алғымыз келетіні туралы.

Бір кездері құпияларды сақтау өте оңай болды. Сіз оларды ешкіммен бөліспейтінсіз де. Ал қазіргі уақытта ешкімге айтқымыз келмейтін ақпаратты компьютерлер мен мобильді құрылғылардағы қолданбалар арқылы браузер қосымшасында жинайды. Сондықтан интернеттегі құпиялылыққа әр адамның өзі қамқорлық жасауы тиіс. Күдікті сілтемелерді баспаңыз, VPN жүктеңіз, сонымен қатар шифрлауды, күшті парольдерді қолданыңыз.

Жеке деректердің желіде сақталуын қамтамасыз етуге көмектесетін қауіпсіздіктің қарапайым тәсілдерін ұсынуға болады:

1. Мессенджерлерде шифрлауды қолданыңыз

Біз әлеуметтік желілерде және әртүрлі мессенджерлерде жиі сөйлесеміз. Біз жеке өмірдегі оқиғалар туралы сөйлесеміз, жұмыс мәселелерін талқылаймыз, ақпаратпен, соның ішінде электрондық поштамен, телефон нөмірлерімен немесе басқа мәліметтермен алмасамыз. Бірақ бұл үнемі қауіпсіз бола бермейді. Біздің мессенджер арқылы жіберетін деректерімізді ұстау хакерлер үшін, сондай-ақ бөгде адамдардың әрекеттері үшін өте оңай және бұл олар үшін тамаша пайда. Бірақ әрқашан да шешім бар.

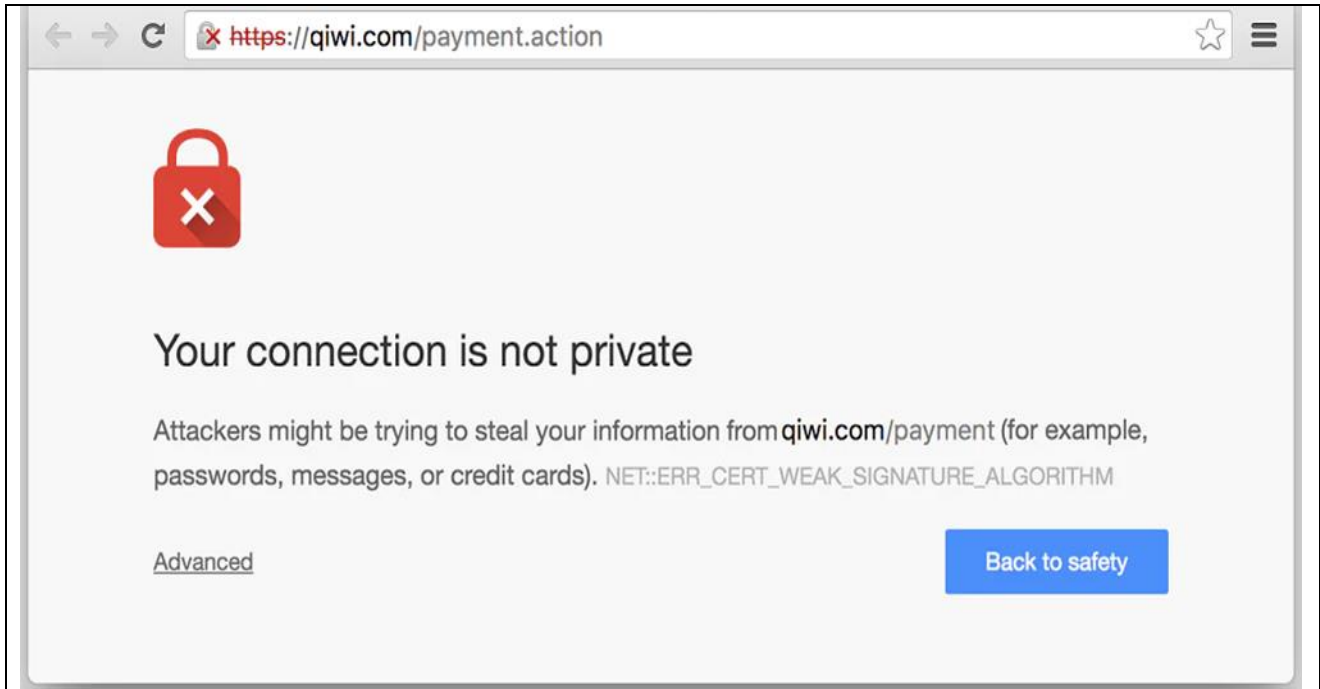


Шифрлау – құпия деректерді қорғаудың тиімді әдісі. Оны деректерді қорғау үшін ғана емес, жеке мәтіндік сөйлесулер кезінде де қолданған жөн. Сізге тек signal, Viber, Telegram және басқалары сияқты шифрланған мессенджерді пайдалану керек. Егер мессенджерде деректерді шифрлаудың ешқандай әдісі болмаса, онда оны қолдануға болмайды.

2. Сілтемелерді басу және Интернеттен алынған құжаттарды ашу

кезінде абай болыңыз!

Кейде адамның немқұрайлылығы көбінесе құрылғыларға вирустар жұқтыруға әкеледі. Әрине, бұл смартфон мен ноутбуктың жұмысындағы ақауларға ғана емес, сонымен қатар жеке деректердің жоғалуына әкеліп соқтырады.



Интернеттегі құпиялылықты веб-сайттарды қарау кезінде сіздің деректеріңізді қорғайтын құралдар арқылы ғана алуға болмайды. Егер біз желіде қауіпсіз болғымыз келсе, ең алдымен электрондық поштаны қорғауымыз керек. Оны жеке мақсатта пайдаланасыз ба, әлде бұл корпоративтік e-mail ма маңызды емес. Ол арқылы деректерді ұрлайтын өте жағымсыз вирустар компьютерге әсер етуі мүмкін.

Банк клиенттері көбінесе электрондық пошта шабуылдарының құрбаны болады. Хакерлер әйгілі банк мекемесіне және олардың хабарламасын немесе оған қосымшасын ашу ауыр зардаптарға әкелуі мүмкін. Жеке немесе кәсіпорын деректеріне де қатысты, сондықтан жіберілген сілтемелерді немесе тіркемелерді ашқанда мүмкіндігінше мұқият болу керек.

3. Компьютердің дискісін қорғаңыз

Үйдегі немесе жұмыс ноутбугының қатты дискісінде біз фотосуреттерді, жеке деректерді ғана емес, сонымен қатар жұмысқа байланысты файлдарды да сақтаймыз. Әрине, олардың үнемі тұтастық пен қауіпсіздікте болғанын қалаймыз және оларға тек біз ғана қол жеткізе аламыз. Сондықтан компьютердің қатты дискісі де белгілі бір қорғауды қажет етеді.



BitLocker-дің кіріктірілген шифрлау мүмкіндігін қолдануға болады. Орнату және пайдалану үшін өте қарапайым. Бұл мүмкіндікті қосып, оны пайдалануды бастау үшін бірнеше минут жеткілікті. Bitlocker көмегімен деректер міндетті түрде қорғалады. Енді ноутбук дискісіне кіру шифрланады және оны белгілі бір құпия сөзді енгізу немесе USB кілтін пайдалану арқылы ғана алуға болады. Желіде қол жетімді үшінші тараптың қатты дискіні шифрлау құралдары бар, бірақ BitLocker амалдық жүйеде бар.

4. Әлсіз құпия сөздерден аулақ болыңыз!

Интернеттегі деректерді қорғау үшін жасай алатын ең оңай нәрселердің бірі- күшті құпия сөздерді пайдалану және оларды ақылмен пайдалану. Сізде әр сайт үшін бөлек құпия сөз болуы керек.



Жақсы құпия сөзді табу қиын емес. Тек әріптерден немесе сандардан тұратын біреуін бұзу арнайы таңбалардан гөрі оңайырақ. Құпия сөздерді мүмкіндігінше қиындатыңыз. Дегенмен, барлық жерде бір құпия сөзді пайдаланбаңыз, себебі хакер оны бұзса, ол сіздің барлық қызметтеріңізге қол жеткізе алады.

Көптеген құпия сөздердің арасында жоғалып кетпеу үшін LastPass немесе KeePass және басқалары сияқты арнайы құпия сөз менеджерлерін қолданған жөн.

5. Екі факторлы аутентификацияны қолданыңыз

Көбінесе бұзудан немесе хакерлік шабуылдан қорғау үшін бір құпия сөз жеткіліксіз. Өзін және клиенттерді құрметтейтін барлық дерлік қызметтер ұзақ уақыт бойы екі факторлы аутентификацияны енгізді. Бұл жағдайда өз деректеріңізді тек парольмен ғана емес, мысалы, жаңа кірген кезде телефонға SMS-хабарлама жіберілетін арнайы кодпен қорғауды ұсынады. Осы авторизация схемасымен жеке деректерді ұрлау қиынырақ болады. Бұл сіздер үшін пайдалы функция.



Сонымен қатар, екі факторлы аутентификацияның арқасында деректерге қол жеткізуге тырысатын адам еңсерілмейтін кедергіге тап болады – ол үнемі өзімізбен бірге болатын телефон. Бұл әдіс электрондық пошта, әлеуметтік немесе жұмыс тіркелгілері үшін пайдаланылуы керек.

6. Қауіпсіз HTTPS протоколын пайдаланыңыз

Сіз кірген веб-сайттар қауіпсіз HTTPS протоколын қолданатынына көз жеткізген жөн. Бұл SSL шифрлау және сайт пен сіздің араңыздағы деректерді қауіпсіз бөлісу үшін қолданылатын арнайы http протоколының кеңейтімі.

Басқаша айтқанда, сайт өзі және оның иесі туралы барлық ақпарат бар сертификат алып, сенімділікке белгілі бір тексеруден өтті.



Әрине, қаскүнемдер өз сайттары үшін осындай сертификат алуға ауыртпалық түсірмейді, сонда да ол біз үшін қауіпті. Https протоколынсыз белгілі бір сайттарды ашқанда өте мұқият болу керек. Олар сіздің құрылғыңыз үшін қауіпті ғана емес, сонымен қатар сіздің деректеріңізді ұрлауы мүмкін.

Бірақ шешім бар болса да бұл хаттама үнемі тексерілмейді. Браузерге арнайы https Everywhere плагинін қосу жеткілікті, ол әр уақытта HTTPS қосылымын тексереді, әр сайтта шифрланған қосылымды қамтамасыз етеді. Бұл қосымша Chrome, Firefox, Opera және Android үшін қол жетімді.

7. VPN пайдаланыңыз

VPN технологиясы оның ішінде өтетін деректерді қорғайтын виртуалды туннель жасайды. VPN қызметін пайдалану кезінде біз не істеп жатқанымызды «көргісі» келетін кез келген адамға тек тасымалдау жүріп жатқаны және жалғасып жатқаны туралы хабарланады. Алайда, бұл виртуалды туннельде не болып жатқанын көру мүмкін емес.



Сіздердің көпшілігіңіз VPN қызметтерінің мүмкіндіктерін қолданыңыз. Олар тыйым салынған сайттарға, әлеуметтік желілерге немесе ресурстарға қол жеткізуге мүмкіндік беріп қана қоймайды, сонымен қатар біздің жеке деректерімізді қорғауға көмектеседі. Егер қоғамдық Wi-Fi желісін жиі қолдансаңыз, бұл құрал тиімді әрі пайдалы болады. VPN қосылымының арқасында тасымалданатын деректерді жергілікті желіде ұстау мүмкін емес.

8. Есіңізде болсын, инкогнито режимі мүлдем дербес емес

Инкогнито режимі – интернет пайдаланушысы аздап құпиялылыққа ие бола алатын қарапайым шешімдердің бірі. Оған кез келген дерлік браузерден қол жеткізуге болады. Өкінішке орай, жеке режимде де кейбір шектеулер бар. Жеке терезені пайдалану арқылы біз мүлдем көрінбейтін болмаймыз және өзімізді бақылаудан қорғамаймыз.

You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. [Learn more](#)

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible to**:

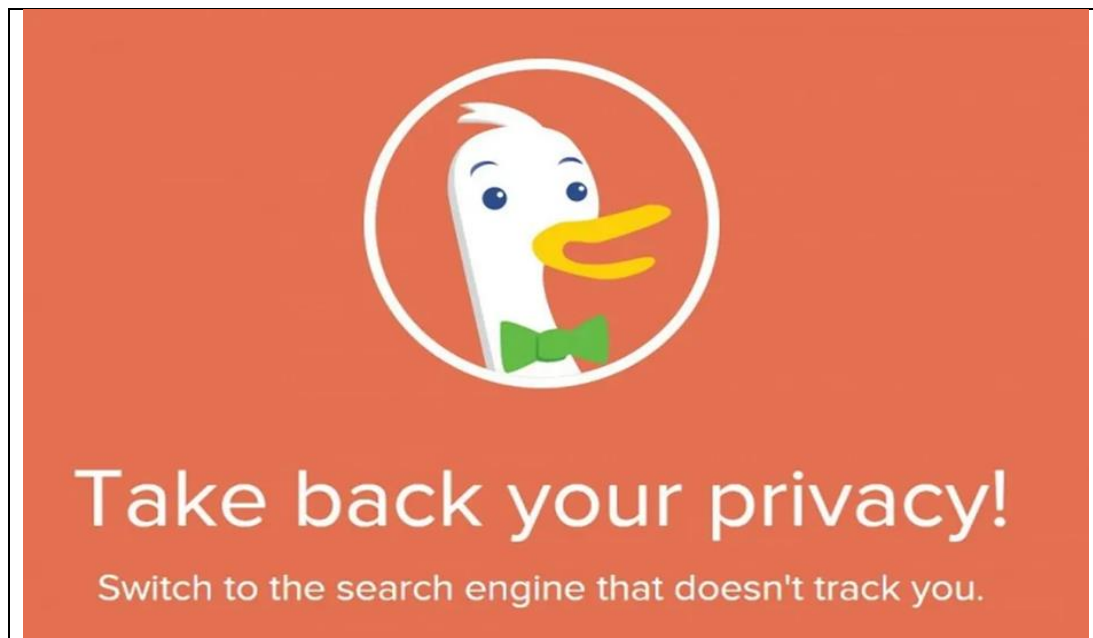
- Websites you visit
- Your employer or school
- Your internet service provider

Кәдімгі шолғышты инкогнито режимінде пайдаланған кезде, кірген ресурстар туралы деректерді жергілікті желі әкімшісі немесе интернет провайдері бақылай алатынын есте ұстаған жөн. Инкогнито режимі сіздің жеке өміріңізді қорғамайды, ол жай ғана орналасқан жеріңізді көрсетпейді немесе шолғыш тарихын сақтамайды. Дегенмен, веб-сайттарға қолжетімді болуы мүмкін жеке деректер көлемі азаяды.

Жақсартылған онлайн құпиялылық үшін Tor Browser сияқты арнайы браузерлерді пайдалану керек. Onion routing желісін пайдалану интернеттегі құпиялылықты мүмкіндігінше сақтауға мүмкіндік береді, дегенмен ол қауіпсіздікке 100% кепілдік бермейді.

9. Қауіпсіз іздеу жүйелерін пайдаланыңыз

Google іздеу жүйесінің танымалдығы туралы көп және ұзақ айтуға болады. Бірақ екінші жағынан, бұл ең «танымал» іздеу жүйелерінің бірі. Жеке деректердің легі ол үшін қарапайым болды.



Дегенмен, желіде анонимділікті қамтамасыз ететін DuckDuckGo түріндегі баламаны пайдалана аламыз. Бұл салыстырмалы түрде танымал іздеу жүйесі емес, бірақ ол біздің назарымызды аударуға лайық, өйткені интернеттегі құпиялылық тақырыбына көбірек адамдар қызығушылық танытады.

Желідегі жеке деректеріңіздің жүз пайыз қауіпсіздігіне кепілдік беретін әдістер болмаса да, жоғарыда сипатталған кеңестердің кем дегенде бірнешеуін іске асыру деректердің қауіпсіздік деңгейін айтарлықтай арттырады және желідегі кибершабуылдардың ең көп таралған түрлерінен қорғайды. Әр адамның өз қауіпсіздігі өзіне және өзінің зейініне байланысты.

2. Балалардың киберқауіпсіздігіне, кибергигиенасына және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша халықаралық және отандық тәжірибе

Қазіргі қоғамның алдында ақпараттық кеңістіктегі коммуникацияларды реттеу және пайдаланушылардың, әсіресе кәмелетке толмағандардың қауіпсіздігін қамтамасыз ету, оларда кибер этиканы дамыту міндеттері тұр.

Цифрлық әлемнің кез-келген жерінде, іс жүзінде, жалпы жауапкершілік қағидаты қолданылады: барлық адамдар не нәрсеге, не істеп жатқандарына, интернетте не жариялайтынына жауап береді.

Әлемдік қоғамдастықта интернеттегі моббинг пен буллингке қарсы күреске бағытталған заң жобалары әзірленген [10]. Германияда кибермоббинг жеке немесе азаматтық-құқықтық құқық бұзушылық болып саналады, бұл 5 жастан жоғары ересектер үшін ең жоғары жазаны тудырады. Жасөспірімдер, әдетте, аз жазаланады-10 күнге дейін қамауға алу немесе мәжбүрлеп түзету жұмыстары.

Ресей Федерациясындағы Азаматтық Бастама және әлеуметтік қызметтер оқу орындарындағы моббинг пен буллинг мәселесін түсініп, кеңес беру жұмыстарын бастады және Сенім телефондары ашылды (мысалы, Санкт-Петербург Үкіметінің Санкт-Петербург қаласының әлеуметтік саясат жөніндегі комитетінде).

Сонымен қатар, ВКонтакте.RU әлеуметтік желісінде – нақты уақыт режимінде кеңес алуға болатын «Анти-Кибермоббинг» (Anticybermobbing) тобы бар.

Алайда, Қазақстанда мобберлер/буллерлер мен кибермоббинг/кибербуллинг құрбандарын анықтайтын заңнамалық база жоқ. Кәмелетке толмағандар арасында осындай құбылыстардың алдын-алу үшін ата-аналар мен мұғалімдерді даярлау бағдарламалары жоқ.

Кәмелетке толмағандардың медиақұзіреттілік саласында балалармен жұмыс істейтін ата-аналардың, мұғалімдердің және басқа мамандардың білімін жетілдіру – кибермоббинг пен кибербуллингке қарсы күресте ең тиімді алдын-алу болуы мүмкін.

Түркия елінде киберқауіпсіздік пен қорғаныс саласындағы қарқынды даму процесінде болса да, киберқауіпсіздік зерттеулері жүргізіліп, оның жұмысы жоғары бағаланады:

- киберқауіпсіздік саласында мамандандырылған технопарктер құру және қолдау,
- инкубациялық киберқорғау орталықтарының санын көбейту,
- киберқауіпсіздік технологияларын өндіруге инвестицияларды ұлғайту,
- бірлескен сынақ орталықтарын құру,
- үлкен деректердің ашық орталарын құру және оларды зерттеушілер үшін ашу,

- жастар өз идеяларын ғылыми-зерттеу орталықтарында жүзеге асыра алатын жағдайлар санының артуы.

Киберқауіпсіздікті түсініп қана қоймай, айтылған мәселелерді және олардың маңыздылығын түсіну, ғылымның осы салаларында зерттеулер жүргізу, олардың арасындағы қатынастарды дұрыс түсіну және орнату, әлеуметтік желідегі бұзуақылықты анықтау және қорғаудың жаңа әдістерін әзірлеу үшін ең бастысы – олардың киберқауіпсіздікке қандай үлес қосатынын түсіну үшін жеткілікті хабардарлық деңгейіне ие болуы керек. Мысалы, шабуылды түсіну үшін криптология, математика, мінез-құлық ғылымдары, әлеуметтану, оқиғаларды басқару және қабылдауды басқару сияқты ғылымның әртүрлі салаларына қатысты жаңа шешімдерді, перспективаларды, тәсілдерді немесе технологияларды әзірлеу немесе пайдалану қажет.

Хабардарлықты арттыру үшін жасалған ұсыныстар:

1. Жаңалықтарды, қауіптер мен шабуылдарды, сондай-ақ қолданылатын әдістер мен технологияларды мұқият қадағалап отыру, олардың артында тұрған мотивация, қолданылатын әдістер мен әдіснамалар жақсы түсініліп, сәйкесінше шешім әзірленуі керек.

2. Жоғары оқу орындарында тереңдетілген зерттеулер, жобалар мен ғылыми жұмыстар жүргізілуі және оларды тәжірибеге енгізу керек.

3. Зиянкестердің мінез-құлқы айқындалып, талдануы керек, олардың мотивациясы нақты анықталуы керек, олардың қолданатын әдістері немесе ортасы бақылауға алынуы тиіс.

4. Қорғау шешімдері мен қорғаныс стратегиялары пайдаланушылардың мінез-құлқын, қателіктерін, осалдықтарын және/немесе білім деңгейін ескере отырып анықталуы керек.

5. Болашақта шабуылдар күрделірек болатынын, ғылымның әртүрлі пәндері мен салаларын қамтитынын, көптеген бірегей және техникалық емес шабуылдарды қамтитынын, ішкі топтық жұмысты қажет ететінін, ынтымақтастыққа негізделетінін, жоғары білімді қамтитынын және ең бастысы интеллектуалды шабуылдар болатынын, соның ішінде жасанды интеллектке деген көзқарастарды түсінетінін біле отырып, жан-жақты зерттеулер болуы керек. Әр салада білімді, тәжірибені және талантты кеңейтуге мүмкіндік беретін шешімдер әзірленуі керек.

6. Шешімді әзірлеу тәсілі – шабуыл мен шабуылдаушы туралы деректерді талдау.

7. Әлемдік киберқауіпсіздік сақтау және қолдау жұмыстары жүргізілуі керек.

8. Киберқауіпсіздікті қамтамасыз етудің маңызды кезеңдерінің бірі – тестілеу. Тұрақты бақылау тетіктері құрылуы, анықталған қауіптер тез арада жойылуы керек және ең бастысы болашаққа болжам жасау арқылы шаралар қабылдануы шарт.

9. Халықаралық ынтымақтастық кеңейтілуі керек.

10. Зерттеу жүргізуге болатын жаңа инфрақұрылымдар мен зертханалар құрылып, олардың жұмысын жандандыру.

11. Жаңа буын шабуылдарының алдын алу үшін, әсіресе ел ішінде, ұлттық шешімдер әзірленуі қажет.

12. Хабардарлық пен сананың жеткіліксіздігі, тәуекелдерді көре алмау немесе оларды елемей ең маңызды қауіп.

Адамдардың хабардарлығын арттыру үшін шаралар қабылдау керек, білім беру қызметіне үлкен мән беру керек, сәйкессіздік деңгейлерін тиісті түрде тексеріп, кемшіліктерді жою керек. Пайдаланушыларға тегін ұсынылатын «Қауіпсіз интернет қызметін» пайдалануға рұқсат етілуі керек.

13. Корпоративтік ақпараттық қауіпсіздік менеджерлері ең көп шағымданатын мәселелердің бірі – қызметкерлердің жетіспеушілігі, қызметкерлердің біліктілігінің жеткіліксіздігі, әртүрлі білім салаларына қажеттілік, қажетті көлемде талдаулар немесе сынақтарды орындай алмау, араласу тобындағы кемшіліктер.

14. Туындауы мүмкін кез келген қауіптерді немесе осалдықтарды біле отырып, ақпараттық қауіпсіздік пен киберқауіпсіздікке қатысты қажетті шараларды мұқият қабылдау және жоғарыда аталған мәселелерді жеке, корпоративтік немесе ұлттық жағымсыз жағдайлар жиі туындауы мүмкін екенін ескере отырып, шұғыл түрде шешу қажет.

Елдің киберқауіпсіздігі мен қорғанысын қамтамасыз ету – көп қырлы мәселе. Мұны қамтамасыз ету үшін инфрақұрылымнан бастап адам ресурстарына дейін активтерді жинақтаудан бастап меншікті құралдарға дейін, мүмкіндіктерді қалыптастырудан бастап инновациялық идеялар мен өнімдерді әзірлеуге дейінгі көптеген мәселелерді назарға алып, экожүйені құру қажет.

Жасанды интеллект көптеген салаларға – білімнен тәрбиеге, жоспарлаудан іске асыруға, жобалаудан өндіріске, стандарттардан сапаға, басқарудан бақылауға дейін – үлкен деректерді талдау, деректер туралы жаңа буынға ғылыми технологиялар мен тәсілдер арқылы әсер етеді, терең оқыту, кванттық есептеу, бұлтты есептеу, заттар интернеті, геймификация, криптология, стеганография, құпиялылықты қорғау, виртуалды валюта, 5G, IPv6, цифрлық егіз – барлығы мықты киберқауіпсіздік экожүйесін құру үшін қажет. Бұл экожүйенің маңызды элементтерінің бірі – SSB киберкластерлерін зерттеу. Бүгінгі таңда бұл жүйеге 127-ден астам компанияның қатысуы, сынақ орталығын құру, университет студенттеріне арналған жобалар байқауын ашу, тренингтерді жоспарлау, университеттермен ынтымақтастық және ортақ мақсаттарға жету нәтижесінде отандық және Ұлттық киберқауіпсіздік өнімдерін әзірлеу осы экожүйенің маңызды элементтердің бірі.

Салауатты экожүйені құру үшін;

- жақсы дамыған инновация мәдениеті;
- кәсіпкерліктің жоғары деңгейі;
- киберқауіпсіздік саласында ғана емес, сонымен қатар отандық және жалпыұлттық өндірістің көптеген салаларында;
- бүкіл әлеммен бәсекелесете;
- жергілікті жерде мемлекеттік қолдау мен ынталандыруды пайдалану;
- деректерден құндылық алу және оны экономикаға айналдыру;

- құрылымдарды құру немесе көбейту қажет.

Сонымен қатар, осы мақсаттарға жету үшін жалпы қадамдар жасау, процесті жеделдету, өнімді әзірлеуге күш салатын университеттер мен мекемелерге қолдау көрсету маңызды.

Әлемдік деңгейде қарасақ, жеке өмірді бұзу – бұл маңызды мәселе. Бұл сұрақ болашақтың ең үлкен проблемаларының біріне айналады. Деректерді жинау арқылы ақысыз қызмет көрсететін компаниялар бүкіл әлем бойынша деректерге ие, жеке адамдардан қоғамдарға, қауымдастықтардан ұлттарға қол жеткізе алады және жалпы модельдер жасайды. Дербес деректер заң шеңберінде қорғалғанымен, заң қабылданғанға дейін алынған деректер құпиялылықты бұзу одан да күрделі мәселелер тудыруы мүмкін.

Төменде мәселенің ауырлығын көрсететін кейбір әлемдік мысалдар келтірілген.

- Қытай әлемде өте танымал әлеуметтік медиа қосымшаларын ел ішінде пайдалануға рұқсат бермейді.

- Facebook кейбір елдерде бұғатталған, кейбір елдерде кіру бұғатталған. Cambridge Analytica жанжалы аясында 50 миллионнан астам пайдаланушының жеке деректері әртүрлі мақсаттарда пайдаланылды.

- IBM барлық қызметкерлеріне USB пайдалануға тыйым салды. Компания тек бұлтты жүйелер арқылы ақпарат алмасуға көшті.

- Ресей Telegram-ға тыйым салды.

- Германия онлайн-аудит туралы Заңға сәйкес барлық есептік жазбаларға қол жеткізе алады.

- Америка Құрама Штаттары 2017 жылдың желтоқсан айынан бастап әлеуметтік медиа және WhatsApp сияқты барлық байланыс қосымшаларын қадағалап келеді.

- Әлемдегі барлық профессор-оқытушылар құрамының электрондық пошта пайдаланушының мекен-жайы Интернетте жарияланды.

- Facebook, Uber және т.б. компания пайдаланушылары туралы ақпараттары Интернетте жарияланды.

- Еліміздің әрбір тұрғынының жеке ақпараты ашылды.

- Жеке және корпоративті деректердің көп бөлігі «қараңғы» немесе Интернетте беріледі.

- Әртүрлі зерттеу шаралары үшін AOL пайдаланушы идентификаторы мен IP мекенжайын ашу арқылы пайдаланушылардың белгілі бір санына тиесілі 20 миллион іздеу деректеріне қол жеткізуді қамтамасыз етті, бірақ бірнеше күн ішінде зерттеушілер бұл сұраулардың кімге тиесілі екенін анықтады.

Оқу-жаттығулар мекемелер, жүйелер мен елдердің кибершабуылдарға қарсы дайын болуы, шабуылдарға үйлестірілген түрде қарсы тұруы, әлсіз жақтары мен осалдықтарын алдын ала анықтауы, хабардарлықты арттыруы, мүмкіндіктерді біріктіруі және нығайтуы, туындауы мүмкін тәуекелдерді көруі және алдын ала сақтық шараларын қабылдауы үшін өткізіледі.

Біздің елімізде осы тұрғыда 4 ұлттық және 1 Халықаралық ілім өткізу тәжірибесі бар. Бұған қоса, әскери салада да жаттығулар өткізіледі. Олардың

соңғысы-НАТО-ның Киберкоалиция жаттығулары. Осы жаттығулардың көпшілігін бақылаған сарапшы ретінде мен бірінші жаттығулармен салыстырғанда мазмұны мен мүмкіндіктері, үйлестіру мен ынтымақтастық тұрғысынан жақсырақ және жан-жақты болғанын байқауға болады.

Осы уақытқа дейін өткізілген осындай іс-шараларда кездескен кейбір мәселелерді елдің институттары/секторы ескеруі керек. Олар мыналар;

- Топтық жұмыс, үйлестіру, ақпарат алмасу, әртүрлі және жана салалардағы сараптамалық білім қауіп-қатерге дайын болу үшін қажет болғандықтан, мүмкіндіктерді дамыту, әлеуетті арттыру, жаңа зерттеу инфрақұрылымдарын құру, бар инфрақұрылымдарды жақсарту және ең бастысы көптеген әртүрлі пәндер бойынша әлеует пен қабілеттерді жинақтау қажет;

- Интернетке қосылу кезінде қауіп немесе шабуыл кез келген уақытта туындауы мүмкін немесе жүйелерге нұқсан келуі мүмкін екенін түсініп, бүкіл әлемге ашық мақсат бар екенін түсіну үшін шаралар қабылдау керек;

- Корпоративтік/салалық аспектілерге үлкен мән беру, командаларды оқыту, мүмкіндіктерді кеңейту, әлеуетті арттыру және ең бастысы, әрбір мекеме / компания өз құрылымында кейбіреулерін құруы тиіс;

- Кез келген анықталған ашық бұзушылық, алынған шабуыл, туындаған қауіп туралы USOM-ға хабарлау немесе үйлестіру керек;

- Дағдарыс жағдайында байланыс пен құпиялылықты бұзбай сақтау маңызды болғандықтан, ең алдымен қажетті жоспарлау жүргізілуі керек.

- Сыни салаларда көбірек академиялық зерттеулер жүргізу керек. Жеке, корпоративтік және ұлттық қауіпсіздікті бұзатын ақпарат жарияланатын басылымдарға енгізілмеуі керек екенін атап өткен жөн;

- Киберқауіпсіздік бойынша оқу орталықтарын құру, университеттер-аландар-секторлар-мекемелер бірлесіп жұмыс істей алатын орта құру қажет;

- Түркия елінде ұлттық хабардарлықты арттыру және ілімдерді кеңірек уақытқа тарату үшін «ұлттық киберқауіпсіздікті қорғау айы» деп жариялануы тиіс.

Киберқауіпсіздік пен қорғаныстың тиімді әлеуетін құру деректерді талдауға, түсіндіруге, заңдылықтар мен қорытындыларды алуға, нәтижелерді алуға және осы деректерден құндылық алуға байланысты. Бұл бағыттағы ең маңызды қадам деректердің анонимді болуы, ашық деректерге айналуы және пайдалануға қол жетімді болуы.

Киберқауіпсіздік пен қорғаныс қазіргі білім, талант, әлеует, Инфрақұрылым, технология, заманауи әдістер, білікті адам ресурстары сияқты көптеген тақырыптарды қамтиды.

Интернет қазіргі уақытта компьютерлер ғана емес, сонымен қатар дамып келе жатқан технологиялары бар барлық электрондық құрылғылар бір-біріне қосылып, қоғамға ұсына алатын кең көлемді кеңістік.

Пайда болған мүмкіндіктердің нәтижесінде пайдаланушылар саны үнемі өсіп келеді және бұл адамдар мен құрылғылар арасында лайықты өзара әрекеттесетін үлкен киберкеңістікті ортаға айналды.

Бүгінгі таңда Интернет пен әлеуметтік желілер арқылы жасалған киберқылмыстар мен шабуылдардың саны, олардың қолданушылары миллиардқа жетеді, бүкіл әлемде өсуде. Осы себепті қоғамның киберқауіпсіздік және әлеуметтік медианы пайдалану туралы сауаттылығын арттыру маңызды.

Екінші жағынан, хабардарлықты арттыруға қоғамның барлық салаларына білім беру және 2023 жылға дейінгі білім беру тұжырымдамасында көрсетілгендей институционалдық ынтымақтастық арқылы экожүйе құру арқылы қол жеткізуге болады. Киберқауіпсіздік саласында да, әлеуметтік медианы пайдалану саласында да провинциялық ұлттық білім басқармасы ұйымдастырған білім беру инфрақұрылымын деконструкциялауды қолдау және күштердің бірлігін қамтамасыз ету үшін қажетті білімі мен тәжірибесі бар сарапшылармен біріктіруге бағытталған. Болашағымызды қалыптастыратын және жаңа ұрпақты тәрбиелейтін мұғалімдеріміз үшін киберқауіпсіздік туралы хабардарлықты арттыру үшін киберқауіпсіздік және әлеуметтік медианы дұрыс пайдалану бойынша семинарлар ұйымдастырып, өткізу тиімді. Еліміздегі кибер соғыс әлеміндегі киберқауіпсіздік туралы хабардарлықты арттыру.

Педагогтер мен білім алушыларға арналған тренингтер, семинарлар мен кездесулер және т.б. әлеуметтік желілердің аккаунттарында туындайтын жеке және әлеуметтік шабуылдың алдын алу және мұғалімдеріміздің дайындығын арттыру мақсатында хабардарлықты арттыру бойынша тренингтер өткізу маңызды. Стамбул провинциясының ұлттық білім басқармасы ретінде киберқауіпсіздік және әлеуметтік медианы саналы түрде пайдалану бойынша іс-шаралар ұйымдастырылады. Киберқауіпсіздік және әлеуметтік медианы дұрыс пайдалану бойынша семинарлар өз нәтижесін беріп жатыр.

Сонымен қатар ата-аналарға қолдау көрсету үшін технологияны дұрыс пайдалану «Интернетті қауіпсіз пайдалану» және «Кибербуллинг» деп аталатын ата-аналарға арналған нұсқаулықтар әзірленіп, ата-аналарға семинарлар өткізу маңызды.

Балаларға көшеде жүру ережесін, жүзуге, велосипедпен жүруге үйрететінінз сияқты, олар цифрлық әлемде қауіпсіз қозғалуы үшін ақпараттық коммуникация құралдары мен интернетті қауіпсіз пайдалануды үйрету керек.

«Қауіпсіз интернет нұсқаулығы» балалардың Интернетке кіруіне тыйым салу оларды дамытудың және бейімделудің тиімді әдісі емес, оның орнына технологияны тиімді, орынды және жауапты пайдалануға бағытталуы керек екенін түсіндіріледі.

Нұсқаулықта отбасыларға балаларға бағыт-бағдар беру үшін «Ақпаратқа ие болыңыз, өзекті болыңыз, жалпы жайлы аумақтарды құрыңыз, қауіпсіздік шараларын қолданыңыз, саналы түрде әрекет етіңіз, балаңызға үлгі болыңыз» деген сияқты ұсыныстар ұсынылады.

Кибербуллингке арналған нұсқаулықта Интернет желісінде кибербуллинг пен қорлау жағдайында отбасылар ұстануға болатын дұрыс әдістер бар. Киберқауіпсіздік әсерінің ерекше белгілері туралы нұсқаулықта отбасыларға балаларының мінез-құлқындағы өзгерістерді бақылау ұсынылады.

Нұсқаулық сонымен қатар интернеттегі қауіпсіздікті қамтамасыз етудің ең жақсы стратегиясы балалармен қарым-қатынас жасау екенін атап көрсетеді.

Білім алушыларға академиялық қолдау көрсетумен қатар, олардың психологиялық денсаулығы мен ата-аналарының денсаулығын қорғауға үлкен мән беретіндігін айта отырып, ата-ана сауаттылығын арттыру мақсатында іс-шаралар жүргізу жоспарланған. қолданылатын нұсқаулар бердік. Біз сондай-ақ квадрат кодтар арқылы қол жеткізуге болатын бейнелер арқылы әңгімелерді қолдадық. Бүгінгі таңда мектеп пен отбасының ынтымақтастығын дамытуды жалғастыру және барлық мүмкіндіктерді пайдалана отырып, балалар бен ата-аналардың кибермәдинетін дамыта отырып, жағымды әдеттерге тәрбиелеу басты мақсат болып табылады.

Ttofi мен Farrington өздерінің мета- талдауларында буллингпен күресудің ең тиімді компоненттерін көрсетеді: психологтардың немесе мұғалімдердің ата-аналармен тұрақты кездесулері (бағдарламаны енгізу кезеңінде кемінде айына/триместрде бір рет), оқыту тренингтерін өткізу, мектеп және балалар өкілдерімен қарқынды жұмыс жасау, бағдарламаның ұзақтығы, жұмысқа тәртіптік әдістерді енгізу және т.б.. Сонымен қатар, мектеп пен мектеп аумағын бақыласа, сыныпты басқарудың (classroom management) жаңа формалары пайда болады және мектептегі буллинг саясаты талқыланып, қабылданған бағдарламалар нәтижесінде мектептегі буллинг жағдайларының жиілігі төмендейді.

Жоғарыда айтылғандай, буллингпен ғана күресу емес, кез келген девиантты немесе агрессивті мінез-құлықпен күресуге бағытталған бағдарламалар да өте көп. Ttofi мен Farrington бағдарламаның әсер ету бағыты

«тәртіптік әдістер» және «құрдастармен жұмыс» барысын түсіндіруде өзгеруі мүмкін деп санайды. Мысалы, ОВРР үшін тәртіптік әдістер жасөспірімдердің мінез-құлқын бақылауды қамтиды, ал Friendly Schools үшін тәртіп мектеп климатын жақсартуға бағытталған – оларда көбінесе әртүрлі тактика бар. Бақылауды мектеп климатын жақсартатын тәжірибе ретінде қарастыру аздық етеді. Бүгінгі күні нақты мектеп ережелерінсіз тәртіпті сақтау мүмкін емес деп болжауға болады, ал ережелердің ашықтығы мен анықтығы мектеп климатының көрсеткіштерін міндетті түрде жақсартады. Сонымен бірге, ОВРР мектеп климатының өзгеруі, оның жақсаруы мектептегі қорлаудың таралуын төмендетеді дегенді білдірмейді.

Келесі бөлімде метаталдау деректерін пайдалана отырып, біз осындай жалпылау элементтерін бөліп көрсетуге тырысамыз.

Құрдастармен жұмыс

Жәбірленуші жасөспірімнің психологиялық әл-ауқатын қолдау және құрдастар үшін әлеуметтік орта құру схемалары қорлау жағдайларымен күресудің танымал әдістері болып табылады. Көптеген мектептер – егер оларда буллингке қарсы толыққанды жұмыс істейтін бағдарлама болмаса - қазір бұл әдісті негізгі әдіс ретінде қолданады. Мысалы, Ұлыбританияда 2007 жылдың өзінде мектептердің 62%-ы оқушыларды қақтығыстарды жұмсақ шешуге

үйреткен. Сондай-ақ «белсенді достық» дағдыларын, яғни жасөспірімдердің өзара әрекеттесуін үйрету жиі кездеседі, олар: 1) бір-бірін құрметтеуге және басқаларға тең қарауға; 2) басқалардың жетістігіне қуану, 3) бір-бірін қорғауға ұмтылады, 4) көлгірсімеу және бір-бірін табиғи қабылдау; 5) адал және бірін-бірі өзгертуге ұмтылмайды. Бастауыш мектепте бұл дағдыларды ойын кезінде, үзіліс кезінде, сабақтардан кейінгі спортпен айналысуда үйретуге болады, орта мектепте жоғары сынып оқушыларының қатысуымен тәлімгерлік немесе кеңес беру кестелері жиі қолданылады. Ересек балалар алдын ала мектеп ішінде немесе сырттан келген мамандардың көмегімен курстардан өтеді.

Мысалы, KiVa жобасы құрдастардың қолдауын сәтті пайдаланады. Menesini, Nocentini және Palladino Noncadiamointrappola («Тұзаққа түсіп қалмайық») деп аталатын веб-жобаның екі зерттеуіне негізделген басқа табысты құрдастық қолдау кестесі туралы хабарлады. Бастапқыда білім алушылар қорлауға және әсіресе кибербуллингке қарсы контентті насихаттау үшін веб-сайт жасады. Сегіз орта мектепте жүргізілген тиімділікті бағалау, бағдарламаға қатысқандар арасында кибербуллинг деңгейі айтарлықтай төмендегенін (әсіресе ұлдар арасында) көрсетті.

Тәртіптік әдістер

Буллинг бастамашыларымен жұмыс істеудің тиімді жолдары туралы үнемі пікірталас жүріп жатыр. Тәртіптік жазаны қолдану және қолдау мектеп қауымдастығы үшін де, оқушылар ұжымы үшін де күрделі этикалық мәселе болып табылады. Сонымен қатар, ата-аналардың ұстанымы бар және егер білім беру процесінің барлық қатысушылары ресми түрде қабылдаған буллингке қатысты жалпы мектеп саясаты болмаса, онда буллинг бастамашыларының кез келген жазасы іс жүзінде заңсыз деп танылуы мүмкін.

Тәртіптік жаза тақырыбына әртүрлі көзқарастарды Rigby қорытындылады. 625 австриялық және неміс мұғалімдерінің арасында жүргізілген сауалнама көптеген адамдар жәбірленушіні өз құқықтарын қорғауға ынталандыруды (шын мәнінде бұл жәбірленушіні өзбетімен жазалауға шақыру) тиімді шара деп санайтынын көрсетті.

Garandeau, Poskiparta және Salmivalli 339 жағдайды талдағаннан кейін, Финляндиядағы KiVa бағдарламасы бойынша әртүрлі мектептерде қолданылатын «конфронтация» және «конфронтациясыз» әдістерді салыстырды. «Конфронтация» орта мектептерде біршама сәтті болды және қысқа мерзімде виктимизация деңгейін төмендетуі мүмкін. Буллингке қарсы әрекет етудің бұл әдісімен агрессор жәбірленушіге, мұғалімге немесе басқа ересек адамға қатысты жасаған әрекеті үшін жазаланады және қорлау әрекетінің дәлелін жасырмайды және қоғамда мұндай арандатуға жол берілмейтінін атап көрсетеді. «Конфронтациясыз» стратегия төменгі сынып білім алушыларына сәтті болды және ұзақ мерзімді перспективада тиімділігін көрсетті. Мұндай стратегияның әдістерінің бірі – медиация болып табылады, бұл қақтығысқан тараптарды жәбірленушілер мен бастамашылар деп бөлуге болмайды.

Смит баяндамасында Ұлыбритания мектептерінің 285 есебіне талдау жасады; оның мәліметі бойынша, әлеуметтік буллинг жағдайларына қатысты, бастамашыларға қарсы тікелей санкцияларының, қолдау топтарының әдістеріне қарағанда тиімділігі біршама төмен. Жетістік көрсеткіштерінің айырмашылығы орта мектептерде төмен болды, ал кибербуллинг жағдайында тікелей тәртіптік жазалар тиімділігін жақсы көрсете білді. Бұл зерттеулер қалпына келтіру тәсілдерінің (оңалту), әсіресе физикалық және ауызша буллинг кең таралған орта мектептердегі табыстылығын жоғары бағалады.

Қалыпқа келтіру тәсілдері (реабилитация)

Тікелей жазалау кейбір жағдайларда кері әсер етуі мүмкін болса да, жазаланбайтын тәсілдер жиі жәбірлеушіге өзін өзі қалағандай ұстауға нақты мүмкіндік береді деп айыпталады. Оңалту тәсілінің іргелі қағидасы – бастамашыға іс үшін жауапкершілікті қайтару, оған келтірілген зиян мен жәбірленушінің тәжірибесін білу. Сондай-ақ бастамашыға «жоғалғанның орнын толтыру» мүмкіндігін беру, яғни жәбірленуші шеккен материалдық, физикалық немесе психологиялық қысымның (шығынның) орнын толтыру маңызды. Буллинкті бастаған бала өз әрекеті үшін жауапты екеніне қарамастан, оның мектеп ережелерін бұзғаны және бұл жол берілмейтіні туралы емес, жәбірленушінің өзін қалай сезінгені туралы: «Сіз басқа адамды қаншалықты ренжіткеніңізді көресіз бе? Жағдайды түзету үшін не істей аласыз?»

Соңғы жылдары мектептерде оңалту әдісін қолдану кеңінен тарады. Гонконг мектептерінде оны пайдалануды бағалаудың үлгісін Wong, Cheng, Ngan and Ma ұсынған. Бақылау мектебімен салыстырғанда, осы тәсілді қолданатын эксперименттік мектеп буллинг жиілігінің айтарлықтай төмендегенін және жәбірлеу құрбандары мен қасында жүрген адамдарда эмпатия мен өзін-өзі бағалаудың жоғары деңгейін көрсетті.

Кибербуллинг мәселесі

Кибербуллинктің ерекшеліктері агрессордың анонимділігі және ықтимал құрбандардың көбірек қамтылуы болып табылады. Қорлайтын мазмұнды көру саны артқан сайын, құқық бұзушылардың саны да қарасы көп болуы мүмкін. Күнделікті өмірде (мектепте, көшеде, т.б.) құрбыларын қорлайтын мектеп оқушыларының да интернетте агрессивті әрекеттерге баратыны анықталды¹⁹. Сондықтан, жалпы қорлауды азайтудың кейбір шаралары (мысалы, эмпатияны үйрену, қақтығыстарды шешу жолдары, әлеуметтік мінез-құлық), тіпті олар негізінен қорлаудың дәстүрлі түрлеріне бағытталған болса да, кибербуллинг жиілігіне әсер етуі мүмкін. Финдік KiVa дәлелді зерттеу қорқытудың азаюы дәстүрлі буллинг сияқты кибербуллинг үшін де маңызды екенін көрсетті.

Кибербуллинктің алдын алу және төмендету ресурстары мен стратегияларына пайдалы шолулар Notar, Padgett and Roden және Ang ұсынады. Жасөспірімдердегі кибербуллинг контекстінде Ang эмпатияны үйрету және желідегі агрессияны қолдайтын сенімдерді өзгерту кибербуллинкті азайтуда ең тиімді болып саналады. Жалпы алғанда, көптеген елдерде кибербуллинг пен цифрлық қауіпсіздік нұсқаулары әзірленуде және балаларға, жастарға, ата-

аналарға және мектептерге кеңес беретін көптеген ашық дереккөздер бар (мысалы, Австралияда Friendly Schools).

Ата-аналар рөлі

Отбасылық қарым-қатынастардың ерекшеліктері білім алушының буллингке бастамашы немесе құрбан ретінде қатысу ықтималдығына қалай әсер ететінін көрсететін зерттеулер бар. Мысалы, ата-аналардың физикалық жазалау мен психологиялық агрессияны қолдануы мұндай отбасынан шыққан баланың мектептегі қорқытуға тартылуының алғышарты болуы мүмкін екені анықталды. Екінші жағынан, ата-аналар қорқытуға қарсы бастамаларды қолдай алады, білім беру және хабардар ету бойынша семинарларға қатысып, баланың мінез-құлқы мен психикалық денсаулығын мұқият бақылай алады.

Бұл талдау өз елдерінде үкімет деңгейінде сыналған және қолдау тапқан сегіз бағдарламаны қарастырады. Бұл бағдарламалардың көпшілігі OBPP бағдарламасына негізделген, бірақ ұлттық перспективамен мектептегі буллингті зерттеу нәтижесінде пайда болды. Америка Құрама Штаттарында Positive Action бағдарламасына жанама байланысты әлеуметтік-эмоционалды оқытумен жұмыс істеуге бағытталған бағдарламалар кең тарады.

Бағдарламалардың көпшілігі Ttofi & Farington белгілеген бағдарлама тиімділігінің критерийлері арқылы талданды. Біз тиімділік деп келесідегідей көрсеткіштерді түсінеміз:

- бағдарламаға апробация және жүзеге асыру кезеңінде буллинктің таралуының тұрақты төмендеуі;
- бағдарламаны пайдаланудың кешіктірілген нәтижелерін бағалаудың болуы;
- әдістемелік ұсыныстарды сипаттау;
- буллингке қарсы құралдарды енгізудің кешенді бағдарламасы.

Зерттелетін бағдарламалар аясында бағдарламаны іске асыру кезеңдері, процеске қатысушылардың әртүрлі санаттарымен жұмыс істеу ерекшеліктері және мектептегі буллинктің таралуының төмендеуі көрсеткіштеріне тікелей талдау жүргізілген.

Буллингке қарсы халықаралық бағдарламалардың салыстырмалы талдауы (OBPP, KiVa, Positive Action)

Бұл бөлімде біз әлемдегі ең кең таралған және кеңінен қолданылатын үш бағдарламаны толығырақ қарастырамыз: OBPP, KiVa және Positive Action. Олардың барлығы әлеуметтік-экономикалық даму көрсеткіштері жоғары елдерде дамығанын атап өткен жөн (Норвегия, Финляндия және АҚШ әл-ауқат пен өмір сапасы бойынша рейтингте жоғары көрсеткіштерге ие).

Olweus Bullying Prevention Programm (Д. Ольвеус қорқытудың алдын алу бағдарламасы) – бастауыш, орта және жоғары сыныптардағы буллингті азайтуға және болдырмауға арналған көп деңгейлі, көп құрамды бағдарлама. Бағдарламаның нақты мақсаттары:

- 1) оқушыларды мектептегі жәбірлеу туралы ақпараттандыру және білімін арттыру;

- 2) педагогтар мен ата-аналарды буллингтің алдын алуға тарту;
- 3) жәбірлеуге қарсы нақты ережелерді әзірлеу;
- 4) жәбірленушілерге қолдау мен қорғау көрсету.

Кесте 1. ОВРР негізгі компоненттері

Жалпы талап Мектеп жағдайына ересектерді тарту және хабардарлығын арттыру	
Мектеп деңгейі • буллингті үйлестіру және алдын алу комитетін құру • комитет пен мектеп қызметкерлері үшін тренингтер өткізу • мектеп бойынша Ольшеустің «Жасөспірімдер арасындағы агрессия» сауалнамасын жүргізу • қызметкерлер үшін пікірталас кездесулерін өткізу • буллингке қарсы жалпы мектеп ережелерін енгізу • мектептегі қадағалау жүйесін қайта қарау және жетілдіру • бағдарламаны іске қосу үшін мектепте бастау шарасын өткізу • ата-аналардың байланысы.	Жеке деңгей • мектеп оқушыларының белсенділігін бақылау (олардың оқу және мектептен тыс қызығушылықтары, үйірмелер, кәсіби хоббилері, спорт түрлері) • кез келген мектеп қызметкерінің буллинг жағдайын байқаған бойда оған араласуын қамтамасыз ету • мектептегі жәбірлеуге қатысатын мектеп оқушыларымен кездесулер өткізу (медиация) • мектептегі жәбірлеуге тартылған балалардың ата-аналарымен кездесулер ұйымдастыру • буллингке тартылған білім алушыларға арналған бағдарламаны жүзеге асырудың жеке жоспарларымен жұмыс жасау
Сынып деңгейі • барлық мектептерде буллингке қарсы ережені жариялау, тарату және сақтау • тұрақты сынып жиналыстарын өткізу • ата-аналар жиналысын өткізу	Қауымдастық деңгейі • буллингті үйлестіру және алдын алу комитетінің құрамына жергілікті қоғамдастық өкілдерін енгізу • мектептегі бағдарламаны қолдау үшін қоғамдастық мүшелерімен серіктестікті дамыту • басқа жергілікті ұйымдарға буллингке қарсы ақпараттарды, қағидаттар мен озық тәжірибелерді таратуға көмектесу



Сурет 1. Түрлі әлеуметтік топтармен буллингке қарсы жұмыс жасайтын ОБРР бағдарламасының кестесі

1-суретте әртүрлі әлеуметтік топтарды өз жұмысына тарту тұрғысынан бағдарламаның көрінісі жинақталған. Құрдастармен, жергілікті қауымдастықпен және жүйе ретінде мектеппен жұмыс істеуге үлкен мән беріледі. Бағдарлама отбасымен де, жалпы қоғаммен де жұмыс істейтініне қарамастан, аталған алғашқы үш санат бағдарламаны қолдауға және таратуға көбірек тартылғанын мойындау керек.

Д. Ольвеус бағдарлама жасау барысында жасөспірімнің виктимизациясы жағдайларының санын сәтті азайтудың негізі ретінде құрдастарымен жұмыс және мұғалімдермен жұмыс жасау идеясына толығымен сенді. Жергілікті қауымдастықтарға келетін болсақ, бұл бағдарламаны мектептен тыс жерде кеңейту мәселесі маңызды рөл атқарады. Әртүрлі елдерде бағдарламаны жүзеге асыруды мектептердің өзі емес, жасөспірімдермен жеке немесе топпен жұмыс істейтін мамандардың жұмысын қаржылай қамтамасыз ете алатын аудандық немесе қалалық жастар орталықтары өз мойнына алады.

Бағдарлама Норвегияда апробациядан өтті және кейінірек Құрама Штаттарда, Канадада, Англияда, Мексикада, Исландияда, Германияда, Швецияда, Хорватияда және т.б. мемлекеттерде қолданыла бастады. Бағдарламаның бірінші қолданылуы 1983 жылы бұқаралық жарнама арқылы басталған Норвегияның жалпы ұлттық буллингке қарсы науқаны және мектептерде сауалнама жүргізу, мұғалімдерге арналған материалдар (оқу

құралдары мен бейнедәрістер) және ата-аналарға арналған кеңестер болды. ОВРР бүкіл әлемге 2001 жылдан бастап тарай бастады.

KiVa («жақсы») – Финляндиядан шыққан мектеп бағдарламасы, ол 2006-2009 жылдары әзірленген және 2009 жылдан бері бұл елдегі мектептегі жәбірлеудің алдын алудың жалғыз бағдарламасы. Жобаның атауы «Kiusaamista Vastaan» сөзінің аббревиатурасы болып табылады, ол «жәбірлеуге қарсы» дегенді білдіреді. Фин тіліндегі «kiva» сөзі «жақсы» дегенді білдіреді және бұл акроним Финляндиядағы қорқытуға қарсы бастама үшін таңдалып алынған. Бағдарлама жалпы білім беретін мектептердің 5 жастан 11 жасқа дейінгі барлық оқушыларына қатысты. Оның мақсаты – мектептегі буллингті төмендету және құрдастар арасындағы виктимизация деңгейін төмендету. Құрдастармен жұмыс

– финдік бағдарламаның негізгі тақырыптарының бірі. Жәбірлеумен айналысатын тұлғалармен жұмыс істеу балалардың буллинг жағдайларын тану және ұжымның мүмкіндіктерін пайдалана отырып оған қарсы тұру қабілетін арттыру болып табылады.

Фин бағдарламасы буллинг оқиғаларының алдын алу бойынша әмбебап жұмыстарды да, мектептегі жәбірлеу жағдайларына араласу үшін арнайы жұмыстарды да қамтиды. Бағдарламаның үш түрлі жас ерекшелігіне бағытталған: балабақша, 1-3 және 4-6 сыныптар үшін нұсқалары бар.

KiVa-дағы нақты әрекеттерге буклеттерге қосымша ретінде бейне ойындар мен анимация сабақтарын пайдалану және мұғалімдермен байланыс кіреді. Сондай-ақ әр мектепте үш мұғалімнен тұратын топ (немесе мектептің басқа қызметкерлері) куә болған немесе анықталған әрбір буллинг жағдайын қарау үшін сынып жетекшісімен жұмыс істейді. Жағдай жәбірленушілермен және бастамашылармен жеке және шағын топтық талқылаулар арқылы, сосын жүйелі кездесулер ұйымдастырулар арқылы қаралады. Сонымен қатар, сыныпта мұғалім әлеуметтік беделі жоғары екі-төрт сыныптастарымен кездесіп, оларды зардап шеккен балаға қолдау көрсетуге шақырады.

Мектептегі буллингке қарсы әмбебап іс-шараға мұғалімдердің оқу жылы бойына сыныпта өткізетін 20 сағаттық білім алушыларға арналған сабақтары кіреді. Сабақтардың негізгі мақсаттары:

а) буллингті қолдаудағы топтық ойындар рөлі туралы хабардар болуды арттыру;

ә) жәбірленушіге қатысты жанашырлық сезімді арттыру; б) жәбірленушіні қолдау стратегияларын күшейту.

Сабақта талқылау, топтық жұмыс, рөлдік ойындар бар. Сабақ өткізу барысында сынып буллингті болдырмау, оның алдын алу және мектептегі буллинг жағдайларымен күресудің ішкі ережелерін әзірлейді.

KiVa бағдарламасы ОВРР-ден мақсатты топтар бойынша емес, бағыты бойынша ерекшеленеді. KiVa, ОВРР сияқты, құрдастарымен, оқытушылармен және жергілікті қауымдастықтармен жұмыс істеуге бағытталған. ОБПП-пен салыстырғанда, KiVa бағдарламасында педагогикалық ұжымды бағдарлама жұмысына қосу басқаша қағида ұстанады: білім беру мекемесіндегі буллингтің барлық жағдайларын қадағалайтын ресми бірлестік болмаған жағдайда, әр

сыныптағы жәбірлеу жағдайын үнемі қадағалау үшін шағын топтар құрылады. KiVa-да оқушылармен жұмыс интерактивті, сонымен қатар АКТ-ны сабақтарға қосу, бұл бағдарламаны бастауыш және орта мектептерде қолдану үшін тартымды етеді.



Сурет 2. Түрлі әлеуметтік топтармен буллингке қарсы жұмыс жасайтын KiVa бағдарламасының кестесі

Отбасымен және жалпы жергілікті қауымдастықпен жұмыс істеу KiVa үшін басымдық емес. KiVa ересек жасөспірімдермен жұмыс жасамайды, сондықтан ол мектептегі буллинг бастамашыларының әлеуметтенуіне баса назар аудармайды. Нәтижесінде, KiVa бүкіл қоғам деңгейіндегі қолдау шараларын ұсынбайды. Мемлекеттік ұйымдарды тартуға, оның ішінде қаржылық қолдауға бағытталған OBPP бағдарламасына қарағанда, бұл бағдарламаны қаржыландыру үшін жеке бастамалар қажет. Дегенмен, KiVa тиімділігі бойынша Норвегиядағы OBPP-ге ұқсас. Финдік бағдарлама ең жас болса да, таралуы бойынша американдық буллингке қарсы бағдарламадан (РА, төменде қарастырылады) айтарлықтай озып кетті. Қазіргі уақытта KiVa Жаңа Зеландия, Ұлыбритания, Швеция, Аргентина, Колумбия және басқа елдермен ынтымақтастықта жұмыс жасайды.

Positive Action, РА (жағымды әрекет) — АҚШ-та девиантты мінез-құлықтың көптеген түрлерімен, соның ішінде буллингпен айналысуға негізделген мультипәндік бағдарлама. Бағдарламаның KiVa және OBPP-тен айырмашылығы, оның бағыты мектептегі буллингке кез-келген девиантты мінез-құлыққа бағытталған. Бұл бастауыш және орта мектеп оқушыларына

арналған мектептегі әлеуметтік-эмоционалды оқыту бағдарламасы. Мұндағы жұмыстың нәтижесі әлеуметтік құпталған мінез-құлықтың артуы, девиантты мінез-құлық жағдайларының азаюы, әлеуметтік-эмоционалды оқыту дағдыларының және мектеп климатының көрсеткіштерінің жақсарту болып табылады.

Бағдарламаның тиімділігін растайтын алғашқы зерттеулер 2001 жылы пайда болды, ал 2015 жылы Чикаго мектептерінде ауқымды мониторинг жүргізілді, бұл оның тиімділігін тағы бір рет растады. Еуропалық буллингке қарсы бағдарламалардан айырмашылығы, Positive Action Америка Құрама Штаттарында сенімді болғанға дейін елдің әртүрлі штаттарында үлкен сынақтардан өткен.

РА бүкіл мектептегі климаттың өзгеруіне назар аударады және аптасына 2-4 рет «сабақтары» бар егжей-тегжейлі оқу бағдарламасынан тұрады – балабақшадан (4-5 жас) 6-сыныпқа дейін әр сыныпқа шамамен 10-15 минуттық

«сабақ»; 7-8 сыныптарда ұзақтығы 15-20 минут болатын тағы 82 «сабақ» енгізу жоспарланған. «Сабақтар» сценарий бойынша және жас ерекшеліктеріне сай жүргізіледі. Сабақты өткізуге қажетті барлық материалдар: плакаттар, қуыршақтар, музыка, ойындар және т.б. беріледі. Оқушыларға арналған материалдарға буклеттер, журналдар және басқа оқу құралдары кіреді. Бағдарламаның мазмұны алты блоктан тұрады. Бірінші блок бағдарламаның философиясы туралы айтады: жағымды және жағымсыз әрекеттердің табиғатымен таныстырады, әлеуметтік қолайлы және девиантты мінез-құлықтың түрлері туралы әңгімелейді. Сабақтардың келесі блоктары физикалық, интеллектуалдық, әлеуметтік және эмоционалдық салаларда жағымды әрекеттерге үйретеді.



Топтардың жұмысқа тартылу деңгейі



Сурет 3. Түрлі әлеуметтік топтармен буллингке қарсы жұмыс жасайтын РА бағдарламасының кестесі

Бағдарламаның ресми таратушылары ұсынған деректерге сүйене отырып, РА девиантты мінез-құлықтың әртүрлі түрлеріне қатысты неғұрлым мазмұнды болғанына қарамастан, ол отбасы құрамдас бөлігімен және жергілікті қауымдастықтармен жұмыс істемейді деп айтуға болады. Бұл ішінара бағдарламаның оқу жоспарын қайта қарауға және қоғамды білім алушылар тең болуы керек вектор ретінде қосуға көбірек бағытталғандығына байланысты (3-сурет).

Осы үш бағдарлама да XX ғасырдың 80 жылдары мен XXI ғасырдың басында жүргізілген ғылыми зерттеулердің негізінде пайда болды және олардың барлығы мектептегі буллингтің алдын алуда орташа және жақсы нәтиже көрсетті. Сонымен қатар, бағдарламалардың өздері аяқталғаннан кейін қайталанатын сынақтармен көрсеткіштер айтарлықтай өзгерген жоқ, бұл олардың маңызды тиімділігінің белгілерінің бірі болып табылады.

Әлемнің әртүрлі елдерінде жүргізілген сынақтар да буллингке қарсы кешенді тәсілдің тиімділігін көрсетті. Барлық үш бағдарлама өз нәтижелерін бағалау үшін меншікті әдістерді, соның ішінде: Д. Ольвеустың

«Бастамашы/жәбірленуші» сауалнамасы, мектептегі буллингке қатысушылардың рөлін анықтауға арналған сауалнама, буллинг құрбандарының мүдделері шкаласы, мектеп ортасын зерттеу және мінез-құлық шкаласын пайдаланды.

Қарастырылған үш бағдарламаны BluePrints агрегаторы бөлектеген параметрлер бойынша салыстыра отырып, айқын айырмашылықтарды көруге болады. Олар 2-кестеде берілген.

«Араласу ерекшелігі» - бағдарламаны іске асыру кезінде мүмкін болатын қосымша мақсаттарды болжауға мүмкіндік беретін бірегей көрсеткіш. Мамандар дайындаған материалдарға енгізілген «бағдарламалық фокустардан» айырмашылығы, «араласу ерекшелігі» қосымша әсер ету бөлігі ретінде жұмыс істейді. Яғни, KiVa сәтті енгізілсе, буллинг жағдайлары азаяды, мектеп оқушыларының мазасыздануы төмендейді, виктимизация мәселесі жойылады, буллингтің алғашқы байқалу нышандарына сүйене отырып, алдын алу шараларын жүргізуге болады. Педагогикалық ұжымның, мектеп әкімшілігінің, ата-аналардың, оқушылардың өздері де сырттан ешкімнің қатысуынсыз бұзақылықтың алдын алу үшін жеткілікті білімге ие болады.

Бұл жағдайда әмбебап профилактика бағдарламаның өз бағытын көрсетеді, өйткені қарастырылатын бағдарламалардың әрқайсысы дәстүрлі буллингтің барлық түрлерімен (денелік, вербальды, әлеуметтік) жұмыс істейді.

ОВРР, KiVa және РА арасындағы айырмашылықты келесідей анықтауға болады.

Кесте 2. Әлемдік буллингке қарсы бағдарламаларды салыстыру

Бағдарлама атауы	ОВРР	KiVa	РА
Факторлар			
Бағдарлама фокусы	Буллингке қарсытұру Деликвентті (қылмысқа итермелейтін) мінез-құлықтың алдын алу Құрдастар арасында әлеуметтік мінез-құлықты дамыту Сабақтан қалмау Зорлық-зомбылық виктимизациясы	• Мазасыздану • Буллингке қарсытұру • Зорлық-зомбылық виктимизациясы	• Академиялық жетістік • Жасөспірімдік • Алкоголизм • Мазасыздық • Буллингке қарсытұру • Депрессия • Эмоциялық өзін-өзіреттеу • ПАЗ белсенді заттарды қолдану • Құрбы-құрдастар арасында әлеуметтік мінез-құлықты дамыту • Сексуалдық мінез-құлық • Темекіге тәуелділік • Сабаққа бару проблемасы
Бағдарлама түрі	• Буллинктің алдыналу • Бүкіл мектеп ортасына бағдарлау	• Буллинктің алдыналу • Бүкіл мектеп ортасына бағдарлау • Жеке көзқарасқа назар аудару	• Девиантты мінез-құлықтың алдын алу • Бүкіл мектеп ортасына бағдарлау • Жеке көзқарасқа назараудару • Әлеуметтік - эмоционалды оқыту

Пайдалану ерекшелігі	• Әмбебап алдыналу • Таңдамалы алдыналу (жоғары қауіптілік)	• Әмбебап алдын алу • Буллинг көрсеткіші бойынша алдын алу • (ерте белгілері бойынша)	• Әмбебап алдын алу
Жас ерекшелік топтары	• 5–11 жас • 12–14 жас • 15–18 жас	• 5–11 жас	• 5–11 жас • 12–14 жас

ОВРР тәжірибесі бар мектептерде буллинктің жоғары қауіпінің алдын алуы керек, өйткені бұл бағдарлама шеңберінде Ольвеус сауалнамасы арқылы мектеп жағдайын үнемі тексеріп отыруы керек. KiVa-мен жұмыс істегенде, біз буллинктің айқын көріністері, мысалы, кейбір мектеп оқушыларының әлсіздерге қатысты денелік агрессиясы туралы айтамыз.

Әртүрлі бағдарламаларды салыстыра отырып, оларды бейімдеудегі ең үлкен қиындықтардың бірі мәдени және лингвистикалық фактор болғанын және болып қала беретінін есте ұстаған жөн. Әдістерді аудару ғана емес, сонымен бірге оларды әртүрлі мәдениеттерде енгізу де буллингке қарсы қолданыстағы бағдарламаларды енгізу процесін баяулататын күрделі кедергі болуы мүмкін.

Қорыта келе айтарымыз, мектептегі жәбірлеу бүкіл әлем бойынша білім беру ұйымдарында жиі кездесетін мәселе. Тіпті бір балаға қатысты қайталанатын агрессивті мінез-құлық барлық оқушыларға кері әсерін тигізіп, жәбірлеудің тікелей қатысушыларына ғана емес, оның куәгерлеріне де әсер етеді. Көптеген буллинктің алдын алу бағдарламалары бар болғанымен, олардың барлығы тиімді деп айта алмаймыз.

Осы тақырып бойынша зерттеулердің көптігі әлі көптеген елдер үшін қолайлы болатын буллингке қарсы біртұтас модельді жасауға әкелген жоқ. Сонымен қатар, осы немесе басқа мемлекет тапсырысы бойынша буллингке қарсы бағдарламалардың тиімділігін бағалау қиын, өйткені мұндай бағдарламалардың назарын жергілікті проблемаларға аударуға болады. Басқа мәселелерді буллинг тақырыбына байланыстыруға болатын: мигранттар мәселесі (Mexico's Anti-Bullying Campaign for Migrants in the U.S.), қылмысты мінез-құлықтың алдын алу (Flemish School-Based Anti-Bullying Programme, Bulli & Pupe), жыныстық қудалауға қарсы әрекет (PBIS: Expect Respect), эмпатия сезімін дамыту және әлеуметтік-эмоционалды оқыту (SAVE, Friendly Schools, Second Step) және т.б. көптеген бағдарламалар бар.

Жәбірлеуге қарсы біртұтас бағдарламаның қажеттілігі бар ма деген

сұрақ ашық күйінде қалып отыр, бірақ оның бүкіл әлем бойынша зерттеулерін жалғастыруда нақты негізгі критерийлері бар буллингке қарсы ұлттық бағдарлама қажет екені анық.

Әлемнің әртүрлі елдерінде жұмыс істейтін ең танымал буллингке қарсы бағдарламаларды зерттеу біздің елімізде мүмкін болатын буллингке қарсы бағдарлама туралы ойлаудың бастапқы қозғаушы нүктесі болады. Еуропада, АҚШ-та және Австралияда сәтті жүзеге асырылып жатқан бағдарламалардың қателіктерін, өсу нүктелерін және тәуекелдерін ескере отырып, Азия елдеріндегі зерттеу тәжірибесіне сүйене отырып және біздің мәдени ерекшеліктерімізді, отандық зерттеулердің нәтижелерін де ескере отырып буллингке қарсы ұлттық бағдарлама әзірлеуге болады.

Мектептегі буллингке қарсы әртүрлі бағдарламаларды салыстыру мемлекеттік көмектің қаншалықты маңызды екенін байқауға мүмкіндік береді. Фандрайзинг және әртүрлі үкіметтік емес ұйымдар арқылы экономикалық қолдау алу мүмкіндігіне қарамастан, ең дамыған және кең таралған бағдарламалар — бұл мемлекеттің тапсырысы бойынша құрылған немесе жергілікті билік органдары қолдауымен ұсынылатын бағдарламалар.

Буллингке қарсы бағдарламаны дамыту құралдарын таңдау маңызды рөл атқарады. Кешенді тәсілдер ең тиімді болып қала береді, онда мектептер бірнеше құрамдас бөліктердің ішінен өздерінің жағдайына неғұрлым сәйкес келетінін тандайды. Мысалы, бұл стратегия үкімет демеушілік ететін оқу материалдары Англияда (Шеффилд тәжірибесі) мұғалімдерге тікелей таратылған буллингке қарсы күресте басым болды. Материалдарда әртүрлі құрамдас бөліктердің сипаттамасы болды, бірақ қандай комбинацияларды және қандай жағдайларда пайдалану керектігін көрсетпейді. Бұл әдіс тиімді болуы мүмкін, өйткені мектептер өз әрекеттері үшін жауапкершілікті сезінеді.

ОВРР және KiVa — буллингке қарсы жасалған материалдардың жақсы мысалдары болып табылады. Осы екі көзқарас арасындағы сәйкессіздікті қазіргі зерттеушілер асыра бағалауы мүмкін. Мектептер мен мұғалімдер өздеріне берілген бағдарламаларды бейімдеуге бейім. Бұл 50-ден аса Швеция мектептерінде жүргізілген зерттеуде байқалды, оның мақсаты жәбірлеуге қарсы сегіз бағдарламаның табыстылығын салыстыру болды. Белгілі бір бағдарламаны қолданатын барлық мектептер шын мәнінде бірнеше бағдарламаның әртүрлі құрамдастарын пайдаланғандығын көруге болады. Сонымен қатар, сегіз бақылау мектебінде де осындай заңдылық байқалған. Осылайша, бағдарлама құрамдастарын бағалау бағдарламаларды тұтастайбағалауға қарағанда маңыздырақ екені анықталды.

Ұсынып отырған буллингке қарсы бағдарламаларды талдау 3 бағдарламаны қамтыды, бірақ бұл сан шекті емес. Бағдарламалардың көпшілігі осы тақырыпта пионер ретінде Ольвеустың зерттеулеріне сүйенеді. Белгілі бір бағдарламаның тиімділігін дәлелдейтін көптеген зерттеулер сол елге арналған Ольвеус сауалнамасына негізделген; кейбір бағдарламалар ОВРР-ны әдіснамалық база ретінде қарастырады.

Девиантты мінез-құлықпен айналысатын Positive Action

бағдарламасы американдық буллингке қарсы бағдарламалардың негізі, сондай-ақ әртүрлі жасөспірімдер ауытқуларына қарсы тұрудың үлгісі болып табылады, бұл оны тақырыптық қамтудың кендігінің арқасында қызықты етеді.

KiVa – буллингке қарсы қолданылатын тиімді және танымал бағдарламалардың ішіндегі ең жасы, ол тиімділік пен ресурстарды пайдалану және жаһандық таралу тұрғысынан ОВРР-мен бәсекелестікке түсе алады.

Көптеген буллингке қарсы бағдарламалар үшін өзекті және қиындық ретінде кибербуллинг мәселесін жеке айтса болады. Салыстырмалы түрде соңғы кезде буллинктің бұл түрі жәбірлеудің жеке әдісі ретінде де, жәбірлеудің дәстүрлі, «бетпе-бет» түрлерінің (әлеуметтік, ауызша, денелік) жалғасы ретінде де зерттелуде. Айта кету керек, бұл талдауда кибербуллингке қарсы бағдарламаларға аса мән берілмеді, дегенмен, жұмыстың басында талқыланғандай, 2011 жылы зерттеушілер жәбірлеудің осы түрімен жұмыс істеу мәселесін қоғамдағы ең маңызды мәселелердің бірі ретінде көтерді. Кейбір зерттеушілер жәбірлеумен жұмысты шынайы өмірде жасамаса, буллингпен онлайн жұмыс істеу қажетті нәтиже бермейді деп санайды. Бұл көзқарас баламалы шынайылықтағыдай емес, цифрлық әлемдегі өмірді түсіну контекстінде қисынды болып көрінеді.

Барлық қарастырылған бағдарламалар мектептегі жәбірлеу жағдайларының санын, виктимизация деңгейін төмендетуге және барлық білім алушылардың жәбірлеудің не екендігі туралы хабардарлығын арттыруға айтарлықтай әсер етеді. Нәтижесінде буллинг жағдайларының саны азайып, сонымен қатар мектеп ортасының жалпы психологиялық климаты жақсарады. Барлық зерттелген бағдарламалар буллингке жеке оқушыға да, топтар деңгейінде: сынып, мектеп, отбасы және жалпы қоғамдастық болып қарсы тұру керек деп есептейді.

Отандық тәжірибе

БҰҰ Балалар Қоры «Әрбір бала үшін UNICEF» жүргізген зерттеу нәтижелеріне сәйкес ұйымының зерттеулері бойынша ұсынымдар

Балалардың Интернетке және цифрлық қол жетімділігі мен оларды пайдаланудың бес аспектісі зерттелді: балалардың интернетке қол жетімділігі және оны пайдалану; Балалардың цифрлық дағдылары; әлеуметтік әл-ауқат және қолдау; ата-аналар мен тәрбиешілердің интернет-медиациясы. Сонымен қатар, ата-аналардың интернетке қол жетімділігі және оны пайдалану, олардың дағдылары; балалардың интернетке қол жеткізуіндегі медиация зерттеулер жүргізілді [11].

Балалардың Интернетке қол жетімділігі және оны пайдалану бойынша жүргізілген зерттеулер нәтижесі:

Қазақстанда балалар интернетке алғаш рет ерте жастан, олардың көпшілігі бес пен сегіз жас аралығында кіреді екен. Олардың көпшілігі интернетке қалаған кезде қол жеткізе алады және ауылдық жерлерге қарағанда

қала тұрғындары көбірек қол жеткізе алады. Достарыңызбен сөйлесу, бейне немесе теледидар көру балалардың интернеттегі ең көп таралған әрекеттерінің бірі болғанымен, олар интернетті оқу және жаңа нәрселерді үйрену үшін де пайдаланады. Балалардың интернетті пайдалануы дағдылар мен қабілеттерін дамытудың жақсы белгісі, бірақ балаларға (және олардың ата-аналарына) олардың жасына сәйкес онлайн-іс-шаралар мен цифрлық қауіпсіздіктің негізгі аспектілері туралы ақпарат беру және қолдау қажет екенін көрсетеді.

- Қазақстандағы балалар Интернетке қол жетімділіктің жоғары деңгейі туралы хабарлайды, ал жас кезінен бастап: 46% алғаш рет 5 жастан 8 жасқа дейін, ал үштен бірі 9 жастан 12 жасқа дейін интернетті қолданады екен.

- Балалардың көпшілігі интернетке қалаған кезде қол жеткізе алады және ерте балалық кезеңнен бастап, қолдарына телефон алып, интернетке кіреді.

- Балалар көбінесе смартфондарын интернетке қосылу үшін пайдаланады, балалардың 92% - ы смартфондарымен интернетке үнемі, күніне бірнеше рет немесе күн сайын кіретінін хабарлады. Орналасқан жеріне байланысты біршама айырмашылық болды: қалалардағы балалар ауылдағы балаларға қарағанда дербес компьютерлер немесе ноутбуктер арқылы интернетке көбірек кірді.

- Интернет балалар үшін өте жағымды нәрсе ретінде қарастырылады: он баланың тоғызы Интернетте өз жасындағы балаларға пайдалы заттар бар деп санайды (94%) және олардың жасындағы балалар интернетке кірген кезде жақсы уақыт өткізеді (93%). Интернетті пайдаланудың ләззаты жас ұлғайған сайын артады: 15 пен 17 жас аралығындағы ересек балалар 9 мен 10 жас аралығындағы балаларға қарағанда интернетке кірген кезде үнемі жақсы уақыт өткізетінін, жақсы әсерде болатынын айтады.

- WhatsApp немесе Telegram сияқты хабар алмасу қолданбаларын пайдалану және бейнеклиптер мен әлеуметтік медиа сайттарында ең көп қаралым болды. Интернеттегі балалардың жалпы әрекеттері: 82% хабар алмасу қолданбаларын пайдаланатынын, 60% бейнеклиптерді және 66% әлеуметтік медианы күнделікті, күніне бірнеше рет немесе тұрақты түрде көретінін хабарлады.

- Қарым-қатынас пен ойын-сауықтан басқа, балалар әдетте интернетті оқу үшін пайдаланатынын хабарлады: 60% Интернетті оқу үшін пайдаланды, ал 46% оны күнделікті, күніне бірнеше рет немесе тұрақты түрде жаңа нәрсе табу үшін пайдаланды.

Бұл нәтижелер жалпы алғанда аймақтық нәтижелерге сәйкес келеді, балалардың басым көпшілігі мазмұнды тұтыну және ойын-сауық пен қарым-қатынас мүмкіндіктері сияқты онлайн режимінде болудың мүмкіндіктерін пайдаланғанымен, жоғары техникалық және цифрлық дағдыларды қажет ететін мүмкіндіктерге қол жеткізе алатын балалардың саны артып келе жатқанын көрсетеді.

Балалардың көпшілігі интернеттегі мазмұнды тұтынады, бірақ мазмұнды немесе шығармашылық әрекеттерді жасауда әлдеқайда шектеулі және интернет ұсынатын мүмкіндіктерді толық пайдаланады.

Балалардың көпшілігі интернетке қалаған кезде қол жеткізе алатынын хабарлайды, үш баланың біреуі (36,9%) интернетке жиі және өзі қалаған кезде кіре алатынын хабарлайды, ал бес баланың екеуі (39,2%) интернетке тұрақты қол жеткізе алатынын хабарлайды.

Бұл балалардың интернетке қол жетімділігіне, сондай-ақ олардың цифрлық дағдыларына әсер етеді.

Үйде және мектепте балалар интернетте көп уақыт өткізеді. Бұл балалардың көп уақытын қайда өткізетініне сәйкес келеді, сонымен қатар үйде және қажет болған жағдайда мектепте интернетке еркін қол жетімділік бар екенін көрсетеді. Әрбір екінші бала (46,9%) үйде күн сайын интернетке кіретінін, ал үштен бірінен астамы (36,1%) мектепте күн сайын интернетке кіретінін хабарлайды. Он баланың үшеуі (31,7%) барлық уақытта дерлік үйде интернетте отырады, ал оннан бірінен астамы (13,3%) мектепте үнемі дерлік интернетте отыратындығын хабарлайды.

Ауылдық жердегі мектептерде балалардың едәуір көп пайызы (25,2%) интернетті ешқашан пайдаланбайды, қалалардағы балаларға қарағанда (15,8%) едәуір кем. Балалардың интернетке қалай және қайда кіретіндігінде жасына немесе жынысына байланысты айтарлықтай айырмашылық жоқ.

Балалар интернетке қосылу үшін смартфондарды жиі пайдаланады: он баланың тоғызы (92%) смартфонды интернетке тұрақты, күніне бірнеше рет немесе күнделікті кіру үшін пайдаланады. Әрбір төртінші бала Интернетке үнемі, күніне бірнеше рет немесе күн сайын ноутбуктан немесе компьютерден кіреді, ал 35,9% интернетке қосылған (Smart) теледидарларынан үнемі, күніне бірнеше рет немесе күнделікті кіреді. Мұндай нәтиже қазірдің өзінде балалардың интернетке кіруінің және олардың интернеттегі белсенділігінің ең көп тараған себептерін меңзейді, өйткені смарт теледидарлар ең алдымен ойын-сауық пен ойын үшін пайдаланылады, ал компьютерлер мен ноутбуктер мектеп сабақтарын немесе іздеуді қоса алғанда, кеңірек ақпараттар үшін пайдаланылуы мүмкін. Планшеттер мен ойын консольдері интернетке кіру үшін айтарлықтай аз пайдаланылады, бес баланың төртеуі (75,9%) ешқашан ойын консолінен интернетке кірмейтінін хабарлайды және осынша пайыз(74%). бала ешқашан планшеттен интернетке кірмейді. Ауыл балаларының 50,1% - ы қала балаларының 38% - салыстырғанда интернетке кіру үшін ешқашан ноутбук немесе компьютерді пайдаланбайтынын хабарлады.

Интернетке кірудегі кедергілер: негізінен мұғалімдердің және ата-аналардың интернетті пайдалануына шектеулер түрінде туындайды.

Үштен бірі дерлік бала кейде мұғалімдер интернетке кіруді шектейтінін хабарлады, ал тағы 13,9% бұл жағдай жиі болатынын хабарлады. Балалардың 34%-ы ата-аналары кейде интернетке кіруді шектейтінін хабарлағанымен оннан аз бөлігі, 7,6% бұл жағдай жиі болатынын хабарлады.

Бұл тосқауыл болмаса да, балалар интернет олардың өмірінде тым көп уақытты алады деп 35,1%-ы ойлайтынын, ал 17,5% бұл өте жиі сезінетінін хабарлады. Бұл қабылдау олардың өміріне мұғалімдер мен ата-аналар сияқты ересектер шектеулер қоюға әкелуі мүмкін деген ой тудырады.

Интернетке немесе құрылғыларға кіру құны интернетке кіру кезінде ең аз хабарланған кедергілердің бірі болып табылады. Алайда, интернетке және цифрлық құрылғыларға қол жетімділік біртүрлі болғанымен, Қазақстандағы балалардың едәуір пайызы интернеттің жасына байланысты (әрбір төртінші адам осылай деп санайды) немесе денсаулығына немесе мүгедектігіне байланысты олар сияқты адамдар үшін емес екенін сезінеді (13,2% кейде немесе жиі осылай сезінеді) немесе олар үшін бұл өте қиын (әрбір бесінші адам кейде немесе жиі осылай сезінеді).

Ұлдармен салыстырғанда (қыздардың 18,5%-ы; ұлдардың 16,1%-ы) интернет қыздар үшін тым күрделі деп санайтынын хабарлады, дегенмен интернетті тым күрделі деп санайтын ұлдар мен қыздардың пайызы арасындағы айырмашылық көп емес). Керісінше, көптеген ұлдар интернетті қыздармен салыстырғанда өте күрделі деп санайды (0,7% - бен салыстырғанда 1,5%), бірақ бұл көрсеткіш олардың негізінде мағыналы қорытынды жасау үшін тым төмен. Кішкентай балалар (9 жастан 11 жасқа дейін және 11 жастан 12 жасқа дейін) 13-14 және 15-17 жас аралығындағы балаларға қарағанда интернетті тым күрделі деп санайды, бұл балалар есейген сайын хабардарлықтың, өзіне деген сенімділіктің және белгілі бір дағдылардың өсуін болжайды.

Қыздар (27,2%) кейде интернет оларға ұлдарға қарағанда қалаған немесе қажет нәрсені бермейтінін сезінуі мүмкін (24,5%), дегенмен ұлдар статистикалық тұрғыдан қыздарға қарағанда мұндай сезімдерді жиі бастан кешірді (4,8% салыстырғанда 6%)), немесе өте жиі (Ұлдардың 2,8%-ы қыздардың 1,6%-ы салыстырғанда). 9-10 жас аралығындағы балалар кейде өздерін басқа жастағы балаларға қарағанда осылай сезінетінін хабарлау ықтималдығы жоғары болды (11-12 жас аралығындағы балалардың 24,4%, 13 пен 14 жас аралығындағы балалардың 26,1% және 15 пен 17 жас аралығындағы балалардың 23,5% салыстырғанда 31,3% жоғары). Олар интернет өздерінің қалағанын бермейді немесе жиі бермейді деп сезінеді.

Балалардың 92,8% - ы интернетке кірген кезде жақсы уақыт өткізетінін айтады. Интернетке кірген кезде жиі немесе үнемі жақсы уақыт өткізетінін хабарлаған.

11 мен 12 жас аралығындағы балалар мен 15 пен 17 жас аралығындағы балалар 13 пен 14 жас аралығындағы балаларға қарағанда интернетте үнемі немесе жиі жақсы уақыт өткізді. 9-10 жас аралығындағы балалар көбінесе интернетке кірген кезде 5,3%-ы ешқашан немесе 9,4%-ы сирек жақсы уақыт өткізетінін білдірді.

Интернетте өз жасындағы балалар үшін пайдалы нәрсе бар деп санайтын ересек жастағы балалар кішкентай балаларға қарағанда интернетте олар үшін көптеген пайдалы нәрселер бар екенін сезінді. Бұл балалар қартайған сайын

және цифрлық дағдылардың жоғары деңгейін дамытқан сайын, олар цифрлық орта ұсынатын мүмкіндіктер мен артықшылықтарды жақсырақ пайдалана алатынын айтатын әдебиеттерге сәйкес келеді. Ересек балалар кішкентай балаларға қарағанда қызықты деп тапқан ақпарат пен мазмұнды қалай және қайдан табуға болатынын біледі, бұл олардың интернеттің олар үшін пайдалы екенін сезіну ықтималдығын арттырады.

Цифрлық технологиялар білім беру ұйымдарында енгізілген балалар интернеттің пайдалы екенін сезінеді, өйткені олар оны оқу үшін көбірек пайдаланады.

Жас ерекшеліктеріне байланысты интернетте пайдалы нәрсе бар деп ойлайтын балалар жауабының үлесі.

Балалардың интернетте жасай алатын әрекеттерінің ауқымы өте үлкен. Бұл зерттеу үш түрлі әрекет тобын кеңінен зерттеді: *ойын-сауық және қарым-қатынас, ақпарат пен білім іздеу, мазмұн жасау немесе шығармашылық.*

Балалардың интернетте ойын-сауық пен қарым-қатынасқа көбірек уақыт бөлуі таңқаларлық емес. Жалпы, WhatsApp немесе Viber сияқты хабар алмасу қолданбаларын пайдалана отырып, бес баланың төртеуі чат қолданбасын күнделікті (48,4%), күніне бірнеше рет (13,5%) немесе тұрақты дерлік (20%) пайдаланатынын хабарлады.

Бейнеклиптерді көру бірдей танымал болды, он баланың жетеуі клиптерді үнемі (13,9%), күніне бірнеше рет (12,3%) немесе күнделікті (43,5%) онлайн көреді.

Ойындар – бұл интернетте күнделікті, үнемі немесе күніне бірнеше рет жасалатын ең аз таралған әрекет, дегенмен әрбір екінші (50,1%) бала әлі күнге дейін кем дегенде күнделікті немесе одан да көп ойын ойнайтынын хабарлайды.

Соңғы айдағы ойын-сауық пен интернеттегі байланыстың жиілігі.

Фокус-топтарға қатысқан көптеген ұлдар қыздар ойын ойнамайды деген пікірде болды және бұл пікірді әдетте фокус-топтардағы қыздар да бөліседі: Олар: «ұлдарға Dota, FraeFire ойынын ойнайды. Олар үнемі телефонмен карта ойындарын ойнайды» деп жауап берді. Қыздар ойнайтын ойындардың түрлері ұлдар ойнайтын ойындардан өзгеше деген пікір кең таралған.

Ақпарат пен білімді іздеу – интернеттегі балалар әрекеттерінің екінші ең көп таралған түрі. Оларға интернеттен медициналық сипаттағы ақпаратты іздеу, өз қалаңыз немесе қалаңыздағы оқиғалар туралы ақпаратты іздеу, және жаңа нәрсені үйрену үшін интернетті пайдалану кіреді. Зерттеуге қатысқан бес баланың үшеуі (59,7%) интернетті кем дегенде күн сайын (40%), күніне бірнеше рет (7,5%) немесе соңғы айда тұрақты (12,1%) оқу немесе мектеп сабақтары үшін пайдаланды, ал оннан бірінен көбі (11,8%) интернетті сол кезеңде оқу үшін мүлдем пайдаланбаған.

Балалардың көпшілігі интернетті ақпарат іздеу немесе оқу үшін жиі пайдаланғанымен, аз балалар ақпаратты іздегеннен кейін интернетте жаңа ақпарат біледі. Сауалнамаға қатысқан барлық балалардың 45%-ы өткен айда интернеттен іздеу арқылы жаңа ақпарат білгендерін хабарлады.

Фокус-топтардағы пікірталастарға қатысқан балалар интернетті тіл сияқты жаңа дағдыларды үйрену үшін қалай пайдалануға болатындығы туралы айтты.

Соңғы айда интернетті пайдаланып ақпарат пен білімді іздеу жиілігі.

Зерттеу барысында зерттелген соңғы іс-шаралар тобы интернетке арналған мазмұнды құруға қатысты болды. Интернеттегі блогты немесе веб-сайтты құру, өзінің музыкасын немесе бейне-жазбаларды жасау және жүктеу және басқалармен бөлісу үшін жүктеу, мысалы, веб-сайт, әлеуметтік медиа немесе TikTok немесе YouTube сияқты қысқа бейне қосымшалары арқылы нақты әрекет зерттелді.

Балалардың көпшілігі соңғы айда веб-сайт немесе блог жасамағанын, сондай-ақ интернетте бөлісу үшін өздерінің музыкаларын немесе бейнелерін жасамағанын хабарлады. Тек төрттен бір бөлігі (25,7%) соңғы айда блог немесе веб-сайт құрды, олардың көпшілігі (9,5%) мұны соңғы айда бір-екі рет жасады, апта сайын 4,2% және күнделікті 6,6%.

Балалар өздерінің бейне-жазбаларын немесе музыкаларын жасау және оларды интернетке жүктеу ықтималдығы жоғары болды: 13,1% - ы мұны бір-екі рет, әр оннан бір бөлігі (9,4%) апта сайын, ал 12,2% - ы күнделікті жасайтындығы анықталды. Жалпы, бұл Қазақстандағы Instagram, Vkontakte және TikTok сияқты сайттардың танымалдылығына сәйкес келуі мүмкін.

Соңғы айда Интернетті пайдаланып мазмұнды жасау жиілігі.

Бұл нәтижелер, әдетте, аймақтық нәтижелерге сәйкес келеді, бұл балалардың көбі мазмұнды тұтыну және ойын-сауық пен қарым-қатынас мүмкіндіктері сияқты онлайн режимінде болу мүмкіндіктерін пайдаланғанымен, жоғары техникалық және цифрлық дағдыларды қажет ететін мүмкіндіктерге қол жеткізе алатын балалардың үлесі бар екенін көрсетеді. Балалардың көпшілігі интернеттегі мазмұнды тұтынады, бірақ мазмұнды немесе шығармашылық әрекеттерді жасауда әлдеқайда шектеулі және интернет ұсынатын мүмкіндіктерді толық пайдаланады.

Интернетте болудың көптеген мүмкіндіктерінің бірі және оны балалар анық пайдаланады – бұл тікелей қарым-қатынас шеңберінде де, балалардың ортасында да, кең мағынада да адамдардың кең ауқымымен қарым-қатынас жасау. Facebook Messenger сияқты WhatsApp, TikTok және Instagram сияқты чат және хабар алмасу қосымшалары отбасымен тікелей және алыс байланыста болуға, сондай-ақ достарына, жігіттеріне немесе қыздарына үнемі қол жеткізуге мүмкіндік береді, сонымен қатар олар өздерінен алыстағы адамдармен байланыс орнатуға және өзара әрекеттесуге мүмкіндік береді.

Балалардың күнделікті немесе одан да аз желіде кіммен сөйлесетінін білу балалардың интернетке қосылудың кейбір артықшылықтарын қалай жинайтынын, сондай-ақ олардың интернетте кездесетін кейбір тәуекелдерге қалай ұшырауы мүмкін екенін түсіну үшін пайдалы. Мысалы, отбасы мүшелерімен, әсіресе ата-аналарымен және қамқоршыларымен, бауырларымен немесе сол жастағы достарымен күнделікті қарым-қатынас жасау ата-ананың

да, баланың да көзқарасы бойынша интернетте болудың көптеген артықшылықтарының бірі болып саналуы мүмкіндігі зор.

Алайда, ересектердің көзқарасы бойынша, балалардың жеке өзі білмейтін және тек интернетте кездесетін адамдармен, әсіресе олардан үлкен адамдармен сөйлесуі балаларға белгілі бір қауіптер мен ықтимал қауіптер тудыруы мүмкін.

Балалар ата-аналарымен күн сайын, күніне бірнеше рет немесе тұрақты, басқа адамдарға қарағанда көбірек сөйлесетінін хабарлады. Одан кейін басқа ересек туыстарымен, бауырларымен қарым-қатынас жасалады

13,6%-ы күнделікті романтикалық серіктестерімен сөйлесетінін хабарлады.

Балалардың жалпы 4,2% - ы интернетте алғаш кездескен 18 жастан асқан бейтаныс адамдармен сөйлескенін, 18 жастан асқан бейтаныс адамдармен бір-екі рет, ал 2,7% ересек бейтаныс адамдармен айына бір рет сөйлескенін хабарлады.

Жас ерекшелігіне байланысты кейбір айырмашылықтар болды: кішкентай балаларға қарағанда ересек жастағы балалар интернетте алғаш кездескен 18 жастан асқан адамдармен кейде немесе үнемі сөйлесетінін хабарлады. Барлығы он баланың жетеуі 15 пен 17 жас аралығындағы балалардың 7,9,2% - ы 18 жастан асқан адаммен сөйлеспегенін хабарлады, ал 13 пен 14 жас аралығындағы балалардың 87,9% - ы, 91,9% - ы 11 жастан 12 жасқа дейін, тоғыз бен он жас аралығындағы балалардың 95,1% ешқашан сөйлеспегенін айтты. Ауылдық жерлерде тұратын балалардың 93,5%-ы қалаларда тұратындармен (85,1%) салыстырғанда, олар алғаш рет онлайн танысқан 18 жастан асқан адаммен ешқашан сөйлеспегенін хабарлады.

Интернеттегі күнделікті қарым-қатынас кезінде балалардың тәуекелге ұшырауы

Балалар интернеттегі ең көп таралған қауіпті іс-әрекеттерге-іс-әрекеттің түрлеріне қатысуы баланың өміріне қауіпті тәуекелдер әкелуі мүмкін.

Балаларға қауіп төндіретін бес түрлі әрекет туралы сұралды: Интернетте жаңа достар немесе контактілер табу, интернеттегі жеке ақпаратыңызды жіберу, ешқашан кездеспеген контактілерге достар қосу, басқа біреу болып көріну және жеке фотосуреттерін немесе бейне-жазбаларын ешқашан бөгде адамға жіберу жеке кездескен жоқ.

Көбінесе Интернеттегі қауіпсіздік туралы жалпы хабарламалар осы әрекеттерге негізделеді және балаларға интернеттегі қауіпсіздікті қамтамасыз ету үшін кеңес берілмейді. Жалпы алғанда, олардың барлығы маңызды хабарламалар, дегенмен олар балалардың интернеттегі мінез-құлқындағы көптеген мотивтерді, соның ішінде эмоционалды қозуды және басқа адамдармен тікелей контексттен және қоршаған ортадан тыс танысу мүмкіндігін ескермейді.

Бұл әсіресе интернеттен жаңа достар немесе байланыстар іздеген балалардың пайызына әсер етеді. Бұл әдеттегі әрекет болмаса да, олардың

оннан бірінен астамы небәрі 14,6%-ы достарын немесе интернеттегі байланыстарын айына кемінде бір рет, ал 12,7% - ы соңғы жылы бір-екі рет іздеді. Жалпы алғанда, 7,2% мұны апта сайын және 4,1%- ы күнделікті жасады.

Дегенмен, фокус-топтардағы балалар достар шеңберін кеңейту интернетте болудың көптеген артықшылықтарының бірі екенін жиі атап өтті, өйткені олар байланыс шеңберін кеңейту үшін жаңа достар іздей алады. Ұлдар мен қыздардың интернеттен қаншалықты жиі жаңа достар іздейтіндігінде айырмашылық аз болғанымен, қалаларда тұратын балалар интернеттен достар іздеуде айтарлықтай жоғары болды. Қалалардағы әрбір екінші (53,5%) баланың үштен екісі (67,3%) ауылдарда тұратын балалардың үштен екісімен салыстырғанда жоғары болды.

Осыған байланысты әрбір оныншы (10,2%) бала ешқашан жеке кездеспеген достарын немесе таныстарын айына бір немесе екі рет, ал 7,7% орта есеппен бір рет байланысқа шыққан. Әрбір оныншы (10,3%) бала өзінің жеке ақпаратын біреуге жібергенін хабарлады, олардың көпшілігі (3,8%) мұны өткен жылы бір-екі рет немесе айына бір рет (3,3%) жасаған.

11,1% бала өздерінің жеке фотосуреттерін немесе бейне-жазбаларын өздері білмейтін адамға жіберген, олардың көпшілігі мұны өткен жылы бір-екі рет (4,7%) немесе айына бір-екі рет (4,2%) жасаған. Бұл деректер балалар интернеттегі қарым-қатынас кезінде белгілі бір дәрежеде қауіп төндірсе де, балалардың көпшілігі бұл әрекеттерден аулақ болатынын көрсетеді. Бұл балаларды интернеттегі қауіпсіздік туралы ақпараттандыруға маңызды әсер етуі мүмкін.

Интернеттегі қауіпті мінез-құлық

Зерттеу барысында сауалнамаға қатысқан балалар арасында ойындар мен әлеуметтік медианы пайдаланудың жоғары деңгейін ескере отырып, көптеген балалардың өздерінің ойын немесе әлеуметтік медиа аккаунттары бар деп болжауға болады. Балалардың төрттен үш бөлігі (72,8%) өздерінің ойын немесе әлеуметтік аккаунттары немесе белсенді сайттарында профильдері бар екенін хабарлады. Мұның өзі балаларға бірден қауіп төндірмейді. Бұл жазбалардың қалай басқарылатындығы және олардың жасына қаншалықты сәйкес келетіндігі балалардың интернетте кездесетін қауіп-қатеріне әсер етуі мүмкін. Мысалы, бұл аккаунттар мен профильдердің барлығы өздерінің профильдері мен деректерін, соның ішінде олар білмейтін адамдарды көре алатындай жалпыға қол жетімді бола ма, бұл балалардың тәуекелдеріне әсер етуі мүмкін. Кейбір балалар үшін өз аккаунттарын ашық түрде сақтау жаңа адамдармен танысудың және өздерінен тыс әлемдерді зерттеудің тәсілі болуы мүмкін; сонымен қатар, бұл баланың жасына сәйкес келмейтін немесе сол баланың өміріне тікелей қауіп төндіретін байланыстарға немесе әңгімелерге мүмкіндік береді.

Қоғамдық, ішінара жеке немесе жеке болып табылатын әлеуметтік желілерде немесе ойындарда белсенді аккаунттары бар балалардың пайызы

Жалпы алғанда, әлеуметтік желілерде немесе ойын желілерінде жеке профильдері бар бес (44%) баланың екеуі өздерінің ойын немесе ойын аккаунттарын көпшілікке жария еткен, ал жеке аккаунттары бар бес (30,3%) баланың үшеуі оларды толығымен жеке етіп орнатқан, яғни тек достары немесе жеке байланыстары үшін ашық, олар профильдерін біледі және олармен бөлісуді қалайды. Тағы бесінші бала (22,2%) өз аккаунтын ішінара жеке етіп құрды; яғни жалпы жұртшылық үшін емес, достары немесе байланыстары үшін ашық. Өте аз пайызы – 3,2% - олардың жазбалары жеке немесе жалпыға ортақ екенін айта алмады, бұл олардың құпиялылық параметрлерін мүлдем түсінбейтінін немесе пайдаланбайтынын көрсетеді.

Көптеген әлеуметтік желілер заң бойынша 13 жастан асқан балаларға қол жетімділікті шектеуге міндетті болса да, 9 бен 10 жас аралығындағы бес баланың үшеуі (59,9%) өздерінің әлеуметтік немесе ойын желілерінде профильдері бар екенін, ал 11 мен 12 жас аралығындағы балалардың үштен екісі (66,2%) әлеуметтік желілердегі немесе олар пайдаланатын ойын сайттарындағы өздерінің профильдері бар екенін хабарлайды.

Кішкентай балалар да ересек балаларға қарағанда өз аккаунттарын ашық және көпшілікке ашық орнатқанын хабарлау ықтималдығы жоғары болды. Жалпы алғанда, 9 бен 10 жас аралығындағы балалардың жартысынан көбі өздерінің профильдері немесе аккаунттары бар, олардың жазбалары 11 мен 12 жас аралығындағы балалардың 43,7% - ы, 13-14 жас аралығындағы балалардың 44,6% - ы және 15 жастан асқан балалардың 38,1% - ы 17 жасқа дейінгілермен салыстырғанда жалпыға қол жетімді екенін хабарлады. Керісінше, ересек әрбір үшінші бала (33,2%) көбінесе толық құпиялылықты сақтайды:

15 пен 17 жас аралығындағы балалар оның аккаунты құпия болғанын хабарлады, бұл 13 пен 14 жас аралығындағы немесе 11-12 жас аралығындағы он баланың үшеуімен салыстырғанда, олардың тек 28,6% - ы 9 бен 10 жас аралығындағы балалар. Бұл дегеніміз, балалар (интернетте кездесетін тәуекелдерді сәтті жеңу дағдыларына ие болу ықтималдығы аз) өз аккаунттарын ашық түрде қалдырады және интернеттегі бейтаныс адамдардың ықтимал қауіптеріне тап болады.

Әлеуметтік желілерде немесе ойындарда белсенді аккаунттары бар балалардың жасы бойынша өз аккаунттарын ашық, жартылай жеке немесе жеке қалдыратын балалардың пайыздық көрсеткіші

Ұлдар қыздарға қарағанда өз аккаунттары мен профильдерін көпшілікке қолжетімді етіп жиі орнататын: әрбір екінші ұл (49,1%) оның аккаунты қыздарға қарағанда (39,8%) жалпыға ортақ екенін хабарлады, ал қыздар өз аккаунттарын ішінара жеке құпиялықты сақтау ықтималдығы жоғары болды (19,1% салыстырғанда 25,1% ұлдарға қарағанда (32,7%) немесе толығымен жеке (27,8%). Бұл қыздардың жалпыға қол жетімді аккаунттардың олар үшін туындауы мүмкін қауіптер туралы көбірек білетіндігін байқатады. Сондай-ақ, бұл олардың жазбалары мен ақпараттарының құпиялылығын қамтамасыз етуге мәжбүр еткен жеке тәжірибелерін көрсетуі мүмкін.

Жалпы, балалардың көпшілігі өздерін интернеттен талап етілуі мүмкін көптеген күнделікті техникалық іс-әрекеттер мен қауіпсіздікті қамтамасыз ету жөніндегі іс-әрекеттерді орындауға қабілетті деп санады. Бесеудің үшеуі (61,4%) қосымшаны телефонға жүктей алатындығымен толық келіскен, ал тағы 17,4% - ы мұны істей алатындығымен келіскен; бес баланың төртеуі (56,7%) немесе қалай сақтау керектігін білетіндерімен (21,4%) келіскен; бес баланың үшеуі дерлік өздері жасаған бейне-жазбаларды немесе бейне-баянды интернетте орналастыра алатынына толық келіскен (37,8%) немесе дерлік келіскен (19,8%).

Негізгі қауіпсіздік дағдыларына келетін болсақ, интернетте өзінің немесе басқалардың қандай суреттерін бөлісу керектігін он баланың жетіден астамы өздерінің контактілер тізімінен біреуді қашан алып тастау керектігін білетіндерімен толық келіскен (50,8%) немесе дерлік келіскен (19,4%) және аз пайызы толық (45,3%) немесе негізінен (18,9%) білді. Сол сияқты, он баланың жетеуі дерлік интернеттегі құпиялылық параметрлерін қалай өзгерту керектігін біледі, олардың 46,3% - ы бұл шағыммен толық келіскен, ал тағы 19,5% - ы негізінен келіскен.

Балалардың көпшілігінің осы негізгі қауіпсіздік дағдыларын білуі хабардарлық пен негізгі қауіпсіздік дағдыларының жағымды көрсеткіші ретінде қарастырылуы керек.

Балалар веб-сайтқа қалай сенуге болатынын: тек төрттен бір бөлігі (24,6%) толығымен келіскен, ал тағы бесінші бөлігі (19,5%) негізінен оны қалай анықтау керектігін білетіндерімен келіскен. Балалардың ұқсас үлесі интернеттен тапқан кескінді немесе бейнені қалай өңдеу немесе өзгерту керектігін біледі (тек 25,8% толығымен келіскен және 19% негізінен бұл мәлімдемемен келіскен).

Әрбір екінші бала интернетті және смартфондарды қалай пайдалану керектігі туралы көп білетінін хабарлауға жеткілікті сенімді сезінеді, ал төрттен бірі (25,7%) негізінен көп білетіндерімен келісетінін айтады. Жалпы алғанда, балалардың 16,5%-ы келіседі және тек 6,8% - ы интернет пен смартфондарды пайдалану туралы көп білетіндігімен толық келіспейді деп санайды.

Интернетте менің құрдастарымды мазалайтын немесе ренжітетін нәрселер бар деген мәлімдемемен келісетін балалар жауабының көрсеткіші

Қазақстандағы балалардың көпшілігі интернет оларға күнделікті өмірде проблемалар тудырды деп есептемейді. Яғни интернет олар үшін қауіпті емес. Ең жиі кездесетін мәселе олардың интернетте өткізген уақыты болды: он баланың біреуі (9,2%) өткен жылы олар бір-екі рет интернетте аз уақыт өткізуге тырысқанын және сәтсіздікке ұшырағанын хабарлады, ал әрбір бесінші (20,4%) бұл кем дегенде айына бір рет болғанын хабарлады. Балалардың жалпы 8% - ы аптасына кемінде бір рет интернетте аз уақыт өткізуге тырысқанын хабарлады.

Осыған байланысты, әрбір оныншы бала (9,6%) өткен жылы бір немесе екі рет өткен жылы Интернетте өткізген уақыт оған қиындық тудырды деп ойлады, ал 14,2% айына кемінде бір рет осылай сезінетінін хабарлады.

Әрбір оныншы бала интернетте өткізген уақытына (10,7%) байланысты олардың бағалары нашарлағанын немесе интернетте өткізген уақыт өткен жылы кем дегенде айына бір рет отбасымен (10,6%) жанжал тудырғанын хабарлады, дегенмен бұл туралы аз балалар хабарлады.

Интернеттегі уақыттың нашарлауы мен проблемалардың кең әлеуетін қабылдауға көбінесе мұғалімдер мен ата-аналар әсер етеді, олар интернетті шамадан тыс пайдалану проблемаларына кінәлі деп санайды, мүмкін, 8,1% өткен жылы бір немесе екі рет емес деп хабарлады интернетте өткізген уақытына байланысты тамақ ішіп, ұйықтамаған, ал тағы 8,2% бұл кем дегенде ай сайын болғанын хабарлады.

Ұйқының болмауы және тамақтан бас тарту – бұл интернетті пайдалануға оңай және балалардың өздері бағалайтын біршама объективті көрсеткіштер.

Жалпы алғанда, балалардың 15,8%-ы өткен жылы бір-екі рет желіде бір нәрсеге ренжігенін хабарлады, ал тағы 8,2% -ы бұл айына кемінде бір рет болғанын хабарлады.

Балалар арасында интернетті пайдалануда туындаған проблемалар

Өткен жылы кем дегенде бір, екі немесе одан да көп рет проблемалар болғанын хабарлаған он баланың үшеуінің көпшілігі (57,5%) оқиғаға реніш тудырған, ал 17,6% проблемаларды өте қатты сезінген.

Интернетте баланы ренжіткен жағдайдағы мазасыздық дәрежесі

Барлық балалар үшін қолайсыз тәжірибені пысықтау мен басқарудағы маңызды қадам – оларды желіде де, оффлайн режимінде де ренжітетін жағдай болған кезде немесе біреу оларды ренжіткен кезде сөйлесетін адамның болуы.

Қолдау көрсете алатын және қажет болған жағдайда шешім қабылдауға және көмек сұрауға көмектесетін біреудің болуы тәуекелдерді сәтті жеңудің және интернетте болу нәтижесінде туындауы мүмкін зиянды болдырмаудың маңызды құрамдас бөлігі.

Дегенмен, әлемдік зерттеулер көрсеткендей балалардың бұл тәжірибені көбінесе өз бетінше немесе ең жақсы жағдайда ересектердің емес, достарының немесе құрдастарының қолдауымен басқаратынын көрсетеді.

Оның себептер әр түрлі: ересектерге деген сенімсіздіктен, оларға сенбейді немесе өздерінің қолайсыз тәжірибесі үшін ұлады, өздерін кінәлайды және олар интернетке қол жетімділіктен айырады деп қорқады, немесе кейбір жағдайларда жастар ересек адаммен сөйлесу қандай да бір қолдау немесе көмек әкеледі деп сенбейді.

Осыған ұқсас көрініс Қазақстанда өткен жылы онлайн режимінде қандай да бір жағымсыз тәжірибені бастан өткерген балаларға қатысты байқалады. Жағымсыз оқиғалары туралы хабарлаған балалардың төрттен бірі бұл туралы ешкімге айтпады, ал біреумен сөйлескендердің үштен бірінен азы (31,5%) достарымен немесе құрдастарымен сөйлесті. Жағымды жағы – әрбір төртіншісі (24,1%) ата-аналарына немесе қамқоршыларына өз тәжірибелері туралы айтқан, дегенмен кішкентай балалардың ересек балаларға қарағанда ата-аналарымен

сөйлесуі әлдеқайда жиі кездеседі. 15 пен 17 жас аралығындағы балаларға қарағанда екі есе кіші балалар (тоғыз бен он жас аралығындағы) ата-аналарына немесе қамқоршыларына өздерінің ата-аналары туралы айтқан (18,6% салыстырғанда 37,7%).

13 пен 14 жас аралығындағы балалар (13,8%) ата-аналарға интернеттегі оқиға туралы ересек жастағы балаларға қарағанда көбірек айтуы мүмкін.

Балалардың оннан бірінен азы ересек (18 жастан асқан) бауырларымен (9,1%), ал одан да азы (8,5%) 18 жасқа дейінгі бауырларымен сөйлескен.

Балалар айыпталудан қорықпай сөйлесе алатын, қиындыққа тап болатын және қолдауға үміттенетін сенімді, ересек адамның болуы, әсіресе кішкентай балалар үшін маңызды механизм. Оларға қолдау мен көмек қажет болған кезде онлайн тәуекелдерді сәтті шарлау және қай жерде екенін білу үшін қажетті білім мен тәжірибеге ие болмауы мүмкін.

Бала интернетте бір жағдайға тап болғаннан кейін соңғы рет қандай әрекет жасады

Интернетте соңғы рет біреулер оларды ренжіткеніне жауап ретінде олар қандай әрекет жасады деген сұраққа, он баланың үшеуі (29,2%) ештеңе істемеді және мәселе өздігінен жойылады деп үміттенді (мәселені елемеді) және төрттен бірінен азы (23,4%). Әрбір оныншы (9,4%) өзін ренжіткен барлық хабарламаларды жойғанын хабарлады, ал дәл сол бөлігі оларды мәжбүрлеуге тырысты.

Тек 17,4% -ы қолданбаның немесе шолғыштың қауіпсіздігін қамтамасыз етуге арналған функцияларды қолдана отырып, белсенді әрекет жасады, мысалы, адамды бұғаттау, ал 5,4% - ы өзін жақсы қорғау және адаммен қарым-қатынасты тоқтату үшін құпиялылық параметрлерін өзгертті, ал 4,8% қолданбада немесе шолғышта шағым жіберу мүмкіндіктерін пайдаланып адамға шағымданды.

Әрбір оныншы бала бұл жағдайға кінәлі болып, белгілі бір кінә мен жауапкершілікті сезініп, бәрін жүрегіне жақын қабылдады, ал 7,5% интернетті біраз уақытқа тоқтатты.

Бұл әдеттен тыс нәрсе болмаса да, бұл жауаптар біршама алаңдаушылық туғызады:

- біріншіден, олар мәселені шешуге немесе жағдайды айтарлықтай өзгертуге әкелмейді;

- екіншіден, олар психикалық денсаулыққа зиянды әсерлердің, сонымен қатар білім мен дамудың салдарына қаупін арттырады; үшіншіден, мүмкін балалардың интернетті мектеп сабақтары, ақпарат іздеу немесе интернетте болудың басқа артықшылықтарын пайдалану сияқты іс-шараларға пайдалануына әсер етеді.

Кейбір балалар интернетте оларды ренжіткен адамды бұғаттағанын хабарлағанымен, бұл үнемі мәселені шеше бермейді. Мысалы, бір қыз бала оқиғаға тап болды, ол ешқашан кездестірмеген 28 жастағы ер адамның Instagram-да оның суретін көріп, оған қажетсіз хабарламалар жібере бастағанын

сипаттады; немесе тағы бір оқиға бөгде адамның қайта-қайта жеке парақшасына хабарламалар жіберіп, соңынан оның қайда тұратынын біліп алғаны т.с.с оқиғалар жиі кездеседі.

Интернетте болу баланың жақын ортасында болмауы мүмкін бірқатар мүмкіндіктер мен тәжірибелерді ашады. Жаңа адамдармен қарым-қатынас жасау және олармен танысу, олардың ортасында да, сыртында да, ойындар, әлеуметтік желілер немесе басқалар болсын, интернетте болудың ерекше тартымдылығын білдіруі мүмкін платформалар. Дегенмен, бұл ата-аналар мен жалпы ересектер үшін ең үлкен қиындықтардың бірі болуы мүмкін. Мысалы: «Бейтаныс адамдар қауіпті болуы мүмкін» деген ойдан қорқу. Яғни, олар интернетте алғаш танысқан белгісіз адамдардың балаларымен байланысты тәуекелдер. Бейтаныс адамдармен, әсіресе ересектермен әлеуметтік желіде бетпе-бет кездесу балалар үшін өте нақты қауіп болғанымен, бүкіл әлем бойынша деректер балаларға ең үлкен қауіп төндіретінін көрсетеді.

Алайда, балалар бейтаныс адамдар тудыратын қауіптерден шынымен зиян келтіргенде, бұл оқиғалар балаға ең көп зиян келтіреді.

Зерттеуге қатысқан балалардан өткен жылы интернетте алғаш танысқан адаммен желіде жеке кездескендері туралы сұралды. Зерттеуге қатысқан балалардың оннан бір бөлігінен астамы интернетте алғаш танысқандармен желіде жеке кездескен. Ұлдар қыздарға қарағанда жеке кездескенін хабарлау ықтималдығы жоғары (сәйкесінше 10,1% - бен салыстырғанда 12,4%), ал ересек жастағы балалар кішкентай балаларға қарағанда жеке кездесулері айтарлықтай жоғары болды. 15 пен 17 жас аралығындағы әрбір бесінші (18,9%) бала дерлік жеке кездесті, ал 9-10 жастағы балалардың тек 5,9%-ы және 11-12 жастағы балалардың 8,5% - ы интернетте алғаш танысқан адаммен кездескен.

Қыздардан гөрі ер балалар интернетте алғаш танысқан адаммен жеке кездескенімен, қалаларда тұратын балалар интернетте алғаш танысқан адаммен кездескенін екі есе жиі хабарлаған. Қалалардағы балалардың жалпы 14,9% - ы біреумен жеке кездескен, ал ауылдарда тұратын балалардың тек 6,3%-ы алғаш интернетте танысқан адаммен жеке кездескенін хабарлады.

Балалардың Интернеттегі мазмұнға байланысты тәуекелдерге ұшырауы

Балалардың қауіпті, зиянды онлайн мазмұнға ұшырауы кіші жастағы балалармен салыстырғанда ересек жастағы балалар арасында біртіндеп өсіп келе жатқаны байқалады. Жалпы алғанда, 15 пен 17 жас аралығындағы әрбір бесінші бала 11-12 жас аралығындағы он баланың бірімен және 9-10 жас аралығындағы балалардың 13,2%-ымен салыстырғанда тамақтанудың бұзылуымен байланысты мәліметтері бар мазмұндағы ақпаратты көрді. Сол сияқты, 15 пен 17 жас аралығындағы балалар интернетте зорлық-зомбылық немесе қантөгіс бар материалдарды (тиісінше 7,6%-бен салыстырғанда 21,9%) немесе жеккөрушілік мәлімдемелері бар хабарламаларды (7%-бен салыстырғанда 21,1%) үш есе көп көрген.

Осындай тенденцияны өзіне зиян келтіретін мазмұнды көрген балалар арасында анықтауға болады: 15 пен 17 жас аралығындағы балалардың 14,5%-ы, ал 13 пен 15 жас аралығындағы балалардың 9,9% -ы, 11 мен 12 жас

аралығындағы балалардың 6,1% -ы және 9 жастан 10 жасқа дейін 5,9% -ы өзіне зиян келтіретін мазмұндағы ақпараттарды көрген.

Бұл көп уақытын интернетте өткізетін балалар, ересек жастағы балалар интернетте үлкен тәуекелге, қауіп-қатерге ұшырауы мүмкін деп болжауға болады.

Кибербуллингтің тәжірибесі мен әсері

Кибербуллинг – бұл интернетте кездесетін зорлық-зомбылықтың ең көп таралған түрлерінің бірі. Ол әртүрлі формада болуы мүмкін және зерттеулердің, елдердің және аймақтардың салыстырмалы талдауы көбінесе стандартталған анықтамалардың болмауымен бұзылады. Бұл зерттеуде балалардан кибербуллинг болуы мүмкін бірқатар мінез-құлық үлгілері, соның ішінде келемеждеу, алып тастау немесе елемеу, бірнеше рет қоңырау шалу, мазақ ету, олар туралы қауесет тарату, жағымсыз немесе дөрекі хабарламалар жіберу немесе қорқыту және т.б. Бұл міндетті түрде қайталанатын әрекеттерді тудырмады, өйткені интернетте жасалған бір ғана оқиғаның жалғасатын немесе қайталанатын әсерін мойындау артып келеді.

Кибербуллингке байланысты зерттеулер жүргізілді. Әрбір бесінші (21,3%) бала соңғы жылы біреуге жағымсыз немесе ренжітетін хабарламалар жіберілгеніне куә болғанын, ал 16,7% біреу туралы жалған қауесеттер немесе әңгімелер таралғанын көргенін хабарлады. Осыған ұқсас пайыз (16,1%) басқа балалардың интернетте біреуді мазақ еткенін көрді, ал он баланың біреуінен сәл астамы басқа балалардың балаларды елемегенін немесе жоққа шығарғанын, олар туралы ренжітетін немесе жағымсыз хабарламалар жариялағанын немесе интернетте жағымсыз немесе қорлайтын қарым-қатынастың басқа түрлерін бастан өткергенін көрді (тиісінше 13%, 12,7% және 12,5%). Соңғы бір жылда он баланың біреуі (8,5%) интернетте басқа балаларға қауіп төніп тұрғанын көрді.

Кибербуллингке ұшырау ер балаларға қарағанда қыз балалар арасында кибербуллингтің барлық түрлерінде жиі кездеседі. Ұл балаларға қарағанда екі есе көп қыз балалар біреудің жағымсыз немесе ренжітетін хабарламалар жібергенін көргендерін хабарлады (қыздардың 34,5% - ы ұлдардың 18,1%-ымен салыстырғанда), ал қыз балалардың ұл балаларға қарағанда бірдей саны біреудің басқалар туралы жалған қауесет таратқанына, біреуді елемеу немесе жоққа шығару, қорқытудың куәсі болғандарын хабарлады.

Интернетте кибербуллингке куә болған балалардың көпшілігі (52,1%) көргендері туралы ешкімге айтпады. Балалар интернеттен көргендері туралы достарымен ғана бөліскен. Барлығы бес баланың екеуі (40%) достарына көргендері туралы, ал төртеуінің біреуінен (23,5%) оқиға туралы ата-аналарына немесе қамқоршыларына айтқан. Оннан бірінен азы ересек бауырымен немесе 18 жасқа толмаған бауырымен (тиісінше 9,7% және 9,4%) бөліскен.

Балалар өткен жылы кибербуллингке куә болғандары туралы кімге айтты Кибербуллинг көбінесе бетпе-бет қорқытуға қарағанда жиі кездеседі деп есептелсе де, деректер бетпе-бет қорқыту (жәбірлеу) кибербуллингтің басқа түрлеріне қарағанда жиі кездесетінін көрсетеді. Соңғы жылы интернеттегі осындай жағдайлармен салыстырғанда біреудің жеке қарым-қатынас кезінде

(бетпе-бет) балаларды қаншалықты жиі қорлағанын немесе оларға дөрекі қарағанын туралы сұрақтар сұралды. Өзара әрекеттесу жиілігіне қарамастан, өткен жылы интернеттегі қорлау мен дөрекі қарым-қатынаспен балалар бетпе-бет келгенін хабарлады. Бұл тәжірибе қаншалықты кең таралған болса, онлайн және офлайн тәжірибелер арасындағы айырмашылық соғұрлым көп болды. Жалпы алғанда, әрбір оныншы (10,7%) бала соңғы жылы бетпе-бет қорлауға ұшырады, бұл 9,1% онлайн және 5,4% бетпе-бет, ал 3,4% онлайн кем дегенде айына бір рет қорлауға ұшырады. Керісінше, балалардың екі есеге жуығы (1,3%) күнделікті бетпе-бет қарым-қатынас кезінде қорланғанын немесе дөрекі қарым-қатынас жасағанын хабарлады. Балалардың 0,7% желіде, ал аптасына кемінде бір рет бетпе-бет сөйлесу кезінде оларға осылай қаралғанын екі есе жиі хабарлады.

Соңғы бір жылдағы интернеттегі қарым-қатынаспен салыстырғанда, біреу жеке қарым-қатынас кезінде Сізді қорлады немесе дөрекі қарады деген сұраққа жауап талданды.

Кибербуллинг нәтижесінде балаларды құрбан ету қорқытудың әртүрлі түрлеріне ұшыраған балаларды жәбірлеу бірдей бір үлгі бойынша жүрді. Барлығы он баланың біреуінен сәл астамы (11,9%) өткен жылы оларға жағымсыз немесе ренжітетін хабарламалар жіберілгенін айтты, ал 6,5% олар туралы жалған қауесеттер немесе әңгімелер таратылғанын хабарлады. Одан да азы (4,6%) оларды соңғы жылы басқа балалар елемені немесе алып тастағанын хабарлады, ал 4,5% басқа балалар интернетте оларға күлгенін хабарлады. Зерттеуде қарастырылған қорқыту құрбандықтарының барлық түрлерінде қыз балалардың ұл балаларға қарағанда құрбан болғандары туралы хабарлау ықтималдығы жоғары болды.

Жалпы алғанда, қыздардың 14,2%-ы ұлдардың 9,5%-ына қарағанда жағымсыз немесе ренжітетін хабарламалар жіберді, ал интернетте олар туралы жалған қауесеттер қыз балалардың 8,4% - ы, ал ұл балалардың 4,5% - ы таралғанын айтты. Бұл ережеден ерекшелік интернетте қауіп төнгендер болды: ұл балаларға (3%) қыз балаларға (2,5%) қарағанда сәл көбірек қауіп төнгені белгілі болды.

Соңғы жылдағы кибербуллингтің жеке тәжірибесі

Балалардың буллинг реакциясы, әдетте, белсенді және пассивті әрекеттердің жиынтығы. Кибербуллингке ұшырағандардың үштен бірі (33,8%) оларды қорлаған адамды бұғаттады (белсенді), ал төрттен бірінен азы мәселені елемеді және ол өздігінен жойылады деп үміттенді және хабарламаларды жойды (пассивті) (сәйкесінше 23% және 22,9%). Тек оннан бір бөлігі ғана қолданбаның құпиялылық параметрлерін немесе контактілерін өзгертіп, оны мазақ еткен адамды тоқтатты (белсенді). Оннан бірінен сәл астамы буллинг орын алған шолғышты немесе қолданбаны жауып тастады, ал оннан бірінен азы буллинг тоқтайды деп үміттеніп, интернетті пайдалануды біраз уақытқа тоқтатты (екеуі де пассивті).

Кибербуллингке жауап ретінде жасалған әрекеттер

«Мен ол адаммен байланыса алмайтындай етіп бұғаттадым» деп 33,8%

Мәселені елемедім немесе мәселе өздігінен шешіледі деп үміттендім 23%

Бұл адамнан келген барлық хабарламаларды жойдым 22,9%

Басқа адамнан кек алуға тырыстым 13,2 %

Браузер терезесін немесе қосымшаны жаптым 13,3 %

Бірдеңе дұрыс болмағаны үшін мен өзімді кінәлі сезіндім 12%

Құпиялылық/контактілер параметрлерін өзгерттім 10,8 %

Интернетті біраз уақыт пайдалануды тоқтаттым 9,7%

Интернеттегі мәселе туралы хабарладым (мысалы, «бұзушылық туралы хабарлау» түймесін басып, интернет-кеңесшімен немесе жеткізушімен байланысқа шықтым 3,6% жауап берген.

Буллингке ұшыраған балалардың едәуір пайызы (26,6%) өз тәжірибелері туралы ешкімге айтпады, дегенмен бесеуінің екеуі (40,8%) достарына оқиға туралы айтты. Балалардың ата-аналарына немесе қамқоршыларына айтпайты 25,3%. Балалар бұл оқиғалар қаншалықты ауыр немесе ықтимал зиянды болуы мүмкін болса да, интернетте өздерінің жағымсыз тәжірибелерін басқалармен бөліспеуге бейім және егер олар бәрібір біреуге айтса, достарына ғана айтатындығы белгілі.

Балалар кибербуллинг туралы кімге айтты?

Сондай-ақ, балалардан өздерінің мінез-құлқы туралы және интернетте басқаларды қорлағаны туралы сұралды. Бұл балалар айтқысы келмейтін немесе айтудан тартынатын мінез-құлық болуы мүмкін екені түсінікті болғанымен, оннан бірінен көбі (11%) соңғы жылы жеке қарым-қатынаста 8,1%-ы біреуді қорлайтын айтты. Жиырма баланың біреуі ғана (4,8%) мұны кем дегенде айына бір рет жасағанын, жеке қарым-қатынаста да, желіде де не істегенін хабарлағандар туралы айтты.

Соңғы жылы бетпе-бет және онлайн режимінде басқа адамдарға ренжіген немесе қорлаған балалар.

Өткен жылы кибербуллинктің қандай да бір түрі туралы айтқан балалардың ішінде ол ренжітетін немесе қорлайтын хабарламалар (50,5%), біреуді елемеу 45%, біреуді мазақ ету 28,5% немесе интернеттегі басқа баланы қорлау түрінде болуы мүмкін 21,9% -ы жауап берді.

Қауіпсіздік тәуекелдерін бастан кешіру тәжірибесі

Қауіпсіздік тәуекелдері – тұлғааралық құпиялылыққа, институционалдық немесе коммерциялық болып табылатындар байланыс, мінез-құлық, мазмұн немесе сауда санаттарына сәйкес келеді және осы төрт санаттың әрқайсысына жататын өтпелі тәуекелдер болып табылады.

Бұл тәуекелдердің бір бөлігі балалардың, ата-аналарының олардың өміріне араласуына қатысты алаңдаушылықтарымен байланысты, сондай-ақ ықтимал қауіптер мен салдарымен байланысты ата-аналардың балалар өмірінің егжей-тегжейлерін онлайн түрде таратуы қысқа, орта немесе ұзақ мерзімді перспективада тудыруы мүмкін.

Балалардан ата-аналарынан, достарынан мұғалімдерге дейін қоршаған ортадағы басқа адамдармен интернетте ақпарат алмасу, соның ішінде

фотосуреттер немесе олардың өмірі туралы басқа мәліметтер сұралды. Балалардың төрттен бірінен астамы (27,1%) ата-аналары немесе қамқоршылары олар туралы ақпаратты – хабарламалар, суреттер немесе бейнелер түрінде – олардың келісімін сұрамай-ақ орналастырғанын айтты, олардың 12,8% - ы бұл ішінара болғанын, ал 8,8 % - ы бұл туралы жиі немесе өте жиі болғанын хабарлады. Достары олар туралы ақпаратты олардың келісетінін немесе келіспейтінін сұрамай-ақ 8,1% орналастырғанын және бұл ішінара болғанын айтты, ал 3% бұл жиі немесе өте жиі болғанын айтты. Мұғалімдер олар туралы ақпаратты интернетте орналастырды, он баланың біреуінен азы (8,5%) бұл кейде (95,8%) немесе жиі немесе өте жиі (2,7%) болғанын айтты.

Жалпы, Қазақстандағы он баланың біреуінен астамы (13%) ата-аналарынан соңғы уақытта олар (бала) туралы жариялаған нәрселерін жоюды сұрағанын, ал өткен жылы 8% ата-аналарынан олар туралы кейде бір нәрсені жоюды сұрағанын, ал тағы 5% - ы мұны жиі немесе өте жиі жасағанын айтты [11].

Зерттеу нәтижелерін талдай келе, білім алушыларға, ата-аналарға педагогтерге кибермәдениет, кибергигиена, киберқауіпсіздікті сақтау ережелерін білу, цифрлық сауаттылықтарын арттыру маңызды.

Қазақстанда балалардың 15,3%-ы күн сайын интернетте жағымсыз контентпен бетпе-бет келеді: бұл бойынша балалардың құқықтарын қорғау комитетінің ұсынымы

 ҚР Оқу-ағарту министрлігінің бастамасымен ЮНИСЕФ-пен бірлесе жүргізілген "Kazakhstan Kids Online" ауқымды зерттеуі негізінде Қазақстанда балалардың интернетті пайдалануымен байланысты елеулі сын-қатерлер анықталды. Зерттеудің негізгі қорытындысы цифрлық әлемде балалар үшін қауіптерді азайту және қолдау стратегияларын әзірлеуге бағытталған.

 Интернет бала өмірінің маңызды бір бөлігіне айналууда. Зерттеу нәтижесіне сәйкес, балалардың 5%-ы желіге алғаш рет төрт жаста, кей жағдайда тіпті одан да ерте жаста кіреді. Ал 9-10 жас аралығындағы балалардың 60%-ы және 11-12 жас аралығындағы балалардың 66%-ы әлеуметтік желілер мен ойын платформаларында өз аккаунттарына ие.

 Ең алаңдатарлық тұжырымдардың бірі – балалардың 15,3%-ы күнделікті, апта сайын немесе кем дегенде айына бір рет интернетте жағымсыз контентпен бетпе-бет келеді. Ол балалардың 11,7%-ы қатты күйзеліске ұшыраған. Бұл мәселе жас ұрпақ арасында киберқауіпсіздікті күшейтудің тез арада қолға алынуы керек екенін көрсетеді.

 Статистикалық деректерге сүйенсек, кибербуллингке куә болған балалардың басым бөлігі (52,1%) ол туралы ешкімге айтпауды жөн көреді. Ал ата-аналардың 17,6%-ы ғана тыйым салынған контентті бұғаттау және зиянды материалдарды сүзгіден өткізу құралдарын пайдаланады.

 Осы тұста Оқу-ағарту министрлігі Балалардың құқықтарын қорғау комитеті ата-аналарға «Ата-ана бақылауы» қосымшасын ұсынады. Бұл онлайн кеңістікте балалардың қауіпсіздігін қамтамасыз ететін тиімді құрал.

Қолданбаны Play MARKET және APP STORE платформаларынан жүктеуге болады.

«Ата-на бақылауы балалардың интернеттегі қауіпсіздігін қамтамасыз етудің жалпы стратегиясының бір бөлігі ғана. Балалармен ашық диалог жүргізу және олардың онлайн өмірін үнемі талқылау маңызды. Біз ата-аналар, педагогтер, АКТ – мамандары мен БАҚ өкілдерінің интернеттегі балалардың қауіпсіздігін қамтамасыз етуде маңызды рөл атқаратынына сенімдіміз», - деп атап өтті Балалардың құқықтарын қорғау комитетінің төрағасы Насымжан Оспанова.

Комитет ата-аналардың ата-аналар бақылауы қосымшаларын пайдаланудың маңыздылығы туралы хабардар болуын арттыруға және оларды онлайн-кеңістікте балалардың қауіпсіздігін қамтамасыз етудің тиімді әдістеріне үйретуге бағытталған кең ауқымды науқан өткізуді мақсат етеді[12].

Халықаралық стандарттау ұйымы (ISO) тәуекелдерді басқарудың жалпы принциптері мен әдістерін белгілейтін ISO/IEC 31000:2018 стандартын әзірледі. Бұл стандартты балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бағдарламаларын әзірлеу үшін пайдалануға болады.

Еуропалық Одақ интернеттегі азаматтардың қауіпсіздігі мен әл-ауқатын қамтамасыз етуге бағытталған онлайн қауіпсіздік стратегиясын жасады. Бұл стратегия балалардың киберқауіпсіздік, кибергигиена және кибермәдениет туралы хабардарлығын арттыру бойынша бірқатар шараларды қамтиды.

Америка Құрама Штаттары сонымен қатар балалардың киберқауіпсіздік туралы хабардарлығын арттыру бойынша бірқатар бағдарламаларды жүзеге асырады. Мысалы, АҚШ-тың Ұлттық қауіпсіздік департаменті халықтың, соның ішінде балалардың киберқауіпсіздік туралы хабардарлығын арттыруға бағытталған «Барлығына арналған киберқауіпсіздік» бағдарламасын іске қосты.

Ресейде балалардың киберқауіпсіздік туралы хабардарлығын арттыру бойынша бірқатар бағдарламалар жүзеге асырылуда. Мысалы, Ресей Федерациясының цифрлық даму, байланыс және бұқаралық коммуникация министрлігі «Балалардың киберқауіпсіздік туралы хабардарлығын арттыруға және олардың интернеттегі қауіпсіз мінез-құлық дағдыларын қалыптастыруға бағытталған балалық шақтың киберқауіпсіздігі» бағдарламасын іске қосты.

Балаларда цифрлық дағдыларды қалыптастыру бойынша нұсқаулықтар:

Цифрлық оқытуды ерте кезінен бастаңыз. Балалар киберқауіпсіздік және кибергигиена туралы мүмкіндігінше ертерек білуі керек.

Кешенді тәсілді қамтамасыз ету. Оқыту киберқауіпсіздік, кибергигиена және кибермәдениеттің барлық аспектілерін қамтуы керек.

Оқытудың әртүрлі әдістерін қолдану. Оқыту балалар үшін қызықты және тартымды болуы керек.

Ата-аналар мен мұғалімдерді тарту. Ата-аналар мен мұғалімдер балаларды киберқауіпсіздік пен кибергигиена туралы оқытуда маңызды рөл атқарады.

Еуропалық Одақ сонымен қатар балалардағы киберқауіпсіздік пен кибергигиена мәселелеріне көп көңіл бөледі. 2018 жылы Еуропалық Одақ осы саладағы негізгі қызмет бағыттарын анықтайтын киберқауіпсіздік стратегиясын қабылдады. Киберқауіпсіздік стратегиясы шеңберінде балалар мен жастарды киберқауіпсіздік мәселелеріне оқыту жөніндегі бағдарламаларды дамыту көзделген.

АҚШ-та балалар мен жастарды киберқауіпсіздікке үйрету бойынша бірқатар бағдарламалар бар. Мысалы, «CyberSmart» бағдарламасы балаларға киберқауіпсіздік негіздерін үйретуге бағытталған. «I-SAFE» бағдарламасы балалар мен жастарды интернетті қауіпсіз пайдалану мәселелеріне үйретуге бағытталған.

Ресейде балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша жұмыс жүргізілуде. 2022 жылы Ресей Федерациясының цифрлық даму, байланыс және бұқаралық коммуникациялар министрлігі Балалар мен жасөспірімдерде «Интернет» ақпараттық-телекоммуникациялық желісінде қауіпсіз мінез-құлық мәдениетін қалыптастыру бойынша әдістемелік ұсыныстарды бекітті.

Халықаралық тәжірибе көрсеткендей, балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру үшін кешенді және жүйелі оқыту қажет. Оқыту осы салалардың барлық аспектілерін қамтуы керек және әртүрлі оқыту әдістерін қолдана отырып жүргізілуі керек. Ата-аналар мен мұғалімдер балаларды киберқауіпсіздік пен кибергигиена туралы оқытуда маңызды рөл атқарады.

Әлемнің әртүрлі елдерінде жүзеге асырылатын нақты бағдарламалар мен жобалардың үлгілері:

Ұлыбританияда балаларға киберқауіпсіздік негіздерін үйретуге бағытталған «be Internet Legends» бағдарламасы жүзеге асырылуда. Бағдарлама веб-сайтты, мобильді қосымшаны және мұғалімдерге арналған оқу материалдарының жиынтығын қамтиды.

Канадада балалар мен жастарға интернетті қауіпсіз пайдалану мәселелерін үйретуге бағытталған «CyberWISE» бағдарламасы жүзеге асырылуда. Бағдарлама веб-сайтты, мобильді қосымшаны және мұғалімдерге арналған оқу материалдарының жиынтығын қамтиды.

Австралияда балалардың интернеттегі қауіпсіздігін қамтамасыз етуге бағытталған «e-Safety» бағдарламасы жүзеге асырылуда. Бағдарлама веб-сайтты, мобильді қосымшаны және ата-аналарға, мұғалімдерге және басқа ересектерге арналған оқу материалдарының жиынтығын қамтиды.

Ресейде балалар мен жастарды киберқауіпсіздік мәселелеріне үйрету бойынша бірқатар бағдарламалар мен жобалар жүзеге асырылуда. Мысалы, «Сетевичок» жобасы балаларды интернеттегі қауіпсіз мінез-құлыққа үйретуге бағытталған. Жоба веб-сайтты, мобильді қосымшаны және ата-аналарға, мұғалімдерге және басқа ересектерге арналған оқу материалдарының жиынтығын қамтиды.

Халықаралық тәжірибені қорытындылай келе, балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастырудың келесі жалпы принциптерін бөліп көрсетуге болады:

Қатысу принципі. Балалар оқу процесіне және жағымды әдеттерді қалыптастыруға белсенді қатысуы керек.

Жүйелілік принципі. Оқу және жағымды әдеттерді қалыптастыру процесі жүйелі және үздіксіз болуы керек.

Интерактивтілік принципі. Оқыту интерактивті және қарым-қатынасқа негізделген болуы керек.

Көрнекілік принципі. Оқыту көрнекі болуы керек және әртүрлі бейнелеу құралдарын қолдануы керек.

Осы принциптерге сүйене отырып, балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бағдарламасын жасауға болады, оған келесі элементтер кіреді:

Балаларға киберқауіпсіздік, кибергигиена және кибермәдениет негіздерін үйрету. Оқыту балалардың жас ерекшеліктеріне және жеке ерекшеліктеріне бағытталуы керек.

Балалардың интернеттегі қауіпсіз мінез-құлық дағдыларын дамыту. Балалар интернеттегі қауіптерді тануды және олардың алдын алу үшін шаралар қабылдауды үйренуі керек.

Балалардың киберқауіпсіздікке, кибергигиенаға және кибермәдениетке жағымды көзқарасын қалыптастыру. Балалар бұл сұрақтардың маңыздылығын түсініп, интернеттегі қауіпсіз мінез-құлыққа ынталандырылуы керек.

Балалардың киберқауіпсіздігіне, кибергигиенасына және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру жөніндегі бағдарламаны іске асыруды балалармен жұмыс істейтін ата-аналар, педагогтер және басқа да ересектер жүзеге асыруы тиіс.

Қазіргі әлемде балалар жас кезінен бастап цифрлық технологиялармен бетпе-бет келеді. Олар оларды оқу, қарым-қатынас, ойын-сауық және басқа мақсаттар үшін пайдаланады. Сондықтан балалардың киберқауіпсіздік, кибергигиена және кибермәдениеті туралы түсініктері болуы және осы салаларда жағымды әдеттер қалыптастыруы маңызды.

Киберқауіпсіздік – бұл алаяқтық, киберқылмыс және зиянды бағдарламалар сияқты интернеттегі әртүрлі қауіптерден қорғану мүмкіндігі.

Халықаралық стандарттау ұйымы (ISO) ISO/IEC 27032:2012 «Ақпараттық қауіпсіздік. Интернеттегі балалардың қауіпсіздігін қамтамасыз ету бойынша ұсыныстар». Бұл стандарт балалардың интернеттегі қауіпсіздігін қамтамасыз ету бойынша ұсыныстарды, соның ішінде келесі аспектілерді қамтиды:

Балаларды интернетті қауіпсіз пайдалануға үйрету: балалар Интернеттегі алаяқтық, киберқылмыс және зиянды бағдарламалар сияқты әртүрлі қауіптер туралы білуі керек. Олар сондай-ақ өздерін осы қауіптерден қалай қорғауға болатындығын білуі керек.

Күшті құпия сөздерді пайдалану: балалар интернеттегі жазбалары үшін күшті құпия сөздерді қолдануы керек. Құпия сөздер күрделі және әріптер, сандар мен таңбалардан тұруы керек.

Қауіпсіздік жаңартуларын орнату: балалар өз құрылғыларына қауіпсіздік жаңартуларын орнатуы керек. Қауіпсіздік жаңартулары құрылғыларды зиянды бағдарламалардан қорғауға көмектеседі.

Еуропалық комиссия сонымен қатар балалардың онлайн қауіпсіздігін қамтамасыз ету бойынша бірқатар ұсыныстар әзірледі. Бұл нұсқаулар келесі аспектілерді қамтиды:

Ата-аналар мен балаларды оқыту: ата-аналар мен балалар интернеттегі әртүрлі қауіптер туралы және олардан қалай қорғану керектігін білуі керек.

Жеке деректерді қорғау: балалар өздерінің жеке деректерін бейтаныс адамдарға бермеуі керек.

Интернеттегі байланыс қауіпсіздігі: Балалар интернетте кіммен сөйлесетініне абай болу керек.

Онлайн төлем қауіпсіздігі: балалар онлайн төлемдерді жасау кезінде абай болу керек.

Кибергигиена – бұл цифрлық технологияны қолданумен байланысты физикалық және психологиялық мәселелерден қорғануға көмектесетін ережелер мен процедуралар жиынтығы.

Дүниежүзілік денсаулық сақтау ұйымы (ДДҰ) балаларға арналған кибергигиена бойынша бірқатар ұсыныстар жасады. Бұл нұсқаулар келесі аспектілерді қамтиды:

Балалардың интернетте өткізетін уақытын шектеу: балаларға күніне екі сағаттан аспайтын уақытты компьютерде немесе басқа цифрлық құрылғыларда өткізуге кеңес беріледі.

Дұрыс қалып: балаларға омыртқа жотасы мен көру проблемаларын болдырмау үшін компьютерде немесе басқа цифрлық құрылғыларда дұрыс отыру маңызды.

Тұрақты үзілістер: балаларға компьютерде немесе басқа цифрлық құрылғыларда үнемі үзіліс жасау ұсынылады.

Дене белсенділігі: балалар күніне кемінде 60 минут физикалық белсенділікпен айналысуы керек.

Кибермәдениет – бұл адамдардың интернеттегі мінез-құлқын реттейтін нормалар мен құндылықтардың жиынтығы.

ЮНЕСКО балаларға арналған кибермәдениет бойынша бірқатар ұсыныстар әзірледі. Бұл нұсқаулар келесі аспектілерді қамтиды:

Басқа адамдарға құрмет: балалар жасына, жынысына, ұлтына немесе дініне қарамастан интернеттегі басқа адамдарды құрметтеуі керек.

Сындарлы қарым-қатынас: Балалар интернетте қорлау мен кемсітушілікке жол бермей, сындарлы әрекет етуі керек.

Шындық пен жауапкершілік: балалар жалған немесе жаңылыстыратын ақпаратты таратпау үшін интернетте адал және жауапты болуы керек.

Жеке өмірді қорғау: балалар жеке өмірін бейтаныс адамдармен жеке ақпаратпен бөліспей-ақ онлайн режимінде қорғауы керек.

Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастырудың халықаралық тәжірибесі балалардың қауіпсіздігі мен әл-ауқатын қамтамасыз ету үшін ата-аналардың, тәрбиешілердің және басқа ересектердің күш-жігерін біріктіру қажет екенін көрсетеді. Тек бірлескен күш-жігермен біз балаларға цифрлық технологияны қауіпсіз және жауапкершілікпен пайдалануға үйрете аламыз.

Білім беру ұйымдарындағы зорлық-зомбылықтың алдын алу бойынша заңнамалық нормативтік құжаттар

Білім беру ұйымдарында буллингтің алдын алу саласында жұмысты ұйымдастыру және жүргізу кезінде Қазақстан Республикасы мен Қарағанды облысының аумағында қолданылатын тиісті нормативтік құқықтық актілерді басшылыққа алу қажет.

- Қазақстан Республикасының конституциясы 1995 жылы 30 тамыз;
- «Бала құқығы туралы БҰҰ конвенциясы»;
- Қазақстан Республикасының 2002 жылғы 8 тамыздағы №345 «Қазақстан Республикасындағы Баланың құқықтары туралы» Заңы;
- Қазақстан Республикасының «Неке (ерлі-зайыптылық) және отбасы туралы» Кодексі (01.04.2019 ж. жағдай бойынша өзгерістермен және толықтырулармен);
- Қазақстан Республикасының 2007 жылғы 27 шілдедегі «Білім туралы» Заңы (19.04.2019 ж. өзгерістермен және толықтырулармен);
- 2014 жылғы 5 шілдедегі Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы Кодексі;
- Қазақстан Республикасы Білім және ғылым министрінің м. а. 2016 жылғы 8 қаңтардағы № 9 бұйрығымен бекітілген «Педагогикалық әдептілік ережелері»;
- Білім беру ұйымдарының ішкі құжаттары (жарғы, жергілікті актілер, бұйрықтар, нұсқаулықтар) ішкі өкімдік ережелер, оқу- тәрбие қызметін және тәртіп пен қауіпсіздікті сақтауды реттейді.

Бала құқығының конвенциясы

- 16-бап: Бірде бір бала оның жеке өміріне, отбасылық өміріне, баспанасына қол сұғылмау немесе хат жазысып-алысу құпиясына не болмаса оның ар-намысы мен абыройына заңсыз араласушылықты болдырмау құқығын жүзеге асыруда ерікті түрде немесе заңсыз араласу объектісі бола алмайды. Бала осындай араласу немесе қол сұғушылықтан заңның қорғауына құқылы.

- 19-бап: Қатысушы мемлекеттер баланың тәніне жасалатын немесе психологиялық түрдегі зорлық-зомбылықтың, қорлау немесе теріс қылықтардың барлық нысандарынан, қамқорлықтың жоқ болуынан немесе немқұрайды қараудан, дөрекі қараудан неболмаса пайдаланудан, ата-анасының, заңды қамқоршыларының немесе балаға қамқорлық жасаушы басқа адамның нәпсіқұмарлық қиянатынан қорғау мақсатында барлық заңды, әкімшілік, әлеуметтік және ағартушы шараларын қабылдайды.

Қатысушы мемлекеттер баланың тәніне жасалатын немесе психологиялық түрдегі зорлық-зомбылықтың, қорлау немесе теріс қылықтардың барлық нысандарынан, қамқорлықтың жоқ болуынан немесе немқұрайды қараудан, дөрекі қараудан не болмаса пайдаланудан, ата-анасының, заңды қамқоршыларының немесе балаға қамқорлық жасаушы басқа адамның нәпсіқұмарлық қиянатынан қорғау мақсатында барлық заңды, әкімшілік, әлеуметтік және ағартушы шараларын қабылдайды.

Қазақстан Республикасының Конституциясы

- *1-бап* Қазақстан Республикасы өзін демократиялық, зайырлы, құқықтық және әлеуметтік мемлекет ретінде орнықтырады, оның ең қымбат қазынасы - адам және адамның өмірі, құқықтары мен бостандықтары.

- *18-бап:* Әркімнің жеке өміріне қол сұғылмауына, өзінің және отбасының құпиясы болуына, ар-намысы мен абыройлы атының қорғалуына құқығы бар.

- *34 бап:* Әркім Қазақстан Республикасының Конституциясын және заңдарын сақтауға, басқа адамдардың құқықтарын, бостандықтарын, абыройы мен қадір-қасиетін құрметтеуге міндетті.

Қазақстан Республикасының 2002 жылғы 8 тамыздағы №345 «Қазақстан Республикасындағы баланың құқықтары туралы» Заңының

1) 1-бап мынадай мазмұндағы 4-1) тармақшамен толықтырылды:

«4-1) баланы жәбірлеу (буллинг) – қорлау сипатындағы жүйелі (екі және одан көп) әрекеттер, қудалау және (немесе) қорқыту, оның ішінде қандай да бір әрекетті жасауға немесе жасаудан бас тартуға мәжбүрлеуге бағытталған әрекеттер, сол сияқты жария түрде немесе бұқаралық ақпарат құралдары және (немесе) телекоммуникация желілері пайдаланыла отырып жасалған дәл сол әрекеттер (кибербуллинг)»;

2) 10-баптың 2-тармағы. Мемлекет баланың жеке басына ешкімнің тиіспеуін қамтамасыз етеді, оны физикалық және (немесе) психикалық күш көрсетуден, адамның қадір-қасиетіне қатыгездікпен, дөрекілікпен қараудан немесе оны қорлаудан, баланы жәбірлеуден (буллингтен), жыныстық қатынас сипатындағы әрекеттерден, баланы қылмыстық іс-әрекетке және қоғамға жат әрекеттер жасауға тартудан, және оны адам мен азаматтың Қазақстан Республикасының Конституциясында бекітілген құқықтары мен бостандығына қысым жасаудың өзге де түрлерінен қорғауды жүзеге асырады.

36-бап: Баланы әлеуметтік ортаның теріс ықпалынан қорғау:

- Мемлекеттік органдар, жеке және заңды тұлғалар баланы оның денсаулығына, имандылық жағынан және рухани дамуына зиян келтіретін әлеуметтік ортаның, ақпараттың, насихат пен үгіттің теріс ықпалынан қорғауға міндетті.

- Салауатты өмір салтын насихаттау мен балаға құқықтық білім беруді мемлекет өз саясатының басым бағыттарының бірі деп таниды.

- Қылмыстық құқық бұзушылықтың, зорлық-зомбылықтың немесе өзге де заңсыз әрекеттің салдарынан тән немесе жан жарақатын алған балаға денсаулығын қалпына келтіру және әлеуметтік бейімделу үшін қажетті көмек

көрсетілуге тиіс.

- 6 бап: Балалар мүддесін көздейтін мемлекеттік саясат мемлекеттік органдар қызметінің басым саласы болып табылады және баланың құқықтарын заң тұрғысынан қамтамасыз етуге; балаларға толымды тәрбие беруді, олардың құқықтарын қорғауды оларды қоғамда толымды өмір сүруге дайындауды қамтамасыз ету мақсатында отбасын мемлекеттік қолдауға; аймақтық ерекшеліктерді ескере отырып, балалардың өмірін жақсартуға бағытталған мемлекеттік ең төменгі әлеуметтік стандарттарды белгілеуге және сақтауға; баланың құқықтары мен заңды мүдделерін бұзғаны, оған зиян келтіргені үшін лауазымды тұлғалардың, азаматтардың жауаптылығына; баланың құқықтары мен заңды мүдделерін қорғау жөніндегі функцияларды жүзеге асыратын қоғамдық бірлестіктер мен өзге де ұйымдарды мемлекеттік қолдауға негізделген.

«Қазақстан Республикасының Білім туралы» Заңы

- 48-бап 6-тармақ «білім беру ұйымдарында оқытудың, тәрбиелеудің, еңбек пен демалудың салауатты және қауіпсіз жағдайларын жасау үшін жауапкершілік олардың басшыларына жүктеледі».

- 28-бап: «Оқу-тәрбие процесі білім алушылардың, тәрбиеленушілердің, педагог қызметкерлердің адами қадір-қасиетін өзара құрметтеу негізінде жүзеге асырылады. Білім алушылар мен тәрбиеленушілерге қатысты физикалық, моральдық және психикалық зорлық-зомбылық әдістерін қолдануға жол берілмейді.»

- 51-бап: «педагог қызметкер білім алушылардың, тәрбиеленушілердің және олардың ата-аналарының немесе өзге де заңды өкілдерінің ар-намысы мен қадір-қасиетін құрметтеуге, білім алушыларды жоғары адамгершілік, ата-аналарды, этномәдени құндылықтарды құрметтеу, қоршаған ортаға ұқыпты қарау рухында тәрбиелеуге міндетті».

«Педагогикалық әдеп қағидаларын бекіту туралы» Қазақстан Республикасы Білім және ғылым министрінің м.а. 2016 жылғы 8 қаңтардағы № 9 бұйрығы:

Педагог мектеп ұжымында сенім білдіру және құрметтеу ахуалын жасауға мүмкіндік туғызады, өзінің абыройын және қадір-қасиетін құрметтеу: педагог өзінің кәсіби назарындағы объектілер болып табылатын оқушының, ата-ананың, адамдардың абыройы мен қадір-қасиетін құрметтейді, олармен қарым-қатынас жасауда өнегелі. Ол баланың дамуын шынымен қалап, оған әрқашан көмектесуге дайын екендігін білдіріп, білім алушының жетістігін (жетіспеушілігін) бағалауда әдептілік танытады. өзінің абыройын және қадір-қасиетін құрметтеу: педагог өзінің кәсіби назарындағы объектілер болып табылатын оқушының, ата-ананың, адамдардың абыройы мен қадір-қасиетін құрметтейді, олармен қарым-қатынас жасауда өнегелі. Ол баланың дамуын шынымен қалап, оған әрқашан көмектесуге дайын екендігін білдіріп, білім алушының жетістігін (жетіспеушілігін) бағалауда әдептілік танытады. Білім беру процесін қатысушыларына қатысты күш көрсету, моральдық және психикалық қысым жасау әдістерін қолдануға мүлдем жол бермейді; Педагог

ұлттаралық қатынастар мәдениетін тәрбиелейді, білім алушыларды жасына, жынысына, тіліне, ұлтына, діни көзқарасына, азаматтығына, шығу тегіне, әлеуметтік, лауазымдық және мүліктік жағдайына немесе өзге декез келген жағдайларға қарамастан барлық ұлттар мен барлық адамдардың құқығы мен қадір-қасиетін құрметтеуге үйретеді; мектеп ұжымында сенім білдіру және құрметтеу ахуалын жасауға мүмкіндік туғызады.

Білім беру ұйымдарының қызметкерлеріне арналған ішкі еңбек тәртібінің ережелерінде педагогикалық және еңбек этикасының нормалары, білім беру ұйымының басшылығы оқушыларға немесе өз әріптестеріне қатысты құрметтемеуге, кемсітуге, қорқытуға, қорлауға, физикалық және психологиялық зорлық-зомбылыққа жол беретін қызметкерлерге қолданатын шаралар, сондай-ақ оқушылар тарапынан қорлауға немесе зорлық-зомбылыққа ұшыраған қызметкерлерді қорғау жөніндегі шаралар көрсетіледі.

Білім беру ұйымдарының ішкі құжаттары (жарғы, жергілікті актілер, бұйрықтар, нұсқаулықтар) Оқу-тәрбие қызметін және тәртіп пен қауіпсіздікті қолдау шараларын реттейді. Олар білім беру ұйымдарының аумағында және үй-жайларында, сабақтарда, әртүрлі сипаттағы зорлық- зомбылық әрекеттерін жасау ережелерін анықтайды және ережелерді бұзғаны үшін санкцияларды қарастырады.

Зорлық-зомбылық фактілері жасырылмауы тиіс:

Қазақстан Республикасының кейбір заңнамалық актілеріне баланың құқықтарын қорғау жөніндегі функцияларды жүзеге асыратын ұйымдардың қызметіне байланысты мәселелер бойынша өзгерістер ментолықтырулар енгізу туралы ҚР Заңына, атап айтқанда 2014 жылғы 5 шілдедегі Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы Кодексіне (2014 ж., 127-1-бап. «Кәмелетке толғандар немесе кәмелетке толмағандарға қатысты құқыққа қарсы әрекеттер туралы хабарламау. Білім беру, денсаулық сақтау, халықты әлеуметтік қорғау ұйымдары қызметкерлерінің құқық қорғау органдарына кәмелетке толмағандардың қылмыстық не әкімшілік құқық бұзушылық белгілері бар іс- әрекеттер (әрекетсіздік) жасау фактілері туралы немесе оларға қатысты білім беру, денсаулық сақтау, халықты әлеуметтік қорғау ұйымдарында, сондай-ақ білім беру, денсаулық сақтау, халықты әлеуметтік қорғау ұйымдарынан тыс кәсіби қызметіне байланысты өздеріне белгілі болған фактілер туралы хабарламауы, егер бұл әрекеттерде қылмыстық жаза қолданылатын, Қазақстан Республикасы Қылмыстық кодексінің 434 бабында көзделген айыппұл салуға әкеп соғады, - жеке тұлғаларға - бес айлық, лауазымды адамдарға - он айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады»[13] .

Ата-аналардың әлеуетін белсенді пайдалану:

Қазақстан Республикасының Неке (ерлі-зайыптылық) және отбасы туралы Кодексінің 71-бабы (01.04.2019ж. берілген өзгерістер мен толықтырулармен) 1- тармақ «ата-аналар өз баласының заңды өкілдері болып табылады және кез келген жеке және заңды тұлғалармен қатынастарда оның құқықтары мен мүдделерін қорғайды»[14].

3. Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша әдістемелік ұсынымдар

Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру ата-аналар, тәрбиешілер және басқа ересектер үшін маңызды міндет.

Білім беру ұйымдарында білім алушыларды интернет кеңістігінде қауіпсіздік ережелеріне үйретуге, интернетке тәуелділіктің, жастар ортасындағы ұлтшылдық көріністердің алдын алуға және жасөспірімдерді құқыққа қарсы іс-әрекетке тарту қаупін жоюға бағытталған іс-шаралар жүйесін іске асыруын қамтамасыз ету маңызды.

Интернетте де шынайы өмірдегідей білім алушыларға қауіп төніп тұр: әлеуметтік желілерде қажетсіз мазмұнның болуы, алдау және бопсалау, қысқа нөмірлер ақылы SMS, зорлық-зомбылық пен экстремизмді насихаттау, құмар ойындар мен интернетке тәуелділік және т. б.

Интернетке тәуелділік – бұл интернетке қосылуға деген ұмтылыс және интернеттен уақытында ажырай алмау. Әр түрлі зерттеулерге сәйкес, интернетке тәуелді адамдар бүгінде бүкіл әлемдегі қолданушылардың шамамен 10% құрайды. Атап айтқанда, кейбір білім алушылардың виртуалды кеңістікке құмарлығы сонша, олар күніне 18 сағатқа дейін компьютерде отырып, интернетті шынайы өмірден артық көре бастайды. Интернетке тәуелділіктің түрлері – интрузивті веб-серфинг, виртуалды қарым-қатынас пен виртуалды танысуға тәуелділік (кең көлемдегі хат-хабарлар, чаттарға, веб-форумдарға үнемі қатысу, желідегі таныстар мен достардың артықтығы), ойынға тәуелділік – бұл желідегі компьютерлік ойындарға деген құмарлық.

Осындай тәуекелдерге байланысты мұғалімдердің міндеті – бұл тәуекелдерді көрсету, ойланбаған әрекеттерден ескерту, білім алушылардың интернеттен алынған ақпаратқа сыни көзқарасы дағдыларын қалыптастыру, интернетті қауіпсіз пайдалану мәдениетіне тәрбиелеу. Сондай-ақ, компьютермен жұмыс істеу кезінде сақталуы керек гигиеналық талаптарға назар аудару керек:

- Негізгі орта және жоғары сынып деңгейіндегі білім алушыларына күніне екі сағатқа дейін монитор алдында жарты сағат сайын 10-15 минуттық үзіліс жасауға болады;

- Бастауыш сынып деңгейіндегі білім алушыларына компьютерде күніне 15 минуттан аспайтындай, сынып-сабақ кезінде бір сабақтан аспауы, ал офтальмологтың қарсы көрсетілімдері болған жағдайда аптасына 3 реттен 10 минут аспайтындай ғана отыруы керек;

- Компьютерде күннің бірінші жартысында жұмыс істеген дұрыс;
- компьютерде жұмыс істегенде бөлме жақсы жарықтандырылуы керек;
- көзден мониторға дейінгі қашықтық - 60 см;
- көзге мезгіл-мезгіл жаттығулар жасау т.б.

Жалпы мемлекеттік білім беру стандарттарына сәйкес білім беру

бағдарламасының құрылымына салауатты және қауіпсіз өмір салты мәдениетін қалыптастыру сияқты бағытты қамтитын білім алушыларды тәрбиелеу және әлеуметтендіру бағдарламасы кіреді. Осы бағдарлама шеңберінде мектеп оқушылары арасында интернет желісінде қауіпсіз жұмыс істеу дағдыларын меңгерудің маңыздылығын насихаттайтын ақпараттық-ағарту жұмыстары жүзеге асырылуы мүмкін.

Білім беру ұйымдарында білім алушылар үшін ақпараттық қауіпсіздік негіздері бойынша сабақтар өткізу; ата-аналарды балалар мен жасөспірімдердің интернет желісінің ресурстарына қолжетімділігін шектейтін, тәрбие міндеттеріне сәйкес келмейтін заманауи бағдарламалық-техникалық құралдармен таныстыру және білім беру ұйымдарында кәмелетке толмағандардың ақпараттық қауіпсіздігі сақтау.

Бастауыш мектеп оқушыларымен жұмыс кезінде ойын әдістерін қолданған жөн.

Негізгі орта білім деңгейінде білім алушылар интернетті белсенді қолдана бастайды. Сонымен қатар, олар музыка жүктейді, электрондық поштаны пайдаланады, онлайн ойындар ойнайды және т.б. Осы жастағы білім алушылар ересектердің рұқсатынсыз интернет желісінде адамдардың не істей алатынын білгісі келетіні қалыпты жағдай. 10-15 жас аралығындағы білім алушылардың интернет-қауіпсіздігін қамтамасыз ету үшін мұғалімдерге:

- Білім алушыларды интернеттегі жауапты, лайықты мінез-құлықпен таныстыру;

- Интернет желісін қауіпсіз пайдаланудың негізгі қауіптері мен ережелері туралы айту;

- ешқашан жеке ақпаратты, соның ішінде жеке профильдер және онлайн конкурстарға тіркелу кезінде фамилиясын, атын, үй мекен-жайын, телефон нөмірлерін, мектеп атауын, электрондық пошта мекен-жайын, достарының немесе туыстарының тегін, жедел хабар алмасу бағдарламаларындағы аттарын, жасын немесе туған күнін, электрондық пошта арқылы, чаттарда, жедел хабар алмасу жүйелерінде, тіркеу нысандарында бермеуге сендіру;

- интернеттегі достармен ересектердің қатысуынсыз жеке кездесулердің қауіптілігін түсіндіру;

- желідегі кез келген нәрсе немесе біреу оларды алаңдатып немесе қорқытып жатқанын хабарлау керектігін түсіндіру;

- форумдар мен чаттардағы мінез-құлық ережелерімен таныстыру, оларды бұзақылық жасау, өсек тарату немесе басқа адамдарға қауіп төндірмеу үшін желіні пайдаланбау керектігін түсіндіру.

Интернеттегі ақпаратты қауіпсіз пайдалану бойынша жоғары сынып оқушыларымен жұмысты ұйымдастыра отырып, білім беру ұйымында пайда болатын бейресми жастар бірлестіктеріне назар аудару керек. Жасөспірімдердің желілік қауіпсіздігі күрделі міндет, өйткені олар ата-аналарына қарағанда интернет туралы көбірек біледі. Дегенмен, ересектердің қатысуы да қажет:

Жасөспірімдермен интернеттегі достары және олар не істейтіні туралы

сөйлесу қажет. Жасөспірімдер лезде хабар алмасу арқылы сөйлесетін адамдар туралы сұрау және бұл адамдар оларға таныс екеніне көз жеткізіп отыру керек.

Қазіргі уақытта интернет-ресурстардың жас ұрпаққа теріс әсер ету мәселесі өткір тұр, және оны жеңу мамандардың психологтердің, мұғалімдердің, дәрігерлердің араласуын талап етеді.

Алайда, бұл құбылыстың алдын-алу көбінесе ата-аналарға байланысты. Бала компьютерде өткізетін уақытын саналы түрде басқарғысы келмейді немесе ересектер басқа позицияға ие болса, экрандағы зорлық-зомбылықтың негізгі қарсыласы бола алмайды. Ата-аналардың басты міндеті – медиа мүмкіндіктерін балаға зиян келтірмей, денсаулық пен дамудың пайдасына бұруға тырысу.

Балалар білуі тиіс:

- интернетте өзіңіздің жеке ақпаратыңызды, оның ішінде мекен-жайыңызды, телефондарыңызды, туыстарыңыздың аты-жөні мен жұмыс орнын және т. б. жарияламау;

- егер әлеуметтік компьютерлік желілерде байланыс жасайтын адам жеке таныс болмаса, онда олармен байланыс өте мұқият болуы керек;

- аты-жөні таныс емес адамдардың хаттары мен хабарламаларына жауап берудің қажеті жоқ. Мұндай жағдайларда ең жақсы әдіс хатты жою немесе белгісіз пайдаланушыны әлеуметтік желіде немесе электрондық пошта жүйесінде бұғаттау;

- интернеттегі қарым-қатынас процесінде пайда болатын кез-келген қауіпті жағдай туралы, қандай да бір қауіп-қатер, бопсалау немесе кездесуге деген тұрақты ұсыныстар және т.б. жағдайда бала ересектерге хабарлауы керек. Ол мұны істеу үшін ата-ана оған әрдайым көмекке келетіндігіне және оны қолдайтындығына сенімді болуыңыз керек;

- әдетте әңгімелесушілер көп болатын форумда пікір алмасу жақсы. Әлеуметтік желілердегі жасөспірім үшін ең «қауіпті» орындар жеке хабарламалар, олар бір-бірімен сол сәтте сөйлесетін пайдаланушылар ғана көреді;

- медиа ақпаратқа, оның ішінде интернеттегі ақпаратқа сыни көзқараспен қарау керек, оны тексеру және сыни талдау қажет.

Ата-ана білуі керек:

- егер сіздің балаңыз әлеуметтік желілерде тұрақты болса, олар үшін ең қызықты тақырыптарды бірлесіп талқылауды тәжірибеге енгізуге тырысыңыз. Сіздің пікіріңіз ол үшін қызықты және пайдалы болуы мүмкін. Баланың байланыстарынан хабардар болу үшін оның өмірдегі шынайы досы ғана емес, сонымен қатар желідегі виртуалды досы болыңыз, осылайша сіз онымен сөйлесуге, сондай-ақ виртуалды кеңістікте болып жатқан оқиғалар туралы білуге көбірек мүмкіндік аласыз;

- онлайн ойындарға қатысу көптеген жасөспірімдерді қатты қызықтырады. Алайда, мұндай ойындардың көпшілігінде құмар ойындар мен сауда-саттықтың әртүрлі түрлері бар. Егер сіз баланың сізден «ойынға» ақша беруіңізді сұрайтынын байқасаңыз, оның мазмұнын түсінуге тырысыңыз. Мұның ең жақсы тәсілі –қызығушылық: балаңыз құмар ойынға қызығушылық

танытса, оның негізгі оқиғалары туралы хабардар болуға тырысыңыз;

- медиа әлемі тек қауіп-қатерді ғана емес, сонымен бірге білім мен дамудың үлкен мүмкіндіктерін де қамтиды. Сондықтан, балаңызбен бірге тек ойын ғана емес, сонымен бірге интернеттің танымдық ресурстарын да белсенді түрде ашыңыз.

Есіңізде болсын:

- кез-келген қарым-қатынас сенімді және серіктестік негізде құрылуы керек. Бұл жерде отбасылық қатынастар да ерекшелік емес;

- балаға виртуалды кеңістікті шарлауға және оны ықтимал қауіптерден қорғауға көмектесу үшін осы әлемде өмір сүруді үйренуіңіз керек;

Тәрбиенің міндеті – баланы қажетсіз қателіктерден қорғау ғана емес, сонымен қатар оны өз өмірінде саналы түрде маңызды таңдау жасауға үйрету.

Баланың медиаәлемнің қауіп-қатеріне ұшырап қана қоймай, ақпарат ағынында саналы әрекет ету маңызды.

Балалар мен жасөспірімдердің ақпараттық қауіпсіздігінің жай-күйін бағалау критерийлерін айқындау мыналарды ескереді:

1. ақпараттың ресурстық әлеуеті;
2. аудиторияның психологиялық ерекшеліктеріне байланысты ақпараттық мазмұнның мазмұны мен формасы;
3. балалар мен жасөспірімдердің жеке және ақыл-ой дамуы үшін жағдайлардың болуы;
4. балалар мен жасөспірімдердің психикалық және психологиялық денсаулығын және амандығын сақтау үшін жағдайлардың болуы;
5. ақпараттық өнімнің моральдық-адамгершілік мазмұны; ақпараттық өнімнің көркемдік-эстетикалық қасиеттері.

«ҚАУІПСІЗ ИНТЕРНЕТ» ТАҚЫРЫП БОЙЫНША САБАҚ ЖОСПАРЫ (5-9 СЫНЫПТАРҒА АРНАЛҒАН)

Мақсаты: кәмелетке толмаған білім алушыларға қазіргі ақпараттық-телекоммуникациялық ортада жауапкершілікті және қауіпсіз мінез-құлық дағдыларын үйрету арқылы олардың ақпараттық қауіпсіздігін қамтамасыз ету.

Міндеттері:

- интернеттегі қауіпсіз жұмыс туралы пайдаланушылардың хабардар болуын зерттеу;
- интернет желісінде қауіпсіз жұмыс істеу ережелерімен танысу;
- ақпараттық кеңістікте бағдарлау;
- Онлайн-технологияларды жауапкершілікпен пайдалануға ықпал ету;
- білім алушылардың ақпараттық мәдениетін қалыптастыру және web-ресурстарды пайдалана отырып, қажетті ақпаратты өз бетінше таба білуі;
- желіде жұмыс істеу кезіндегі тәртіпті сақтауға тәрбиелеу.

Білім алушылар білуі тиіс:

- интернет желісінің ақпараттық қызметтерінің тізімі;
- интернет желісінде қауіпсіз жұмыс істеу ережесі;
- ғаламдық компьютерлік желінің қауіптілігі.

Білім алушылар дағдысының болуы:

- Онлайн-технологияларды пайдалануға жауапкершілікпен қарау;
- веб-шолғышпен (web-браузер) жұмыс істеу;
- ақпараттық ресурстарды пайдалану;
- интернеттен ақпарат іздеу.

Сабақ түрі: жаңа материалды үйрену сабағы.

Оқыту әдістері мен формалары: ауызша (пікірталас, әңгіме), бейне әдіс, көрнекі, (демонстрация), практикалық; ішінара іздеу, проблемалық, қызығушылықты ынталандыру әдісі; оқытудың интерактивті түрі (пікір алмасу, ақпарат).

Веб-ресурстарға сілтемелер:

- 1) «Касперский зертханасы» антивирусы[15];
- 2) қауіпсіз веб-аймақ[16];
- 3) <http://www.interneshka.net> – интернетті қауіпсіз пайдалану бойынша халықаралық онлайн-конкурс;
- 4) интернетті қауіпсіз пайдалану жөніндегі портал[17];
- 5) <http://content-filtering.ru> – «сіздің жеке интернетіңіз» интернет БАҚ;

Сабақ кезеңдері:

1. Сабақты ұйымдастыру. Сабақтың мақсатын қою.
2. Бейне материалды қарау [18]
3. Сабақтың тақырыбы және сабақта негізгі мәселені қою.
2. Жаңа материалды зерттеу. Топтағы пікірталас. Сұрақты теориялық жариялау (білім алушылардың хабарламалары).
3. Практикалық жұмыс. Интернеттен ақпарат іздеу. Табылған материал

бойынша пікірталас.

4. Зерттелген материалды бекіту. Интернеттегі қауіпсіз жұмыс ережелері бойынша ұсыныстар.

5. Тестілеу.

6. Сабақты қорытындылау. Топтың жұмысын бағалау. Үй тапсырмасы.

Сабақ барысы

1. Сабақты ұйымдастыру. Сабақтың мақсатын қою.

Ғаламдық желінің дамуы біздің әдеттегі өмір салтымызды өзгертті, біліміміз бен тәжірибеміздің шекарасын кеңейтті. Енді бүкіл әлем бойынша миллиондаған компьютерлерде сақталған кез-келген ақпаратқа қол жеткізу мүмкіндігі пайда болды. Бірақ екінші жағынан, миллиондаған компьютерлер компьютеріңізге кіруде қолжетімдік бар. Күмәнданбаңыз, олар оны пайдаланады, бұл олар үшін мүмкіндік. «Балалар және интернет» бейне-ролигін көру – 1 мин. (таңдау бойынша)

- youtube-те қалай қауіпсіз болуға болады[19,20]

- Интернеттегі ойын-сауық және қауіпсіздік [21]

- интернеттегі алаяқтықтан сақ болыңыз [22]

- Спамнан қорғау[23]

Интернет желісінің құрбаны болмауға қалай болады? Біздің сабағымыздың тақырыбы – *«Қауіпсіз Интернет»*.

Сабақтың басты мәселесі: Желідегі жұмысты қалай қауіпсіз етуге болады?

2. Жаңа материалды зерттеу.

«Қолдаймын-қолдамаймын» ойыны (4 мин).

Тақтадағы бірнеше сөздерден қарама-қарсы көзқарасты көрсететін дәлелдер келтіруге тырысыңыз.

1. Интернеттің қашықтықтан білім берудің шексіз мүмкіндіктері бар. Бұл өте қолайлы!

2. Интернет – бұл жаһандық жарнама ресурсы. Бұл өте жақсы!

3. Интернеттегі байланыс жаман, өйткені ол көбінесе нақты қарым-қатынасты виртуалды түрде алмастырады.

4. Интернет – дүкендер жаман, өйткені бұл интернеттегі алаяқтықтың ең танымал түрі.

5. Интернетте сіз адам туралы ақпаратты біле аласыз (тұрғылықты жері және электрондық пошта мекенжайы, ұялы телефон нөмірі). Және бұл да өте жақсы!

Педагог білім алушыларға «бізді қандай қауіптер күтіп тұр?»,

«Виртуалды шындық дегеніміз не?». (Бірнеше білім алушыларға алдын-ала «Интернетке тәуелділік» тақырыптары бойынша қысқа хабарламалар дайындаған жөн,

«Зиянды және қалаусыз бағдарламалар», «интернет арқылы адамға психологиялық әсер ету», «Қалаусыз мазмұндағы материалдар», «интернет-алаяқтар»).

«Қол алысу арқылы сәлемдесу» Сергіту сәті.

Қатысушыларға 10 секунд ішінде мүмкіндігінше көп адамдармен қол алысу ұсынылады.

Талқылау.

- қанша адам амандаса алды?

- біреуде психологиялық ыңғайсыздық болды ма? Егер-иә болса, оған не себеп болды? Жағдайды талдау.

Интернетте сөйлесу арқылы біз бейтаныс адамдарды жиі қосамыз. Әлеуметтік желілерде және олармен байланысыңыз. Біз олар туралы ештеңе білмейміз. Ал шынайы өмірде адам туралы қол алысу арқылы қанша ақпарат біле аламыз? Дегенмен, жақын жерде тыңдауға, қолдау көрсетуге, қиын уақытта көмектесуге дайын адамдар бар екенін білу өте маңызды. Ал желіде қалай? Педагог сабақтың басты сұрағына жауап беруді ұсынады – «желідегі жұмысты қалай қауіпсіз етуге болады?»

3. Практикалық жұмыс.

Сіз не істей аласыз? Не болмайды? Неге мұқият қарау керек? Білім алушыларға ресурстарды қарау ұсынылады [24-26]

Педагог бұл туралы web- парақтардан не оқуға болатынын және білім алушылардан қауіпсіз жұмыс ережелерін тұжырымдауды сұрайды.

4. Зерттелген материалды бекіту.

Интернет – бұл адамдардың өзара әрекеттесуінің жаңа ортасы. Онда адамдарға ежелден белгілі көптеген ережелер мен заңдылықтар жаңа дыбысқа ие болады. Мен белгілі суреттерді қолдана отырып, кейбір қарапайым ұсыныстарды тұжырымдауға тырысамын.

Заманауи интернет – бұл кең ғана емес, сонымен қатар теңшелетін тіршілік ету ортасы! Бұл өз кеңістігін ұйымдастыра алатын және оны басқаруды үйренетін адамға жақсы. Өз әсеріңізді блогқа жазыңыз, фотосуреттер мен бейнелердің галереяларын жасаңыз,

Достарыңызға сенетін адамдарды қосыңыз. Содан кейін желіде мағынасыз жүрудің орнына сіздің интернет байланысыңыз пайдалы болады.

Рефлексия.

Педагог білім алушыларға сабақта өз жұмыстарын талдауды ұсынады.

Есіңізде болсын, интернет оқу, демалу немесе достарыңызбен сөйлесу үшін тамаша және пайдалы құрал бола алады. Бірақ – нақты әлем сияқты желі де қауіпті болуы мүмкін!

Сабақты қорытындылай келе, педагог білім алушылардың белсенділігін бағалайды.

Үй тапсырмасы туралы ақпарат, оны орындау туралы нұсқаулық:

1. «Ақпараттық қауіпсіздік» ұғымына анықтама беріңіз.

2. «Менің қауіпсіз желім» ақпараттық парағын жасаңыз.

9 СЫНЫПТАРҒА АРНАЛҒАН «ҚАУІПСІЗ ИНТЕРНЕТ» ТАҚЫРЫБЫНДА САБАҚ ЖОСПАРЫНЫҢ ҮЛГІСІ

Мақсаты: Интернет желісінде қауіпсіз жұмыс істеу ережелерімен танысу.

Міндеттері:

- интернет желісіндегі қауіпсіз жұмыс туралы білім алушылардың хабардар болуын зерделеу;
- интернетте қауіпсіз жұмыс істеу ережелерін тұжырымдау;
- ақпараттық кеңістікте шарлауды үйрету;
- онлайн-технологияларды жауапкершілікпен пайдалануға ықпал ету;
- білім алушылардың ақпараттық мәдениетін қалыптастыру;
- сыни ойлауды дамыту;

Білім алушылар білуі керек:

- Интернет желісінің ақпараттық қызметтерінің тізбесі;
- Ғаламдық компьютерлік желінің қауіптілігі.

Білім алушылар дағдысының болуы:

- Веб-шолғышпен жұмыс істеу;
- Ақпараттық ресурстарды пайдалану;
- Интернет желісіндегі ақпаратты іздеу
- Онлайн-технологияларды пайдалануға жауапкершілікпен қарау.

Сабақ түрі: жаңа материалды үйрену сабағы

Оқыту әдістері мен формалары: ауызша (пікірталас, әңгіме), бейне әдіс, көрнекі (демонстрация), практикалық; ішінара іздеу, проблемалық, қызығушылықты ынталандыру әдісі; оқытудың интерактивті түрі (пікір алмасу, ақпарат).

Бағдарламалық-дидактикалық қамтамасыз ету: презентация «Қауіпсіз Интернет», «Интернет желісіндегі оқушылардың қауіпсіздігі» бейне-ролик, тест, ақпараттық плакаттар, web-ресурстардың мекен-жайлары бар карточкалар.

1. Интернетті және ұялы байланысты пайдалы және қауіпсіз пайдалану бойынша онлайн-конкурс[27]
2. «Цифорлық әлем әліпбиі»[28]
3. «Қауіпсіз интернет лигасы»[29]
4. «Интернеттегі балалар мен жастардың қауіпсіздік негіздері» - интерактивті қауіпсіздік курсы[30]

Сабақ кезеңдері:

1. Сабақты ұйымдастыру.
2. Сабақтың мақсатын қою (3 мин).
3. Сабақтың тақырыбы мен негізгі сұрағын қою.
3. Жаңа материалды зерттеу (26 мин). Бейнені қарау. (16 минут).

4. Сергіту сәті.
5. Топтық пікірталас.
6. Практикалық жұмыс (7 мин). Құпия сөз жасау. Зерттелген материалды бекіту (7 мин).
7. Тестілеу.
8. Сабақты қорытындылау (2 мин). Оқушылардың жұмысын бағалау. Үй тапсырмасы туралы ақпарат.

Сабақ барысы

1. Сабақты ұйымдастыру.
2. Сабақтың мақсатын қою (3 мин).

Ғаламдық желінің дамуы біздің әдеттегі өмір салтымызды өзгертті, біліміміз бен тәжірибеміздің аясын кеңейтті. Енді сіз бүкіл әлем бойынша миллиондаған компьютерлерде сақталған кез-келген ақпаратқа қол жеткізе аласыз.

- Қалай интернет желісінің құрбаны болмауға болады? Біздің сабағымыздың тақырыбы – *«Қауіпсіз Интернет»*.

Сабақтың басты сұрағы: Желідегі жұмысты қалай қауіпсіз етуге болады?

2. Жаңа материалды зерттеу (20 мин).

Бүгінгі таңда интернетті аз адамдар пайдаланбайды. Күн сайын ғаламдық желіде жұмыс істеуге арналған құралдардың саны мен әртүрлілігі артып келеді: браузерлер, қосымшалар, электрондық пошта клиенттері, түрлі бағдарламалар. Дәл қазір хабарламаны басқа континентке жіберуге, әлеуметтік желіге кіруге, жазушының өмірбаянынан қызықты фактіні табуға мүмкіндік бар. «Интернет» әрқашан пайдалы және жақсы нәрсені білдіре ме?

Тапсырма: Білім алушыларды екі топқа бөлу: бірінші топ – парақтарға келесі бейнеде айтылатын қауіптерді жазу;

Екінші топ ұсынылған параққа желіде қауіпсіз жұмыс істеу ережелерін жазу.

«Қауіпті интернет»	«Қауіпсіз интернет»

Бейне-роликті қарау. Әр топ өзіне берілген тапсырмаларды отындау.

- Сабақтың басты сұрағына жауап берейік – «Желідегі жұмысты қалай қауіпсіз етуге болады?»

«Қауіпті интернет» парақтарын талқылау, «Қауіпсіз интернет» ережелерін тұжырымдау (4 мин).

Сіз қауіптер тізіміне тағы бір нәрсе қосар ма едіңіз? Бұл қауіптерден қалай аулақ болуға болады?

Тағы басқа білетін қауіпті мәселелерді қосуыңызға болады, мысалы: спам, вирустардың таралуы, кибербуллинг, интернетке тәуелділік.

3. Практикалық жұмыс (7 мин).

Электрондық поштадан құпия сөзді жоғалтқан кезде адамдарда көптеген мәселелер туындайды.

Құпия сөз не үшін қажет? Құпия сөзді қалай сенімді етуге болады?

Жұптық жұмыс: компьютерде практикалық жұмыс.

«Цифрлық әлем алфавиті». (<http://www.edu.yar.ru/azbuka/password.php#game>)

«Неге үшін пароль керек» комиксін. Талқылау.

Әлемдегі ең танымал үш пароль келесідей көрінеді: «құпия сөз», «password», «monkey» и және «123456»

Құпия сөзді таңдаудың қарапайым ережелері: ұзындығы кемінде 8 таңба, екі регистрдің әріптерін пайдалану, әріптер мен сандарды, сондай-ақ арнайы таңбаларды пайдалану.

Неліктен пароль ретінде сөздік сөзді таңдаған жөн емес? (Өйткені сөздік сөздерді киберқылмыскерлер тезірек табады)

Слайд 5. Парольдерді қалыптастыру мысалдарын қараңыз.

4. Зерттелген материалды бекіту (7 мин).

Тестілеу (7 мин). Бүгінгі сабақ тақырыбы бойынша білім алушылармен шағын тестілеу өткізу.

5. Сабақты қорытындылау (2 мин.).

Қауіпсіз интернет тақырыбына бей-жай қарамағаныңызға қуаныштымын. Белсенді қатысқаныңыз үшін рахмет (топтың жұмысын бағалау).

Үй тапсырмасы туралы ақпарат, оны орындау туралы нұсқаулық.

1. «Менің қауіпсіз желім» ақпараттық парағын жасаңыз

2. «Интернетте қауіпсіз жұмыс істеу ережелері» жадынамасын жасаңыз.

«Қауіпсіз интернет» білім алушылармен тест жұмысы

1. Интернет желісінде ашық қолжетімділікте қандай жеке ақпаратты жарияламау керек?

a) үй телефонының нөмірі

b) ұялы телефон нөмірі

c) сіздің e-mail

d) сүйікті кітаптардың, әндердің атаулары

e) өз мектебіңіздің, сыныбыңыздың нөмірі

f) сіздің фотосуреттеріңіз

g) лақап атыңыз

h) үй жануарының лақап аты

2. Компьютерге желілік шабуылдың салдары болуы мүмкін:

a) бағдарламалардың жұмыс істемеуі

b) компьютердің бұзылуы

c) ақпаратты ұрлау немесе жою

d) компьютерді зиянды бағдарламалармен жұқтыру

3. Жалған сайт-бұл...

a) ақылы бағдарламалық жасақтама үшін жалған, қарақшылық кілттерді тарататын сайт

b) басқа сайттың көрінісі ретінде жасырылған сайт

c) спам тарату үшін құрылған сайт

d) мұнда дұрыс жауап жоқ

4. Сіз достарыңыздан сізге белгісіз мазмұнның күтпеген файлдарын алдыңыз. Сіздің әрекеттеріңіз:

a) файлды ашып, мазмұнымен танысамын

b) файлды компьютерге сақтап, содан кейін антивирустық бағдарламамен тексеремін және вирустар болмаған жағдайда файлды ашамын

c) күдікті файлды ашпай-ақ жойып, өшіремін

5. Сіздің кіріс жәшігіңізге оны бес досыңызға жіберу керек деген хат келді. Қандай әрекет жасау керек?

a) оны бес досыңызға жібересіз

b) оны бес емес, он досыңа жібересіз

c) мұндай хаттарды ешкімге де жібермейсіз

d) жіберушіге бұдан былай мұндай хаттарды алғыңыз келмейтін айтып жауап бересіз.

6. Кибербуллинг дегеніміз не?

a) Интернет желісінде жасалатын алаяқтықтар

b) әңгімеге қатысушылар арасында жанжал тудыру мақсатында Интернет желісінде арандатушылық хабарламаларды орналастыру

c) басқаны қорқыту, қорлау немесе басқаша қысым көрсету мақсатында орналастырылған желідегі кез келген хабарламалар немесе жарияланымдар

7. Құпия сөздерді қалай сақтау керек (мысалы, электрондық поштадан немесе әлеуметтік желідегі профильден)?

a) дәптерге жазу

b) компьютерде жасырын файлда сақтау

c) құпия сөз менеджерін пайдалану

d) есте сақтау

e) мониторға түрлі-түсті пароль жапсырмаларын жабыстыру

8. Шабуылдаушылар желінің сенімді пайдаланушыларынан жеке ақпаратты алу арқылы алдайтын алаяқтық деп аталады:

a) крекинг

b) серфинг

c) фишинг

d) биллинг

9. Вирус сіздің компьютеріңізге қалай енетінін көрсетіңіз (бір немесе бірнеше опцияны таңдаңыз):

a) электрондық пошта арқылы

b) интернеттен вирус жұққан файлдарды жүктеу кезінде

c) флэш-дискілер арқылы

d) вирус жұққан веб-сайтты жүктеу кезінде

Тест кілті: A,b,c,e,f; 2 – a,c,d; 3 – b; 4 – b,c; 5 – c; 6 – c; 7 – d; 8 – c; 9 – a,b,c,d, әр белгіленген үшін дұрыс әріп 1 ұпай. Ең көбі 19 ұпай.

Қате белгіленген әріп үшін минус – 0.5 балл.

«5» - 18-19 балл

«4» - 14-17.5 балл

«3» - 10-13.5 балл.

«ИНТЕРНЕТТЕГІ ҚАУІПСІЗДІК» САБАҒЫНЫҢ ҮЛГІЛІК ЖОСПАРЫ (9-11 СЫНЫПТАР ҮШІН)

Сабақтың мақсаты: білім алушылардың заманауи ақпараттық-телекоммуникациялық ортада қауіпсіз және жауапты мінез-құлық дағдыларын қалыптастыруға ықпал ету.

Міндеттері:

- білім алушылардың интернетте қауіпсіз жұмыс істеу ережелерін қалыптастыру;

- қазіргі ақпараттық кеңістіктегі салауаттылыққа үйрету;

- интернеттегі жұмыс туралы құқықтық білімнің негізін қалау;

- білім алушылардың ақпараттық мәдениетін қалыптастыру;

- web-ресурстарды пайдалана отырып, қажетті ақпаратты өз бетінше табу қабілетін дамыту;

- сыни ойлауды дамыту;

- желіде жұмыс істеу кезінде білім алушылардың жауапкершілігі мен тәртіптілігін тәрбиелеу.

Құрал-жабдық: компьютерлік сынып, ДК, мультимедиялық проектор.

Сабақ барысы

I. Ұйымдастыру

II. Зейінді белсендіру

Бүгін бізде өте маңызды тақырып, айтылатын мәселелер әрқайсыңызға қатысты. Суреттерге қарап, сабағымыздың тақырыбын анықтауға тырысу.

Интернет біздің өмірімізге енді. Интернет біздің көмекшіміз – бізге жұмыс істеуге, саяхаттауға, демалуға, достарымызбен сөйлесуге көмектеседі. Интернет біздің мұғалім – жаңа білім алуға, уақтылы ақпарат алуға көмектеседі.

Бірақ Интернетке саяхат тәжірибесіз адамның орманға баруы сияқты. Орманда сіз адасып, батпаққа түсіп, улы саңырауқұлақтар немесе жидектер жинап, жабайы аңдардың айбатына ұшырап кетуіңіз әбден мүмкін. Бірақ, егер адам орманды білсе, онда кім тұратынын білсе, онда өсетін өсімдіктерді білсе, онда орманға бару пайда мен рахатқа бөлейді.

Интернетте көптеген пайдалы, қажетті және қызықты нәрселер бар, бірақ әр веб-бетте сізді әмияныңызға, физикалық немесе психикалық денсаулығыңызға, тіпті өміріңізге қауіпті ақпарат күтуі мүмкін.

Біздің сабағымыздың міндеті – осы қауіптерді бағалау және әр жағдайда мінез-құлық стратегиясын жасау.

III. Жаңа ақпараттар



1 топ – «Вирустар»

1. Біздің компьютерде вирустар не істейді? (вирустардың түрлері, таралу жолдары, деструктивті әрекеттер);

2. Антивирустық бағдарламалар (мақсаты, мүмкіндіктері, қауіпсіздік кеңестері).

2 топ – «Интернеттегі алаяқтар»

1. Қос веб-сайттар;

2. Интернет-бопсалау;

3. Қауіпсіздікті тексерудегі «алаяқтық»

4. Инвестициялық жобалар және қаржы пирамидалары

- «Интернеттегі қауіпсіздік және ойын-сауық» бейнеролигі көрсетіледі

3 топ – «Интернеттегі ақпарат»

1. Қауіпсіз байланыс дегеніміз не?

2. Интернетке тәуелділік

3. Қандай сайттарға ешқашан кіруге болмайды

- «Интернеттегі қауіпсіздік» бейнеролигі көрсетіледі

4 топ – «Интернеттегі этика және құқық»

1. Интернеттің этикалық нормалары

2. Зиянды бағдарламалар

3. Зияткерлік меншікті қорғау

- «Мен және Интернет» бейнеролигін қарау

IV. Материалды бекіту

Компьютерде тест тапсыру арқылы бүгінгі сабақты қаншалықты жақсы меңгергендерін тексеру. (Білім алушылардың ДК-дегі жеке жұмысы)

V. Кері байланыс. Сабақты қорытындылау

VI. Үй тапсырмасы

1. Интернеттегі қауіпсіз мінез құлықтың негізгі ережелерін жазу;

2. Интернеттегі сақтық туралы бастауыш сынып білім алушыларына арнап ертегі ойлап табу.

VII. Рефлексия

«ҚАУІПСІЗ ИНТЕРНЕТ» ТАҚЫРЫБЫ БОЙЫНША САБАҚТЫҢ ЖОСПАРЫ (9–11 СЫНЫП)

Мақсаты: кәмелеттік жасқа толмаған білім алушылар мен тәрбиеленушілерге ақпараттық және телекоммуникациялық ортада жауапкершілік пен қауіпсіз мінез –құлық дағдыларын қалыптастыру арқылы ақпараттық қауіпсіздікті қамтамасыз ету.

Міндеттері:

- Пайдаланушылардың интернеттегі қауіпсіз жұмыс туралы хабардарлығын зерттеу;
- интернетте қауіпсіз жұмыс жасау ережелерімен танысу;
- ақпараттық кеңістікті бағдарлау; online-технологияларды жауапкершілікпен қолдануға көмектесу;
- білім алушылардың ақпараттық мәдениетін қалыптастыру, web–ресурстарды пайдалана отырып, қажетті ақпаратты өз бетінше таба білу;
- желіде жұмыс істеу кезінде тәртіптілікке тәрбиелеу.

Білім алушылар білуге тиіс:

- Интернет желісіндегі ақпараттық қызметтердің тізімін;
- Интернетте қауіпсіз жұмыс жасау ережелерін;
- Жаһандық компьютерлік желінің қауіптілігі.

Оқушылар білуі керек:

- Онлайн-технологияларды қолдануға жауапкершілікпен қарау;
- Веб-браузермен жұмыс жасау;
- Ақпараттық ресурстарды пайдалану;
- Интернеттен ақпаратты іздеу.

Сабақтың түрі: жаңа материалды меңгеру сабағы.

Оқытудың әдістері мен формалары: ауызша (пікірталас, әңгіме), бейне әдіс, көрнекі (демонстрациялық), практикалық; ішінара ізденіс, проблемалық, қызығушылықты ынталандыру әдісі; оқытудың интерактивті түрі (пікір алмасу, ақпарат алмасу).

Web-ресурстарға
сілтемелер:

- 1) антивирус «Касперский лабораториясы»[31];
- 2) қауіпсіз web–зона[32];
- 3) Интернетті қауіпсіз пайдалануға арналған халықаралық онлайн–конкурс[33];
- 4) Интернет БАҚ «Сіздің жеке интернетіңіз»[34].

Сабақ кезеңі:

1. Сабақтың басталуын ұйымдастыру. Сабақтың мақсатын қою. Бейнеролик қарау
http://video.mail.ru/mail/illari.sochi/_myvideo/1.html. Тақырыпты бекіту және сабақтың негізгі сұрағы.
2. Жаңа материалды меңгеру. Топтық талқылау. Мәселені теориялық

қамту (білім алушыларға хабарлама).

3. Практикалық жұмыс. Ақпаратты интернеттен іздеу.

Табылған материалды талқылау.

4. Оқыған материалды бекіту. Қауіпсіз жұмыс Ережелері бойынша ұсыныстар. Тестілеу.

5. Сабақты қорытындылау. Топтың жұмысын бағалау. Үй жұмысы. Сабақ барысы

1. Сабақтың басталуын ұйымдастыру. Сабақтың мақсатын қою. Жаһандық желінің дамуы біздің әдеттегі өмір салтымызды өзгертті,

біліміміз бен тәжірибеміздің шекарасын кеңейтті. Енді бүкіл әлем бойынша миллиондаған компьютерлерде сақталған кез келген ақпаратқа қол жеткізуге болады. Бірақ екінші жағынан, миллиондаған компьютерлерге сіздің компьютеріңіз қолжетімді болып отыр. Олар бұл мүмкіндікті пайдаланатынына күмәніңіз болмасын. Дәл қазір бастайды.

(«Балалар мен интернет» бейнеролигін қарау – 1 мин. (таңдау бойынша). (<http://www.youtube.com>); YouTube <http://www.youtube.com> сайтында қалай қауіпсіз болу керек. Интернеттегі ойын-сауық және қауіпсіздік <http://www.youtube.com/>. Интернеттегі алаяқтықтан сақ болыңыз <http://www.youtube.com/>. Әлемге Gmail көзімен – Спамнан қорғану).

Қалай Интернеттің құрбаны болмау керек? Біздің сабақтың тақырыбы – «Қауіпсіз Интернет». Сабақтың негізгі сұрағы:

1. Желіні қалай қауіпсіз етуге болады?

2. Жаңа материалды меңгеру. «Қолдаймын немесе қарсымын» ойыны. Мұғалім «Қолдаймын немесе қарсымын» ойынын ұсынады. Слайдта бірнеше мәлімдемелер бар. Қарама–қарсы көзқарасты көрсететін дәлелдер келтіруге тырысыңыз.

1. Интернетте қашықтықтан білім алудың шексіз мүмкіндіктері бар. Бұл да жақсы!

2. Интернет – жаһандық жарнама ресурсы. Бұл да жақсы!

3. Интернет желісіндегі байланыс – бұл жаман, себебі ол шынайы виртуалды байланыстың орнын жиі алмастырады.

4. Интернет – күшті антидепрессант болып табылады.

5. Интернетте адам туралы ақпаратты білуге болады (тұрғылықты жері мен электронды поштасы, ұялы телефон нөмірі). Бұл да жақсы!

Виртуалды кедергілер

Мұғалім оқушыларды «Бізді қандай қауіп күтіп тұр?», «Біздің жолымызда қандай виртуалды кедергі бар?» секілді сұрақтарға жауап беруге шақырады. («Интернет–тәуелділік», «Зиянды және қажетсіз бағдарламалар», «Интернет арқылы адамға психологиялық әсер ету», «Қажет емес мазмұндағы материалдар», «Интернет–алаяқтар» тақырыптары бойынша бірнеше білім алушы алдын ала қысқа хабарламалар дайындағаны жөн).

«Қол алысу» сергіту сәті.

Қатысушылар 10 секунд ішінде неғұрлым көбірек адамдармен қол алысып үлгеру керек.

Талқылау.

Кім қанша адаммен амандасып үлгерді? Кімде психологиялық ыңғайсыздық туындады? Егер болса, ол қандай нәрсемен байланысты?

Жағдайды талдау.

Ғаламторда сөйлескен кезде біз әлеуметтік желілерімізге бейтаныс адамдарды қосып, олармен жиі араласамыз. Біз олар туралы ештеңе білмейміз, тек олардың атын ғана білеміз. Біз атынан немесе қол алысудан адам туралы қаншалықты көп ақпаратты біле аламыз? Дегенмен, жанымызда тыңдауға, қолдау көрсетуге, қиын уақытта көмектесуге дайын адамдар бар екенін білу өте маңызды.

Мұғалім сабақтың – «Желіде жұмыс істеуді қалай қауіпсіз ету керек?» деген негізгі сұрағына жауап беруді ұсынады.

2 Практикалық жұмыстар.

Не нәрсе рұқсат? Нені жасауға болмайды? Не нәрсеге сақтықпен қарау керек?

Білім алушыларға ресурстарды қарау ұсынылады [35,36,37].

Мұғалім бұл туралы web-парақшаларда не оқуға болатынын сұрайды және оқушылардан қауіпсіз жұмыс ережелерін құрастыруды сұрайды.

Түйіндеме (табылған ақпаратты талқылау). Оқушылар веб-сайттарға кіру кезінде қандай қауіпсіздік ережелерін таңдады?

4. Материалды бекіту.

Интернет – адамдардың өзара қарым–қатынасының жаңа ортасы. Онда бұрыннан адамдарға белгілі көптеген ережелер мен үлгілер жаңа сипатқа ие болады.

Өзімізге белгілі сипаттарды пайдалана отырып, бірнеше қарапайым нұсқауларды тұжырымдаймыз.

Заманауи интернет – бұл кең ауқымды ғана емес, сонымен қатар құрылымданатын орта! Бұл ол жерде өз кеңістігін реттей алатын және оны басқаруды үйренетіндер үшін жақсы. Блогқа өз әсерлеріңізді жазыңыз, фотосуреттеріңіз бен бейнелеріңіздің галереяларын жасаңыз және сенетін адамдарды достар ретінде қосыңыз. Содан кейін, интернетті мәнсіз шарлай берудің орнына, сіздің интернет байланысыңыз пайда әкеледі.

Рефлексия. Бұл кезеңде интернет қауіпсіздігі сабағын түгендеу ұсынылады: үстелде үш смайлик жатыр, білім алушылар оқушының көңіл–күйіне сәйкес келетінін таңдап, олардың алдына қою керек.

Есіңізде болсын, интернет оқу, демалу немесе достармен сөйлесу үшін тамаша және пайдалы орта болуы мүмкін. Бірақ – нақты әлем сияқты – интернет те қауіпті болуы мүмкін!

Білім алушыларды бағалау.

Үй тапсырмасы туралы ақпарат, оны орындау туралы нұсқаулар:

1. «Ақпараттық қауіпсіздік» түсінігіне анықтама беріңіз.

2. «Менің қауіпсіз желім» ақпарат парағын жасаңыз.

«ИНТЕРНЕТТІ ҚАУІПСІЗ ПАЙДАЛАНУ» СЫНЫП САҒАТЫ

Интернет – ертегі елі екені белгілі. Әрине әлі де қажетті білім мен тәжірибеге ие болмай тұрып зиянды бағдарламалардың тұзағына түсу немесе орынсыз байланысқа түсу оңай. Ересектер өздері үшін тұра алады, бірақ балаларға Интернеттің қауіптілігі оларға зиянды әсер етуі мүмкін.

Бірақ балаларға желіні пайдалануға тыйым салудың мағынасы бар ма?
Жоқ! Балаларға желіні пайдалануға тыйым салу – бұл шешім емес. Бұндай тыйым баланы қорғауға көмектеспейді. Балалардың желіде кездесетін барлық тәуекелдері бұрыннан белгілі және зерттелген олар кейбір қарапайым ережелерді сақтау проблемаларды болдырмауға көмектеседі.

Мақсаты:

- заманауи ақпараттық-коммуникациялық ортада жауапкершілікті және қауіпсіз мінез-құлық дағдыларын қалыптастыру арқылы білім алушылардың ақпараттық қауіпсіздігін қамтамасыз ету. Оларды интернеттегі жеке және ақпараттық қауіпсіздікке үйрету; білім алушылардың өзін-өзі бақылауын дамыту және ақпараттық ресурстарға мұқият қарауға тәрбиелеу; жеке және ақпараттық қауіпсіздікті қамтамасыз ету мақсатында ақпараттық қоғамда мінез-құлық дағдыларын қалыптастыру.

Міндеттері:

- Интернет желісінде таратылатын ақпараттық өнімдерге сыни көзбен қарау;
- сенімді мәліметтерді дұрыс емес, зиянды, қауіпсіз ақпараттан ажырату;
- білім алушылардың денсаулығына, адамгершілік және психикалық дамуына, ар-намысына, қадір-қасиетіне және беделіне зиян келтіретін ақпаратты таңудан аулақ болу;
- білім алушылардың тәжірибесіздігі мен сенімсіздігін теріс пайдалану белгілерін, оларды заңсыз әрекеттерге тарту әрекеттерін тану;
- Интернет желісіндегі балалардың мінез-құлық нормалары мен ережелері;
- Интернетте қауіпсіз жұмысты ұйымдастыру;
- интернетте қауіпсіз жұмыс істеу қаупін анықтау.

Сынып сағатының барысы:

Бір-біріңізге бұрылыңыз, бір-біріңіздің көздеріңізге қараңыз, бір-біріңізге күліңіз, сабақта бір-біріңізге жақсы жұмыс көңіл-күйін тілеңіз. Енді маған қара. Сізге де бірге жұмыс істеуді, жаңа нәрсе ашуды тілеймін.

Тақырыптың анықтамасы

- Балалар, осы суретке қарап, бүгін мен сізбен не туралы сөйлескім келеді деп ойлайсыз?
- Иә, ұрыс, бірақ тек интернет туралы емес, қауіпсіз интернет туралы.

- Балалар, қауіпсіздік дегеніміз не?
- Қауіпсіздік туралы қашан айтамыз?
- Сіз бәріңіз компьютермен таныссыз және әрқайсыңыз да Интернетке «кірдіңіз».
- Ал Интернет дегеніміз не?

Қазіргі уақытта адамдар интернетте көп уақыт өткізеді. Біреу ақпарат іздеумен айналысады, біреу әлеуметтік желілерде достарымен немесе әріптестерімен байланысады. Интернеттің көптеген мүмкіндіктерге ие екендігі даусыз. Бірақ сонымен бірге ғаламдық желіде көптеген ықтимал қауіптер бар.

Бүгін біз сіздермен интернеттің қаншалықты қауіпті екендігі және осы қауіптің деңгейін қалай төмендетуге болатындығы туралы сөйлесетін боламыз.

Интернет – бұл әр түрлі ақпараттың үлкен ағыны. Мұнда біз пайдалы, маңызды және мағыналы нәрсе таба аламыз.

Мысалы, сіз соңғы жаңалықтарды оқи аласыз, аптаның ауа-райы болжамын біле аласыз, қызықты жазушы туралы көптеген қызықты нәрселерді таба аласыз, қызықты фильмді, сүйікті музыканы жүктеп, көре аласыз, ерекше тағамның рецептін таба аласыз және т.б.

Сонымен қатар, пайдаланушының уақытын алатын мүлдем пайдасыз ресурстар мен порталдар бар. Біз оларды мақсатты түрде қарастырмаймыз, өйткені бұл әркімнің жеке ісі – өмірдің баға жетпес сағаттарын ысырап ету немесе жоғалту. Бірақ желідегі ақпараттың тағы бір категориясы бар, ол біздің сабақта талқыланады. Бұл адамдарға, әсіресе кішкентайларға зиян келтіретін материалдар.

Топтық жұмыс: «Сіз электронды хат алдыңыз».

«Қымбатты досым! Маған Сіздің пікірлеріңіз ұнайды. Сіз ақылды және мейірімді адам екеніңізді көре аласыз. Менің Сізге қызықты ұсынысым бар. Бүгін саябақта кешкі сағат 5-те кездесейік. Менің қолымда аю ойыншық болады. Кездесуге дейін! Кездесу туралы ешкімге айтпаңыз! Бұл біздің кішкентай құпиямыз».

Топтарда кеңес алыңыз және қалай ояну керектігін айтыңыз әрекет ету хатты оқу арқылы (топтарда талқылау, сөйлеу).

Рефлексия

- Сабақ қызықты болса, тақтаға күлімсіреген смайликті бекітіңіз.
- Сабақта кімге жайлы болды, түзу сызықты смайликті бекітіңіз.
- Сабақта қызықсыз болды, көңілсіз смайликті тіркеңіз.

Сізге өмірде де, Интернетте де бәрі керемет болғанын тілеймін!

Енді балалардың интернетті және ұялы байланысты қауіпсіз пайдалану ережелері туралы жадынаманы ұсынамын:

1. Әрқашан ата-анаңыздан интернеттегі бейтаныс нәрселер туралы сұраңыз. Олар сізге не қауіпсіз және нені қалай жасау керектігі туралы кеңес береді.

2. Интернетте біреумен дос болуды бастамас бұрын, ата-анаңызға хабарлаңыз, олармен қалай қауіпсіз сөйлесу керектігін сұраңыз.

3. Сайттарға тіркелу кезінде жеке ақпаратты көрсетпеуге тырысыңыз, себебі ол бейтаныс адамдарға қол жетімді болуы мүмкін. Сіз қай жерде тұрасыз, қай мектепте оқисыз, телефон нөмірін тек достарыңыз бен туыстарыңыз білуі керек.

4. Веб-камераны достарыңызбен сөйлескен кезде ғана пайдаланыңыз. Бейтаныс адамдар сіздің әңгімеңізді көре алмайтындығына көз жеткізіңіз, себебі ол жазылуы мүмкін.

5. Бейтаныс адамдардың қалаусыз хаттары «спам» деп аталады. Егер мұндай хат алған болсаңыз, оған жауап бермеңіз, оны ата-анаңызға көрсетіңіз. Егер сіз осындай хатқа жауап берсеңіз, жіберуші сіздің электрондық поштаңызды пайдаланып жатқаныңызды біледі және сізге «спам» жіберуді жалғастырады.

6. Егер сізге бейтаныс мекен-жайдан хабарлама келсе, оны ашпағаныңыз жөн. Мұндай хаттарда вирустар болуы мүмкін.

7. Егер сіз фото-бейнематериалдарды жарияласаңыз, оларды әркім көре алатынын білуіңіз керек.

«КИБЕРҚАУІПСІЗДІКТІҢ БІРЫҢҒАЙ САБАҒЫ» ШЕҢБЕРІНДЕ «ИНТЕРНЕТ ЖЕЛІСІНДЕГІ ҚАУІПСІЗДІК» ТАҚЫРЫБЫНДА АҚПАРАТТЫҚ ХАБАРЛАМА

Хабарламаның мақсаты – ақпараттық қауіпсіздік саласындағы білім алушылардың хабардар болу деңгейін арттыру, қазіргі ақпараттық-телекоммуникациялық ортадағы жауапты және қауіпсіз мінез-құлық ережелерімен танысу.

I. Интернеттегі қауіпсіздік

1. Интернеттегі жалпы қауіпсіздік

Интернет біздің өміріміздің ажырамас бөлігіне айналды. Оның көмегімен біз ақпарат аламыз, байланыс жасаймыз, деректермен алмасамыз, тауарлар мен қызметтерге ақы төлейміз, жоғары оқу орындарына түсу үшін құжаттарды жібереміз және тағы басқалар жасаймыз. Сонымен қатар, интернет қауіп-қатерге толы, сондықтан олардан аулақ болу үшін олар туралы не білуіміз керек.

Интернетте қандай қауіптер күтуге болады?

Ең алдымен, бұл қаржылық немесе басқа да пайда көргісі келетін алаяқтардың әрекеттері. Алаяқтар әртүрлі құралдар мен әдістерді қолдана алады. Мысалы, вирустық бағдарламалық жасақтама (немесе «вирустар»), жалған сайттар, алаяқтық хаттар, әлеуметтік желілердегі және электрондық пошта қызметтеріндегі есептік жазбаларға парольдерді ұстау және сәйкестендіру.

Вирустар

Вирустар кірістірілген файлдар, электрондық пошталардағы немесе әлеуметтік желілердегі сілтемелер, алынбалы медиа, вирус жұқтырған сайттар арқылы таралуы мүмкін. Вирус туралы хабарламаны бөтен адам да, таныс адам да жібере алады, ол әлеуметтік желінің немесе пошта хат алмасуының жұқтырған вирусы.

Алаяқтық мақсатында арнайы құрылған сайттар немесе қарапайым ресурстар жұқтырылуы мүмкін, бірақ бұл жерде ақпараттық қауіпсіздіктің осалдығы бар.

Ұсыныстар:

- Жаңартылған вирустық қолтаңба базалары бар антивирустық бағдарламалық жасақтаманы қолданыңыз.
- Файлда немесе сілтемеде вирус жоқ екеніне көз жеткізбей, әлеуметтік желі немесе басқа байланыс құралдары арқылы электрондық пошта арқылы алынған кірістірілген файлдарды немесе сілтемелерді ашпаңыз.
- Сайттың домендік атауын мұқият тексеріңіз (мысалы, www.yandex.ru), өйткені шабуылдаушылар жәбірленушіні адастыру үшін жиі ұқсас сайт атауларын пайдаланады (мысалы, www.yadndex.ru).
- Сайт компьютердің қауіпсіздігіне қауіп төндіруі мүмкін екендігі

туралы браузердің немесе іздеу жүйесінің ескертулеріне назар аударыңыз.

- Компьютерге тексерілмеген алынбалы медианы қоспаңыз.
- Компьютерді құлыптан босату үшін ақша аудару немесе SMS жіберу сияқты шабуылдаушылардың арандатуына қарсы тұрыңыз.

Алаяқтық хаттар

Алаяқар ақшаны азғыру үшін әлеуметтік инженерияның әртүрлі әдістерін (қорқыту, бопсалау, жәбірленушінің сезімін ойнау – ашкөздік немесе эмпатия сияқты) қолдана алады. Мұндай жағдайларда олар белгілі бір сценарий бойынша хаттар жазады.

Ұсыныстар:

- Хатты мұқият қарап шығыңыз. Сипатталған фактілердің дұрыстығын тексеріңіз. Егер хатта кішігірім сыйақы үшін үлкен пайда ұсынылса, бұл алаяқтық болуы мүмкін.
- Мұндай хаттарды елеменіз.

Әлеуметтік желілердегі және басқа қызметтердегі аккаунттарға қол жеткізу

Алаяқар көбінесе жәбірленушінің аккаунттарына, мысалы, әлеуметтік желілерде, пошта және басқа қызметтерде қол жеткізуге тырысады. Олар ұрланған есептік жазбаларды спам мен вирустарды тарату үшін пайдаланады.

Алаяқтар жәбірленушінің есептік жазбасына келесі жолдармен қол жеткізе алады:

- Жәбірленушіні өз деректерін жалған сайтқа енгізуге мәжбүрлеу.
- Жәбірленушінің құпия сөзін алыңыз, егер ол күрделі болмаса.
- Жәбірленушінің құпия сөзін «құпия сұрақ» арқылы немесе электрондық поштаны тіркеу кезінде қалпына келтіріңіз.
- Қорғалмаған байланыс арналары арқылы беру кезінде жәбірленушінің құпия сөзін ұстаңыз.

Әдетте, жеке басын ұрлау үшін фишингтік сайттар қолданылады. Фишинг (ағылш. балық аулау-балық аулау, аулау)-пайдаланушылардың құпия деректеріне — логиндер мен парольдерге қол жеткізуге бағытталған интернет-алаяқтықтың бір түрі. Зиянкестер белгілі ресурстардың интерфейсін көшіретін фишингтік сайттар жасайды, ал жәбірленушілер сайттардың жалған екенін түсінбестен оларға логиндер мен парольдерді енгізеді.

Ұсыныстар:

- Күрделі құпия сөздерді қолданыңыз (олар кем дегенде 10 таңбадан тұрады, бас және кіші әріптерді, сандарды және арнайы таңбаларды қамтиды, пайдаланушы аты мен ол туралы белгілі фактілерді қамтымайды).
- Құпия сөзіңізді ешкімге бермеңіз.
- Құпия сөзді қалпына келтіру үшін құпия сұрақты немесе электрондық поштаны емес, тіркелгіге байланысты ұялы нөмірді пайдаланыңыз.
- Тіркелгі деректерін — логиндер мен парольдерді — қорғалмаған

байланыс арналары арқылы жібермеңіз (әдетте ашық және жалпыға ортақ wi-Fi желілері қорғалмайды).

- Тіркелгі деректерін енгізетін сайттардың домендік атауларын мұқият тексеріңіз.

Тегін Wi-Fi желілерін пайдалану кезінде деректерді ұрлау

Біз қазір компьютер немесе смартфон арқылы көп сөйлесеміз және оны жиі қоғамдық орындарда жасаймыз — құпия сөзбен қорғалмаған Wi-Fi желісіне қосылу арқылы. Айналасындағылардың ешқайсысы экранға қарамаса, құпиялылық сезімі пайда болады. Шын мәнінде, деректерді ашық Wi-Fi нүктесі арқылы беру - бұл белгілі бір мағынада адам көп жиналатын жерде толық дауыспен сөйлесу.

Зиянкестер жалпы атаулары бар желілерді жасайды және оған қосылған пайдаланушылардың Интернетте не істейтінін көреді: әлеуметтік желілерде жеке хабарламаларды оқиды және жазады, парольдерді немесе банк карталарының деректерін енгізеді.

Ұсыныстар

- Мобильді интернетті пайдаланыңыз(EDGE, 3G, LTE).

- Қоғамдық Wi-Fi желісіне қосылған кезде маңызды есептік жазбалардың құпия сөздерін енгізбеңіз.

- Тек деректерді шифрлайтын сайттарға кіруге тырысыңыз (HTTPS – бұл әдетте браузерлерде жасыл құлыппен белгіленеді).

- Арнайы қорғаныс құралдарын пайдаланыңыз-арнайы қауіпсіз бетті қарау режимі бар браузерлер немесе антивирустық компаниялар әзірлейтін қорғаушы бағдарламалар.

2. Интернеттегі төлем қауіпсіздігі (жоғары сынып оқушылары үшін)

Интернеттегі алаяқтық операциялардың көпшілігі нақты өмірдегі себептердей адамның абайсыздық, ақпараттанбау, аңғалдық, немқұрайлылық сияқты қасиеттерінен сәтті болады.

2.1. Төлем алаяқтығының жалпы мысалдары төлем қызметтерінен түскен жалған қоңыраулар

Алаяқ қоңырау шалып, өзін банктің немесе төлем қызметінің қызметкері ретінде көрсете алады және кез-келген төлем деректерін, мысалы, телефонға келген парольді немесе кодты жазуды сұрай алады. Қоңыраудың мақсаты – картадан немесе әмияннан ақша ұрлауға болатын төлем деректерін тарту.

Ұсыныстар

- Есіңізде болсын, банктер мен төлем қызметтері ешқашан пошта арқылы да, телефон арқылы да пароль, пин-код немесе SMS-код туралы хабарлауды сұрамайды.

- Әмияныңыздан немесе банк картаңыздан құпия сөздерді, пин-кодтарды және SMS кодтарын ешкімге бермеңіз.

Бейтаныс адамның SMS паролін алдауы

Пайдаланушыға төлем жасау үшін парольмен банктен немесе төлем қызметінен SMS келуі мүмкін. Осыдан кейін бірден осы ұялы телефон нөмірін қате енгізгенін айтқан адам қоңырау шалып, пайдаланушыға жаңа келген SMS-тен кодты хабарлауды сұрайды. Шын мәнінде, SMS коды – бұл бейтаныс адамның шотына емес, пайдаланушының шотына арналған пароль. Құпия сөздің көмегімен шабуылдаушы әмиянның немесе интернет-Банктің параметрлерін өзгерте алады, ақша ұрлайды және т.б.

Ұсыныстар

- Банктерден, төлем қызметтерінен, сондай-ақ ұялы байланыс операторларынан ұялы нөмірге келетін құпия сөздерді, пин-кодтарды және SMS кодтарын ешкімге бермеңіз

Төлем қызметтерінен жалған хаттар

Пайдаланушы төлем қызметі, өз банкі немесе басқа төлем қызметтері атынан жалған хат ала алады. Мысалы, оның шоты бұғатталған және құлыпты ашу үшін сілтемеге өтіп, деректеріңізді енгізу керек. Мұндай хаттардың жалғыз мақсаты-адамды жалған (фишингтік) сайтқа кіргізу және ұрланатын жеке мәліметтерін сол жерге енгізу. Болашақта бұл деректерді, мысалы, пайдаланушының шотына кіру үшін пайдалануға болады. Сонымен қатар, мұндай сайтта компьютерді вирус жұқтыруы мүмкін.

Ұсыныстар

- Төлем қызметтері мен банктер шотты бұғаттау туралы хабарламаларды ешқашан электрондық пошта арқылы жібермейтінін ұмытпаңыз;

- Мұндай электрондық пошталардың сілтемелеріне өтпеңіз және парольдеріңізді енгізбеңіз;

- Бөгде сайттарда, тіпті олар банктің сайтына өте ұқсас болса да, Яндекс. Ақша немесе басқа төлем қызметі.

- Кез-келген сайтта төлем деректерін енгізбес бұрын браузердегі сайттың мекен-жайы тексеріңіз.

Жалған лотерея ұтыстары

Пайдаланушы белгілі бір жүлдені жеңіп алғаны туралы хабарлама (телефон, пошта немесе SMS арқылы) ала алады, ал оны алу үшін «салық төлеу», «жеткізу ақысын төлеу» немесе жай ғана шотты толтыру қажет. Әрине, пайдаланушы уәде етілген сыйлықты алмайды.

Жалған лотерея белгілері

- Пайдаланушы бұл лотереяға ешқашан қатысқан емес және ол туралы ештеңе білмейді.

- Пайдаланушы ешқашан өзінің жеке деректерін ресурста немесе атынан хабарлама келетін ұйымда қалдырған емес.

- Хабарлама сауатсыз, емле қателері бар.

- Жіберушінің пошталық мекен-жайы-жалпыға қол жетімді пошта қызметі. Мысалы, gmail.com, mail.ru, yandex.ru.

Файлдарды тегін жүктеу

Көбінесе файлды тегін жүктеп алғысы келетін немесе бейнені жарнамасыз сапалы түрде көргісі келетін пайдаланушыларға сайтта мобильді нөмірді енгізу ұсынылады. Егер солай болса, ақылы SMS жазылымы қосылуы мүмкін және көрсетілген нөмірден ақша алынады.

Ұсыныстар

- Ұялы нөміріңізді бейтаныс сайттарда көрсетпеңіз.
- Егер жазылым әлдеқашан жасалған болса, ұялы байланыс операторының қолдау қызметіне қоңырау шалыңыз және оны өшіруді сұраңыз.

2.2. Ашылмайтын төлем деректері

...сіз картанызды жоғалттыңыз, сол кезде не істеу керек?

Банкке шұғыл қоңырау шалыңыз, оны бұғаттауды және қайта шығаруды сұраңыз. Сіз картаны бұғаттамайынша, оның қолында болған кез келген адам оны пайдалана алады — мысалы, интернет-дүкенде қымбат затты сатып алу үшін төлей алады.

...сіз жасамаған төлем туралы хабарлама келді.

Банкке операцияны тоқтату туралы өтініш беріңіз, онда не болғанын мүмкіндігінше егжей-тегжейлі сипаттаңыз. Банк Сіздің өтінішіңізді қарап, ақшаңызды қайтарады. Өтінішті кешіктірмеңіз: ол операция жасалған сәттен бастап 30-дан 60 күнге дейін өңделуі керек.

...сіз электрондық әмиянның құпия сөзін ұмытып қалдыңыз.

Төлем қызметінің веб-сайтына кіріп, «құпия сөзді қалпына келтіру» сілтемесін басыңыз – жүйе әмиян байланған ұялы нөмірді сұрайды. Телефон нөмірімен сіз парольді қалпына келтіру коды бар SMS аласыз.

2.3. Карталармен төлеу кезіндегі қауіпсіздік

Егер сіз келесі ұсыныстарды ұстанатын болсаңыз, банктік картаңыздың қауіпсіздігін қамтамасыз ету қиын емес:

- Карта нөмірін басқа адамдарға бермеңіз;
- Банк картасын қауіпсіз жерде сақтаңыз;
- Жазылған құпия сөздер мен кодтарды картаның жанында ұстамаңыз.
- Интернетте сауда үшін бөлек карта жасаңыз;
- Онлайн сатып алу (сатып алу әрекетін жасау) үшін тек жеке компьютерді пайдаланыңыз;
- Компьютердің антивирустық қорғанысын үнемі жаңартып отырыңыз;
- Танымал және сенімді интернет-дүкендерден сатып алуға тырысыңыз;
- Төлемді растамас бұрын браузердің мекенжай жолағында <https> протоколы бар екеніне көз жеткізіңіз. Тек осы протокол деректерді қауіпсіз тасымалдауды қамтамасыз етеді;
- Барлық төлемдер туралы ақпарат алу үшін банкте SMS хабарлама қызметін қосыңыз;

- Электрондық пошта бойынша алынған тауарларды төлеу және жеткізу құжаттарын сақтаңыз;

Интернет-банкте карталарыңыз бойынша орындалған операциялардың тарихын үнемі қарап отырыңыз;

- Интернеттен сатып алу кезінде қоғамдық Wi-Fi қолданбаңыз – банктік карта деректерін алаяқтар ұстап алуы мүмкін.

II. Ақпараттық саладағы балаларды қорғау туралы заңдар.

Қазақстан Республикасының 2018 жылғы 2 шілдедегі № 169 «Балаларды денсаулығы мен дамуына зардабын тигізетін ақпараттан қорғау туралы» Заңы;

Киберқауіпсіздік тұжырымдамасын бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы.

«ИНТЕРНЕТ ЖЕЛІСІНДЕГІ ҚАУІПСІЗДІК» ТАҚЫРЫБЫНДА СЫНЫПТАН ТЫС ІС-ШАРА ЖОСПАРЫ

Іс-шара формасы: Семинар

Мақсатты аудитория: Білім алушылар және педагогтер

Мақсаты: Интернет желісінің қауіптерін және олармен күресу әдістерін зерттеу

Міндеттері:

- «Интернет», «Вирус» ұғымдарымен танысу, Интернет желісінде жұмыс істеу кезінде қауіпсіздік әдістерін зерттеу;

- ақпараттық мәдениетке қызығушылықты дамыту; логикалық ойлау әдістерін қалыптастыру; талдау және жалпылау, қорытынды жасау қабілетін дамыту;

- дәлдікке, тәуелсіздікке тәрбиелеу, топтық жұмыс, ынтымақтастық дағдыларын қалыптастыру;

- компьютермен жұмыс кезінде санитарлық нормаларды сақтау, қауіпсіздік ережелерін сақтау, сабақта қолданылатын формалар мен әдістердің оңтайлы үйлесімі;

Білім алушыларды алдын-ала даярлау: информатика сабақтарында оқылған материалдарын қайталау;

Құрал-жабдық: ДК, проектор, интерактивті тақта (немесе экран), компьютер, дәптерлер, презентация, тест, бейне фрагмент.

Барысы:

1. Ұйымдастыру сәті:

Тақырыбын оның мақсаттары мен міндеттерін хабарлау; Іс-шараның қысқаша жоспарымен таныстыру.

2. Тақырыпқа кіріспе:

Бүгін іс-шара «Интернет желісіндегі қауіпсіздік» тақырыбына арналды.

Ескерту. Білім алушылар негізгі анықтамаларды дәптерге дәріс барысында дербес жазады.

Интернет – бұл компьютерлік желілер, ақпараттық-есептеу ресурстары арқылы ақпаратты берудің жаһандық әлемдік жүйесі.

Бүгінгі таңда кез-келген адам Интернет желісін пайдаланады. Интернеттің мүмкіндіктері шексіз: оқу, қажетті ақпаратты табу, ақша аудару, демалу және т.б. Алайда, көптеген пайдаланушылар бізді Дүниежүзілік желіде қандай қауіп күтіп тұрғанын ойламайды.

Компьютерде жұмыс істеген кезде қандай қауіптерге тап болғаныңызды ойластырып, еске түсірейік, мүмкін достарыңыздан қандай да бір қауіптер туралы естіген шығарсыз? (білім алушылармен сұрақ-жауап)

3. Жаңа материал түсіндіріледі:

Енді интернет желісіндегі статистикаға жүгінейік. Ең қауіпті тәкекелдердің рейтингі келесідей бөлінеді:

1. Зиянды бағдарламалар;

2. Ақпаратты ұрлау;
3. Қызметкерлердің немқұрайлылығы;
4. Хакерлік шабуылдар;
5. Қаржылық алаяқтық;
6. Спам;
7. Аппараттық және бағдарламалық жасақтама ақаулары.

Көріп отырғаныңыздай, қауіптер өте көп және олардың барлығы бір – бірімен байланысты, мысалы, қызметкерлердің немқұрайлылығына байланысты ақпаратты ұрлау орын алуы мүмкін, ал ақпаратты ұрлау өз кезегінде қаржылық алаяқтыққа байланысты болуы мүмкін.

Бірақ вирустар қауіп-қатерлер арасында көшбасшы болып табылады. Вирустар дегеніміз не және олар қандай екенін қарастырайық.

Компьютерлік вирус – бұл компьютерлік бағдарламалардың бір түрі немесе зиянды код, оның айрықша ерекшелігі – көбею қабілеті (өзін-өзі репликациялау).

Жіктеу

Қазіргі уақытта вирустарды жіктеу мен атаудың бірыңғай жүйесі жоқ. Вирустарды келесі топтарға бөлу.

Зардап шеккен объектілер бойынша:

Файлдық вирустар. Бұл паразиттік вирустар, олар көшірмелерін таратқан кезде орындалатын файлдардың мазмұнын өзгертеді, ал вирус шабуылдаған файлдар көп жағдайда жұмыс қабілеттілігін толығымен немесе ішінара жоғалтады)

Жүктеу вирустары. Бұл икемді немесе қатты дискінің бірінші секторына жазылатын және компьютер жүктелген кезде орындалатын компьютерлік вирустар.

Сценарий вирустары. Инфекцияланбаған сценарийлерге өздігінен ену үшін сценарий тілдерінің біреуінің (Javascript, VBScript) болуын талап етеді.

Макровирустар. Бұл Microsoft Office сияқты бағдарламалық жасақтама пакеттеріне ендірілген макро тілдерде жасалған компьютерлік вирустардың бір түрі.

Бастапқы кодқа әсер ететін вирустар. Бұл типтегі вирустар бағдарламаның бастапқы кодына немесе оның компоненттеріне (OBJ -, LIB -, DCU файлдары), сондай - ақ VCL және Active X компоненттеріне әсер етеді.

Зардап шеккен операциялық жүйелер мен платформалар бойынша

- DOS
- Microsoft Windows
- Unix
- Linux

Вирус қолданатын технологиялар бойынша:

Полиморфты вирустар. Жаңа файлдар мен жүйелік дискілік аймақтарды жұқтырған кезде жергілікті кодты шифрлайтын вирус.

Жасырын вирустар. Вирус өзінің жүйеде болуын толығымен немесе ішінара жасырады, вирус жұқтырған нысандар (жүктеу секторлары, файлдық

жүйе элементтері, жад және т.б.) туралы қосымша ақпаратты оқуды, жазуды, сақтауды жүзеге асыратын операциялық жүйеге жүгінуді тоқтатады.

Руткит. Жүйеде шабуылдаушының немесе зиянды бағдарламаның іздерін жасыруға арналған бағдарлама немесе бағдарламалар жиынтығы.

Вирус жазылған тіл бойынша:

- Құрастыру
- жоғары деңгейлі бағдарламалау тілі
- сценарий тілі және т.б.

Қосымша зиянды функционалдылық бойынша:

Артқы есіктер. Жүйеге қайта кіру мақсатында бастапқы қол жетімділікті алғаннан кейін хакерлер өзі бұзған компьютерде орнататын бағдарламалар. Компьютерде зиянды бағдарламаларға ену үшін артқы есік ретінде қызмет ететін жүйелерге орнатады.

Тыңшылар. Spyware – пайдаланушының келісімінсіз компьютердің конфигурациясы, пайдаланушы қызметі және кез келген басқа құпия ақпарат туралы ақпарат жинау қызметін жүзеге асыратын бағдарламалық жасақтама.

Ботнеттер. Бұл бірнеше хосттардан тұратын, боттары жұмыс істейтін компьютерлік желі – дербес бағдарламалық жасақтама. Әдетте заңсыз немесе мақұлданбаған әрекеттер үшін қолданылады-спам жіберу, қашықтағы жүйеде парольдерді асыра пайдалану, қызмет көрсетуден бас тарту шабуылдары.

Күн сайын жаңа вирустар пайда болады. Қазақстан Республикасының Қылмыстық-процестік кодексіне сәйкес Қазақстанда зиянды бағдарламаларды құру және тарату заңмен қудаланатынын білу керек. білім алушыларды ақпараттандыру.

Сондай-ақ Қазақстан Республикасының Президенті Қ.Тоқаевтың 2023 жылғы 20 наурызда № 145 Жарлығымен бекіткен Қазақстан Республикасының Ақпараттық доктринасы бар.

Доктринады «Сенім және құпиялылық. Ақпаратты трансляциялайтын медиалық процеске қатысушылар, оның ішінде БАҚ бұрмалау және манипуляция жасау элементтерінсіз объективті және анық ақпарат беруге мүдделі болуға тиіс. Барлық шаралар коммуникативтік процестің барлық қатысушылары арасында сенім деңгейін арттыруға бағытталуға тиіс. Бұл ретте доктрина әркімнің жеке өміріне қол сұғылмаушылық жеке және отбасылық құпия, өзінің ар-намысы мен қадір-қасиетін қорғау құқығын қолдайды» және «медиасаланың жаңа субъектілері (интернет-платформалар, әлеуметтік желілер, инфлюенсерлер және т.б.) қызметінің ашықтығын қамтамасыз ететін заңнамалық шараларды қабылдау» делінген.

Сондай-ақ Доктрина жалған ақпаратқа қарсы іс-қимылдың мемлекеттік тетігін жетілдіруге, ақпараттық процестің барлық қатысушылары арасында тиімді коммуникациялар жүйесін құруға мүмкіндік береді, Әділетті Қазақстанды құру бағыты аясында ақпараттық саланың міндеттерін шешуге ықпал ететін болады.

Осыған сәйкес компьютерлердегі ақпаратты қорғау, компьютерлік вирустармен, балалар порно сайттарымен күресу және компьютерлік желілерде

ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша информатика мен компьютерлік сауаттылықты оқыту кезінде білім бері ұйымдарында құқықтық қауіпсіздік жүргізілуі тиіс.

Сондықтан желілік қауіптердің құрбаны болмас үшін өзіңізді, достарыңызды, жеке немесе жұмыс компьютеріңізді қалай қорғауға болатынын туралы баяндаймыз.

Сонымен, желілік қауіптермен қалай күресуге болады?

Кеңес:

1. Кешенді қорғаныс жүйесін орнату.

Кәдімгі антивирусты орнату. Бүгінгі таңда антивирус, брандмауэр, спамға қарсы сүзгі және компьютерді толық қорғауға арналған бірнеше модульді қамтитын «кешенді қорғаныс жүйелері» өзекті.

Кеңес: Күн сайын жаңа вирустар пайда болады, сондықтан қолтаңба базаларын үнемі жаңартып отыруды ұмытпаңыз! Бағдарламаны автоматты түрде жаңартуға орнатқан дұрыс!.

2. Электрондық поштаға абай болу.

Электрондық пошта арқылы маңызды ақпаратты жібермеңіз!. Электрондық пошта тіркемелерін ашуға тыйым салыңыз, өйткені көптеген вирустар тіркемелерде болады және тіркеме ашылғаннан кейін бірден тарала бастайды. Microsoft Outlook және Windows Mail бағдарламалары қауіпті тіркемелерді бұғаттауға көмектеседі.

3. Mozilla Firefox, Google Chrome және Apple Safari браузерлерін пайдаланыңыз.

Көптеген құрттар мен зиянды сценарийлер Internet Explorer және Opera. Танымалдылық рейтингінде IE көш бастап тұр, бірақ ол Windows жүйесіне енгізілгендіктен ғана. Opera браузері өте танымал, өйткені оның ыңғайлы және көптеген параметрлері бар. Қауіпсіздік деңгейі бір браузерде де, екінші браузерде де бірқатар кемшіліктерге ие, сондықтан оларды мүлдем қолданбаған дұрыс.

4. Windows амалдық жүйесін жаңартыңыз.

Windows амалдық жүйесін үнемі жаңартып отырыңыз. Microsoft корпорациясы мезгіл-мезгіл компьютерді қорғауға көмектесетін арнайы қауіпсіздік жаңартуларын шығарады. Бұл жаңартулар ықтимал қауіпті кіру нүктелерін жабу арқылы компьютерге вирустық және басқа шабуылдардың алдын алады.

5. SMS хабарламаларын жібермеңіз.

Енді басқа адамдардың SMS-теріне және қоңырауларды басып шығаруға қол жеткізуді ұсынатын сайттар өте танымал, сонымен қатар файлдарды жүктеу кезінде олар сізге нөміріңізді енгізуді ұсынады немесе кенеттен SMS жіберу арқылы жоюға болатын блоктау терезесі пайда болады.

SMS жіберген кезде, егер сізге төлем үшін қысқа нөмірге хабарлама жіберу қажет болған жағдайда, телефон шотынан біраз қаражатыңыздан айырыласыз, ал одан да қиын жағдайда компьютерде қорқынышты вирус пайда болады.

Сондықтан тіркелу кезінде ешқашан SMS-хабарлама жібермеңіз немесе телефон нөміріңізді күмәнді сайттарға енгізбеңіз!.

6. Лицензиялық бағдарламаны пайдаланыңыз.

Егер бағдарламалардың қарақшылық нұскаларын немесе зиянды бағдарламаның жүктеп алсаңыз, оны іске қосып, антивирустың ескертуін саналы түрде елемейтін болсаңыз, вирусты компьютерге орналасуына өзіңіз жағдай жасайсыз. Сонымен қатар, бағдарлама неғұрлым танымал болса, мұндай ықтималдық соғұрлым жоғары болады. Сондықтан сақ болыңыз! Лицензияланған бағдарламалар сізді осындай қауіптен құтқарады!

7. Брандмауэрді қолданыңыз.

Windows брандмауэрін немесе басқа брандмауэрді қолданыңыз вирусты компьютерге қосылуға тырысқанда күдікті әрекет туралы ескертеді. Ол сондай-ақ вирустарға және хакерлерге компьютерге ықтимал қауіпті бағдарламаларды жүктеуге тыйым салуға мүмкіндік береді.

8. Күрделі құпия сөздерді қолданыңыз.

Статистика көрсеткендей, барлық парольдердің 80%-ы қарапайым сөздер: телефон немесе машина маркалары, туған күн немесе өзінің есімдері және 123 сияқты парольдер. Мұндай парольдер хакерлердің жұмысын едәуір жеңілдетеді. Ең дұрысы, парольдер кем дегенде жеті немесе он екі таңбадан тұруы керек. Бес таңбадан тұратын парольді бұзу уақыты екі-төрт сағатты құрайды, ал жеті таңбалы парольді бұзу үшін екі-төрт жыл қажет болады.

Әр түрлі регистрлердің әріптерін, сандарды және әр түрлі белгішелерді біріктіретін парольдерді қолданған дұрыс.

9. Сақтық көшірме жасаңыз.

Кішкене қауіп төнген кезде, компьютеріңізден құнды ақпаратты жоюға болады, ал одан да жаманы – ұрланғаны. Сыртқы құрылғыдағы маңызды деректердің сақтық көшірмесін жасауды ұмытпаңыз – флэш-карта, оптикалық диск, портативті қатты диск.

10. «Ата-ана бақылауы» мүмкіндігі сізді қауіпсіз етеді.

Балалар психикасы үшін Интернет – бұл психологиялық жарақат алу қаупі және қылмыскерлердің құрбаны болу қаупі.

Ата-анаңыздан желіде талқылайтын тақырыптар мен жаңа Интернет таныстарының шеңберін жасыруға тырыспаңыз, бұл сізге желіде көрген ақпаратты шынымен бағалауға және алданудың құрбаны болмауға көмектеседі.

Осы қарапайым ережелерді сақтай отырып, сіз танымал желілік қауіптерден аулақ бола аласыз.

5. Өзіндік жұмыс

Материалды бекіту үшін компьютерлік тестілеу.

Енді бүгін осы материалды қаншалықты мұқият тыңдағаныңызды тексеру үшін тест тапсырмалары ұсынылады.

Компьютерде орындаңыз.

«Интернет желісіндегі қауіпсіздік» файлын таңдаңыз

Тестте 10 сұрақ бар, әр сұрақта бір ғана дұрыс жауап берілуі керек.

Тест нәтижелері бойынша тест соңында өз нәтижелеріңізді көре аласыз.

Компьютер сізге қоятын баға және бүгінгі сабақ үшін Сіздің бағаңыз болады.

Тест:

1. Сөйлемді аяқтаңыз: зиянды бағдарламаларды (соның ішінде вирустарды) құру және тарату...

- A. Әкімшілік кодекске
- B. Еңбек кодексіне
- C. Қылмыстық кодекске
- D. Азаматтық кодекске

2. Бүгінгі күні вирустардың қандай классификациясы жоқ?

- A. Зардап шеккен нысандар бойынша
- B. Зардап шеккен операциялық жүйелер мен платформалар бойынша
- C. Зардап шеккен файлдар саны бойынша
- D. Қосымша зиянды функционалдылық бойынша

3. Берілген парольдердің қайсысы сенімді

- A. 123456789
- B. qwerty
- C. annaivanova
- D. 13u91A_Ivanova

4. Антивирустық бағдарламалар сіздің компьютеріңіздің қауіпсіздігін қамтамасыз ету үшін сізге қажет:

- A. Бірнеше антивирустық бағдарламаларды орнатыңыз
- B. Интернеттен жүктелген барлық файлдарды жойыңыз
- C. Антивирустық базаларды уақтылы жаңарту
- D. Компьютерді интернеттен ажыратыңыз

5. Браузерлердің қайсысы басқаларға қарағанда қауіпсіз емес деп саналады:

- A. Mozilla Firefox
- B. Internet Explorer
- C. Google Chrome
- D. Opera

6. Электрондық поштамен жұмыс істеу кезінде қандай әрекеттерді орындау ұсынылмайды?

- A. Электрондық хаттарды жіберу
- B. Электрондық поштаңызға фотосуреттер қосу
- C. Белгісіз электрондық пошта тіркемелерін ашу
- D. Жіберілген қалтада электрондық хаттарды қалдыру

7. Егер экранда одан әрі жұмыс істеу үшін SMS жіберуді сұрайтын терезе пайда болса, не істеу керек?

- A. SMS хабарлама жіберу
- B. Қатты дискіні пішімдеуді орындау
- C. Компьютерді қайта іске қосу
- D. SMS хабарлама жібермеу

8. Неліктен сақтық көшірме жасау керек?

- A. Ақпарат барлығына қол жетімді болуы үшін

- В. Маңызды ақпаратты жоғалтпау үшін
- С. Жүйені қалпына келтіру операциясын орындау үшін
- Д. Құжаттарды басып шығару мүмкіндігі болуы үшін

10. Егер веб-сайтта кенеттен компьютерді қайта іске қосуды сұрайтын компьютерді жылдам тексеру туралы хабарлама пайда болса, не істеу керек?

- А. Компьютерді қайта іске қосу
- В. Қатты дискіні пішімдеу
- С. Сайтты жауып, компьютерді тексеру
- Д. Компьютерді өшіру.

6. Топтық жұмыс:

Білім алушылар мен педагогтерден (араласып) тұратын 3 топқа бөлінуіміз керек. Топтық жұмыс компьютерлерде орындалады және компьютер нөмірі бойынша материалды қай топ әзірлегенін анықтаймыз:

1. 1-топ: №1 – №4 компьютерлерде – Қазақстан Республикасының Президенті Қ.Тоқаевтың 2023 жылғы 20 наурызда № 145 Жарлығымен бекіткен Қазақстан Республикасының Ақпараттық доктринасы туралы ақпаратты тауып, топтық талдау жасап, баяндау керек.

2. 2-топ: №5 – №8 компьютерлерде – сіз «желілік этикет» деп аталатын желідегі байланыс ережелерін тауып, топтық талдау жасап, түсіндіру керек

3. 3-топ: №9 – №12 компьютерлерде – антивирустық бағдарламалар туралы ақпарат табу керек және олардың түрлері және танымал антивирустардың қысқаша сипаттамасын талдап, түсіндіру ұсынылады.

6. Семинар қорытындысы: әр топтың жауабына баға беру, талдау Кері байланыс орнату.

*ЖАМБЫЛ ОБЛЫСЫ, ТАРАЗ ҚАЛАСЫ, №56 ОРТА МЕКТЕБІНІҢ ПЕДАГОГ-
ПСИХОЛОГІ ҚЫДЫРБАЕВА МАРЖАН ЖҰМАТАЙҚЫЗЫНЫҢ
ТӘЖІРИБЕСІНЕН*

*Тақырыбы: «Буллинг және кибербуллинг және оның алдын алу
жолдары»*

Формасы: ата-аналарға арналған семинар-тренинг

Мақсаты: Мектепте буллинг мәселесі бойынша ата-аналардың білімдерін жандандыру.

Міндеттер: Ата-аналарды «Буллинг» ұғымымен таныстыру. Ата-аналардың белсенді педагогикалық ұстанымын қалыптастыру. Ата-аналарды айдап салу жағдайын тануға үйрету. Ата-аналарды өз баласын буллингтен қорғау әдістерімен таныстыру.

Құрал-жабдықтар: мультимедиялық проектор, презентация, бейдждер, рефлексивті парақтар, фломастерлер, доптар.

Сабақтың ұзақтығы: 60 минут.

1.Кіріспе бөлім. Топпен, топтық ережелермен танысу. Психолог: Қайырлы күн, құрметті ата-аналар. Біз буллинг ұғымымен, оның негізгі сипаттарымен танысып, келесі сұрақтарға жауап табуға тырысамыз: бала буллингке ұшыраған жағдайда ата-аналарға не істеу керек? Бала агрессор болған жағдайда және мұндай жағдайлардың пайда болмауы үшін не істеу керек. Талқылауға кіріспес бұрын танысайық. Жүргізілу барысында ережелерді шеңбер бойында атап айтамын. «Шеңбер – қатысушылардың теңдігінің символы, сөйлейтін адамға құрмет қағидаты, мен-айтушымын, бағалау, құпиялылық - барлық ақпарат шеңберде қалады».

Сергіту сәті. «Танысу» жаттығуы – шеңбер бойынша қатысушылар өз атын айтып, мына сұраққа жауап береді: менің көңіл-күйім қандай?

«Ассоциация» жаттығуы. Психолог: «буллинг» сөзімен қандай ассоциациялар бар? Ата-аналар қалауы бойынша сөйлейді.

2. *Негізгі бөлігі* «Мектептегі буллинг» мультимедиялық презентациясын қолдану. Буллинг – ертеден келе жатқан жаңа термин, ғасырлық құбылысбалалардың әлімжеттілігі деп айтуға болады. Іс жүзінде әр сыныпта күлкіге қалатын, кейде кейбір кезде басқалар тарапынан мазақтау, кейде барлық сынып оқушылары тарапынан ашық қорлау объектілері болып табылатын балалар бар. Балалар ұжымында буллинг көбінесе жасөспірімдердің бос болмауының нәтижесі болып табылады. Буллинг (ағылш. bullying – сыныптастар тобы тарапынан балаға қатысты қорқыту, физикалық және/немесе психологиялық террор), – бұл физикалық немесе психикалық күшті жеке тұлға немесе топ осы жағдайда әлсіз адамға дене немесе психологиялық ауырсыну тудырған кезде қатал қарым-қатынас нысаны болып табылады. Буллинг проблемасын шешудің тиімді әдістерін әзірлеуге көшпес бұрын осы құбылыстың түрлерін, себептерін және олардың барлық алуан түрлерінде

мүмкін болатын көріністерін зерттеу қажет. Буллинг келесі түрлерін бөліп көрсетеді:

Психологиялық (моральдық) зорлық-зомбылық:

1. Вебальды (мазақтау, лақап есім беру, шексіз ескертулер мен объективті емес бағалаулар, мазасыздану, басқа балалардың қатысуымен кемсіту, дене жарақатын жою қаупі, шантаж, шағым беру қаупі, достасуды тоқтату, қорқыту, жеккөрушілік, құрбандыққа жала жабу, қорлау.

2. Әлеуметтік ерекшелік (бойкот, бас тарту, оқшаулау, құрбанның (баламен ойнаудан бас тарту, онымен бір партада отырғысы келмейді);

3. Кибербуллинг – интернетте қорлайтын мәтіндерді, бейнелер мен фотосуреттерді, қауіп-қатерлерді жариялау және тарату, сондай-ақ онлайн арқылы өзін «құрбандыққа» беру (12-15 жастағы оқушылардың 30%-ға дейін ұшырайды). Соңғы уақытта тарату троллинг (trolling – қармақтың басына балық аулау) – қатысушылар арасындағы қақтығыстарды, өзара тіл тигізуді туғызу мақсатында ғаламторда (форумдарда, дискуссиялық топтарда, блогтарда және т.б.) арандатушылық хабарламаларды орналастыру.

4. Физикалық зорлық-зомбылық ұру, соққы жасау, бүлдіру және заттарды алу, ұрлық және т.б.

Әртүрлі көзқарастар бойынша буллингтің бірінші түрі кең таралған:

1. Сөздік қорлау (қорлау, жәбірлеу, өрескел әзілдер, ауызша арандату, әдепсіз әзілдер және т. б.).

2. Бойкот.

3. Физикалық жазу.

4. Өсек және естігенін тарату,

5. Ұрлық.

5. Зерттеулер көрсеткендей, төменгі сыныптарда буллинг жағдайларының кездесуінің жиілігі жоғары, ер балалар арасында кең таралған, 14-15 жасқа қарай төмендейді, кибербуллинг 13-15 жастағы жасөспірімдер арасында кең таралған, көбінесе қыздарға тән.

Буллингтің негізгі сипаттамалары

✓ Қастықпен;

✓ Тұрақтылық;

✓ Күш теңсіздігі;

✓ Топтық процесс (қатысушылардың кең ауқымына қатысты);

✓ Өз өзінен тоқтай алмау.

6. Барлық қатысушыларға теріс психологиялық әсер ету. Статистика бойынша, буллинг кезінде балалардың көп пайызы көмек көрсетпейді: 62% балалардың буллинг туралы айтпайды, 24% достарымен бөліседі, 2% ата-аналарына айтады.

Балалар неге көмек сұрамайды?

1. Мұны өз бетінше жеңгісі келеді;

2. Балалар жәбірлеушіден қорқуы мүмкін;

3. Әлсіздік үшін бас тартудан қорқады;
4. Ешкім оған қамқорлық жасамайды деп ойлайды;
5. Балалар олардың құрдастары одан бас тартады деп қорқуы мүмкін.

Буллингтегі рөлдерді бөлу Жоғарыда айтылғандай, буллинг – әрдайым ұжымдық құбылыс. Оған саналы немесе еріксіз қатысатын балаларды төрт санатқа бөлуге болады: бастамашылар, қудалаушылар, бақылаушылар, құрбандар.

Бастамашылары бір-үш бала, олардың мақсаты өзін-өзі нық орнықтыру, ұжымда беделге ие болу, сондықтан олар агрессивті қылықтар көрсетеді. Кейбір жағдайларда зорлық-зомбылыққа басқа балаға қатысты жеке жеккөрушілік немесе мұқият жоспарланған кек алушылық себеп болуы мүмкін. Бастаушылар топтың бір немесе бірнеше қатысушыларын демонстрациялайды, күледі немесе елемейді. Олардың назарына ұмтылады, сынып көшбасшысының рөліне ие болғысы келеді.

- өз отбасындағы зорлық-зомбылықтан зардап шегетін және сыныптағы ең нашар зорлық-зомбылықпен өзінің қайғысын өтейтін балалар;

- оқушылар, лидерлік пен билікке талпыныс, басқалардың есебінен өзін көрсету;

- тез қозғыш және өте импульсивті, агрессивті мінез-құлық танытатын балалар;

- тәртіпті жиі бұзатын балалар;

- басқаларды өз мәселелерінде айыптауға бейім.

- агрессивті балалар;

- физикалық мықты балалар.

Буллингтің құрбаны немесе объектісі:

* жиі қорқынышты болады,

* тыныш балалар,

* жиі физикалық әлсіздік,

* стандартты емес келбеті бар балалар,

* оқуда ерекше болу,

* сезімтал, өзіне қарсы тұра алмайтын, сенімділік көрсету, оны қорғау,

* белгілі бір саладағы талант немесе, керісінше, үлгерімі нашар,

* өзін-өзі бағалауы төмен немесе керісінше жоғары балалар.

Буллингтің құрбаны кез келген оқушы бола алады. «Сайқымазақ», «Көнгіш құрбаны», «Құл», «Ақ қарға», «Танымал емес», «Өсекші». «Агрессорлар»: агрессор шабуылшы, бас тартушы агрессор,

Ата-аналарға баланың буллингтің құрбаны болғанын қалай түсінуге болады?

Егер сіздің балаңыз:

* мектепке бармай, мектепке бармаудың кез келген мүмкіндігіне қуанатын болса;

* мектептен қысыммен қайтқанда;

* нақты себепсіз жиі жыласа;

- * өз сыныптастарынан ешкімді ешқашан есіне алмаса;
- * мектеп өмірі туралы өте аз айтса;
- * жалғыздық. Оны ешкім туған күндеріне қонаққа шақырмаса және ол ешкімді өзіне шақырғысы келмесе. Бұл жағдайда сіздің балаңыз буллингтің объектісі болуы мүмкін.

Топтық жұмыстар

Құрметті қатысушылар: қазір сіздер екі топқа бөлініңіздер. Қатысушылар лимон-апельсин деп саналады. Қазір сіздермен келесі сұрақтардың жауабын табуға тырысайық:

1. «Лимондар» тобы топтық пікірталас барысында «ата-аналарға жәбірлеушінің құрбаны болған жағдайда не істеу керек?» деген сұраққа жауап табуға тырысады.

2. «Апельсиндер» тобы «буллер бала болған жағдайда ата-аналарға не істеу керек?» деген сұраққа жауап табуға тырысады».

Талқылаудан кейін әр топтың өкілі осы мәселе бойынша айтады. Психолог ата-аналардың нақты ұсыныстарын талқылайды, қорытынды жасайды.

**ЖАМБЫЛ ОБЛЫСЫ, МОЙЫНҚҰМ АУДАНЫ БІЛІМ БӨЛІМІНІҢ
ӘДІСКЕРІ РАЙЫМБЕКОВА ГҮЛНАР ЖАМБЫЛБАЕВНАНЫҢ
ТӘЖІРИБЕСІНЕН**

*Тақырыбы: «Мектепте өткізілетін буллингiнiң алдын алу бойынша
жаттығулар мен ойындар»*

«Алақан» жаттығуы

Мақсаты: басқаға көңіл бөлу және өзінің жақсы қасиетін түсіне білу, өзін-өзі бағалау.

Қажетті құралдар: қағаз және қалам.

Нұсқау: әр адам қағаз бетіне алақанның суретін салады. Ортасына өз атын жазады, әрбір саусақта өзіне ұнайтын нәрсені жазады. Содан кейін парақты оң жақ көршісіне береді, ол 30 секунд ішінде парақтың сыртына сол адамға, яғни, алақан иесінің бойында ұнайтын нәрсе туралы жазады.

Осылайша бүкіл шеңбер арқылы жүргізіліп шығады.

«Шатастыру» ойыны

Нұсқау: жүргізуші таңдалады, ол сыртқа шығады. Қалғандары орындарынан тұрып шеңбер құрады, бір-бірлерінің қолынан ұстайды және өзінің орналасқан жерін «шатастырып» әр бағытта өзгертеді.

Жүргізушінің міндеті – қатысушылардың шеңберді қайта құратындай етіп орнына келтіру. Егер тапсырманы орындау тым ұзаққа созылса, жүргізушіге бір жұп қолды ажыратып, осы қатысушыларды қажетті орынға қайтадан ауыстыруға мүмкіндік беріледі.

«Біз немен ұқсаспыз» жаттығуы

Мақсаты: бір қарағанда, кездейсоқ кездескен адамдардың тіл табуы мен өзара түсіністігін көрсету.

Топ жетекшісі қатысушыларды жұптарға бөледі. Жұптың ішінде қатысушыларға ортақ нәрсе табу ұсынылады. Бұл сыртқы келбеті, мүдделері, тұрғылықты жері, тағам құмарлығы және т.б. ерекшеліктері болуы мүмкін. Содан кейін жұптар төрттікке біріктіріледі, олардың ішінде ортақ қасиеттер іздестіріледі. Одан әрі сегіз адамнан тұратын топтар құрып, ойынды қайталауға болады.

«Менің мықты жақтарым» жаттығуы

Педагог-психологтің нұсқауы: «Әр қайссыңыздың күшті жақтарыңыз бар, өзіңізді бағалай білесіз. Бұл қасиетіңіз сізге өз күштеріңізге деген сенімділік және ішкі бостандық сезімдерін береді.

Парақ бетінің бірінші бағанына өзіңіздің күшті жақтарыңызды жазыңыз. Ал екінші бағанға өзіңізге тән емес, алайда өз бойыңызда дамытқыңыз келетін қасиеттерді сипаттап жазыңыз. Тізімді жасауға сізге 5 минут уақыт беріледі.

Содан кейін барлығы үлкен шеңбер құрып отырып әрбір қатысушы өз тізімін оқиды және сипаттап айтып береді.

Әр қатысушыға сөйлеуге 2 минут уақыт беріледі. Тыңдаушылар кейбір деректерді нақтылауды және толықтыруды сұрауы мүмкін, бірақ өз пікірлерін қоса білдіруге болмайды. Сіз сол қасиеттердің мықты жағы екенін түсіндіруге міндетті емессіз. Оған сіздің өзіңіздің сенімді болғаныңыз жеткілікті.

Ескерту. Шеңберде талқылауды қатысушылар саны көп болғанда – 7-8 адамнан тұратын топтарда өткізген жөн. Соңында ұжымдық пікірталасты өткізу керек, пікірде болған жалпы жаттығуды орындау кезінде әр адамның бастан кешкен сезімдеріне назар аудару қажет.

«Басқа адамға жағымды сөз айтқым келеді» жаттығуы

Нұсқаулық. Бөлмеге кезекпен кірген қатысушыларға алдымен басқа қатысушыларды мақтап, содан кейін өзін мақтау ұсынылады. Тапсырманы орындау барысында педагог-психолог қоршаған ортада оң реакция тудырған мақтауға назар аударады. Содан кейін қатысушыларға өздерін мақтаған кезде не сезінгенін, не ұнағаны туралы айтып беру ұсынады: өз атына мақтауды тыңдау немесе басқасын мақтау қалай әсер еткені туралы пікірлерін айтады. Соңында қатысушылар достарын, таныстарын және тіпті бейтаныс адамдарды да мақтауы керек.

«Бізде таңдау бар» жаттығуы

Ескерту. Педагог-психолог қатысушыларда өмірде жиі таңдауға тура келетіндігі, кейде бұл өте қиын таңдау болатындығы туралы пікірді қалыптастыруы керек. Біз әрқашан өзіміз қалайтын және ұнайтын нәрсені жасай алмаймыз. Буллингке қатысты күш көрсете отырып, қорқытып, ұрып-соғып қол жеткізу оңайырақ және конструктивті – бейбіт уағдаласу (келісімге келу) әлдеқайда қиын.

Педагог-психологтің нұсқауы: «Таныс емес қалада достарыңыз, ата-аналарыңыз, туыстарыңыздың болмайтынын елестетіңіз. Сізде тұрғын үй, жұмыс жоқ, бірақ алғашқы күндерге жететін өте аз ғана ақшаң бар. Сізге аман қалу үшін әрекет ету алгоритмін анықтау қажет.

Мен сіздерге көмек берейін. Сізге ақша қажет және сіз оларды жұмыс жасап ала аласыз, алайда сізде білім жоқ». Ары қарай қатысушыларға 30 минут ішінде жазбаша сұрақтарға жауап беру ұсынылады: Сіз қай қалада немесе қай елде тұрасыз? Қазір жылдың қай мезгілі? Сіз не істеуді жоспарлап отырсыз? Сіздің іс-әрекетіңіз қандай? Сіз не істей аласыз? (Жұмыс түрлерінің тізімін жасаңыз.) Содан кейін не болады? Барлығына жауап бергеннен кейін талқылау өтеді. Қосалқы жұмыстар – бұл уақытша табыс, ал жалпы оқу керек деген қорытынды жасалады. Бірақ ең алдымен таңдауды анықтау үшін сізге өз мүмкіндіктеріңіз бен қабілеттеріңізді жете анықтау қажет.

«Кемелер мен жартастар» жаттығуы

Мақсаты: шиеленісті шешу, қарым-қатынас дағдыларын дамыту, өзара түсіністік деңгейін арттыру. Ойыншылардың жартысы – «кемелер», жартысы – «жартастар». «Жартастар» еденге отырғызылады, «кемелер» көзді жұмып, бөлмеде ретсіз қозғалады. «Кеме» жақындағанда «жартас» толқындар тасқа домалайтын дыбыс шығарады. «Жартастың» мақсаты – «кеменің құлауына» жол бермеу. Содан кейін ойнайтындардың рөлдері ауысады.

«Патша» ойыны

Педагог-психологтің сөзі: «Кім бір кездері патша болуды армандады? Патша болған адам қандай артықшылыққа ие болады? Бұл қандай қиындықтар әкеледі? Сіз қайырымды патшаның қайырымсыз патшадан айырмашылығын қандай екенін білесіз бе? Мен сізге патша болу ойынын ұсынғым келеді. Әрине, мәңгі емес, тек он минутқа ғана».

Ойыншылар Патшаны анықтайды. Қалған қатысушылар, қызметшілер, олар бұйрық берген барлық нәрсені істеу керек. Патша басқа қатысушыларды ренжітетін немесе қорлайтын бұйрықтар беруге құқығы жоқ.

Мысалы, ол қызметкерлерге жұмсайтын, қолына су құю, иілу, су әкеліп беру сияқты бұйрықтар беруіне болады.

Басқару уақыты аяқталған кезде қатысушылар топқа жиналып ойынан алынған нәтижені талқылайды. Ол келесі жолы патша болатын адамның қайырымды патша болу мүмкіндіктерін қайта қарауға көмектеседі.

Талқылау сұрақтары:

- ✓ Патша болған кезде өзіңізді қалай сезіндіңіз?
- ✓ Бұл рөлде сізге не ұнады?
- ✓ Айналаңыздағыларға бұйрық беру оңай болды ма?
- ✓ Қызметші болған кезде не сезіндіңіз?
- ✓ Патшаның тілеуін орындау оңай болды ма?
- ✓ Патша Асқар (Маді) болғанда, ол сен үшін мейірімді немесе зұлым патша болды ма?
- ✓ Қайырымды патша өз тілектерін орындай алды ма?

«Аяқталмаған сөйлемдер - жауапкершілік» жаттығуы

Мақсаты: өзіне немесе басқаларға жауапкершілік сезімін білдіре отырып, түсінуге көмектесу.

Ұсыныстар айтылып жазылады; үзіліс кезінде қатысушылар бұл ұсыныстарды аяқтау керек; бірінші реакция ең дұрыс деп саналады; егер қандай да бір ұсыныс сәйкес келмесе, оны қабылдамауға болады; соңында барлығын аяқтау үшін біраз уақыт береді.

- ✓ Мен үшін жауапты болу дегенді білдіреді ...
- ✓ Кейбір адамдар басқаларға қарағанда жауапты, бұл кейбір адамдар...
- ✓ Жауапсыз адамдар – бұл
- ✓ Мен басқаларға деген жауапкершілігімді білдіремін....

✓ Мен жауапты адамды білемін...
✓ Менің жауапкершілігім қаншалықты күшті болса, соғұрлым менде көп...

- ✓ Мен басқа үшін жауапты болуға қорқамын...
- ✓ Өзіне қатысты жауапты болу – бұл...
- ✓ Мен жауаптымын...

Жұптармен шеңберде талқылау жүргізіледі. Жүргізуші қатысушылардың көзқарастарын анықтауға және өз сезімдерін, ойларын, әрекеттері үшін жауапкершілік дәрежесін түсінуге көмектеседі. Талқылауды өткізу кезінде қатысушыларға екі позицияның артықшылықтары мен кемшіліктерін сезінуге болады: «өзгелер үшін жауапкершілік» және «басқаларға жауапты қарым-қатынас». Төменде келтірілген мысалдар осы мәселеде жетекшілік етуге көмектеседі.

❖ Мен басқаларға жауапкершілікті сезінген кезде, мен... (түзетемін, қорғаймын, құтқарамын, бақылаймын, олардың сезімін қабылдаймын...).

❖ Жауапкершілікті сезіне отырып, мені алаңдатты... (шешімдер, егжей-тегжейлі мәселелер, жауаптар, мән-жайлар, қателеспеу үшін орындау...).

❖ Басқаларға жауапты қарым-қатынас көрсете отырып, мен... (эмпатия (мазасыздану, сезімдерді түсіну), көңіл көтеремін, бөлісемін, жанжалдасу, тыңдаймын...).

❖ Мен көмекші/жолсерік, т.б. басқаға жол көрсетушімін.

❖ Менің ойымша, адам өзі үшін және өз іс-әрекеттері үшін жауап береді.

❖ Мен адамдарға сенемін және олар қандай болса да қабылдаймын.

«Дөрекі» жаттығуы

Педагог-психологтің нұсқауы: «Сіз буфетте кезекте тұрасыз және кенеттен сіздің алдыңызды орап, біреу «басып кіреді!» Жағдай өміршең, себебі көп жағдайда өз ренішін білдіру үшін айтарға сөз жоқ. Иә, тіпті ондай адамның бассыздығын басуға сөз де табылмайды. Дегенмен, не істеу керек? Өйткені, мұндай жағдайлар сөзсіз болуы мүмкін. Бұл жағдайды талдауға тырысамыз. Жұптарға бөлінеміз. Әр жұппен сол жақта тәртіпті түрде кезекте тұрған жан, ал оң жақта «бассыз» тап береді.

Осы жағдайға бассыздық жасаған жанның ынтасын басу үшін өз пікіріңізді білдіріңіз.

Бастаймыз! Енді рөлдерді ауыстырыңыз.

Ал енді осы жағдайда ең жақсы жауап үшін байқау өткізейік.

*ЖАМБЫЛ ОБЛЫСЫ, Н.ТІЛЕНДИЕВ АТЫНДАҒЫ МЕКТЕП-
ИНТЕРНАТЫ ДИРЕКТОРЫНЫҢ ТӘРБИЕ ІСІ ЖӨНІНДЕГІ ОРЫНБАСАРЫ
СЕЙТЖАНОВА АЙЖАН МЫРЗАБАЙҚЫЗЫНЫҢ ТӘЖІРИБЕСІНЕН*

Тақырыбы: «Жасөспірімдер арасында буллингтің алдын-алу. Әр ата-ана нені білуі тиіс?»

Формасы: ата-аналар жиналысы.

Мақсаты: Құқықтық санасы мен мәдениеті жоғары деңгейде дамыған тұлғаны қалыптастыруда ата-аналарға бағыт беру.

Міндеттері:

- ✓ Ата-аналарға жас ұрпақты буллинг пен қатыгездікпен, сондай-ақ балалар мен жасөспірімдердің әлеуметтік және психикалық денсаулығына зардабын тигізетін ақпараттың теріс әсерінен қорғау туралы түсіндіру;
- ✓ Жасөспірімдердің өз іс-әрекетіне жауапты қарым-қатынасын қалыптастыру мәселелерінде ата-аналарға құзыретті көмек көрсету;
- ✓ Ата-аналардың белсенді педагогикалық ұстанымын қалыптастыру.

Барысы: Құрметті ата - аналар, бүгін мен сіздерге балаларыңызға қауіпті буллинг туралы мәлімет беріледі.

Буллинг – бұл өзін қорғай алмайтын адамға қатысты бір адамның немесе адамдар тобының тарапынан түрлі зорлық-зомбылық пен қорлау түрлерінің қайталанатын актілері.

Буллинг әрқашан құрбандықты жою, оның қорқынышын тудыру, қорлау, бағындыру мақсатын көздейді. Оқушыларды бір адам да, бір топ адам да жарақаттай алады.

Ақпараттық-коммуникациялық технологиялардың көмегімен қорлайтын фотосуреттер, қорлайтын хабарламалар мен қауіп-қатерлер таратылады. Мұндай құбылыс кибербуллинг деп аталады.

Мектептегі физикалық зорлық-зомбылық, өзгелердің қатарында кіші және орта жастағы (11-15 жас) жасөспірімдер арасында көп таралған төбелестерде көрінеді. Ересек жасөспірімдер жиі көзге көрінбейтін, бірақ сөзбен қорлау сияқты зорлық-зомбылықтың бастапқыда аса байқалмайтын түрлеріне тартылады.

Физикалық емес зорлық-зомбылық байқалады:

- ✓ ренжіген пікірлерден;
- ✓ қорлаудан;
- ✓ ойнап айту емес, ашуланудан.

Балаға қатысты зорлық-зомбылық туралы оның мінез-құлқының, көңіл күйінің ерекшеліктерін, сыртқы түрін, сабаққа «себепсіз» келмеуі және үлгерімінің төмендеуі болып табылады. Егер сіз өз балаңызда жақсы емес елеулі өзгерістерді байқасаңыз, бұл ойлануға және оны мұқият қадағалауға себеп болады, ал баланың жарақат алу туралы қауіптер расталған жағдайда

дереу мектеп әкімшілігіне немесе сынып жетекшісіне немесе педагог-психологқа хабарласыңыз.

Буллинг туралы аңыздар мен ғылыми фактілер

1-ші аңыз - Осындай ауқымда мектептегі зорлық-зомбылық соңғы жылдары ғана пайда болды.

Бұл жалған. 1910 жылы Венада Зигмунд Фрейд, Альфред Адлер және Уильям Стекел «суицид туралы, атап айтқанда, орта мектеп оқушыларының арасында суицид туралы» тақырыбы бойынша Австро-Венгрияда алғашқы конгресс өткізді. З.Фрейд оның рухтандырушысы және теоретигі болды. Барлық уақытта мектеп әлі жетілмеген тұлғаларды – балалар мен жасөспірімдерді жинайтын болғандықтан, онда зорлық-зомбылық мәселесі болды және болады деп түсіндірді.

2-ші аңыз – Буллинг, тәртіптің басқа түрлері сияқты, тек әлсіз мұғалімнің сыныбында болуы мүмкін.

Бұл ұстаным статистиканы білмегеннен туындап негізделеді. Зерттеулер растайды: кез келген мектепте және кез келген мұғалімде, әсіресе жақсы мұғалімде де (себебі балалар одан қатты қорықпайды) жарақат, арандатушылық, физикалық немесе эмоциялық қысым фактісі немесе фактілері болуы мүмкін.

3-ші аңыз - Зорлық-зомбылық көп емес (біздің мектепте ол мүлдем жоқ!), ол бастауыш және орта буында 10%-дай оқушылар қатысты.

Доктор Дэн Олвеустың мәліметтері бойынша, әлемнің барлық дамыған елдерінде (Жапониядан басқа) шамамен 16% қыз және 17,5% ұл бала буллингтің құрбандарына ай сайын 2-3 рет ұшырайды және бұл олардың қандай мектепте оқитындарына қатысты емес. Олар қымбат элиталық немесе бюджеттік әлеуметтік жағдайы төмен ауданда оқуы мүмкін. 7% қыз және 12% ұлдардың өздері улаудың бастамашысы – Буллер болып табылады. Осы деректер әртүрлі елдер үшін толық сәйкес келеді.

4-ші аңыз – Буллинг жасөспірімдер ортасына тән, ал бастауыш мектепте бұл феномен жоқ.

Д. Олвеустың мәліметтері бойынша сыныптар бойынша буллинг феноменінің кездесу жиілігінің өзгеру статистикасы бар.

5-ші аңыз - Тек физикалық зорлық-зомбылық жағдайлары педагогикалық ұжымның мазасыздығын туғызуы тиіс.

Мұндай ұстаным әлемдік статистикаға қайшы келеді: балалар агрессивті сипаттағы физикалық әсерлерге, көбінесе агрессияның басқа түрлеріне байланысты өздерін «жәбірленуші» күйін бастан кешіреді. Статистика бойынша әртүрлі елдерде кездесу жиілігі бойынша бірінші орында сөз жарақаты – (қорлау, зұлым әзілдер, сөз арандату, шақыру, әдепсіз әзілдер және т.б.). Екінші орында бойкот, үшінші орында-физикалық зорлық-зомбылық. Төртіншіден – есту және өсек айту, бесінші – ұрлық. Бұдан әрі біз суицидтің себебі физикалық зорлық-зомбылық емес, референттік топ тарапынан оқшаулау, бойкот екенін көреміз.

6-шы аңыз – Буллерлер «бақытсыз» балалар, өзін-өзі бағалауы төмен, құрдастарымен басқаша байланыс жасай алмайтын балалар болады.

Бұл қауіпті жаңылыс. Статистика көрсетіп отырғандай, агрессорлар өзін-өзі жоғары бағалайды, олардың мінез-құлқын өзін бақылай алатын аффектіге байланысты емес, бұл қолдан ұйымдастырылған, алдын ала жоспарланған есеп. Олар өздерін өте дұрыс ұстай алады, қысымды сезінбесе ашықтан – ашық зұлымдықты қасақана жасайды.

7-ші аңыз - Буллингтің құрбандары «өздері кінәлі» болған, құрдастарымен қарым-қатынас жасай алмайтын балалар болады.

Ішінара бұл дұрыс, бірақ басқа да балалар бар, олар әлеуметтенген, достары бар, олар әлі күнге дейін қалыпты, өз-өздерін бағалауы орташа. Статистика бойынша буллингтің құрбаны кез келген оқушы бола алады. Буллинкте ең нашары – куәгерлердің әсері оған белсенді қатыспайтын балалар.

Буллинг адамдардың психологиялық жағымсыз қасиеттерін тудырады. Неліктен?

1) Буллинг жұқпалы;

2) Онда сіз өзіңізді, күш пен әлсіздік арасында таңдауға мәжбүр боласыз (душар болғандар жиі күлкілі және өкінішті көрінеді), әлсіз болғанын көрсеткісі келмейді;

3) Сіздің жеке жауапкершілікті сезінбеуіңізгетез итермелейді, бірақ ол басқалар сияқты болуға итермелейді;

4) Құрбандардың қайғы-қасіреті қайтадан қайталана береді, ал сізде осыған қатысты аяныш сезімі бола бермейтінің сезесіз. Нейтралды күй кешесіз.

Ұсыныстар:

Сіздің балаңызды мектеп буллингі бойынша қауіпті тобына түспеу үшін келесі түрде әрекет етуге үйретіңіз: өзін қарапайым ұстау:

- ✓ өзінің табыстарымен, ата-аналарымен және достарымен, заттарымен мақтанбау;
- ✓ мұғалімдерге, құрдастарына жағымпазданбай өзін лайықты ұстау;
- ✓ сыныптастар арасында кем дегенде бір дос табу;
- ✓ сыныптастарын қонаққа шақыру;
- ✓ өз сыныптастарының пікірін құрметтеуді үйрену;
- ✓ құрдастарымен дауласқанда әрқашан жеңуге тырыспау;
- ✓ егер балаңыздікі шын мәнінде дұрыс болмаса, ұтуды және басқаға жол беруді үйрену;
- ✓ балаға оқу ғана емес, сынып ұжымының мүшесі болуға көмектесу;
- ✓ тіпті олар сізге қажетсіз болып көрінсе де, баланы мектептің іс-шараларына қарсы қоймау.

Ата-аналарға арналған жалпы әдістемелік ұсыныстар

Баланың көзінше ұрыс-керіске, көпшілік алдындағы дауға жол бермеңіз, ол оның мінез-құлық ерекшелігін қалыптастыруы мүмкін, және ол әлеуметтік қоршаған ортаға таралады.

✓ Сіздің балаңыз мектепке дейін және мектепте тамақтанатынын қадағалаңыз. Көптеген балалар мектептен тамақтанбай келеді, бұл да агрессивті мінез-құлықты тудырады.

✓ Баланың мәселелеріне бей-жай қарамаңыз, ата-аналар жиналысы өткізілетін уақытта ғана емес, сондай-ақ тоқсан бойы мектепке баруға тырысыңыз.

Ата-аналар жиналысына барғаннан кейін көптеген ата-аналар баланы неғұрлым көбірек жазалауға және сол арқылы ұятқа қалдым деп кек алуға бір мақсатпен үйлеріне оралады. Тәрбиелеудің осындай тактикасынан кейін ата-ана мен бала арасындағы жанжалдар қарым-қатынастың дәстүрлі түріне айналады, балалар тек ата-анасына ғана емес, ересектерге де сенуден бас тартады, өздерінің проблемалары мен қиындықтары туралы айтудан қорқады, өтірік айтады және теріс қарайды, тұйық болады, үйден қашып кетеді, қолдау іздейді.

Егер алдын алу шаралары көмектеспесе, сіздің балаңыз буллингтің құрбаны болса, Сізге ата-ана ретінде қажет:

Ренжіген баланың ата-аналарына кеңестер:

✓ Оны осы жағдаймен жалғыз қалдырмаңыз.
✓ Баланы тыңдап, түсініңіз: жанжалдың мәні неде, қанша уақыт болды, балаға қауіп бар ма?

✓ Өз балаңызбен сөйлесіңіз.

✓ Егер басқа балалар оны ұрса, мазаласа, заттары жоғалып, мазақтап күлсе, қорласа, дереу әрекет етіңіз.

✓ Айдап салуға душар болған бала жақсы табысқа жетсе немесе жақсы әрекеттер жасаса да, сыныптастардың көңілін жаулап ала алмайтынын есте сақтаңыз.

Ол жақсы баға алса, оны «оқымысты» (ботаник) деп мазақ қылады, біреуге көмектессе, «әлсіз» деп атайды. Оның жетістіктері топты тағы да үлкен шабуылдарға итермелейді. Тыныштық сақтаңыз. Балаңызға сіздің кез-келген жағдайды жеңе алатыныңызды білу маңызды. Буллерлердің ата-анасымен сөйлесіңіз. Бірақ олармен қақтығысқа түспеңіз. Балаларға бірлесіп көмек көрсету қажет.

Кибербуллинг. Балаға қалай көмектесуге болады?

Алдымен сіздің (балаңыздың) әлеуметтік желілерді қолдануда сенімді құпия пароль сөзі бар екеніне көз жеткізу керек.

Егер балаңыздың кибербуллинг фактісі белгілі болса, оның телефонын алу немесе интернетке кіргізбеу емес, ол сіздің қалай жазалайтыныңызға байланысты, ал ол соншалықты зардап шегеді.

Балаға көмектесуге дайын екенін түсініңіз және оған ұрыспаңыз немесе айыптамаңыз. Баламен бірге жағдайды анықтаңыз. Жанжал қашан пайда болды? Себебі не болды? Қысымға кімдер қатысады? Баланың өмірі мен

денсаулығына қауіп бар ма? Қысымға байланысты дәлелдемелер жинаңыз (скриншоттар, электронды хаттар, фотосуреттер және т.б.) Агрессорға дұрыс жауап беруге үйретіңіз.

Қысымды тоқтатудың ең жақсы жолы – реніштерді елемеу. Балаға агрессорларды бұғаттауға немесе оларды «қара тізімге» қосуға көмектесіңіз. Кейде орын алған ресурстарға байланысты баланың аккаунтын уақытша жою керек.

- Көмек сұраңыз.
- Егер қысым ашық түрде немесе топта болса, ресурстарды әкімшілікке ренжітетіндерді бұғаттауды өтініп, скриншоттарды кибербуллингтің дәлелдемелерімен бірге бекіту керек.
- Егер қысымға мектеп оқушылары қатысса, жағдай туралы сынып жетекшісіне немесе психологқа немесе мектеп әкімшілігіне айтыңыз.
- Егер баланың өмірі мен денсаулығына қауіп төнсе, арызға барлық жиналған дәлелдемелерді қоса отырып, құқық қорғау органдарына хабарласыңыз. Зерттеулерге сүйенетін болсақ кибершабуылға бесінші – алтыншы сынып оқушылары жиі ұшырайды.

Егер сіздің балаңыз ренжітуші ретінде қысымға тартылған болса:

Ақиқатын анықтауға тырысыңыз, бірақ ұзақ жауап алудан аулақ болыңыз.

- Егер бала байланысқа шықпаса, оған: «Мен білемін, көптеген балаларға осындай нәрселер туралы айту қиын, бірақ мен саған көмектескім келеді және сен дайын болған кезде бұл туралы сөйлесе аламыз» деп айтыңыз.
- Мектеп әкімшілігін хабардар етіңіз.
- Егер олар жағдай туралы сізбен сөйлескісі келсе, басқа ата-аналарға қатысты қорғаныс позициясын құптамаңыз.
- Өз балаңызды иеліктен шығуымен жазаламаңыз, бірақ оған мұндай мінез-құлықтың салдары болатынын түсініңіздер.
- Бұл салдардың қандай екенін және қалай болатыны туралы әңгімелесу.
- Қалыпты күнделікті өмірді қолдауға тырысыңыз.
- Балаларыңызға жарақат алғандардың куәгері бола отырып, олар бірге қатысушы бола алатынын түсіндіріңіз.

Шеңбер бойынша рефлексия:

бүгін мен білдім...

қызықты болды...

қиын болды...

мен түсіндім...

енді мен істей аламын...

мен тырысамын...

мені таң қалдырды...

жиналыс маған берді...

Қорытынды жасап, ата-аналармен пікір алмасу.

**ҚАЗІРГІ ЗАМАНҒЫ ИНТЕРНЕТ-ТЕХНОЛОГИЯЛАР КЕҢІСТІГІНДЕ
КӘМЕЛЕТКЕ ТОЛМАҒАНДАРДЫҢ ПСИХОЛОГИЯЛЫҚ ЗОРЛЫҚ-
ЗОМБЫЛЫҒЫНАН ҚОРҒАУ ЖӨНІНДЕГІ КЕШЕНДІ ЖҰМЫС
БАҒДАРЛАМАСЫ**

«Кәмелетке толмағандардың киберқауіпсіздігі мен кибергигиенасы»

№	Жұмыс бағыты	Жоспарланған шаралар	
		Шаралар атауы	Жұмыс мазмұны
I	Кәмелетке толмағандармен жұмыс		
1	Психологиялық қызмет бойынша мектеп базасында кәмелетке толмағандармен, оның ішінде каникул уақытында психологиялық - ағартушылық жұмыстарды ұйымдастыру.	Ағартушылық әңгіме	Әлеуметтік медиа: мифтер мен шындық. Мен сөйлесе аламын ба? Байланыс нақты және виртуалды. Қауіпсіз интернет ортасы. Мен және менің отбасым. Отбасылық құндылықтар. Жанжалдарды сындарлы шешу. Мен және менің әлемім. Мен ойнайтын ойындар. Ойындар нақты және виртуалды.
		Пікірталас	«Жоқ» деп қалай айту керек және достарыңызды жоғалтпау керек?

2.	Психологиялық қызмет бойынша мектеп базасында кәмелетке толмағандармен және кәмелетке толмағандарда агрессивті және құрбандық мінез-құлқын қалыптастыруға ықпал ететін себептер мен жағдайлардың туындауының алдын алу бойынша профилактика субъектілерінің топтық және жеке жұмысын ұйымдастыру.	Қарым-қатынасклубы	«Менің қарым-қатынасым әлемі»
		Кәмелетке толмағандарда моббинг пен буллингтен қорғау бойынша күресудіңкопинг - стратегияларын қалыптастыру тренингі.	«Мен қалаймын, білемін, аламын!» «Мен, сен, ол – тату отбасы»
		Жасөспірімдер арасындағы агрессивті мінез- құлықтың алдын-алу бойынша психологиялық тренинг.	«Викторина»
3.	Психологиялық қызмет бойынша мектеп базасында құқықтық және ІТ бағыттағы мамандарды тарта отырып, кәмелетке толмағандарды хабардар ету бойынша жұмысты ұйымдастыру.	Шағын дәріс Презентация Сұхбат	«Сіздің денсаулығыңыз бен дамуыңызға зиян келтіретін ақпарат». «Кәмелетке толмағандарды қорғау туралы заң». «Сіздің қауіпсіз интернет кеңістігіңіз»
II	Ата-аналармен жұмыс		

1.	Кәмелетке толмағандарға қатысты зорлық - зомбылықтың алдын алу мәселелерінде, оның ішінде Интернет-ресурстарды пайдалана отырып, Психологиялық қызмет бойынша мектеп базасында Ата-аналармен психологиялық-ағартушылық жұмыстарды ұйымдастыру.	Ағартушылық сұқбат	Әлеуметтік желілер: аңыздар мен шындық. Бала-ата-ана қарым-қатынасының мәселелері. Жасөспірімнің қарым-қатынасынақты және виртуалды. Қауіпсіз интернет ортасы. Отбасылық құндылықтар. Балалармен қақтығыстарды сындарлы шешу жолдары.
		Шағын дәріс	Кәмелетке толмағандардың компьютерлік және виртуалды тәуелділігі: себептері, қалыптасу шарттары және анықтау әдістері. Кәмелетке толмағандарда құрбандық мінез-құлқының қалыптасуының психологиялық себептері. Кәмелетке толмағандардың агрессивті мінез-құлқының қалыптасуының психологиялық себептері. Жасөспірімдер ортасындағы Моббинг және қорқыту әлеуметтік-психологиялық құбылыс ретінде.
2.	Психологиялық қызмет бойынша мектеп базасында Ата-аналармен және ата-ана мен бала арасындағы қарым-қатынас мәселелерінде ата-ана құзыреттілігін арттыру және отбасы ішіндегі жанжалдардың алдын алу мақсатында алдын алу субъектілерімен	Ата-аналар лекторийі Ата-аналарға арналған қарым-қатынас клубы Ата-аналарға арналған пікірталас	«Баланы интернет кеңістігінде зорлық-зомбылықтан қалай қорғауға болады» «Біз біргеміз» «Табысты ата-ана»

	топтық және жеке жұмысты ұйымдастыру.		
3.	Кәмелетке толмағандардың дербес деректерін, оның ішінде зиян келтіретін ақпараттан қорғау мәселелерінде құзыреттілікті арттыру мақсатында психологиялық қызмет бойынша мектеп базасында және профилактика субъектілерінде құқықтық және IT бағыттағы мамандарды тарта отырып, ата-аналарды ақпараттандыру жөніндегі жұмысты ұйымдастыру.	Шағын дәріс Презентация Сұқбат	«Баланың денсаулығы мен дамуына зиян келтіретін ақпарат». «Баланы кибершабуылдан қалай қорғауға болады». «Қазақстан Республикасының балаларды дәстүрлі отбасылық құндылықтарды теріске шығаруды насихаттайтын ақпараттан қорғау жөніндегі кейбір заңнамалық актілері». «Баланы дамыту, қарым-қатынас жасау және оқыту үшін қауіпсіз интернет құру»
III	Алдын алу субъектілерінің мамандарымен жұмыс		
1.	Интернет - кеңістікті пайдалана отырып, кәмелетке толмағандарға қатысты зорлық - зомбылықтың алдын алу, профилактика субъектілерінің базаларында мамандармен психологиялық-ағартушылық жұмыстарды ұйымдастыру.	Сұқбат Шағын дәріс	«Баланы кибершабуылдан қалай қорғауға болады». «Баланы мектептегі қудалау: себептері, шарттары, анықтау әдістері» Кәмелетке толмағандарда құрбандық мінез-құлқының қалыптасуының психологиялық себептері. Кәмелетке толмағандардың агрессивті мінез-құлқының қалыптасуының психологиялық себептері. «Мұғалімдердің кибербуллинг: себептері мен қорғау тәсілдері». Жасөспірімдер ортасындағы Моббинг және қорқыту

			әлеуметтік-психологиялық құбылыс ретінде. «Кибербуллинг феномені және оның әлеуметтік алдын алу» Кәмелетке толмағандарда Интернетке тәуелділікті анықтайтын психологиялық маркерлер. Кәмелетке толмағандардағы құрбандық мінез-құлқын анықтайтын психологиялық маркерлер. Кәмелетке толмағандардың мінез-құлқындағы моббинг және буллинг белгілерін анықтаудың психологиялық маркерлері.
2.	Интернет-кеңістікте зорлық-зомбылықтың алдын алу бойынша кәмелетке толмағандармен және ата-аналармен жұмысты ұйымдастыру және оның мазмұны мәселелерінде кәсіби құзыреттілікті қалыптастыру бойынша профилактика субъектілерінің мамандарын әдістемелік сүйемелдеу.	Шеберлік сыныбы Кәсіби шеберлік тренингі Тәжірибеге бағытталған семинарлар Дөңгелек үстел Қосымша кәсіптік білім беру бағдарламалары	«Кәмелетке толмағандар арасындағы кибербуллинг пен кибербуллингтің алдын алу бойынша әлеуметтік жарнаманы әзірлеу технологиялары». «Құрдастарымен, оның ішінде интернет-кеңістікте тиімді қарым-қатынас жасау бойынша кәмелетке толмағандармен мотивациялық жұмыстың психологиялық-педагогикалық технологиялары». «Кәмелетке толмағандармен тиімді қарым-қатынас» «Кәмелетке толмағандар арасындағы жанжалды жағдайларды шешудің тиімді психологиялық-педагогикалық тәсілдері». «Оқушылар ұжымындағы Кибермоббинг және кибербуллинг: кәмелетке толмағандарды заманауи коммуникациялық технологиялар кеңістігіндегі құрдастарының агрессиясынан

			қорғау тәсілдері». «Кәмелетке толмағандар арасындағы психологиялық қысымды тану технологиялары». «Кибербуллинг: кәмелетке Толмағандарды интернет-кеңістікте қудалаудан қорғау мәселелері». «Кәмелетке толмағандар арасында кибербуллинг пен кибербуллингтің алдын алу бойынша әлеуметтік-педагогикалық қолдау және психологиялық-педагогикалық технологиялар».

Волонтерлерді, қоғамдық ұйымдарды, бала құқықтарын қорғау органдарын, алдын алу субъектілерін тарту.

Күтілетін нәтижелер:

Бағдарлама 7 жастан 18 жасқа дейінгі кәмелетке толмағандарды, олардың ата-аналарын, балалармен жұмыс істейтін мұғалімдер мен мамандарды интернет-кеңістікте кәмелетке толмағандар арасындағы психологиялық қысым жағдайларын тану және жою әдістеріне оқытуға бағытталған.

Бағдарлама 7 жастан 18 жасқа дейінгі кәмелетке толмағандарды, олардың ата-аналарын, балалармен жұмыс істейтін мұғалімдер мен мамандарды интернет-кеңістікте кәмелетке толмағандар арасындағы психологиялық қысым жағдайларын тану және жою әдістеріне оқытуға бағытталған.

Кибермоббинг пен кибербуллингтің алдын алу мақсатында кәмелетке толмағандарда агрессиялық және құрбандық мінез-құлқын қалыптастыруға ықпал ететін себептер мен жағдайлардың туындауының алдын алу бойынша кәмелетке толмағандармен топтық және жеке жұмысты ұйымдастыру көзделген.

Кәмелетке толмағандардың қарым-қатынас клубтарына, тренинг бағдарламаларына қатысуы: моббинг пен буллингтен қорғау бойынша коппинг-стратегияларды қалыптастыру, жасөспірімдер арасында агрессиялық мінез-құлықтың алдын алу, жасөспірімдер арасында құрбандық мінез-құлықтың алдын алу, кәмелетке толмағандарда моббинг пен буллингтен қорғаудың тиімді дағдыларын қалыптастыруға мүмкіндік береді, құрдастарымен жанжалсыз тұлғааралық өзара іс-қимылды үйретеді, қатысушылардың агрессиялық мінез-құлқын түзетуге мүмкіндік береді.

Интернет-кеңістікте зорлық-зомбылықтың алдын алу бойынша кәмелетке толмағандармен және ата-аналармен жұмысты ұйымдастыру және оның мазмұны мәселелерінде кәсіби құзыреттілікті қалыптастыру бойынша профилактика субъектілерінің мамандарын әдістемелік сүйемелдеу жеке блок болып табылады. Кәсіби шеберлік тренингтерінің бағдарламаларынан, практикаға бағытталған семинарлардан, шеберлік сыныптарынан өту, дөңгелек үстелдерге қатысу мамандарды агрессияның себептері мен салдарларымен, «моббинг» және «буллинг» ұғымдарының айырмашылықтарымен және оларды қалыптастырудың негізгі фазаларымен таныстыруға мүмкіндік береді.

Сондай-ақ, қатысушыларға кәмелетке толмағандар арасында әлеуетті мобберлер мен буллерлерді, сондай-ақ олардың құрбандарын ерте анықтаудың әлеуметтік-психологиялық технологияларын зерделеу мүмкіндігі беріледі.

Бағдарламаға қатысу кәмелетке толмағандармен жұмыс істейтін мамандарға бингке қарсы және буллингке қарсы бағдарламаларды енгізу тәжірибесімен танысуға көмектеседі. Қазіргі заманғы коммуникациялық технологиялар кеңістігінде зорлық-зомбылықтан қорғау және құқықтық және IT бағыттағы мамандарды тарта отырып, баланың құқықтарын қамтамасыз ету мәселелерінде кәмелетке толмағандар мен олардың ата-аналарын хабардар ету жөніндегі жұмысты ұйымдастыру маңызды сәт болып табылады.

КӘМЕЛЕТКЕ ТОЛМАҒАНДАРМЕН ПРОФИЛАКТИКАЛЫҚ ЖҰМЫС ЖӨНІНДЕГІ ӘДІСТЕМЕЛІК ҰСЫНЫМДАР

Психологиялық қызмет бойынша мектеп базасында кәмелетке толмағандармен психологиялық- ағартушылық жұмыстарды ұйымдастыру

Психологиялық білім беру қызмет түрі ретінде кәмелетке толмағандарды оқыту кезеңінде де, мектеп демалысы кезінде де жүзеге асырылуы мүмкін. Кәмелетке толмағандарға психологиялық білім беруді психологиялық қызмет бойынша мектеп базасында, сондай-ақ білім беру мекемелерінің, кітапханалардың базасында және тұрғылықты жері бойынша шағын аудандар мен оқушылар бөлмелері кеңестерінің базасында жүргізеді.

Кәмелетке толмағандарға психологиялық білім берудің ең өзекті тақырыбы:

- «Кәмелетке толмағандардың кибербуллинг және киберббингі: ескерту себептері мен мүмкіндіктері»;
- «Кәмелетке толмағандардың әлеуметтік-психологиялық бейімсіздігі: себептері мен жеңу жолдары»;
- «Кәмелетке толмағандар арасындағы агрессивті мінез-құлық»;
- «Жанжал: туу себептері және шешу жолдары»;
- «Есірткі туралы аңыздар» және т.б.

Психологиялық ағарту негізінен психологтың кәмелетке толмағандармен сөйлесуі түрінде құрылады және өзара әрекеттесудің интерактивті әдісін ұсынады.

Кәмелетке толмағандар алдында сөйлеуге дайындық кезінде психолог білім алушыларға тек психологиялық теорияны ғана емес, тұлғааралық қатынастарды оңтайландыру және жақсарту үшін нақты психологиялық әсерді қамтамасыз ету маңызды екенін есте ұстауы керек.

Психологиялық ағартудың тиімділігі психологтың құзыреттілігі мен кәсібилігіне байланысты, ол кәмелетке толмағандарға психологиялық шындықтарды олар үшін түсінікті қарапайым, қол жетімді тілде жеткізе білуі керек. Психолог үшін кәсіби немесе жеке тәжірибеге негізделген иллюстрациялық мысалдар келтіре білу маңызды.

Кәмелетке толмағандарға психологиялық білім берудің тиімділігін арттыру психологтың жұмыстың белсенді түрлерін қолдануына ықпал етеді, мысалы: әңгіме, пікірталас, пікірталас, ұжымдық шығармашылық іс, коллаж, психологиялық қонақ бөлме, психологиялық ток-шоу, психологиялық аукцион, мастер-класс, психологиялық тірі журнал және т. б.

1. Пікір-талас психолог пен кәмелетке толмағандардың әртүрлі сипаттағы мәселелерді тең дәрежеде талқылауы. Бұл қатысушылардың алдында әркімнің өз жауабы бар сұрақ қоюды қамтиды. Пікірталас барысында қатысушылар қойылған сұраққа бәрін қанағаттандыратын жаңа жауап тұжырымдайды. Талқылаудың нәтижесі жалпы келісім, мәселені жақсы түсіну, көру, бірлескен шешім қабылдау болуы мүмкін.

Пікір-таласты өткізудің ұйымдастырушылық және мазмұндық шарттары мыналарды қамтиды:

а) талқылауға шығарылатын мәселе ішкі қарама-қайшылықты қамтуы керек және талқылау тақырыбына бірнеше көзқарасы болуы керек;

б) қатысушылар пікір-таласқа басқа дәлелдерді есту және түсіну, басқа көзқарастарды қолдау және оларды жеткізу ғана емес;

в) пікір-талас барысында психолог пен қатысушылардың әңгіме тақырыбын түсінуі дамуы тиіс;

г) мәселені талқылау кезінде дәлелдеу негізделген және дәлелді болуы керек;

Пікір-талас кезінде психологқа оның қатысушыларымен қарым-қатынастың келесі шарттары мен принциптерін сақтау маңызды:

- барлық пікір-таласқа қатысушылардың ұстанымдары туралы нақты түсінік беру;

- дұрыс және құрметпен қарым-қатынас ережелерін ескере отырып, пікірталасты жүргізудің рұқсат етілген әдістерін ғана пайдалану;

- әрбір қатысушының өз пікірін білдіру кезінде ашықтық қағидатын іске асыруды және оны қабылдауды қамтамасыз ету;

- пікір-таласқа қатысушылардың әрқайсысының сөйлеу үшін тең құқықтары мен мүмкіндіктері бар, ал барлық қатысушылардың пікірлері маңызды болған кезде теңдік қағидатын сақтау;

- біреудің пікірін құрметтеу және қатысушының сілтеме жасаған беделін емес, мәлімдеменің мәнін қабылдау;

- сөз бостандығы қағидатын сақтау, бұл кез-келген қатысушының пікірін өзгерту және басқалардың пікірлерімен ортақ тіл табысу мүмкіндігін, сондай-ақ пікірталастың кез-келген қатысушысына түсініктеме алу еркіндігін білдіреді.

Пікір-таластарды ұйымдастырудың тәсілдері әртүрлі: жұптасқан пікірталастар, топтық және жеке, онда әр қатысушы өз көзқарасын қорғайды.

Пікір-талас аяқталуы мүмкін: топтардың бірін жеңу; жалпы көзқарасты қабылдау; әркім өз пікірімен қалады.

2. Пікір-сайыс – бұл пікірталастың бір түрі және ұжымдық талқылау мен дау-дамайды қамтиды. Пікір-таластың пікір-сайыстан айырмашылығы, өмірдің қажеттілігіне қарай өздігінен пайда болуы мүмкін. Пікір-сайыс әрқашан оның қатысушылары анықтаған белгілі бір тақырып бойынша өткізілетін арнайы ұйымдастырылған іс-шара болып табылады.

Пікір-сайысты өткізудің маңызды шарттары – қатысушылардың өздері таңдаған тақырыптың тартымдылығы, өзектілігі, мәселелігі және пікір-таластығы болып табылады. Саяси, құқықтық, адамгершілік, этикалық және эстетикалық тақырыптарда пікірсайыстар өткізіледі.

Тақырыпты анықтағаннан кейін пікірталасты ұйымдастырудың екі әдісі мүмкін: алдын-ала ұйымдастырушылар мен психолог тобы дайындаған жоспарланған пікірталас және дау-дамай.

Бірінші тәсілі, пікір-талас ұйымдастыру үлкен мәнге ие, оны дайындау, ол мынадай элементтерді қамтиды:

1. Пікір-сайыс барысын әзірлеу, тақырыпты нақтылауға және оны сөзбе-сөз қайталамай дәйекті түрде ашуға мүмкіндік беретін (3-5) сұрақтар құрастыру;

2. Қатысушыларды сөйлесуге және талқылауға ынталандыру үшін оларды қалай дайындау керектігін ойластыру;

3. Пікір-сайысты ыңғайлы өткізу үшін аудиторияны дайындау;

4. Қаралатын мәселеге жалпы көзқарас әзірлей отырып, әрбір мәселені талқылау нәтижелері бойынша қорытынды шығару;

5. Қорытындылау кезінде – әңгіме басында және соңында болған нәрсе жақсы есте қалатын) «шектік ережелерді» ескеру.

Пікір-сайыс құрылымы келесідей көрінуі мүмкін:

- кіріспе бөлім – «байланыс орнату»;
- әртүрлі көзқарастарды айту және талқылау;
- дұрыс емес көзқарастарды нақтылау, олардың қателігін дәлелдеу;
- дұрыс позицияларды анықтау, олардың негізделген дәлелдері;
- тұжырымдарды құрылымдау, аудиторияның жалпы ұстанымы мен бірауыздылық дәрежесін анықтау.

Қатысушылар тақырыпты анықтағаннан кейін бірден мәселені талқылауға дайын болған кезде, олар белгілі бір өмірлік тәжірибеге ие, бұл сізге осы мәселе бойынша сөйлесуге мүмкіндік береді, қажетті ақпаратқа ие болады, сонымен қатар жүргізуші импровизация және даулы мәселелер бойынша әңгіме жүргізу құзыреттеріне ие болған жағдайда пікірсайысты жүргізгені жөн.

4. ҰШЖ (ұжымдық шығармашылық жұмыс) істі жүргізу туралы шешімді бірлесіп қабылдау, оны ұжымдық жоспарлау, бірлесіп дайындау, іске асыру және нәтижені талдау болып табылады.

Ұжымдық шығармашылық қызметті ұйымдастыру: бәсекелестік, ойын және импровизация қағидаларын жүзеге асыруға негізделген.

Ұжымдық шығармашылық істі дайындау және жүргізу мыналарды қамтиды:

- қатысушылар идеяларды «лақтыратын» ми шабуылы. Бұл кезеңнің басты шарты – барлық идеялар ерекше түрде қабылданады;
- шешім қабылдау әр идеяны ең жақсысын тандаумен өлшеуді қамтиды, оның барысында айтылған көзқарастарды талқылау кезінде әдептілік пен ізгілікті сақтау маңызды;
- міндеттерді бөлу тапсырманы орындау үшін жауапкершілікті қабылдауға дайын нақты орындаушыларды анықтауды қамтиды;
- қабылданған идеяны жүзеге асыру, оны жүзеге асырудың сәттілігі барлық қатысушылармен ынтымақтастық жасау және қажетті әрекеттерді нақты орындау қабілетіне байланысты;

- нәтижені талдау жұмысты аяқтайды және нәтижені бағалауды қамтиды, оның негізгі шарты қатысушылардың өз жұмысын сыни бағалау мүмкіндігі болып табылады.

4. Коллаж – бұл ескі журналдардан, символдардан, цитаталардан алынған суреттерді қолдана отырып, қағаз парақтарында берілген құбылыстың бейнесі жасалатын технология. Топтық жұмыста «тірі коллаж» модификациясы жиі қолданылады, онда берілген құбылыстың бейнесі пантомима, әдеби, музыкалық үзінділер, плакаттар, рөлдік көріністер және т.б. көмегімен жасалады.

5. Психологиялық қонақ бөлме – бейресми тақырыптық қарым-қатынасты ұйымдастыру (ерекше интерьер құру, кездесу рәсімін енгізу, «ерекше» қонақтарды шақыру және оларды таныстыру, қарым-қатынасты ұйымдастыру және т.б.).

6. Психологиялық ток-шоу – пікірталасты өткізу мен ұйымдастырудың ерекше түрі, ол: тақырыптық сценарийдің болуын; талқыланатын мәселе бойынша ерекше пікірі бар қонақтарды шақыруды; иллюстрация ретінде проблемалық жағдайларды ойнатуды, бейнесабактарды, фильмдерден кадрларды пайдалануды; «залға» арналған тапсырмаларды қосуды және т.б.) көздейді.

7. Психологиялық аукцион өз идеяларын, таланттарын, өмір салтын және т.б. «сақтау» (қорғау) бойынша жұмысты ұйымдастыру, ол ерекше интерьер, өткізу сценарийін, атрибуттарды және т.б. құруды көздейді.

8. Шеберлік сыныбы – қатысушылардың «шеберлікке» кез-келген салада қандай да бір дағдыларды меңгеруін көрсету және оларды меңгергісі келетіндерді ерекше салтанатты жағдайда, «шебердің» жарқын эмоционалды презентациясымен және іс-шараның алдын-ала жарнамасымен өткізуді үйрету.

9. Жұмыс істеп тұрған психологиялық журнал кез-келген өзекті мәселені (тақырыпты) «журнал» айдарларының көмегімен әртүрлі тұрғыдан қарастыруды қамтиды: репортаж, жаңалықтар, эзілдер, дөңгелек үстел, онда материал қатысушылар презентация, хабарлама, драматизация және т.б. түрінде ұсынады.

Белсенді жұмыс түрлерін қолдана отырып, кәмелетке толмағандарға психологиялық білім беруді дайындау жұмыстың мақсатты бағыттарын анықтай отырып, проблемалық-бағытталған тақырыптарды тұжырымдай отырып, қажет болған жағдайда жұмыс мазмұнының сценарийлерін жасай отырып, психологиялық – ағартушылық жұмыс бағдарламаларын әзірлеуді қамтиды.

КӘМЕЛЕТКЕ ТОЛМАҒАНДАРМЕН ПСИХОЛОГИЯЛЫҚ- АҒАРТУШЫЛЫҚ ЖҰМЫС БАҒДАРЛАМАСЫ

Мақсаты – білім алушылардың психологиялық сауаттылығын арттыру, балалардың құрдастарымен және ата-аналармен қарым-қатынасындағы психологиялық мәселелердің алдын алу.

Білім алушыларға арналған әңгіме тақырыптары:

1. Көшбасшылық
2. Топтағы билік мәселесі
3. Әлеуметтік рөлдер
4. Психология тұрғысынан алкоголь мен нашақорлыққа салыну
5. Құрдастарымен, ата-аналармен және мұғалімдермен қарым-қатынас
6. Агрессия мәселесі
7. Білім алушыларды қарым-қатынас тәсілдеріне үйрету
8. Кәсіби өзін-өзі анықтау мәселелері
9. Тұлғалық, даралық қасиеттер
10. Әлеуметтік желі: аңыздар мен шындық
11. Менің басқалармен сөйлесе алу шеберлігім
12. Шынайы және виртуалды қарым-қатынас
13. Қауіпсіз интернет ортасы
14. Мен және менің отбасым
15. Отбасылық құндылықтар
16. Қақтығыстарды сындарлы шешу
17. Мен және менің әлемім
18. Мен ойнайтын ойындар
19. Шынайы және виртуалды ойындар
20. Киберқауіпсіздік
21. Кибермәдениет пен кибергигиена.

Кәмелетке толмағандарда агрессиялық және құрбандық мінез-құлқын қалыптастыруға ықпал ететін себептер мен жағдайлардың туындауының алдын алу бойынша профилактика субъектілерінің топтық және жеке жұмысын ұйымдастыру

Жастар – қоғам дамуының маңызды ресурсы, ал жастар мен жасөспірімдер қылмысы – агрессияның, қатыгездіктің көрінісі және кәмелетке толмағандар арасында жалпы қылмыстың қалыптасуы үшін өнімдік орта.

Жасөспірімдер арасындағы топтық қылмыстың алдын алудың, оның ішінде кәмелетке толмағандарда агрессивті және құрбандық мінез-құлқының қалыптасуының тиімділігін қамтамасыз ету мемлекеттік билік пен басқару құрылымының барлық деңгейлерінде психологтардың, мұғалімдердің, балалармен жұмыс істейтін мамандардың, медицина қызметкерлерінің және ата-аналардың жастар мәселелерін жан-жақты шешуді қамтиды: федералды, аймақтық, қалалық, аудандық.

Кәмелетке толмағандарда агрессивті және құрбандық мінез-құлқының қалыптасуының алдын-алу, себептер мен жағдайларды талдау көрсеткендей, жасөспірімдер мен балалардың бос уақытын ұйымдастырумен байланысты мәселелерді түбегейлі шешпей тиімді бола алмайды. Осыған байланысты, психологиялық қызмет бойынша мектеп базасында алдын-алу субъектілері негізінде қызығушылық клубтарын, қарым-қатынас топтарын, шығармашылық үйірмелерді дамыту жұмыстары қайта жанданды, онда кәмелетке толмағандардың шығармашылыққа деген табиғи қызығушылығы оң бағытқа ие болады. Кәмелетке толмағандармен топтық жұмыс бағдарламалары жасалады, олар құрдастарымен тұлғааралық қатынастарда агрессияның көріністерін, сондай-ақ құрбандық мінез-құлқында көрінетін аутоагрессияны жан-жақты ақпараттандыруға және алдын алуға бағытталған.

Құрбандық мінез – құлқы немесе құрбандық агрессияның көріністерінің бірі болып табылады. Виктимизация – бұл басқа адамдардың агрессиясын кездейсоқ тудыратын адамның мінез-құлқының ерекшелігі. Бұл термин латынның «*victima*» — құрбандық деген сөзінен шыққан.

Әлеуметтік психология тұрғысынан зардап шеккен мінез-құлық – бұл келесі факторларға негізделген ауытқу:

- бейімділік;
- сыртқы жағдайлар;
- қоғамның әсері.

Жасөспірімдер виктимизация кешеніне өте сезімтал. Ересек адам көбінесе теріс жағдайлардың, құбылыстардың, адамдардың құрбанына айналады.

Жәбірленушінің психологиясы өзін көрсететін жағдайларда, жәбірленуші мінез-құлық қылмысқа әсер етпеуі мүмкін, бірақ шешуші рөл атқара алатын заңды және заңсыз әрекеттерде көрінеді. Жәбірленуші түрі әртүрлі жолдармен көрінеді: эмоционалдық тұрақсыздықпен, мойынсұнушылықпен, қарым-қатынастағы қиындықтармен, өз сезімдерін бұрмаланған қабылдаумен және т.б. егер адамдар өмірге қауіпті сәттерде дұрыс емес әрекет етуге бейім болса, олар, ең алдымен, өзгерістерге ұшырайды. Жеке қарым-қатынас сипаттың келесі қасиеттерін анықтайды:

- бағыныштылық;
- сендіру, сену;
- абайсыздық және жеңіл ойлы;
- өз өзін қорғай алмау.

Жасөспірімдерді шынайы өмірде өз құрдастарымен қудалау мен қорлаудың қазіргі жағдайында олар виртуалды әлемге жасөспірімді ұрып-соғу және қорлау көріністері бар YouTube бейнелерін жариялау, әлеуметтік желілерде пікір беретін фотосуреттерді, жеке ақпаратты және т.б. жариялау арқылы жіберіледі.

Кибербуллинг деп аталатын қорлаудың жаңа түрлері балаларда, ата-аналарда және мамандарда үлкен алаңдаушылық тудырады.

Психологиялық қызмет жұмысының ерекшелігі қазіргі заманғы интернет

- технологиялар кеңістігінде кәмелетке толмағандар арасында кибербуллинг пен киберббингтің туындауының алдын алу бойынша профилактикалық жұмыс шеңберінде мамандардың балалармен ведомствоаралық өзара іс-қимылын ұйымдастыруға және тиімді іске асыруға мүмкіндік береді. Орталық интернет- технологиялар ортасында кәмелетке толмағандардың зорлық-зомбылығының алдын алу бойынша психологиялық-педагогикалық қызметке балалармен жұмыс істейтін педагогтар мен мамандарды даярлауды қамтамасыз етуге арналған ресурстарға ие. Орталық мамандары кибербуллингке немесе киберббингке ұшыраған ата-аналармен және кәмелетке толмағандармен алдын алу жұмыстары үшін құзыреттерге ие.

Осыған байланысты психологиялық қызмет бойынша мамандар ең өзекті мәселелер бойынша профилактикалық қызметті жүзеге асыруға мүмкіндік беретін топтық жұмыс бағдарламаларын әзірлейді:

-қазіргі заманғы интернет-технологиялар кеңістігінде кәмелетке толмағандардың психологиялық зорлық-зомбылығынан қорғау жөніндегі кешенді жұмыс бағдарламасы «кәмелетке толмағандардың Кибермоббингі және кибербуллингі: араласу стратегиясы және алдын алу»;

- физикалық зорлық-зомбылықтан аман қалған балаларға арналған психокоррекциялық топтың бағдарламасы;

- 14-16 жас аралығындағы жасөспірімдер үшін өзін-өзі бағалауды арттыруға арналған тренинг бағдарламасы;

- ассертивтілік тренингі бағдарламасы;

- 10-12 және 13-15 жастағы кәмелетке толмағандарға арналған «Өзіңе сен» және тағы басқа ассертивтілікті дамытудың психологиялық тренингінің бағдарламалары.

КӘМЕЛЕТКЕ ТОЛМАҒАН БІЛІМ АЛУШЫЛАРМЕН АҚПАРАТТАНДЫРУ ЖҰМЫСЫН ҰЙЫМДАСТЫРУ

Кәмелетке толмағандар арасында қолданушылардың жоғары белсенділігі олардың Интернет кеңістігінің қауіптілігі мен олардан аулақ болу немесе оларды жеңу жолдары туралы білмеуінің төмендігімен үйлеседі, сондықтан кәмелетке толмағандарды тәрбиелеу мен алдын алу қажеттілігі айқын.

Көбінесе жасөспірімдер мен балалар интернет кеңістігін қауіпсіз дамытуда ата-аналардан немесе мұғалімдерден тиісті көмек ала алмайды, өйткені оларда да әлі де қажетті тәжірибе мен білім жоқ.

Бұл кәмелетке толмағандардың медиа құзыреттілік саласындағы және интернет-ресурстарды пайдаланушылардың құқықтық қорғалуы саласындағы білімдерін жетілдіру, бұл киберқорлық пен киберқорқынышпен күресте ең тиімді профилактика бола алады.

Демек, профилактикалық жұмыстың маңызды аспектісі, оның ішінде кибербуллингтің алдын алу, ведомствоаралық өзара іс -қимыл шеңберінде АТ мамандарын тарту болып табылады.

Мектеп базасында кәмелетке толмағандарды ақпараттандыру бойынша заңгерлік және IT мамандарын тарта отырып профилактикалық жұмыстар жүргізілуде «Психологиялық орталық» және әртүрлі формадағы алдын алу субъектілері:

- ақпараттық және тәрбиелік сұқбаттар;
- пікірталастар;
- презентациялар;
- интернет-ресурстармен жұмыс жасау бойынша шеберлік сыныптар;
- кәмелетке толмағандарға арналған ақпараттық буклеттер

мен жадынамалар әзірлеу және тарату және т.б.

Ата -аналармен профилактикалық жұмыс бойынша әдістемелік нұсқаулар

Кәмелетке толмағандарға қатысты зорлық-зомбылықтың алдын алу, оның ішінде интернет – ресурстарды пайдалану бойынша психологиялық қызмет және профилактика пәндері негізінде ата -аналармен психологиялық-ағартушылық жұмысты ұйымдастыру

Зорлық-зомбылықтан зардап шеккен кәмелетке толмағандарға көмектесуден басқа, оның ішінде интернет -ресурстарды қолдану арқылы балаларға қатыгездіктің алдын алуға, кемінде екі кезеңді қамтитын тиімді профилактикалық жүйені құруға үлкен мән беріледі.

«Психологиялық орталық» мемлекеттік бюджеттік білім беру мекемесінің мамандары жүргізетін алғашқы профилактика зорлық-зомбылыққа қатысы бар тараптарға қудалаушыға (агрессорға) және жәбірленушіге кешенді әсерден тұрады. Бұл әсер тұлғаның қалыпты және жан -жақты дамуы үшін жағдайларды

қамтамасыз етуге, қауіпсіз және жайлы микроорта құруға бағытталған шаралардың кең спектрін қамтиды: «тәуекел тобындағы» отбасыларға уақытында көмек көрсету, кәмелетке толмағандардың жақын ортасынан адамдар арасында алкоголизм мен нашақорлықтың алдын алу. Балаларға дұрыс жыныстық тәрбие беру, олардың гендерлік қатынастар туралы, әр түрлі жағдайларда, соның ішінде қазіргі заманғы ақпараттық интернет-технологиялар жағдайында кәмелетке толмағандардың мінез-құлқының әлеуметтік қолайлы және қауіпсіз түрлері туралы білімдерін қалыптастырудың маңызы зор.

Кәмелетке толмағандарға қатысты зорлық-зомбылықтың алғашқы алдын алу сатысында, соның ішінде мектептер мен басқа балалар мекемелерінде интернет-ресурстарды пайдалану кезінде психологиялық орталықтың мамандары балалардың өміріне қауіп төндіретін жағдайларда ересектерге арналған стратегияны әзірлеуге бағытталған ата-аналармен түсіндірме әңгімелер жүргізеді. Ата-аналық құзыреттілікке арналған тренингтер кәмелетке толмағандарда, оның ішінде Интернет ортасында қауіпсіз мінез-құлықты қалыптастыру дағдыларын дамыту үшін өткізіледі.

Басқалардың заңсыз әрекеттерінің алдын алуға көп көңіл бөлінеді, мысалы, ата-аналарға балаларды қоғамда ғана емес, сонымен бірге ақпараттық технологиялар кеңістігінде де қауіпсіз мінез-құлық ережелерін сақтауға үйретеді.

Сонымен бірге, білім беру, медициналық және басқа да білім беру мекемелеріндегі стендтерде психологиялық орталықтың мамандары зорлық-зомбылыққа ұшыраған кәмелетке толмағандарға көмек пен қолдау көрсететін адамдар мен ұйымдардың мекенжайлары мен байланыс телефондары туралы ақпаратты орналастырады. ақпараттық желілер немесе әлеуметтік қауіпті жағдайда.

Кәмелетке толмағандарды қарым-қатынас және өзара қолдау клубтарына, топтық жұмыстарға және бос уақыттарын толық өткізуге, қызығушылықтары мен қарым-қатынас дағдыларын дамытуға арналған басқа да бірлестіктерге тартуға көмектесу үшін түрлі шаралар өткізіледі. Мұның бәрі Интернетте, қоғамдық орындарда (дискотекалар, кафелер және т.б.), оқу орындарында және т.б. жерлерде жүргізіледі.

Екіншілік профилактика жасөспірімдерде пайда болған психикалық ауытқуларды теңестіру, суицидтік әрекеттерді және қайталама құрбандылықты болдырмау үшін ведомствоаралық өзара іс -қимыл шеңберінде зорлық-зомбылықтан зардап шеккен кәмелетке толмағандардың ата -аналарына медициналық, психологиялық және педагогикалық көмек көрсетуден тұрады. Соңғысы әсіресе жасөспірімдерде жиі байқалады, олардың арасында құрбандардың болуы туралы кең тараған миф бар, соның арқасында олардың қол сұғылмаушылығына бірнеше рет шабуыл жасалуы мүмкін.

Мұндай жағдайларда психологиялық қызмет мамандары, құқық қорғау органдарында және халыққа әлеуметтік қызмет көрсету орталықтарында көрсетілетін психологиялық көмек ата-аналар мен зардап шеккендердің өздеріне. Орталықта заңгерлерден басқа әр түрлі мамандар жұмыс істейді:

кәмелетке толмағандардың ата -аналарына жоғары білікті көмек көрсететін әлеуметтік жұмыс мамандары, педагог -психологтар, әдіскерлер және т.б.

1. Ата-аналар мен мамандардың психологиялық-педагогикалық біліміне арналған буклеттердің мазмұнын әдістемелік әзірлеу, мысалы, ата-аналарға арналған буклеттер, «Балалар және компьютер», «Кибергигиена», «Кибермәдениет», «Киберқауіпсіздік» т.б. тақырыптарда ақпараттар беру.

Біз компьютердің балаға зияны бар ма және интернеттің оның психикасына қалай әсер ететіні туралы қалағанымызша сөз таластыра аламыз. Бірақ бұл нақты дәлелді өзгертпейді: балалар бұрыннан интернетке үйреніп, компьютерді өзімізден жақсы түсінеді.

Біз қаласақ та, қаламасақ та, біздің балалар компьютерді қолданады, өйткені ең қызықты және сәнділердің бәрі бұрыннан теледидар экранынан интернетке көшірілген. Дәл осы жерде олар соңғы музыканы табады, ең сәнді фильмдерді жүктейді және бағдарламалық жасақтаманы жаңартады. Ең бастысы, қарым -қатынас дәл осы жерде – чаттар мен форумдарда, олар әлеуметтік желілерде танысады, достар мен пікірлестерді табады, ғашық болады және ең жақын адамдармен бөліседі – бұл қандай да бір себептермен ата-аналармен немесе достарымен талқыланбайды.

Бір жағынан, интернет жасөспірім үшін үлкен мүмкіндіктерге толы. Бірақ, екінші жағынан, интернет қауіпке толы: банальды плагиат пен виртуалды бұзушылардан чат пайдаланушыларын ренжіткен, бүркеншік аттың артына жасырынған, нағыз қылмыскерлер мен педофилдерге дейін. Сондықтан балаларға онлайн қауіпсіздігінің негізгі ережелерін түсіндіру, содан кейін олардың сақталуын мұқият бақылау өте маңызды.

1. Компьютерді көрнекті жерге қойыңыз. Егер монитор көз алдында болса, оқушының тыйым салынған сайттарға бару қаупі әлдеқайда төмен.

2. Келісім жасаңыз. Баланың компьютерде қанша уақыт өткізетінін, қандай сайттарға кіруге болатынын келісіңіз. Сіз барлық тармақтарды жазып, оларды бұзғаны үшін айыппұлды талап етіп қабырғаға іліп қоюыңызға болады.

3. Балаларды жеке ақпаратты бермеуге үйрету. Егер сіздің балаңыз чат бөлмелері мен форумдарды қолданатын болса, виртуалды достарға сіздің нақты атыңыз бен тегіңізді, мекен -жайыңызды немесе достарыңыздың атын айта алмайтыныңызды түсіндіріңіз.

4. Жеке кездесулерге тыйым салу. Балаға интернетте жеке кездеспеген адамдармен - мектепте, аулада, елде сөйлесуге тыйым салған дұрыс. Бірақ егер виртуалды таныстар пайда болса, сіз олармен ата -ананың рұқсатынсыз кездесе алмайсыз.

5. Балаңызбен сөйлесіңіз. Нағыз адамдар туралы айтқандай интернеттегі достарыңыз туралы және олардың не істейтіні туралы сұраңыз.

6. Хабарда болыңыз. Балалардың қандай сайттарды пайдаланатынын білу маңызды. Тәртіп сақтайтын модераторлары бар сайттарға артықшылық

беріледі. Көптеген чаттар мен форумдардың жеке сөйлесу мүмкіндігі бар. Баланың бейтаныс адамдармен оңаша сөйлеспеуін талап етіңіз.

7. Қатаң шарт қойыңыз. интернеттен бір нәрсені жүктеу үшін (музыка, кино немесе жаңа ойын) бала әр уақытта сіздің рұқсатыңызды алу керек.

8. Балаңызды сақтықпен бөлісуге үйретіңіз. Егер біреу интернетте баланы қорласа немесе қорқытса, міндетті түрде ата -анасына хабарлаңыз.

9. Жақсы сөйлесу ережелерін ұмытпаңыз. Балаңызбен интернетте сыпайы болу туралы сөйлесіңіз. Сіз форумдар мен чаттарда адамдарды қорлауға немесе мазақ ете алмайсыз.

10. Бірге ойнаңыз. Егер бала онлайн ойындарды қолданатын болса, онда оны қорғаудың ең сенімді әдісі – әсіресе ата-анасымен ойнау.

11. Фотосуреттерге мұқият назар аударыңыз. Балаңызға фотосуреттер адам туралы ақпарат бере алатынын түсіндіріңіз. Сіз фотосуреттерді Интернетте оңай танылатын бөлшектермен орналастыра алмайсыз – үй нөмірлері, көше атаулары, көлік нөмірлері, мектеп атаулары.

12. Интернеттегі ақпарат барлығына қолжетімді екенін балаңызға көрсетіңіз. Оның өз блогында немесе әлеуметтік желідегі парақшасында жариялайтынын сыныптастары, мұғалімдері, достарының ата -аналары оқи алады, сондықтан авторға зиян келтіретін ештеңе жазудан сақ болу керек.

13. Іріктеуге үйретіңіз. Қажет емес материалдарды блоктауға мүмкіндік беретін көптеген бағдарламалар бар. Ең жақсы нұсқаны анықтау үшін интернет-провайдеріңіздің өкілімен сөйлесіңіз.

14. Ережелердің орындалуын бақылау. Егер сіздің балаңыз тәжірибелі қолданушы болса да, ол сіздің келісімшарт ережелерін сақтайтынын үнемі тексеріп отырыңыз.

2. Ата-ананы не толғандыруы мүмкін?

Баланың компьютерлік ойындар ойнауды немесе интернетте сөйлесуді ұнатпайтынын, бірақ оған тәуелді екенін қалай анықтауға болады? Әкелер мен аналарға төмендегілерді ескерту қажет:

- Отбасымен және достарымен қарым -қатынастың бұзылуы. Бала аулада серуендеуді тоқтатады, сыныптастарын үйге шақырмайды. Ол енді сізге өз кәсібі туралы айтқысы келмейді. Сіздің ұлыңыз немесе қызыңыз киноға бару немесе коньки тебу туралы ұсыныстарыңызды қабылдамайды. Бос уақыттың барлығын қазір компьютер тұтынады.

- Барлық басқа әрекеттерге қызығушылықтың жоғалуы. Бұрын бала жақсы оқитын. Енді үй тапсырмасын орындамайды. Мәжбүрлеу мүмкін емес, ал нашар бағалар оған тиіспейді. Жақында бала әкеге немесе шешеге бірінші көмекші болды. Бүгін сіз мені аздап көмектесуге көндіре алмайсыз. Егер бала кез келген секцияға барса, ол жұмыстан шығады.

- Бала алдай бастайды. Ол ата -анасына оның сабақ оқығанына, серуендеуге шыққанына сендіреді, бірақ ол күні бойы компьютерде отырды. Жамандыққа жол бермеу үшін мектептегі нашар бағаларды жасырады.

- Тамақ ішу тәртібі бұзылады. Баланың тәбеті нашарлайды. Үйде, ата-ана бақылауынсыз, компьютерлік техник тамақтануды ұмытады. Ал егер ол тамақ жесе, онда компьютерде отырады және өте зиянды нәрсе (чиптер, крекер, шоколад барлары).

- Ұйқының бұзылуы пайда болады. Баланы жанжалсыз компьютерден жұлып алып, төсекке жатқызу мүмкін емес. Оның ұйықтап кетуі қиын, ұйқысы тынышсыз, қорқынышты түстер көреді.

- Психикалық шаршау. Баланың басы жиі ауырады, тез шаршайды. Есте сақтау мен зейін нашарлайды. Оның жүйкесі тозған, тез мазасызданады.

Әдетте, ата-аналар барлық көріністер олардың алдында барлық даңқында пайда болған кезде ғана әрекет ете бастайды. Ең жиі кездесетін реакция – баланың ойнауына тыйым салу, үйдегі компьютерден алшақ ұстау. Бұл проблемалардан қалай аулақ бола аласыз? Кеңес біреу: балаларыңызбен жақын болыңыз, оларды не толғандырады және не мазалайтынын біліңіз. Балаңыздың виртуалды әлемге қашпай, шынайы өмірдегі мәселелерді шешуіне көмектесіңіз.

3. *Ата -ана кітабы Виктимизм – жәбірленушінің психологиясы*

Кейбір адамдардың жеке қасиеттері, әсіресе олардың зиянына бағытталған болса, таң қалдырады. Бұл мінез -құлық ерекшеліктеріне виктимизация кіреді – қылмыс пен жазатайым оқиғалардың құрбаны болуға бейім адамның қасиеттерінің жиынтығы. Ұғым психология мен криминалистикада қарастырылады.

Жәбірленуші – байқаусызда басқа адамдардан агрессияға ұшыраған адамның мінез-құлқының ерекшелігі. Бұл термин латынның «victima» – құрбан деген сөзінен шыққан.

Жәбірленуші феномені құқықтық және әлеуметтік психологияның тоғысында тұр. Соңғысының көзқарасы бойынша, жәбірленушінің мінез-құлқы келесі факторларға негізделген ауытқу болып табылады:

- бейімділік;
- сыртқы жағдайлар;
- қоғамның әсері.

Жасөспірімдер виктимизация кешеніне ең сезімтал. Ересектерге қарағанда жетілмеген тұлға көбінесе жағымсыз жағдайлардың, құбылыстардың, адамдардың құрбаны болады. Оған зиян келтіруге басқа адам ғана міндетті емес, ол жабайы жануар, элемент, қарулы қақтығыс себеп болуы мүмкін. Бұл мәселе қазіргі психологиядағы ең өзекті мәселелердің бірі.

Жәбірленудің себептері – адам интуитивті түрде әлеуетті жаудың алдында өзінің әлсіз жақтарын көрсетпеуге, қақтығыстар мен қауіпті жағдайларды болдырмауға тырысады. Егер бұл болмаса – құрбандықтың виктимдік мінез-құлқы көрінеді.

Адам өзіне қиындық туғызу нәтижесінде нақты не істейді?

Өзіне күш қолдануға итермелейтін адамдардың үш түрін бөліп көрсетуге болады:

1. Пассивті бағынышты. Яғни, жәбірленуші шабуылдаушының талаптарын орындайды, бірақ ол баяу жасайды немесе сөздер мен бұйрықтарды қате түсінеді. Мұндай адамдар сипатталған синдромы бар адамдардың жалпы санының ішінде ең көп (40%).

2. Жалған провокациялық. Потенциалды жәбірленуші білместен қиырлықпен, шынын айтқанда және т.б. қарсыласты агрессияға итермелеу үшін бәрін жасайды:

3. Тұрақсыз тип. Мінез-құлықтың екі түрінің ауысуы, олардың шешімдері мен әрекеттерінің сәйкес келмеуі, назар аудармаудың немесе түсінбеушіліктің көрінісі.

Өзін-өзі бағалаудың жеткіліксіздігі, мазасыздық, эмоционалды тұрақсыздық адамды құрбан болу қаупіне ұшыратады.

Жәбірленушінің мінез-құلقىның себептері көбінесе отбасылық қарым-қатынаста болады. Құрбандық мінез-құлықтың пайда болуының алғышарттары келесі факторлар болып табылады:

- зорлық -зомбылық;
- ата -ана құрбаны синдромы;
- жеке адам өскен қолайсыз орта (қолайсыз, толық емес отбасы);
- әртүрлі қоғамға қарсы топтарда болу.

Адам өзін жәбірленуші ретінде көрсететін жағдайлардағы виктимизация белгілері қылмыстың жасалуына әсер етуі мүмкін немесе әсер етпейтін заңды және заңсыз әрекеттерде көрінеді.

Жеке тұлғаның жәбірленуші түрі әртүрлі түрде: ол эмоционалды тұрақсыздықта, бағынуға құмарлықта, қарым-қатынастағы қиындықтарда, өз сезімдерін бұрмаланған қабылдауда және т.б. көрінеді. Егер адамдар өмірге қауіп төндіретін сәтте дұрыс емес әрекет етсе, онда олар қиыншылыққа душар болады.

Жеке құрбандық келесі белгілермен анықталады:

- бағыну;
- сендіру, сенгіштік;
- немқұрайлылық пен жеңіл ойлылық;
- өзін -өзі қорғай алмау.

Қылмыскер-жәбірленуші қарым-қатынасы оқиғаларының тең жартысында жасалған зорлық-зомбылық кездейсоқтық емес, өзара қарым-қатынастағы адамдардың кінәсі болып табылады. Адам факторы маңызды рөл атқарады.

Кейбір адамдар көп жағдайда, басқалары аз дәрежеде осал, бірақ зорлық-зомбылық қылмыстардың абсолютті көпшілігінде жәбірленушінің әрекеті агрессияға түрткі болады.

Адам өзіне агрессияны тартатындай қай жерде қателік жіберіп алды?

Ол өзін дөрекі немесе керісінше, жалқау, эмоционалды ұстау арқылы қиыншылыққа ұшырайды. Сонымен қатар, виктимділік мінез-құлық психологиясы ықтимал құрбандықтың өзі агрессия мен зорлық-зомбылыққа бейім болатынын көрсетеді.

Құрбандықтан қалай құтылуға болатыны туралы кеңестер. Психологиялық тұрғыдан алғанда, виктимизация – бұл нормадан ауытқу, оны түзету мен емдеуге болады. Аурудың нақты емі жоқ, және оның туындау себебіне байланысты болады.

Виктимділік мінез -құлықты екі жолмен жоюға болады:

- дәрі-дәрмектер (седативтік препараттар, транквилизаторлар, антидепрессанттар және т.б.).

- психологиялық түзету мен психотерапияның көмегімен.

Түзету мінез-құлықты немесе сезімді түзету арқылы, өзін-өзі бақылауды үйрену, өзін-өзі бағалауды жоғарылату, басқалармен қарым-қатынас орнату, тиімді қарым-қатынас және басқа әдістерді үйрену арқылы жүзеге асады.

Адамның қолайсыз жағдайға бейімділігі – әрқашан оның кінәсінен болмайды. Сонымен қатар, құрбандық мінез-құлық феномені агрессорды ақтамайды (мысалы, зорлаушы немесе өлтіруші) және өз кінәсін жәбірленушіге аудармайды.

Соған қарамастан, егер мәселе қимыл пен іс-әрекетте болса, оларды басқаруды үйрену керек. Мінез-құлықтың дұрыс емес екенін түсініп, ары қарай ақымақтық жасамау және жоқ жерден мәселе таппау үшін оны түзетуге мүмкіндік бар.

4. Ата-ана кітабы. Қатыгез бала (ата -аналарға психолог)

«Ол мысықты таяқпен қатты ұрғаны сонша, қатты ашуланды, біз оны зорға ажыратын алдық. Ал мысықты тағы да ұрып өлтіріп қоймасын деп, туысқандар, а беріп жібердік. Мектепте менің ұлым топ балаларды жинап, басқаларды мазақтайды және ұрып соғады дегенге мен сенбегенмін. Өйткені мен оны барынша жақсы тәрбиелеуге тырыстым».

Сайттан алған жазба

Қатігездік – бұл қатты жүрекпен шамадан тыс агрессия. Бала агрессивті реакция бергенде, біз оның бір нәрсеге қатты ренжігенін, көңілі қалғанын және осылайша қарсылық көрсететінін түсінеміз. Мүмкін ол көмек сұрайды немесе біздің мәселемізге назар аударады. Мұндай агрессия жағымсыз болса да, түсіністік пен жанашырлықты тудырады. Бірақ егер бала ішкі уайымға опасыздық жасамаса, бірақ басқалардың денсаулығына қауіпті әрекеттерді салқын және байсалды түрде жасаса, оған сонша жылу мен үміт сыйлаған ата -анасын ауыртады, қорқытады, жігерлендіреді және жай ғана үмітсіздікке түседі. Балалардың суықтылығы - эмоционалды саланың дамымай қалу салдары.

Өкінішке орай, бұл синдром өте жиі кездеседі, сондықтан эмоционалды сауықтыру бағдарламалары сұранысқа ие. Біз балаларға жаңа ойыншықтар алу үшін заттарды ұқыпты ұстауды, балалар бөлмесінде компьютерде тыныш отыруды үйреттік... Бірақ олар немқұрайлы және қатыгез...

Тұрақты жұмыс пен өмірдің қарқыны қазіргі ата-ананың баламен терең эмоционалды байланыс орнатуына, оның алаңдаушылығын сезінуіне мүмкіндік

бермейді. Балалардың тәжірибесін жоққа шығарып, олардың шынайылығы мен ашықтығына сенуге бола ма? Балалардың қатыгездігі – бұл олардың сезіміне немқұрайды қарауымыздың табиғи нәтижесі. Біреу оны агрессивті түрде, ашық түрде жасайды. Біреу сабырлылықпен, бірақ табандылықпен, баланың ешбір шағымы ата-ананың жүрегіне әсер етпейтіндігін көрсетті. Содан кейін бала логикалық түрде қоршаған әлем оған мән бермейді, оны ешкім жақсы көрмейді деген қорытындыға келеді.

Эмоционалды суықтылықтың ең терең көрінісі – тактильді сезімталдықтың жоғалуы. Балалар кейде өздерін қысады немесе бірнәрсемен алақандарын қатты ұрады.

Біз балаларды сәл құшақтап, еркелетеміз, оларды компьютерде немесе теледидар экранында «тәрбиелеуге» қалдырамыз, ал көзбен көру қабылдауы олардың сезімталдығының ошағына айналады.

Олар қиялмен өмір сүреді, оларда шындық сезімі дамымаған. Сондықтан олар сезімталдық шегін төмендете алатын күшті және ашулы кейіпкерлерді өздерінің батыры ретінде таңдай отырып, виртуалды әлемнің тұтқынына оңай түседі. Олар біреуді ұрғанда және ренжіткенде, аяушылықты сезінбейді.

5. Неге балалар қатігез болады?

1. Балалық шақтағы агрессия қатаң қарым-қатынас немесе салқын қарым- қатынастың салдары болуы мүмкін. Бірінші жағдайда бәрі түсінікті. Егер баланы ұрса, тамақтандырмаса, үстемдік жасаса және қорласа, ол қарым-қатынаста басқа тәсілмен «оңалуға» тырысады. Тек осылай ғана ол әділеттілікті қалпына келтіре алады. Мұндай балалар тез өсуді және ата-анасынан кек алуды армандайды. Екінші жағдай күрделірек. Жақсы беделге ие отбасылар суық үй синдромымен жиі ауырады: олар бала тәрбиесімен мұқият айналысады, ақшаны аямайды. Баллаардың қатыгездік жағдайларын көрген ата-аналар көбінесе баланың жай ғана еркелігі деп қабылдайды. Олар ұру керек деп ойлайды ма? Бірақ дәл осылай ата -аналар бірінші жағдайда жасады және ұқсас нәтиже алды. Оларға ортақ нәрсе – отбасында жылы, нәзік, қуанышты қарым-қатынастың болмауы. Отбасындағы жалғыз адамның бақыты мен қуанышы отбасының қалған мүшелері үшін құндылық емес. Әркім өз мүддесі бойынша өмір сүреді. Ал үйде? Сіздің міндеттеріңізді орындап, сыпайы болу жеткілікті.

2. Қатыгездіктің негізгі себебі – өзіне сенімсіздік, жаман оқиғаларды, жаман өзгерістерді шыдамсыздықпен күту. Агрессия арқылы күштелу жеңілдейді. Балалар өмір сүретін белгісіздік, үнемі өзінен, отбасынан қорқу мазасыздықты арттыруы мүмкін. Сонымен қатар, мұндай алаңдаушылықтың себебі салыстырмалы түрде кедейлік болуы мүмкін: сыныптастарыңыздың ата-аналары қымбат көліктерді басқарады, ал сіздің отбасыңыз мұндай сатып алуды жоспарлап қана қоймай, үнемдеу, аз ақша жұмсау және т.б. туралы айтады.

3. Ерекше қатыгездіктің себептері арасында үшінші орында теледидар мен интернет. Зорлық көріністер, имитациялық ойындар, «атқыштар» агрессия тудыруы мүмкін. Экран технологиясы жастардың мінез-құлқына әсер етуі мүмкін. Жас суицидтер туралы фильмдердің көрсетілуі суицид санының

айтарлықтай өсуіне әкеледі. Бір-бірін көңілді музыкамен «жоятын» жануарлар туралы мультфильмдерді көргеннен кейін, дәл осындай құмарлықтағы бала үй мысығын қағып кетуі немесе велосипедпен тасбақаның үстінен жүріп өтуі мүмкін. Экрандық технологиялар сезімталдық пен шындық сезімін өзгертеді. Акцент тактильден визуалды тәжірибеге ауысады, сурет ауыртпалық емес, маңызды болады.

4. Қатыгездік – бұл жәбірлеушілерден қорғану әдісі, жауап ретінде оған да сондай ауырту және ренжітуге ұмтылу болып табылады. Әсіресе қатал мұғалімдер әрқашан қатыгездік нысаны болып табылады. Оларға бірінші болып лақап аттар қою және орындықтарын бормен бояу секілді әрекеттерге барады.

5. Кек алудың нысаны сыртқы жағынан басқалардан ерекшеленетін балалар – әсіресе ұзын бойлы, өте толық, басқа этникалық топтардың өкілдері болуы мүмкін. Балалардың қорқыныштары осылайша жойылады. Кіші мектеп оқушылары адасып кетуге бейім және іс жүзінде жеңілмейтін болып, «ұқсамайтындармен» жасырын және өте қатал соғыс бастайды.

6. Қатыгездік балалардың қарым-қатынастарына араласпауды жөн көретін ересектердің немқұрайдылығынан да туындайды.

6. Балаларды басқаларды сүйуге қалай үйретуге болады?

1. Адамдар арасындағы жақындасудың үш кезеңі бар: агрессия – аяушылық – сүйіспеншілік. Егер оларға сүйіспеншілік қана емес, ешкімнің аяушылығы болмаса, олар қатігез болады. Туғаннан бастап әр адам тәндік қатынасқа деген қажеттілікті сезінеді. Егер баланы елемей қойса, оған қол тигізбесе, нәзіктікпен бауырына баспаса, ол әртүрлі жолдармен сүйіспеншілікті сұрай бастайды. Ол ауырады, мысалы, ол үнемі шағымданады, өйткені ауырса ғана анасы мейірімділікпен асты-үстіне түсіп қамқор болады. Егер аяушылық болмаса, бопсалау ашулану түріне айналады: заттарды еденге лақтырады, киімін жыртады, «өртегенді», ойыншықтарын жоғалтады. Бұл мінез-құлық сүйіспеншіліктің қажеттілігін білдіреді.

2. Егер бала кішкентайынан тәрбиемен «кодталған» болса, ол қатыгездік таныта алмайды. Қол көтерген баланы тоқтататын формулалар бар. Сіз балаға «бумеранг заңы» туралы айтыңыз: ренжіту мен қиянат жасау ерте ме, кеш пе, жәбірлеуші мен оның туыстарының басына түседі.

Өмірдің қаншалықты таңқаларлық және кешірімді екендігі туралы мағыналық әңгімелер, ертегілер мен астарлы әңгімелер айтыңыз.

3. Баланы кешірім сұрауға және кешіруге үйретіңіз. Бұл реніштен аман қалудың және адамдармен қарым-қатынасты сақтаудың сенімді жолы. Адамдардың қасақана ренжітуі өте сирек, ал кездейсоқ реніш үшін олар аяусыз кек алады. Өзіңіз кешірім сұраңыз. Егер реніш жеңіл болса да, оған бірге күлуге болады: кешірім сұрау бізге басқа адамның сезімдері маңызды екенін түсінуге мүмкіндік береді.

4. Лексикада сын есімдерді, азайтатын сөздерді, баланың есімінің нәзік нұсқаларын қолданыңыз. Сізден басқа ешкім баланы олай атамайтындай еркелету мен есімдер нұсқаларын: «Айналайын», Патшам, Төрем, «Жаным»,

«Күнім» және балаңыздың есімдеріне байланысты еркелетіп айту тәсілдерін ойлап табыңыз.

Сіз үшін бала қаншалықты құнды және ерекше екенін сезінуі тиіс.

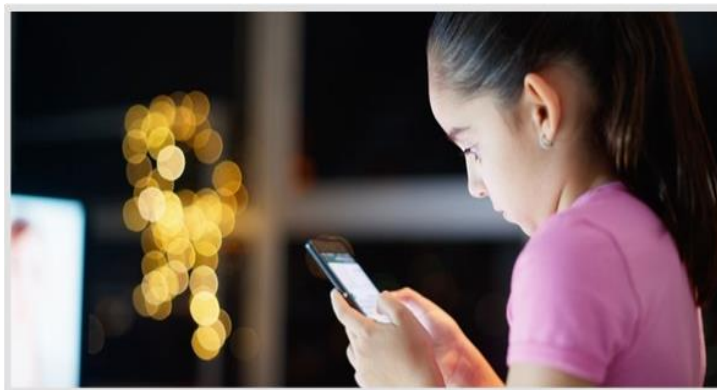
Жүрегі нәзіктік пен сүйіспеншілікке толы бала қатыгез бола алмайды.

5. Есіңізде болсын, өмір дүрбелеңге, қорқынышқа, қиялға толы. Балаға үнемі жайлылық пен жігер қажет. «Ештеңе етпейді.... Ренжіме.... Мен сізге көмектесемін... Менің қасыңда екенімді көріп тұрсың...». Бұл сөздер ересектерге де әсер етеді, олар бізге не жақсы көретінімізді айтады.

6. Агрессия өзгеруі мүмкін. Агрессияға қарсы күрес – сүйіспеншілік пен нәзіктіктің көрінісі. Адамзатты құтқаратын супер қаһармандар туралы фильмдермен қатар үйде сүйіспеншілік туралы фильмдер болуы керек. Мелодрамалар 9 жастан 12 жасқа дейін агрессивті мінез-құлық формаларын белсенді меңгерген ұлдарға онша қызығушылық танытпайды. Бірақ кейінірек, қарсы жыныстағы тұлғаға қызығу тудыратын қатынастар оларды байыпты қабылдай бастағанда, оларға жақсы романтикалық комедиялар ұсыныңыз.

7. Өзіл – бұл төбелеске қарағанда тиімдірек қару. Күлкілі теңеулерді қолданыңыз, араластырыңыз, егер жағдай сәл өзгерсе, жанжалды шешу оңай екенін көрсетіңіз.

*АТА-АНАЛАРҒА КЕҢЕС
БАЛАЛАРҒА КИБЕРҚАУІПСІЗДІКТІ ҚАЛАЙ ҮЙРЕТУГЕ БОЛАДЫ?*



Қашықтықтан оқытудың күрт өсуі нәтижесінде ата-аналарға балалардың интернеттегі әрекеттерін бақылау әлдеқайда қиындай түсуде. Балалар желіде ата-аналар қалағаннан әлдеқайда көп уақыт өткізеді. Ата-аналардың көпшілігі үнемі балалардың интернеттегі әрекеттерін бақылауға уақыт таба алмайды.

Касперский Зертханасының жақында жүргізген зерттеуі мәселенің күрделі екендігін көрсетеді. Міне, бүгінгі жастармен жүргізілген зерттеудің нәтижесі:

- Жасөспірімдердің 73% -ы смартфонсыз өмір сүре алмайды, ал олардың жартысы жатарда өздерімен бірге телефонды алып ұйықтайды.

- 8-16 жас аралығындағы балалардың 44% -ы үнемі әлеуметтік желіде, ойын-сауық қосымшалары мен әлеуметтік медианы артық көреді.

- Балалардың 40% - ы интернетте құпия ақпаратты, соның ішінде үй мекен- жайын жариялап қояды.

- Жастардың үштен бірі интернетте өздерінің жасы туралы қате ақпарат береді.

- Балалардың 37% - ы интернетте қауіп-қатерге тап болды, соның ішінде кибербуллинг, қаржылық қауіптер немесе қажетсіз, зиянды мазмұндағы ақпараттар.

Бірде-бір ата-ана баланың смартфоны мен ноутбугында не істеп жатқанын бақылай алмайды. Бақылау болған жағдайда ол мүмкін бе?

Технология балалық шақтан бастап, содан кейін ересек өмірде маңызды рөл атқарады. Алғашқы жылдарда баланың интернеттегі қауіпсіздікті қамтамасыз ету үшін қажетті дағдыларды дамыту мүмкіндігі бар.

Идеал тәсіл – балалардың қауіпсіздігін қамтамасыз ету үшін оларға білім беру және мүмкіндік беру қажет.

Балаларыңызды қорғау үшін үйреніңіз

Егер сіз балаларыңыздың қауіпсіз болуын қаласаңыз, алдымен олар интернетке кірген кезде қандай қауіптерге тап болатынын түсінуіңіз керек. Мұны өзіңіз түсінгеннен кейін, сіз балаларға желіде қауіпсіз және көңілді уақыт өткізуге көмектесе аласыз.

Интернетте көптеген керемет ресурстар бар, олар негізгі қауіптер туралы айтады, тіпті техникадан алшақ адамдар да түсінеді. Сіз Kaspersky

Resource Center – де материалдарды зерттеуден бастай аласыз ол – Интернеттегі қауіпсіздік туралы түсінікті мақалалары бар тегін ресурс. Мұнда балаларға көрсетуге болатын ең маңызды терминдер мен инфографиканың анықтамалары берілген. Сондай-ақ, ресурста/ресурстық орталық/threats соңғы қауіптер туралы жаңалықтар және отбасыңызды қалай қорғауға болатындығы туралы кеңестер бар.

Жалпы, балалар үшін интернетте кездесетін қауіптердің үш санаты бар:

- *Бейтаныс адамдар.* Зиянкестер әлеуметтік медиа сайттары мен онлайн ойындар сияқты балаларды қызықтыратын сайттарда жасырынып жүр. Мұндай шабуылдаушылар көбінесе өздерін балалар етіп көрсетеді. Бұл әдіс кэтфишинг деп аталады. Сондай-ақ, хакерлер мен киберқылмыскерлер бар, олар қауіпсіздіктің жеткіліксіз деңгейі бар барлық пайдаланушыларға шабуыл жасайды, бұл баланың немесе ересек адамның болуы маңызды емес. Олар сондай-ақ баланың құпия сөздерін немесе төлем ақпаратын алдап анықтауға тырысуы мүмкін.

- *Құрдастар.* Сіздің балаңыз таныстарының қорлауына немесе қорлауына ұшырауы мүмкін. Бұл көбінесе жеке әлеуметтік медиа чаттарында және хабар алмасу қосымшаларында болады. Кейде басқа балалар сіздің балаңыздың жеке ақпаратын жариялай алады, бұл оған үлкен азап әкеледі. Егер мұндай ақпарат жыныстық сипатта болса, мысалы, интимдік фотосуреттер, бұл ауыр қылмыс болуы мүмкін.

- *Өз бетінше.* Бақылаусыз балалар өздері үшін желіде қауіпті жағдайлар жасай алады. Олар көбінесе батырмаларды басады немесе бағдарламалық жасақтаманы өз әрекеттерінің салдарын түсінбестен орнатады, сонымен қатар туған күні немесе мекен-жайы сияқты жеке ақпаратты жариялайды.

Бұл қауіптердің кейбірі әлеуметтік қауіптер болып табылады – олар бопсалаумен немесе манипуляциямен байланысты. Көбінесе бейтаныс адам баланың сеніміне ие болады, содан кейін оны пайдаланады. Бұл қауіптерден қорғану үшін бала басқа адамдармен қалай қауіпсіз қарым-қатынас жасау керектігін білуі керек.

Қауіптің тағы бір түрі – деректерге қол жеткізу үшін технологияны қолданатын цифрлық қауіптер. Бұл зиянды бағдарламалар (мысалы, жеке ақпараттарды ұрлау) немесе фишинг (жалған веб-сайтқа алаяқтықпен кіруге мәжбүр ету) болуы мүмкін. Қауіптің бұл түрінен қорғау үшін балаға интернетті қалай дұрыс пайдалану керектігін және сенімді антивирустық бағдарламаларды орнатуды түсіндіру қажет.

Балалармен киберқауіпсіздік туралы сөйлесуге арналған 5 кеңес

Әр бала ерекше. Интернеттегі әр түрлі тақырыптар әркімді қызықтырады және қауіп-қатерді әркім әр түрлі шешеді. Балаларға Интернеттегі қауіпсіздік туралы айтудың әмбебап дұрыс әдісі жоқ. Сіз баланы осы тақырыпқа қызықтырудың жолдарын тауып, оған не істеу керектігін түсінуге көмектесуіңіз керек. Диалогты бастау үшін бірнеше кеңестер берілген.

1. *Балаларға арналған білім беру ресурстарын пайдаланыңыз.*

Көбінесе балалармен олардың интернеттегі қауіпсіздігі туралы сөйлесу оңай емес. Бұл әсіресе қолданылатын көптеген ұғымдарды түсінбейтін кішкентай балалармен қиын. Бастауыш сыныптағы балаға желіде киберқылмыскерлер бар екенін қалай түсіндіруге болады? Ең бастысы, бұл ақпаратты баланы қорқытпай қалай жеткізуге болады?

Киберқауіпсіздіктің негізгі ұғымдарын түсіндіруге көмектесетін ақпараттар мен кеңестер, балаларға арналған шағын, қызықты әңгімелерді ұсынуға болады. Құпиялылықты қалай басқаруға болатынын, күшті құпия сөзді қалай таңдауға болатынын және кибербуллинг құрбандарына не істеу керектігін түсіндіру маңызды. Киберқауіпсіздіктің негіздерін оларға қажетсіз алаңдаушылық туғызбай түсінуге көмектесетін балаларға арналған кітаптарды ұсынуға болады. Олар: 1. Сюзан Кингтің «Балаларға арналған онлайн қауіпсіздік кітабы». Бұл кітап балаларға кибербуллинг, фишинг және зиянды бағдарламалар сияқты әртүрлі онлайн қауіпсіздік қатерлері туралы айтады. Ол сондай-ақ өзіңізді осы қауіптерден қалай қорғауға болатыны туралы кеңестер береді. 2. Линди Смиттің «Балаларға арналған Кибермәдениет». Бұл кітап балаларды этикалық қарым-қатынас ережелері және ақпаратты тұтыну мәдениеті сияқты кибермәдениет негіздерімен таныстырады. Ол сондай-ақ балаларға сыни ойлауды дамытуға көмектеседі, осылайша олар Интернеттен тапқан ақпаратты бағалай алады. Бұл кітаптар түсінікті тілде жазылған және оларды балаларға қызықты ететін иллюстрацияларды қамтиды. Олар балаларға Интернеттегі қауіпсіздік, гигиена және мәдениеттің маңыздылығы туралы білуге көмектеседі.

Сонымен қатар пайдалы болуы мүмкін тағы бірнеше кітаптар: Джон Роббинстің «Балалар мен жасөспірімдерге арналған киберқауіпсіздік» ;

Сюзан Кингтің «Кибербуллинг: өзіңізді және достарыңызды қалай қорғауға болады»;

Линди Смиттің «Зиянды бағдарламалар: компьютерді қалай қорғауға болады»;

Дженнифер Фрэнк «Интернеттегі қауіпсіздік: Цифрлық әлемде қалай қауіпсіз болу керек»;

Дженнифер Фрэнктің «Балаларға арналған Кибергигиена». Бұл кітап балаларға кибергигиена ережелерін сақтаудың маңыздылығы туралы айтады, Мысалы, компьютерді дұрыс пайдалану, салауаттылықты және Интернеттегі қауіпсіздік ережелерін сақтау.

2. Интернетте жұмыс істеудің негізгі ережелерін орнатыңыз

Балаңызбен бірге Интернетті пайдаланудың бірнеше негізгі ережелері туралы келісіңіз. Кішкентай балалар үшін бұл ережелер түсінікті және қарапайым болуы керек. Мысалы, ережелер келесідей болуы мүмкін:

- Ересектердің рұқсатынсыз Интернетке шықпау;
- Экранының алдында күніне 30 минуттан артық отырмау;
- Тек белгілі бір қолданбаларға рұқсат етіледі (мысалы, қауіпсіз іздеуі бар YouTube немесе сүзгілері бар веб-шолғыш).

- Ойындарды орнатуға рұқсат сұрау.

Сіз бұл ережелерді жазып, оларды мезгіл-мезгіл жаңарта аласыз.

Сіздің балаңыз есейген сайын оған қосымша еркіндік қажет болуы мүмкін. Ережелерді аздап кеңейтуге болады, сонда олар мыналарды қамтиды:

- Ешқашан интернетте нақты атыңыз бен мекен-жайыңызды атамаңыз.

- Рұқсатсыз қосымшалардағы төлемдерге рұқсат бермеңіз.

- Күмәнді қолданбалардан аулақ болыңыз.

- Жеке ақпаратыңызды және фотосуреттеріңізді жарияламаңыз.

- Егер біреу қажетсіз әрекеттерді жасауға тырысса, ересектерге хабарласыңыз.

Бала жасөспірімдік шаққа енген сайын, оның желіде өмір сүруін қолдайтын ережелерді ойлап табуға тура келеді. Есейген шақта балалармен бірге пайдалы, бірақ шектеусіз ережелер жасауға болады.

Жоғарыда сіз қолдануға болатын ережелердің мысалдары ғана берілген. Әр бала әр түрлі және ерекше қажеттіліктерге ие, сондықтан сіз өзіңіздің балаңызға сәйкес келетін ережелерді жасауыңыз қажет.

3. Қауіптерге емес, мүмкіндіктерге назар аударыңыз

Цифрлық әлем балалар мен ата-аналарды қорқытпауы керек. Не болуы мүмкін екендігі туралы алаңдамау, балаларды желідегі қауіпсіздік үшін қажетті дағдыларға үйретуге көңіл бөлу әлдеқайда дұрыс.

Сұрақтар мен мәлімдемелердің тізімін жасауға, оны балалармен талқылауға және олардың барлық сұрақтарға жауаптарды білетінін және барлық мәлімдемелермен келісетінін түсінуге болады. *Бұл тізімде келесі элементтер болуы мүмкін:*

- Егер біреу ыңғайсыздық тудырған болса не істеу керек?

- Интернетте қандай ақпаратты хабарлауға болады және тек жеке нені хабарлауға болады?

- Сіз бейтаныс адамдармен емес, достарыңызбен ғана сөйлесе аласыз.

- Сайттың шынайы немесе жалған екенін қалай тексеруге болады?

- Неліктен қауіпті сайттардан аулақ болу керек?

- Күшті құпия сөзді қалай жасауға және телефонды екі факторлы аутентификация үшін қалай пайдалануға болады?

- Онлайн төлем жасамас бұрын үнемі ата-анадан рұқсат сұрау керек.

- Интернетте құпиялар мен фотосуреттерді орналастырған кезде абай болу керек.

- Егер күмән туындаса, ересек адаммен сөйлесіп, көмек сұрау керек.

Бұл киберқауіпсіздік дағдылары ересектерге де қажет. Егер сіз баланы ерте жастан бастап осы белсенді тәсілге үйретсеңіз, ол ересек жаста қауіпсіздікті қалай қамтамасыз ету керектігін біледі.

4. Сенімді және жайлы орта мен ахуал орнатыңыз

Идеал әлемде онлайн қауіпсіздік сұрақтары туындаған кезде балалар әрқашан да сізден көмек сұрайды. Бірақ шынайы әлемде олай болмайды.

Кейде балалар көмек сұрау қиыншылыққа әкелуі мүмкін деп ойлайды. Мысалы, егер бала интернеттегі мінез-құлық ережелерін бұзу нәтижесінде фишингтік алаяқтықтың немесе кэтфишингтің құрбаны болса, онда бұл жағдайда бала күрделі дилеммаға тап болады: егер ол сіздің кеңесіңізді сұраса, ережелерді бұзуға байланысты проблемалар туындауы мүмкін деп ойлайды.

Сондықтан балаңызға қажет кезде оны әрдайым қолдайтындығыңызды білдіру өте маңызды. Бала ең бастысы оның қауіпсіз екенін білсін. Егер бірдеңе дұрыс болмаса, үйренуге болатын жағымды нәрселерді табуға тырысыңыз.

Сондай-ақ, балалар олардың проблемаларын ата-анасы түсінбейді деп алаңдауы мүмкін. Бұл қудалау мен қорлау жағдайында болуы мүмкін – нақты мектеп ауласында да, цифрлық әлемде де туындауы мүмкін мәселелер. Мұндай мәселеде ата-ана ретінде балалардың өз сезімдері туралы айтуы және олардың мәселелеріне байыпты қарауыңыз үнемі маңызды. Бұл сізге маңызды болып көрінбесе де, бұл олар үшін маңызды болуы мүмкін.

Ең бастысы, ата-аналар балаларына үлгі болуы керек. Желідегі өзіңіздің мінез-құлқыңыз әрқашан қауіпсіз және жауапты екеніне көз жеткізіңіз. Балалардың жанында болған кезде құрылғылар экранының алдында өткізетін уақытты шектеуге тырысыңыз.

5. Дұрыс қауіпсіздік құралдарын қолданыңыз

Интернет қауіпсіздігі – бұл ересектер үшін де, балалар үшін де қиын міндет. Көптеген күрделі қауіптер бар және бала барлық ережелерді сақтаған кезде де қиындықтарға тап болуы мүмкін.

Сонымен, ересектер интернеттегі қауіпсіздікті қалай қамтамасыз ете алады? Ол үшін цифрлық қызметтерді пайдалану кезінде туындайтын негізгі қауіптерді болдырмауға көмектесетін әртүрлі құралдар қолданылады. Сіздің үйіңіздегі әрбір құрылғыда келесі құралдар болуы керек:

Антивирус – интернет қауіпсіздігінің негізі. Ол фондық режимде жұмыс істейді және вирустардан, соның ішінде трояндардан, төлем бағдарламаларының тыңшылық бағдарламаларынан қорғайды. Зиянды бағдарлама сіздің құрылғыңызды жұқтыруға тырысқанда, антивирус оны тоқтатады.

Антифишинг. Фишинг – киберқылмыскерлер қолданатын ең танымал әдістердің бірі, қарапайым, бірақ өте деструктивті. Сіз де, сіздің балаңыз да кездейсоқ жалған сілтемеден өтпеуі үшін қосымша қорғаныс қажет.

Веб-камераны қорғау. Егер шабуылдаушы веб-камераға кірсе, ол сізге және сіздің балаларыңызға тыңшылық жасай алады. Үй тапсырмасын орындау кезінде ZOOM-да веб-камераны өшіру мүмкін емес. Оның орнына мұндай қауіптен қорғайтын құрал қажет.

Мазмұн блокаторы. Хакерлер мен вирустардың құрбаны болмаудың ең жақсы жолы – қауіпті мазмұннан аулақ болу. Балалардың интернеттің қауіпті аймағына кіруіне жол бермеу үшін мазмұн блокаторларын пайдалануға болады.

VPN. VPN – бір жерден екінші жерге жылжу кезінде сіздің деректеріңізді қорғайды. Бұл әсіресе бала жалпыға ортақ Wi-Fi желілерін пайдаланса өте маңызды.

Құпия сөзбен қорғау. Балаларға күшті пароль ережелерін сақтау өте қиын. Құпия сөзді қорғау құралы күшті құпия сөзді жасайды және оны келесі кіру үшін сақтайды.

Бағдарламаның бұл түрі желіде кездесетін кездейсоқ қауіптің алдын алуға көмектеседі.

Балалардың киберқауіпсіздігін қалай қамтамасыз етуге болады?

Ата-ана болу – ең үлкен жауапкершілік. Әрбір ата-ана балаларының әлемді зерттеп, өздерін тауып, қызықты мүмкіндіктерді пайдаланғанын қалайды, бірақ қауіпсіз және мүмкіндігінше тәуекелдерді болдырмайды.

Кейде балаларының электронды құрылғыларды қолданғанын көргенде неліктен ата-аналар қатты алаңдайды. Ата-аналарда сұрақ туындайды: *бұл құрылғылар оқу құралы және білім көзі ме, әлде олар балаларға қауіп төндіре ме? осындай алаңдаушылық көп туындап жатады.*

Жоғарыда келтірілген кеңестер балалармен киберқауіпсіздік туралы нәтижелі сөйлесуге, оларды қорғауға және өз қауіпсіздігін қамтамасыз ету үшін қажетті дағдыларды дамытуға көмектеседі.

Бірақ кейде ата-аналарға қосымша көмек қажет. Kaspersky Safe Kids-отбасыларға арналған жетекші киберқауіпсіздік платформаларының бірі, ол негізгі құралдар жиынтығын ұсынады:

- GPS арқылы бақылау балалардың орналасқан жерін кез келген уақытта бақылауға мүмкіндік береді. Сіз картаға қауіпсіз аймақ орнатып, егер бала одан тыс болса, хабарлама ала аласыз.

- Балаңыздың құрылғыны пайдалануын автоматты түрде басқару үшін құрылғыны пайдалану уақытын бақылау. Бұл мүмкіндік баланың күн сайын ойындар мен әлеуметтік желілерде өткізетін уақытын шектеуге және баланы ұйықтар алдында құрылғыны өшіруге мүмкіндік береді.

- Мазмұнды сүзу қауіпті мазмұннан қорғауды қамтамасыз етеді және интернетте және YouTube-те іздеу кезінде орынсыз мазмұнды жасыруға мүмкіндік береді. Сіз шектеулер деңгейін өз қалауыңыз бойынша басқара аласыз.

Интернеттің әлемінде әр балаға қорғаныс қажет.

БАЛАЛАРДЫ ИНТЕРНЕТТЕГІ ЫҚТИМАЛ ҚАУІПТІ ТӘУЕКЕЛДЕРДЕН ҚОРҒАУ ТУРАЛЫ АТА-АНАҒА КЕҢЕС

Сонымен қатар ересектердің ең маңызды міндеті – балаларға интернеттің қауіптілігі туралы ескерту. Балалармен интернетті пайдалану кезінде туындауы мүмкін барлық мәселелерді талқылау қажет.

Балалардың интернеттегі ықтимал қауіпті тәуекелдері туралы:

Бірінші тәуекел – бұл жеке компьютердегі жеке ақпараттың қауіпсіздігі, бұл вирустардан, зиянды бағдарламалардан қорғауды және бағдарламалық жасақтаманы үнемі жаңартып отыруды білдіреді. Бұл жағдайда балаларыңызды қалай қорғауға болады? Ең алдымен, деректерді қорғау деңгейін арттыру. Мұны көптеген бағдарламаларда қол жетімді сүзгі параметрлері мен мазмұнды сүзу опцияларын пайдалану арқылы жасауға болады. Сонымен қатар, зиянды бағдарламаларды жұқтыру қаупі жоғары. Шынында да, оны тарату және компьютерлерге ену үшін көптеген әдістер қолданылады. Олардың ішінде тек поштаны, компакт-дискілерді, иілгіш дискілерді және басқа ауыстырылатын ақпарат тасымалдаушыларын немесе интернеттен жүктелген файлдарды атап өтуге болады. Мысалы, жедел хабар алмасу бағдарламалық жасақтамасы бүгінде вирустарды таратудың қарапайым әдісі болып табылады, өйткені олар файлдарды тікелей тасымалдау үшін жиі қолданылады. Бұл әдісті хакерлер трояндық вирустарды тарату үшін жиі қолданады. Әлеуметтік инженерия мәселелерінде тәжірибесіз балалар қаскүнемнің айла-амалдарына оңай түсе алады.

Компьютерде жеке ақпаратты жоғалту қаупін болдырмау үшін қарапайым қауіпсіздік ережелерін сақтау қажет:

- Амалдық жүйені үнемі жаңартып отырыңыз.
- Тек лицензияланған бағдарламалар мен сенімді көздерден алынған деректерді пайдаланыңыз. Көбінесе вирустар бағдарламалардың қарақшылық көшірмелерін, әсіресе компьютерлік ойындарды жұқтырады.
- Базаларын үнемі жаңартып отыратын антивирустық бағдарламаны қолданыңыз және компьютерде апта сайын вирустар бар-жоғын тексеріңіз.
- «Сақтық көшірмелер» деп аталатын маңызды файлдардың сақтық көшірмесін жасаңыз (мысалы, бөлек, тек сол үшін және арнайы қатты дискіде немесе usb дискісінде).
- Интернетке мазмұнды жүктеу кезінде абай болыңыз. Есіңізде болсын: Дүниежүзілік желіде ақпарат жарияланғаннан кейін оның әрбір көшірмесін бақылау және жою мүмкін болмайды.
- Интернеттен мазмұнды жүктеу кезінде абай болыңыз: кішкене күмәндансаңыз, деректерді компьютерге «жүктеуден» бас тартыңыз.
- Құпия сөздерді мезгіл-мезгіл өзгертуге тырысыңыз (мысалы, электрондық поштадан, әлеуметтік медиа профильдерінен), бірақ оңай бұзылатын құпия сөздерді (туған күндер, телефон нөмірлері және т.б.) пайдаланбаңыз. Құпия сөздерді ешкімге бермеңіз!

- Интернетті басқа біреудің құрылғысында қолданған кезде парольдерді сақтамаңыз және жұмыс аяқталғаннан кейін әлеуметтік желідегі, поштадағы және басқа сайттардағы есептік жазбаңыздан шығуды ұмытпаңыз.
- Осы ережелердің барлығын балаларыңызға түсіндіріңіз!

Екінші тәуекел – байланыс деректерін жариялау.

Интернетте (чаттар, әлеуметтік желілер және т. б.) балалар басқа балалармен сөйлесе алады және жаңа достар таба алады, бұл баланың жеке басын, байланыс ақпаратын (толық аты-жөні, пошталық мекен-жайы және телефон нөмірі), оның өмірінің егжей-тегжейін, күн тәртібін және т.б. анықтауға болатын белгілі бір жеке ақпаратпен алмасуды білдіреді. сондай-ақ, берілген мәліметтердің әртүрлі түрлерін (мысалы, мектеп атауы, спорт клубы, тұрғылықты жері және т.б.) байланыстыру арқылы орнатыңыз. Мұндай ақпаратты қылмыстық мақсатта пайдаланылуы мүмкін.

Сондықтан, балаларыңызға жағымды мысал келтіре отырып, байланыс деректерін немесе басқа жеке ақпаратты жариялау кезінде абай болуға тырысыңыз. Бейтаныс адамға жіберілген кез-келген фотосуреттер немесе жеке мәліметтер интернетте жалпыға қол жетімді болуы мүмкін. Интерактивті күнделіктер ұзақ уақыт бойы көпшілікке қол жетімді болуы мүмкін. Интернетте мәтін немесе фотосурет жарияланғаннан кейін оларды бақылау мүмкін емес. Оларды әртүрлі жерлерге оңай көшіруге болады және оларды толығымен жою мүмкін болмауы мүмкін.

Балалармен бірге олардың қажеттіліктерін талқылау кезінде қауіпсіздік ережелерін сақтаңыз:

- Балалармен жеке ақпарат берудің ықтимал қауіпті салдарын және жеке ақпаратты жасыру ұсынылатын жағдайларды (әр баланың жасын және психологиялық тепе-теңдігін ескере отырып) талқылаңыз.
- Есіңізде болсын: сіз ешқашан парольдерді ешкімге, тіпті ұзақ уақыт достарыңызға бермеуіңіз керек. Сонымен қатар, парольді үнемі өзгерту керек. Мұны балаларыңызға үйретіңіз.
- Интернет – бұл қоғамдық орын. Кез-келген ақпаратты немесе олардың фотосуреттерін (сондай-ақ басқа адамдардың фотосуреттерін) жарияламас бұрын, әлемдегі кез-келген адам бұл ақпаратқа қол жеткізе алатындығын есте ұстаған жөн.
- Бала кез-келген уақытта ата-анасымен интернеттегі жағымсыз тәжірибелер туралы сөйлесе алатындығын білуі керек, бұл айыптау мен жазадан гөрі ересектерден қолдау мен көмек алатынын түсінеді.

Үшінші тәуекел – қажетсіз мазмұнға қол жеткізу.

Бұл зорлық-зомбылық, есірткі, порнография, суицидке итермелейтін беттер, тамактанудан бас тарту, кісі өлтіру, ұлтшыл немесе ашық фашистік идеологиясы бар беттер және т.б. болуы мүмкін. Өйткені, мұның бәрі интернетте шектеусіз қол жетімді. Көбінесе бұл беттерді қарау балаға да

байланысты емес, өйткені көптеген сайттарда кез-келген ақпаратты, көбінесе порнографиялық сипаттағы қалқымалы терезелер көрсетіледі.

Мұндай ақпарат жиі еліктіреді және болып жатқан оқиғалардың мағынасын толық түсіне алмайтын балалар мен жасөспірімдерге қатты психологиялық қысым көрсетуі мүмкін және ұқсас мазмұндағы сайттарды қарау мен зерттеуден бас тартуы мүмкін. Мұндай ақпараттың балалар мен жасөспірімдердің әлі жетілмеген психикасына әсерін болжау мүмкін емес; мұндай сайттардың әсерінен балалар эмоционалды түрде ғана емес, сонымен қатар олардың физикалық денсаулығына да тікелей зиян келтіруі мүмкін.

Антивирустық бағдарламалардың, интернет-браузерлердің қосымша функциялары арқылы мазмұнды сүзуді орнату немесе WindowsVista-да ата-ана бақылауы немесе Kasperskyinternetsecurity-ге енгізілген ата-ана бақылауы сияқты арнайы бағдарламалық жасақтаманы орнату балаларды осы қажетсіз ақпараттан қорғауға көмектеседі.

Егер ересектер де компьютерді қолданса, онда бала үшін сүзу және ата-ана бақылауы конфигурацияланатын жеке пайдаланушы тіркелгісін жасаған дұрыс. Бұл жағдайда сіз әкімші функцияларын орындайсыз (бөлек есептік жазба): жүйенің параметрлерін басқара аласыз және компьютердің басқа пайдаланушыларының осындай құқықтарын шектей отырып, жаңа бағдарламалық жасақтаманы орната аласыз. Жұмыс үшін күшті және қорғалған құпия сөздерді жасауды ұмытпаңыз.

Қажет емес ақпаратты электрондық пошта арқылы да алуға болады, сондықтан спамды сүзу арқылы баланың кіріс жәшігін орнату және осылайша қажетсіз хабарламалардың көпшілігінің алдын алу маңызды. Электрондық поштаны пайдаланудың тағы бір қауіпсіз, бірақ өте шектеулі тәсілі – бұл параметрлерді бала тек көрсетілген мекен-жайлардан хабарлама алатындай етіп орнату. Көптеген электрондық пошта бағдарламалары белгілі бір электрондық пошта мекен-жайларынан жіберілген хабарларды бұғаттауға мүмкіндік береді.

Төртінші тәуекел – бейтаныс адамдармен байланыс.

Чаттарда, онлайн-мессенджерлерде (ICQ, Skype, MSN және т.б.), әлеуметтік желілерде, танысу сайттарында, форумдарда, блогтарда және т.б. қарым-қатынас кезінде осындай тәуекелдерге тап болуыңыз мүмкін.

Балалар мен жастар үшін интернет негізінен достармен ғана емес, бейтаныс адамдармен де кездесуге болатын әлеуметтік орта. Интернетте қолданушы ренжітуі, қорқытуы немесе тіпті қорлауы мүмкін. Киберкеңістіктің пайда болуымен интернет пен ұялы телефонның көмегімен виртуалды ортада жүзеге асырылатын, қорқыныш тудыруға және сол арқылы бағынуға бағытталған буллингті, қорлауды, жәбірлеуді, физикалық немесе психологиялық террорды білдіретін кибербуллинг (bullying, bully – Dragon, Badger, grubyan, зорлаушы) сияқты құбылыс күшейе түсуде. Мектептегі буллинг әдетте сабақтан кейін басталады, бірақ интернетте қорлаушы кез келген уақытта құрбанын басып озуы мүмкін. Ақыр соңында, интернетте буллинг немесе қорлау техникалық тұрғыдан оңай жүзеге асырылады: зиянды

хабарлама жіберу немесе кең аудиторияға қол жетімді буллинг мәтінін жариялау үшін бірнеше рет жіберу. Сонымен қатар, нақты әлемнен айырмашылығы, виртуалдылық анонимділікке мүмкіндік береді және жазаның төмен ықтималдығын қамтамасыз етеді.

Соңғы уақытта кибербуллингтің негізгі алаңы әлеуметтік медиа болып табылады. Оларда адамды тек хабарламалар арқылы ғана қорлауға болмайды-жәбірленушінің парағы бұзылған (немесе оның атына жалған), онда жалған және қорлайтын мазмұн орналастырылған жағдайлар жиі кездеседі.

Көбінесе балалар бұл туралы ата-аналарға хабарлау жағдайды нашарлатады, нәтижесінде буллинг жағдайын қолдайды деп санайды.

Егер бала интернетте қорлауға тап болмаса да, бірақ интернет арқылы сөйлескенді ұнатса да, мұндай тәуекелдер алдын-ала талқылануы керек және алаңдаушылық туындаған кезде жасалуы керек әрекеттер туралы кеңес беруі керек.

Ең алдымен, бала интернетте, нақты өмірдегідей, әр адамның құрметпен қарауға құқығы бар екенін түсінуі керек, сондықтан басқа пайдаланушыларды жала жабуға немесе қорлауға тыйым салынады. Балаларға интернетте сөйлескен кезде олар басқа пайдаланушылармен достық қарым-қатынаста болуы керек екенін түсіндіріңіз. Ешқандай жағдайда дөрекі және қорлайтын жағымсыз сөздерді жазудың қажеті жоқ. Бірнеше рет басуды қажет ететін кейбір әрекеттерді болдырмау өте қиын және балалар жағдайдың қаншалықты ауыр болатынын түсінбеуі мүмкін. Бірақ қажет болған жағдайда анонимді пайдаланушыларды бақылауға болады.

Егер сіздің балаңыз «жағымсыз сұхбаттасушымен» жеке кездескен болса, сөйлесуді, электрондық пошта клиентін жабу немесе тіпті компьютерді өшіру арқылы байланысты үзуге болатындығын түсіндіру қажет. Егер мәселені бейбіт жолмен шешу мүмкін болмаса, бұл ресурстан мүлдем кетіп, жеке ақпаратыңызды сол жерден алып тастағаныңыз жөн болар. Бала мұндай адамдармен қарым-қатынасты жалғастыруға болмайтынын түсінуі керек (қорлайтын хабарламалар мен хаттарды оқып, оларға жауап беру), бірақ егер зиянды хабарламалар заңды бұзу болса (жеке адамға қарсы қылмыс), онда оларды сақтау және ересектерге көрсету қажет. Сонымен қатар, электрондық пошта бағдарламасының параметрлерін белгілі бір жіберушіден хабарламалар бөлек қалтаға түсетіндей етіп реттеуге болады. Бұл жағдайда балаға оларды оқудың қажеті жоқ. Егер сіз өзіңізді немесе балаларыңызды қорлайтын материалдарды тапсаңыз, бұл ақпаратты жою үшін сайт әкімшісіне (чат модераторына) хабарласыңыз. Егер мұндай жағдай болмаса немесе әкімші сізге жоюдан бас тартса, онда онымен және барлық беттердегі корреспонденцияның скриншоттарын қорлайтын ақпаратпен сақтаңыз және полицияға хабарласыңыз.

Әсіресе қауіпті адаммен жеке кездесу, онымен жыныстық қатынасқа түсуге итермелеу, бопсалау және қанау мақсатында достық қарым-қатынас орнату.

Балаларды осындай қауіптен қорғау үшін кейбір ережелерді сақтау қажет:

- Балаңызбен сенімді қарым-қатынаста болыңыз, сонда сіз баланың желіде кіммен сөйлесетінін үнемі біліп отырасыз. Баланың кімге «достық» тіркейтініне, кіммен желіде сөйлескенді ұнататынына назар аударыңыз – ол кімдер: құрдастары немесе өзінен үлкен адамдар болуы мүмкін.

- Балаңызға интернетте жеке сипаттағы ақпаратты (телефон нөмірі, үй мекен-жайы, мектеп атауы/нөмірі және т.б.) жарияламау, виртуалды таныстарыңызға фотосуреттеріңізді немесе бейнелеріңізді жібермеу керектігін түсіндіріңіз.

- Балаға тіркеуді қажет ететін ресурстарда (чаттарда, форумдарда, жедел хабар алмасу қызметтері арқылы, онлайн ойындарда) сөйлескен кезде нақты атауды қолданбаған дұрыс екенін түсіндіріңіз. Оған жеке ақпараты жоқ лақап ат таңдауға көмектесіңіз.

- Балаңызға интернеттен бейтаныс адамдармен кездесудің қауіптілігін түсіндіріңіз. Желіде адам өзін кез-келген адам ретінде көрсете алады, сондықтан интернет-досымен нақты кездесуге ересектердің сүйемелдеуімен бару керек.

- Баланың ер мен әйел арасындағы жыныстық қатынас тақырыбына деген танымдық қызығушылығын интернеттегі зиянкестер белсенді түрде қолданады. Осы тақырып бойынша балаңызбен өзіңіз сөйлесуге тырысыңыз. Оған адамдар арасындағы қалыпты қарым-қатынас сеніммен, жауапкершілікпен және қамқорлықпен байланысты екенін түсіндіріңіз, бірақ интернетте махаббат тақырыбы мүлдем дұрыс емес, ол дөрекі, зиянкестік әрекетте немесе арам пиғылда болатынын түсіндіру керек.

- Баланың сүйікті ісіне қатысуы, бос уақытын арнай алатын жасына сәйкес келетін іс-шараларға қатысуы маңызды.

Бесінші тәуекел-бақылаусыз сатып алу.

Интернет арқылы сатып алу бұл қауіп бүгінде өте өзекті. Балаға интернетте немесе ұялы телефон арқылы жасалған кез-келген сатып алуды ересек адам жасауы керек немесе оның рұқсатымен жүзеге асырылуы керек екенін түсіндіру қажет. Интернетте ұсынылатын осы немесе басқа қызметтерді пайдалану туралы әрқашан бірлесіп шешім қабылдаңыз.

Сонымен қатар, білместіктен, тәжірибесіздіктен, жарнаманың әсерінен бала ұялы шот арқылы сатып алулар жасай алады, сондықтан оператормен бірлесе отырып, баланың ұялы телефонында телефонға, SMS хабарламаларына немесе шығындарға қажетті құлыптарды орнатыңыз.

Алтыншы тәуекел -интернетке тәуелділік. Интернетке тәуелділік-желіден тыс болған кезде интернетке кіруге деген ұмтылыс және желіде болған кезде интернеттен шыға алмау.

- Интрузивті веб-серфинг – Бүкіләлемдік ғаламтордағы шексіз саяхат, ақпарат іздеу;

- Виртуалды қарым-қатынас пен виртуалды танысуға тәуелділік (хат-хабарлар, чаттарға, веб-форумдарға үнемі қатысу, желідегі таныстар мен достардың көптігі);

- Ойынға тәуелділік – желідегі компьютерлік ойындарға деген құмарлық;

- Ақша жұмсауға деген ұмтылыс – желіде құмар ойындар ойнау, интернет-дүкендерде қажетсіз сатып алу немесе интернет-аукциондарға үнемі қатысу;

- Интернет арқылы фильмдерді көруге тәуелділік;

- Киберсексуалдық тәуелділік – порно сайттарға кіруге және киберсекспен айналысуға тарту.

Әрбір бесінші бала интернетте уақыт өткізуге тырысады, интернетте бірнеше сағат бойы көп мақсатсыз отыру және оған қол жеткізе алмаған кезде өзін жайсыз сезінеді. 10% жағдайда балалар отбасын, достарын немесе мектепті елемейді, интернетте ұзақ отыруына байланысты ұйықтамау немесе тамақтанбау дағдысына айналады.

Не істеу керек? Ең алдымен, балаңызда интернетке тәуелділіктің мүмкін белгілеріне назар аудару керек.

- Ең алдымен, балаңыз желіде қанша уақыт өткізетінін, компьютерде жұмыс істеуге, сабақтарды аяқтауға, ұйықтауға, дұрыс тамақтануға, серуендеуге немқұрайлы қарамайтынын бағалаңыз.

- Балаңызбен интернетте не істейтіні туралы сөйлесіңіз. Әлеуметтік желілер толық жұмыс күнінің елесін жасайды – мысалы бала неғұрлым көп қарым-қатынас жасаса, достары соғұрлым көп болады, соғұрлым көп ақпарат алу, барлық хабарламаларға жауап беру, барлық оқиғаларды қадағалау, өзін көрсету т.б. Балаңыздың қызығушылығы нақты хоббимен қамтамасыз етіле ме, әлде ол ештеңені жіберіп алмауға тырысады ма және процестің өзі үшін жаңартуларды қадағалайды ма, соны анықтаңыз. Бала үшін желідегі қарым-қатынастың қаншалықты маңызды екенін және оның достарымен нақты қарым-қатынасты алмастыратынын білуге тырысыңыз.

- Интернеттен шыққаннан кейін балаңыздың көңіл-күйі мен мінез-құлқының өзгеруін бақылаңыз. Депрессия, ашуланшақтық, мазасыздық, қарым-қатынасқа құлықсыздық сияқты психикалық белгілердің көрінісі болуы мүмкін. Физикалық белгілердің ішінен мыналарды ажыратуға болады: бас ауруы, арқа ауруы, ұйқының бұзылуы, физикалық белсенділіктің төмендеуі, тәбеттің төмендеуі және басқалар.

- Мектеп психологымен және сынып жетекшісімен балаңыздың мінез-құлқы, оның үлгерімі және басқа оқушылармен қарым-қатынасы туралы сөйлесіңіз. Дабыл факторлары – оқшаулану, жасырыну, байланысқа түсуге құлықсыздық. Сабақ барысында балаңыздың телефонды немесе басқа мобильді құрылғыларды пайдаланып интернетке кіруге деген ұмтылысы бар-жоғын біліңіз.

Егер балаңызда интернетке тәуелділіктің мүмкін белгілерін тапсаңыз, келесі әрекет алгоритмін ұстануыңыз керек:

1. Баламен байланыс орнатуға тырысыңыз. Оның не қызықтыратынын, оны не мазалайтынын және т.б. біліңіз.

2. Балаңызға интернетті пайдалануға тыйым салмаңыз, бірақ пайдалану ережесін орнатуға тырысыңыз (баланың интернетте өткізетін уақыты, үй сабақтарын өткізгенге дейін желіде отыруына тыйым салу және т.б.). Ол үшін желідегі уақытты шектейтін арнайы ата-аналық бақылау бағдарламаларын пайдалануға болады.

3. Интернетке тек компьютермен немесе ортақ бөлмедегі компьютермен кіруді шектеңіз – бұл баланың желідегі әрекетін бақылауды жеңілдетеді. Балаңыздың қандай сайттарға кіретінін қадағалаңыз.

4. Балаңыздан бір апта ішінде интернетте өткізетін уақыттың не үшін жұмсалатынын егжей-тегжейлі жазып алуын сұраңыз. Бұл мәселені көрнекі түрде көруге және түсінуге, сондай-ақ кейбір жағымсыз әрекеттерден арылуға көмектеседі.

5. Балаңызды бірге бір нәрсе жасауға шақырыңыз, оны бір нәрсеге тартуға тырысыңыз. Кибершабуылды нақты өмірге жеткізуге тырысыңыз. Мысалы, көптеген компьютерлік ойындар үшін ұқсас үстел ойындары бар, оларды бүкіл отбасымен немесе достарымен ойнауға болады – бір-бірімен «жанды» сөйлескенде. Баланың бос уақытын арнай алатын интернетке байланысты емес хоббиі болуы маңызды.

6. Интернетке тәуелді балалар субъективті түрде желісіз жасай алмайтындығын сезінеді. Бұл туралы балаңызбен әдептілікпен сөйлесуге тырысыңыз. Егер жағдай болса, онымен қандай да бір себептермен интернетсіз жасауға мәжбүр болған жағдайды талқылаңыз. Баланың түсінуі маңызды – егер ол интернет-қоғамдастықтың өмірінен біраз уақытқа «ажырап кетсе» ештеңе болмайды.

7. Егер күрделі мәселелер туындаса, маманнан көмек сұраңыз.

Қорытындылай келе, интернетті пайдалану кезінде балаңызды қалай қорғауға болатындығы туралы жалпы ұсыныстарға келуге болады:

1. Компьютерді бүкіл отбасы үшін ортақ бөлмеге орнатыңыз

Бұл жағдайда интернет туралы сөйлесу және оның қолданылуын көру күнделікті өмірде табиғи болады. Егер компьютер ортақ бөлмеде болса, мәселелерді талқылау оңайырақ болуы мүмкін. Сонымен қатар, интернетті бірге пайдалануға болады.

2. Интернетті талқылаңыз

Интернетте де, нақты өмірде де баланың және оның достарының әрекеттеріне қызығушылық танытыңыз. Балаңызға интернетте мүмкін болатын әдемі және қызықты нәрселер туралы, сондай-ақ кездесетін қиындықтар туралы айтыңыз. Интернеттегі кез-келген жағдайда ынғайсыздық сезінсе, балаңызбен жасалуы керек әрекеттерді талқылаңыз.

3. Компьютерді пайдалану туралы көбірек біліңіз

Егер өзіңіз интернет қолданушысы болсаңыз, балаларға дұрыс тактиканы анықтау және оларға интернеттен пайдалы материал табуға көмектесу оңайырақ болады. Дегенмен, балалардың қауіпсіздігін қалай қамтамасыз ету керектігін білу үшін компьютерлік сауаттылық деңгейіңізді үнемі арттырыңыз

(мысалы, курстарға қатысу, арнайы әдебиеттерді оқу, сарапшылармен кеңесу). Отбасыңыздың барлық мүшелерін компьютерде және интернетте қауіпсіз жұмыс істеудің негізгі принциптерімен үнемі таныстырыңыз.

4. Интернетті бірге пайдаланыңыз

Балаларға қолайлы сайттарды табыңыз немесе пайдалы ақпаратты қалай табуға болатынын біліңіз: бірге саяхаттауды жоспарлаңыз, мектеп тапсырмаларына көмектесу үшін білім беру сайттарын шолыңыз немесе балалардың хоббиі туралы ақпаратты табыңыз. Интернеттегі веб-сайттарды бірге қарау балаға табылған ақпараттың маңыздылығын бағалауға көмектеседі. Таңдаулылар қалтасына сүйікті сайттарды қосуға болады, осылайша бұрын бірге қаралған веб-сайттарды бір рет басу арқылы ашуға болады.

5. Балаңызбен интернетті пайдалану әдісі мен уақыты туралы келіссөздер жүргізіңіз

Баламен компьютерде немесе телефонда өткізетін уақытын, сондай-ақ ол кіре алатын веб-сайттардың тізімін келісу пайдалы болуы мүмкін. Мұны балалармен талқылап, барлығына сәйкес келетін белгілі бір шешімге келу керек.

6. Баламен сенімді қарым-қатынас орнатыңыз

Бұл баланың интернетте жағымсыз тәжірибеге тап болуының салдарын болдырмауға көмектеседі. Баланың ата-анасымен жағымды эмоционалды байланысы оны болған оқиға туралы әңгімеге тартуға көмектеседі. Бала сізге сенуі керек және сіздің де алаңдайтыныңызды түсінуі керек және жағдайды түсініп, оған көмектескіңіз келеді, бірақ ешқандай жағдайда жазаламаңыз [38].

ИНТЕРНЕТ-КЕҢІСТІГІНДЕ КӘМЕЛЕТКЕ ТОЛМАҒАНДАР АРАСЫНДА ЗОРЛЫҚ-ЗОМБЫЛЫҚТЫ БОЛДЫРМАУҒА ҚАТЫСТЫ ПРОФИЛАКТИКАЛЫҚ ЖҰМЫС БОЙЫНША ӘДІСТЕМЕЛІК ҰСЫНЫМДАР

Интернет-кеңістікті пайдалана отырып, кәмелетке толмағандарға қатысты зорлық-зомбылықты болдырмау, профилактика субъектілерінің базаларында мамандармен психологиялық-ағартушылық жұмысты ұйымдастыру

Кәмелетке толмағандардағы зорлық-зомбылықтың, сондай-ақ агрессивті және құрбандық мінез-құлқының және жасөспірімдер арасында топтық қылмыстың пайда болуының алдын алу үшін жас ұрпақтың оң әлеуметтенуін қалыптастыру, кәмелетке толмағандардың қоғамнан алыстауын азайту маңызды мәселе болып табылады. Сондықтан жастардың бос уақытын ұйымдастыру дағдылары бар, бейресми жасөспірімдер - жастар топтары мен бірлестіктерінің көшбасшылары болуға қабілетті мамандар даярлауды талап ететін іс-шаралар өткізу, халықты БАҚ арқылы оң бағыттағы кәмелетке толмағандармен жұмыс топтары мен бағдарламалары туралы хабардар ету қажет.

Кәмелетке толмағандардың медиакомпетенциялары саласында балалармен жұмыс істейтін педагогтар мен басқа да мамандардың білімін жетілдіру – интернет-кеңістікті пайдалана отырып, кәмелетке толмағандарға қатысты зорлық-зомбылықтың алдын алудың неғұрлым тиімді тәсілі болуы мүмкін.

Психологиялық қызмет жұмысының ерекшелігі қазіргі заманғы интернет-технологиялар кеңістігінде кәмелетке толмағандар арасында кибербуллинг пен киберббингтің туындауының алдын алу бойынша профилактикалық жұмыс шеңберінде мамандардың ведомствоаралық өзара іс-қимылын ұйымдастыруға және тиімді іске асыруға мүмкіндік береді. Орталық интернет-технологиялар ортасында кәмелетке толмағандардың зорлық-зомбылығының алдын алу бойынша психологиялық-педагогикалық қызметке балалармен жұмыс істейтін педагогтар мен мамандарды даярлауды қамтамасыз етуге арналған ресурстарға ие.

Осы мақсатта психологиялық қызмет мамандары алдын алу субъектілерінің педагогтарымен және мамандарымен ағартушылық жұмыс бағдарламасын, сондай-ақ кәмелетке толмағандар арасында кибербуллингтің алдын алу жөніндегі мамандармен тақырыптық әңгімелер әзірлейді:

- Кәмелетке толмағандар арасындағы кибербуллингтің психологиялық себептері;
- Кәмелетке толмағандарда құрбандық мінез-құлқының қалыптасуының психологиялық себептері;
- Кәмелетке толмағандардың агрессивті мінез-құлқының қалыптасуының психологиялық себептері және т. б.

Кибербуллингтің алдын алу бойынша мамандармен тақырыптық әңгімелерге әдістемелік материалдар:

Кәмелетке толмағандар арасындағы кибербуллингтің психологиялық себептері интернет-технологиялар ортасында зорлық-зомбылық көрсетудің психологиялық себептері:

Қорқыныш: қорқытудың құрбаны болудан қорқу мобберлер болып табылатын белсенді топқа қосылуға мәжбүр етеді.

Бедел: бәрінің көз алдында болу, назар аудару қажеттілігі.

Қақтығыстар: көбінесе мәдениетаралық. Мәдени айырмашылықтар бірден дұшпандықты тудыруы мүмкін, бұл қақтығыстар әртүрлі белгілерге, мысалы, тілге, сыртқы келбетке және дәстүрге сәйкес кіші түрлерге бөлінеді.

Зерігу: жасөспірімдер көбінесе тек қана қобалжудан және зерігуден, не істеу керектігін білмей, өздерінің виртуалды беделін, мысалы, біреудің фотосуретіне теріс түсініктеме бере бастайды.

Күш: өз күшін көрсету басқа факторлармен қатар себеп болады, өйткені әр адамның өзінің артықшылығын көрсету, көрсету қажеттілігі бар, бірақ әр адамда бұл әртүрлі дәрежеде көрінеді.

Толық сезіне алмау: өзінің кемістік сезімі бойынша кілкіге қалу мүмкіндігі бар. Сондай-ақ, кемістігінен «жалтару» немесе оны кибербуллинг арқылы басқа адамға бағыттау мүмкіндігі бар.

Жеке дағдарыс: кибербуллингтің себебі достықтың бұзылуы, сондай-ақ махаббаттық қарым-қатынастардың бұзылуы, қызғаныш пен жеккөрушілік сезімі, мысалы, жіберілген қате немесе сәтсіздік болуы мүмкін.

1. Білім беру ұйымдарындағы кибербуллинг

Мұғалімдер мектепте кибермоббингтің жағдайлардың пайда болу кезеңін дер уақытында анықтай алмайды. Әдетте, мұғалімдер қақтығыстың ушығу кезеңінде кибермоббинг туралы өте кеш біледі. Мектептегі кибер террорды білудің алдын-алу шаралары қақтығыстарды жеңілдетуге және оның таралуына жол бермейді.

Мектептегі кибершабуылдың белгілері:

1. *«E-mail» анонимділігі:* оқушылар өздерінің мекен-жайларынан басқа адамдарға жасырын және ақысыз түрде қорлайтын хаттар жаза алады. Анонимді пошта жәшіктері басқа оқушыларды қудалау үшін жиі қолданылатындығын ескерген жөн.

2. *Психологиялық климаттың нашарлауы:* сыныптағы оқушылар арасындағы қарым-қатынас қыза түседі, қақтығыстар саны артады, содан кейін бұл кибербуллингтің пайда болуына негіз болады.

3. *Достық қарым-қатынас үзіледі.* Қыздар достықтың бұзылуына ең сезімтал болып табылады, өйткені олар бір-бірін бір-біріне қарсы пайдалану үшін жеткілікті жеке ақпаратты біледі.

4. *Мектеп іс-шаралары.* Түрлі экскурсиялық сапарлар, мерекелер, байқаулар және т.б. барысында сынып ұжымының қаншалықты ұйымшыл екендігі және тұлғааралық сынып ішіндегі қарым-қатынастардың «бұзылу шегі» қайда екендігі көрінеді.

Кибербуллинг құрбандарында көрінетін белгілер:

Денсаулық: денсаулық көрсеткіштері төмендейді. Оларға мыналар: бас ауруы, іштің ауыруы, ұйқы проблемалары, көңіл-күй проблемалары, оның ішінде көңіл-күйдің өзгеруі жатады.

Мінез-құлық: жасөспірімнің күтпеген жақындығы мен оқшаулануы, назарды нақты әлемнің сүйкімділігінен виртуалды әлемнің, ойын әлемінің құндылықтарына ауыстыру, оқу орнындағы үлгерімнің күрт төмендеуі алаңдаушылық тудыруы мүмкін.

Заттардың жоғалуы: оқушының жеке заттарының немесе оның ақшасының күтпеген жоғалуы, олардың жоғалып кетуін анықтау ата-аналарға қиын болмайды.

Кибертеррордың маңыздылығын төмендету: кибершабуыл құрбандары көбінесе ересектермен қарым-қатынас кезінде интернетте өзін қорлау жағдайларын жасырады.

Психологтарға арналған семинар бағдарламасы «эмоционалды салада бұзылыстары бар бастауыш мектеп жасындағы кәмелетке толмағандармен топтық жұмыстың ерекшеліктері»

Эмоционалды сала кіші мектеп оқушыларының дамуындағы маңызды компонент болып табылады. Егер оның қатысушылары, біріншіден, екіншісінің эмоционалды жағдайын «оқи» алмаса, екіншіден, олардың эмоцияларын басқара алмаса, ешқандай байланыс, өзара әрекеттесу тиімді болмайды.

Сіздің эмоцияларыңыз бен сезімдеріңізді түсіну өсіп келе жатқан адамның жеке басының қалыптасуындағы маңызды сәт болып табылады. Барлық қарапайым қарапайымдылықпен эмоцияларды тану және беру баладан белгілі бір білім мен даму деңгейін талап ететін өте күрделі процесс.

Психологтардың зерттеулері көрсеткендей, жас студенттер тұтастай алғанда адамның эмоционалды жағдайын дұрыс қабылдай алады, қайғы-қасіретті, қорқынышты және тандануды тануда қиындықтар туындайды. Эмоцияларды анықтау кезінде балалар пантомимикаға (позалар, қимылдар) мән бермей, бет әлпетіне назар аударады.

Осылайша, 7-9 жастағы балалардың эмоционалды, ішкі жағдайлары және олардың көріністері туралы түсініктері жеткіліксіз, көбінесе өзін-өзі реттеу және өзін-өзі бақылау дағдылары жоқ деп қорытынды жасауға болады. Бастауыш мектеп жасындағы балалардың жас ерекшеліктерін, рефлексия, эмпатия дағдыларын дамыту қажеттілігін ескере отырып, топтық жұмыс тиімді болып табылады. Эмоционалды проблемалар, егер оларды уақтылы түзету шаралары қабылданбаса, балалардың оқуда артта қалуы, үлгермеуі және әлеуметтік-психологиялық бейімделудің әртүрлі формалары пайда болатын негіз болып табылады. Балалардың эмоционалды сферасының бұзылуын түзету жұмысында ерекше орын арнайы құрылған түзету сабақтарына жатады. Топтық жұмысқа қатысу өз эмоцияларын және басқа адамдардың эмоцияларын тану қабілетін дамытуға, өз сезімдерін барабар білдіру дағдыларын дамытуға, өзін-өзі реттеу негіздерін, рефлексиялық және эмпатияны қалыптастыруға және

дамытуға, сондай-ақ қатысушылардан да, жүргізушілерден де барабар кері байланыс алуға ықпал етеді.

Мақсаты: психологтарды эмоционалды салада бұзушылықтары бар бастауыш мектеп жасындағы кәмелетке толмағандармен топтық жұмыстың ерекшеліктерімен таныстыру.

Семинар мазмұны: топтық және топтық жұмыстың теориялық аспектілерін, сондай-ақ практикалық жұмыс дағдыларын қарастыруды көздейді.

Формалары: дәрістер, тренинг жаттығулары.

Семинар жоспары:

Уақыты	Мазмұны
10.00-10.15	Топ қатысушыларымен танысу
10.15-11.30	Эмоционалды саладағы бұзылулар. Себептері, салдары, жою әдістері
11.40-13.00	Кіші топ жұмысы балалардың эмоционалдық саласындағы бұзушылықтарды түзетудегі маңызды және жауапты кезең ретінде (көшбасшыларды дайындау, топты жинау ерекшелігі, топтық жұмысқа көрсеткіштер мен қарсы көрсеткіштер)
13.00.-14.00	Үзіліс
14.00-15.30	Эмоционалды саладағы бұзушылықтарды түзетуге бағытталған топтық жұмыстағы динамикалық процестер (топтық жұмыс кезеңдері)
15.45-16.45	Эмоционалды саладағы бұзушылықты түзетуге бағытталған топтықжұмыс қатысушыларының жеке динамикасын талдау.
16.45 – 17.00	Кері байланыс, қорытынды жасау

Топтық тренингтік жұмыс бағдарламасын әзірлеу бойынша әдістемелік ұсынымдар

1. Негіздеме. Преамбула.
2. Мақсаты:
3. Міндеттері:
4. Жұмыс формасы:
5. Қатысушылар саны:
6. Бағдарламаның ұзақтығы:
7. Жұмыс тәртібі:
8. Бағдарламаның мазмұны:

Тренинг бағдарламасымен жұмыс кезеңдері

Мінез-құлық терапиясының қағидаларына сүйене отырып, кез-келген мінез-құлық бағдарламасының бастапқы нүктесі-бұл адамдардың көп немесе аз бөлігіне тән мінез-құлық проблемасы. Егер бұл адамдар тобы (мүмкін) осы мәселені шешуге қабілетті сұранысқа ие болса немесе Сіздің жұмысыңызға ақы

төлей алатын басқа ұйымдар болса, онда бағдарламаны әзірлеу белгілі бір перспективаларға ие.

Бұл жағдайда, мақсатты түрде төмендегідей іс-әрекеттер жасау керек:

1. Бағдарламаны әзірлеу мақсаттары мен перспективаларын айқындау.

1.1. Осы бағдарлама қандай клиенттер тобына арналғанын анықтаңыз және атаңыз.

1.2. Сіздің бағдарламаңызбен шешкіңіз келетін осы клиенттердің мәселелерін тұжырымдап, жазып алыңыз.

1.3. Клиенттермен кездесетін адамдардың мәселелерін тұжырымдап, жазып алыңыз.

1.4. Сіз қалыптастыратын немесе клиенттерден бас тарту керек болатын дағдыларды атаңыз.

Егер сіз осы тапсырманы дәл орындай алсаңыз, онда мінез-құлық бағдарламасын қалыптастыру перспективалары айқын және нақты.

«Үлгілер»

1) мерекелік үстелде ішу туралы тұрақты ұсыныстан бас тарта алмайтын адамдар.

2) кез-келген компанияда ол тез арада қажетсіз мас күйге түседі, бұл жағдайда бөртпе әрекеттер жасайды, алкогольге қосымша ақша жұмсайды, содан кейін өкінеді.

3) компаниядағы күтпеген «құлықтар» мен реніштер бұл адамды қонаққа шақырудан сақ болуға әкеледі. Отбасы бұл адамның мас күйінде жиі пайда болуынан зардап шегеді. Жұмыста олар оған сенуді тоқтатады. Мас күйінде машинаны басқаруға байланысты қауіп бар.

4) өзі үшін спирттің соңғы дозасын анықтау білігі және осы дозадан асырмай тойға қатысу білігі. Алкогольдің тұрақты ұсыныстарына жауап ретінде сыпайы және дәлелді түрде «жоқ» деп айта білу. Компанияда ішуге байланысты иррационалды, сенімді жою.

Клиенттер тобының үлгілері:

- емтихан немесе жауапты көпшілік алдында сөйлеу алдында шамадан тыс толқуды сезінетін адамдар;

- тәуелділіктен арылу үшін жеткілікті дағдылары жоқ адамдар;

- сыртқы келбетінен ұялатын және нәтижесінде әлеуметтік байланыстардан бас тартатын адамдар;

- өз қалаларында басқа ұлт немесе басқа дін адамдарының болуын жек көретін адамдар.

2. Әдебиеттер талдауы.

Әрине, сіз алкогольизм немесе діни шовинизм сияқты мәселе бойынша тиісті әдебиеттермен танысуыңыз керек. Егер сіз өзіңіздің мақсаттарыңызға толық сәйкес келетін жарияланған бағдарламаны таба алсаңыз, үлкен сәттілік болады. Әдебиеттерден сізді қызықтыратын мінез-құлық бұзылыстарының мәні туралы ең маңызды ақпаратты жазыңыз, сонымен қатар мамандар ұсынған оларды жеңу жолдарын схемалық түрде суреттеу мағынасы бар. Барлық мүмкін

ақпарат көздерін, соның ішінде Интернетті тексеріңіз, осы саладағы белгілі мамандардан көмек сұраңыз.

Егер осы жұмыстың нәтижесінде қызықты ештеңе табылмаса-мінез-құлық жаттығуларының стандартты тақырыптарын қолдануға тырысыңыз немесе проблемалардың жеке, авторлық шешімдерін табуға тырысыңыз.

3. Дағдыларды нақтылау.

Енді сіз өзіңіздің бағдарламаңызда үйрететін Дағдылар мен олардың элементтерін нақтылауға кірісе аласыз. Мүмкіндігінше кішігірім және нақты сипатталған дағдыларды бөліп көрсетуге тырысыңыз. Мүмкін болса, белгіленген дағдыларды ұйымдастырыңыз, бірінші және маңызды дағдыларды атап өтіңіз.

4. Дағдылардың танымдық негізін анықтау.

Клиенттерге шеберлікті көрсету үшін қолданылатын дағдылардың мәтіндік немесе графикалық сипаттамасын дайындаңыз.

5. Демонстрациялық рөлдік ойындарды дайындау.

2-3 демонстрациялық рөлдік ойындардың сипаттамасын дайындаңыз және осы ойында орындалуы керек сценарийді жазыңыз. Бұл сценарийді ко-жаттықтырушымен 3-4 рет ойнаңыз және кез-келген бейтаныс адамдардан осы сценарийде көрсетілетін шеберліктің мағынасы туралы мүмкіндігінше көп сұрақтар қойыңыз.

Бұл сізге шеберліктің танымдық компонентінің мазмұнын пысықтауға көмектеседі.

Өзін-өзі талдау

6. Рөлдік ойындарды дайындау.

Кем дегенде 6 Қауіпсіздік рөлдік ойындарын әзірлеңіз және оларды қиындату немесе жеңілдету нұсқаларын қарастырыңыз. Сақтандыру рөлдік ойыны арқылы біз негізгі демонстрациялық рөлдік ойынға балама бола алатын әлеуметтік жағдайдың сипаттамаларын түсінеміз. Бұл сақтандыру рөлдік ойындарының мәні мынада: жаттықтырушымен бірнеше рет ойнағаннан кейін, негізгі жағдай топты жалықтыруы мүмкін. Бұл жағдайда шеберліктің өзін сақтай отырып, сақтандыру жағдайлары қолданылады.

Сақтандыру рөлдік ойындарының сценарийлері серіктес пен бас кейіпкердің нұсқауларымен бірге карталарға басып шығарылады. Картаның артқы жағында жағдайды жеңілдету немесе қиындату нұсқаларын белгілеңіз.

1. БАЛАЛАРДЫҢ КИБЕРМӘДЕНИЕТІНЕ ҚАТЫСТЫ ЖАҒЫМДЫ ӘДЕТТЕРДІ ҚАЛЫПТАСТЫРУ БОЙЫНША СЫНЫП САҒАТЫТАРЫ МЕН СЫНЫПТАН ТЫС ІС-ШАРАЛАР ҮЛГІСІ

Мақсаты: Балалардың кибермәдениетке қатысты жағымды әдеттерін қалыптастыру. Адамдарға құрмет, адалдық пен жауапкершілік, жеке өмірін қорғау, интернетті жағымды мақсатта пайдалануға дағдыландыру.

Міндеттері:

- Балаларды кибермәдениет негіздерімен таныстыру;
- Балаларда сыни ойлауды және интернетте алынған ақпаратты бағалау қабілетін дамыту;
- Балаларда интернетте қауіпсіз және жауапты мінез-құлық дағдыларын қалыптастыру.

Әдістері:

- Әңгімелер
- Ойындар
- Жобалық қызмет
- Көркем шығармалармен жұмыс

Материалдар:

- Компьютерлер
- Интернет
- Презентациялар
- Бейнелер
- Ойыншықтар
- Кітаптар

Жұмыс жоспары:

1 кезең:

- Кибермәдениет негіздерімен танысу.
- Интернеттегі мінез-құлық ережелерін талқылау.

2 кезең:

- Сыни ойлауды дамыту және интернетте алынған ақпаратты бағалау мүмкіндігі.
- Балаларды интернеттегі қауіпті жағдайларды тануға және болдырмауға үйрету.

3 кезең:

- Интернетте қауіпсіз және жауапты мінез-құлық дағдыларын қалыптастыру.
- Балаларды жеке өмірін қорғауға үйрету.

Нақты іс-шаралар үлгісі:

1. «Интернеттегі мінез-құлық ережелері» әңгімесі

Мақсаты: білім алушыларды кибермәдениет негіздерімен таныстыру.

Әңгіме барысы:

Педагог балаларға кибермәдениеттің не екенін және оның не үшін маңызды екенін түсіндіреді.

Педагог балаларға интернеттегі мінез-құлық ережелері туралы айтады, мысалы, басқа адамдарға құрмет, адалдық пен жауапкершілік, жеке өмірін қорғау, интернетті жағымды мақсатта пайдалану дағдыларын қалыптастыру.

2. «Интернет-сауалнама» ойыны

Мақсаты: балаларда сыни ойлауды және интернетте алынған ақпаратты бағалау қабілетін дамыту.

Ойын барысы:

Педагог білім алушыларға қызығушылық тудыратын тақырып бойынша интернет-сауалнама жүргізуді ұсынады.

Білім алушылар сауалнама тақырыбын таңдап, сұрақтар қояды.

Білім алушылар сауалнама жүргізеді және нәтижелерді талдайды.

3. «Менің қауіпсіз Интернетім» жобасы

Мақсаты: Білім алушылардың интернеттегі қауіпсіз және жауапты мінез-құлық дағдыларын қалыптастыру.

Жобаның барысы:

- Білім алушылар интернеттегі қауіпсіз мінез-құлыққа арналған жоба әзірлейді.

- Жоба плакаттарды, парақшаларды, презентацияларды, бейнелерді қамтуы мүмкін.

- Білім алушылар өз жобаларын сынып жиналысында немесе басқа форматтарда ұсынады.

-

4. Көркем шығармалармен жұмыс

Мақсаты: Білім алушылар кибермәдениетке деген оң көзқарасын қалыптастыру.

Жұмыс барысы:

- Педагог білім алушыларға кибермәдениет туралы әңгімелер, ертегілер, өлеңдер оқиды.

- Балалар оқығандарын талқылайды, өз әсерлерімен бөліседі.

Қорытынды:

Білім алушыларға кибермәдениетке қатысты жағымды әдеттерді қалыптастыру ата-аналар, тәрбиешілер және басқа ересектер үшін маңызды міндет болып табылады. Біртұтас тәрбие беру барысында балаларға интернетті қауіпсіз және жауапкершілікпен пайдалануға көмектесе аламыз.

*«Білім алушыларда кибермәдениет дағдыларын қалыптастыру»
тақырыбы бойынша сыныптан тыс іс-шаралар үлгісі*

Қазіргі жағдайда, балалар жас кезінен бастап цифрлық технологияларға тап болған кезде, олардың кибермәдениетке қатысты жағымды әдеттерін қалыптастыру ата-аналар, тәрбиешілер және басқа ересектер үшін маңызды міндет.

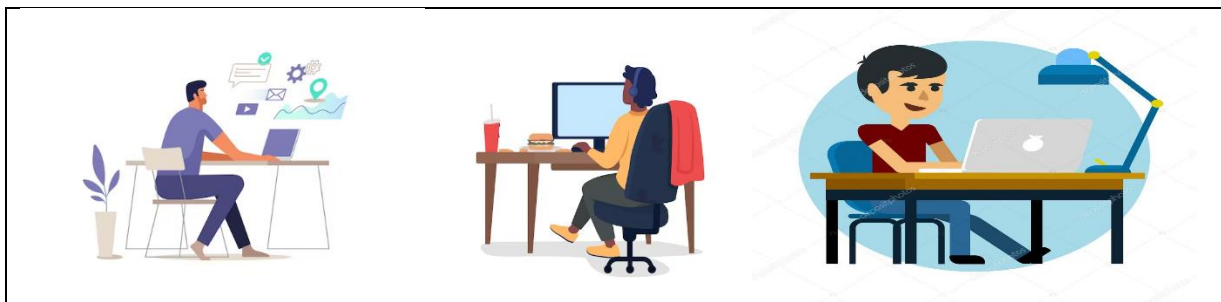
Кибермәдениет дегеніміз не?

Кибермәдениет – бұл адамдардың интернеттегі мінез-құлқын реттейтін нормалар мен құндылықтардың жиынтығы. Кибермәдениет келесі аспектілерді қамтиды:

Этика. Кибермәдениет басқа адамдарға құрмет, адалдық және жауапкершілік сияқты онлайн мінез-құлық этикасын сақтауды қамтиды.

«Интернеттегі этикалық нормалар»

Интернет бүкіл адамзаттың меншігіне айналды. Интернеттің иесі жоқ, өйткені ол әртүрлі географиялық байланыстары бар желілердің жиынтығы. Интернеттің көптеген пайдалы және зиянды қасиеттері бар, оларды мүдделі адамдар пайдаланады.



2011 жылдың 3 маусымында Интернетке қол жетімділікті адамның негізгі құқығы деп таныған БҰҰ қарары қабылданды. Осылайша, белгілі бір аймақтарды интернеттен ажырату адам құқықтарын бұзу болып табылады.



Интернет, ең алдымен, ақпаратты ашық сақтау және тарату құралы.

Адам ақпараттық қоғамда өмір сүреді, сондықтан ол ақпарат, оны пайдалану, беру туралы заңдарды білуі және орындауы керек. Ал ақпарат өз кезегінде құқықтық реттеу объектісі болып табылады.



Интернеттің жаһандық сипаты қандай органдар құқықтық мәселелер бойынша дауларды қарауы керек екенін анықтауда күрделі қиындықтар туғызады. Бірақ ең қызығы, интернетте біртұтас басқару орталығы мүлдем жоқ болса да, ол біздің өмірімізде сәтті дамып, көбірек орын алуда.



1. Интернет құқығы – бұл интернет желісіндегі құқықтық қатынастарды реттейтін әртүрлі құқықтық нормаларды қамтитын құқықтық ойдың бағыты.

Жалпы интернетке қатысты кейбір жалпы Нормативтік құқықтық актілер жасалды. Атап айтқанда:

1. Бүгінгі таңда қолданыстағы барлық нормативтік (заңға тәуелді) актілер желінің жұмыс істеуінің жекелеген жағдайларын реттейді, яғни бүкіл интернетке қатысты жалпы заң жобасы жоқ.

2. Интернет үшін зияткерлік және өнеркәсіптік меншіктің заңнамалық актілеріне қатысты нормалар өзекті.

3. Интернеттің аумақтық шектеулері болмағандықтан, сәйкесінше халықаралық (мемлекетаралық) деңгейде құқықтық қатынастарды реттеу жоқ.

Әр түрлі елдердегі бірдей мәселе әр түрлі жолмен шешілуі мүмкін. Бір елде бір нәрсе бар, ол мүлдем заңды, ал екіншісінде қылмыстық жазалануы мүмкін.



Сонымен қатар, интернетте орналастырылған барлық ақпарат Жердің кез келген жерінде кез келген адамға қол жетімді болуы мүмкін екенін ескеру қажет. Мысалы, AliExpress Интернет-дүкені, мұнда әлемнің барлық адамдары сатып алушылар болып табылады, олар орыстар, белорустар, немістер, американдықтар және басқалар. Бұл жағдайда сатушы үшін жергілікті соттарда орын алуы мүмкін дауларды шешу үшін клиенттер елдерінің заңнамасын білу өте маңызды.



Алайда, егер адам мен мемлекет арасында байланыс болса, онда, әрине, мемлекет адамға өзінің юрисдикциясын белгілейді, яғни бұл жағдайда адам өзінің аумағында орналасқан Мемлекеттің заңы бойынша интернеттегі қызметі үшін жазалануы мүмкін.



Ақпаратты белгілі бір серверге жиі орналастыру арқылы адам өзі мен аумақ арасында байланыс орнатады, бірақ бұл әрдайым бола бермейді. Серверді орналастыру елі домендік атауды тіркеу елімен сәйкес келмеуі мүмкін, сонымен қатар домендік атаудың иесі интернетте осы домендік атауды қолданатын компьютерді біріншісіне қатысты әлемнің мүлдем басқа бөлігінде орналасқан басқа компьютермен оңай алмастыра алады.

Бұл жағдайларды интернет саласындағы ұлттық және аймақтық заңнамаларды толық біріздендіру арқылы ғана жеңуге болады.

2. Интернеттегі Этика.

Қарым-қатынастағы барлық адамдар өздерінің білім, даму және білім деңгейіне сәйкес әрекет етеді.

Бірақ интернет әлемнің кез-келген нүктесінен адаммен сөйлесуге және сонымен бірге логиннің артында жасырын қалуға мүмкіндік беретіндіктен, барлық қол жетімділік пен рұқсат сезімі пайда болады. Сондықтан адамдар көбіне агрессивті және дөрекі әрекет ете бастайды.



Сондықтан электрондық поштаның пайда болуымен қатар желілік этикет ұғымы енгізілді. Содан кейін интернеттің дамуымен желілік этикетте көрсетілген ережелер барлық мүмкін форумдарға, телеконференцияларға, сайттарға, чаттарға және т.б. таралды.

Желілік этикет («сетикет, нетикет» деп те аталады) – бұл мінез-құлық ережелері, желідегі байланыс, дәстүрлер және көпшілік ұстанатын интернет-қоғамдастық мәдениеті.



Этикет ережелері жалпыға бірдей емес және қатаң түрде белгіленбейді – әр түрлі қауымдастықтарда олар әр түрлі болуы мүмкін.

Этикеттің негізгі мақсаты қоғамдағы қарым-қатынасты қиындатпау болғандықтан, ережелер қоғамдастықтың мақсаттарына, қабылданған қарым-қатынас стиліне, техникалық шектеулерге және т.б. негізделуі мүмкін. Кейбір ережелер жазылады, тіпті ресми жарғы түрінде, кейде жай тізім түрінде жасалады, басқа ережелер еш жерде жазылмаған, бірақ қоғамдастық мүшелерінің көпшілігіне белгілі және қатаң сақталады.

Көбінесе, этикеттің айқын бұзылуы деп қорлау және жеке тұлғаға ауысу, тақырыптан зиянды кету (офтопиялық), жарнамалар мен өзіне арналмаған жерлерде өзін-өзі жарнамалау түсініледі. Сондай-ақ, жала жабу және басқа да зиянды жалған ақпарат (алдау) немесе плагиат этикетті бұзуы мүмкін.

Жалпы этикет ұсыныстарын үш санатқа бөлуге болады:

1. Психологиялық, эмоционалды – «сен» немесе «сіз»-ге жүгіну, эмодзилерді пайдалану және қанша мөлшерде қолдану, телефондарда аймақ кодын көрсету, жаңадан бастаушыларға қолдау көрсету немесе олардың сұрақтарын елемей және т.б.

2. Техникалық, ресімдеу – белгілі бір ұзындықтағы жолдарды пайдалану, транслитті пайдалану, хабарлама немесе қолтаңба өлшеміне шектеулер, кеңейтілген форматтауға рұқсат беру (курсивпен, түспен, фонмен, жақтаулармен қою және т.б.), бас әріптермен хабарлама жазуға рұқсат беру және т. б.

3. Әкімшілік-тақырыптарды атау ережелері, дәйексөз ережелері, жарнаманың рұқсат етілуі, сілтеменің рұқсат етілуі (яғни дау үшін дау), қоғамдастық тақырыбын ұстану қажеттілігі және т.б.



Алайда, бір желілік қауымдастықтың ережелеріне үйренген адамдар байқаусызда екіншісінің ережелерін бұзуы мүмкін. Сондықтан барлық дерлік интернет-қауымдастықтар ережелермен танысуды және оларды сақтауға ресми келісімін білдіруді талап етеді.



Электрондық поштаны жазу ережелері үлгісінде интернеттегі қарым-қатынастың негізгі ережелерін бөліп көрсетейік:

- Электрондық поштаны жазу кезінде «тақырып» өрісін толтыру этикалық болады, өйткені тақырыптарды басшылыққа ала отырып, бүкіл тізімнен қажетті электрондық поштаны табу оңайырақ. Поштамен жұмыс істеуге арналған көптеген бағдарламалар, бұл фразаны өздері – автоматты түрде енгізеді.

- Егер хатқа жауап ретінде сіз фразаны келтіруіңіз керек болса, оны қандай да бір символмен, мысалы, үлкенірек белгімен таңдап, бос жолмен фразаларыңыздан бөлуге болады. Тағы да, көптеген бағдарламалар мұны автоматты түрде жасайды.

- Егер сіз мәтінді үлкен әріптермен жазсаңыз, интернетте сіз қатты айқайлап жатырсыз деп ойлайсыз. Оқудың ыңғайлылығына көп көңіл бөлінеді, мысалы, егер сіз бас әріптермен хабарлама жазсаңыз, бұл оқырманға оқуға ыңғайсыздық тудырады.

- Егер электрондық пошта ресми болса, онда хаттың авторы туралы ақпаратты қамтитын қолтаңбаны пайдалану маңызды: Толық аты-жөні,

лауазымы, байланыс ақпараты. Көптеген бағдарламалар дайын қолтаңбаны сақтауға және оны автоматты түрде қосуға мүмкіндік береді, сондықтан барлық адресаттарға көрсеткіңіз келетін ақпаратты қолтаңбаға қою өте маңызды.

- Грамматикалық қателіктер жібермеу өте дұрыс болады. Электрондық поштамен жұмыс істеуге арналған көптеген мәтіндік бағдарламаларда емлені тексерудің кіріктірілген жүйелері бар. Бірақ, әрине, әрдайым бағдарламаға үміттенудің қажеті жоқ, жібермес бұрын хатты мұқият оқып шығу керек.

- Үлкен көлемді файлдары бар электрондық поштаны жіберудің қажеті жоқ, оларды бірнеше шағын файлдарға бөліп, жеке электрондық пошталармен жіберген дұрыс.

- Кәдімгі корреспонденцияда біз смайликтерді жиі қолданамыз – бұл мәтіндік таңбалардың тіркесімі, яғни біз смайликтерді қолданған кезде, хат жанды болып шығады, бірақ электрондық поштадағы эмодзилерді асыра пайдалану жағымсыз болып саналады.

Бүгінгі таңда көптеген смайликтер бар, бірақ ең көп таралғаны:

- қуанышты білдіретін күлімсіреу;
- қайғы, өкініш немесе көңілсіздік білдіреді;
- иронияны білдіретін көзді қысатын тұлға, яғни сөздерді сөзбе-сөз қабылдаудың қажеті жоқ.

Интернеттегі қарым-қатынас этикетінің ережелері.

Интернеттегі ақпарат алмасу мен байланыстың танымал құралдары- блогтар, форумдар, чаттар, телеконференциялар.

Сондай-ақ, қазіргі уақытта интернет желісінде әртүрлі әлеуметтік қызметтер кеңінен қолданылады, бұл олардың пайдаланушыларына ақпарат алмасуға және желіде бірлескен қызмет жүргізуге мүмкіндік береді.

Интернеттің әлеуметтік қызметтеріне мыналар жатады: әлеуметтік желілер, мультимедиялық ресурстарды сақтауға арналған қызметтер, әлеуметтік бетбелгілер, құжаттармен бірлесіп жұмыс істеуге арналған қызметтер.

Әлеуметтік медиа мүдделері немесе қызметі ұқсас адамдардан тұратын онлайн қауымдастықтар құруға бағытталған. Ең танымал әлеуметтік желілер, ең алдымен, достар, бұрынғы сыныптастар мен курстастарды, сондай-ақ мұғалімдерді табуға арналған.



Осы ақпарат алмасу құралдарының барлығы белгілі бір тақырып бойынша мүмкіндігінше көп адамдармен сөйлесуге бағытталған. Сондықтан өз пікіріңізді сыпайы және дұрыс айту өте маңызды. Егер оның пікірі сіздікінен өзгеше болса, адамға шабуыл жасаудың қажеті жоқ.



Мұнда сіз өзіңіздің бүркеншік атыңызды немесе лақап атыңызды таңдауыңыз керек (бұл ағылшын тілінен *Nickname*-лақап ат дегенді білдіреді), ол сіздің жынысыңызды түсінеді және сонымен бірге лақап ат басқа мүшелерге қатысты дұрыс болуы керек, яғни олардың сезімдерін қорлаудың қажеті жоқ.

Егер сіз біреуге жүгінсеңіз, оны жазыңыз лақап ат фразаның басында. Егер сіз мәтінді бас әріптермен немесе көптеген леп белгілерімен жазсаңыз, бұл сіздің айқайлағаныңызды білдіреді.

Чаттан шыққанда өмірдегі сияқты, әңгімелесушілермен қоштасыңыз және қажет болса, келесі бірлескен әңгіменің уақыты туралы келіссөздер жүргізіңіз.

Интернетті пайдалану кезіндегі негізгі мінез-құлық ережелерін шағын жадынамаға біріктірейік:

1. Өзіңізді анық көрсетіңіз, анонимділікке жол бермеңіз.
2. Адресатыңызды құрметтеңіз. Нақты өмірдегідей стандарттарды ұстаныңыз.
3. Сауатты және қысқаша жазыңыз. Қойылған сұраққа нақты жауап беріңіз.
4. Басқалардың уақыты мен мүмкіндіктерін құрметтеңіз.
5. Бас әріппен жазбаңыз. Мұндай жазба айқай ретінде қабылданады. Сонымен қатар, мұндай мәтін нашар оқылады.
6. Қақтығыстарға араласпаңыз және оларға жол бермеңіз. Эмоциялардың әсерінен жасалған хабарламаларды жіберуден аулақ болыңыз. Басқалардың қателіктерін кешіруді үйреніңіз.
7. Хат алмасудың толық құпиялылығына үміттенбеңіз.
8. Сыпайылық ережелерін сақтаңыз. Есіңізде болсын, сіз әрқашанда өмірдегідей адаммен сөйлесесіз.

3. Қарым-қатынас стилі. Кибермәдениет интернеттегі қарым-қатынас стилін анықтайды, ол құрметті, мейірімді және сындарлы болуы керек.

«Интернеттегі қарым-қатынас стилі»

Интернет ерекше коммуникативті орта ретінде және тілді жүзеге асырудың бұрын болмаған саласы ретінде өзімен бірге қарым-қатынастың жаңа тәсілдерін, сөйлеу мінез-құлқының стереотиптерін, тілдің өмір сүруінің жаңа формаларын әкелді. Интернет сілтемелермен байланысты мәтін, бейне және аудио ақпараты бар көптеген құжаттармен толтырылған, ол сызықтық емес, интерактивтілік, имманенттілікпен сипатталады.

Интернеттің тілі ауызша және жазбаша сөйлеу формасының белгілерін біріктіре отырып, олардан ерекшеленеді. Бұл байланыс құралы басқа құралдар жасай алмайтын нәрсені жасай алады, сондықтан оны коммуникацияның жаңа түрі ретінде қарастыру керек. Д. Кристал қарым-қатынастың бұл түрінің мәнін өзіндік формуламен сипаттады: «ауызша сөйлеу формасы + жазбаша сөйлеу формасы + компьютер арқылы жүзеге асырылатын белгілер» [39].

Электрондық мәтіндер басқа мәтіндерге ұқсамайды. Олар сәйкессіздікті, синхрондылықты анықтайды, өйткені олар көптеген компьютерлерде бірден қол жетімді. Электрондық мәтіндер мәтіннің басқа мәтіндердің ішінде біріктірілу немесе басқа мәтіндерге сілтемелер болуы мүмкіндігіне байланысты өткізгіш шекараларға ие. Барлық осы ерекшеліктер тілге із қалдырады және ауызша және жазбаша сөйлеу формасына тән белгілермен бірге интернет тілін қарым-қатынастың нағыз үшінші құралы етеді. Арнайы желілік этикет, теруге мүмкіндік беретін стиль, латын және кириллица, аббревиатуралар, транслитерацияны қолдану және т.б.

4. Құндылықтар. Кибермәдениет толеранттылық, ынтымақтастық және шығармашылық сияқты құндылықтарды насихаттайды.

Интернеттегі құндылықтар

Құндылықтар мәдениетті бейнелейтін негізгі құбылыстар болып табылады.

Электрондық және ақпараттық-коммуникациялық технологияларды пайдалануды зерттеуде мәдени контекстті талдау өте маңызды. Себебі ақпараттық технологияларды енгізу мен қолданудың қаншалықты сәтті болатынын анықтауда мәдени құндылықтар маңызды рөл атқарады.

Бұл мәдени ерекшеліктер белгілі бір ақпараттық технологияларды қабылдау ерекшелігін және сәйкесінше белгілі бір ақпараттық технологияны таңдауды анықтайтындығына байланысты. Электрондық байланыс құралдарын таңдауда мәдениет маңызды рөл атқарады (мысалы, факс немесе электрондық пошта)

Құндылықтарды қоғам дамуының маңызды материалдық емес активтерінің бірі деп атауға болады. Олар адамдардың мінез-құлқын басқарады, сонымен қатар көптеген зерттеулерде көрсетілген экономикалық дамуға айтарлықтай әсер етеді[42].

Тиісінше, қоғамдағы белгілі бір өзгерістер адамдардың негізгі құндылықтарына қалай әсер ететінін түсіну маңызды.

5. Балаларда кибермәдениетке қатысты жағымды әдеттерді қалай

қалыптастыруға болады?

Балалардың кибермәдениетке қатысты жағымды әдеттерін қалыптастыру үшін:

- Балаға үйретуді жас кезінен бастау керек. Балалар кибермәдениет туралы мүмкіндігінше ертерек білуі керек.
- Кешенді тәсілді қамтамасыз ету. Үйрету кибермәдениеттің барлық аспектілерін қамтуы керек.
- Тәрбиенің әртүрлі әдістерін қолданыңыз. Кибермәдениетке тәрбие балалар үшін қызықты және тартымды болуы керек.
- Ата-аналар мен мұғалімдерді тарту. Ата-аналар мен мұғалімдер балаларды кибермәдениет туралы оқытуда маңызды рөл атқарады.

Тәрбиенің нақты әдістері:

Балаларға кибермәдениет туралы білім беру үшін келесі әдістерді қолдануға болады:

Әңгімелер мен талқылаулар. Әңгімелер мен пікірталастар балаларға кибермәдениет принциптері туралы білуге және оларды ата-аналармен немесе мұғалімдермен талқылауға мүмкіндік береді.

Ойындар мен викториналар. Ойындар мен викториналар балаларға кибермәдениет туралы алған білімдерін ойын түрінде бекітуге көмектеседі.

Мультфильмдер мен бейнелерді қарау. Мультфильмдер мен бейнелер балаларға кибермәдениет принциптерін көрнекі түрде көрсетуге көмектеседі.

Кітаптар мен мақалаларды оқу. Кітаптар мен мақалаларды оқу балаларға әртүрлі дереккөздерден кибермәдениет туралы көбірек білуге мүмкіндік береді.

Кибермәдениет туралы кітаптар

Әйгілі американдық публицист Марк Дери өзінің шығармаларында кибермәдениет құбылыстарының кең ауқымын қарастырады. 90-шы жылдардағы кибермәдениеттің 60-шы жылдардағы контрмәдениетпен байланысы, компьютерлік технологияның өнердің барлық бағыттары – электронды музыка мен роботомәдениеттің қалыптасуына әсері туралы баяндайды. Жеке кітаптарды, картиналарды, қондырғылар мен тәжірибелерді талдай отырып, автор қазіргі заманғы кибермәдениет адамзатты адам табиғатының эволюциясын басқаруға апаратын жолдармен күресуге тырысады.

Кибермәдениет туралы сабақ тақырыптарының үлгілері:

1. «Интернеттегі этикалық нормалар» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Интернетте қандай этикалық нормаларды сақтау керек?
- Кибербуллингке қалай қарсы тұруға болады?
- Интернеттегі адамдар арасындағы қарым-қатынас қандай болуы керек?

2. «Интернеттегі қарым-қатынас стилі» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Интернеттегі сындарлы диалогты қалай құруға болады?
- Интернетте қандай сөздер мен сөз тіркестерінен аулақ болу керек?

- Интернетте қандай эмоциялар болуы керек?

3. «Интернеттегі құндылықтар» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Интернетте қандай құндылықтарды насихаттау керек?

- Интернеттегі жеккөрушілікті насихаттауға қалай қарсы тұруға болады?

- Интернеттегі түрлі мәдениеттер арасындағы қарым-қатынас қандай болуы керек?

Балалардың кибермәдениетке қатысты жағымды әдеттерін қалыптастыру ата-аналар, тәрбиешілер және басқа ересектер үшін маңызды міндет. Білім беру ұйымдарында педагог, ата-ана, білім алушылар арасында кибермәдениетке қатысты жағымды әдеттерге байланысты іс-шараларды жиі ұйымдастырған дұрыс. Бұл білім алушылардың қоғамда әлеуметтік да, сондай-ақ цифрлық әлемде де мәдени деңгейін көтеруге ықпал етеді.

2. БАЛАЛАРҒА КИБЕРГИГИЕНАҒА ҚАТЫСТЫ ТҮСІНІКТЕРІ МЕН ДАҒДЫЛАРЫН ҚАЛЫПТАСТЫРУ БОЙЫНША СЫНЫП ТЫС ІС- ШАРАЛАР ҮЛГІСІ

Цифрлық технологиялар барған сайын маңызды рөл атқаратын қазіргі әлемде балалардың кибергигиенаға қатысты жағымды әдеттерін қалыптастыру ата-аналар, тәрбиешілер және басқа ересектер үшін маңызды міндет болып отыр.

Кибергигиена дегеніміз не?

Кибергигиена – бұл цифрлық технологияны қолданумен байланысты физикалық және психологиялық мәселелерден қорғануға көмектесетін ережелер мен процедуралардың жиынтығы.

Кибергигиена келесі аспектілерді қамтиды:

Физикалық денсаулық. Кибергигиена физикалық денсаулықты сақтауға көмектесетін цифрлық технологияларды қолдану ережелерін сақтауды қамтиды, мысалы, балалардың интернетте өткізетін уақытын шектеу, дұрыс қалып ережелерін сақтау. Кибергигиена балалардың физикалық денсаулығын қорғауға көмектесетін ережелерді сақтауды қамтиды, мысалы, балалардың компьютерде өткізетін уақытын шектеу, дұрыс қалып және қол гигиенасы. т. б.

Психикалық денсаулық. Кибергигиена сонымен қатар балалардың психикалық денсаулығын сақтауға бағытталған, мысалы, цифрлық тәуелділіктің алдын алу, сыни ойлауды қалыптастыру және т. б.

Кибергигиена сонымен қатар балалардың психикалық денсаулығын қорғауға көмектесетін ережелерді сақтауды қамтиды, мысалы, балалардың интернетте өткізетін уақытын шектеу және цифрлық тәуелділіктің алдын алу.

Балаларда кибергигиенаға қатысты жағымды әдеттерді қалай қалыптастыруға болады?

Кибергигиена бойынша нақты тақырыптық сабақ үлгілері:

1. «Физикалық денсаулық және цифрлық технологиялар» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Цифрлық технологияны пайдалану кезінде физикалық денсаулықты қалай сақтауға болады?
- Цифрлық тәуелділікті қалай болдырмауға болады?
- Цифрлық технологиялармен айналысу үшін қауіпсіз жұмыс орнын қалай ұйымдастыруға болады?

2. «Психикалық денсаулық және цифрлық технологиялар» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Өзіңізді цифрлық технологияның теріс әсерінен қалай қорғауға болады?
- Цифрлық технологияны қолдану кезінде сыни ойлауды қалай дамытуға болады?

- Шығармашылықты дамыту үшін цифрлық технологияны қалай пайдалануға болады?

3. «Интернеттегі физикалық денсаулық» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Компьютерде қанша уақыт өткізуге болады?
- Компьютерде қалай дұрыс отыру керек?
- Қолды қалай дұрыс жуу керек?

4.«Интернеттегі психикалық денсаулық» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Цифрлық технологияға қалай тәуелді болмауға болады?
- Интернетте пайда болуы мүмкін жағымсыз эмоцияларға қалай қарсы тұруға болады?
- Өзіңізді жалған жаңалықтардан қалай қорғауға болады?

5. «Компьютерде жұмыс істеу кезінде дененің дұрыс орналасуы» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Неліктен компьютерде дұрыс отыру маңызды?
- Компьютерде жұмыс істегенде омыртқаның денсаулығы мен көру қабілетін сақтау үшін қандай ережелерді сақтау керек?

6. «Интернетте өткізілетін уақытты шектеу» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Интернетте күніне қанша уақыт өткізуге болады?
- Интернетте өткізілетін уақытты қалай шектеуге болады?

7. «Қауіпсіз және позитивті сайттар мен қосымшалар» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Қауіпсіз сайттар мен қосымшаларды қауіпті сайттардан қалай ажыратуға болады?
- Интернеттегі зиянды мазмұннан өзіңізді қалай қорғауға болады?

Ата-аналарға арналған ұсыныстар

- Балаларыңызға үлгі болыңыз. Балалардың бұл маңызды екенін көруі үшін кибергигиена ережелерін өзіңіз сақтаңыз.

- Балалармен кибергигиена мәселелерін талқылаңыз. Олардың сұрақтарына жауап беріңіз және қиын сәттерді түсінуге көмектесіңіз.

- Цифрлық технологияны пайдалану ережелерін орнатыңыз.

- Балалардың интернетте өткізетін уақытын шектеңіз және олардың осы ережелерді сақтайтынына көз жеткізіңіз.

- Балалардың цифрлық технологияны пайдалануын бақылау. Олар қандай сайттар мен қолданбаларға кіретінін және интернетте кіммен сөйлесетінін қадағалаңыз.

- Балаларды физикалық белсенділікпен айналысуға шақырыңыз. Балалардың таза ауада және спортпен айналысуға жеткілікті уақыт бөлетініне

көз жеткізіңіз.

- Балаларды компьютерде дұрыс отыруға үйретіңіз. Балаларға денсаулығына зиян келтірмеу үшін компьютерде қалай дұрыс отыру керектігін көрсетіңіз.

- Балалармен цифрлық технологияны қолданумен байланысты ықтимал қауіптерді талқылаңыз. Балаларға осы қауіптерден қалай қорғану керектігін түсіндіріңіз.

Педагогтерге ұсыныстар

- Кибергигиена сұрақтарын оқу жоспарлары мен бағдарламаларына қосыңыз. Балаларды кибергигиенаға үйрету білім беру процесінің бөлігі болуы керек.

- Оқытудың түрлі әдістерін қолданыңыз. Балаларға кибергигиенаны ойын және интерактивті түрде үйретіңіз.

- Ата-аналармен ынтымақтастықта болыңыз.

«БАЛАЛАРДА КИБЕРҚАУІПСІЗДІККЕ ҚАТЫСТЫ ЖАҒЫМДЫ ӘДЕТТЕРДІ ҚАЛЫПТАСТЫРУ» ТАҚЫРЫБЫ БОЙЫНША СЫНЫПТАН ТЫС ІС-ШАРАЛАР МЕН СЫНЫП САҒАТТАРЫНЫҢ ТАҚЫРЫПТЫҚ ҮЛГІЛЕРІ

Қазіргі әлемде балалар жас кезінен бастап цифрлық технологиялармен бетпе-бет келеді. Олар оларды оқу, қарым-қатынас, ойын-сауық және басқа мақсаттар үшін пайдаланады. Сондықтан балалардың киберқауіпсіздік туралы түсінігі болуы және осы салада жағымды әдеттер қалыптастыруы маңызды.

Киберқауіпсіздік дегеніміз не?

Киберқауіпсіздік – бұл алаяқтық, киберқылмыс және зиянды бағдарламалар сияқты интернеттегі әртүрлі қауіптерден қорғану мүмкіндігі.

Балалардың киберқауіпсіздікке қатысты жағымды әдеттерін қалай қалыптастыруға болады?

Балалардың киберқауіпсіздікке қатысты жағымды әдеттерін қалыптастыру үшін:

- Балалар киберқауіпсіздік туралы мүмкіндігінше ертерек білуі керек.
- Кешенді тәсілді қамтамасыз ету. Олар киберқауіпсіздіктің барлық аспектілерін қамтуы керек.

Баланың терең алуы үшін түрлі әдістерді қолданыңыз.



Білім алушыға өнімді білім алуға көмектесетін көптеген әдістер бар. Олардың кейбіреулері:

Кесте жасаңыз. Кесте сіздің күнінiзді ұйымдастыруға, басымдықтарды белгілеуге және кейiнге қалдырудан аулақ болуға және интернетте бос уақытын өткізуден аулақ болуға мүмкіндік береді. Сабақ кестесін, үй тапсырмасын, демалысты және басқа әрекеттерді ескеретін кесте құруға тырысыңыз.

Оқытудың әртүрлі әдістерін қолданыңыз. Әр адам әртүрлі тәсілдермен үйренеді, сондықтан сіз үшін не жақсы жұмыс істейтiнін анықтау үшін әртүрлі оқыту әдістерін қолданып көрген жөн. Бұл оқу материалдарын оқу, жазбаларды жазу, достарыңызбен талқылау және т. б. болуы мүмкін.

Алаңдататын нәрселерден аулақ болыңыз. Телефон, әлеуметтік медиа, желідегі түрлі ойындар мен оқиғалар және т.б. сияқты көптеген нәрселер сізді оқудан алшақтатуы мүмкін.

Мотивацияңызды сақтаңыз. Осы мақсаттарға жету үшін мақсаттар қойыңыз. Мотивация сізге ынта мен тиімділікті сақтауға көмектеседі.

Қажет болса, көмек сұраңыз. Егер сізде қиындықтар туындаса, материалды түсінуге көмектесетін мұғалімдерге, ата-аналарға немесе басқа мамандарға хабарласыңыз.

Үнемі жаттығу жасаңыз. Тұрақты жұмыс сізге материалды жақсы сіңіруге және емтихан немесе тест тапсырмалары алдында стресстен аулақ болуға көмектеседі.

Сабаққа белсенді қатысу: сабаққа белсенді қатысу материалды жақсы есте сақтауға көмектеседі, сонымен қатар мұғалімнен кері байланыс алуға және түсініксіз сәттерді нақтылауға мүмкіндік береді.

Рефераттарды жазу: рефераттарды жүргізу ақпаратты жүйелеуге және білімді ретке келтіруге көмектеседі, бұл есте сақтаудың тиімдірек болуына ықпал етеді.

Тұрақты қайталау: зерттелген материалды үнемі қайталау оны есте сақтауға көмектеседі.

Түрлі дерек көздерді пайдалану: оқулықтар, интернет-ресурстар, кітаптар мен журналдар сияқты әр түрлі ақпарат көздерін пайдалану тақырып туралы толық түсінік алуға көмектеседі.

Басқа оқушылармен ынтымақтастық: басқа оқушылармен ынтымақтастық сізге жаңа білім мен мәселелерді шешудің тәсілдерін алуға көмектеседі.

Көмек сұраңыз: егер сізде оқу қиын болса, мұғалімнен немесе тәрбиешіден көмек сұраудан тартынбаңыз.

Өзін-өзі бағалау: өзін-өзі бағалау оқу процесінің маңызды факторы. Қателіктерді ғана емес, прогресс пен жетістіктеріңізді бағалаңыз.

Жалпы, нәтижелі оқу үшін жұмыс пен демалыс арасындағы тепе-теңдікті сақтау, уақытты жоспарлау және эмоцияларыңызды басқаруды үйрену қажет. Осы принциптерді ұстану оқуда жетістікке жетуге көмектеседі.

Білім алушылармен бірге жасауға болатын киберқауіпсіздік әрекеттерін сақтау бойынша сыныптан тыс іс-шаралардың тақырыптық үлгілері:

1. «Интернеттегі жеке деректеріңізді қалай қорғауға болады» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Интернеттегі бейтаныс адамдарға қандай жеке мәліметтер беруге болмайды?

- Жеке деректеріңізді ұрлықтан қалай қорғауға болады?

2. «Интернеттегі алаяқтықты қалай тануға болады» сабағы

Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Интернеттегі алаяқтықтың қандай белгілері бар?

- Интернеттегі алаяқтықтың құрбаны болмау үшін не істеу керек?

3. «Компьютерді зиянды бағдарламадан қалай қорғауға болады» сабағы
Бұл сабақта балалар келесі мәселелерді талқылай алады:

- Зиянды бағдарлама дегеніміз не?

- Компьютерді зиянды бағдарламадан қалай қорғауға болады?

Балалардың киберқауіпсіздікке қатысты жағымды әдеттерін қалыптастыру ата-аналар, педагогтер, тәрбиешілер және басқа ересектердің міндеті.

Балалардың киберқауіпсіздікке қатысты жағымды әдеттерін қалыптастыру бойынша әдістемелік ұсыныстар

Мақсаты: балалардың интернет желісінде қауіпсіз мінез-құлық дағдыларын қалыптастыру.

Міндеттері :

- Балаларды киберқауіпсіздіктің негізгі ұғымдарымен таныстыру.
- Балаларды киберқауіпсіздік қауіптерін тануға үйрету.
- Балалардың интернеттегі қауіпсіз мінез-құлық дағдыларын тәрбиелеу.

Принциптері:

Қол жетімділік. Киберқауіпсіздік туралы ақпарат балаларға түсінікті және қол жетімді түрде қол жетімді болуы керек.

Жас сәйкестігі. Киберқауіпсіздік туралы ақпарат балалардың жасына және даму деңгейіне сәйкес келуі керек.

Ынтымақтастық. Интернет желісінде қауіпсіз мінез-құлық дағдыларын қалыптастыру балалармен, ата-аналармен және мұғалімдермен ынтымақтастықта жүзеге асырылуы керек.

Әдістері:

- Әңгімелер.
- Ойындар.
- Конкурстар.
- Викториналар.
- Шығармашылық жұмыстарды құру.

Формалары:

- Жеке сабақтар.
- Топтық сабақтар.
- Сынып сағаты.
- Сыныптан тыс жұмыстар.

Мазмұны:

Киберқауіпсіздіктің негізгі ұғымдары:

Киберқауіпсіздік — ақпараттық-телекоммуникациялық желілерде туындайтын қауіптерден, оның ішінде ақпаратқа рұқсатсыз қол жеткізуден, оны бұрмалаудан немесе жоюдан, оған қол жеткізуді бұғаттаудан, сондай-ақ осындай ақпаратқа қатысты өзге де заңсыз әрекеттерден қорғалу жай-күйі.

Киберқауіптер — ақпараттық қауіпсіздікті бұзуға бағытталған әрекеттер. Оларға мыналар жатады:

- Ақпаратқа рұқсатсыз қол жеткізу
- Ақпаратты алу, көшіру, өзгерту немесе жою
- Ақпаратқа қол жеткізуді бұғаттау
- Ақпаратты заңсыз пайдалану

Киберқауіпсіздік қаупі:

Зиянды бағдарламалық жасақтама (вирустар, трояндық бағдарламалар, тыңшылық бағдарламалар және т. б.)

- Phishing (электрондық пошта немесе әлеуметтік медиа алаяқтық)
- Спам (қалаусыз электрондық пошта)
- Кибербуллинг (интернеттегі қорлау)
- Интернетке тәуелділік

Интернеттегі қауіпсіз мінез-құлық ережелері:

- Құпия сөздерді, логиндерді, телефон нөмірлерін және электрондық пошта мекен-жайларын қоса, жеке деректерді ешкімге бермеу.
- Электрондық пошталарда күдікті сілтемелер мен тіркемелерді ашпау.
- Күшті құпия сөздерді қолдану және оларды үнемі өзгерту.
- Антивирустық бағдарламалық жасақтаманы орнатыңыз және оны үнемі жаңартып отыру.
- Тексерілмеген дерек көздерден файлдарды жүктемеу.
- Әлеуметтік желілердегі жеке ақпараттан сақ болу.
- Интернеттегі бейтаныс адамдармен араласпау.

Балалардың киберқауіпсіздікке қатысты жағымды әдеттерін қалыптастыру бойынша іс-шараларды өткізу бойынша ұсынымдар:

- Іс-шаралар балалар үшін қызықты және тартымды болуы керек.
- Ақпарат қол жетімді және түсінікті түрде ұсынылуы керек.
- Балалар іс-шаралардың белсенді қатысушылары болуы керек.
- Балалардың алған білімдерін іс жүзінде қолдана алуы маңызды.

Іс-шаралардың тақырыптық үлгілері:

1. «Балаларға арналған киберқауіпсіздік» әңгімесі. Бұл әңгімеде балалар киберқауіпсіздіктің негізгі ұғымдарымен, киберқауіпсіздік түрлерімен және интернет желісіндегі қауіпсіз мінез-құлық ережелерімен танысады.
2. «Интернеттегі қауіпсіздік» ойыны. Бұл ойында балалар киберқауіпсіздік қатерлерін тануды және әртүрлі жағдайларда дұрыс шешім қабылдауды үйренеді.
3. «Киберқауіпсіздік бойынша үздік байқау». Бұл байқауда балалар интернеттегі қауіпсіз мінез-құлық ережелерін білуде жарысады.
4. «Киберқауіпсіздік» Викторинасы. Бұл викторинада балалар киберқауіпсіздік туралы білімдерін тексереді.
5. «Киберқауіпсіздік» тақырыбында шығармашылық жұмыстар жасау. Осы іс-шара аясында балалар киберқауіпсіздік туралы суреттер сала алады, әңгімелер немесе өлеңдер жаза алады.

1. Балалардың киберқауіпсіздікке қатысты жағымды әдеттерін қалыптастыру тақырыбындағы әдістемелік ұсыныстар

Мақсаты: балалардың интернет желісінде қауіпсіз мінез-құлық дағдыларын қалыптастыру.

Міндеттері:

- Балаларды Киберқауіпсіздіктің негізгі ұғымдарымен таныстыру.
- Балаларды киберқауіпсіздік қауіптерін тануға үйрету.
- Балалардың интернеттегі қауіпсіз мінез-құлық дағдыларын тәрбиелеу.

Ұсынылатын жұмыс формалары мен әдістері:

Әңгімелер, пікірталастар, рөлдік ойындар, викториналар, конкурстар.

Плакаттар, буклеттер, мультфильмдер сияқты көрнекі материалдарды пайдалану.

Жұмыстың негізгі бағыттары:

- Балаларды киберқауіпсіздіктің негізгі ұғымдарымен таныстыру.
- Балалар киберқауіпсіздік деген не, интернет желісінде қандай қауіптер бар және олардан қалай қорғануға болатынын түсінуі керек.
- Балалардың киберқауіпсіздік қауіпін тану дағдыларын қалыптастыру.
- Балалар күдікті сілтемелерді, электрондық пошта тіркемелерін, әлеуметтік медиа хабарламаларын және басқа да киберқауіпсіздік қауіптерін тани білуі керек.
- Балалардың интернеттегі қауіпсіз мінез-құлық дағдыларын тәрбиелеу.
- Балалар интернеттегі қауіпсіз мінез-құлық ережелерін білуі және сақтауы керек.

Іс-шаралардың нақты үлгілері:

1. Балалармен киберқауіпсіздік туралы әңгіме жүргізу.

Әңгіме барысында келесі мәселелерді талқылауға болады:

- Киберқауіпсіздік дегеніміз не?
- Интернет желісінде қандай қауіптер бар?
- Олардан қалай қорғануға болады?

2. Киберқауіпсіздік туралы пікірталас.

Пікір-талас барысында келесі мәселелерді талқылауға болады:

- Шабуылдаушылар балалардың жеке деректеріне қандай жолдармен қол жеткізе алады?
- Фишингтік шабуылдардан қалай қорғануға болады?
- Интернет желісіндегі дербес деректермен қалай дұрыс жұмыс істеу керек?

3. Рөлдік ойын «Киберқауіптерден қалай қорғануға болады».

Рөлдік ойын барысында балалар интернет желісіндегі қауіпсіздікке байланысты әртүрлі рөлдерді көре алады. Мысалы, олар балаларын киберқауіптерден қорғауға тырысатын ата-аналардың рөлін немесе балалардың жеке деректеріне қол жеткізуге тырысатын зиянкестердің рөлін ойнауы мүмкін.

4. Киберқауіпсіздік бойынша Викторина.

Викторина ауызша немесе жазбаша түрде өткізілуі мүмкін. Онда Киберқауіпсіздіктің негізгі ұғымдарын білуге арналған сұрақтар, сондай-ақ киберқауіпсіздік қатерлерін тануға арналған сұрақтар қойылуы мүмкін.

5. Киберқауіпсіздік тақырыбындағы суреттер немесе қолөнер байқауы.

Байқау топта да, жеке тәртіпте де өткізілуі мүмкін. Балалар интернеттегі қауіпсіз мінез-құлық ережелерін бейнелейтін сурет сала алады немесе қолөнер жасай алады.

6. Ата-аналармен жұмыс.

Балаларды киберқауіптерден тиімді қорғауды қамтамасыз ету үшін ата-аналармен тығыз жұмыс істеу маңызды. Ата-аналар интернеттегі қауіпсіз мінез-құлық ережелері туралы білуі керек және олар балаларына осы ережелерді сақтауға көмектесуі керек.

Ата-аналармен жұмыс аясында келесі іс-шараларды өткізуге болады:

Киберқауіпсіздік тақырыбындағы ата-аналар жиналысы.

Ата-аналар жиналыстарында келесі мәселелерді талқылауға болады:

- Балаларға интернеттегі қауіпсіз мінез-құлықты қалай үйретуге болады?
- Балалардың интернет желісін пайдалануын қалай бақылауға болады?
- Киберқауіптерге байланысты жағдайларға қалай жауап беруге болады?

Білім беру ұйымының сайтында киберқауіпсіздік туралы материалдарды жариялау.

Білім беру ұйымының сайтына ата-аналарға қол жетімді болатын киберқауіпсіздік туралы материалдарды орналастыруға болады. Бұл материалдарда интернеттегі қауіпсіз мінез-құлық ережелері, сондай-ақ балаларға киберқауіптерден аулақ болуға көмектесу туралы ақпарат болуы мүмкін.

7. Балалармен және ата-аналармен бірлескен іс-шаралар өткізу.

Бірлескен іс-шаралар шеңберінде балалар мен ата-аналар киберқауіпсіздік мәселелерін бірге талқылай алады, сондай-ақ интернет желісінде қауіпсіз мінез-құлық дағдыларын қалыптастыруға бағытталған іс-шараларға қатыса алады.

Жұмыс тиімділігін бағалау.

Балаларда киберқауіпсіздікке қатысты жағымды әдеттерді қалыптастыру бойынша жұмыстың тиімділігін келесі критерийлер бойынша бағалауға болады:

- Балалардың киберқауіпсіздіктің негізгі ұғымдарын білуі.
- Балалардың киберқауіпсіздік қауіптерін тану қабілеті.

- Балалардың интернеттегі қауіпсіз мінез-құлық ережелерін сақтауы. Жұмыстың тиімділігін бағалау үшін келесі әдістерді қолдануға болады: *Балаларды киберқауіпсіздіктің негізгі ұғымдарын білуге тестілеу.*

Киберқауіпсіздік қатерлерін тану дағдыларын дамытуға бағытталған *практикалық сабақтар өткізу.*

Интернеттегі балалардың мінез-құлқын бақылау.

Балаларда киберқауіпсіздікке қатысты жағымды әдеттерді қалыптастыру жүйелі тәсілді қажет ететін маңызды міндет. Балаларда киберқауіпсіздікті сақтау үшін педагогтер мен ата-аналардың тығыз ынтымақтастығы маңызды

2. Балалардың киберқауіпсіздікке қатысты жағымды әдеттерін қалыптастыру тақырыбындағы әдістемелік ұсыныстар

- Жеке ақпаратқа рұқсатсыз қол жеткізу
- Кибербуллинг
- Бейтаныс адамдармен байланыс
- Интернетке тәуелділік
- Балаларды осы қауіптерден қорғау үшін олардың киберқауіпсіздікке

қатысты жағымды әдеттерін қалыптастыру қажет.

Мақсаты: балаларда интернет желісінде қауіпсіз мінез-құлық дағдыларын қалыптастыру.

Міндеттері:

- Балаларды киберқауіпсіздіктің негізгі ұғымдарымен таныстыру
- Балаларды киберқауіпсіздік қауіптерін тануға үйрету
- Балаларда интернеттегі қауіпсіз мінез-құлық дағдыларын тәрбиелеу

Киберқауіпсіздікке қатысты жағымды әдеттерді қалыптастырудың негізгі принциптері

Реттілік. Интернеттегі қауіпсіз мінез-құлық дағдыларын қалыптастыру қарапайым ережелерден бастап біртіндеп жүруі керек.

Жүйелілік. Интернеттегі қауіпсіз мінез-құлық дағдылары үнемі қайталану арқылы бекітілуі керек.

Жағымды көңіл-күй. Балалар киберқауіпсіздік ережелерін сақтағаны үшін жағымды эмоциялар алуы керек.

Киберқауіпсіздікке қатысты жағымды әдеттерді қалыптастыру әдістері:

Оқыту. Балаларға киберқауіпсіздік дегеніміз не, интернетте қандай қауіптер бар және оларды қалай болдырмауға болатындығы туралы айту керек.

Тәжірибе. Балаларға киберқауіпсіздік ережелерін сақтауға машықтануға мүмкіндік беру қажет.

Талқылау. Балалармен киберқауіпсіздікке байланысты жағдайларды талқылау және оларды талдау маңызды.

Үлгі Балалар ересектердің киберқауіпсіздік ережелерін сақтайтынын көруі керек.

Киберқауіпсіздікке қатысты жағымды әдеттерді қалыптастыру бойынша

іс-шаралар үлгісі:

Киберқауіпсіздікке қатысты жағымды әдеттерді қалыптастыру үшін келесі әрекеттерді орындауға болады:

Ата-аналармен кездесу. Ата-аналармен кездесулерде оларға киберқауіпсіздіктің маңыздылығы және балаларына бұл мәселеде қалай көмектесе алатындығы туралы айтуға болады.

Мектептегі сабақтар. Мектептегі сабақтарда балаларға киберқауіпсіздік туралы және интернет желісіндегі қауіпсіздік ережелерін қалай сақтау керектігі туралы айтуға болады.

Конкурстар. Киберқауіпсіздік бойынша конкурстар өткізу балаларға алған білімдері мен дағдыларын бекітуге көмектеседі.

Әңгімелер. Балалармен киберқауіпсіздік туралы сөйлесу оларға интернеттегі қауіпсіздік ережелерін сақтаудың маңыздылығын түсінуге көмектеседі.

Киберқауіпсіздікке қатысты жағымды әдеттерді қалыптастыру ата-аналардың, тәрбиешілердің және балалардың бірлескен күш-жігерімен шешілуі керек маңызды міндет.

Киберқауіпсіздікке қатысты жағымды әдеттерді қалыптастыру үшін келесі әрекеттерді орындауға болады:

ҚОРЫТЫНДЫ

Бүгін біз өз өмірімізді компьютерсіз және интернетсіз елестете алмаймыз. Қазіргі уақытта Дүниежүзілік желінің пайдасы мен зияны туралы көптеген даулы әңгімелер туындауда. Балалар мен жасөспірімдер интернеттің белсенді пайдаланушылары, өйткені ол өскелең ұрпаққа жаңалық ашуға, қарым-қатынас пен шығармашылыққа керемет мүмкіндіктер береді. Бірақ кез-келген құбылыстың өзінің ашық және көлеңке жақтары бар, көбінесе балалар мен жастар желіде кездесетін барлық мүмкін проблемаларды толық түсінбейді.

Интернет – бұл ересектерге тиесілі және балаларға жарамсыз материалдарды қамтитын әлемге ашық терезе, сондықтан киберкеңістікті пайдалану арқылы белгілі бір қауіптер бар.

Ата-аналар мен ересектер балаларға қалай көмектесуі керек. Барлық мүмкін қиындықтардан аулақ болу, олардың интернетте болуын қауіпсіз ету, оларды Дүниежүзілік желіде шарлауға үйрету ме? Қарапайым жауап жоқ. Тәуекелдер баланың жасына және компьютерлік сауаттылығына байланысты әр түрлі болуы мүмкін.

Әрине, осы заманауи технологияларды пайдаланудан бас тарту балаларды онлайн кеңістікте қорғау мәселесінің шешімі емес. Жазатайым оқиғалардың алдын алу үшін баланы абай болуға, белгілі бір ережелерді сақтауға, жауапты болуға, ересектердің жағымды үлгісін ұстануға үйрету керек.

Сонымен қатар ересектердің ең маңызды міндеті – балаларға интернеттің қауіптілігі туралы ескерту. Балалармен интернетті пайдалану кезінде туындауы мүмкін барлық мәселелерді талқылау қажет.

Дегенімен балалардың күнделікті өмірде интернетті пайдалануда киберқауіпсіздік, кибергигиена, кибермәдениет ережелерін сақтауда білімнің жетіспеушілігі, оларды тығырыққа тіреп, келеңсіз жайттарға ұрындырып жатуы педогогтерді де, ата-аналарды да ойландыратын мәселе.

Интернет – бұл керемет орын және сіздің балаларыңыз тәуекелдерге қарамастан, оның артықшылықтарын ерте ме, кеш пе пайдаланады. Егер сіз өзіңізді және балаларыңызды интернетті қауіпсіз пайдалану ережелеріне уақтылы үйретсеңіз, егер барлық отбасы мүшелері ықтимал қауіптер туралы көбірек білсе, онда Сіз интернет желісінің барлық артықшылықтарын өз қауіпсіздігіңізге қауіп төндірмей пайдалана аласыз.

Жеке басыңызды және деректеріңізді қорғау үшін киберқауіпсіздік мамандары ұсынған барлық ережелер мен әдістерді қолдану қажет.

Әдістемелік ұсынымдамада берілген қарапайым нұсқауларды орындау арқылы педагогтер білім алшыларды, ата-ана балаларын киберқауіптерден қорғауға және жеке ақпараттарды қауіпсіз сақтауға көмектесе алады. Сонымен қатар білім алушылардың кибермәдениет, кибергигиена, киберқауіпсіздік ережелерін сақтау, интернетті қолданудағы мәдениеттілігі арттыру туралы білімдерін кеңейте алады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Мемлекет басшысы Қасым-Жомарт Тоқаевтың Ұлттық құрылтайдың «Әділетті Қазақстан – Адал азамат» атты екінші отырысында сөйлеген сөзі» - 2023 жылғы 17 маусым Түркістан қаласы
2. Киберқауіпсіздік тұжырымдамасын бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы
3. Қазақстан Республикасының 2018 жылғығы 2 шілдедегі № 169 «Балаларды денсаулығы мен дамуына зардабын тигізетін ақпараттан қорғау туралы» Заңы
4. Қазақстан Республикасы Үкіметінің «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту» туралы 2016 жылғы 20 желтоқсандағы № 832 қаулысы
5. Карауылбаев С.К., Артюхина М., Жумабаева А.М., Муратова Г.И. Границы развития интернет- педагогики/ / Педагогика және психология. Абай ат. ҚазҰПУ, 2020. – Б.2-10
6. Плешаков В.А. Перспективы киберонтологического подхода в современном образовании // Вестник Московского городского педагогического университета. Серия: педагогика и психология. 2014. № 3(29). – С. 1-18
7. Воинова О.И., Плешаков В.А. Киберонтологический подход в образовании: Монография / Под ред. В.А. Плешакова. – Норильск: НИИ, 2012. – 244 с
8. Игібаева А.Қ, Төлеуханова А.Д., С. Аманжолов Абай атындағы ҚазҰПУ Хабаршысы «Педагогика ғылымдары» сериясы №4 (68), Өскемен – 2020. – 12 б
9. <https://cisoclub.ru/kibergigiena-dlja-detej-kak-obuchit-mladshie-pokolenija-bezopasnosti-v-internete>
10. Оңтүстік Корея 2007 ж.; Франция 2011ж.; АҚШ 2008-2011ж.ж
11. «Kazakhstan Kids Online Қазақстандағы балалардың цифрлық өмірі» UNICEF әрбір бала үшін 12.11.2023ж
12. <https://www.gov.kz/memleket/entities/bala?lang=ru>
13. Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы Кодексі 2014 жылғы 5 шілдедегі № 235-V ҚРЗ.
14. Қазақстан Республикасы Үкіметінің «Неке (ерлі-зайыптылық) және отбасы туралы» 2007 жылғы 24 желтоқсандағы N 1269 Қаулысы.
15. <http://www.kaspersky.ru>
16. <http://www.onlandia.org.ua/rus/>
17. <http://www.saferinternet.ru>
18. http://video.mail.ru/mail/illari.sochi/_myvideo/1.html
19. <http://www.youtube.com/watch?v=hbvvgg63ewo&feature=autoplay&list=pld70b32df5c50a1d7&playnext=1>
21. <Http://www.youtube.com/watch?v=3ap1rkr0rce&feature=relmfu>

22. [Http://www.youtube.com/watch?v=amcsvzxcd9w&feature=bfa&list=pld70b32df5c50a1d7&lf=autoplay](http://www.youtube.com/watch?v=amcsvzxcd9w&feature=bfa&list=pld70b32df5c50a1d7&lf=autoplay)
23. [Http://www.youtube.com/watch?v=xrsnlkvempy&feature=relmfu](http://www.youtube.com/watch?v=xrsnlkvempy&feature=relmfu)
24. [Http://content-filtering.ru/aboutus](http://content-filtering.ru/aboutus),
25. [Http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_rooma.html](http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_rooma.html)
26. [Http://www.youtube.com/watch?v=y37ax5tpc3s&feature=related](http://www.youtube.com/watch?v=y37ax5tpc3s&feature=related).
27. <http://www.interneshka.net>
28. <http://www.edu.yar.ru/azbuka/password.php#game>
29. <http://www.ligainternet.ru/>
30. http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/quiz_ks3.htm
31. <http://www.kaspersky.ru> –
32. <http://www.onlandia.org>.
33. <http://www.interneshka.net>
34. <http://content-filtering.ru>
35. <http://content-filtering.ru>;
36. <http://www.microsoft.com/>
37. <http://www.youtube.com/>
38. http://www.oszone.net/6213/#_ftn1
39. Crystal D. Language and the Internet. Cambridge: University press, 2001. 272 p
40. Harrison L.E. Who prospers? How cultural values shape economic and political success. New York: Basic Books, 1992. 288 p.].
41. Harrison L.E., Huntington S.P. (Eds.). Culture matters: How values shape human progress. New York: Basic Books, 2000. 348 p
42. Inglehart R., Baker W.E. Modernization, cultural change and the persistence of traditional values // American Sociological Review. 2000. № 65 (1). P. 19-51
43. <https://cyberacademy.ppu.edu.kz/files/2023/teacher->

«Қауіпсіз Интернет» тақырыбы бойынша білім алушылардың қорытынды сауалнамасының үлгі материалдары

1. Жасыңызды көрсетіңіз _____
 2. Интернет деген не? _____
 3. Интернетте қандай қауіптер бар? _____
-
-

4. Интернетті пайдалану қауіпсіз, егер: жауаптар тізімінен бір немесе бірнеше нұсқаны таңдасаңыз.

а) компьютеріңізді қорғаңыз, желіде өзіңізді қорғаңыз, ережелерді сақтау

ә) жеке ақпаратты жария ету, басқаларға қамқорлық жасау, операциялық жүйені жүйелі түрде жаңарту

б) компьютеріңізді қорғаңыз, құжаттардың сақтық көшірмелерін жасаңыз, тіпті интернетте де заңға бағыну керек

5. «Интернетте өзіңізді қалай қорғауға болады?» жауаптар тізімінен бір немесе бірнеше нұсқаны таңдаңыз

а) компьютерді қорғау, белгісіз адамдармен танысу шеңберін кеңейту

ә) мүмкіндігінше өзі туралы аз ақпарат беруге тырысу

б) өзінің, достарының мен туыстарының суреттерін орналастыру

6. «Мен компьютерімді қалай қорғаймын?» жауаптар тізімінен бір нұсқаны таңдаңыз

а) сөндіріп, шкафқа жасыру

ә) антивирустық бағдарламаны орнату

7. «Антивирустық бағдарлама тиімді болуы үшін не істеу керек?» жауаптар тізімінен бір немесе бірнеше нұсқаны таңдаңыз.

а) антивирустық бағдарлама болмағаны дұрыс

ә) антивирустық мәліметтер базасын жаңарту

б) сайт қорғалған деген сенімділігі жоқ сайттарға кірмеу

8. «Қауіпті бағдарламаларды кім жасайды?» жауаптар тізімінен бір немесе бірнеше нұсқаны таңдаңыз

а) құпия билеуші

ә) хакерлер

б) тыңшылар

в) өлім тілегіштер

9. «Интернеттегі мінез-құлық ережелерін түгендеңіз» Егер сіз бұл сұрақтың жауабын білмесеңіз, онда «Жауап жоқ» деп жазыңыз. _____

10. «Сіз үшін «Қауіпсіз Интернет» дегеніміз не?» егер сіз бұл сұрақтың жауабын білмесеңіз, «Жауап жоқ» деп жазыңыз.

Жауабыңызға рахмет!

2-қосымша

*Интернет желісіндегі қауіпсіздік негіздерін сақтау бойынша кеңес
Интернет желісінде жұмыс істеу ережелері:*

1. Бейтаныс сайттарға кірмеңіз.
2. Word немесе Excel файлы сізге пошта арқылы, тіпті таныс адамнан келсе, оны ашпас бұрын, онда вирустың бар-жоғын тексеріңіз.
3. Егер сіз бейтаныс қосымшаны алсаңыз, ешбір жағдайда оны іске қоспаңыз, керісінше, бірден жойып, кәрзеңкенібосатыңыз.
4. Құпия сөзіңізді ешқашан ешкімге жібермеңіз.
5. Құпия сөздер үшін есте сақтау қиын сандар мен әріптерді қолдануға тырысыңыз.
6. Интернетте сөйлескенде, жеке деректеріңізді көрсетпеңіз, бүркеншік атты (лақап атты) қолданыңыз.
7. Ересектердің қарауынсыз, интернеттен танысқан адамдармен ешқашан кездеспейсіз.
8. Егер желіде тіркелу қажет болса, онда олар оны жеке ақпарат көрсетілмейтіндей етіп жасауы керек.
9. Қазіргі уақытта сайттардың мазмұнын сүзетін көптеген бағдарламалар бар. Сайттардың мазмұнын бірге көру үшін отбасы мүшелерінің арасында сенімді қарым-қатынас болуы керек.
10. Интернетте жарияланған барлық ақпаратқа сене беруге болмайды.
11. Экранда маңызды ақпарат бар компьютерді қараусыз қалдырмаңыз.
12. Немқұрайды қараудан сақ болыңыз.
13. Жалпыға ортақ компьютерде маңызды ақпаратты сақтамаңыз.

*Кибермәдениет пен кибергигиенаны сақтау бойынша кеңес**Кибер шабуыл кезінде кәмелетке толмағандарға арналған кеңестер:*

1. Теріс қылықтарыңызды киберкеңістікке бірден жарияламаңыз. Бала агрессивті хабарламаларға жауап бермес бұрын ересектерден кеңес сұрауы керек. Ал жасөспірімдерге бірнеше ережелер ұсынылуы керек: жауап хабарын жібермес бұрын ашулануды, реніш пен ашуды басу керек.

2. Виртуалды беделді құру маңызды, анонимділік елесімен пара бермеу керек. Кибер кеңістік көбінесе жасырындық арқылы «бостандық» мүмкіндігін көрсетеді, бірақ сіз лақап аттың артында тұрған адамды тануға болатынын есте ұстаған жөн. Мобберлердің іс-әрекетіне байланысты нақты зиянмен құпия ашылады. Браузерлер мен қосымшалар пайдаланушылардың әр түрлі әрекеттерінің тарихын жазады және әркімнің желідегі беделін анықтайды. Оны оңай және тез кетіруге болады, бірақ оны түзету өте қиын және уақытты қажет етеді.

3. Шабуылдың дәлелдерін сақтаған жөн. Егер бала кенеттен кез келген хабарламадан, бейнеден немесе суреттен ренжісе, онда сіз ата –анадан көмек сұрауыңыз керек. Ал жасөспірімдер үшін – ересектерден ыңғайлы уақытта кеңес сұрау үшін шабуыл фактісі бар бетті сақтаңыз немесе басып шығарыңыз.

4. Бір ғана негативті елеменіз. Дәл осылай жасаған дұрыс, өйткені мұндай мінез-құлықпен кибершабуыл бірінші (бастапқы) кезеңде тоқтайды. Интернетті қолданушылардың ең жақсы ережесі – «жеткіліксіздіктің ең жақсы жолы – елемеу».

5. Егер сіз киберқауіпсіздік куәгері болсаңыз, онда сіздің әрекетіңіз келесідей болуы керек:

- Сіз агрессорға қарсы сөйлеуіңіз керек және қазіргі қоғамда мұндай мінез-құлыққа жол берілмейтінін көрсетуіңіз керек.

- Жәбірленушіні қолдау – виртуалды кеңістікте жеке немесе ашық түрде оған эмоционалды қолдау көрсетіңіз.

- Ересек адамға кибер шабуыл туралы айт.

6. Агрессорды блоктаңыз. Хабаршылардың белгілі бір IP-адресстерден хабарлама жіберуді блоктау функциясы бар. Әңгімедегі мұндай үзіліс көбінесе агрессорды қорқытуды жалғастырудан бас тартады.

7. Жүйелі қатерлерді елеменіз. Бұл жағдайда шабуыл фактісін растау үшін құқық қорғау органдарына хабарласыңыз.

Кәмелетке толмағандарда компьютерлік тәуелділіктің ерте белгілерін анықтауға арналған тест-сауалнамалар

Тесттер әртүрлі жастағы білім алушылардың компьютерлік тәуелділік деңгейін анықтауға мүмкіндік береді.

Сауалнама-тесттер екі блоктан тұрады: бірінші блок білім алушыларға, екінші блок ата-аналарға арналған.

Нұсқаулық: он сұрақты мұқият оқып шығыңыз. Сіз олардың әрқайсысын дұрыс немесе дұрыс емес деп бағалауыңыз керек. Егер сұрақ сізге дұрыс немесе негізінен дұрысырақ болып көрінсе, «иә», егер дұрыс емес болса – «жоқ» деп белгілеңіз.

I блок. Білім беру ұйымдарының білім алушыларына арналған тесттер I нұсқа.

1. Онлайн көбірек уақыт өткізетіндігіңізді Сіз жиі байқайсыз ба? (иә/жоқ)
2. Желіде көбірек уақыт өткізу үшін үй шаруасын жиі жасамай қоясыз ба? (иә/жоқ)
3. Айналаңыздағы адамдар сіздің желіде өткізетін уақыт мөлшеріңізге жиі қызығушылық білдіре ме? (иә/жоқ)
4. Сіз мектепте үлгеріміңіз нашар болғанын байқадыңыз ба, себебі сізде оқуға уақыт жоқ, өйткені сіз желіде тым көп уақыт өткізесіз бе? (иә/жоқ)
5. Интернетте өзіңіздің қалай қайтадан отырғаныңызды жиі елестете аласыз ба? (иә/жоқ)
6. Сіз интернетсіз өмірдің зерігу, бос және қуанышсыз екенін жиі сезінесіз бе? (иә/жоқ)
7. Біреу сізді интернеттен алшақтатуға тырысқанда, сіз жиі тосқауыл қоясыз ба, айқайлайсыз ба немесе ашуланасыз ба? (иә/жоқ)
8. Интернетте түнімен ұзақ отырып, ұйықтамай қалатын кездеріңіз жиі бола ма? (иә/жоқ)
9. Сіз компьютерде отырған кезде шабыттану, толқу сезінесіз бе? (иә/жоқ)
10. Сіз компьютерді күнделікті қолдана бастағаннан бері ұйқының бұзылуы болды ма және/немесе ұйқы режимі өзгерді ме? (иә/жоқ)

2 нұсқа.

1. Сіз білімнің бір бөлігін компьютерлік ойындармен алмастыру туралы мұғалімдерге, ата аналарға өтініш жасадыңыз ба? (иә/жоқ)
2. Сіз өзіңізді әрқашан компьютерлік ойынды бірден тоқтата алмайтындай сезінесіз бе? (иә/жоқ)
3. Егер сіз компьютерде ұзақ уақыт ойнамасаңыз, сіз ашуланасыз ба немесе мазасызданасыз ба? (иә/жоқ)

4. Әдетте сіз компьютерлік ойындарды жоспарлағаннан да ұзағырақ ойнайсыз ба? (иә/жоқ)

5. Сізге ата-аналар, мұғалімдер, достар келген кезде шұғыл түрде компьютерлік ойын немесе сайт терезесін жабуға тура келді ме? (иә/жоқ)

6. Көңіл-күйіңізді түзету үшін (мысалы, кінәлау, ашуланшақтық) немесе жай ғана тынышталу үшін компьютерлік ойынға отырған кездеріңіз болды ме? (иә/жоқ)

7. Компьютерде ойнағаннан кейін сіздің басыңыз ауыра ма? (иә/жоқ)

8. Сіз компьютерлік ойын үшін тамақ ішуді кейінге шегересіз бе? (иә/жоқ)

9. Сіз компьютерлік ойынға байланысты жеке гигиенаны ұстанбайсыз ба? (иә/жоқ)

10. Кәдімгі өмірде сіз компьютерде ойнаған кезде жоғалып кететін зерігу, ашуланшақтық, еңсенің басылуын сезінесіз бе? (иә/жоқ)

Нәтижелерді есептеу: тестілеуді жүргізген мамандар жүргізеді.

«Иә» – 1 ұпай,

«Жоқ» – 0 ұпай.

Алынған ұпайлар қосылады.

0 – 3 ұпай – компьютерге тәуелділіктің төмен деңгейі.

4 – 6 ұпай – компьютерлік тәуелділіктің орташа деңгейі.

7 – 10 ұпай – компьютерлік тәуелділіктің жоғары деңгейі.

II блок. Ата-аналар үшін тесттер 1 нұсқа.

Сіздің балаңыз,...

1. Үйге келіп, ең алдымен компьютерге отырады? (иә/жоқ)

2. Үй шаруасын, оқуды тастады, бағынбайтын болды ма? (иә/жоқ)

3. Егер оны компьютерден алшақтатса, мазасыз, дөрекі ме? (иә/жоқ)

4. Компьютерден тұрмай тамақтана ма? (иә/жоқ)

5. Егер компьютер қолжетімсіз немесе бұзылса немен айналысатынын білмей ме? (иә/жоқ)

6. Компьютерде отыру уақытын басқара алмай ма? (иә/жоқ)

7. Компьютерлік ойындарға көп ақша жұмсайды ма? (иә/жоқ)

8. Достарымен араласуды тоқтатты, көп уақытын онлайн өткізе ме? (иә/жоқ)

9. Түрлі тыйым салынған сайттарға кіреді ме? (иә/жоқ)

10. Үнемі компьютерлік ойындар туралы, Интернеттегі қарым-қатынас туралы айтады ма? (иә/жоқ)

2 нұсқа.

Сіздің балаңыз,...

1. Ойынды аяқтау керек болғанда ашуланады ма? (иә/жоқ)

2. Компьютер ойынының кесірінен отбасына, туыстарына уақыт бөлмейтін болы ма? (иә/жоқ)

3. Компьютерлік ойыннан кейін басының, көзінің ауырғаны туралы шағымдана ма? (иә/жоқ)

4. Интернетте көбірек уақыт өткізгісі келетінін айтады ма? (иә/жоқ)
5. Компьютерлік ойын кезінде, шындықтан мүлде алшақтап, ойын әлеміне толықтай ауысады ма? (иә/жоқ)
6. Компьютер ойынының кесірінен тамаққа, жеке бас гигиенасына немқұрайлы қарайды ма? (иә/жоқ)
7. Компьютерде жүйелі түрде өткізген уақыттың нәтижесінде сабаққа, спорт секцияларына, үйірмелерге деген қызығушылық жоғалды ма? (иә/жоқ)
8. Көбінесе компьютерлік ойындар ойнағанда немесе желіде сөйлескенде жақсы көңіл-күйде бола ма? (иә/жоқ)
9. Интернетте ұзақ уақыт отыру негізінде күн тәртібін бұза ма? (иә/жоқ)
10. Шынайы өмірдегі достармен салыстырғанда виртуалды достармен қарым-қатынасты жақсы көреді? (иә/жоқ)

Нәтижені есептеу: ата-аналар орындайды.

«Иә» – 1 ұпай,

«Жоқ» – 0 ұпай.

Алынған ұпайлар қорытындыланады.

0 – 3 ұпай – компьютерге тәуелділіктің төмен деңгейі; ата-аналар мәселені өзбетімен шеше алады (ұсынымдарды қараңыз);

4 – 6 ұпай – компьютерге тәуелділіктің орташа деңгейі, мәселені шешу үшін маманнан (психолог) кеңес алу қажет;

7 – 10 ұпай – компьютерге тәуелділіктің жоғары деңгейі, компьютерге шамадан тыс құмарлық, баланың психологиялық тәуелділігіне әкеп соғуы мүмкін; ата-аналар өздігінен туындаған мәселені шеше алмайды, сондықтан маманнан (психолог, психотерапевт) көмек сұрау қажет.

«Абайлаңыз, вирус!» Сауалнама үлгісі:

Компьютерлік вирустардың негізгі тарату арнасы қандай?

1. Веб-парақшалар
2. Электрондық пошта
3. Флеш-жинақтар(флешки)

Вирустардың компьютерге енуін болдырмау үшін сіз:

1. Интернетті пайдаланбау
2. Антивирустық құралдарды орнату және жаңарту
3. Компьютердің жанында түшкірмеу және жөтелмеу

Егер вирус анықталса, сізге қажет:

1. Оны алып тастау және одан әрі зақымдануын болдырмау
2. Вирустың қандай түрі бар екенін анықтау
3. Оның компьютерге қалай келгенін табу

Хакерлерге компьютерге кіруге және файлдар мен құжаттарды қарауға не кедергі болады:

1. Брандмауэрді қолдану
2. Операциялық жүйені жаңарту
3. Вирусқа қарсы бағдарлама

Қазақстан Республикасының Қылмыстық кодексіне сәйкес елімізде қандай заңсыз әрекет жауапқа тартылады?

1. Компьютерлік вирустардың жойылуы
2. Зиян келтіретін компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату
3. Компьютерді қорғау үшін бағдарламалық құралды орнату

«Абайлаңыз, Интернет!» Сауалнама үлгісі

1. Интернетте қандай ақпаратты жариялауға болмайды?

1. Сіздің қызығушылығыңыз
2. Сіздің лақап атыңыз
3. Үйдің мекенжайы

2. Әлеуметтік желілер неліктен қауіпті?

1. Жеке ақпаратты кез келген адам әртүрлі мақсаттарда пайдалана алады
2. Танылмаған сілтемелерді көргенде, компьютеріңіз бұзылуы мүмкін
3. Жоғарыда айтылғандардың бәрі рас

3. Виртуалды сұхбаттасушы кездесуді ұсынады, не істеу керек?

1. Ата-аналармен кеңесіп, олардың келісімінсіз ештеңе жасамау
2. Кездесуге жалғыз бару
3. Өзіңізбен бірге досыңызды шақыру
4. *Интернетте заңмен не тыйым салынған?*
 1. Өзіңіз туралы ақпаратты орналастыру
 2. Өзге адамның келісімінсіз, ол туралы ақпаратты жариялау
 3. Файлдарды жеке пайдалану үшін көшіру
4. *Интернетте этикет ережелері бар ма?*
 1. Интернет – ережеге бағынбайтын кеңістік
 2. Ерекше жағдайларда
 3. Иә, шынайы өмірдегідей

Киберқауіпсіздік: цифрлық әлемде өзін-өзі қорғау

Сабақ мақсаты

- Білім алушыларды киберқауіпсіздік негіздерімен таныстыру, интернетте қауіпсіз мінез-құлық дағдыларын қалыптастыру;
- интерактивті сценарийлер арқылы киберқауіптерден қорғау дағдыларын

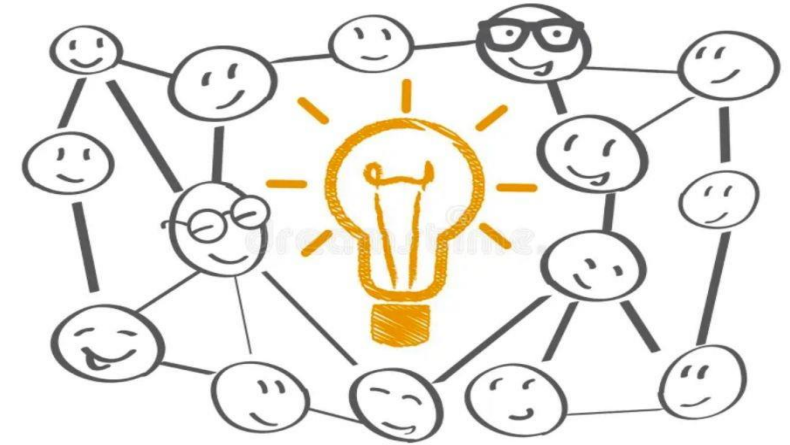


Ұсынылатын

сабақ формасы:

Құндылықтар

- Балалардың киберқауіпсіздігіне, кибергигиенасына және кибермәдениетіне қатысты пайдалы әдеттер мен дағдылар, экологиялық цифрлық мәдениет
- Сабақ бейнероликтер мен анимациялық бейнелерді, оқу ойынын пайдалануды қамтиды және ақпаратты талдауды, топтық жұмысты қамтиды.



Кіріспе:

Сабақ
тақырыбын
ұсыну
және
оның
маңызды
лығын
талқылау

Талқылауға арналған сұрақтар:

- «Киберқауіпсіздік» термині нені білдіреді?
- Интернеттегі қауіпсіздікті қамтамасыз ету не үшін маңызды?



Киберқауіпсіздік

Киберқауіпсіздікке байланысты нақты
өмірлік жағдайлардағы мысалдар

фишинг

Зиянды
бағдарламалар

кибербуллинг



Алаяқтық

Құпиялық

Құпия сөз
қауіпсіздігі

Әлеуметтік желі және фишинг:

Сауле әлеуметтік желіде өзінің ең жақын досының аккаунтына ұқсас аккаунттан хабарлама алады.

Хабарламада досының паролін ұмытып кеткені және Сәуледен есептік жазбасына кіруді қалпына келтіруге көмектесу үшін паролін жіберуін сұрайтыны туралы айтылған.

Сұрақ: Сәуле қандай қадамдар жасайды?



Дәурен жаңа ойынды онлайн сатып алуды шешеді. Ол оны өте төмен бағамен ұсынатын, бірақ төлем үшін несие картасының мәліметтерін енгізуді талап ететін сайтты табады.

Сұрақ: Дәурен қандай сақтық шара қабылдауы керек?

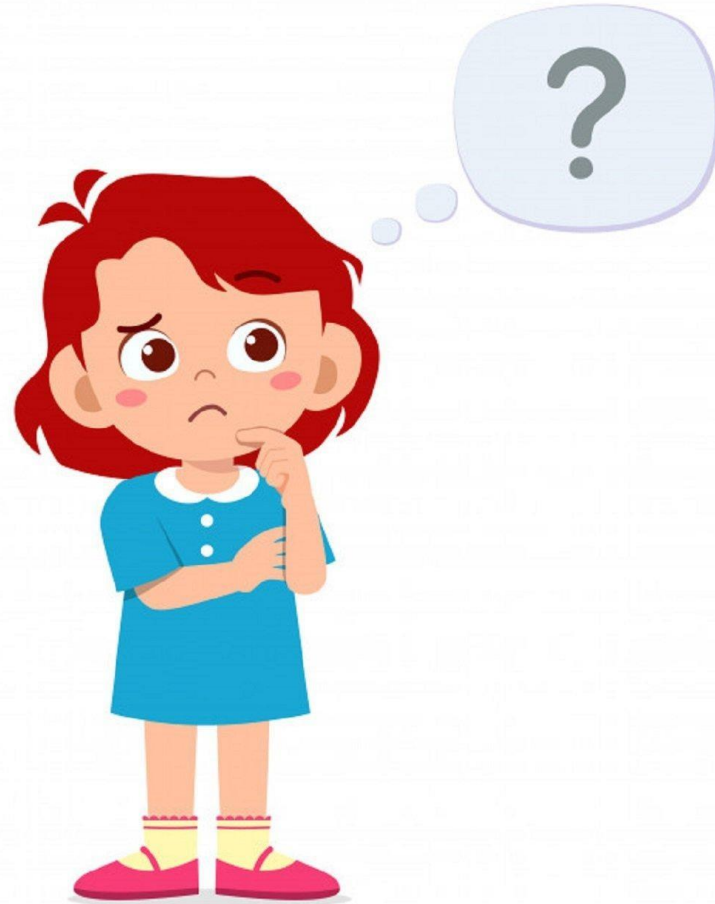
Онлайн сауда және карта қауіпсіздігі



Мобилді қауіпсіздік

**Айнұр
смартфонын
қоғамдық жерде
жоғалтады.
Оның
телефонында
жеке
фотосуреттері
мен
контактілері
сақталған.**

***Сұрақ: Ол өз
деректерін
қорғау үшін
қандай
қадамдар
жасауы
керек?***



Онлайн ойындар мен чаттар:

Асан онлайн мультиплеерде ойын ойнайды және жаңа ойыншымен танысады. Бұл ойыншы Асанға жеке мәліметтерімен бөлісуді ұсынады, егер олай болмаса олар бірге ойнай алмайтындығын айтады.

Сұрақ: Асанға қалай жауап беру керек?



Әлеуметтік
желілерде,
чаттарда және
онлайн
ойындарда
қауіпсіз қарым-
қатынас
ережелерін
үйрету

Интернеттегі қауіпсіз



Балжан
достарымен
фотосуреттермен
бөлісу үшін
сайтта аккаунт
жасайды. Ол
«123456» құпия
сөзін таңдайды,
себебі оны есте
сақтау оңай.

*Сұрақ: Балжан
құпия сөзді
таңдауда қандай
қауіпсіздік
шараларын
жіберіп алды?*

Құпия сөз қауіпсіздігі:



Кибербуллинг

**Маржан
әлеуметтік
желілерде
кибербуллингк
е тап болады.**

*Сұрақ: Ол өзін
қорғау үшін
қандай қадамдар
жасай алады
және көмекке
қалай жүгінуге
болады?*



**Білім алушылардан
кері байланыс алу;
Сабақты қорытындылау**

Кері байланыс және қорытынды

Бүгін не білдіңіз?

Не үйрендіңіз?

Сіз үшін не жаңалық болды?

Болашақта бұл білімді қалай қолданасыз?

Мазмұны

	Кіріспе.....	3
	..	
1	Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетінің ағымдағы жағдайын теориялық негіздеу және талдау	7
2	Балалардың киберқауіпсіздігіне, кибергигиенасына және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша халықаралық және отандық тәжірибе	27
3	Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша әдістемелік ұсынымдар	71
	Қорытынды.....	184
	Пайдаланған әдебиеттер тізімі.....	185
	Қосымша.....	187

ВВЕДЕНИЕ

За последние годы сеть Интернет вошла в нашу жизнь и стала важным современным источником информации и средством общения. Сегодняшние дети уже не представляют себе мир без смартфона и планшета, браузера и онлайн-игр. И так же, как мы учим малышей чистить зубы и правильно переходить дорогу, мы стараемся рассказывать им об основных правилах безопасного использования сети Интернет.

Сегодня, по данным Института развития Интернета, им пользуются 14 789 448 граждан Казахстана. Растет и число школьников, ежедневно использующих социальные сети. Технический прогресс делает информацию все более доступной. Владение информацией по-прежнему дает особые преимущества. «Кто владеет информацией, то владеет миром». [Nathan Mayer Rothschild]

В Интернете, как и в реальной жизни, учащихся подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т. п.

И Интернет с каждым годом становится более доступным в Казахстане. Согласно данным Internet World Stats, проникновение Интернета в стране в 2022 г. достигло 86%. Возможно, это связано с тем, что Интернет - услуги дешевеют. Так, данные Глобального индекса доступности сети Интернет (Internet Accessibility Index) показывают, что в 2022 году Казахстан занял 5 место из 164 стран по самым низким интернет-тарифам за широкополосное подключение Сети в месяц — 10,8 долларов (на 0,7 долл. дешевле, чем в 2021 г.) и за мобильный интернет (1 Гб) — 0,8 долларов (на 0,1 дешевле, чем в 2021 г.).

Стремительная цифровизация общества и распространение интернет-пользования в стране актуализирует проблему информационной грамотности подрастающего поколения. В силу возрастных особенностей наиболее уязвимой считается школьная молодежь, которая только учится критически мыслить и соблюдать информационную гигиену.

Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Безусловно, проведение комплексной работы с детьми остается в первую очередь за родителями. При этом сложно переоценить и тот вклад, который может внести школа. Для современных школьников именно учитель, а не интернет и компьютер, остается центральной фигурой в учебной и внеучебной деятельности

Формирование информационного пространства включают как положительные, так и негативные стороны. При том, что развитие виртуальной

среды формирует новые возможности, Интернет-среда позволяет хулиганам оставаться скрытыми от правосудия. Поскольку они анонимны, то не боятся наказания, потому что им не приходится сталкиваться со своими жертвами. Родители и педагоги должны знать об этом аспекте кибербуллинга, поскольку у хулигана мало стимулов прекратить свое поведение. Наилучший подход может заключаться в том, чтобы побудить жертву покинуть онлайн-платформу, используемую агрессором, поэтому родители и учителя должны научиться пользоваться Интернетом и понимать свои возможности [1].

Международный центр журналистики MediaNet при поддержке Фонда им. Конрада Аденауэра реализовали проект по изучению уровня медиа и информационной грамотности казахстанских школьников.

Исследование проходило в период с 23 сентября по 20 декабря 2022 года. Основным методом сбора данных стал онлайн-опрос учащихся 9 классов. Опрос проводился путём массовой рассылки анкеты для самозаполнения учащимися в школах Казахстана. Всего в опросе приняли участие более 6800 учащихся. По итогам обработки и «чистки» данных для анализа осталось 5922 анкеты. [2]

Интернет-зависимость – это навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. В частности, некоторые учащиеся настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Видами интернет-зависимости являются навязчивый веб-серфинг, пристрастие к виртуальному общению и виртуальным знакомствам (большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети), игровая зависимость — навязчивое увлечение компьютерными играми по сети.

К контентным рискам относятся материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет – это виртуальное пространство риска. Противозаконный контент распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям. Вредоносный (опасный) контент, способный нанести прямой вред психическому и физическому здоровью детей и подростков. Неэтичный контент, который не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, «только для взрослых»).

Особо опасны сайты, на которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения, способы самоубийства, сайты, посвященные наркотикам, сайты, на которых размещены полные ненависти

сообщения, направленные против отдельных групп или лиц. Столкновения с контентными рисками могут иметь негативные последствия для эмоциональной сферы, психологического развития, социализации, а также физического здоровья детей и подростков.

Если в начале 2000-х годов одну музыкальная композиция нужно было скачивать в течение полутора часов. Сегодня мы за несколько минут загружаем на планшет целый сезон любимого телешоу, чтобы смотреть его по дороге на работу. И если раньше основными угрозами, которые таит в себе увлечение компьютером и Интернетом, взрослые считали нарушение зрения, осанки, развитие зависимости и нежелательный контент, то сегодня все чаще называются такие явления, как потеря конфиденциальности, кибербуллинг, фейкньюз, финансовое мошенничество, самым распространенным среди несовершеннолетних, стал риск нежелательной коммуникации.

В марте 2021 года Комитет ООН по правам ребенка принял Замечание общего порядка №25 (GC25), направленное на помощь государствам и некоммерческим организациям в толковании Конвенции ООН о правах ребенка в цифровую эпоху. Вместе с экспертами и организациями по всему миру более 700 детей из 27 стран помогли сформировать этот по истине важный документ.

Права детей в цифровую эпоху закреплены в Конвенции о правах ребенка. Комитет ООН по правам ребенка (КПР), который следит за выполнением Конвенции, определил, как следует обращаться с молодыми людьми и детьми в цифровом мире и как следует защищать их права.

Комитет провел консультации с правительствами, гражданским обществом и более чем 700 детьми и подростками в 27 странах, спрашивая их, как цифровые технологии влияют на их права и какие действия они хотели бы видеть предпринятыми для их защиты. Выводы были изложены в «Замечании общего порядка».

Комитет рекомендовал государствам принять решительные меры, в том числе законодательного характера, для защиты детей от вредного и вводящего в заблуждение контента. Дети также должны быть защищены от всех форм насилия, происходящего в цифровой среде, включая торговлю детьми, гендерное насилие, киберагрессию, кибератаки и информационную войну.

1. Теоретическое обоснование и анализ текущей ситуации кибербезопасности, кибергигиены и киберкультуры детей

«Кибербезопасность — это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды и ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее: доступность; целостность, которая может включать аутентичность и конфиденциальность». [3].

Официально вопросы информационной безопасности и кибербезопасность в Казахстане поднимают не первый год. Государством разработан перечень нормативно-правовых актов в защиту и поддержку детей и молодежи. Приложение 1.

Многие организации используют термин «информационная безопасность», который обозначает безопасность информации во всех ее формах и на любых носителях, а не только электронных данных в цифровой сфере. Кибербезопасность, напротив, может быть больше связана с защитой только цифровой информации и более широкого круга ресурсов, связанных с киберпространством или затронутых им, как видно из определения МСЭ. Несмотря на небольшие концептуальные расхождения между обоими терминами, они в значительной степени перекрываются, особенно в том, что касается основных целей защиты доступности, целостности и конфиденциальности информации. Некоторые организации используют термин «кибербезопасность» как синоним термина «информационная безопасность». Другие считают, что термин «кибербезопасность» заменил более традиционный термин «информационная безопасность», хотя и с потерей некоторых его более широких значений и коннотаций, связанных с информационными системами, в пользу свойств, скорее характеризующих информационно коммуникативные технологии (ИКТ); есть и те, кто использует термин «кибербезопасность» как общий термин, включающий как «информационную безопасность», так и более узкий (и реже используемый) термин «безопасность ИКТ», который конкретно относится к безопасности инфраструктуры ИКТ (например, оборудования программного обеспечения, сетей и технических процессов).

Признание важности кибербезопасности международным сообществом и Организацией Объединенных Наций. Понимание того, что враждебная деятельность в киберпространстве составляет угрозу как для международного

сообщества, так и, конкретно, для организаций системы Организации Объединенных Наций, получило документальное отражение в резолюциях и докладах соответствующих директивных и руководящих органов и механизмов внутренней координации, по крайней мере, с начала 1990-х годов. Предметные дискуссии по этому вопросу идут по параллельным направлениям. С одной стороны, они ведутся государствами как членами директивных и руководящих органов Организации Объединенных Наций, разрабатывающих глобальные меры реагирования на появление киберпреступности и кибер-угроз («обращенный вовне» аспект работы Организации Объединенных Наций в области кибербезопасности, в отношении которого компетенция общесистемной координации принадлежит Комитету высокого уровня по программам Координационного совета руководителей системы Организации Объединенных Наций — КСР), и, с другой стороны, организациями системы Организации Объединенных Наций, стремящимися усилить, как коллективно, так и самостоятельно, свою внутреннюю организационную готовность и меры реагирования на связанные с этим проблемы («обращенный вовнутрь» аспект, входящий в компетенцию Комитета высокого уровня по вопросам управления). Признание двуединой роли системы Организации Объединенных Наций в этом вопросе подтверждается заключительными словами выступления Генерального секретаря, которое он сделал в рамках КСР не так давно, в 2019 году: «Системе Организации Объединенных Наций необходимо взять на себя ведущую роль и выработать единую позицию в отношении кибербезопасности и угроз в этой области, одновременно служа платформой для обсуждения государствами-членами и другими заинтересованными сторонами вопросов кибербезопасности в ее различных аспектах»(СЕВ/2019/2, para. 39.).

Кибербезопасность или cyber security – это меры, которые принимают для защиты данных или устройств, которые подключены к сети, от несанкционированного доступа и использования в преступных целях. Кибербезопасность – это то, что обеспечивает конфиденциальность, целостность и доступность данных на протяжении их всего жизненного цикла. Если физическая безопасность направлена на защиту от преступной деятельности или случайного повреждения людей и физического имущества, то кибербезопасность защищает компьютерные и серверные системы, приложения пользователей и данные, которые они в них хранят. Кибербезопасность может защитить все: от личной информации до сложных государственных систем.

Взгляды и опыт детей необходимо учитывать при разработке директивных мер, регулирующих использование молодежью цифровых технологий, а также при разработке самих технологий. ЮНИСЕФ поддерживает проекты Global Kids Online и Disrupting Harm, направленные на сбор данных о цифровых правах, возможностях и рисках для детей, чтобы лучше понять, как использование цифровых технологий способствует их развитию и когда оно усиливает риск причинения им вреда.

Учреждения ООН и партнеры, включая новаторов из частного сектора, работают над повышением безопасности в Интернете, особенно для детей и

молодежи. При поддержке МСЭ, ЮНИСЕФ и ЮНОДК День безопасного Интернета отмечается ежегодно в феврале месяце. День безопасного Интернета направлен на повышение осведомленности о новых проблемах и вызовах в цифровой сфере. Приложение 2.

Чаще всего источниками рисков в Сети становились незнакомые люди. Этим рискам подвержены не только взрослые, но и подростки и даже дети младшего школьного возраста. Например, в 2017 году в ходе опроса Фонда «Национальные ресурсы образования» о наличии в сети Интернет-угроз для несовершеннолетних высказались 93% из 5 тысяч респондентов.

По их мнению, подростки становятся жертвами мошеннических действий, сталкиваются с нежелательным для психологического развития содержанием, принимают за истину ложную информацию, а также порой неумышленно, по незнанию, сами совершают в сети противоправные действия. По их мнению, подростки становятся жертвами мошеннических действий, сталкиваются с нежелательным для психологического развития содержанием, принимают за истину ложную информацию, а также порой неумышленно, по незнанию, сами совершают в сети противоправные действия.

Безусловно, проведение комплексной работы с детьми остается в первую очередь за родителями. При этом сложно переоценить и тот вклад, который может внести школа. Для современных школьников именно учитель, а не интернет и компьютер, остается центральной фигурой в учебной и внеучебной деятельности — только 1,5% подростков считают, что учеба стала бы интересней, если бы преподавателя полностью заменили компьютерные технологии. Цифровое обучение приветствуют 47% школьников, но только в том случае, если будут использоваться современные увлекательные программы, а вторую половину урока будет интересно вести учитель. Каждый пятый подросток считает, что компьютер уместен не на всех предметах и не на каждом уроке, а 7% учащихся полностью отказались бы от компьютера в пользу занятий с учителем, способным организовать разные формы работы для всего класса. Половина подростков от 13 до 18 лет считают, что для положительного воздействия школы на учеников нужны доверительные отношения между учителями и учащимися, а 41% школьников полагает, что педагоги должны быть авторитетами для своих учеников. Почти половина школьников (42%) считают, что в случае нарушения их прав нужно обратиться к учителю.

Как сообщил портал Mel.fm, с сентября 2019 года в расписании британских школ появились уроки, где ученикам рассказывают об особенностях взаимоотношений между людьми, безопасном общении в Сети и заботе о своем психическом здоровье. Занятия обязательные. Подобные занятия проводятся и в школах России. Материалы отобраны для помощи в обучении подростков безопасному использованию Интернета и повышения их цифровой грамотности.

На основе масштабного исследования «Kazakhstan Kids Online», проведенного по инициативе Министерства просвещения Республики

Казахстан, совместно с ЮНИСЕФ, выявлены значительные риски, сопряженные с использованием интернета детьми в Казахстане. Основным вывод исследования связан с необходимостью разработки стратегий по минимизации рисков и поддержке детей в цифровом мире.

Интернет становится важной частью жизни детей уже с раннего возраста. По исследованию, 5% из них впервые выходят в сеть в возрасте четырех лет или младше. 60% детей в возрасте от 9 до 10 лет и 66% детей от 11 до 12 лет уже имеют собственные аккаунты в социальных сетях и игровых платформах.

Один из наиболее тревожных выводов – 15,3% детей сталкиваются с чем-то негативным ежедневно, еженедельно или хотя бы раз в месяц в интернете. Это вызывает серьезные чувства расстройства у 11,7% детей, что подчеркивает неотложную необходимость в укреплении кибербезопасности среди младшего поколения.

Статистика также показывает, что многие дети, ставшие свидетелями кибербуллинга (52,1%), предпочитают об этом никому не говорить. Только 17,6% родителей используют инструменты блокировки запрещенного контента и фильтрации вредного материала.

В ответ на эти вызовы Комитет по охране прав детей Министерства просвещения рекомендует родителям приложение «Родительский Контроль». Это эффективный инструмент, который позволяет обеспечить безопасность детей в онлайн-пространстве. Приложение доступно для скачивания на платформах PLAY MARKET и APP STORE.

«Родительский контроль – это лишь часть общей стратегии по обеспечению безопасности детей в интернете. Важно поддерживать открытый диалог с детьми и регулярно обсуждать их онлайн-жизнь. Мы убеждены, что родители, педагоги, ИКТ-специалисты и СМИ играют важную роль в обеспечении безопасности детей в интернете», – отметила Насымжан Оспанова, председатель Комитета по охране прав детей Министерства просвещения республики Казахстан.

Комитет по охране прав детей намерены проводить широкомасштабные кампании, направленные на повышение осведомленности родителей о важности использования приложений родительского контроля и обучение их эффективным методам обеспечения безопасности детей в онлайн-пространстве.

В марте 2021 года Комитет ООН по правам ребенка принял Замечание общего порядка №25 (GC25), направленное на помощь государствам и некоммерческим организациям в толковании Конвенции ООН о правах ребенка в цифровую эпоху. Вместе с экспертами и организациями по всему миру более 700 детей из 27 стран помогли сформировать этот по истине важный документ.

Замечание общего порядка № 25 о правах детей в связи с цифровой средой было запущено в Австралии, в честь чего 15 июня 2021 года состоялась онлайн-встреча, подготовленная фондом 5RightsFoundation совместно с исследовательским центром Young & Resilient. В рамках данного события произошло обсуждение возможностей воплощения некоторых рекомендаций данного документа в Австралии. В рамках данной встречи эксперты

представили свои отчеты об информировании детей по вопросам GC25. С докладами выступили профессор Барни Гловер, вице-канцлер и президент Западного Сиднейского университета; профессор Аманда Терд и Лилли Муди, Исследовательский центр Young and Resilient Западного Сиднейского университета; Джули Инман Грант, Австралийский комиссар по вопросам безопасности и Маргарет Шихан, генеральный директор Австралийского детского фонда.

После докладов состоялась панельная дискуссия «Права детей на данные: Что дальше для Австралии? с участием Линды Рафтри, соавтором Манифеста ЮНИСЕФ по управлению детскими данными. <http://www.fid.su/>

Более 60% подростков в возрасте 14-15 лет проводят в Сети 3 и более часа

9 из 10 учащихся каждый день используют Интернет для общения в мессенджерах и социальных сетях

Учащиеся не склонны воспринимать Интернет в качестве источника угроз

82% не испытывают сложности с поиском нужной информации и определением нужных источников в сети

Недостаточно внимания уделяется тому, что активность в Сети может отслеживаться

Навык использования специальных сервисов по фактчекингу имеет слабое распространение.[4]

Более 60% подростков в возрасте 14-15 лет проводят в Сети 3 и более часа.

Как показало исследование, 92% школьников в возрасте 14-15 лет предпочитают пользоваться мобильным Интернетом. Этот показатель чуть выше среди девушек и в казахско язычной среде и ожидаемо снижается в группе тех, кто находится в сети Интернет каждый день 5 и более часов.

В целом структура ежедневного пользования Интернетом по продолжительности в часах, полученная по результатам опроса, указывает на то, что более 60% подростков в возрасте 14-15 лет проводят в Сети 3 и более часа. Причём, по мере повышения ежедневной продолжительности пользования Интернет, доля парней, пользующихся Интернетом понижается, а доля девушек, наоборот, увеличивается.

Та же тенденция наблюдается и в зависимости от языка обучения. Среди учеников школ с казахским языком обучения доля тех, кто пользуется Интернетом, уменьшается в зависимости от продолжительности в часах. А в школах с русским и другим языком обучения — увеличивается.

9 из 10 учащихся каждый день используют Интернет для общения в мессенджерах и социальных сетях

Всем известно, что Интернет привлекателен для подростков не только как источник информации, но и как средство для общения, познания, самовыражения и признания. Это подтверждают и полученные нами результаты опроса:

- 8 из 10 каждый день смотрят YouTube, 8 из 10 каждый день заходят в Сеть в учебных и образовательных целях.

Наиболее популярными занятиями в Интернет среди подростков 14-15 лет согласно анкетированию, получены данные:

80-91% — пользование интерактивными ресурсами: мессенджерами, социальными сетями, YouTube, которые позволяют не только познавать новое, но и общаться как в одностороннем (комментирование, размещение публикаций, постов, видео и т.д.), так и в двустороннем порядке (обмен сообщениями, фото, аудио, видео и т.д.). Данные ресурсы больше востребованы среди девушек и в русскоязычной среде.

57-79% — образовательные и познавательные ресурсы: поиск информации при подготовке домашнего задания, использование образовательных порталов, поиск информации по интересам. Данные ресурсы больше востребованы среди девушек и в казахскоязычной среде.

29-55% — ресурсы развлекательного характера: онлайн-игры, онлайн-кинотеатры и интернет-магазины. Эти ресурсы больше востребованы среди парней и в русскоязычной среде.

47-49% — новостные ресурсы. Эти ресурсы больше востребованы среди парней и в казахскоязычной среде.

Гипотеза, которую удалось проверить, гласит, что из-за неудач в учебе, дети пытаются уйти от проблем в другую реальность, чтобы реализоваться там, что приводит к более длительному нахождению онлайн. Согласно данным по продолжительности ежедневного пользования Интернет в часах, отмечается незначительное превышение доли пользования 5 и более часов в группах с успеваемостью «по всем предметам получаю оценку «4» и «3» (в среднем 27%) и по всем предметам получаю оценку «3» и ниже» (при среднем показателе 25%).

При этом распределение ответов по видам Интернет - активности вызывает недоумение факты, что в группах с успеваемостью на оценку «4» и «3» и на «3» и ниже заметно больше доли тех, кто предпочитает играть в онлайн-игры (36% и 39% при среднем показателе 28%), смотреть художественные фильмы (22% и 26% при среднем показателе 21%) и смотреть видео на YouTube (55% и 58% при среднем показателе 52%).

Результаты исследования позволяют говорить о связи между успеваемостью в учебе и выбором активностей в сети Интернет, но, к сожалению, данных для определения зависимости переменных и наличия эскапистской тенденции в поведении подростков с низкой успеваемостью — недостаточно.

Сетевые угрозы безопасности детей.

Мошенничество в отношении детей.

Признаки интернет-мошенничества бывает непросто распознать даже взрослым. Совершать противоправные действия в сети преступники могут как через Интернет, так и через локальное подключение. В России хищение чужого имущества или приобретение права на чужое имущество путем ввода,

удаления, блокирования, модификации компьютерной информации определяется законодательством как «Мошенничество в сфере компьютерной информации». Ответственность по указанной статье наступает с 16 лет. [5]

Возможные схемы мошенничества:

1) Фишинг (получение доступа к логинам, паролям, банковским данным). Мошенники организуют рассылку сообщений якобы от имени банка со ссылками на поддельные страницы официальных сайтов. Вводя свои персональные данные (номера банковских карт, логины, пароли), жертва неосознанно передает конфиденциальную информацию мошенникам. А те, в свою очередь, используют сведения для завладения денежными средствами. Для предупреждения школьников о подобных схемах мошенничества можно:

- рассказать о специализированных интернет-ресурсах проверки сайтов на факты совершения мошеннических действий (например, сайт <https://довериевсети.рф/>) и других сервисах контроля репутации сайта на предмет мошеннических действий (негативные отзывы, жалобы на сайт, проверка на вирусы). Напомнить, что достоверный сайт обязательно содержит сведения об авторах и их контактные данные;

- обратить внимание детей на то, что нельзя вводить данные банковских карт на сомнительных сайтах интернет-магазинов (cvc/cvv-код, срок действия, номер карты);

- напомнить, что никому не стоит передавать или выкладывать в Сеть конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес прописки и фактического места жительства, слишком личные фотографии;

2) *Поддельные интернет-магазины.* В интернете существует большое количество поддельных магазинов, недобросовестных продавцов и лжепредпринимателей, которые могут обмануть, не предоставить товар или завладеть персональными данными для мошеннических действий. При заказе через Интернет нужно руководствоваться некоторыми правилами:

- обязательно нужно проверить интернет-магазин перед совершением покупки: на официальном сайте должны быть приведены сведения о правоустанавливающих документах, соглашение на использование и обработку персональных данных, адрес фактического расположения, данные о потребительских свойствах товара.

- не сообщать свои персональные данные и не переводить денежные средства лицам, которые не являются сторонами сайта. Развитие интернет-торговли нередко вызывает у ребят желание не только купить, но и начать продавать товары. Некоторые школьники организуют группы продаж товаров из Китая, например, с площадок Aliexpress, некоторые выставляют на продажу свои поделки, творческие работы, личные вещи, размещают объявления об оказании услуг. Посоветуйте детям не продавать товары через неспециализированные интернет-сайты, социальные сети, рассылку рекламных сообщений. За регулярное распространение товаров и услуг, осуществляемое с нарушениями, можно быть обвиненным в незаконном предпринимательстве.

3) *Сборы средств на «благотворительность».* В социальных сетях все шире распространяется практика сбора средств на лечение, питание, покупку медикаментов и оборудование, помощь в трудной жизненной ситуации как для людей, так и для животных. Желание помочь — очень благородный порыв, но лучше убедиться, что эта помощь достигнет адресата. Злоумышленники могут симитировать официальную страницу по сбору средств для благотворительных целей, указав при этом свой расчетный счет. Часто это происходит во время ликвидаций последствий аварий и катастроф, терактов с большим количеством пострадавших: люди торопятся оказать помощь нуждающимся, не тратят времени на проверку информации, а потому иногда переводят деньги мошенникам.

Что можно сделать?

- проверить источник: для какой группы в социальных сетях происходит сбор пожертвований;
- проверить через поисковик, существуют ли аналогичные группы, направленные на поддержку этому же человеку, животному, организации — иногда мошенники делают страницу-клон в надежде перехватить часть посетителей сообщества с хорошей репутацией;
- связаться с администраторами группы для уточнения деталей, задавая им при этом как можно больше вопросов, позволяющих определить их причастность к этому сбору средств;
- постараться связаться с родственниками/ представителями лица или лиц, для которых организован сбор средств.

Иногда в ходе длительного онлайн-общения собеседник начинает ссылаться на наличие проблем, решение которых требует финансовых средств. Расскажите ученикам, что не следует без обсуждения со взрослыми переводить деньги малознакомому человеку, с которым общались только в режиме онлайн, какие бы причины ни называл собеседник (операции, долги, «проблемы, о которых не расскажешь родителям»).

4) *Вирусный контент.* Меняет или полностью блокирует доступ к персональному компьютеру. В такой ситуации пользователю часто приходит требование осуществить перевод или отправить СМС на предлагаемый номер для восстановления пароля. В других случаях компьютер может подвергнуться заражению «трояном», который делает доступными для злоумышленников личные данные.

Стоит относиться с осторожностью к скачиванию программных продуктов из файлообменных сетей и торрентов. Подозрительные файлы не открывайте и не сохраняйте. Не отвечайте на сомнительные рассылки. И главное — не посещайте ресурсы с неоднозначной репутацией, которые вызывают у вас (или у вашей антивирусной программы) любые подозрения.

5) *Информация о легком заработке.* Сейчас в Сети набирают популярность объявления о легком и высоком заработке для подростков. Зачастую такая работа связана с вовлечением ребят в мошеннические или преступные схемы. Как правило, речь идет о распространении наркотических

средств: подростки делают «закладки» в назначенных куратором местах, а затем их забирают клиенты. Стоимость такой подработки для школьников весьма привлекательна. Нередко ребята соглашаются, не догадываясь о характере доставляемого товара. Но иногда желание заработать перевешивает здравый смысл, и некоторые подростки соглашаются участвовать в распространении наркотиков, рассчитывая остаться безнаказанными.

Опасности, которым дети подвергают себя и других при использовании сети Интернет.

Съемка фото и видео для размещения в сети Интернет, сопряженная с опасностью для жизни и здоровья.

В последнее время среди интернет-пользователей набирает популярность фото- и видеосъемка как повседневных, так и ярких жизненных моментов, и размещение данного контента в сети Интернет. Некоторые примеры такого поведения детей:

Подросток становится невольным свидетелем вооруженного конфликта, стрельбы, взрыва и первым делом снимает происходящее на мобильный телефон. Вместо того чтобы предпринять необходимые меры безопасности (убежать, вызвать полицию), он снимает «уникальное видео» ради популярности в Сети, рискуя жизнью и здоровьем.

Выбор подростком опасных или экстремальных увлечений. Например, «руфтинг» (прогулки по крышам), «скайуокинг» (покорение самых высоких точек в городе без специального снаряжения) или «зацепинг» (проезд вне салона электропоезда, трамвая – на крыше или подножке). Ради популярности в Интернете дети стремятся заснять свои «подвиги», что ведет к негативным последствиям. Такие увлечения сами по себе представляют смертельную опасность, а использование камеры только увеличивает риск оступиться, потерять равновесие или не заметить угрозу.

Стремление поразить интернет-друзей яркими или опасными фотографиями, сделанными в формате селфи. Селфи на воде, на краях обрывов или скал, на железных и автомобильных дорогах, на крышах домов или промышленных объектов, вблизи линий электропередач могут привести к крайне негативным последствиям для жизни и здоровья ребенка.

Предотвратить подобные ситуации можно через формирование у обучающихся культуры личной безопасности. Она состоит в готовности защитить себя и окружающих от неблагоприятного воздействия, угроз и наступления нежелательных последствий. Подростку можно объяснить, что при возникновении опасных ситуаций необходимо в первую очередь, позаботиться о безопасности себя и других людей, а затем вызвать полицию. При беседе на тему опасных увлечений нужно постараться принять точку зрения ребенка, услышать от него аргументы в пользу его хобби. Главное – занять доброжелательную позицию со своей стороны, ненавязчиво предложить альтернативные виды деятельности, проходящие в безопасных условиях. Важно не переусердствовать, но при этом донести до ребенка посыл, что он не безразличен вам, своей семье, близким и друзьям.

Игнорирование опасности в виртуальной среде.

Зачастую происходящее в сети Интернет не воспринимается подростками как часть реальной жизни. В большинстве случаев дети воспринимают сетевое общение как игру, не понимая, что за экраном — живые люди со своими представлениями, мнением, реакциями на то или иное явление.

Например, школьник публикует в социальных сетях сообщения, призывающие к деструктивному действию. Но друзья учащегося или ребята из его класса не воспринимают такие публикации всерьез и оставляют данный факт без внимания.

Для профилактики подобных ситуаций можно предпринять следующее:

- объяснить обучающимся, что такие публикации могут представлять реальную опасность;
- донести до подростков, что сообщить о таких публикациях учителям и родителям — осознанный поступок взрослого человека;
- напомнить, что все случаи стрельбы или вооруженного нападения в школах начинаются с публикаций в социальных сетях, которые никто не воспринимает всерьез;
- объяснить ребятам, что лучше лишний раз перестраховаться и сообщить об угрозе, чем рисковать своей жизнью и жизнью своих одноклассников;
- по возможности лично обращать внимание на содержание контента, размещаемого учениками в социальных сетях;
- провести аналогичные мероприятия с родителями обучающихся, ознакомить их с информацией, сообщенной ранее подросткам.

Основные типы злоумышленников в киберсреде

- **Хакеры.** Лица или группы, которые взламывают сети, чтобы дезорганизовать, повредить или парализовать их, в основном ради известности или самоутверждения.
- **Хактивисты.** Хакеры с определенными мотивами, которые рассматривают свою деятельность как форму гражданского неповиновения или как средство политического или идеологического самовыражения.
- **Киберпреступники.** Лица, которые участвуют в преступной деятельности с использованием информационных технологий (уголовных преступлениях, таких как мошенничество, кража, вымогательство и т. п., с помощью компьютеризированных средств) или в преступной деятельности в среде информационных технологий (например, распространение вирусов или вредоносных кодов и другие действия, которые могут быть совершены только в среде компьютеризированных средств). В зависимости от уровня технической подготовки и организационного потенциала участники такой деятельности могут быть разными, от небольших группировок до крупных организованных преступных сообществ.
- **Лица, занимающиеся промышленным шпионажем.** Злоумышленники этой категории, которых иногда выделяют в отдельную подкатегорию преступников, преследуют специфические цели — получение

сведений, составляющих коммерческую тайну, шантаж с целью получения экономических выгод или причинение ущерба конкурентам — и чаще всего встречаются в корпоративном мире.

- Государственные или действующие при поддержке государства группы. Злоумышленники с серьезной квалификацией и хорошо обеспеченные ресурсами, чью деятельность, как правило, трудно обнаружить, отследить или идентифицировать, которые могут скрытно преследовать сложные, часто косвенные и неочевидные цели и непосредственно привлекаются или косвенно финансируются государственными властями или военными структурами. В прошлом государства в основном создавали потенциал проведения расследований, но в последние годы стало общепризнанным фактом, что некоторые из них приобрели еще и потенциал наступательных действий.

- Инсайдеры. Субъекты, которые в силу договорных отношений с данной организацией не считаются внешними, создавая угрозу для нее изнутри. К ним, в частности, могут относиться недовольные сотрудники, плохо обученный персонал или сторонние обслуживающие организации. (доклад стр. 14) Противоправные действия детей в сети Интернет.

Какие действия подростков в сети Интернет могут привести к негативным последствиям:

Оскорбление личности в Интернете.

Важно проводить работу с подростками, направленную на повышение их правовой сознательности. Обучающиеся несут ответственность за то, что пишут в сети Интернет, и должны об этом знать. Ученикам можно рекомендовать:

- не вступать в перепалку с теми людьми, целью которых является осознанная провокация другого человека на проявление эмоций;

- не реагировать на оскорбительные сообщения, прекратить общение и закрыть страницу от посторонних лиц. Следует разъяснить школьникам, что не стоит стесняться рассказывать учителям и родителям об угрозах, полученных через Интернет. В таком случае есть шанс наиболее достойного выхода из ситуации. Цель интернет-провокаторов — специально запугать человека, но сами они очень боятся ответственности.

Важно обратить внимание подростков, что если они сами являются агрессорами в интернет - среде, ошибочно думать, что об этом никто не узнает.

Переписка может очень быстро распространиться в Сети и служить доказательством действий, противоречащих нормам права.

Травля в Интернете: кибербуллинг.

Изменение психологической обстановки в классе может являться свидетельством начала травли одного или нескольких учеников. Об этом могут говорить насмешки одноклассников над сверстником, чрезмерное увлечение неопределенными видео в телефонах.

Если вам кажется, что в детском коллективе негативная обстановка, но еще неясно, кто является жертвой, необходимо установить лидера и аутсайдера группы. Также полезно понимать, кто в классе является интровертом, а кто —

экстравертом. Как правило, больше страдают интроверты — они чувствительнее к нарушению границ, и их проще ранить. Определение социальных ролей в классе поможет понять, кому необходима помощь, а чьи границы лучше не нарушать.

Переход травли в активную фазу нельзя оставлять без внимания. Оскорбления, драки, неуместные шутки необходимо пресекать. Важно провести беседу со всеми участниками конфликта. Бездействие в подобной ситуации невозможно, иначе конфликт может зайти очень далеко, а его последствия могут быть очень печальными для всех его участников. Важно, не осуждать только зачинщика травли. Скорее всего он действует так, потому что его поддерживает весь класс. Целесообразно привлекать к разбору ситуации педагога-психолога. Специалист сможет поддержать жертву травли, организовать беседу с участниками конфликта и дать рекомендации о необходимости подключения родителей и других одноклассников к разрешению проблемы.

Подросткам, ставшим жертвами буллинга в Интернете, необходимо рекомендовать обращаться к родителям и педагогам в случаях продолжения агрессии в свою сторону даже после ограничения доступа к своему аккаунту. Взрослые помогут принять адекватное и взвешенное решение.

Родители представляют интересы несовершеннолетних детей, поэтому должны быть в курсе происходящего с ними. Информацию до них необходимо доносить аккуратно, но настойчиво. Родителям стоит рекомендовать следить за эмоциональным состоянием ребенка. В том случае, если ребенок явно подавлен и напуган, родителям целесообразно получить доступ к его аккаунтам в социальных сетях, чтобы определить, исходит ли угроза от тех людей, с которыми он общается в Сети.

- Следует обратить внимание обучающихся на следующие моменты:
- в интернет-травле они могут оказаться как по одну, так и по другую сторону;
- любая переписка может храниться очень долго (минимум полгода), к тому же любые материалы сейчас можно сохранить, создав архив;
- даже при использовании VPN-сервисов, предотвращающих отслеживание активности в Интернете, есть другие способы установления зачинщика интернет-травли.

Майнинг криптовалюты.

Заработок в Интернете обрел большую популярность, особенно среди подростков. Новым видом деятельности, приносящей доход посредством использования интернет-технологий, стала добыча виртуальной криптовалюты (майнинг). Вместе с тем такой заработок представляет собой опасность как для жизни и здоровья детей, так и для окружающих людей. Ведь для этой деятельности необходима «майнинг ферма» — большое количество специального оборудования, сосредоточенного в одном помещении. Электропроводка в жилых домах не рассчитана на такие нагрузки. Поэтому при майнинге риск пожара в домах существенно увеличивается. Случаи возгорания

из-за работы «майнинг ферм» уже имели место. Например, в городе Артем Приморского края пожар разгорелся на площади 500 квадратных метров, в результате чего выгорели полностью восемь квартир. Похожий инцидент произошел в Томской области, когда проводка домов не выдержала нагрузки, в результате случилось короткое замыкание.

Помимо этого «майнинговые фермы» создают повышенный уровень шума. Чаще всего это связано с работой системного оборудования, но также сильный шум могут создавать кондиционеры, круглосуточно работающие для охлаждения помещений. Регулярное шумовое воздействие неблагоприятно сказывается как на нервной системе, так и на ходе сна. Для восстановления и отдыха человеку необходима спокойная бесшумная обстановка. После длительного нахождения в шумном помещении человек может испытывать повышенную раздражительность и утомляемость, качество сна ухудшается.

Риски, связанные с использованием теневых ИТ.

Сообщается, что это явление получило распространение в некоторых организациях, особенно в их отделениях на местах или подразделениях, которые иным образом дальше отстоят от централизованного контроля. В таких условиях риски часто усиливаются тем, что центральные подразделения ИКТ и кибербезопасности имеют ограниченное представление об используемых на местах ИКТ. И в этом случае пандемия COVID-19, внезапно потребовав удаленного выполнения многих функций, еще больше усугубила эту проблему, поскольку многие пользователи начали использовать средства сетевого взаимодействия, включая конференцсвязь, помимо решений, включенных в используемые организациями пакеты программного обеспечения. Однако многие услуги, к которым пользователи обращались в качестве потенциальных альтернатив, не были изучены или одобрены для массового использования специалистами организаций по кибербезопасности, что может создавать риск для организаций (например, из-за того, что применяются не стандарты, которые рекомендованы на уровне организации в отношении аутентификации или конфиденциальности, а другие стандарты). Так, в самом начале пандемии Специальная группа по информационной безопасности изучила использование одной популярной онлайн-платформы видео конференц-связи, чтобы оценить ее пригодность для использования организациями системы Организации Объединенных Наций, однако эксперты по кибербезопасности не смогли прийти к окончательному и однозначному решению — рекомендовать или не рекомендовать ее, — которое было бы действительным для всей системы. Вместо этого они изложили ряд вариантов, а также предостережений и мер предосторожности, которые следует учитывать при использовании этой онлайн-платформы в определенных условиях.

Некоторые предложения по более тщательному контролю за теньвым ИТ. Инспекторы считают, что проблемы кибербезопасности, связанные с использованием теневых ИТ, требуют большего внимания с уравниванием необходимости контроля в среде, подверженной киберрискам, и оправданными целями и конструктивной мотивацией пользователей к инновациям и

использованию альтернативных решений при их наличии. В этой связи имеются основания не считать сразу нежелательным стремление некоторых пользователей использовать теневые ИТ-решения, поскольку считается здоровым признаком готовности к инновациям, для которых подразделения, как правило, должны иметь определенные ресурсы и свободу действий, в идеале в безопасной и защищенной вычислительной среде. В этой связи могут быть восприняты, например, такие идеи: создание или расширение безопасных сред для цифровых инноваций; привлечение внимания к развитию распределенных ИКТ в более децентрализованных условиях с привлечением местных координаторов ИКТ; а также активизация обучения конечных пользователей и мер по повышению осведомленности для получения надежной и четкой информации о безопасности и рисках использования сторонних сервисов вне стандартных процедур и практики и информации об утвержденных организацией альтернативах, а также рекомендаций о более безопасном использовании таких решений. (доклад ООН)

Важность кибербезопасности в цифровую эпоху. В современном цифровом мире кибербезопасность стала важным вопросом для международных организаций, и организации системы Организации Объединенных Наций не являются исключением. Цифровая трансформация, растущая зависимость от информационно-коммуникационных технологий (ИКТ) и кибер-решений, а также тот факт, что угрозы для кибербезопасности постоянно растут, как по изощренности, так и по разрушительному потенциалу, привели к беспрецедентному увеличению рисков для кибербезопасности, с которыми сталкиваются Организации системы Организации Объединенных Наций. Инциденты, которые когда-то считались экстраординарными, становятся все более частыми и обычными. Инспекторы напоминают письмо, адресованное Генеральному секретарю в 2017 году, в котором представители комитетов по надзору системы Организации Объединенных Наций, собравшиеся на свое организованное впервые совещание, в числе трех основных проблем, вызывающих озабоченность у организаций системы Организации Объединенных Наций назвали необходимость того, чтобы руководство уделяло должное внимание новым и возникающим рискам, в частности глобальным и критическим для деятельности организаций угрозам, возникающих для кибербезопасности, а также рискам, появляющимся в результате новых способов работы по мере ускорения цифровой трансформации (Письмо на имя Генерального секретаря от 26 января 2017 года.). этой связи организации — участницы Объединенной инспекционной группы (ОИГ) поддержали изучение ОИГ правил и практики кибербезопасности, имеющих в системе Организации Объединенных Наций, которое было проведено ОИГ в рамках ее программы работы на 2020 год, став последним из серии обзоров на технологическую тематику по таким вопросам, как управление ИКТ, ведение интернет-сайтов и использование услуг облачных вычислений (JIU/REP/2008/5; JIU/REP/2008/6; JIU/REP/2011/9 и JIU/REP/2019/5.).

С учётом широкого проникновения в повседневную жизнь интернета тема кибербуллинга в социальных сетях становится всё более актуальной с разных точек зрения (имеет широкий общественный резонанс и исследуется социологами, педагогами, психологами). Кибербуллингом занимаются люди разных возрастных групп: дети, подростки, взрослые. Для разных возрастных групп применяются разные термины, которые очень быстро получают распространение в средствах массовой информации и интернет-пространстве: «киберхарассмент», «киберсталкинг», «нецивилизованность онлайн», «кибернецивилизованность». [6]

В современном цифровом мире мы уже не представляем свою жизнь без постоянного доступа в Интернет, общения в социальных сетях, возможности расплачиваться в магазинах телефоном и даже иметь удостоверение личности на смартфоне. Наиболее активными пользователями являются люди в возрасте 13–24 лет. Согласно различным опросам, 27% респондентов-подростков проводят в социальных сетях более 5 часов в день, а четверть из них проверяют обновления каждые полчаса [7]

Но в этом быстром цифровом развитии есть и другая сторона — кибератаки злоумышленников, которые хотят похитить ваши личные данные, навредить бизнесу или своровать ваши деньги с банковской карты. Чтобы ничего из вышеперечисленного с вами не произошло, важно знать, как защитить себя от подобных случаев. Поможет в этом кибербезопасность и в данном материале мы подробно расскажем все о кибербезопасности: как работает кибербезопасность, какие есть виды кибербезопасности, а также расскажем все, что нужно знать для кибербезопасности.

Анализ особенностей трансформации ролевой структуры кибербуллинга в сети в сравнении с буллингом в реальной жизни у пользователей популярных социальных сетей позволил выявить личностные характеристики и поведенческие стратегии его участников. Особенное внимание заслуживают «свидетели» кибернасилия: чем больше респондент является «свидетелем», тем больше вероятность у него стать «инициатором» кибербуллинга (умеренная положительная корреляция между шкалами «свидетель» и «инициатор»). С одной стороны, прошлый опыт в роли агрессора в онлайн-контексте может быть тем фактором, который усиливает негативное поведение свидетелей, с другой стороны, постоянное наблюдение за травлей в онлайн-сети может привести к потере чувствительности в отношении чувств других людей, а также к закреплению деструктивных форм поведения за счёт осознания безнаказанности и анонимности в онлайн-среде. [6]

Дети и подростки были связаны и зависимы от использования Интернета и других социальных сетей во время пандемии COVID19 как для обучения, так и для общения. Вынужденная изоляция из-за болезни сделала многих из этих молодых людей более уязвимыми для действий хулиганов. Кроме того, поскольку онлайн-среда стала основным форумом для выражения идей во время карантина, вызванного пандемией, количество онлайн-контента, используемого подростками, оказывает негативное влияние. Преступники не

осознают вреда и вреда себе и другим в результате своих действий в сети. Среди них рычание, горе как эффект, возникающий в результате кибербуллинга. Что-то сбивает с толку, так это трудности жертвы в ограничении и отрицании негативного влияния кибербуллинга. Несмотря на некоторые разногласия в книгах по поводу значения кибербуллинга, общей чертой считается наличие «намерения причинить вред жертве» со стороны агрессора [8]

Интернет является причиной проблемы кибербуллинга, которая возникает среди детей и подростков. Также невозможно, чтобы дети в будущем не пользовались интернет-СМИ, потому что они не могут решить проблему кибербуллинга. Сейчас это требует реального внимания и действий. Самооценка детей, которые становятся преступниками и жертвами кибербуллинга, безусловно, отличается от тех, кто этого не испытывает. Кроме того, последствия кибербуллинга связаны с отчаянием или самоубийством. Было показано, что хулиганы, их жертвы и жертвы хулиганов испытывают эмоциональные и поведенческие проблемы. По этой причине крайне важно сосредоточиться на хулиганах и жертвах агрессии, а также на детях и молодых людях, ставших жертвами. Некоторые методы кибербуллинга, такие как опыт жертв и преступников, включают обмен мгновенными сообщениями, чаты и электронную почту. Несмотря на неблагоприятные последствия кибербуллинга, исследования показали, что большинство подростков не предпримут никаких действий, если узнают об инциденте кибербуллинга с участием друга или одноклассника. Причина, которую молодые люди назвали для этого, состоит в том, чтобы избегать конфликтов и поддерживать групповую гармонию. Это предполагает, что молодые люди должны быть более осведомлены о последствиях инцидентов кибербуллинга, поскольку исследования ясно показывают очень неблагоприятные последствия получения сообщений о кибербуллинге [8]

Общее определение киберзапугивания описывает его как «онлайн-поведение, которое включает в себя три характеристики: (1) оно совершается отдельными лицами или группами с использованием электронных или цифровых средств массовой информации; (2) неоднократно передаются враждебные или агрессивные сообщения; и (3) поведение осуществляется с намерением причинить дискомфорт или причинить вред объекту» [9]

Киберзапугивание подростков отличается от традиционного буллинга. CDC (Центр противодействия заболеваниям в США) определяет традиционное издевательство как «любое нежелательное агрессивное поведение другого подростка или группы молодых людей, которые не являются братьями и сестрами, которое связано с наблюдаемым или предполагаемым дисбалансом власти и повторяется несколько раз или с высокой вероятностью повторится. Запугивание может причинить вред или страдания целевой молодежи, в том числе физический, психологический, социальный или образовательный вред». Киберзапугивание действительно включает в себя те же три основные характеристики: нежелательное агрессивное поведение, повторение сообщений

и причинение вреда жертве. Разница в том, что традиционный буллинг в основном происходит в школьных стенах, тогда как кибербуллинг может происходить в любое время суток [8]

Итак, кибербуллинг – это запугивание с использованием цифровых технологий, которые могут включать сотовые телефоны, электронную почту и приложения для социальных сетей. Кибербуллинг включает в себя [9]

- Розыгрыш: повторные зависания; анонимные, насмешливые или угрожающие телефонные звонки.
- Обмен изображениями: пересылка или обмен нелестными или личными изображениями без разрешения.
- Изображения откровенно сексуального характера. Пересылка или обмен изображениями сексуального характера с лицами моложе 18 лет является уголовным преступлением (детская порнография), за которое может быть возбуждено уголовное дело.
- Текст и электронная почта: отправка оскорбительных или угрожающих текстовых сообщений или электронных писем.
- Личная онлайн-информация: Публикация в Интернете чьей-то частной, личной или неловкой информации без разрешения или распространение слухов в Интернете.
- Кража личных данных: принятие чьей-либо личности в Интернете и негативное представление их таким образом, что это наносит ущерб их репутации или отношениям.
- Сайты ненависти: создание сайтов ненависти или реализация кампаний социального исключения с использованием приложений социальных сетей.

Как и в случае с обычным издевательством, кибербуллинг может включать использование технологии учащимся школы или несколькими учащимися для проведения кампании против другого учащегося. Это может включать в себя подготовку жертвы к нападению или унижению со стороны других, видеозапись их страданий и размещение видео в Интернете и так далее.

Несмотря на эти очевидные различия, между обычным и кибербуллингом также есть значительное сходство. Одним из них является наличие дисбаланса сил. У хулигана есть определенные уровни контроля над жертвой из-за его или ее намерения причинить вред жертве, унижить, смутить и беспокоить, а также мотивация изолировать или подвергнуть остракизму. Эти намерения одинаковы как в обычном, так и в кибербуллинге. Кроме того, виды поведения, характеризующие конвенциональное и кибербуллинг, совпадают. Хулиган распространяет слухи, угрожает или оскорбляет свою жертву. Традиционно дети, над которыми издевались, также вели себя так, а именно, чтобы поднять свой социальный статус, поддержать самооценку, из-за гнева и разочарования, из-за социальных проблем или из-за того, что над ними издевались.

Интернет играет важную роль в повседневности подрастающего поколения. Более 60% подростков в возрасте 14-15 лет проводят в сети 3 и более часов. На первом месте (80-91%) – пользование интерактивными

ресурсами, такими как мессенджеры, социальные сети, YouTube, которые позволяют не только ознакомиться с той или иной информацией, но и подразумевают двустороннюю или одностороннюю коммуникацию.

Исследование показывает, что в подростковой среде устоялось убеждение, что Интернет не представляет опасности для сохранности личных данных, хотя большинство отмечают важность конфиденциальности. При этом наблюдается сравнительно низкая популярность факт чекинговых сервисов – к ним хотя бы раз обращались лишь 29% учащихся.

В этой связи, может быть востребованными образовательные курсы по повышению медиа грамотности учащейся молодежи с фокусом на усиление навыков по проверке информации и усилению критического мышления. [10]

Под кибергигиеной подразумевается совокупность навыков и знаний, уменьшающих риски пребывания в сети. Это понятие складывается из нескольких составляющих. Важно знать об угрозах, подстерегающих пользователей на просторах интернета. Кибергигиена позволяет избежать многих опасностей. Каждый пользователь должен понимать, что работа в интернете таит в себе определенный риск. Осознание данного факта позволяет избежать множества проблем. Атаке мошенников может подвернуться любой пользователь.

Ни одна организация системы ООН не может утверждать, что она не подвергалась в какой-либо форме кибератакам большей или меньшей серьезности. Вредоносные действия, направленные против пользователей информационных систем (такие как фишинг, кража личных данных, перехват канала связи и т. п.) или инфраструктуры (вредоносное ПО, распределенные атаки «отказ в обслуживании» и т. п.), на сегодняшний день являются наиболее распространенным источником ставших известными угроз. Хотя угрозы кибербезопасности обычно связаны с современными технологиями и программными решениями, экспертное сообщество видит заметный сдвиг от хакерских атак на серверы, сети и конечные устройства к атакам на людей с использованием методов социальной инженерии, направленных на манипулирование людьми с целью выманивания у них конфиденциальной информации для мошеннических или других незаконных целей. Пандемия коронавирусной инфекции (COVID-19) еще больше усугубила риски, связанные с социальной инженерией: более двух третей участвующих организаций сообщили о резком усилении угроз и уязвимостей кибербезопасности во время глобальных ограничительных мер, которые лишили многих пользователей доступа к централизованно управляемым ресурсами кибербезопасности. [2]

В то же время сообщаемое влияние инцидентов, с которыми столкнулись участвующие организации, было ограниченным, что может привести к преждевременному выводу об отсутствии серьезных причин для беспокойства. Это не тот вывод, к которому пришли инспекторы. Во-первых, собранные данные неизбежно предполагают наличие некоторых не просматриваемых зон, в том числе возникающих из-за понятного нежелания раскрывать известный

уровень уязвимости и из-за непрозрачного характера киберактивности в целом, указывая на то, что точные масштабы угрозы и связанных с ней последствий может быть просто неизвестны. Чаще всего, особенно в случае более изощренных атак, злоумышленникам невыгодно раскрывать свое присутствие или использованные ими уязвимости, поэтому число проникновений в систему и утечек данных, вероятно, гораздо больше, чем сообщается. Доля «известных неизвестных» по сравнению с тем, что известно о масштабах угрозы кибербезопасности, велика, но доля «неизвестных неизвестных» может вызывать еще большее беспокойство. Таким образом, было бы ошибкой судить о серьезности угрозы по степени ее известной материализации в прошлом. Потенциал ущерба остается высоким и требует постоянного внимания и расстановки приоритетов.

Международный вычислительный центр Организации Объединенных Наций как ключевой поставщик услуг кибербезопасности для системы.

Международный вычислительный центр Организации Объединенных Наций в течение ряда лет предоставляет услуги по кибербезопасности примерно двум третям организаций системы Организации Объединенных Наций, хотя клиентская база каждой из его 13 связанных с этим услуг существенно различается. В этом разделе его каталога услуг наблюдается значительный рост по разным направлениям, при том, что на него по-прежнему приходится лишь небольшая часть бюджетных расходов Центра. Согласно отзывам участвующих организаций, они по-разному оценивали услуги кибербезопасности Международного вычислительного центра Организации Объединенных Наций, при этом «Общая аналитика угроз безопасности» была признана ее флагманской услугой. Еще в 2019 году ОИГ предлагала эффективнее использовать нереализованный потенциал Центра, особенно его услуги кибербезопасности. Организациям системы Организации Объединенных Наций и Центру рекомендуется найти больше точек соприкосновения, чтобы в возросших масштабах дополнить имеющиеся внутренние возможности организаций общими услугами. В этом духе исполнительным главам участвующих организаций предлагается пересмотреть нынешние договоренности организаций и вновь рассмотреть возможности использования предоставляемых Центром услуг кибербезопасности. Деятельность Международного вычислительного центра Организации Объединенных Наций как межучрежденческой структуры, функционирующей в соответствии с правилами и в рамках административной структуры Всемирной организации здравоохранения, основана на модели самоокупаемости и совместного обслуживания. Эта модель как содействовала, так и препятствовала превращению Центра в узел кибербезопасности всей системы. В результате возникла ситуация, в которой предложение услуг Международного вычислительного центра Организации Объединенных Наций зависит от предоставления клиентами авансового начального финансирования затрат на разработку новой услуги для удовлетворения спроса, в то время как многие могут позволить себе приобретение разработанной таким образом услуги

только после того, как на нее уже подпишется критическая масса клиентов. Учитывая проблемы, связанные с кибербезопасностью, и риски, с которыми сталкиваются организации, было сочтено своевременным изучить возможность использования добровольных взносов в качестве дополнительного механизма финансирования для прямого привлечения в больших объемах ресурсов для обеспечения кибербезопасности в рамках всей системы. Доклад.

Учащиеся не склонны воспринимать Интернет в качестве источника угроз.

С помощью виртуального пространства подросток может легко удовлетворить свои потребности в коммуникации, а также самостоятельно формировать круг своего общения. При этом вероятно, что они не до конца осознают риски, связанные с дезинформацией и манипуляциями в Сети. В этой связи важно определить уровень информационной грамотности подростков 14-15 лет посредством оценки навыков пользования информацией в Сети.

Проведенные исследования [10] позволили определить четыре группы навыков:

Навыки соблюдения принципов безопасности и защиты информации в сети Интернет.

Навыки поиска информации в сети Интернет.

Навыки критического восприятия информации в сети Интернет.

Навыки проверки и распространения информации в сети Интернет.

В целом, опрос показывает, что большинство учащихся придерживается базовых правил безопасности в Интернете. 69% стараются использовать двухфакторную аутентификацию. Примерно столько же опрошенных ограничивают контакты с незнакомцами в соцсетях и игнорируют сообщения с незнакомых адресов. 66% используют разные пароли для разных сервисов.

При этом надо отметить, что привычка открывать ссылки и сообщения, присланные с незнакомых адресов/контактов, больше характерна для парней, проживающих в сельской местности, посещающих школу с казахским языком обучения. Разные пароли на сервисах, как и использование антивирусных программ чаще используют парни, учащиеся школ с русским языком обучения.

Одновременно, исследование показывает, что учащиеся не склонны воспринимать Интернет в качестве источника угроз. Почти каждый второй объясняет свое невнимание к вопросам безопасности в Сети тем, что ему нечего скрывать в Интернет. Среди учеников школ с казахским языком обучения разделяющих данное мнение в два раза больше, чем среди учеников школ с русским языком обучения (52% против 28%). Также данное мнение в большей степени характерно для учеников, которые проводят в Интернет до 2 часов в день (44% при среднем 40%).

Интересно, что у 62% подростков родители не имеют доступ к их аккаунтам в соцсетях. Только каждый третий (34%) обращается за помощью к взрослым, если не может найти нужную информацию в Интернет. 38% не обратится к родителям, даже если будет сомневаться в правдивости информации. Особенно это заметно в русскоговорящей среде и среди тех, кто

проводит в Интернет 5 и более часов в день (20% и 19% соответственно при среднем показателе 29%).

82% не испытывают сложности с поиском нужной информации и определением нужных источников в сети

Вторая группа навыков (навыки поиска информации в сети Интернет) оценивалась по 7 утверждениям, представленным на рисунке 4.

Выяснилось, что абсолютное большинство учащихся (82%) не испытывает сложности с поиском нужной информации и определением нужных источников в сети. Также большинство опрошенных отмечает, что поиск информации в Интернете не занимает у них много времени. При этом заметно, что парни, учащиеся школ с русским языком обучения, ученики с хорошей успеваемостью реже испытывают сложности с поиском.

Большинство учащихся не ограничиваются просмотром результатов запроса только на первой странице. Первым результатам поиска чаще доверяют парни, ученики с низкой успеваемостью, те, кто проводит в Интернет не более 2-х часов в день.

Больше половины опрошенных предпочитает вести поиск самостоятельно, без помощи со стороны более опытных людей. При этом запросы обычно формулируют линейно, без использования дополнительных фильтров и спецсимволов.

Недостаточно внимания уделяется тому, что активность в Сети может отслеживаться

Для оценки третьей группы навыков респондентам были предложены 8 утверждений. Полученные данные указывают на то, что большинство учащихся периодически чистит свои подписки и контакты в соцсетях, но недостаточно внимания уделяет тому, что их активность в сети может отслеживаться.

Навыки критического восприятия информации проявляются в игнорировании всплывающих окон и рекомендаций, а также в использовании разных источников информации и сопоставлении разных точек зрения. Причём, чем меньше времени в день учащийся проводит в Интернете, тем слабее данные навыки проявляются.

Практика составления списка референтных источников информации не является устойчивой. Чаще референтные источники в Сети имеют учащиеся городских школ и школ с русским языком обучения, а также те, кто проводит в Интернете 5 и более часов в день.

О том, что они могут поменять своё отношение к событию после просмотра всего лишь одной новости, чаще всего говорят девушки, учащиеся сельских школ и школ с казахским языком обучения.

Подавляющее большинство учащихся уверены, что могут отличить правдивую информацию от фейковой (70%). Особенно уверенными себя чувствуют парни и учащиеся городских школ. Данная убежденность основывается на том, что информация, полученная из Сети, часто вызывает сомнения и даёт основание для перепроверки в других источниках перед её распространением. Надо отметить, что наибольшее недоверие информация из

Сети вызывает среди девушек, учеников с хорошей успеваемостью и тех, чьё время ежедневного пребывания в Интернете ограничено 2-мя часами.

Навык использования специальных сервисов по фактчекингу имеет слабое распространение

Навыки проверки и распространения информации в сети Интернет оценивались на основе 8 утверждений на рисунке 6.

По итогам опроса, 72% учащихся указывают на наличие базовых навыков фактчекинга — они проверяют первоисточник и дату публикации, прежде чем переслать её другому человеку. Также высока информированность (68%) о наличии законодательной ответственности за репост фейковой информации в Интернете.

При этом навык использования специальных сервисов по фактчекингу имеет слабое распространение (29%). Чаще всего об использовании подобных ресурсов говорили парни, ученики с низкой успеваемостью, а также те, кто проводит в Интернете не более 2-х часов в день. [10]

С развитием новых информационных технологий, особенно с появлением сети интернета, среди современных школьников широко начал использоваться кибербуллинг. Осуществляется он с помощью разных средств телекоммуникаций. А относятся к нему: размещение разных записей в виде фото и видео в социальных сетях, портящих репутацию жертвы. Также это могут быть унижительные комментарии, имитирование чужих профилей на разных сайтах. Кроме того, к кибербуллингу относятся и обиды и угрозы на телефон, электронный адрес или другие электронные устройства [11]

Дети и подростки были связаны и зависимы от использования Интернета и других социальных сетей во время пандемии COVID19 как для обучения, так и для общения. Вынужденная изоляция из-за болезни сделала многих из этих молодых людей более уязвимыми для действий хулиганов. Кроме того, поскольку онлайн-среда стала основным форумом для выражения идей во время карантина, вызванного пандемией, количество онлайн-контента, используемого подростками, оказывает негативное влияние. Преступники не осознают вреда и вреда себе и другим в результате своих действий в сети. Среди них рычание, горе как эффект, возникающий в результате кибербуллинга. Что-то сбивает с толку, так это трудности жертвы в ограничении и отрицании негативного влияния кибербуллинга. Несмотря на некоторые разногласия в книгах по поводу значения кибербуллинга, общей чертой считается наличие «намерения причинить вред жертве» со стороны агрессора [8]

Родителям важно дать понять, ребенку что в сети можно столкнуться с целым рядом угроз — например, киберсталкингом или кэтфишингом [<https://factcheck.kz/nauka/media-i-informacionnaya-gramotnost-shkolnikov-kazahstana-rezultaty-issledovaniya>]. «Но поскольку родители иногда не совсем понимают, что могут случиться такие проблемы, такие волонтерские программы как “QauipsizInternet” играют очень большую роль в правильном понимании информационной грамотности. Киберсталкинг (англ. cyberstalking)

– навязчивое преследование или домогательство в интернете со стороны одного человека или группы лиц. Кэтфишинг (англ. – catfishing) – вид онлайн-мошенничества, когда человек или так называемый кэтфишер (catfish) создает фальшивый профиль в социальной сети или на сайте знакомств с целью мошенничества или обмана.

Интернет является причиной проблемы кибербуллинга, которая возникает среди детей и подростков. Также невозможно, чтобы дети в будущем не пользовались интернет-СМИ, потому что они не могут решить проблему кибербуллинга. Сейчас это требует реального внимания и действий. Самооценка детей, которые становятся преступниками и жертвами кибербуллинга, безусловно, отличается от тех, кто этого не испытывает. Кроме того, последствия кибербуллинга связаны с отчаянием или самоубийством. Было показано, что хулиганы, их жертвы и жертвы хулиганов испытывают эмоциональные и поведенческие проблемы. По этой причине крайне важно сосредоточиться на хулиганах и жертвах агрессии, а также на детях и молодых людях, ставших жертвами. Некоторые методы кибербуллинга, такие как опыт жертв и преступников, включают обмен мгновенными сообщениями, чаты и электронную почту. Несмотря на неблагоприятные последствия кибербуллинга, исследования показали, что большинство подростков не предпримут никаких действий, если узнают об инциденте кибербуллинга с участием друга или одноклассника. Причина, которую молодые люди назвали для этого, состоит в том, чтобы избегать конфликтов и поддерживать групповую гармонию. Это предполагает, что молодые люди должны быть более осведомлены о последствиях инцидентов кибербуллинга, поскольку исследования ясно показывают очень неблагоприятные последствия получения сообщений о кибербуллинге [8]

Киберзащита — способность предотвращать кибератаки. Это принятие активных мер для прогнозирования кибератак со стороны злоумышленника и противодействия вторжениям. Все стратегии и тактики киберзащиты имеют общую цель — предотвращать киберугрозы, пресекать их и реагировать на них. Сегодня у киберпреступников намного больше возможностей и мотивации, чтобы совершать кибератаки: из-за финансовой выгоды, политических или социальных мотивов. Критическая инфраструктура, включая образование, здравоохранение, финансовые учреждения, правительства и производство, использует компьютеры или интеллектуальные устройства, как основную часть своей деятельности. За последние два десятилетия кибератаки были предприняты против критически важной инфраструктуры во всех развитых странах, и бесчисленное количество предприятий понесли большие убытки. Ежегодно в мире происходит более 2000 подтвержденных утечек данных, каждая из которых стоит в среднем более 3,9 млн долларов. С 2000 года киберпреступники украли личную информацию более 3,5 миллиардов человек, что составляет половину населения мира, поэтому сегодня специалисты по кибербезопасности очень востребованы, как и знания мер предосторожностей, о которых мы будем говорить ниже.

Основные виды кибератак.

Для того, чтобы уберечь себя от кибератак, нужно для начала понимать, какие виды угроз могут быть:

Фишинг — злоумышленники отправляют электронные письма или сообщения жертвам, замаскированные под законные, и таким образом выманивают у них деньги или важные данные. Также они могут подменять URL.

Боты и автоматические атаки — большинство кибератак осуществляют автоматизированные боты, которые могут сканировать системы на наличие уязвимостей, пытаться угадывать пароли и заражать системы вредоносными программами.

DDoS-атаки — отправка больших объемов фальшивого трафика в компьютерную систему до тех пор, пока объем трафика не переполнит ее, лишив доступа законных пользователей.

Вредоносное ПО — программное обеспечение, созданное для помощи или проведения кибератак или нанесения ущерба компьютерным системам. Обычно оно способно распространяться и заражать дополнительные компьютерные системы.

Направления кибербезопасности Кибербезопасность критической инфраструктуры

Организации критической инфраструктуры более уязвимы для атак, чем другие, потому что диспетчерское управление и сбор данных часто полагаются на устаревшее программное обеспечение, поэтому они нуждаются в кибербезопасности.

Сетевая безопасность включает устранение уязвимостей, влияющих на ваши операционные системы и сетевую архитектуру — серверы и хосты, маршрутизаторы и точки беспроводного доступа, а также сетевые протоколы.

Облачная безопасность связана с защитой данных, приложений и инфраструктуры в облаке. Безопасность IoT (Интернета вещей) Безопасность IoT — защита интеллектуальных устройств, подключенных к IoT. Они подключаются к сети без вмешательства человека. Например, это могут быть интеллектуальные пожарные сигнализации, освещение, термостаты и другие устройства. Безопасность приложений Безопасность приложений — устранение уязвимостей, возникающих в результате небезопасных процессов разработки при проектировании, кодировании и публикации программного обеспечения или веб-сайта.

Основные меры по защите личных данных от кибератак

Установите надежное антивирусное программное обеспечение

Хорошая и надежная антивирусная программа — обязательный элемент любой системы кибербезопасности. Она обнаруживает и удаляет вирусы и вредоносные программы. Она также сканирует и отфильтровывает потенциально опасные загрузки и электронные письма. Важный момент: чтобы себя обезопасить, нужно будет не забывать регулярно обновлять это программное обеспечение.

Используйте сложные пароли

Будь то ответы на контрольные вопросы или пароли, убедитесь, что они сложные, чтобы хакерам было трудно их взломать. Чтобы получить ответы на контрольные вопросы, попробуйте перевести их на другой язык. Это может сделать их трудными для расшифровки, а также менее восприимчивыми к социальным технологиям. Использование пробела перед или после ваших паролей также хорошая идея, чтобы сбить хакера с толку. Использование комбинации верхнего и нижнего регистра также помогает, помимо использования буквенно-цифровых символов.

Защитите свою сеть с помощью брандмауэра

Брандмауэр защищает как аппаратное, так и программное обеспечение, что делает его удобным для любой компании с физическими серверами. Но брандмауэр также блокирует или удерживает вирусы от проникновения в вашу сеть, в то время как антивирус нацеливается на программное обеспечение, которое уже пораженное вирусом. Другими словами, они хорошо работают вместе. Установка брандмауэра помогает защитить сетевой трафик малого бизнеса — как входящий, так и исходящий. Это может помешать хакерам атаковать вашу сеть, заблокировав определенные веб-сайты. Его также можно настроить так, чтобы ограничить отправку служебных данных и конфиденциальных электронных писем из сети вашей компании.

Под кибергигиеной подразумевается совокупность навыков и знаний, уменьшающих риски пребывания в сети. Это понятие складывается из нескольких составляющих. Важно знать об угрозах, подстерегающих пользователей на просторах интернета. Кибергигиена позволяет избежать многих опасностей. Каждый пользователь должен понимать, что работа в интернете таит в себе определенный риск. Осознание данного факта позволяет избежать множества проблем. Атаке мошенников может подвернуться любой пользователь. Хорошая новость состоит в том, что уберечься от угроз не так трудно, как многие считают.

Обеспечение безопасности учетных записей: Учетные записи есть у всех пользователей – это страницы в соц. сетях, электронный почтовый ящик. К ним причисляют все логины, для которых требуется введение пароля. Никто не должен знать вашего пароля или иметь возможность его подбора – это одно из главных правил кибергигиены. Надежность – основа безопасности. При этом самом пользователь не должен его забыть или потерять. Логин с паролем являются главными дверями замка, именно их будут штурмовать в первую очередь. Общие защитные механизмы представляет сама система либо сайт: блокирует доступ после нескольких неудачных попыток, ограничивает временные промежутки между попытками. При помощи проверки «Я не робот» оценивается надежность пароля и корректность при обращении с ним. Но если пароль ненадежен, никакая общая защита не поможет. Главные инструменты кибергигиены – это антивирусные программы. Нужно понимать, как выявить вирус на компьютере и как правильно использовать таких защитников, что предпринять при наличии подозрений на заражение. Необходимо позаботиться

о защите от вредоносных писем, которые регулярно приходят на электронную почту, фишинговых ресурсов. В фишинговых рассылках присутствуют файлы, похожие на простые документы, но в действительности – это программы. Стоит только предпринять попытку их открыть, и они активируются от имени пользователя. Начнут выполнять свое предназначение, открывая доступ к вашему ПК или смартфону. Поскольку их активация произошла от вашего имени, у злоумышленника появятся такие права, как и у вас. Или в сообщениях могут скрываться ссылки на фишинговые ресурсы. Фишинговыми называют сайты, по виду не отличимые от настоящих, рассчитанные на введение пароля и логина. Стоит только их ввести, и они окажутся у злоумышленников. Многие из таких ресурсов очень трудно отличить от подлинных, но всегда найдется зацепка.

При работе в интернете соблюдайте следующие правила:

- Распознавайте действия злоумышленников и не идите у них на поводу.
- Управляйте данными.
- Сохраняйте бдительность.
- Не пренебрегайте использованием антивирусных программ.

Введение данных должно быть осознанным. Научитесь распознавать фишинговые ресурсы от подлинных. Не запускайте «троянов». Не поддавайтесь просьбам «знакомых» и «родных» о срочном переводе денег, предварительно не удостоверившись в том, что это именно они. Защита персональных данных в интернете очень важна, контролируйте их распространение. Ограничьте доступ к ним. Подавляющая часть случаев утечек личных данных происходит из-за халатности самих владельцев. Не так давно произошел скандал, связанных с утечкой персональных данных в ЦОНе. Это произошло, потому что владельцы документов, использовали общие компьютеры для их загрузки в систему, после чего не позаботились об удалении. В итоге на общих компьютерах в ЦОНе скопился внушительный архив «забытой» документации и любой из посетителей мог сделать копию себе на съемный носитель. Четко осознавайте свои действия и своевременно реагируйте, если что-то идет не так. Изучите свой компьютер и установленные на нем программы.

Детская кибербезопасность: Кибергигиена важна не только для взрослых, но и для детей, ведь они также проводят много времени в интернете. И у большинства юных пользователей сети нет необходимых знаний и навыков в сфере кибербезопасности. Развитие навыков безопасных контактов с виртуальной средой должно быть начато как можно раньше. При таком подходе у ребенка это войдет в привычку. Многие родители оказывались в ситуации, когда их чадо «зависает» за просмотром видео в сети. Взрослые выражают неодобрение, что ребенок слишком много времени посвящает этому занятию. Да и выбранный контент их не всегда устраивает. Ребенок отвечает на это родителям: «Если бы в ваши детские годы были онлайн-ролики, вы бы тоже их смотрели. Большое количество людей не расстается со смартфонами. Гаджеты для них выступают органом чувств, обеспечивающим связь с

интернетом. Они повзрослели вместе с глобальной сетью, она стала неотъемлемой составляющей их жизни. В интернет-пространстве у них формируется персональный образ. И подавляющая часть пользователей выходит в сеть через телефон – это относится и к детям. Проблема заключается в том, что многие забывают о кибергигиене. Родители стараются воспитать в своем ребенке самостоятельность, но их не покидает естественная тревога.

Место нахождения опасности: Учитывая особенности детского и подросткового поведения в сети, их потребности, важно сделать акцент на анонимности и приватности, защитить репутацию. Приложение родительского контроля UniSafe Kids позволит избежать многих проблем при нахождении ребенка в сети.

Взрослые всегда будут знать:

- сколько времени их чадо проводит в интернете;
- какие сайты посещает;
- какими приложениями пользуется.

Пользу от UniSafe Kids уже оценили многие родители, переживающие за цифровую безопасность, стремящиеся защитить персональные данные. Все подростки знают, что в интернете предостаточно мошенников. Им гораздо интереснее, что злоумышленники могут украсть именно у них, и какой вред могут нанести им хакерские атаки. Результаты одного из исследований, проведенного компанией Proofpoint (корпорация занимается производством решений, обеспечивающих безопасность электронной почты), меньше 1% всех атак базируется на уязвимости систем. Подавляющая же часть атак происходит по вине человеческого фактора. Технические средства контроля атак все время модернизируются, автоматизированные комплексы дают возможность своевременно реагировать на большой процент инцидентов, но это не распространяется на ошибочные и халатные действия самих пользователей, несоблюдения правил цифровой безопасности. Навыки кибергигиены уже давно стали необходимостью. Но для их формирования требуется время, поэтому приобретать необходимые знания и умения нужно уже сейчас. Как быть родителям и педагогам? Устанавливать запреты, совершать проверки или отпустить ситуацию? Прежде всего, понять, что полный контроль над поведением ребенка в сети установить нереально. Но взрослые обязаны стать авторитетным информационным источником. Кибергигиеной для детей нельзя пренебрегать, особенно если учесть, что грань между реальностью и виртуальным миром уже давно перестала быть четкой. Базовые приемы цифровой безопасности: Надежная защита персональных данных даст возможность избежать серьезных проблем, кражи денежных средств, документов. Правила поведения в интернете для детей и взрослых позволят предотвратить контакты со злоумышленниками.

Киберкультура (английское *cyberculture*) — вид современной культуры, который формируется её носителями с помощью цифровой техники, прежде всего персональных компьютеров, порождённых наукой кибернетикой. Наиболее масштабным видом киберкультуры можно назвать интернет-

культуру, то есть глобальную массовую культуру, формирующуюся всеми пользователями Интернета в ходе использования компьютерных устройств, держащих цифровую связь по протоколу IP. Внутри интернет-культуры можно выделять другие киберкультуры, такие как геймерство (киберспорт), чаты, имиджборды, свободное ПО, вики-движение и многое другое. Геймерство при этом может быть «оффлайновым», то есть являться киберкультурой, но не являться интернет-культурой. Пользователи Фидонета на раннем этапе сформировали «киберкультуру пользователей компьютерной сети» вне Интернета, а затем в целом влились в интернет-культуру, оказав на неё специфичное влияние. Массовая культура пользователей Интернета на ранних этапах его развития была в основном тождественна культуре пользования электронной почтой (Usenet и его аналоги) и стала стремительно развиваться в разных направлениях с появлением Всемирной паутины. Англоязычное понятие *cyberculture* определяется Оксфордским словарём как «состояние общества в результате использования средств автоматизации и компьютеризации». Носители киберкультуры являются предметом изучения киберпсихологии.

Исследования киберкультуры, экспериментальный тип теории, возникший на рубеже 1980–1990-х гг. Киберкультура и группы по её изучению начали формироваться благодаря распространению персональных компьютеров и появлению Интернета. Киберкультура – это собирательное понятие, которое характеризует культурный переход из 20 в 21 в. Переход оказался отличным от прогнозов 1960-х гг., в которых предсказывались космические полёты на Марс, прогресс и управление будущим. Стало понятно, что будущее – это не линейное развитие старых технологий, а иной способ определять техническое и понимать человеческое. Технологии развивались в сторону микротехнологий, встраивались в повседневность, стали частью культурного производства; эксперименты со звуком и визуальностью изменили перцептивный канон (техно-музыка и рейв), гипертекстовые режимы письма меняли каноны литературы. Локальные культуры стали видимы друг для друга в глобальном пространстве коммуникаций. Киберкультура обращалась к многообразию субкультур с их эстетическим различием на фоне стремительного освоения искусством технологических возможностей. Исследователи пытались понять, какие эффекты реальности и телесные трансформации могут быть произведены новой технологией глобальной коммуникации и виртуальной реальности, а также биотехнологией.

Центры изучения киберкультуры появлялись в различных странах и на разных континентах. На истории групп 1990-х гг. можно проследить формирование глобального культурного поля с разнообразием подходов и эстетик. Ранние исследовательские подходы влияли на формирование новых дисциплин: исследования науки и технологий (STS), медиаархеологию, философию видеоигр. Прослеживается их влияние на новые направления в философии: неоматериализм, спекулятивный реализм, объектно-ориентированную философию и т. д.

При анализе киберкультурных инициатив 1990-х гг. можно выделить следующие направления.

Во-первых, как собирательное понятие 1990-х гг., киберкультура характеризуется переходом от понимания технологии как прикладной сферы управления и решения системных проблем к пониманию технологии как нового медиума культуры. Она также характеризуется сдвигом в понимании медиума от языка как доминантного опосредования реальности к технологии как материальной и дискурсивной практике.

Во-вторых, киберкультура связана с парадигмальным переходом к другому пониманию реальности и виртуальности, техники и языка, глобального и локального, к другим типам смыслообразования. С одной стороны, рос интерес к исследованиям микрополитик и технологически обусловленных практик телесности: это исследования постгуманизма как отказ от классической теории субъекта, кибертелесности (Sofoulis. 2002), активности материального (Беннетт. 2018), философии аффекта (Hansen. 2000; Hansen. 2014). С другой стороны, существовал интерес к культуре трансгрессии, радикального расширения опыта, ритуалам, конспирологии и оккультизму. Позднее он оформился в понятиях гипер(хайпо)верия (Н. Ланд) или призракологии (М. Фишер), в российском контексте близкие идеи формировались в блогах математика и активиста киберкультуры М. Вербицкого и психоделического реализма группы «Медицинская герменевтика».

Киберкультура предполагала движение в сторону многообразия и интенсивного обмена культур с их эстетическим различием на фоне стремительного освоения искусством технологических форм. Формировался особый тип исследований технологического расширения восприятия и семантического многообразия, гипертекстовых режимов литературного и исследовательского письма и культурных кодов, построенных на многослойных динамичных образах, которые размывают границы объектов и идентичностей.

(
https://lomonosovmsu.ru/file/event/4469/eid4469_attach_7a78fde9e62875f6980377f21f0632c03f60ffaf.pdf

Безопасность детей и молодежи в Интернете. [Мир, достоинство и равенство на здоровой планете. ООН <https://www.un.org/ru/global-issues/child-and-youth-safety-online>]

Молодежь является движущей силой развития сетевых технологий во всем мире: в 2022 году 75% подростков в возрасте от 15 до 24 лет будут пользоваться Интернетом, в то время как среди остального населения мира этот показатель составит 65%. Дети также проводят в Интернете больше времени, чем когда-либо прежде. И они приходят к этому раньше. Каждые полсекунды в мире один ребенок впервые выходит в Интернет!

Это создало для детей и молодежи беспрецедентные возможности для общения, обучения, социализации и игр, приобщая их к новым идеям и более разнообразным источникам информации.

Но вместе с этими возможностями приходят и серьезные риски. Кибербуллинг и другие формы насилия со стороны сверстников могут затрагивать молодых людей каждый раз, когда они заходят в социальные сети или на платформы обмена мгновенными сообщениями. Более трети молодых людей в 30 странах сообщают, что подвергались кибербуллингу, а каждый пятый прогуливал школу из-за этого.

При работе в Интернете дети и подростки могут столкнуться с разжиганием ненависти и насилием, включая сообщения, подстрекающие к членовредительству и даже самоубийству. Молодые пользователи Интернета также уязвимы для вербовки экстремистскими и террористическими группами.

Цифровые платформы также используются для распространения дезинформации и теорий заговора, которые оказывают вредное воздействие на детей и подростков.

Наибольшую тревогу вызывает угроза сексуальной эксплуатации и насилия в Интернете. Никогда еще не было так легко для детей, совершивших сексуальные преступления, связаться со своими потенциальными жертвами, поделиться изображениями и побудить других к совершению преступлений. Около 80% детей в 25 странах сообщают, что чувствуют себя в опасности сексуального насилия или эксплуатации в Интернете.

Дети также могут подвергаться риску, когда технологические компании нарушают их конфиденциальность для сбора данных в маркетинговых целях. Маркетинг, ориентированный на детей, через приложения - и чрезмерное время, проведенное за экраном, - может поставить под угрозу здоровое развитие ребенка.

Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

В Интернете, как и в реальной жизни, учащихся подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т. п.

Интернет-зависимость — это навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. В частности, некоторые учащиеся настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Видами интернет-зависимости являются навязчивый веб-серфинг, пристрастие к виртуальному общению и виртуальным знакомствам (большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети), игровая зависимость — навязчивое увлечение компьютерными играми по сети.

Задача педагогов в связи с имеющимися рисками состоит в том, чтобы указать на эти риски, предостеречь от необдуманных поступков, сформировать у учащихся навыки критического отношения к получаемой в Интернете информации, воспитать культуру безопасного использования Интернет. Также следует обратить внимание на гигиенические требования, которые необходимо соблюдать при работе с компьютером: - школьникам среднего и старшего возраста можно проводить перед монитором до двух часов в день, устраивая 10-15-минутные перерывы каждые полчаса; - ребенок младшего возраста может находиться за компьютером не более 15 минут в день, в условиях классно-урочной деятельности – не более одного урока, а при наличии противопоказаний офтальмолога – только 10 минут, не более 3 раз в неделю; - лучше работать за компьютером в первой половине дня; - комната должна быть хорошо освещена; - при работе за компьютером следить за осанкой, мебель должна соответствовать росту; - расстояние от глаз до монитора – 60 см; - периодически делать зарядку для глаз.

В соответствии с федеральными государственными образовательными стандартами общего образования в структуру основной образовательной программы основного общего образования включена программа воспитания и социализации учащихся, которая содержит такое направление, как формирование культуры здорового и безопасного образа жизни. В рамках этой программы может осуществляться информационно-просветительская работа среди школьников, пропагандирующая важность владения навыками безопасной работы в сети Интернет.

В образовательных организациях необходимо проводить занятия для учащихся по основам информационной безопасности («основы медиа-безопасности»); знакомить родителей с современными программно-техническими средствами (сетевыми фильтрами, программами «родительский контроль»), ограничивающими доступ детей и подростков к ресурсам сети Интернет, несовместимыми с задачами воспитания; проводить специальные мероприятия по вопросам информационной безопасности несовершеннолетних. В качестве возможного варианта предоставления учащимся соответствующих знаний может быть использована учебная программа «Интернет: возможности, компетенции, безопасность», разработанной специалистами факультета психологии МГУ им. М.В. Ломоносова, Федерального института развития образования и Фонда Развития Интернет, рекомендованная Министерством образования и науки РФ (<http://detionline.com> – главная страница, <http://detionline.com/internetproject/about><http://detionline.com/assets/files/research/BookTheorye.pdf> - теория, http://detionline.com/assets/files/research/Book_Praktikum.pdf - практика). Содержание программы направлено на обучение учащихся полезному и безопасному использованию сети Интернет и социальных сетей, обучению критической оценке онлайн контента и навыкам сетевой коммуникации. Авторами программы разработано методическое пособие для преподавателей и практикумы для проведения уроков, а также запущен интернет-ресурс

«Разбираем Интернет» (www.razbiraeminternet.ru). На этом сайте в игровой форме представлены мультимедийные средства обучения для детей и подростков, надо рекомендовать обучающимся посещать этот сайт. Содержательная часть и объем учебного курса может определяться индивидуально, в зависимости от потребностей конкретной общеобразовательной организации и учащихся. Обучение навыкам безопасного и эффективного использования интернет-ресурсов возможно в рамках учебного курса «Основы безопасности жизнедеятельности» и в рамках программ факультативов, кружков, элективных курсов, а также индивидуальных учебных планов, реализуемых образовательными организациями. Материалы бесплатны и доступны для скачивания www.razbiraeminternet.ru/teacher.

Академией повышения квалификации и профессиональной переподготовки работников образования (г. Москва) разработан учебно-методический комплект «Здоровье и безопасность детей в мире компьютерных технологий и Интернет». УМК разработан с учетом потребностей образовательных организаций в области безопасной работы в Интернет и ориентирован на руководителей, методистов, педагогов, заинтересованных в повышении своей компетентности в области безопасного применения ИКТ. Методическое приложение к программе можно использовать при организации просветительской работы с родителями и учащимися https://edu.tatar.ru/upload/images/files/children_health_and_care_in_it.pdf.

Рекомендации по безопасному использованию Интернета для несовершеннолетних и их родителей даны и на сайте Майкрософт <http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx>, <http://www.microsoft.com/ru-ru/security/default.aspx>. Вышеуказанные сетевые ресурсы могут быть использованы для проведения педсоветов в образовательных организациях по вопросам безопасности детей в сети Интернет. Рекомендуется провести анкетирование обучающихся и родителей по вопросам безопасного использования сети Интернет.

При работе с младшими школьниками целесообразно использовать игровые методы. В основной школе учащиеся активно начинают использовать Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайн-игры и так далее. Все более часто их любимым способом общения становится мгновенный обмен сообщениями. Для учащихся этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным.

Педагогам для обеспечения интернет-безопасности учащихся 10-15 лет необходимо:

- познакомить учащихся с ответственным, достойным поведением в Интернете;
- рассказать об основных опасностях и правилах безопасного использования сети Интернет;
- убедить никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов,

название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете;

- объяснить опасность личных встреч с друзьями по Интернету без присутствия взрослых;

- убедить сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им.

- ознакомь с правилами поведения на форумах и чатах, убедить их, что они не должны использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

Организуя работу с учащимися старших классов по безопасному использованию информации в Интернете, следует обратить внимание на неформальные молодежные объединения, которые возникают в образовательной организации.

Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее, участие взрослых тоже необходимо:

- Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. - Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы. - Интересуйтесь, какими чатами и досками объявлений пользуются подростки, и с кем они общаются.

- Поощряйте использование модерируемых (контролируемых) чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.

- Настаивайте, чтобы подростки осторожно соглашались или не соглашались вовсе на личные встречи с друзьями из Интернета.

- Напоминайте, какие опасности это может за собой повлечь.

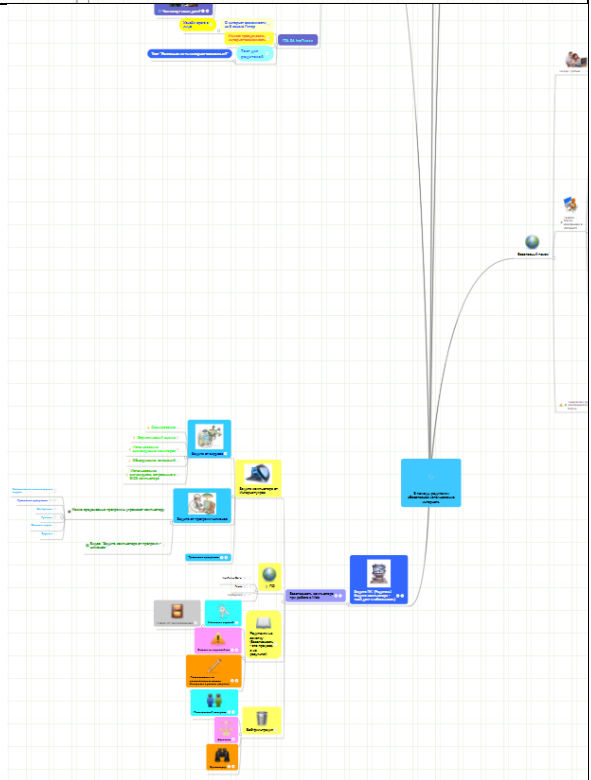
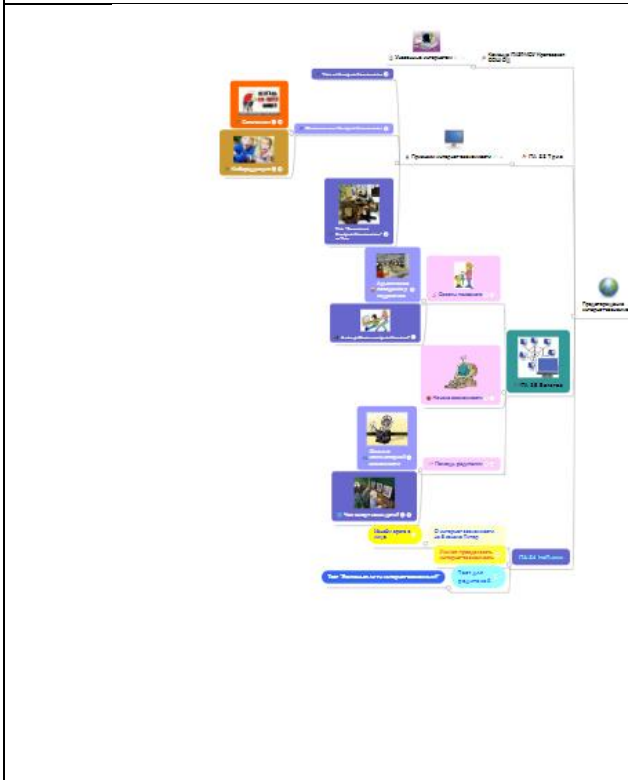
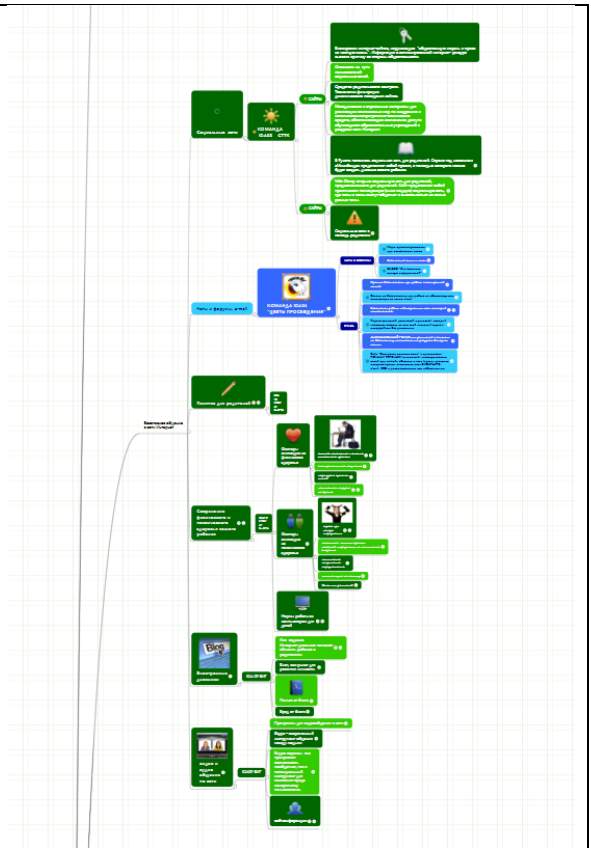
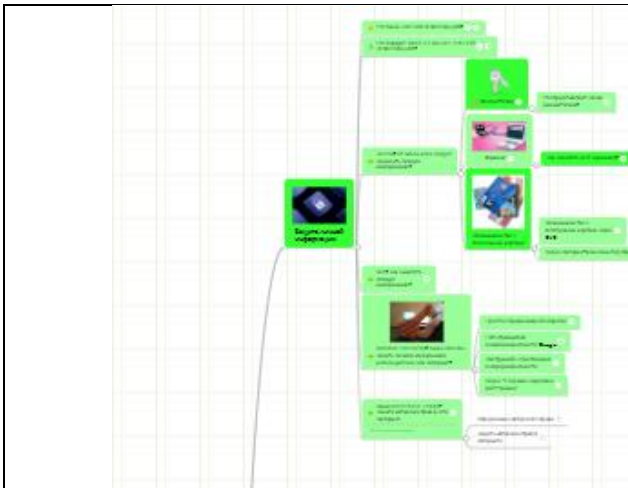
- Убедите подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.

- Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

- Обсудите с подростками азартные сетевые игры и связанный с ними риск. Результатами мероприятий по безопасному использованию Интернета могут стать как бумажные, так и электронные ресурсы, созданные учащимися: рисунки, сочинения (рассказы, сказки, стихи), буклеты, презентации. Интересной формой представления результатов могут стать театрализованные выступления и видеофильмы учащихся. Для учащихся старших классов при создании материалов по безопасности можно использовать сервисы Интернета для совместной деятельности. Работа команды учащихся в этом случае можем

проводиться дистанционно. Одним из примеров является схема «Безопасность детей в Интернете». [12]

Рекомендуем обратить внимание на создание условия для ознакомления с результатами творчества учащихся. Разработанные материалы можно размещать на сайте образовательной организации, в социальных сетях, блогах и сетевых сообществах. Для эффективной профилактики интернет-зависимости, профилактики националистических проявлений в молодежной среде и устранения риска вовлечения подростков в противоправную деятельность педагогам необходимо проводить разъяснительную и консультационную работу с родителями учащихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в Интернет. Возможно проведение бесед о работе учащихся в сети Интернет на классных и общешкольных родительских собраниях или при индивидуальных встречах; информирование через школьный сайт на страничке для родителей. На таких страничках можно разместить рекомендации по профилактике компьютерной зависимости у детей, по обеспечению безопасности детей в Интернете. [13,14]



2. Международный и отечественный опыт по формированию полезных привычек в отношении кибербезопасности, кибергигиены и киберкультуры детей.

Термин "кибербезопасность" и его производные (киберпространство, киберзащита, кибератаки, кибернападение и другие) не имеют единого общепризнанного юридического определения на международном уровне.

В тоже время на уровне ООН имеется ряд документов, таких как Глобальная программа кибербезопасности Международного союза электросвязи или Резолюция Генеральной Ассамблеи ООН "Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур", в которых содержатся подходы к пониманию кибербезопасности, охватывающие сферу безопасного использования информационно-коммуникационных технологий в вопросах обеспечения неприкосновенности частной жизни, конфиденциальности, целостности и доступности информации в электронной форме, защиты критической информационно-коммуникационной инфраструктуры, взаимодействующей с Интернетом (в том числе информационных систем, аппаратно-программных комплексов, телекоммуникационных систем, сетей телекоммуникаций, систем защиты информации, программного обеспечения) от вредоносного воздействия программно-техническими методами.

При этом многие страны не рассматривают в руководящих документах вопросы защиты от вредной или незаконной информации, распространяемой с использованием ИКТ в контексте понимания кибербезопасности из-за опасений в чрезмерном ограничении права на доступ и свободное распространение информации.

Отдельные страны рассматривают через призму кибербезопасности только неконтролируемое распространение в Интернете, как всемирной системе объединенных сетей телекоммуникаций и вычислительных ресурсов, электронных материалов, пропагандирующих терроризм, детскую порнографию и некоторые виды незаконной информации, в первую очередь, по причине технической сложности установления источника распространения такой информации.

При этом некоторые страны в оценке угроз и принимаемых в отношении них мер противодействия придерживаются понятия информационной безопасности применительно ко всем аспектам использования ИКТ, выстраивая соответствующую модель правового регулирования и системы государственного управления.

Так, например, *стратегия Норвегии* отмечает, что новые услуги и устройства предъявляют весьма высокие требования к компетенции простых пользователей. Но главная ответственность за обеспечение безопасности информации, систем и сетей возлагается на владельца или оператора. Такие работы должны быть частью ежедневной работы и финансироваться наряду с текущими операциями. Стоимость мер по содействию информационной

безопасности должна быть соразмерна оценке риска в отдельных сферах управления (глобальный индекс кибербезопасности составляет 0,735).

Эстония придает особое значение безопасности информационных систем. Рекомендуемые меры носят гражданский характер и основываются на правовом регулировании, обучении и сотрудничестве (глобальный индекс кибербезопасности составляет 0,706).

В основе стратегии Финляндии лежит понимание кибербезопасности как проблемы экономического характера, тесно связанной с развитием финского информационного общества (глобальный индекс кибербезопасности составляет 0,618).

Словакией обеспечение информационной безопасности рассматривается в качестве необходимого условия нормального функционирования и развития общества. Поэтому цель стратегии – служить прочным фундаментом для защиты информации. Стратегия направлена как на предотвращение угроз, так и на обеспечение готовности и устойчивости средств их предотвращения (глобальный индекс кибербезопасности составляет 0,618).

Ключевые цели стратегии кибербезопасности *Чешской Республики* включают в себя защиту информационно-коммуникационных систем от уязвимостей, которым эти системы подвергнуты, и уменьшение потенциального ущерба от атак на системы. Основной фокус стратегии приходится на проблемы свободного доступа к информационным сервисам, целостности и конфиденциальности данных в Чешской Республике (глобальный индекс кибербезопасности составляет 0,500).

Франция ориентируется на то, чтобы информационные системы были способны противостоять событиям, которые могут отрицательно повлиять на доступность, целостность и конфиденциальность информации, делает упор на технические средства защиты информации, борьбу с киберпреступностью и установлением киберзащиты (глобальный индекс кибербезопасности составляет 0,588).

Стратегия Германии закладывает основу для безопасности критически важных информационных систем. Германия сосредоточена на предотвращении и уголовном преследовании кибератак, а также выхода из строя IT-оборудования, вызванного случайными факторами. Стратегия кибербезопасности Германии определяет уровень кибербезопасности, достигнутый суммой всех национальных и международных мер, принятых для защиты и доступа к информации и коммуникациям, целостности, достоверности и конфиденциальности данных в киберпространстве, а также укреплением германского технологического суверенитета и экономического потенциала во всем диапазоне основных стратегических IT-компетенций (глобальный индекс кибербезопасности составляет 0,706).

Программа развития электронной информационной безопасности Литвы ориентируется на определении целей и мероприятий, направленных на обеспечение электронной информационной безопасности, развитие оборота

электронной информации, а также обеспечение ее конфиденциальности, доступности и целостности в киберпространстве. Кроме того, стратегия Литвы направлена на защиту персональных данных, телекоммуникационных сетей, информационных систем и критически важных инфраструктур от нарушения безопасности и кибератак из-за пределов «электронного периметра» (глобальный индекс кибербезопасности составляет 0,441).

Нидерланды, с одной стороны, стремятся к безопасным и надежным информационно-коммуникационным системам, опасаясь серьезных нарушений в этих системах, а с другой стороны, признают необходимость свободы и открытости Интернет-пространства. В стратегии дается определение кибербезопасности. «Кибербезопасность – это защищенность от сбоев и неправильной эксплуатации информационно-телекоммуникационных систем. Сбои и неправильная эксплуатация могут отрицательно повлиять на доступность и надежность информационно-телекоммуникационных систем, поставить под угрозу конфиденциальность и целостность информации, хранящейся в системах» (глобальный индекс кибербезопасности составляет 0,676).

Стратегия безопасности ИКТ Австрии заключается в распространении интегральных подходов к безопасности, реализованных в системе "электронного правительства", к другим областям, включая те, которые должны быть созданы на транснациональном уровне в целях обеспечения долгосрочной жизнеспособности экономики *Австрии* (глобальный индекс кибербезопасности составляет 0,676).

Подход Великобритании направлен на развитие кибербезопасности. Цель: вывести Соединенное Королевство на первое место по инновациям, инвестициям и качеству сервисов в сфере информационно-телекоммуникационных технологий, и тем самым, в полной мере воспользоваться всеми преимуществами и достоинствами киберпространства. Необходимо исключить риски типа кибератак преступников, террористов и других государств с целью сделать киберпространство безопасным для граждан и экономики (глобальный индекс кибербезопасности составляет 0,706).

Национальная стратегия Швейцарии отмечает необходимость уменьшения влияния преобладающих интересов нескольких стран, участвующих в Интернет-индустрии, рассматривает применение описываемых в ней мер «в мирное время, и тем самым, явным образом исключает войны».

При этом отказоустойчивая военная инфраструктура рассматривается как важный элемент стратегического резерва для других субъектов в случае полномасштабного кризиса. Поскольку действующее законодательство в различных отраслях отражает кибераспекты существующих задач и обязанностей государственного и частного сектора, решение вопросов кибербезопасности в рамках единого специального *киберзакона Швейцарии* считается непригодным, так как «непрерывно адаптироваться к изменениям должно действующее законодательство" (глобальный индекс кибербезопасности составляет 0,353).

Таким образом, в каждой стране национальное понимание кибербезопасности и ключевых приоритетов значительно различается.

Как следствие, различаются и подходы к составлению стратегий кибербезопасности. Тем не менее, руководящие документы, охватывающие вопросы кибербезопасности, как правило, предусматривают:

- построение государственной системы управления в сфере обеспечения кибербезопасности;
- определение соответствующего механизма (в основном общественно-государственного партнерства), позволяющего частным и государственным заинтересованным сторонам обсуждать проблемы обеспечения безопасности национальных информационных инфраструктур;
- определение необходимой политики безопасности и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для частного и государственного сектора (например, обязательное информирование об инцидентах безопасности, базовые меры обеспечения безопасности и руководства к действию, новые нормы материально-технического обеспечения).

Как свидетельствует мировой опыт, полную защиту от ошибок в программном обеспечении или инцидентов информационной безопасности достигнуть невозможно, но путем осознанного ответственного поведения снизить их частоту и вероятность, обеспечить высокую скорость восстановления работоспособности информационных систем и ресурсов, чтобы не допустить разрушительных последствий, жизненно необходимо.

Координация этой сферы во многих странах в значительной степени выстраивается вокруг гражданского регулятора в области информационных технологий и связи (Агентство информационной безопасности KISA - Корея, Центр информационной безопасности Министерства информационных технологий – Республика Узбекистан, и др.), либо органа, ответственного за защиту и безопасность информации (Бюро безопасности информационной техники – Германия, Агентство безопасности информационных систем при Министерстве обороны – Франция, Агентство национальной безопасности Чехии, Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, Оперативно-аналитический центр при Президенте Республики Беларусь, Служба специальной связи и защиты информации Украины. В Европейском союзе регулятором в этой сфере является Агентство информационной и сетевой безопасности).

В России, согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Такую защищенность ребенку должны обеспечить, прежде всего, семья и школа. Это задача не только семейного, но и школьного воспитания. Проведение уроков медиа безопасности планируется в образовательных учреждениях на постоянной основе, начиная с первого класса, в рамках школьной программы, в том числе уроков ОБЖ.

Цель проведения уроков медиа безопасности – обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи уроков медиа безопасности:

1. информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2. информирование учащихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3. ознакомление учащихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

4. обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

5. профилактика формирования у учащихся интернет-зависимости и игровой зависимости (игромании, гэмблинга);

6. предупреждение совершения учащимися правонарушений с использованием информационно-телекоммуникационных технологий.

Ожидаемые результаты.

В ходе уроков медиа безопасности дети должны научиться сделать более безопасным и полезным свое общение в Интернете и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и

репутации;

- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Нормативная правовая база защиты детей от информации, причиняющей вред их здоровью, репутации, нравственному, духовному и социальному развитию.

Защита детей от информации, причиняющей вред их здоровью, репутации и развитию, регулируется:

1. Нормами международного права:

- ст. 13, 17, 34 Конвенции ООН о правах ребенка 1989 г.
- Европейской декларацией о свободе обмена информацией в Интернете 2003 г.
- Европейской конвенцией о совместном кинопроизводстве 1992 г.
- Европейской конвенцией о трансграничном телевидении 1989 г.
- Европейской конвенцией о правонарушениях в сфере электронной информации 2001 г.
- Европейской рамочной конвенцией о безопасном использовании мобильных телефонов маленькими детьми и подростками (06.02.2007 г.)
- Рекомендациями Комитета Министров государств — членов Совета Европы: относительно принципов распространения видеозаписей, содержащих насилие, жестокость или имеющих порнографическое содержание (22.04.1989 г.), о демонстрации насилия в электронных средствах массовой информации (30.10.1997 г.)
- Рекомендация в сфере регулирования в отношении кибер-контента (саморегулирования и защиты пользователей от незаконного или вредного содержания новых коммуникаций и информационных услуг), о мерах поддержки демократического и социального распространения цифрового вещания (28.05.2003 г.)
- Рекомендации по расширению возможностей детей в новой информационно-коммуникационной среде (27.09.2006 г.), о поощрении свободы выражения мнений и информации в новой информационной и коммуникационной среде, о мерах по развитию уважения к свободе слова и информации в связи с Интернет-фильтрами
- Рекомендациями Европейского парламента и Совета ЕС о защите несовершеннолетних и человеческого достоинства и права на ответ в

отношении конкурентоспособности индустрии европейских аудиовизуальных и информационных онлайн услуг (20.12.2006 г.)

- Модельным законом МПА СНГ «О противодействии торговле людьми», принятым на тридцатом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (03.04.2008 г.)

- Рекомендациями по унификации и гармонизации законодательства государств — участников СНГ в сфере борьбы с торговлей людьми (03.04.2008 г.)

Модельным законом МПА СНГ «О защите детей от информации, причиняющей вред их здоровью и развитию» (03.12.2009 г.)

Рекомендациями по унификации и гармонизации законодательства государств — участников СНГ в сфере защиты детей от информации, причиняющей вред их здоровью и развитию (28.10.2010 г.)

2. Федеральным законодательством:

- ст. 14, 14.1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»

- ст. 31 Основ законодательства Российской Федерации о культуре от 09.10.1992 г. № 3612-1

- ст. 4, 37 Закона Российской Федерации от 27.12.1991 г. «О средствах массовой информации» № 2124-1

- ст. 46 Федерального закона от 08.01.1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах»

- Федеральным законом от 13.03.2006 г. № 38-ФЗ «О рекламе»

- Федеральным законом от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (вступает в действие 01.09.2012 г.)

- Федеральным законом от 21.07.2011 г. № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» (вступает в действие 01.09.2012 г.)

- Стратегией национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента Российской Федерации от 12.05.2009 г. № 537, и Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 г. № ПР-1895, в которых закреплены общие принципы обеспечения информационной безопасности граждан и государства;

3. Нормативными правовыми актами субъектов Российской Федерации.

4. Приказом Генерального прокурора Российской Федерации от 26.11.2007 г. № 188 «Об организации прокурорского надзора за исполнением законов о несовершеннолетних и молодежи» (п. 3.2) – предусмотрено проведение систематических проверок соблюдения законодательства о защите детей от информации, наносящей вред их здоровью, репутации, нравственному и духовному развитию, в деятельности средств массовой информации, органов

и учреждений образования и культуры. Прокуроры должны привлекать к установленной ответственности юридических и физических лиц, виновных в распространении указанной информации или пропагандирующих насилие и жестокость, порнографию, наркоманию, антиобщественное поведение, в том числе употребление алкоголя, наркотиков, табачных изделий, а также пресекать в пределах предоставленных законом полномочий использование средств массовой информации и информационно-телекоммуникационных сетей, в том числе сети Интернет, для сексуальной эксплуатации и совершения иных преступлений против несовершеннолетних.

Для сведения. Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает

правила медиа безопасности детей при обороте на территории России продукции средств массовой информации, печатной, аудиовизуальной продукции на любых видах носителей, программ для ЭВМ и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи.

Он содержит ряд новационных норм, предусматривающих создание организационно-правовых механизмов защиты детей от распространения в сети Интернет вредной для них информации (возрастную классификацию информационной продукции, ее маркировку, применение сертифицированных технических и программно-аппаратных средств). Устанавливаются требования к распространению среди детей информации, в том числе требования к осуществлению классификации информационной продукции, ее экспертизы, государственного надзора и контроля за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

Согласно новому закону доступ детей к информации, распространяемой посредством информационно-телекоммуникационных сетей, может предоставляться операторами связи в Интернет-кафе, образовательных и других учреждениях, в пунктах коллективного доступа только при условии применения ими технических, программно-аппаратных средств защиты детей.

В информационной продукции для детей, в том числе размещаемой в информационно-телекоммуникационных сетях (включая сеть Интернет) и сетях подвижной радиотелефонной связи, не допускается размещать объявления о привлечении детей к участию в создании информационной продукции, причиняющей вред их здоровью и (или) развитию.

К информации, причиняющей вред здоровью и (или) развитию детей, законом отнесена информация, запрещенная для распространения среди детей, а также информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью,

самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера.

К информации, ограниченной для распространения среди детей определенных возрастных категорий, относится информация:

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Согласно действующей до вступления в силу указанного Федерального закона от 21.07.2011 г. № 252-ФЗ редакции статьи 14 Федерального закона «Об основных гарантиях прав ребенка в Российской Федерации» органы государственной власти Российской Федерации принимают меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, а также от распространения печатной продукции, аудио- и видеопроизведений, пропагандирующей насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение.

В целях обеспечения здоровья, физической, интеллектуальной, нравственной, психической безопасности детей федеральным законом, законами субъектов Российской Федерации устанавливаются нормативы распространения печатной продукции, аудио- и видеопроизведений, иной продукции, не рекомендуемой ребенку для пользования в соответствии с

пунктом 1 настоящей статьи до достижения им возраста 18 лет.

В соответствии со статьей 14.1. Федерального закона «Об основных гарантиях прав ребенка в Российской Федерации» (введена Федеральным законом от 28.04.2009 г. № 71-ФЗ) в целях содействия физическому, интеллектуальному, психическому, духовному и нравственному развитию детей и формированию у них навыков здорового образа жизни органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации, органы местного самоуправления в соответствии с их компетенцией создают благоприятные условия для осуществления деятельности организаций, образующих социальную инфраструктуру для детей (включая места для их доступа к сети «Интернет»).

Законами субъектов Российской Федерации в целях предупреждения причинения вреда здоровью детей, их физическому, интеллектуальному, психическому, духовному и нравственному развитию могут устанавливаться, в частности, меры по недопущению нахождения детей (лиц, не достигших возраста 18 лет) в ночное время в общественных местах, в том числе на объектах (на территориях, в помещениях) юридических лиц или граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, которые предназначены для обеспечения доступа к сети «Интернет» и в иных общественных местах без сопровождения родителей (лиц, их заменяющих) или лиц, осуществляющих мероприятия с участием детей.

За несоблюдение установленных требований к обеспечению родителями (лицами, их заменяющими), лицами, осуществляющими мероприятия с участием детей, а также юридическими лицами или гражданами, осуществляющими предпринимательскую деятельность без образования юридического лица, мер по содействию физическому, интеллектуальному, психическому, духовному и нравственному развитию детей и предупреждению причинения им вреда законами субъектов Российской Федерации может устанавливаться административная ответственность.

В целях защиты несовершеннолетних от злоупотреблений их доверием и недостатком опыта Федеральным законом от 13.03.2006 г. № 38-ФЗ «О рекламе» установлен комплекс ограничений при распространении рекламной продукции.

В рекламе (в том числе распространяемой в информационно-телекоммуникационных сетях) не допускаются (ст. 6): 1) дискредитация родителей и воспитателей, подрыв доверия к ним у несовершеннолетних; 2) побуждение несовершеннолетних к тому, чтобы они убедили родителей или других лиц приобрести рекламируемый товар; 3) создание у несовершеннолетних искаженного представления о доступности товара для семьи с любым уровнем достатка; 4) создание у несовершеннолетних впечатления о том, что обладание рекламируемым товаром ставит их в предпочтительное положение перед их сверстниками; 5) формирование комплекса неполноценности у несовершеннолетних, не обладающих рекламируемым товаром; 6) показ несовершеннолетних в опасных ситуациях;

7) преуменьшение уровня необходимых для использования рекламируемого товара навыков у несовершеннолетних той возрастной группы, для которой этот товар предназначен; 8) формирование у несовершеннолетних комплекса неполноценности, связанного с их внешней непривлекательностью.

Законом запрещено также распространение ненадлежащей рекламы, в том числе: побуждающей к совершению противоправных действий (п. 1 ч. 4 ст. 5 Закона о рекламе); призывающей к насилию и жестокости (п. 2 ч. 4 ст. 5 Закона о рекламе); содержащей демонстрацию процессов курения и потребления алкогольной продукции, а также пива и напитков, изготавливаемых на его основе (п. 5 ст. 5 Закона о рекламе); использующей бранные слова, непристойные и оскорбительные образы, сравнения и выражения (ч. 6 ст. 5 Закона о рекламе).

Действуют ограничения для рекламы, размещаемой в детских и образовательных телепередачах, радиопрограммах и радиопередачах (ч. 7 ст. 14, ч. 6 ст. 15 Закона о рекламе). Установлены ограничения для рекламы отдельных видов продукции, представляющей опасность для здоровья и развития детей: алкогольной продукции (ст. 21), пива и напитков, изготавливаемых на его основе (ст. 22), табака, табачных изделий и курительных принадлежностей (ст. 23), лекарственных средств, медицинской техники, изделий медицинского назначения и медицинских услуг (ст. 24), основанных на риске игр, пари (ст. 27). Такая реклама не должна обращаться к несовершеннолетним и использовать их образы, не может размещаться в предназначенных для несовершеннолетних печатных изданиях, аудио- и видеопродукции.

В настоящее время информационная безопасность детей при просмотре аудиовизуальных произведений регулируется также комплексом установленных законодательством РФ требований к содержанию аудиовизуальной информационной продукции, предназначенной для распространения среди разных возрастных групп несовершеннолетних.

В целях упорядочения публичной демонстрации и распространения аудиовизуальных произведений на любых видах носителей, защиты детей и подростков от аудиовизуальной продукции, которая может нанести вред их здоровью, эмоциональному и интеллектуальному развитию, введена возрастная классификация аудиовизуальных произведений, соответствующая психо-возрастным особенностям восприятия зрительской аудиторией: фильм разрешен для показа в любой зрительской аудитории; детям до 12 лет просмотр фильма разрешен в сопровождении родителей; фильм разрешен для показа зрителям, достигшим 14 лет; фильм разрешен для показа зрителям, достигшим 16 лет; фильм разрешен для показа зрителям, достигшим 18 лет (Приказ Роскультуры от 15.03.2005 г. № 112 (ред. от 01.07.2005) "Об утверждении Руководства по возрастной классификации аудиовизуальных произведений, положения и состава экспертного совета по возрастной классификации аудиовизуальных произведений").

Для исключения доступа учащихся образовательных учреждений к

ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания, за счет средств федерального бюджета в федеральных государственных образовательных учреждениях, государственных образовательных учреждений субъектов РФ и муниципальных образовательных учреждений, реализующих общеобразовательные программы начального общего, основного общего и среднего (полного) общего образования, к сети Интернет, предусмотрены внедрение и актуализация системы исключения доступа к интернет-ресурсам, несовместимым с задачами образования и воспитания учащихся, внедрение в этих целях средств контентной фильтрации и иных аппаратно-программных и технико-технологических устройств. [16]

В 2014–2015 учебном году Фондом Развития Интернет было проведено исследование межличностных отношений российских детей и подростков в Интернете. Было проанализированы особенности современной подростковой дружбы; различия между реальной и виртуальной дружбой; значение для современного подростка виртуальных друзей.

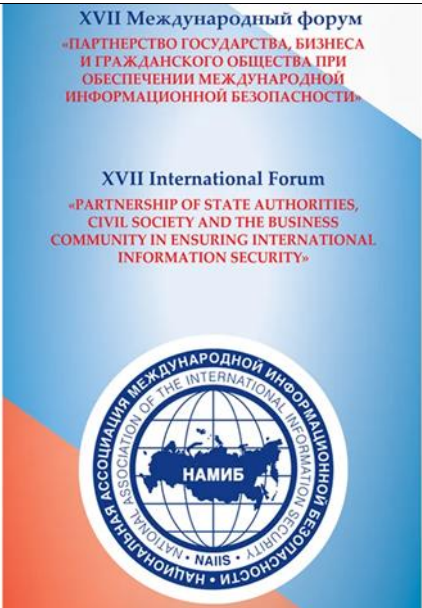
Чтобы ответить на поставленные выше вопросы, сотрудниками Фонда было проведено специальное исследование. Сбор данных проводился в рамках образовательного проекта «Предметные сборы: Малая Академия Подмосковья-2015». В анкетировании приняли участие 130 человек, учащиеся 8-х классов школ Московской области (возраст — 13–14 лет; 63 мальчика и 67 девочек). Сотрудниками Фонда Развития Интернет была подготовлена анкета, включающая 43 вопроса, объединенных по разделам: дружба и межличностные отношения в реальной жизни; особенности и характеристики виртуальной дружбы; использование подростками Интернета; жизнь подростков в социальных сетях (действия — лайки, блокировка и удаление из друзей, контент и 28 события). В частности, в одном из вопросов подросткам было предложено закончить два следующих предложения: «Дружба в реальной жизни — это...» и «Дружба в социальных сетях — это...». По итогам контент-анализа полученных ответов были выделены категории, на основе которых сравнивались взгляды подростков на реальную и виртуальную дружбу.

Исследование отношения российских детей и подростков к персональным данным и рискам, возникающим вследствие неосторожного обращения с личной информацией в Интернете (2014–2015 гг.)

В данном исследовании анализируется отношение российских детей и подростков к персональным данным, проблемы, возникающие в результате их неправомерного использования, а также отношение родителей к данному вопросу и возможности оказания ими помощи своим детям в защите персональных данных. Для этого сотрудниками Фонда был осуществлен контент-анализ информации, которую сообщает о себе подростковая аудитория, проведенный на основе поиска социальной сети ВКонтакте (март, 2015 г). Для проверки и уточнения данных, представляемых поиском, также было проведено исследование 100 профилей московских подростков 14–17 лет (54 мальчика и 46 девочек). Отмечалось наличие либо отсутствие различных видов персональной информации на странице. Кроме этого, дополнительно был

проведен анализ содержимого записей на стенах этих подростков в социальной сети (итого 1000, по 10 последних в каждом профиле записей).

Для сравнительного анализа в работе были использованы данные, полученные в ходе исследования 2010 года, проведенного в рамках проекта Еврокомиссии EU Kids Online II (выборка по 11 регионам Российской Федерации составила 1025 пар родитель-ребенок в возрасте от 9 до 16 лет). Кроме этого, для анализа динамики рисков, возникающих вследствие неосторожного обращения с персональными данными, нами были использованы результаты исследования цифровой компетентности российских подростков и их родителей (2012–2013 г.). Выборку составили 1203 подростка 12–17 лет и 1209 родителей детей этого возраста из 58 городов с населением от 100 тысяч человек и во всех 8 федеральных округах России.

	Интернет глазами школьника. Взаимодействие в школьном коллективе не ограничивается учебным процессом и неформальными контактами учащихся. Современные школьники все чаще обращаются к ресурсам Интернета, имея различную мотивацию: поиск информации, развлечения, общение и многое другое. Каким видят школьники Интернет? Каким они хотят его видеть? Как оптимизировать Сеть и сделать ее удобной и безопасной для школьников? — Ответы на эти и многие другие вопросы дает исследование «Интернет глазами школьника».

В рамках данного исследовательского проекта нами было опрошено 460 респондентов, учащихся школ Москвы и Московской области. [17]

НАМИБ – национальная ассоциация международной интернациональной безопасности, в сентябре 2023 года провела форум, по теме: «Международная безопасность в глобальном ИКТ- среде, в условиях формирования многополярного мира». Целью международного форума было обсуждение актуальных проблем развития сотрудничества по вопросам обеспечения использования ИКТ -среды и формирование системы международной информационной безопасности в новых геополитических условиях. Ссылка сайта с программой [17]

Исторически кибербуллинг можно обнаружить на площадках,

популярных у интернет-аудитории. С распространением интернета в начале 2000-х гг. он чаще всего проявлялся в сетевых чатах. После появления в России социальных сетей (с 2006 г. – «ВКонтакте», «Одноклассники»; с 2010 г. – «Инстаграм») [2; 4] они стали лидерами по количеству эпизодов кибер- травли в онлайн-среде. Согласно исследованию 2019 г. феномен кибербуллинга чаще всего проявлялся в социальных сетях – в 40,3% случаев (на «ВКонтакте» приходится 20,3%, «Инстаграм» – 5,9%, «Фейсбук» – 4,4%).

По данным Mail.ru Group, Исследование Mail.ru Group на тему кибербуллинга и отношения пользователей к этому явлению [18] на ноябрь 2019 г. с кибербуллингом сталкивались 58% опрошенных россиян, а 4% из них признались, что выступили в роли инициаторов. 47% респондентов отметили, что встречались с агрессией чаще в виртуальной, нежели в реальной жизни.

Программа KiVa финансировалась Министерством образования и культуры Финляндии.

Программа KiVa по борьбе с издевательствами началась в 2006 году в Университете Турку в Финляндии для учащихся в возрасте от 7 до 15 лет. Она преподается в виде серии уроков для учащихся и онлайн-игр в течение года, обучая детей тому, как поддерживать и высказываться, если они узнают о том, что кто-то подвергается кибербуллингу [9]

Программа KiVa финансировалась Министерством образования и культуры Финляндии. Программа KiVa по борьбе с издевательствами началась в 2006 году в Университете Турку в Финляндии для учащихся в возрасте от 7 до 15 лет. Она преподается в виде серии уроков для учащихся и онлайн-игр в течение года, обучая детей тому, как поддерживать и высказываться, если они узнают о том, что кто-то подвергается кибербуллингу [9]

Вмешательство фокусируется на реакциях свидетелей на ситуацию издевательства. Реакция на ситуацию издевательства получает то, что программа KiVa намеревается изменить. Цель KiVa — заставить окружающих идентифицировать себя с жертвой, а не с хулиганом. Выявив жертву и почувствовав сочувствие к ней, агрессор больше не будет получать положительных ответов или привлекать внимание. Программа направлена на то, чтобы лишить власти посты хулиганов в социальных сетях. Это внимание, как правило, помогает и подкрепляет обидчика. Без подкрепления социальное вознаграждение хулиганов и, следовательно, их мотивация к хулиганству будут устранены [9]

Эта программа не наказывает обидчика; вместо этого он отмечает тех, кто поддерживает жертв киберзапугивания. «Программа предназначена для достижения эффекта, прежде всего, путем поощрения учащихся к поддержке пострадавших сверстников, а не к социальному вознаграждению хулиганов. Кроме того, взрослым (учителям и родителям) предоставляется информация о буллинге и эффективности вмешательства и предотвращения». Онf направлен на то, чтобы сделать социальные сети безопасным пространством для школьников, которым они могут пользоваться для развития и эмоциональным вовлечением (то есть польза и удовлетворение) [9]

В Испании в школах Cyber Program 2.0 преподают в течение года в рамках 19 одночасовых занятий. «Было подтверждено, что программа уменьшает агрессивное/киберзапугивающее поведение». Программа ставит перед собой четыре цели на учебный год, выявить и осмыслить травлю/кибербуллинг, проанализировать последствия буллинга/кибербуллинга; разработать стратегии преодоления для предотвращения и сокращения буллинга/кибербуллинга; и (4) развивать положительные черты, такие как эмпатия, активное слушание и социальные навыки. CyberProgram 2.0 достигает этих целей, разбивая программу на три модуля: «Концептуализация и определение ролей», «Последствия», «Права и обязанности» и «Стратегии выживания» [9]

В CyberProgram 2.0 есть 25 различных действий. Первые пять заданий помогают учащимся определить, что такое киберзапугивание, следующие пять заданий учат студентов анализировать прямые и косвенные последствия акта киберзапугивания, а программа завершается пятнадцатью заданиями, предназначенными для анализа моделей запугивания с точки зрения жертв, агрессор, наблюдатель. Каждое занятие будет включать в себя цель, направленную на повышение сочувствия, взгляд на последствия этого киберпреступления, позитивные стратегии, чтобы справиться с этой ситуацией, а также обсуждение или дебаты [9]

Важно понимать, что киберзапугивание в школах не может быть устранено, но учитель может реализовать программу по сокращению случаев кибербуллинга и эффективному использованию социальных сетей. Чтобы этот или любой другой план был успешным, необходимо включить в него две части. Во-первых, это обязательное обучение родителей, учителей и персонала киберзапугиванию. Это образование поможет взрослым поддерживать учащихся, понимая, на каких сайтах находятся их ученики; они также изучат терминологию киберзапугивания. Кроме того, они будут обучены тому, как стать союзником против киберзапугивания. Это будет включать в себя изучение того, на что следует обращать внимание, если вы

подозреваете, что ребенок подвергается киберзапугиванию, и к кому обращаться, если ребенок стал жертвой киберзапугивания. Вторая часть будет обучать студентов ежемесячной программе, которая проводится в течение учебного года. Программа будет работать со школьниками, чтобы они стали союзниками против киберзапугивания [9]

Итак, буллинг это глобальное и массовое явление, основой которого является власть, лидерство и конкуренция, организованное преимущественно детским коллективом, в первую очередь в школе. Буллинг охватывает неравенство силы и власти, что приводит жертву в состояние, в котором она не в состоянии защитить себя от негативных действий. Поэтому возникает острая потребность в подготовке педагогов и психологов с определенными теоретическими знаниями, специальными навыками и умениями, для предупреждения и преодоления такого негативного явления, как буллинг.

США и Канада

В Сан-Франциско субкультурные молодёжные движения были связаны с новыми технологиями и заложили идеологию открытого доступа, технооптимизма и карнавальной мультимедийной эстетики. По словам американского писателя и футуролога С. Брандона, хиппи-поколение «залпом проглотило компьютеры, почти как дозу» (Савицкая. 2018. С. 12). За ними следовало поколение скептиков, предложивших популярный жанр киберпанковской антиутопии (писатели У. Гибсон, Б. Стерлинг и др.). В среде киберпанка появился журнал Mondo2000, затем более уважаемый Wired. Если литературный киберпанк воспроизводил анархистский сценарий сопротивления и эскапизма, то теоретики искали способы понять технологию как новую культурную парадигму. Интерпретировались теории предшествующего периода, в частности книги Г. М. Маклюэна и Э. Тоффлера. Значительную роль играли постструктуралистские работы Ж. Делёза, Ж. Деррида, Ж. Бодрийяра, Ж.-Ф. Лиотара и др. В журналах печатались тексты писателя Х. Бея с его теорией автономных зон и изучавшей технологическое бессознательное Э. Ронелл. Сборник «Технокультура» (Technoculture. 1991) собрал актуальные статьи в их междисциплинарном пересечении, включавшем социологию научного знания, культурные исследования, феминистскую эпистемологию, психоанализ кино и теорию литературной и научной фантастики.

В сборнике «Технокультура» был опубликован «Манифест киборга» Д. Харауэй, написанный в 1985 г. Этот манифест был назван культовым текстом новой технокультуры. Харауэй предложила фигуру киборга (киборганического-органического) как ключевой репрезентации постгуманизма, который постулирует отказ от бинарности – природа/культура, техника/биология. Харауэй описала переход от ранней кибернетической парадигмы к современной и показала это на ряде дисциплин: от доминирования власти к распределённым информатикам господства, от реалистического романа к фантастике, от микробиологии к иммунологии, от репрезентации к симуляции, от целостного организма к комплексу биотических систем. Природа лишается естественности, а культурная инстанция лишается доминирования над природой. В пространстве, где различие природы и культуры было обязательным, обнаруживается территория политики, технологии, семиотики, которая оперирует формированием различий тел, социальных правил, технологий доступа.

Харауэй была участницей «научных войн» реалистов с антиреалистами и феминистской критики научной эпистемологии 1980-х гг. об устройстве знания: кто и как формирует научный объект и в чью пользу он работает. Её критика способов познания показала, что научный объект (в том числе природа, общество, техника) – это исторические понятия о «естественном», которые связаны с политическими и гендерными фильтрами, исключаящими из научного знания множество акторов, опытов и голосов.

Другой значимый центр киберкультурных исследований Северной

Америки находился в Канаде, где исследователи А. Крокер и М. Крокер (последователи торонтской школы Г. Инниса и Г. М. Маклюэна) с 1993 г. издавали культовый журнал CTheory, в котором исследовали трансформацию киберкультуры от раннего оптимизма к социальному и интеллектуальному неравенству. Одним из значимых центров для исследования звука и визуальности в новом искусстве была Studio XX в Торонто.

Австралия

Австралийская арт-группа VNS Matrix и ряд исследователей (З. Софулис, В. Кирби, М. Уорк и др.) изменили местную культурную идентичность, превратив Австралию из провинции в лидеры технологической культуры. Именно здесь был создан центр SymbioticA, в котором учёные и художники вместе работали над созданием нового творческого направления, получившего название science art.

В 2002 г. издан сборник «Предваряя киберкультуру: интеллектуальная история киберкультуры и киберкультурных исследований» («Prefiguring Cyberculture: Intellectual History of Cyberculture and Cyberculture Studies»). В сборнике анализируется теоретическая развилка в понимании киберкультуры и киборга. С одной стороны, в концепции, представленной книгой П. Эдвардса «Закрытый мир. Компьютеры и дискурсивные политики американской холодной войны» (Edwards. 1996) доказывается, что милитаризм формирует концепцию киборга как замещения тела машинами, подобно захвату космоса в фильмах «Звёздные войны» и «Космическая Одиссея». С другой стороны, З. Софулис в статье «Манифест киборга» Харауэй как эффект (кибер)землетрясения» (Sofoulis. 2002) показывала, как эпистемологическое решение Харауэй позволяет выйти из замкнутого круга власти и подчинения. Она констатировала, что подход Харауэй сильно повлиял на большинство киберкультурных и технонаучных исследований и произвёл эффект «землетрясения» в эпистемологии культурологии. З. Софулис была ключевой фигурой, формировавшей киберкультурные исследования в Австралии, и одной из основоположниц (кибер)феминистских подходов в теории технологии, философии аффекта, экологии.

Другая знаковая фигура австралийской киберкультуры – М. Уорк. В начале 2000-х гг. он переехал в США, где позже совершил трансгендерный переход. В своей ранней книге «Виртуальная республика» (Wark. 1997) Уоркразрабатывал концепцию новой культурной парадигмы как «глобального медиасобытия», в котором переопределяются социальные отношения, гендерные и расовые политики. В наиболее известной книге Уорк под названием «Манифест хакера» («A Hacker Manifesto», 2004) исследовалось появление новых форм социального неравенства, возникающего из-за частной собственности на результаты интеллектуального производства. Формирующаяся классовая структура разделяет хакеров, создающих новые культурные коды, и присваивающий их класс векторалистов, которые контролируют сети и монетизируют информацию через законы превращения в товар интеллектуальной собственности.

Европейская ситуация характеризуется не только контркультурами и новыми технологическими ситуациями (как в США или Австралии), но и глобальными политическими трансформациями, вызванными окончанием «холодной войны» и падением Берлинской стены с последующим объединением Европы. Медиахудожники создавали объединения искусства новых медиа и осуществляли обмен между западноевропейскими и постсоциалистическими арт-сообществами. На выставке современного искусства «Документа IX» (Кассель, Германия, 1992) был представлен спецпроект Van-Gogh TV «Piazza Virtuale». Его идея состояла в том, чтобы через видеотелефоны соединить людей разных стран и континентов в едином коммуникационном поле. На практике это значило раздать видеотелефоны творческим сообществам разных стран «Запада и Востока», которые будут создавать медиаперформансы и альтернативное телевидение. Таким образом, зрители становились одновременно и создателями трансляций. С технической точки зрения наибольшую трудность представляла задача объединить десятки камер и вывести их одновременно на десятки мониторов в студию, транслировать на экраны, расставленные на территории выставок «Документа», и получать видео и телефонные акции и звонки в реальном времени.

Многие исследовательские, художественные и социальные инициативы 1990-х гг. привели к созданию горизонтальных координирующих и информирующих проектов – подписных листов или массовых рассылок. Группы исследователей объединялись в социальные сети через массовые почтовые рассылки, создающие онлайн-сообщества. Из этой модели впоследствии возник ранний вариант «Живого журнала».

Подписной лист почтовой рассылки Nettime был как инструментом создания сообщества, так и платформой для критических интернациональных дискуссий. Он был предложен теоретиком медиа Г. Ловинком (Ловинк. 2019) и П. Шульцем в 1995 г. Задача платформы состояла в формировании нового поля для новых форм исследования и производства киберкультуры, а также для разработки её коммуникационных тактик, свободных от академических канонов. С той же целью была создана информационная сеть роттердамской галереи V2, объединявшая интернациональные сообщества медиахудожников.

О создании Faces – сети и подписного листа почтовой рассылки, было формально объявлено в 1997 г. на съезде Киберфеминистского интернационала, проходившего в рамках выставки «Документа X» в Касселе. Лист был результатом многолетней работы формирования сообщества, проводимой куратором и исследовательницей медиаискусства К. Р. Хоффман. Киберфеминистский интернационал был созван группой медиахудожниц OBN (К. Солльфранк и др.) и активистками Faces Д. Маккарти, В. Джорджевич и др.

По аналогии с европейскими сетевыми сообществами была сделана Нью-Йоркская сеть Rizoma. Подписные листы в начале координировали собрания и конференции, а позднее листы трансформировались в издания, координационные сети и базы данных. Наиболее полная база данных ранней киберкультуры Monoscope включала основные инициативы, имена и тексты

раннего периода киберкультуры. База создавалась с 1990-х гг. и впоследствии была переведена на программное обеспечение «Википедии».

Другая ранняя форма сетевых сообществ – соединение сайтов перекрёстными ссылками (Rings of sites). С 2003 г. на 3D-платформе Second Life стали возникать проекты художников и виртуальные арт-галереи. Параллельно происходит сближение самоорганизованных арт-сообществ с исследовательскими центрами. Ф. Киттлер создал Группу исследования литературы и медиа в Касселе (1986–1990), затем преподавал теорию медиа в Берлинском университете. В Кёльне в 1989 г. как «электронный Баухауз» была организована Академия медиаискусства. В группе создавших её исследователей состоял один из основателей медиаархеологии – З. Цилински (2019).

История Группы исследований кибернетической культуры в Уорикском университете, связанной с преподавателями философии С. Плант и Н. Ландом, оказалась непродолжительной по времени (1994–1998), но в дальнейшем повлияла на формирование философских движений спекулятивного реализма, киберфеминизма, акселерационизма.

Одновременно формировались центры и галереи в нелегально занятых помещениях: например, галерея V2 в Роттердаме, галерея MUU в Хельсинки, «Галерея 21» и «Кибер-фемин-клуб» в Санкт-Петербурге, хакерские группы «grrls» (First cyberfeminism international... 1997), группа Tiqqun во Франции в конце 1990-х гг.

В это время проводились конференции и фестивали в смешанном субкультурном и академическом формате: DEAF (Голландский фестиваль электронного искусства, Роттердам, с 1994); Next 5 Minutes и «Тактические медиа» (Амстердам, Роттердам, с 1993); «Третья реальность» (Санкт-Петербург, 1993–1996); конференция, выставка и мастерские электронного искусства Штюбниц (Санкт-Петербург, кураторы А. Медош, А. Митрофанова, 1994). В 1994 г. в лондонском Институте современного искусства ICA прошла организованная Плант конференция под названием «Соблазнённое и отвергнутое: Тело в виртуальном мире – Киберпространство женщин». Группа исследований кибернетической культуры дважды проводил в Уорикском университете конференцию «Виртуальные образы будущего: киберотика, технология и постчеловеческий прагматизм» (Virtual Futures. 1998). В более коммерческом и массовом формате проходили Международный симпозиум электронного искусства (ISEA) и SIGGRAPH, проводимая Ассоциацией вычислительной техники по вопросам компьютерной графики. ARS Electronica стала центральным событием искусства новых технологий.

Отдел ООН по борьбе с киберпреступностью помогает вычислить педофилов и защитить детей. [19]

(Первоначально опубликовано Центром новостей ООН)

Что делает ООН для защиты молодых людей в Интернете.

Безграничный характер Интернета означает, что обеспечение безопасности молодых людей в сети является глобальной задачей. ООН

активно работает над защитой детей и молодежи в Интернете с помощью различных программ и инициатив.

Кибербезопасность

Инициатива по защите детей в Интернете (COP) - это многосторонняя сеть, созданная Международным союзом электросвязи (МСЭ) с целью повышения осведомленности о безопасности детей в Интернете и разработки практических инструментов для оказания помощи правительствам, промышленным предприятиям и педагогам. Руководство МСЭ по защите детей в Интернете представляет собой всеобъемлющий набор рекомендаций для всех соответствующих заинтересованных сторон о том, как внести свой вклад в развитие безопасной и расширяющей возможности детей и молодежи среды в Интернете.

Детский фонд ООН (ЮНИСЕФ) объединился с платформами социальных сетей, чтобы ответить на некоторые из наиболее распространенных вопросов о киберзапугивании и дать советы о том, как с ним бороться. Эта инициатива ЮНИСЕФ направлена на то, чтобы положить конец киберзапугиванию.

Каждый первый четверг ноября Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) отмечает Международный день борьбы с насилием и запугиванием в школе, включая киберзапугивание, признавая, что насилие в школе во всех его формах является нарушением прав детей и подростков на образование, здоровье и благополучие. Этот день дает возможность заинтересованным сторонам во всем мире активизировать усилия по обеспечению безопасности учащихся в школе и в онлайн-пространстве.

ЮНИСЕФ предотвращает сексуальную эксплуатацию детей в Интернете и реагирует на нее на страновом и глобальном уровнях. Он поддерживает скоординированные национальные меры по борьбе с сексуальной эксплуатацией детей в Интернете в более чем 20 странах, используя модель глобального альянса WePROTECT, укрепляя потенциал специалистов на местах по оказанию услуг жертвам.

Всемирная организация здравоохранения (ВОЗ) в своем отчете за 2022 год о предотвращении онлайн-насилия в отношении детей уделяет особое внимание сексуальному насилию над детьми, включая груминг и надругательство над сексуальным образом, а также кибер-агрессию и домогательства. В докладе подчеркивается важность реализации образовательных программ, ориентированных на детей и родителей.

Торговля людьми — это преступление, в результате которого люди становятся объектом торговли и эксплуатации в корыстных целях. Торговцы людьми стали умело использовать интернет-платформы для вербовки жертв и привлечения клиентов. Дети и подростки подвержены обманным уловкам в поисках признания, внимания или дружбы, и часто «обхаживаются» торговцами людьми в социальных сетях. Управление ООН по наркотикам и преступности (УНП ООН) поддерживает государства-члены в их усилиях по предотвращению и борьбе с торговлей людьми, в том числе посредством

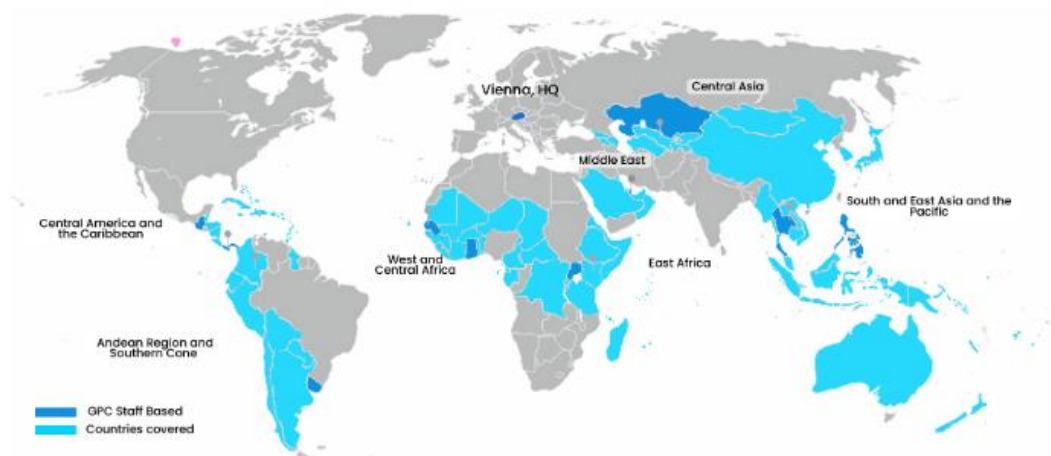
мероприятий по повышению осведомленности о безопасности в Интернете, направленных на детей и подростков.

ЮНЕСКО возглавляет глобальные усилия по разработке нормативных решений для повышения достоверности информации на цифровых платформах в условиях роста дезинформации. В феврале 2023 года агентство ООН провело конференцию «Интернет, как источник достоверной информации», на которой обсуждался ряд глобальных руководящих принципов, направленных на создание безопасной и надежной интернет-среды для пользователей при защите свободы выражения мнений и доступа к информации. Руководство призывает цифровые платформы признать свою особую ответственность перед детьми. Поскольку в детском возрасте происходит становление личности. При этом возможности детей влиять на принятие мер директивного характера крайне ограничены.

ЮНЕСКО также является ведущим учреждением ООН по продвижению медийной и информационной грамотности (МИГ), которая дает людям возможность критически осмысливать информацию и использовать цифровые инструменты. ЮНЕСКО стремится вооружить молодежь навыками медийной и информационной грамотности, чтобы они могли стать активными участниками процесса создания и распространения знаний и информации о ресурсах МИГ. С 2016 года ЮНЕСКО проводит Форум молодежной повестки дня, чтобы помочь молодым людям узнать о последних достижениях в области МИГ. Это часть ежегодной Глобальной недели медийной и информационной грамотности — важной возможности для заинтересованных сторон проанализировать и отметить прогресс, достигнутый на пути к медийной и информационной грамотности для всех.



Объединенные Нации.



Конференция участников Конвенции Организации Объединенных Наций о трансграничной организованной преступности определила киберпреступность, преступления с использованием личных данных,

незаконный оборот культурных ценностей, экологические преступления, пиратство, торговлю органами и мошенничество в медицине в качестве новых и возникающих преступлений, вызывающих обеспокоенность. Появление этих новых видов преступлений приводит к необходимости реагирования правоохранительных органов на соответствующую адаптацию своих усилий и возможностей.

Цели: Повышение институциональной эффективности и результативности в предотвращении, пресечении, расследовании, судебном преследовании киберпреступлений в соответствии с принципами прав человека;

Укрепление национальной и международной связи и сотрудничества между правительством, правоохранительными органами и частным сектором для улучшения, предотвращения, нарушения и расследования киберпреступности;

Расширение знаний и повышение осведомленности общества о снижении рисков киберпреступности;

Принятие эффективно-правовой базы, ведущей к устойчивому и долгосрочному реагированию на борьбу с киберпреступностью в соответствии с международным стандартом.

Модель воздействия и содействия изменению потенциала государств-членов в области борьбы с киберпреступностью.

Хотя доступ в Интернет рассматривается как показатель развития, заметный рост киберпреступлений на национальном, региональном и глобальном уровнях показал необходимость противодействия киберзависимым и киберпреступлениям. Растущее число пользователей Интернета, использующих широкополосную и мобильную передачу данных, привело к увеличению числа потенциальных жертв киберпреступлений.

Во время пандемии COVID-19 организованная преступность продемонстрировала способность адаптировать свою деятельность к «новым нормам», несмотря на карантин и закрытие границ. Новые криминальные направления, разработанные организованной преступностью в этот период (онлайн-торговля наркотиками и оружием, цифровое мошенничество, программы-вымогатели, вредоносное ПО как услуга и т. д.), представляют собой новую криминальную взаимосвязь, которая уже влияет на безопасность и социально-экономическое развитие Государства-члены, особенно наименее развитые, которые имеют низкий потенциал для борьбы с киберпреступностью и проведения цифровых расследований. Киберзависимые и киберпреступления прибыльны и могут позволить преступным организациям расширять свои рынки через границы и достигать новых жертв с минимальной логистикой и меньшими рисками. В УНП ООН мы наблюдаем, что организованная преступность уже использует весь потенциал цифровых инструментов в преступных целях, максимально используя социальные сети для охвата жертв, скрываясь в даркнете, используя передовые методы анонимизации и сокрывая преступные доходы с помощью криптовалютных транзакций.

В этой ситуации государства-члены обычно характеризуются отсутствием:

Понимание картины национальных угроз и имеющихся возможностей.

Обученный персонал.

Соответствующее оборудование.

Соответствующее законодательство или законодательные рекомендации

Функциональные рамки внутреннего и международного сотрудничества.

Информирование общественности.

Эта первоначальная ситуация и необходимые изменения варьируются от государства-члена к государству-члену. Однако УНП ООН через Глобальную программу по киберпреступности применяет уникальную модель технической помощи, адаптированную к каждой стране и региону, чтобы способствовать позитивным изменениям в направлении глобальных целей и результатов.

В этом контексте возросшей связности и уязвимости способность предотвращать, обнаруживать, преследовать и противодействовать киберпреступности никогда не была более актуальной. Для этого крайне важно обеспечить, чтобы государства-члены имели обновленный потенциал для эффективного расследования и судебного преследования организованной преступности, действующей в Интернете.

В модели борьбы с киберпреступностью Глобальной программы используется постепенный процесс, и продолжительность каждого этапа зависит от обстоятельств в конкретной стране. Учитывая глобальную картину киберугроз и их возможные последствия на региональном и национальном уровне:

УНП ООН оценивает возможности государства-члена противодействовать и предотвращать киберпреступность

1. На основе этой оценки, принимая во внимание национальные, двусторонние и многосторонние усилия по наращиванию потенциала, УНП ООН и государства-члены согласовывают индивидуальный национальный план действий с учетом внешних обстоятельств и дополнительного вклада третьих сторон.

2. Первоначальное обучение отдельных специалистов в области уголовного правосудия проводится в различных областях вмешательства. Когда это возможно и доступно, академии правоохранительных органов участвуют в разработке и проведении обучения для обеспечения устойчивости на уровне страны.

3. После обучения национальные учреждения по предотвращению и противодействию киберпреступности обеспечиваются необходимым оборудованием (на основе имеющихся пожертвований).

4. Кибергруппы и наставники УНП ООН, базирующиеся в регионах или странах, оказывают поддержку подготовленным национальным должностным лицам в их работе по борьбе с киберпреступностью (киберзависимыми и киберпреступными).

5. Киберкоманды и наставники сокращают свою поддержку, поскольку обученные специалисты по уголовному правосудию становятся тренерами и могут повторить свое обучение дома и в других странах.

6. Материалы, руководства, кампании по повышению осведомленности и мероприятия по сотрудничеству в различных областях вмешательства разрабатываются в координации с местными властями для обеспечения преемственности и комплексного подхода в противодействии и предотвращении киберпреступности.



Международного определения киберпреступности не существует. В широком смысле киберпреступность можно охарактеризовать как широкое понятие, охватывающее киберзависимые и киберпреступления.

Киберзависимые преступления требуют инфраструктуры ИКТ и часто характеризуются созданием, распространением и развертыванием вредоносных программ, программ-вымогателей, атаками на критически важную национальную инфраструктуру (например, киберзахват электростанции организованной преступной группой), захватом веб-сайта. в автономном режиме, перегружая его данными (DDoS-атака [распределенный отказ в обслуживании]) или получая доступ к конфиденциальным данным клиента.

Киберпреступность может происходить и в автономном мире, но ей также могут способствовать ИКТ. Обычно это включает онлайн-мошенничество, покупку наркотиков через Интернет и отмывание денег через Интернет.

Учитывая масштабы рисков киберпреступности, специализированные области, связанные с этим видом преступности и его преодоления, а также разнообразные возможности, которыми обладают государства-члены для предотвращения и противодействия киберпреступности, Глобальная программа по киберпреступности способствует долгосрочному и устойчивому наращиванию потенциала для предотвращения киберпреступности и борьбы с ней. путем поддержки национальных структур.

Программа включает в свой пакет услуг техническую помощь, начиная от предотвращения преступлений и заканчивая судебным разбирательством по ним; от обнаружения до предоставления суду цифровых доказательств; сбор и анализ доказательств; поддержка расследования, судебного преследования и вынесения приговора; в киберзависимых и киберпреступлениях, включая сексуальное насилие и эксплуатацию детей в Интернете, а также преступное/незаконное использование виртуальных активов.

В частности, УНП ООН использует свой специализированный опыт реагирования систем уголовного правосудия для оказания технической помощи в наращивании потенциала, нормативной помощи, предотвращении и повышении осведомленности, сотрудничестве, а также исследованиях и анализе тенденций киберпреступности. Этот опыт предоставляется посредством целостного программного подхода: наращивание

потенциала/техническая помощь, сотрудничество и нормативная помощь/правовая база.

Этот подход применяется в областях вмешательства, в которых осуществляет свою деятельность Глобальная программа по киберпреступности, включая киберрасследования, сексуальное насилие и эксплуатацию детей в Интернете, цифровую судебную экспертизу, цифровые доказательства, виртуальные активы и профилактику.



Киберрасследования

Работать над созданием и укреплением навыков и потенциала специалистов уголовного правосудия и сотрудников правоохранительных органов по предотвращению, пресечению, расследованию, судебному преследованию и осуждению киберзависимых и киберпреступлений.



Сексуальное насилие и эксплуатация детей в Интернете.

Координировать выявление и реагирование между всеми участниками на случаи сексуального насилия и эксплуатации детей в Интернете, а также материалы о сексуальном насилии над детьми, обеспечивая подход, ориентированный на жертв.



Цифровая криминалистика

Работать над созданием и укреплением навыков и потенциала специалистов уголовного правосудия в области выявления, изъятия, обработки, сохранения и сообщения цифровых доказательств.



Цифровые доказательства

Работать над созданием и укреплением навыков и возможностей специалистов уголовного правосудия в области выявления, понимания, запроса, анализа, сохранения и представления цифровых доказательств.



Виртуальные активы

Признавая уникальные особенности виртуальных активов, работайте над созданием и укреплением навыков и возможностей специалистов уголовного правосудия и сотрудников правоохранительных органов по расследованию, отслеживанию и анализу виртуальных активов.

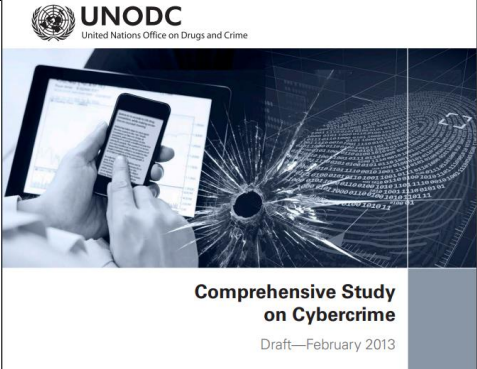


Профилактика

Работайте над обучением людей безопасному использованию технологий для снижения/снижения риска стать жертвой преступлений.

Комплексное исследование киберпреступности.

<https://www.unodc.org/unodc/en/corruption/identity-related-crime.html>

РЕЗОЛЮЦИИ ЭКОСОС Резолюция ЭКОСОС 2004/26 Резолюция ЭКОСОС 2007/20 Резолюция ЭКОСОС 2009/22 Резолюция ЭКОСОС 2011/35 Резолюция ЭКОСОС 2013/39	 ОТЧЕТЫ О ВСТРЕЧАХ Отчет о первом совещании Отчет о втором совещании Отчет о третьем совещании Отчет о четвертом совещании Отчет о пятом совещании Отчет о шестом совещании https://www.unodc.org/unodc/en/corruption/identity-related-crime.html

Расширение возможностей подразделения кибербезопасности. Независимо от того, какому подразделению организации поручено обеспечение кибербезопасности, инспекторы подчеркивают, что важно обеспечить, чтобы соображения кибербезопасности могли без ограничений высказываться и учитываться ответственными лицами, принимающими решения.

	Организацией ОН подготовлены и предоставлены для ознакомления материалы доклада объединенной инспекционной группы, по теме: «Кибербезопасность в организациях системы Организации Объединенных Наций», при подготовке Хорхе Флорес Каллехас, Айши Айфифи, Николая Лозинского. (Женева, 2021) https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_russian.pdf



Эти задачи должны решаться там, где соответствующие сотрудники могут самостоятельно выходить на исполнительное руководство и вносить реальный вклад в деятельность других систем организации, таких как общеорганизационное управление рисками, управление информацией и знаниями, физическая охрана и безопасность, — мысль, которая проводится на протяжении всего доклада. Залогом этого служит наличие мощного внутреннего механизма управления с участием многих заинтересованных сторон, включая все соответствующие подразделения. Некоторые хорошо проработанные примеры таких многосторонних и многоуровневых механизмов управления были предоставлены ВОИС и ИКАО. [2]

3. Методические рекомендации по формированию полезных привычек в отношении кибербезопасности, кибергигиены, киберкультуры детей.

Методические рекомендации и информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников.

Методические рекомендации разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направленных на обучение учащихся правилам безопасного поведения в интернет-пространстве, профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность. [10]

В организациях образования необходимо проводить занятия для учащихся по основам информационной безопасности («основы медиабезопасности»); знакомить родителей с современными программно-техническими средствами (сетевыми фильтрами, программами «родительский контроль»), ограничивающими доступ детей и подростков к ресурсам сети Интернет, несовместимыми с задачами воспитания; проводить специальные мероприятия по вопросам информационной безопасности несовершеннолетних.

В качестве возможного варианта предоставления обучающимся соответствующих знаний может быть использована разработанная учебная программа «Интернет: возможности, компетенции, безопасность», разработанной специалистами факультета психологии МГУ им. М.В. Ломоносова, Федерального института развития образования и Фонда Развития Интернет, рекомендованная Министерством образования и науки РФ [11]

Содержательная часть и объем учебного курса может определяться индивидуально, в зависимости от потребностей конкретной общеобразовательной организации и учащихся. Обучение навыкам безопасного и эффективного использования интернет-ресурсов возможно в рамках учебного курса «Основы безопасности жизнедеятельности» и в рамках программ факультативов, кружков, элективных курсов, а также индивидуальных учебных планов, реализуемых образовательными организациями.

Вышеуказанные сетевые ресурсы могут быть использованы для проведения педсоветов в образовательных организациях по вопросам безопасности детей в сети Интернет.

В основной школе учащиеся активно начинают использовать Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайн-игры и так далее. Все более часто их любимым способом общения становится мгновенный обмен сообщениями. Для учащихся этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным.

Педагогам для обеспечения интернет-безопасности учащихся 10-15 лет необходимо:

- познакомить учащихся с ответственным, достойным поведением в Интернете;

- рассказать об основных опасностях и правилах безопасного использования сети Интернет;

- убедить никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете;

- объяснить опасность личных встреч с друзьями по Интернету без присутствия взрослых;

- убедить сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им.

- ознакомить с правилами поведения на форумах и чатах, убедить их, что они не должны использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

Организуя работу с учащимися старших классов по безопасному использованию информации в Интернете, следует обратить внимание на неформальные молодежные объединения, которые возникают в образовательной организации. Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее, участие взрослых тоже необходимо:

Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.

Интересуйтесь, какими чатами и досками объявлений пользуются подростки, и с кем они общаются. Поощряйте использование контролируемых (контролируемых) чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.

Настаивайте, чтобы подростки осторожно соглашались или не соглашались вовсе на личные встречи с друзьями из Интернета. Напоминайте, какие опасности это может за собой повлечь.

Убедите подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.

Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

Обсудите с подростками азартные сетевые игры и связанный с ними риск.

Результатами мероприятий по безопасному использованию Интернета могут стать как бумажные, так и электронные ресурсы, созданные учащимися:

рисунки, сочинения (рассказы, сказки, стихи), буклеты, презентации. Интересной формой представления результатов могут стать театрализованные выступления и видеофильмы учащихся.

Для учащихся старших классов при создании материалов по безопасности можно использовать сервисы Интернета для совместной деятельности. Работа команды учащихся в этом случае может проводиться дистанционно. Одним из примеров является схема «Безопасность детей в Интернете» [24]

Рекомендуем обратить внимание на создание условия для ознакомления с результатами творчества учащихся. Разработанные материалы можно размещать на сайте образовательной организации, в социальных сетях, блогах и сетевых сообществах.

Для эффективной профилактики интернет-зависимости, профилактики националистических проявлений в молодежной среде и устранения риска вовлечения подростков в противоправную деятельность педагогам необходимо проводить разъяснительную и консультационную работу с родителями учащихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в Интернет.

Возможно проведение бесед о работе учащихся в сети Интернет на классных и общешкольных родительских собраниях или при индивидуальных встречах; информирование через школьный сайт на страничке для родителей. На таких страничках можно разместить рекомендации по профилактике компьютерной зависимости у детей, по обеспечению безопасности детей в Интернете.

Эффективной мерой является установка на компьютер программного обеспечения с функциями «родительского контроля». Родителям можно порекомендовать установить на домашнем компьютере бесплатную программу «Интернет Цензор www.icensor.ru.

Родителям могут быть даны следующие рекомендации по формированию у учащихся навыков безопасного поведения в сети Интернет:

Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.

Научите детей не загружать программы, музыку или файлы без вашего разрешения.

Позволяйте заходить на детские сайты только с хорошей репутацией и контролируемым общением.

Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.

Приучите детей сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Единство родительских и педагогических усилий поможет оптимально использовать «плюсы» и нейтрализовать «минусы» работы с ресурсами всемирной Сети.

При сегодняшнем уровне развития телекоммуникационных и информационных технологий мы зачастую не имеем возможности оградить несовершеннолетних от негативной и вредной для них информации. Переизбыток жестокости и насилия в общедоступных источниках массовой информации может сформировать у них искаженную картину мира и неправильные, порой даже опасные, жизненные установки. Необходимо постоянно совершенствовать нормативные акты, направленного на защиту детей от разрушительного, травмирующего их психику информационного воздействия, а также от информации, способной развить в ребенке порочные наклонности, а также вводит запрет на информацию, вызывающую у детей страх, ужас и панику, а также оправдывающую насилие и противоправное поведение.

Методические рекомендации педагогам

по формированию информационной безопасности у детей и подростков

- Проводите работу по формированию информационной культуры у детей и подростков как одной из составляющих духовной культуры общества.

- Включайте в тематику родительских собраний, педагогического всеобуча темы: «Компьютер: добро или зло», «Информационная компетентность: отбор компьютерных сайтов и программ для детей».

- Знакомьте родителей с видами информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также с негативными последствиями распространения такой информации.

- Проводите медиа-уроки с целью привития обучающимся навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде («Защита прав детей в сети Интернет»).

- Формируйте психологическую, социальную, информационную компетентность детей с целью профилактики «ухода» ребёнка в интересы виртуального мира.

- Работайте над собственной информационной культурой с целью компетентного диалогического общения с учащимися.

- Обучайте родителей, детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях.

По формированию информационной безопасности детей, в работе на занятиях могут быть использованы следующие формы работы: лекции, беседы, тренинги, диспуты, дискуссии, кинолектории, интеллект-карты, исследования, театрализация, встречи с интересными людьми, выпуск газеты, телепередачи,

онлайн передачи, создание сайта, интернет практикум, онлайн игры и другие формы.

Психологические рекомендации родителям и педагогам

Родители и педагоги должны повышать уровень цифровой компетентности как важнейшего навыка XXI в., обеспечивающего не только эффективность использования интернета, но и его безопасность.

- Цифровую грамотность следует преподавать отдельным предметом (факультативом) в школьной программе, целью которой являлось бы обучение способам совладания с онлайн-рисками, в первую очередь кибер-агрессией.

- Необходимо разрабатывать специфические образовательные программы по повышению цифровой компетентности с опережающим эффектом и возможностями быстрой трансформации с учётом темпов развития новых технологий. Эффективность использования ИКТ в учебно-образовательном процессе предполагает высокий уровень цифровой компетентности у всех участников образовательного процесса.

- Родители и педагоги должны обучать активным и пассивным стратегиям совладания с кибербуллингом, таким как поиск социальной поддержки, дистанцирование и др.

- Родители создают правила и ограничения использования интернетом. Чрезмерное использование интернета следует рассматривать как отдельную онлайн-угрозу и чрезмерную информационную «нагрузку». Родители переживают достаточно обоснованные страхи, связанные с онлайн-рисками и их последствиями, например, дети могут стать жертвами сексуальных домогательств или жертвами кибер-агрессии в онлайн, страдают их социализация, дружба в реальном мире, они оставляют избыточную информацию о себе, режим медиа-многозначности оказывает негативное воздействие на их психику и познавательную деятельность.

- Родители должны постоянно проверять сайты, которые посещают их дети, его контакты, профили. Родители могут использовать технические ограничения в виде специальных программ, которые блокируют и фильтруют сайты или устанавливают ограничения во времени пользования интернет-ресурсами.

Общение на равных с продвинутыми в области интернет-технологий детьми и подростками возможно при условии владения достаточными «цифровыми» знаниями и умениями у родителей и педагогов, способных обеспечить безопасное использование интернет-ресурсов.

*Рекомендации для родителей обучающихся
по вопросам информационной безопасности.*

Стремительное развитие компьютерных технологий качественно меняет окружающую жизнь и порождает множество проблем, в частности, проблему формирования информационной культуры и безопасности среди старших подростков.

Существуют различные мнения о том, когда нужно давать детям доступ в Интернет. Зарубежные специалисты сходятся в том, что запрет на Интернет

может быть действенным только до тех пор, пока это не ограничивает потребности ребенка в сфере образования. Современные школы уже подключены к Интернет, и преподавание информатики начинается со второго класса. Почти каждый подросток имеет доступ к Интернет либо с домашнего компьютера, либо с сотового телефона. Компьютер и Интернет, как всякие сложные технологические продукты, наряду с неоспоримыми преимуществами могут нанести серьезный вред подростку. Одним из главных вопросов, связанных с компьютеризацией, является изучение влияния компьютера на организм, психическое состояние и развитие ребенка.

При современном уровне развития техники вредными для детей и, вообще, пользователей любых возрастов, являются скорее не излучения, а умственное и нервное переутомление.

Вот выдержка из аннотации к книге З. и Н. Некрасовых «Как оттащить ребенка от компьютера и что с ним делать», вышедшей в издательстве «София»: «Дети и подростки прирастают к розетке тогда, когда реальный мир не может предложить им других полноценных занятий. Не надо бороться с компьютером, борьба не укрепляет семьи. Надо просто понять истинные потребности своих детей и найти в себе силы и время общаться, играть, слушать их.

Просто посмотреть на все (в том числе и на компьютеры, ТВ, мобильник, плеер и прочие розеточные изобретения) глазами детей и подростков. И тогда виртуальный мир станет помощником вашей семье, для чего он, собственно, и предназначен».

Родители должны помнить, что ребенок проходит в своем психологическом развитии определенные стадии, которые достаточно сильно отличаются друг от друга. Это также отражается и на интересах детей при работе в Интернете. Родителям важно знать, какие особенности имеют дети в том или ином возрасте, для того чтобы правильно расставлять акценты внимания при своих беседах с детьми о правилах безопасности в Интернете.

Кроме того, нужно учитывать, что наши дети начинают осваивать Интернет в разном возрасте:

Кто-то в возрасте 14 – 17 лет, находясь в старших классах, кто-то в 10 – 13 лет, а кто-то еще в дошкольном возрасте получает первый опыт взаимодействия с Интернетом.

Подростки, как правило, проходят через период низкой самооценки; ищут поддержку у друзей и не охотно слушаются родителей, более старшие ищут свое место в мире и пытаются обрести собственную независимость; в то же время они охотно приобщаются к семейным ценностям.

В этом возрасте подростки уже полноценно общаются с окружающим миром. Они бурлят новыми мыслями и идеями, но испытывают недостаток жизненного опыта.

Родителям важно продолжать следить, как используют Интернет их дети в этом возрасте.

В этом возрасте дети уже слышаны о том, какая информация существует в Интернете. И совершенно нормально, что они хотят все это сами увидеть, услышать, прочесть. Доступ к нежелательным материалам (например, порнографическим картинкам или инструкциям по изготовлению взрывчатки) можно легко заблокировать при помощи программных фильтров.

Они скачивают музыку, пользуются электронной почтой, службами мгновенного обмена сообщениями и играют. Кроме того, подростки активно используют поисковые машины. Большинство пользовалось чатами, и многие общались в приватном режиме. Мальчики в этом возрасте склонны сметать все ограничения и жаждут грубого юмора, крови, азартных игр и картинок для взрослых. Девочкам больше нравится общаться в чатах; и юные дамы более чувствительны к сексуальным домогательствам в Интернете.

Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее участие взрослых тоже необходимо. Особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и ребенком. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Родители должны также помнить о необходимости хранить свои пароли в секрете, чтобы подростки не смогли зарегистрироваться под именем старших.

Взрослым важно помнить, что даже самые искушенные дети не видят опасностей Интернета и не осознают рисков его использования. Проблема заключается в том, что у детей еще не сформированы критерии различия. Ребенку, в силу особенностей его психологического развития, интересно все. Оставить ребенка один на один с компьютером в Интернете, это все равно, что бросить его одного на улице большого и незнакомого города. Когда ребенок часами сидит один за компьютером, происходит почти тоже самое скорее всего, он слоняется по виртуальным улицам и подворотням. Поэтому родители и педагоги, сначала сами должны научиться азам компьютерной безопасности, а потом научить этому своих детей. Для этого нужна хорошо продуманная методика обучения основам информационной безопасности.

Организация режима доступа к образовательным ресурсам Интернет:

- проведение инструктажей по доступу к образовательным ресурсам Интернет;
- установка программ-фильтров на школьные компьютеры (приложение 1.5);
- проведение лектория для родителей учащихся по режиму доступа детей к образовательным ресурсам (приложение 1.6);
- тесты и анкеты для родителей по изучению ИКТ компетенций школьников, а также для диагностики определения степени компьютерной зависимости подростков (приложение 1.2);
- памятки родителям (приложение 1.4);

1) Десять фактов, которые нужно сообщить детям ради безопасности в Интернет.

2) Памятка для родителей по безопасному использованию сети Интернет.

3) Рекомендации родителям по предупреждению компьютерной зависимости у ребенка.

4) Основные правила безопасности в сети Интернет для родителей.

5) Что делать, если ребенок столкнулся с какой-либо интернет угрозой?

6) Рекомендации родителям, с помощью которых можно всегда достойно выйти из ситуации, пользователя пытается донимать сетевой грубиян.

7) Цензура компьютерных игр.

8) Советы родителям по предупреждению развития компьютерной зависимости у детей.

9) Что делать, если Ваш ребенок стал потенциальной целью преступника?

10) Преступники в интернете: что можно сделать для снижения опасности?

11) Как сделать общение в интернете комфортным?

12) Советы по повышению безопасности участия Ваших детей в онлайн-играх

13) Как предостеречь детей от игр на деньги?

14) Как поступать, если дети столкнулись с грифферами?

● профилактика основных интернет-рисков (приложение 1.5)

Организация контроля использования ресурсов Интернета подростком в домашних условиях, с помощью программ Родительского контроля:

● ограничивать время, которое он проводит за экраном монитора,

● блокировать доступ к некоторым сайтам,

● блокировать доступ к другим интернет-сервисам,

● запрещать запуск некоторых игр и программ.

При среднем уровне защиты работает фильтр на сайты, посвященные оружию, наркотикам, разного рода непристойностям и содержащим нецензурную лексику.

Видеть в современной технике только добро или только зло это крайности, которых следует избегать. Техника всего лишь инструмент в человеческих руках, предназначенный для достижения тех или иных целей. И как при использовании любого инструмента, работа в Интернет требует определенной техники, а точнее культуры безопасности.

При всей важности технических средств, понятно, что они являются всего лишь частью осуществления политики информационной безопасности. Она включает воспитательные и образовательные мероприятия.

В проведении политики информационной безопасности школы принимают участие все заинтересованные в этом лица: педагоги, учащиеся, их родители. Документально политика использования ресурсов сети Интернет зафиксирована в «Правилах использования сети Интернет в муниципальном общеобразовательном учреждении».

В помощь классным руководителям для проведения классных часов и родительского лектория могут быть использованы:

- разработки классных часов по информационной безопасности (приложение 1.1, 1.6)

1. Родителям о безопасности детей во Всемирной паутине.
2. Правила безопасности и этикета в Интернете для подростка.
3. Информационные технологии как основа единого информационного пространства школы
4. Компьютер в жизни школьника.
5. Механизм обеспечения информационной безопасности учащихся в школе при использовании Интернета.
6. Информационная безопасность.
7. Безопасность в сети интернет.
8. Обеспечение информационной безопасности при работе с Интернет.
9. Информационная безопасность семьи и ребенка.
10. Актуальные проблемы безопасности образовательной среды: мониторинг как инструмент выявления проблемных зон.
11. Правила безопасности и этикета в Интернете для подростка.

Формирование информационной культуры и безопасности процесс длительный и сложный, но важный и необходимый. Интернет может быть и всемирной энциклопедией, объединяющей информационные ресурсы во всем мире. Но он может превратиться и в зловещую паутину, губящую людей, если люди будут искать в ней нечистоты и превращать ее во всемирную помойку. Задача взрослых (педагогов, родителей) формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности.

Возникает проблема: «Каким же образом решать задачу просвещения родителей в вопросах информационной безопасности?»

Во-первых, необходимы беседы о работе детей в сети Интернет, которые проводятся на заседаниях школьного «Родительского лектория», на классных и общешкольных родительских собраниях.

Мы понимаем, что родителям часто бывает сложно контролировать своих детей, т.к. дети уже знают гораздо больше их, поэтому советуем начинать воспитание информационной культуры с раннего возраста.

Во-вторых, в каждой школе создан школьный сайт или блог, где открыта страничка для родителей с размещенными рекомендациями, сводящимися к простым и очевидным правилам, советам, рекомендациям. На страницах сайта, родительских собраниях необходимо организовать «ликбез» с целью повышения компьютерной грамотности родителей, познакомить с проблемами, которые могут возникнуть при работе на компьютере. Тематика вопросов может быть такова:

1. Что дети должны знать о вредоносных и нежелательных программах в интернете?
2. Что такое вирус?

3. Что такое нежелательное программное обеспечение? Как можно определить, что ваш компьютер заражен? Как снизить риск заражения?

4. Повышение уровня безопасности компьютера.

Кто как не родители смогут обеспечить и проконтролировать безопасность информационной среды у своих детей, которые владеют компьютером значительно лучше их самих?

Поэтому вторым направлением работы с родителями является их знакомство с возможными интернет-рисками и их профилактикой (приложение 5).

Сюда можно отнести вопросы:

1. Онлайновое пиратство у себя дома и как его предотвратить.

2. Безопасное общение детей в интернете.

3. В чем состоит общение детей в чатах и системах обмена мгновенными сообщениями

4. Кибермошенничество. Как его предупредить?

5. Кибербуллинг. Как справиться с кибербуллингом?

6. Предупреждение встреч с незнакомцами и грумингом.

7. Рекомендации по предупреждению.

При этом мы рекомендуем соблюдать родителям ряд правил:

Первое правило – это внимательное отношение к действиям своих детей в Интернете. Мы советуем родителям активно участвовать в общении ребёнка с Интернетом, особенно на этапе освоения, и не отправлять его в «свободное плавание» по Интернету. Родители должны обязательно следить за контактами детей в Сети и знакомиться с сайтами, которые они посещают.

Второе важное правило постоянное напоминание подросткам о возможностях и опасностях работы с ресурсами Интернет. Родителям необходимо объяснять своему ребёнку, что если он столкнулся с негативом или насилием со стороны другого пользователя, то обязательно должен сообщить об этом близким людям. Важно контролировать трату денежных средств при скачивании платной информации и получению платных услуг, особенно путём отправки денег. Мы рекомендуем родителям сформировать список полезных, интересных и безопасных ресурсов, которыми могут пользоваться подростки

Третье правило для родителей – контроль за работой детей в Интернете. Эффективной мерой является установка на компьютер программного обеспечения с функциями «родительского контроля».

Повышение своего уровня компьютерной грамотности – одно из главных правил для родителей, которым небезразлична информационная безопасность их детей.

Соблюдение этих простых и в то же время эффективных правил позволит родителям защитить своих детей от сетевых угроз и сделать пользование Интернет ресурсами максимально полезным. Единство родительских и педагогических усилий поможет нам оптимально использовать «плюсы» и нейтрализовать «минусы» работы с ресурсами всемирной Сети.

Приложения 1.1-1.6 включают материалы, необходимые для организации рекомендуемого вида деятельности. Данные приложения помогут:

- педагогам грамотно организовать мероприятия, направленные на формирование у родителей ответственного отношения к информационной безопасности детей;

- оформить стенды в образовательном учреждении по информационной безопасности для различных возрастных категорий (родители, старшие подростки);

- родителям оценить степень компьютерной зависимости своего ребенка, уровень своих знаний по информационной безопасности, овладеть опытом контроля деятельности детей в Интернете, правильно реагировать на возникшие проблемы и грамотно предупреждать их появление в дальнейшем.

Приложение 1.1 Разработки родительских собраний

Приложение 1.2 Тестовые задания, анкеты для родителей

Приложение 1.3. Методики создания практических заданий, адресованных родителям

Приложение 1.4. Памятки и советы родителям

Приложение 1.5. Профилактика основных интернет-рисков и борьба с ними

Приложение 1.6. Примерная тематика открытых мероприятий

Для педагогов.

- Мероприятия с родителями по основам информационной безопасности детей в сети Интернет

1) С периодичностью не реже 1 раз в учебный год необходимо проводить общешкольное и/или классные тематические родительские собрания, посвящённые вопросам информационной безопасности детей в сети Интернет (по возможности с участием специалистов в области компьютерной коммуникации).

2) Классным руководителям необходимо проводить в рамках родительских собраний семинары по обмену опытом обеспечения безопасности ребенка в информационном обществе. Формы проведения родительского всеобуча на тему детской безопасности в Интернет могут включать:

- общешкольные и классные родительские собрания на тему «Возможности и опасности ребенка в Интернете»;

- практические занятия по повышению уровня безопасности детей в Интернете при помощи технических и технологических средств;

- информирование по данной проблеме на страницах сайтов образовательного учреждения;

- выпуск и распространение информационных буклетов по проблеме безопасности детей в Интернете;

- семинары для родителей по обмену опытом обеспечения безопасности ребенка в информационном обществе

- участие родителей в Неделе безопасности в Интернете (<http://ipk.68edu.ru/docs/bezopasnostdeti/nedelyainternet.pdf>).

Приложение 1.1

Разработки родительских собраний.

Родительское собрание № 1. «Родителям о безопасности детей во Всемирной паутине». (<http://nsportal.ru/shkola/materialydl yaroditelei/library/roditelskoesobranieroditelyamobezopasnostideteyvo>)

Цель: Формирование ответственного отношения по обеспечению безопасности детей при работе в сети Интернет.

Задачи:

1. Создать условия для знакомства с возможностями, открываемыми цифровыми технологиями и глобальной сетью Интернет по обеспечению безопасного использования детьми ресурсов Интернета.

3. Расширение информационного поля родителей о влиянии интернета на здоровье и безопасность ребёнка. [26]

Приёмы технологии критического мышления:

Верные и неверные утверждения; таблицы: ПМИ; резюме.

Предварительная работа:

Поиск материала об использовании ресурсов сети Интернет детьми;

Анкетирование учащихся.

Организация:

1) родители сидят за столами, перед ними лежит бумага, ручки;

2) объявляется тема родительского собрания;

3) учитель предлагает заполнить анкету.

Стадия вызова.

Перед каждым из родителей лежит лист с фактами о пребывании детей в Интернет. Готовится классным руководителем перед родительским собранием. Достаточно 5-7 высказываний. Пример:

1. школьники класса все зарегистрированы в Тик Ток?

2. Все дети обмениваются короткими сообщениями; (Смотрит мультики, видео; слушает музыку; размещает фотографии, видео; знакомится, дружат, и т.д.)

3. 75% юных Интернет пользователей выходят в сеть самостоятельно;

4. 88% двухлетние выходят в сеть вместе с родителями, а к 14 годам совместное использование сетью сохраняется лишь для 7% ребят.

5. 100% родителей разрешают своим детям путешествовать по Всемирной паутине.

6. Путешествия по сети Интернет оказывают положительное влияние на успехи ребёнка.

7. Путешествия по сети Интернет оказывают положительное влияние на здоровье ребёнка.

8. 93% родителей не применяют никаких мер для повышения безопасности при посещении детьми сети Интернет.

9. Основная часть родителей не знает какие угрозы подстерегают детей наиболее часто при посещении Интернета.

10. Большинство родителей считают, что наиболее эффективным способом защиты детей от Интернет-угроз являются специализированные системы фильтрации контента и наблюдение взрослых.

Стадия содержания.

1. Классный руководитель демонстрирует презентацию «Результаты школьных исследований «Дети в Интернете и родители»», «Обеспечение безопасности детей при работе в Интернет» (Приложение 1.2). В ходе просмотра родители заполняют вторую колонку таблицы и сверяют её с первой.

2. Родителями заполняется таблица ПМИ: что хорошего, негативного в использовании детьми сети Интернет и что показалось интересным.

Плюсы Минусы Интересно

Родителям предлагается высказаться, затем раздаются результаты детских анкет (Приложение 1.1).

Родители сверяют свои результаты и ответы своего ребёнка.

Стадия рефлексии.

В конце родительского собрания предлагается написать родителям краткий вывод (приём резюме). Я понял, что ...

Меня удивило, что ...

Меня заинтересовало, что ...

Все выводы проговариваются вслух. Затем родителям раздаются буклеты (приложения 1.3) которые предлагается прочитать и обсудить вместе с детьми, поместить рядом с компьютером ребёнка.

Родительское собрание № 2.

Правила безопасности и этикета в Интернете для подростка.

Задачи:

Показать родителям важность и значимость проблемы формирования сетевого этикета у подростка.

Рассказать родителям о правилах общения в Интернете. Ознакомить родителей с источниками информации по проблеме безопасности ребенка в Интернете.

Вопросы обсуждения: статистика и цифры о роли Интернета в жизни школьников. Влияние Интернет - общения на формирование личности ребенка.

Подготовительная работа:

Анкетирование учащихся, подготовка статистики. Подготовка шаблонов.

Оформление на доске.

Ход собрания:

Вступительное слово классного руководителя.

Интернет - общение в жизни ребенка — это хорошо или плохо? Сколько и как должен общаться ребенок в Интернете? Нужно ли ограничивать общение детей в сети? Важно ли прививать этические понятия ребенку по отношению к общению в Интернете? На эти и другие вопросы мы постараемся ответить.

Обратимся к статистике. Результат анкеты учащихся и родителей класса. Учитель знакомит с результатами анкетирования родителей и учеников.
Анкета для родителей.

ФИО родителя. класса в котором учится ребенок.

1. Есть ли у вашего ребенка сотовый телефон? Да. Нет
2. Есть ли в нем Интернете. Да. Нет
3. Сколько времени ребенок проводит за телефоном?
4. Какие средства для общения в Интернете Вы знаете.
5. Общается ли в Интернете ваш ребенок с друзьями? Да. Нет
6. Какими средствами общения в Интернете пользуется ребенок.
7. Посещает ли ребенок социальные сети?
8. Какие вы знаете сети, которые посещает ваш ребенок?
9. Есть ли у ребенка блог или живой журнал? Да. Нет.
10. Посылает ли ребенок сообщения в чаты? Да. нет.
11. Говорите ли вы с ребенком о правилах поведения в чатах? Да. Нет.
12. Говорите ли вы с ребенком об опасностях в Интернете? Да. Нет.

Анкета учащегося. (проводится и анализируется до собрания)

Фамилия Имя _____ Класс _____

1. Есть у тебя сотовый телефон?
2. Подключен ли Интернет?
3. Сколько времени проводишь в телефоне?
4. Какие средства для общения в Интернете ты знаешь?
5. Общаешься ли в Интернете с друзьями?
6. Какими средствами общения в Интернете ты пользуешься?
7. Посещаешь ли социальные сети?
8. Есть ли у тебя любимые социальные сети или сайты?
9. Часто ли общаешься в чатах?
10. Знаешь ли ты правила этикета в Интернете?
11. Какие опасности могут подстерегать тебя в Интернете?
12. Разговаривал ли ты с родителями о правилах поведения в сети?

Анализ анкет. Постановка проблемы.

Анализ анкеты детей и родителей показал результаты.....

В связи с тем, что дети

В связи с тем, что родители.....

Необходимо.....

Поговорить об опасностях в Интернете, которые подстерегают ребенка.

По материалам Компьютерной газеты мы можем узнать о проблеме безопасности детей в сети.

«Уже давно для многих Интернет стал жизненно необходимой вещью, без которой человек не представляет своей жизни. Мы глубоко погрузились в его просторы и отказаться от этого изобретения человечества многим просто не под силу, особенно если эти многие — дети. Специфика человеческой психики такова, что мы быстро привыкаем к новой среде, в которой комфортно себя

чувствуем, когда это происходит быстро и комфортно, то не замечаем как вообще в нее попали.

Проблема защиты детей в Сети находит самый широкий резонанс и это не случайно. Согласно последней СТАТИСТИКЕ:

- около 70 % детей выходят в Сеть без контроля взрослых:
- 68% из вышедших в Интернет детей «серфят» в поисках интересных фактов:

- 19% детей иногда посещают порносайты, еще 9% делают это регулярно. 38% детей, просматривают страницы о насилии, 16% детей просматривают страницы с расистским содержанием, 26% детей участвуют в чатах о сексе.

- 25% пятилетних детей активно используют Интернет. В 2020 году 32 % пятилетних детей свободно пользуются Интернетом. Эта цифра достигает 75% среди детей возраста 15–17 лет.

Данные, собранные в результате опроса «Использование компьютера и Интернета детьми и подростками в 2020 году», проведенного департаментом образования США показывают, что дети начинают пользоваться Интернетом в самом раннем возрасте.

- Дети опережают взрослых по количеству времени, которое они проводят в Интернете.

- Дети в возрасте между 7 и 10 годами составляют половину общего числа пользователей Интернета. Большинство из них выходит в Сеть из дома и самыми частыми их занятиями являются онлайн-игры.

- 44% детей один раз подвергались сексуальным домогательствам в Интернете. 11% подверглись им несколько раз.

- 14.5% детей, принявших участие в опросе, назначали встречи с незнакомцами через Интернет, 10% из них ходили на встречи в одиночку, а 7% никому не сообщили, что с кем-то встречаются.

Как воспитывать своего ребенка в контексте интернет-безопасности — дело каждого, иногда достаточно просто строгого слова родителя. Тем не менее, сам факт существования руководств, говорит об актуальности темы и ее крайней значимости. (памятки для родителей о информационной безопасности)

Одной из проблем современных пользователей является соблюдение этикета, или сетикета.

Давайте остановимся на понятиях: этикет, сетикет (сетевой этикет)

Этикет (от франц. Etiquette этикетка, надпись, впервые появившаяся при дворе Людовика 14) этикет (не писанные), общепринятые правила поведения в обществе.

Сетикет, нетикет (неологизм, является слиянием слов «сеть» (англ. net) и «этикет») правила поведения, общения в Сети, традиции и культура интернет-сообщества, которых придерживаются большинство. Это понятие появилось в середине 80х годов XX века в эхо конференциях сети FIDO.

Для того чтобы разработать свои практические рекомендации для родителей и детей необходимо объединиться в творческие группы.

Работа в творческих группах.

Первая группа.

Цель: Разработка принципов ведения диалога в сети.

Родителям выдается шаблон таблицы и отдельные модули карточки.

Родители распределяют по теме все модули и карточки с народной мудростью. Получают готовую карту «Принципов ведения диалога в сети»

Сетевой этикет – новое понятие. Интернет развивается и расширяется, все больше людей общается в сети. Начиная общаться в блогах друг с другом, они допускают множество незаметных на первый взгляд ошибок. Эти ошибки могут доставить неприятности собеседникам в сети. Избежать этих ошибок помогут несколько советов. С принципами необходимо познакомить детей.

Перед началом ведения дискуссии в сети следует усвоить некоторые принципы ведения диалога в блоге, форуме, чате...

Принцип вежливого тона: «Вежливость ничего не стоит, но приносит многое»

В ходе общения в сети очень важно обратиться к партнёру по имени как можно непринуждённое, давая понять, что его имя для вас много значит.

Принцип внимания. «Понимай самого себя и уважай другого» Важное условие успешного ведения беседы в сети исключительное внимание к собеседнику.

Ещё лучше сопровождать диалог в сети фразами: «Да!», «Понимаю тебя...», «Спасибо, это интересно...», «Приятно это читать...» и т.д.

Такая реакция является приглашением высказаться свободно и непринуждённо. Она помогает выразить одобрение, интерес, понимание. Можно проявить стремление получить дополнительные факты и прояснить позицию человека: «Пожалуйста, уточните это...», «Не можете ли ещё раз подробнее, укажите источники?», «Не объясните ли вы это?». Помогают сближению следующие фразы: «Как я понял тебя...», «Ты можешь поправить меня, если я ошибаюсь...», «Другими словами...» и т.д.

Принцип рациональности. Необходимо в ходе диалога в сети вести себя «Лучше одно слово, чем девять» сдержанно, если даже собеседник проявляет эмоции. Неконтролируемые эмоции отрицательно сказываются на процессе общения в сети.

Принцип понимания. «Мир силен не оружием, а людьми доброй воли.» Постарайтесь понять собеседника в сети. Невнимание к его точке зрения ограничивает возможность выработки различных точек зрения на один вопрос.

Принцип общения. «Обдумывай хоть неделю, но скажи ясно.» Если постоянные читатели не вступает в дискуссию в сети, привлечите его внимание интересной темой.

Принцип отказа от поучительного тона. «Доброе слово железные ворота отперет» Не старайтесь поучать. Будьте открыты для аргументов и постарайтесь убедить собеседника в необходимости информации.

Принцип разграничения между собеседником и предметом разговора. «Зла за зло не воздавай», необходимо вникать в проблему, а не выяснять отношения друг с другом.

Вторая группа.

Цель: Знакомство с Правилами этикета при общении и переписке в чатах или по электронной почте. Подготовка рекомендаций для родителей и детей по источнику сайт: «Этикет от А до Я» [27]. В этом документе описываются простые правила этикета при общении пользователей по электронной почте.

Адреса и персональные имена.

Персональное имя (не то же самое, что подпись) произвольная строка, которую многие мэйлеры (программы электронной почты) позволяют присоединять к вашим сообщениям в качестве текстового комментария.

- Если ваша система позволяет, всегда пишите персональное имя: оно является для вас лучшей «визитной карточкой», чем адрес e-mail

- Используйте осмысленные имена. Выражения типа «догадайся сам» не только мешают определить автора письма, но и оскорбляют интеллект адресата

- Если ваша почтовая система позволяет отправлять письма вместе с именами адресатов, используйте эту возможность. Таким образом, администратору сети будет легче найти адресата по имени, если сам адрес окажется ошибочным.

Пример: адрес 344188@foo.chaos.com содержит меньше информации, чем 344188@foo.chaos.com (Ford Prefect).

Тема письма (Subject)

- Длина, содержание и формат письма. Не забывайте давать названия своим письмам. Практически все мэйлеры позволяют присваивать почтовым сообщениям названия, и часто пользователь ориентируется именно по названиям, когда просматривает свою почту.

- Избегайте бессмысленных названий. Например, отправляя письмо службе технической поддержки Word Perfect, не следует называть его Word Perfess тем же успехом вы могли бы вообще ничего не писать.

- Если вы при ответе на письмо меняете тему разговора, не забудьте изменить и название

- Точный заголовок самый простой способ определить тему беседы, и если вы измените тему, оставив заголовок прежним, адресат может прийти в замешательство.

- Старайтесь, чтобы длина вашего письма отвечала стилю беседы: если вы просто отвечаете на вопрос, делайте это кратко и по существу.

- Держитесь как можно ближе к теме. Если вы хотите поговорить о чем-то новом, лучше послать отдельное письмо. Тогда ваш адресат сможет хранить его отдельно.

Ответы.

- Не пишите весь текст заглавными буквами, его становится тяжело читать (хотя краткое выделение может использоваться как усиление).

Старайтесь разбивать ваше письмо на логические абзацы и избегайте чрезмерно длинных предложений.

- Старайтесь не допускать грамматических ошибок. Полное ошибок и опечаток письмо трудно читать.

То, что электронная почта быстрый способ связи, вовсе не означает, что можно расслабиться и забыть о правописании (по моему опыту, самое безграмотное сообщение электронное).

Если вы считаете свои мысли достойными изложения в письме, позаботьтесь, чтобы они были изложены правильно

- Избегайте публичных флэймов писем, составленных под влиянием эмоций. Послания, отправленные в момент душевных переживаний, чаще всего только ухудшают ситуацию. Возможно, позже вы будете раскаиваться в своих словах, поэтому перед тем как начать «флэймовую войну», спокойно обдумайте положение. (Попробуйте сварить себе кофе удивительно, как быстро улягутся ваши эмоции с помощью чашечки хорошего кофе.)

- Если ваш мэйлер поддерживает различные параметры оформления текста (жирный шрифт, курсив и т.д.), убедитесь, что мэйлер адресата обладает такими же возможностями. К тому времени, как был составлен этот документ, большинство программ электронной почты в Internet могли работать только с текстом, хотя ситуация, конечно, изменяется.

- Трижды подумайте перед тем, как включать номер вашей кредитной карточки в свои электронные письма. Электронную почту могут перехватить, и ваш счет в банке подвергнется опасности

- Включайте в ваше послание отрывки письма, на которое отвечаете. Помните, электронная почта не разговор по телефону в реальном времени, и ваш адресат может забыть содержание предыдущего письма (особенно, если он ведет активную переписку). Включайте отрывки оригинального текста в ваш ответ, и адресат легче поймет, о чем идет речь

- Не переусердствуйте в цитировании предыдущих посланий. Очень неприятно получать обратно собственное письмо на пяти страницах (в качестве комментария) с маленькой припиской типа "я согласен" в конце. Отделяйте каким-то образом текст вашего послания от текста цитируемых писем, тогда ваш ответ будет легче читаться. Обычно используется для этих целей знак >, хотя это и не единственный вариант.

- Старайтесь не смешивать в своем послании информацию общего и личного характера

- Спросите себя: так ли уж необходим ваш ответ. Например, если вы получили письмо в результате веерной рассылки, вряд ли стоит извещать каждого из адресатов о своем отношении к нему лучше послать письмо непосредственно автору.

Подписи

Подпись небольшой текстовый отрывок в конце сообщения, обычно содержит информацию о контактах.

Большинство мэйлеров могут автоматически "приклеивать" подпись к исходящим сообщениям.

- Если можете, используйте подпись. Она должна идентифицировать вас и содержать данные об альтернативных каналах связи (обычный телефон, факс). На многих системах, в частности, тех, где почта проходит через шлюзы, ваша подпись может быть единственным идентификатором.

- Делайте свою подпись покороче строчек вполне достаточно. Неоправданно длинные подписи загружают каналы связи

- Некоторые мэйлеры позволяют добавлять случайные строки к вашей подписи: будьте с этим аккуратнее. В любом случае помните

- Краткость сестра таланта. Цитата на сотни слов из «Критики чистого разума» Канта в качестве подписи вряд ли порадует ваших адресатов

- консультант вряд ли сможет вам помочь ему для этого просто не хватит для этого информации

- Изменяющиеся подписи лучше всего смотрятся, если носят шуточный характер. Высказывания на политическую тему, например, могут расстроить некоторых людей, в то время как короткая шутка только поднимает настроение.

Простые правила вежливости

Электронная почта средство связи между людьми, и без правил вежливости здесь не обойтись.

- Если вы обращаетесь к кому-либо с просьбой, не забудьте сказать «пожалуйста». В то же время, если Кто-то помогает вам, никогда не вредно сказать «спасибо». Хотя это может показаться банальным, вы будете удивлены тем, какое количество людей являются образцами вежливости в реальной жизни и словно забывают о своих манерах в переписке по e-mail.

- Не ждите, что вам ответят немедленно. Тот факт, что вы в течение десяти минут не получили ответа на свой вопрос, вовсе не означает, что адресат вас игнорирует

- Помните, что не существует надежной почтовой системы. Неразумно помещать очень личную информацию в электронное письмо, если только вы не собираетесь его зашифровать с помощью надежной программы шифрования. Помните об адресате. Вы не единственный человек, который пострадает в случае, если деликатное сообщение попадет в плохие руки;

- Включайте в свое письмо полную информацию по теме, особенно, если рассчитываете на квалифицированный ответ. Например, если вы посылаете сообщение «Программа электронных таблиц не работает» в службу технической поддержки компании «Lotus».

Хотя электронная почта похожа на разговор в реальном времени, она лишена возможности жестикულიции.

Для решения этой проблемы в Internet используются "смайлики" последовательности ASCII символов, которые напоминают лицо, если смотреть на них, повернув голову набок.

Чаще всего применяют такие "смайлики": :) или :)улыбка; обычно используется для выражения радости, удовольствия (иногда встречается \ или \

«усмешка»). :(или :((несчастное лицо; выражает сожаление или разочарование. ;) или ;) подмигивающее лицо; обычно выражает иронию и означает, что слова не следует понимать слишком буквально.

Существуют сотни различных «смайликов», одни используются чаще, другие реже.

Правильное использование «смайликов» способно придать вашему письму живой характер и даже заменить жестикуляцию. Однако, не переусердствуйте.

И наконец...

Помните, что e-mail средство связи с живыми людьми. Перед тем, как послать письмо, прочтите его внимательно еще раз и поставьте себя на место получателя.

Третья группа

Цель: Разработать Соглашение о кодексе поведения в Интернете.

Примерный шаблон (по материалам сайта: Microsoft <http://www.microsoft.com/rus/protect/athome/children/famwebrules.msp>)

Соглашение

Я ФИО _____ обязуюсь:

Обращаться к моим родителям, чтобы узнать правила пользования Интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в интернете (____ минут или ____ часов).

Никогда не выдавать...

Всегда немедленно сообщать родителям...

Никогда не соглашаться...

Никогда никому, кроме своих родителей, не выдавать...

Вести себя в интернете правильно и не делать...

Никогда не загружать, не устанавливать и не...

Никогда не делать без разрешения родителей...

Сообщить моим родителям мое....

Я ФИО _____ обязуюсь:

Обращаться к моим родителям, чтобы узнать правила пользования Интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в интернете (____ минут или ____ часов).

Никогда не выдавать без разрешения родителей личную информацию: домашний адрес, номер телефона, рабочий адрес или номер телефона родителей, номера кредитных карточек или название и расположение моей школы.

Всегда немедленно сообщать родителям, если я увижу или получу в интернете что-либо тревожащее меня или угрожающее мне; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в интернете.

Никогда не соглашаться лично встретиться с человеком, с которым я познакомился в Интернете, без разрешения родителей. Никогда никому, кроме своих родителей, не выдавать пароли интернета (даже лучшим друзьям).

Вести себя в интернете правильно и не делать ничего, что может обидеть или разозлить других людей или противоречит закону.

Никогда не загружать, не устанавливать и не копировать ничего с дисков или из Интернета без должного разрешения.

Никогда не делать без разрешения родителей в интернете ничего, требующего платы.

Сообщить моим родителям мое регистрационное имя в Интернете и имена в чате, перечисленные ниже:

Имя (ребенок) _____ Дата _____

Родитель или законный представитель _____ Дата _____

Представление группами результата.

1. Принципы ведения диалога в сети.

2. Правила этикета при общении по электронной почте.

3. Соглашение о кодексе поведения в Интернете.

Подведение итогов. Собрание заканчивается высказываниями детей на тему: «Интернет для меня это....» и выводами родителей: «Мы должны с детьми говорить на тему безопасности и этикета в Интернете...» [28, 29, 30, 31, 32]

Родительское собрание № 3.

Материалы для проведения родительского собрания

«Информационные технологии как основа открытого информационного пространства школы»

Анкета для родителей № 1.

Уважаемые родители! В школе информационные технологии применяются в различных направлениях: учебная деятельность (урочная и внеклассная), воспитательная (классные часы и различные школьные мероприятия), ИКТ являются основой единого информационного пространства школы (администрация школы, педагог, обучающийся, родитель) сайт школы, работа «Кунделик» - электронного журнала, учебно материальная база школы, цифровые образовательные ресурсы и т.п. В том числе, информационные технологии прочно вошли в деятельность и досуг детей. Просим Вас ответить на несколько вопросов. (Все вопросы не являются обязательными для ответа. Если Вы выбираете «другое» не забудьте поставить напротив галочку, по возможности написать ответ).

1. В каком классе учится Ваш ребенок?_

2. Отношение к внедрению ИТ в образование. (Внедрение информационных технологий (ИТ) в образование относится к числу крупномасштабных инноваций, пришедших в российскую школу в последние десятилетия. Среди ИТ, внедряемых в сфере образования, можно выделить следующие: обучающие, тренажеры, справочные, единые информационными образовательные пространства (сайт школы, дистанционное обучение, электронные дневники), техническое обеспечение кабинетов и др.)

● скорее положительно

● скорее отрицательно (не вижу необходимости)

Другое: _____

3. Информационные технологии и обучение

- в школе проводятся различные мероприятия с применением информационных технологий (проектная деятельность, уроки, классные часы и родительские собрания).

- урок, с применением новых информационных технологий более популярен у моего ребенка (более интересен, понятен и т.п. со слов ребенка)

- ребенок с интересом и удовольствием выполняет проекты (рефераты, доклады), используя Компьютер

- ребенок готовится к уроку, используя компьютер (Интернет, полезные ссылки на сайте школы, рекомендуемые учителем сайты и т.п.)

- классный руководитель проводит родительские собрания с использованием компьютера

Другое: _____

4. Работа Электронного журнала «Кунделик». (Одной из возможностей ресурса является просмотр на страницах этого ресурса в Интернете оценок учащегося, которые выставляют учителя на уроках и их комментарии, домашнее задание... (пароль доступа индивидуален для каждого пользователя))

- в нашем классе есть «Электронный журнал», его работа очень важна для нас;

- в нашем классе есть «Электронный журнал», но в его работе нет необходимости;

- возможности «Электронного журнала» очень важные, но в нашем классе он не работает и думаю, что нет в нем необходимости,

Другое: _____

5. Посещение Школьного сайта

- часто посещаем (в том числе раздел Новости)

- очень редко посещаем

- не посещаем

Другое: _____

6. Школьный сайт. Напишите, пожалуйста, что бы Вы хотели бы изменить в работе сайта.

7. Есть ли у Вас дома компьютер?

- да (один)

- да (несколько)

- нет

Другое: _____

8. Кто пользуется компьютером у Вас дома?

- только родители

- только ребенок

- все члены семьи (родители и дети)

Примерный список вопросов, которые планируется обсудить на родительском собрании

1. В каком возрасте следует разрешить детям посещение интернета?

2. Следует ли разрешать детям иметь собственные учетные записи электронной почты?

3. Какими внутрисемейными правилами следует руководствоваться при использовании интернета?

4. Как дети могут обезопасить себя при пользовании службами мгновенных сообщений?

5. Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями?

6. Могут ли дети стать интернет-зависимыми?

7. Что должны знать дети о компьютерных вирусах?

8. Как проследить какие сайты посещают дети в интернете?

9. Что следует предпринять, если моего ребенка преследуют в интернете?

10. Помогает ли фильтрующее программное обеспечение?

11. На какие положения политики конфиденциальности детского сайта нужно обращать внимание?

12. Какие угрозы встречаются наиболее часто?

13. Как научить детей отличать правду от лжи в Интернет?

Анкета для родителей №2

1. Имеете ли вы компьютер?

2. Сколько времени проводит ваш ребенок за компьютером?

3. С какой целью он использует компьютер?

1) подготовка к урокам

2) поиск внеучебной информации (музыка, фильмы ...)

3) общение

4) чтение книг

5) компьютерные игры

4. В какие игры играет Ваш ребенок?

5. Какие сайты посещает Ваш ребенок?

6. Боитесь ли Вы общения вашего ребенка с компьютером?

7. Изменилось ли поведение вашего ребенка после того, как он стал активно общаться с компьютером?

8. Как вы относитесь к увлечению детей компьютерными играми?

9. Посещает ли ваш ребенок компьютерный клуб?

10. Вызывает ли у вас это тревогу?

11. Считаете ли вы необходимым использование компьютера на школьных уроках по различным предметам?

12. Как Вы считаете: КОМПЬЮТЕР ЭТО:

1) друг

2) враг

3) свой вариант ответа

Приложение 1.2.

Тестовые задания, анкеты для родителей

Тест №1. «Определение зависимости подростков от компьютерных игр»
(А.В. Котлярова).

Отметьте утверждение, которое соответствует поведению Вашего ребенка

Утверждение да или нет

1. Ребенок испытывает затруднения, грустит, раздражается при необходимости закончить игру;

2. Ради компьютерной игры ребенок жертвует временем проведением с семьей, друзьями;

3. Ребенок преимущественно находится в хорошем настроении, занимаясь компьютерными играми;

4. Из-за компьютерной игры ребенок пренебрегает сном;

5. Игра за компьютером главное средство для снятия стресса ребенка;

6. После игры за компьютером у ребенка возникают головные боли;

7. В обычной жизни ребенок испытывает пустоту, раздраженность, подавленность, которые исчезают при игре за компьютером;

8. При помощи игры на компьютере ребенок решает жизненные проблемы, достигает жизненных целей;

9. После компьютерной игры у ребенка возникает нарушение аппетита, стула;

10. Из-за компьютерной игры у ребенка возникают проблемы с учебой, но он продолжает в нее играть;

11. Из-за компьютерной игры ребенок пренебрегает питанием;

12. Ребенок испытывает потребность проводить за игрой все больше времени;

13. Из-за компьютерной игры ребенок пренебрегает гигиеной;

14. Во время игры ребенок полностью отрешается от действительности, целиком переносясь в мир игры;

15. После компьютерной игры у ребенка возникает сухость слизистой оболочки глаз;

16. Из-за компьютерной игры у ребенка появляются проблемы в семье, отношениях с людьми, но он продолжает играть;

17. Игра за компьютером служит ведущим средством для достижения комфортного состояния ребенка;

Анализ обработки анкеты: За каждый ответ «да» начисляется 1 балл. Если сумма выбранных ответов составляет более трех баллов, то велика вероятность того, что увлечение вашего ребенка компьютерными играми может перерасти в зависимость.

Тест №2 для родителей на наличие игровой интернет - зависимости их ребёнка.

Поставьте один балл за каждый вопрос, на который вы ответили положительно.

Вопросы:

1. Много ли времени ребенок проводит за компьютером, игровой панелью, планшетом, карманным персональным компьютером, смартфоном, играя в компьютерные игры?

2. Легко ли он прекращает игру по вашему требованию?
3. Часто ли бывают ситуации, когда ребенок прячется от вас и играет в компьютерные игры?
4. Часто ли он рассказывает вам о персонажах из компьютерных игр и игровых ситуациях?
5. Часто ли ребенок с друзьями обсуждает игровые ситуации?
6. Изменился ли резко его внешний вид, одежда?
7. Появились ли у него странные и нетипичные предметы: меч, плащ, необычные аксессуары, обувь?
8. Просит ли он у вас обновить компьютер? Сделать его мощнее, быстрее?
9. Просит ли ребенок деньги на игры или на непонятные вам цели?
- 10.. Изменились ли резко его привычки?

Если сумма баллов дает больше 5, то вам надо обратить внимание на возможную игровую зависимость вашего ребенка.

Тест №3 «Проверка степени компьютерной зависимости ребенка»

К ребенку, увлеченному игрой, обращается родитель с просьбой о помощи. И для ориентировки в степени «застревания» ребенка в компьютере необходимо пройти уровни обращения:

1-й уровень. Просьба формулируется просто, например “Сынок, помоги, пожалуйста, подвинуть кресло”.

Способы реагирования:

А. Ребенок легко откликается на просьбу, помогает, может увлечься этой помощью, переключиться на другое дело, отвлечься, забыть о компьютере. Такое поведение полную свободу от компьютера на момент тестирования.

Б. Ребенок откликается со второго - третьего раза, демонстрирует недовольство, огрызается, такая реакция может быть при 1й степени зависимости в пределах первого месяца овладения компьютером или на начальном этапе 2й степени.

В. Ребенок не откликается на просьбу, явно не слышит, игру не прерывает такое поведение свойственно зависимости 2-3 степени.

2-й уровень в случае, если ребенок вел себя по схеме Б или В, необходимо, через какой-то промежуток времени, например, на следующий день, обратиться к ребенку с развернутой, аргументированной просьбой, например: «Сынок, помоги мне, пожалуйста, подвинуть кресло. Я одна справиться не могу. Мне нужна твоя помощь. Пожалуйста, прерви свое занятие и помоги мне». Если реакция на просьбу будет аналогичной, то можно делать вывод о наличии зависимости у ребенка и необходимости предоставить ему помощь.

Анкета для родителей (приложение к родительскому собранию №1)

1. минут, ... часов в течении дня я провожу за компьютером.
2. Для учёбы я использую Интернет минут, ... часов в день.
3. В Интернете я люблю.....

4. В социальных сетях, «Инстаграм» я «сизжу» минут, ... часов.
5. В социальных сетях мне нравится.....
6. Я посещаю такие детские социальные сети как
7. Мои родители контролируют время моей работы, посещения социальных сетей (да / нет др.)
8. Подключаясь к Интернет, появляются такие угрозы, как

Существуют определенные сайты, которые вы можете посоветовать родителям, для определения Интернет- зависимости, зависимости от компьютерных игр в режиме реального времени. Родитель, придя домой, в спокойной обстановке более правдиво ответит на вопросы, возможно, осознает уровень опасности.

Ресурсы: Определение Интернет зависимости

<http://psyhelp.ru/internet/test.php>

http://psychology.net.ru/tests/start.html?test_id=6

<http://shkolazhizni.ru/test/27/>

Тесты на определение зависимости от компьютерных игр

<http://www.vrcalternativa.ru/articles/igromaniatest.>

Приложение 1.3.

Методики создания практических заданий, адресованных родителям.

1. Мероприятия с родителями по основам информационной безопасности детей в сети Интернет

1) С периодичностью не реже 1 раз в учебный год необходимо проводить общешкольное и/или классные тематические родительские собрания, посвящённые вопросам информационной безопасности детей в сети

Интернет (по возможности с участием специалистов в области компьютерной коммуникации).

2) Рекомендовать классным руководителям проводить в рамках родительских собраний семинары по обмену опытом обеспечения безопасности ребенка в информационном обществе.

3) Работа с родителями включает в себя следующие формы:

1. Отправной точкой каждого учебного года является оформление Советом Старшекласников стенда "Опасности Интернета", где собрана информация о запрещённых и полезных сайтах, статистические данные, об ответственности родителей за здоровье своих детей.

2. Педагогом - психологом школы разрабатываются и проводятся родительские собрания, на которых рассказывается о том, какие правила должны соблюдать родители, чтобы их дети избежали участи стать зависимыми от телефона и компьютерных игр;

3. Психологическим клубом «Доверие», где занимаются наравне с другими учащимися «дети группы риска» разрабатываются памятки, буклеты для родителей.

4. Совместные родительские собрания с детьми, на которых в форме игры рассказывается о истории появления компьютера, о правилах пользования

Интернетом, как быть взаимно вежливым в Интернете, как необходимо фильтровать нужную информацию.

5. Выступление на родительском собрании медицинского работника на тему: «Компьютер и здоровье» Предлагаемые темы родительских собраний:

Компьютер в жизни подростка

Поколение КОМП

Внимание: дети в Интернете

Виртуальная агрессия

Компьютер без вреда.

Приложение 1.4.

Памятки и советы родителям

Информацию для родителей необходимо подготовить актуальную на период проведения родительского собрания. Желательно, чтобы классный руководитель на собрание мог пригласить системного администратора программы «Кунделик», подготовить актуальные факты, о времени пребывания детей в интернете, проблемы с которыми школьники чаще всего сталкиваются, когда пребывание в социальных сетях и на различных запрещенных сайтах превышает 3 часов в день.

Приложение 2 к родительскому собранию № 1 .

Результаты школьных исследований «Дети в Интернете и родители» 78% детей регулярно пользуются детскими социальными сетями, предпочитая те же сервисы, что и взрослые;

Около 42% детей из общего числа зарегистрированных в соцсетях пользуются «Тик Ток»;

Опросы обучающихся средних классов показывает, что большая половина зарегистрированы в «Тик Ток» давно, и готовы зарегистрироваться хоть сейчас и все оставшиеся, потому что «это круто», «там все наши», «там прикольно».

Опрос учащихся 7-11 классов показал, что если у ребенка есть сотовый телефон с выходом в Интернет, то школьник в обязательном порядке каждый день зависает в социальных сетях. Что ребенок делает в Интернете? Что и все остальные: пишет короткие сообщения; смотрит мультики (младшие); слушает музыку; размещает фотографии, видео; знакомится, дружится, (ведь в реальной жизни не всегда получается) и так далее;

60% детей имеют доступ к сети Интернет дома, 28% в школе, 10% у друзей и лишь 2% в Интернет-кафе.

Причем 100% опрошенных родителей указали, что разрешают своим детям путешествовать по Всемирной сети.

На вопрос «Оказывают ли путешествия по сети на школьные успехи Вашего ребенка?» 64% родителей ответили положительно, а 36% родителей указали, что путешествия по Интернету не влияют на успеваемость их ребенка.

На вопрос «Оказывают ли путешествия по сети на здоровье Вашего ребенка?» лишь 43% родителей ответили положительно. 57% считают, что путешествия по сети не влияют на здоровье детей.

На вопрос «Что Вас больше всего настораживает при использовании Вашим ребенком сети Интернет?» около 32% родителей указали вредоносные сайты, 28% сайты с негативным и противоправным контентом.

Большинство родителей считают, что наиболее эффективным способом защиты детей от Интернет-угроз являются специализированные системы фильтрации контента и наблюдение взрослых.

Все большее количество детей получает возможность работать в Интернет. Но вместе с тем все острее встает проблема обеспечения безопасности наших детей в Интернет. Так как изначально Интернет развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители и взрослые?

Следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

Общие советы по управлению безопасностью детей в возрасте 14 – 17 лет при работе в интернете.

1. Измените в соответствии с интересами и запросами подростка список домашних правил использования подростком Интернета, требуйте его соблюдения.

2. Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются.

3. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.

4. Интересуйтесь, какими чатами и досками объявлений пользуются подростки и с кем они общаются.

5. Поощряйте использование модулируемых чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.

6. Возьмите за правило знакомиться с сайтами, которые посещают ваши дети. Убедитесь, что они не посещают сайты с оскорбительным содержанием, не публикуют личную информацию или свои фотографии.

7. Настаивайте, чтобы подростки никогда не соглашались на личные встречи с друзьями из Интернета без вашего участия. Напоминайте, какие опасности это может за собой повлечь.

8. Требуйте от подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.

9. Требуйте от подростков не загружать программы, музыку или файлы без консультаций с вами.

10. Объясните, что иначе подростки могут нарушить авторские права и тем самым закон.

11. Настаивайте на том, чтобы подростки ставили вас в известность, если что-либо или кто-либо в Сети тревожит или угрожает им. Объясните, что угрозы им – это также и угроза всей семье. Оставайтесь в случае чего спокойными и напомните детям, что они в безопасности, если рассказали вам. Помогайте им решить возникшие проблемы.

12. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

13. Постоянно напоминайте, что ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Убедитесь, что подростки советуются с вами перед покупкой или продажей чего-либо в Интернете.

15. Обсудите с подростками азартные сетевые игры и связанный с ними риск. Напомните, что детям нельзя в них играть.

16. Поддерживайте уровень безопасности вашего компьютера на должном уровне. Если ваш ребенок лучше вас разбирается в программном обеспечении, то почему бы не поручить ему заботу о безопасности ваших семейных компьютеров?

Риски, с которыми подростки сталкиваются в сети и советы по профилактике и правильной реакции при возникновении угрозы.

Большинство старших подростков используют Интернет для получения информации. Однако, информация, выдаваемая Интернетом, может оказаться нежелательной и вредной для здоровья ребенка (страдает эмоциональная сфера подростка, также может быть нанесен прямой вред физическому здоровью ребенка.).

Примеры противозаконной, неэтичной и вредоносной информации:

- информация о насилии, жестокости и агрессии,
- информация, разжигающая расовую ненависть, нетерпимость по отношению к другим людям по национальным, социальным, групповым признакам,
- пропаганда саморазрушений;
- пропаганда азартных игр,
- пропаганда и распространение наркотических веществ, отравляющих веществ,
- пропаганда анорексии (отказ от приема пищи) и булимии (чрезмерное потребление пищи),
- пропаганда деятельности различных сект, неформальных молодежных движений,
- нецензурная лексика

Распространение противозаконной информации преследуется по закону, например, распространение наркотических веществ через Интернет, порнографических материалов с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям

Что делать.

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. РОДИТЕЛЬСКИЙ контроль возможен и нужен в Интернете. Родители могут решить какое содержимое в Интернете могут просматривать их дети, отследить, какие сайты посещал ребенок, ограничить время пользования Интернетом

Ресурсы в помощь родителю:

<http://licensor.ru/>

<http://www.oszone.net/6213/>

2. Используйте опцию «Безопасный поиск», которую предоставляют популярные поисковых систем и почтовых служб. Опция легко настраивается самостоятельно.

3. Каждому пользователю домашнего ПК – свой пароль и логин. Учетная запись администратора должна быть у родителя, тогда только родитель сможет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера.

4. Самое важное: доверительные отношения. Чем больше Вы общаетесь с ребенком на интересующие его темы, тем меньше тайн от Вас будет у него.

Интернет для старшего подростка – среда общения. Общение также может стать угрозой для Вашего ребенка, если он: подвергался ли Ваш ребенок травле, кибербуллингу (буллинг запугивание, унижение, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе)

Как распознать опасность:

Обратите внимание на психологические особенности вашего ребенка. Признаки того, что ребёнок подвергается кибербуллингу, различны, но есть несколько общих моментов:

- признаки эмоционального дистресса на протяжении и после использования Интернета;
- прекращение общения с друзьями;
- избегание школы или школьных компаний;
- нестабильные оценки, выражение или отыгрывание злости в домашней обстановке,
- перемены в настроении, поведении, сне и аппетите;
- не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками;
- склонны к депрессии;

Что делать:

Научите: правильной реакции (оскорбляют – либо покинь данный ресурс, либо игнорируй хулигана); правольному поведению (никогда никого не оскорбляй сам)

Объясните: личная информация, выложенная в Интернет, может быть использована против тебя

Воспользуйтесь опцией: «заблокировать пользователя» или «занести в чёрный список». При серьезных проблемах (угрозы перешли в реальную жизнь, касаются жизни или здоровья ребенка, а также членов вашей семьи, потрачены деньги и т.д)

Скопируйте и сохраните информацию со страницы сайта.

Обратитесь в правоохранительные органы

Подвергся грумингу установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации.

Как распознать опасность?

1. в компьютере стали появились материалы откровенного содержания.
2. ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый.
3. ребенок стал замкнутым и подавленным.
4. звонит по неизвестным вам номерам (либо звонят ему), при звонках старается уйти, в содержание разговора не посвящает

Как предупредить опасность:

1. объяснить, что нельзя: помещать личные данные в Интернет – сетях (ФИО, домашний адрес, телефон);
 - пересылать виртуальным знакомым свои фотографии или видео;
 - ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи;
 - использовать реальное имя при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сетевые сайты мгновенного обмена сообщениями, в онлайн играх);
2. в доверительной беседе постарайтесь предупредить об опасности встречи с неизвестными людьми из Интернета. Договоритесь, что если ребенок пойдет на такую встречу, то только с вами;
3. создайте условия, чтобы ваш ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время;
4. поговорите с ребенком на тему взаимоотношений мужчины и женщины (каким бы взрослым вы не считали бы своего ребенка). Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в Интернете тема любви часто представляется в неправильной, вульгарной форме;

Что делать:

1. сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов;
2. обратитесь к представителям власти;

Памятка №1

Памятка для родителей по безопасному использованию сети Интернет

Если ваши дети пользуются Интернетом дома, вы уже знаете, насколько важно защитить их от неподобающего содержимого и нежелательных контактов. Подростки должны иметь практически неограниченный доступ к содержимому, сайтам или действиям. Они хорошо разбираются с тем, как использовать Интернет, однако родителям все равно следует напоминать им о соответствующих правилах безопасности. Родители всегда должны быть готовы помочь своим детям подросткам разобраться, какие сообщения являются непристойными, а также избегать опасных ситуаций. Родителям рекомендуется напоминать детям подросткам о том, какую личную информацию не следует предоставлять через Интернет. Советы по безопасности, которые рекомендуется выполнять, когда ваши дети подростки используют Интернет:

Старайтесь по-прежнему поддерживать как можно более открытое общение внутри семьи и позитивное отношение к компьютерам. Обсуждайте с детьми их общение, друзей и действия в Интернете точно так же, как другие действия и друзей.

Просите детей подростков рассказывать вам, если что-то или кто-то в Интернете доставляет им чувство неудобства или страха. Если вы подросток и вам не нравится что-то или кто-то в Интернете, расскажите об этом.

1. Создайте список семейных правил использования Интернете дома. Укажите виды сайтов, которые можно посещать без ограничений, время подключения к Интернету, расскажите, какую информацию не следует разглашать в Интернете, а также предоставьте инструкции по общению с другими в Интернете, включая общение в социальных сетях.

2. Компьютеры, подключенные к Интернету, должны находиться в открытом месте, а не в спальне ребенка подростка.

3. Изучите средства фильтрации Интернет содержимого и используйте их в качестве дополнения к контролю со стороны родителей.

4. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер.

5. Следите за тем, какие сайты посещает ваш ребенок подросток и с кем он общается. Просите их пользоваться контролируруемыми чатами, настаивайте на том, чтобы они использовали только общедоступные чаты.

6. Настаивайте на том, чтобы они никогда не соглашались на встречу с друзьями, с которыми они познакомились в Сети.

7. Научите детей не загружать программы, музыку или файлы без вашего разрешения. Обмен файлами и использование текста, изображений или

рисунков с вебсайтов может привести к нарушению авторских прав и может быть незаконным.

8. Поговорите со своими детьми подростками о содержимом в Интернете, предназначенном для взрослых, и порнографии, а также укажите им позитивные сайты, посвященные вопросам здоровья и сексуальности.

9. Помогите им защитить себя от спама. Проинструктируйте своих детей подростков никогда не давать свой адрес электронной почты при общении в Интернете, не отвечать на нежелательные почтовые сообщения и пользоваться фильтром электронной почты.

10. Знайте, какие сайты ваши дети подростки посещают чаще всего. Убедитесь, что ваши дети не посещают сайты, содержащие оскорбительные материалы, и не публикуют свою личную информацию. Следите за тем, какие фотографии публикуют ваши дети подростки и их друзья.

11. Учите своих детей отзывчивости, этике и правильному поведению в Интернете. Они не должны использовать Интернет для распространения сплетен, клеветы или запугивания других.

12. Проследите за тем, чтобы дети спрашивали у вас, прежде чем совершать финансовые операции в Интернете, включая заказ, покупку или продажу товаров.

13. Обсудите со своими детьми подростками азартные игры в Интернете, а также потенциальные риски, связанные с ними. Напомните им о том, что азартные игры в Интернете являются незаконными.

Памятка №2

Рекомендации родителям по предупреждению компьютерной зависимости у ребёнка

Для профилактики компьютерной зависимости психологи советуют следующее:

1. Показывать личный положительный пример. Важно, чтобы слова не расходились с делом и, если отец разрешает играть сыну не более часа в день, то сам не должен играть по три-четыре.

2. Ограничьте время работы с компьютером, объяснив, что компьютер – не право, а привилегия, поэтому общение с ним подлежит контролю со стороны родителей. Резко запрещать работать на компьютере нельзя. Если ребёнок уже склонен к компьютерной зависимости, он может проводить за компьютером два часа в будний день и три – в выходной, но обязательно с перерывами.

3. Предложить другие возможности времяпрепровождения. Можно составить список дел, которыми можно заняться в свободное время. Желательно, чтобы в списке были совместные занятия (походы в кино, на природу, игра в шахматы и т.д.)

4. Использовать компьютер как элемент эффективного воспитания, в качестве поощрения (например, за правильно и вовремя сделанное домашнее задание, уборку квартиры).

5. Обращать внимание на игры, в которые играют дети, т.к. некоторые из них могут стать причиной бессонницы, раздражительности, агрессивности, специфических страхов.

6. Обсуждать игры вместе с ребёнком. Отдавать предпочтение развивающим играм. Крайне важно научить ребёнка критически относиться к компьютерным играм, показывать, что это очень малая часть доступных развлечений, что жизнь гораздо разнообразней, что игра не заменит общения.

7. Если родители самостоятельно не могут справиться с проблемой, необходимо обращаться к психологам.

Памятка №3

Основные правила безопасности для родителей.

1. Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.

2. Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.

3. Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.

4. Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.

5. Спрашивайте ребенка о том, что он видел и делал в Интернете.

6. Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя, не содержащее никакой личной информации.

7. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также "показывать" свои фотографии.

8. Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете — правда. Приучите его спрашивать то, в чем он не уверен.

9. Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.

10. Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации.

11. Не позволяйте Вашему ребенку встречаться с онлайн знакомыми, без Вашего разрешения или в отсутствии взрослого человека.

12. Постараться регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;

13. Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости также неприятно, как и слышать;

14. Проверяйте актуальность уже установленных правил. Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.

Памятка №4

Что делать, если ребенок уже столкнулся с какой-либо Интернет-угрозой.

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказывать.

2. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате интернет - мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в интернете.

3. Если ситуация связана с насилием в интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.

4. Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.

5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

Памятка №5.

Рекомендации родителям, с помощью которых можно всегда достойно выйти из ситуации, когда пользователя пытается донимать сетевой грубиян

1. Чат.

Если при общении в тематическом чате к вам пристает пользователь с оскорблениями, злыми шутками или издевательствами, отправьте его в игнор-лист (персональный «черный список») или сообщите администратору чата о его неприемлемом поведении. Скорее всего, грубиян будет забанен, то есть исключен из числа пользователей. Грубить хаму в ответ чревато получением такого же бана.

2. Онлайн мессенджеры.

Отвязаться от нежелательного собеседника в аське проще всего. Добавив разбушевавшегося грубияна в «черный список», вы больше никогда не увидите и не услышите его. Чтобы предотвратить дальнейшие беседы с «клонами» хама (то есть его «реинкарнациями» под другими номерами ICQ), необходимо поставить в настройках клиента запрет на получение сообщений от неавторизованных пользователей.

Тогда вы будете получать сообщения только от тех контактов, которые одобрите сами.

3. Социальные сети.

Решить проблему хамства в социальных сетях обычно помогают модераторы ресурса, которые обязаны внимательно следить за публичными сообщениями пользователей. В случае добросовестной работы модераторов Вы даже не успеете прочитать оскорбительное послание. Если же сетевой грубиян доносит вас по личной почте, вы всегда можете пожаловаться тому же модератору в индивидуальном порядке.

4. Сайты знакомств.

К сожалению, приличная часть посетителей сайтов знакомств приходят туда вовсе не для того, чтобы найти себе друзей и любимых. Сайты знакомств являются излюбленным местом обитания сетевых хамов, любителей онлайн-издевательств и розыгрышей. Поэтому, пользуясь подобными ресурсами, нужно быть предельно внимательным и быть морально готовым к неадекватным сообщениям. Отвечать на провокации и грубости вовсе не обязательно, а кнопка жалобы администрации всегда под рукой.

5. Форумы.

Свои местные хамы и так называемые тролли (провокаторы) есть на каждом популярном форуме. От обычных собеседников, не согласных с Вашим мнением, их отличает провокационный тон сообщений, открытые издевательства или откровенная глупость аргументов. Пытаться доказать таким людям совершенно бесполезно, так как они преследуют единственную цель – позлить вас. Лучше представьте, что этого пользователя вовсе не существует на форуме и его сообщений тоже. Продолжайте беседу в привычной манере, не реагируя на попытки тролля вывести вас из себя. Вероятно, вскоре ему надоест тратить время зря и он оставит вас в покое.

Если же Вы сами не прочь сорвать злость и плохое настроение в Интернете, можете рискнуть пообщаться с сетевым хамом на его языке. В конце концов, он первый начал и вы не обязаны быть вежливым. Однако опускание до уровня банального грубияна занятие не делающее чести никому, поэтому куда лучше будет не обращать на него внимания.

Памятка №6

Цензура компьютерных игр

Цензура взрослыми компьютерных игр вещь, совершенно необходимая, причем не надейтесь, что за вас это кто-то сделает. Каждая игра, попадающая в руки ребенка, вначале должна быть просмотрена кем-то из взрослых. Вникните

в ее содержание, задайтесь вопросами: что даст эта игра вашему ребенку, какие качества личности будет развивать в нем, не будет ли формировать агрессивный стиль поведения, не даст ли какую-то опасную информацию?

Игра должна:

развивать; должны быть исключены бранные слова и выражения; не должны формировать циничное отношение к происходящему; должны быть исключены агрессивные послы и негативная информация; не вызывать привыкания к боли, драматичным ситуациям; не учить противозаконным вещам; Не содержать сексуальной тематики.

Аналогичной цензуре должны подвергаться и фильмы, которые смотрят дети, так как агрессия, негативная информация, чувство страха от просмотра фильмов также вредны для детской психики

Памятка №7

Ваш ребенок жертва преступника.

Уважаемые родители! Обратите внимание на следующие признаки, позволяющие определить, что ребенок подвергся атаке злоумышленников в сети.

- Ваш ребенок проводит много времени в Интернете. Большинство детей, преследуемых Интернет-преступниками, проводят большое количество времени в Сети, особенно в чатах; как правило закрывают дверь в свою комнату и скрывают, чем они занимаются, сидя за компьютером.

- В семейном компьютере появились материалы откровенного содержания. В качестве предлога для начала сексуальных обсуждений злоумышленники могут снабжать детей фотографиями, ссылками на соответствующие сайты и присылать сообщения эротической окраски. Для того чтобы внушить ребенку мысль о естественности сексуальных отношений между взрослыми и детьми, преступники могут использовать фотографии с изображением детской порнографии. Имейте в виду, что ваш ребенок может прятать порнографические файлы на дисках, особенно если другие члены семьи пользуются тем же компьютером.

- Вашему ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам неизвестны. Установив в Интернете контакт с вашим ребенком, некоторые злоумышленники могут попытаться вовлечь детей в секс по телефону или попытаться встретиться в реальной жизни.

Если дети не решаются дать номер телефона, злоумышленник может сообщить им свой. Не разрешайте своему ребенку лично встречаться с незнакомцем без контроля с вашей стороны.

- Ваш ребенок получает письма, подарки или посылки от неизвестного вам лица. Обычно преследователи посылают своим потенциальным жертвам письма, фотографии и подарки. В других странах они порой даже отправляют билеты на самолет, чтобы соблазнить ребенка личной встречей. Ваш ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый. Интернет-преступники усердно вбивают клин между детьми и их семьями и часто

преувеличивают небольшие неприятности в отношениях ребенка с близкими. Кроме того, дети, подвергающиеся сексуальному преследованию, становятся замкнутыми и подавленными.

- Ваш ребенок использует чью-то чужую учетную запись для выхода в Интернет. Даже дети, не имеющие доступа в Сеть дома, могут встретить преследователя, выйдя в Интернет у друзей или в каком-нибудь общественном месте, например библиотеке. Иногда преступники предоставляют своим жертвам учетную запись, чтобы иметь возможность с ними общаться.

Советы родителям по предотвращению развития компьютерной зависимости у детей.

- Часто причиной возникновения компьютерной зависимости у детей и подростков становятся неуверенность в себе и отсутствие возможности самовыражения. В таких случаях родители должны поддержать ребенка и помочь ему разобраться с возникшими проблемами.

- Абсолютно неправильно критиковать ребенка, проводящего слишком много времени за компьютером. Это может только углубить проблему и отдалить ребенка от родителей.

- Если ребенок страдает игровой завистью, нужно постараться понять его и в какой-то мере разделить его интерес к компьютерным играм. Это не только сблизит ребенка с родителями, но и увеличит его доверие к ним, а значит, ребенок с большей уверенностью будет следовать советам родителей и с большим доверием делиться с ними своими проблемами.

- Критика воспринимается ребенком, как отказ родителей понять его интересы и потому вызывает замкнутость и в некоторых случаях агрессию.

- Основной мерой предотвращения возникновения зависимости любого типа у детей является правильное воспитание ребенка. При этом важно не ограничивать детей в их действиях (например, запрещать те или иные игры), а объяснять, почему то или иное занятие или увлечение для него не желательно.

- Рекомендуется ограничивать доступ детей к играм и фильмам, основанным на насилии. В то же время если ребенок все же встретился с такой информацией нужно в доступной форме объяснить ему почему такая информация для него опасна и почему он не должен стремиться узнать ее.

- Категорический запрет того или иного вида информации безо всяких объяснений только увеличит интерес ребенка к этой информации, а существование запрета сделает невозможным обсуждение проблемы между родителями и ребенком.

Дети и подростки нуждаются в самовыражении. За неимением других средств выражения своих мыслей и энергии они обращаются к компьютеру и компьютерным играм, которые создают иллюзию реальности безграничных возможностей, лишенной ответственности. Такая иллюзия оказывает разрушительное действие на психику.

Опасности. Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций.

Компьютер. Повысьте уровень общей безопасности Вашего компьютера.

Время. Следите за достижением равновесия у вашего ребенка между временем, проводимым в Интернете и вне его.

Правила. Обсудите внутрисемейные правила пользования Интернетом.

Этикет. Научите детей уважать других в Интернете.

Что делать, если ваш ребенок стал потенциальной целью преступника?

Регулярно проверяйте компьютер на наличие материалов откровенного характера или

Каких – либо свидетельств об общении с сексуальной окраской – это настораживающие признаки.

Контролируйте доступ вашего ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно Интернет- преступники впервые встречают своих потенциальных жертв в чатах, а затем продолжают общаться с ними посредством электронной почты или мгновенных сообщений.

Не вините детей. Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе.

Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом. Если ваш ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей власти.

Преступники в интернете: что можно сделать для снижения опасности?

Пользуясь возможностями Интернета, дети подвергаются опасности вступить в контакт со злоумышленниками. Анонимность общения в Интернете способствует быстрому возникновению доверительных и дружеских отношений. Преступники используют преимущества этой анонимности для завязывания отношений с неопытными молодыми людьми. Вы сможете защитить своих детей, если поймете возможную опасность общения через Интернет и будете в курсе того, чем они занимаются в Сети.

Как сделать общение в интернете комфортным?

Контролируйте использование чата вашим ребенком. Помните о том, что дети могут участвовать в чатах, расположенных на сайтах, при помощи программ поддержки чатов, сотовых телефонов и даже некоторых онлайн-игр.

Добейтесь того, чтобы дети никогда не сообщали в чатах свои личные данные. Так, при выборе псевдонима необходимо выбирать имя, не выдающее личные данные детей. Например, вместо псевдонима DetroitSue можно использовать SassySue. Следует настоять на том, чтобы дети не посылали своих фотографий тем, с кем они познакомились в чате. Дети должны знать, что они всегда могут обратиться к вам за советом или помощью. Предупредите ребенка о том, что, если что-либо в чате вызовет у него чувство дискомфорта,

необходимо немедленно его покинуть и сообщить о происшедшем кому-нибудь из взрослых. Пусть дети всегда сообщают вам об участниках чата, которые предлагают им встретиться в частных комнатах чата.

У детей должно быть настороженное отношение к попыткам собеседников перевести общение из виртуальной плоскости в реальную. Им никогда нельзя соглашаться на личную встречу с незнакомыми людьми, с которыми они познакомились в Интернете.

Скажите детям, чтобы они посещали только модерируемые чаты. Перед тем как вступить в беседу, пусть ознакомятся с положениями и условиями участия в чате, правилами поведения и положением о конфиденциальности.

Советы по повышению безопасности участия ваших детей в онлайн-играх по сети.

Получите информацию. Ознакомьтесь с классификацией игр и условиями конфиденциальности, а также прочтите правила на сайте игры. В качестве примера можно познакомиться с кодексом поведения. Будьте в курсе, в какие игры и с кем играют ваши дети. Поместите компьютер или игровую консоль (например, Xbox) туда, где экран хорошо просматривается; искренне интересуйтесь, во что дети играют.

Установите правила. Это следует сделать до выхода детей в Интернет; кроме того, убедитесь, что ребенок их понимает. С примером такого рода домашних правил можно ознакомиться, прочитав «Внутрисемейные правила пользования Интернетом».

Контролируйте чат и сообщения во время игр. Попросите детей сообщать вам, если другой игрок употребляет нецензурные слова; в этом случае можно выделить обидчика в списке и отключить или заблокировать его сообщения. Другой вариант – сообщить о некорректно ведущем себя игроке администраторам игры по электронной почте, в чате или другим способом. Для дополнительной информации о возможных мерах воздействия на таких игроков можно обратиться на официальный сайт игры. Обучите детей навыкам безопасности. Скажите детям, что, если кто-либо из игроков будет вести себя оскорбительно, игру следует остановить и немедленно сообщить вам. При необходимости – связаться с администратором.

Убедитесь в конфиденциальности. Требуйте от детей никогда не выдавать в игровом чате личную информацию (например, имя, пол или домашний адрес), фотографии и не соглашаться на встречи.

Убедитесь, что дети знают о необходимости обратиться к вам за помощью в случае чего. Выбирайте соответствующие имена. Заставьте ребенка использовать подходящие имена героев, соответствующие игровым правилам. Эти имена не должны раскрывать никакую личную информацию или провоцировать домогательство.

Примечание: Для компьютеров и игровых консолей есть технология маскировки или скрытия голоса, позволяющая изменить настоящий голос ребенка. Имейте в виду, что взрослые также могут пользоваться этой программой и выдавать себя не за того, кто они есть на самом деле.

Берегитесь хулиганов.

Играйте вместе. Безопаснее всего для детей играть через Интернет вместе с вами. Возможно, им этого хочется меньше всего на свете (особенно тем, кто постарше), но это очень хороший способ научиться общению в Сети.

Как предостеречь детей от игр на деньги?

Родители должны решить, во что можно играть их детям. Обсудите жанр игр (скажем, только бильярд, стратегии и шахматы) и количество участников (можно ведь играть и одному).

Напоминайте детям, что им нельзя играть на деньги. Предложите им играть в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей, выигрышей. Помогите детям понять механизм таких игр. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают.

Не позволяйте детям использовать номера ваших кредитных карт в Интернете. Держите их в недоступном для детей месте. В сетевых играх на деньги они обычно требуются. Дети могут ненароком влезть в долги.

Объясните, что к играм на деньги можно пристраститься. Всегда есть опасность приобретения зависимости. Это как болезнь. Особенно если есть кредитная карта и положительный баланс на ней; человек может играть, пока не истратит все до конца.

Контролируйте поведение своих детей в Интернете.

Следите за тем, какие сайты посещают ваши дети и что они делают в Интернете.

Как поступать, если дети столкнулись с гриферами?

Пусть ваши дети их игнорируют. Если ребенок не будет реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

Посоветуйте детям изменить параметры игры. Добейтесь, чтобы ребенок играл в игры, правила или режимы которых можно изменить, например, невозможность убить товарищей по команде. Таким образом, тактика гриферов становится бессмысленной.

Порекомендуйте создать частную игру. Большинство многопользовательских игр позволяет создавать закрытые комнаты, куда можно пускать только друзей.

Пусть дети играют на сайтах со строгими правилами. Там, где установлены строгие правила, администратор сможет немедленно заблокировать хулиганов.

Пусть играют в игры, где от гриферов можно легко избавиться. Предложите ребенку играть в те игры, где сообщения хулиганов можно отключить или проголосовать за их исключение из игры. Придумайте еще что-нибудь. Если обидчик продолжает беспокоить вашего ребенка, добейтесь, чтобы он сменил игру или сделал перерыв и вернулся позже. Сообщайте о

«дырах» в игре. Поищите вместе с ребенком уязвимости в игре или новые способы жульничества. Сообщайте о своих находках администратору.

Пусть ваши дети воздерживаются отвечать огнем на огонь. Убедитесь, что ребенок не использует против обидчиков их же тактику; скорее всего, это спровоцирует гриферов на еще более озлобленное поведение. Или, что еще хуже, создаст о ребенке впечатление как об обидчике. Рекомендуйте детям избегать провокаций с именами. Ребенок избежит многих проблем, если не станет использовать псевдоним, который может спровоцировать обидчика. Пусть дети не выдают личную информацию. Хулиганы (да и вообще кто угодно) могут использовать настоящие имена, номера телефонов, а также домашние или электронные адреса, чтобы причинить ребенку неприятности.

Снижение риска хищения личных данных.

Посещая вебсайты, нужно самостоятельно набирать в обозревателе адрес вебсайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Нужно как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации. При немедленном обращении компания может уменьшить ущерб, нанесенный вашей семье и другим лицам.

Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно

использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки.

Что делать в случае хищения личных данных?

Если вы подозреваете, что ваши личные данные украдены, немедленно принимайте меры:

- Измените пароли.
- Поставьте в известность отдел обслуживания клиентов соответствующих организаций.
- Поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета.
- Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.

- Записывайте и сохраняйте абсолютно все.

- После выполнения всех действий всегда делайте копии документов.

В виртуальном мире есть свои правила Интернет гигиены.

Как можно определить, что ваш компьютер заражен?

Ваш компьютер может начать работать медленнее или прекращать работать и перезагружаться каждые несколько минут. Иногда вирус атакует

файлы, необходимые для запуска компьютера. В подобном случае вы можете, нажав кнопку запуска, обнаружить, что смотрите на пустой экран.

Все эти симптомы являются типичными признаками заражения компьютера вирусом, хотя они могут вызываться также проблемами в аппаратной части или программном обеспечении, не имеющими ничего общего с вирусным заражением.

Совет: Помните, что, открыв и запустив зараженный файл, вы можете не сразу узнать, что получили вредоносную программу, так как вирусы часто начинают свою разрушительную работу не сразу. Пусть дети будут внимательны к сообщениям о том, что они отправили электронное письмо, содержащее вирус. Это может значить, что вирус указал ваш электронный адрес в качестве отправителя зараженного письма. Это необязательно означает, что на вашем компьютере есть вирус. Некоторые вирусы умеют фальсифицировать электронные адреса.

Если компьютер внезапно начал медленно работать или вы видите всплывающие окна, даже если не подключены к Интернету, то, возможно, вы стали жертвой программ шпионов и других нежелательных программ. Они автоматически загружаются в систему без всякого уведомления. Часто они бывают прикреплены к другому файлу, который вы скачали или установили. Программа шпион может загрузиться на ваш компьютер, даже если вы просто щелкнули по баннеру.

Памятка № 8

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя

Уважаемые родители!

1. Предупредите детей, что:

- Пиратство – это обычное воровство.

2. Объясните вашим детям, что:

- если они незаконно скачивают файлы, то ваш компьютер рискует стать уязвимым для вирусов или программ шпионов.

- подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции.

- официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией

- распространители пиратских продуктов, преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя

3. Обсудите с детьми допустимые траты на музыкальные записи или игры, чтобы у молодого поколения не было соблазна для незаконного скачивания.

4. Научите детей законным методам скачивания В Интернете существует множество мест, где вы и ваши дети можете скачать программы, фильмы, игры и музыку бесплатно или за небольшую цену. Например, сайт MSN Music предлагает более миллиона записей от разных студий

5. Сами будьте примером.

Памятка № 9

Основы безопасного ведения интернет-журнала.

Уважаемые родители!

Правильное ведение дневника может дать детям и их родителям возможность общаться и поделиться друг с другом опытом; дети могут поведать родителям о новых технологиях, а родители могут дать ряд ценных жизненных советов.

Другое преимущество – привитие ответственности и дисциплины ведения дневника; возможность творческого самовыражения; новые возможности общения с друзьями и родственниками, обучение компьютерным и Интернет-технологиям, а также развитие навыков набора на клавиатуре, правописания, письменной речи и редактирования.

Чтобы Интернет-дневник не стал источником опасности:

Требуйте от ваших детей:

- никогда не публиковать в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения.

- никогда не помещать в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверять, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

Объясните, что публикуемая в Интернете информация остается там надолго и кто угодно может легко распечатать веб-журнал или сохранить его на своем компьютере.

Рекомендуйте детям:

- пользоваться веб-журналами только с ясно сформулированными условиями использования и проверять, можно ли защитить с помощью пароля сами веб-журналы, а не только учетные записи пользователя (даже если это так, лучше держать в уме, что любой человек может получить доступ к Интернет-дневнику).

- не стремиться соревноваться с другими детьми, ведущими веб-журналы.

Пусть дети стараются вести свой блог в положительном ключе и не использовать его для злословия или нападок в адрес других детей. разрешения правообладателя

Памятка № 10

Безопасный интернет вне дома.

Уважаемые родители! Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но, как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям выходить в Интернет самостоятельно, им следует уяснить некоторые моменты.

Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций. В заключение беседы установите определенные ограничения на использование Интернета и обсудите их с детьми. Сообща вы сможете создать для ребят уют и безопасность в Интернете.

Если вы не уверены, с чего начать, вот несколько мыслей о том, как сделать посещение Интернета для детей полностью безопасным.

- Установите правила работы в Интернете для детей и будьте непреклонны.

- Научите детей предпринимать следующие меры предосторожности по сохранению конфиденциальности личной информации:

- Представляясь, следует использовать только имя или псевдоним.

- Никогда нельзя сообщать номер телефона или адрес проживания или учебы.

- Никогда не посылать свои фотографии.

- Никогда не разрешайте детям встречаться со знакомыми по Интернету без контроля со стороны взрослых.

- Объясните детям, что разница между правильным и неправильным одинакова как в Интернете, так и в реальной жизни.

- Научите детей доверять интуиции. Если их в Интернете что-либо беспокоит, им следует сообщить об этом вам.

- Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

- Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

- Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр и других программ – является кражей.

- Скажите детям, что им никогда не следует встречаться с друзьями из Интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.

- Скажите детям, что не все, что они читают или видят в Интернете, – правда. Приучите их спрашивать вас, если они не уверены.

- Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

- Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Регулярно посещайте Интернет - дневник своего ребенка, если он его ведет, для проверки.

- Будьте внимательны к вашим детям!

Приложение 5.

Профилактика основных интернет рисков и борьба с ними.

Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.

Предупреждение столкновения с вредоносными программами

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.

3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.

4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.

5. Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.

6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п.).

7. Расскажите ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.

8. Расскажите ребенку, если он пользуется интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки — по этой информации злоумышленники могут многое узнать о вашем ребенке.

Как избавиться от вредоносных программ

1. Загрузите компьютер в безопасном режиме (включите компьютер, нажмите и, удерживая клавишу F8, выберите Безопасный режим (Safe Mode) в открывшемся меню).

2. Проведите полную антивирусную проверку компьютера.

3. Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей.

4. При невозможности самостоятельно решить проблему обратитесь за помощью в службу технической поддержки производителя установленного на вашем компьютере антивирусного ПО или в технический сервис.

Повысьте уровень безопасности вашего компьютера

Если на вашем компьютере установлена операционная система Microsoft® Windows® XP Service Pack 2, то можно использовать Windows Security Center. Эта программа позволяет просматривать информацию о состоянии защиты компьютера и изменять настройки, а также получать дополнительные сведения по вопросам безопасности.

Security Center показывает состояние трех важных компонентов безопасности: брандмауэра Интернета, антивирусных программ и службы автоматического обновления. Кроме того, он служит для перехода к другим разделам безопасности, а также поиска технической поддержки и ресурсов, имеющих отношение к защите компьютера.

Security Center работает в фоновом режиме, постоянно проверяя состояние трех наиболее важных компонентов. Для того чтобы повысить уровень общей безопасности в Windows XP, нужно проделать следующее:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Центр обеспечения безопасности/Security Center;
- убедитесь, что включены основные компоненты безопасности (брандмауэр, автоматическое обновление, защита от вирусов).

Включить или отключить брандмауэр и автоматическое обновление вы можете непосредственно в Центре обеспечения безопасности.

Для управления защитой от вирусов обратитесь к настройкам установленного антивирусного программного обеспечения.

Блокируйте доступ к неподходящим материалам.

Один из наилучших способов защиты от нежелательной информации – это блокирование доступа еще до того, как она может быть получена.

Microsoft предлагает несколько таких способов.

Для того чтобы блокировать доступ к нежелательной информации в Internet Explorer® и MSN Explorer, нужно выполнить следующее:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Свойства обозревателя/Internet Options;

- в появившемся окне перейдите на вкладку Содержание/Content;
- в разделе Ограничение доступа/Content Advisor нажмите кнопку Включить/Enable;
- в появившемся окне введите пароль, который будет защищать вводимые вами ограничения от изменения детьми;
- в окне Ограничение доступа/Content Advisor вы можете блокировать доступ к нежелательной информации.

Повысьте уровень безопасности ребенка с электронной почтой.

Для повышения уровня безопасности при работе ребенка с электронной почтой в меню программы Outlook® Express в разделе Сервис/Tools выберите команду Параметры/Options.

Перейдите на вкладку Безопасность/Security.

При помощи переключателя выберите зону безопасности для Internet Explorer/Select the Internet Explorer security zone to use вы можете уменьшить вероятность появления вирусов на вашем компьютере. Для этих же целей служит переключатель «Не разрешать сохранение или открытие вложений, которые могут содержать вирусы» / Do not allow attachments to be saved or opened that could potentially be a virus. Если же вирус все же попал на ваш компьютер, ограничить его дальнейшее распространение вы можете, установив галочку Предупреждать, если приложения пытаются отправить почту от моего имени/Warn me when other applications try to send mail as me.

Для защиты пересылаемых писем от подделки и от возможности перехвата и прочтения кем-либо, кроме указанного получателя, есть возможность Шифровать содержимое и вложения всех исходящих сообщений/Encrypt content and attachments for all outgoing messages и Подписывать все отправляемые сообщения/Digitally sign all outgoing messages.

Заблокируйте поступление спама

Чтобы блокировать поступление спама (нежелательной почты), необходимо воспользоваться почтовым сервером, имеющим защиту от спама (например, hotmail.com), или почтовым клиентом, имеющим спам-фильтр (например, Microsoft Outlook).

Чтобы настроить спам-фильтр для почтового ящика, размещенного на сервере hotmail.com, необходимо зайти в этот почтовый ящик и перейти по ссылке Options и в вертикальном меню выбрать вкладку Mail.

Перейдя по ссылке Junk Email Filter, вы можете изменить настройки фильтра нежелательной почты. При помощи ссылки Block Senders, находящейся на вкладке Mail, вы можете добавить любого отправителя в список заблокированных, при этом почта от этого отправителя не будет поступать в ваш почтовый ящик.

В случае, если ваш почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться фильтром, встроенным в Microsoft Outlook.

Для настройки этого фильтра в меню Microsoft Outlook выберите Сервис/Tools, в открывшемся меню выберите команду Параметры/Options. В открывшемся диалоговом окне перейдите на вкладку Настройки/Preferences и

нажмите кнопку Нежелательная почта/Junk Email. В появившемся диалоговом окне вы можете внести изменения в настройки фильтра нежелательной почты. Кроме того, вы можете воспользоваться спам-фильтрами других разработчиков.

Создайте отдельные учетные записи для разных пользователей

Windows XP позволяет создать несколько учетных записей. Каждый пользователь сможет входить в систему независимо и иметь уникальный профиль с собственным рабочим столом и папкой «Мои документы». Родитель может создать себе учетную запись администратора, дающую полный контроль над компьютером, а детям – ограниченные учетные записи. Пользователи с ограниченными учетными записями не смогут изменить системные настройки или установить новое аппаратное или программное обеспечение, включая большинство игр, медиаплееров и программ поддержки чатов.

Для того чтобы создать отдельную учетную запись для ребенка с ограниченными правами доступа для работы в Интернете, необходимо выполнить следующие действия:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Учетные записи пользователей/User Accounts;
- в открывшемся окне выберите Создание учетной записи/Create a new account, введите ее имя;
- на этапе выбора типа учетной записи установите переключатель в положение Ограниченная запись/Limited;
- после нажатия кнопки Создать учетную запись/Create Account процесс создания учетной записи с ограниченными правами будет завершён, ваш ребенок сможет выбрать ее при следующем входе в систему.

Повысьте уровень конфиденциальности при общении вашего ребенка в интернете с помощью INTERNET EXPLORER.

Сохранение конфиденциальности личной информации вашего ребенка при его работе в Интернете является важным механизмом безопасности.

Для того чтобы повысить уровень конфиденциальности при общении вашего ребенка в Интернете, выполните следующие действия:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Свойства обозревателя/Internet Options;
- в появившемся окне перейдите на вкладку Конфиденциальность/Privacy;
- при помощи ползунка выберите необходимый уровень конфиденциальности.

Создавайте надежные пароли

Пароли – это ключи, которыми можно разблокировать компьютер и учетные записи в Интернете. Чем надежнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться вашими личными данными в корыстных целях, например, открыть новые счета

кредитных карт, обратиться за ипотекой или даже общаться через Интернет от вашего имени. Вы можете не подозревать о

таких действиях до тех пор, пока не станет слишком поздно. Создавать надежные пароли несложно. Для укрепления безопасности компьютера достаточно приложить незначительные усилия, с которыми можно познакомиться на сайте Microsoft по адресу <http://www.microsoft.com/rus/athome/security/privacy/password.msp>

Обычно подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. Ознакомьтесь с этими советами, чтобы защитить компьютеры, которыми вы пользуетесь в школе, от вирусов, хакеров, программ шпионов и других возможных атак.

В настоящее время все большее распространение получают беспроводные сети. Это дает возможность путешествовать по Интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях. Такие сети очень удобны, но их использование сопряжено со снижением уровня безопасности. Если вы устанавливаете беспроводную сеть дома или собираетесь активно использовать беспроводными сетями общего назначения, прочитайте соответствующие разделы брошюры и обратите особое внимание на информацию по безопасности.

Принимайте необходимые меры предосторожности, пользуясь беспроводной связью!

Кибермошенничество — один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Предупреждение кибермошенничества

1. Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в интернете.

2. Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки

3. Не отправляйте о себе слишком много информации при совершении интернет-покупок: данные счетов, пароли, домашние адреса и телефоны. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.

4. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут

предотвратить кражу конфиденциальных данных или другие подобные действия.

5. Убедитесь в безопасности сайта, на котором Вы или Ваш ребенок планируете совершить покупку:

- Ознакомьтесь с отзывами покупателей.
- Избегайте предоплаты.
- Проверьте реквизиты и название юридического лица – владельца магазина.
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации
- домена (сервис Whois).
- Поинтересуйтесь возможностью получения кассового чека и других документов за покупку.
- Сравните цены в различных интернет магазинах.
- Позвоните в справочную магазина.
- Обратите внимание на правила интернет магазина.
- Выясните, сколько точно вам придется заплатить.

Как справляться с кибермошенничеством

1. Проговорите с ребенком всю ситуацию. Он должен рассказать, какой сайт он посещал, на какие баннеры нажимал, какими услугами сети пользовался, что видел и т.д. Сохраните все электронные свидетельства совершенных действий и операций, скриншоты экранов – они могут служить доказательствами в дальнейшем.

2. Фишинг и вишинг: В случае хищения данных, поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета. Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Английское слово буллинг (bullying, от bully – драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Исследования буллинга начались еще в 70х годов прошлого столетия. Это поведение всегда присутствует в подростковой среде. В современном информационном обществе для буллинга все чаще используются инфокоммуникационные технологии. Буллинг, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона, называют кибербуллингом. Многие исследования показывают, что кибербуллинг часто сопровождается традиционным буллингом.

Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью

сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унижительный контент.

Предотвращение кибербуллинга

1. Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.

2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором, и тем более пытаться ответить ему тем же. Возможно стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием.

3. Обратите внимание на психологические особенности вашего ребенка. Специалисты выделяют характерные черты, типичные для жертв буллинга, они часто бывают:

пугливы, чувствительны, замкнуты и застенчивы;
тревожны, неуверенны в себе, несчастны;
склонны к депрессии;

не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками; мальчики могут быть физически слабее своих ровесников.

4. Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребенка.

5. Объясните детям, что личная информация, которую они выкладывают в интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.

6. Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.

7. Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в интернете.

8. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь. Если поступающие угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, а также членов вашей семьи, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут попадать под статьи действия уголовного и административного кодексов о правонарушениях.

Как справляться с кибербуллингом

1. Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию.

2. Сохраните все возможные свидетельства происходящего (скриншоты экрана, электронные письма, фотографии и т.п.).

3. Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он вам рассказал и показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ему уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.

4. Повторите ребенку простейшие правила безопасности при использовании интернета, дайте советы по дальнейшему предотвращению кибербуллинга.

Встречи с незнакомцами и груминг

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать груминг — установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети.

Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече.

Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед вебкамерой.

Предупреждение встреч с незнакомцами и груминга

1. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети. Обратите внимание, кого ребенок добавляет к себе «в друзья», с кем предпочитает общаться в сети — с ровесниками или людьми старше себя.

2. Объясните ребенку, что нельзя разглашать в интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т. д.), а также пересылать виртуальным знакомым свои фотографии или видео.

3. Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также нехорошо ставить на аватарку фотографии других людей без их разрешения.

4. Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя.

Помогите ему выбрать ник, не содержащий никакой личной информации.

5. Объясните ребенку опасность встречи с незнакомыми людьми из интернета. В сети человек может представиться кем угодно, поэтому на

реальную встречу с интернет другом надо обязательно ходить в сопровождении взрослых.

6. Детский познавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в интернете. Постарайтесь сами поговорить с ребенком на эту тему. Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в интернете тема любви часто представляется в неправильной, вульгарной форме. Важно, чтобы ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время.

Как противостоять грумингу

1. Если ребенок желает познакомиться с новым интернет другом, следует настоять на сопровождении ребенка на эту встречу

2. Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию

3. Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он рассказал или показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ребенку уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.

4. Сохраните все свидетельства переписки и контактов незнакомца с ребенком (скриншоты экрана, электронные письма, фотографии и т.п.).

5. При обнаружении признаков совращения следует не медленно сообщить об этом в правоохранительные органы.

6. Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению груминга.

Контентные риски

К контентным рискам относятся материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска. Противозаконный контент распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям. Вредоносный (опасный) контент, способный нанести прямой вред психическому и физическому здоровью детей и подростков. Неэтичный контент, который не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, «только для взрослых»).

Особо опасны сайты, на которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения, способы самоубийства, сайты, посвященные наркотикам, сайты, на которых размещены полные ненависти сообщения, направленные против отдельных групп или лиц. Столкновения с

контентными рисками могут иметь негативные последствия для эмоциональной сферы, психологического развития, социализации, а также физического здоровья детей и подростков.

Рекомендации по предупреждению контентных рисков

1. Используйте специальные технические средства, чтобы ограничивать доступ ребенка к негативной информации – программы родительского контроля и контентной фильтрации, настройки безопасного поиска. Часто пакет функций родительского контроля уже есть в вашей антивирусной программе. Программы родительского контроля позволяют: установить запрет на посещения сайтов различного негативного содержания, сайтов онлайн знакомств, сайтов с вредоносным содержанием; ограничить время доступа ребенка к интернету; производить мониторинг переписки в социальных сетях и онлайн мессенджерах (чатах); блокировать сомнительные поисковые запросы в поисковых системах; блокировать баннеры; а также отслеживать все действия ребенка в сети.

2. Если ребенок пользуется общим компьютером, для каждого члена семьи создайте свою учетную запись на компьютере. Ваша учетная запись должна иметь надежный пароль и обладать правами администратора, чтобы ребенок не мог менять установленные вами настройки и программы.

3. Регулярно следите за активностью вашего ребенка в сети. Просматривайте историю посещений сайтов, чтобы быть уверенным, что среди них нет опасных. При необходимости обновляйте настройки технических средств безопасности.

4. Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда. Необходимо проверять информацию, увиденную в интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных. Расскажите об этих правилах вашим детям.

5. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети. Попад случайно на какой-либо опасный, но интересный сайт, ребенок может продолжить поиск подобных ресурсов. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов.

6. Важно помнить, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую могут выступать более эффективными средствами для обеспечения безопасности вашего ребенка, чем постоянное

отслеживание посещаемых сайтов и блокировка всевозможного контента.

Интернет-зависимость

— навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. (Гриффит В., 1996). По

своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в интернет. Исследователи отмечают, что большая часть

Интернет зависимых (91 %) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.

Предупреждение интернет-зависимости

1. Оцените, сколько времени ваш ребенок проводит в сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.

2. Поговорите с ребенком о том, чем он занимается в интернете. Социальные сети создают иллюзию полной занятости — чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить — ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать,

насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.

3. Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.

4. Поговорите со школьным психологом и классным руководителем о поведении вашего ребенка, его успеваемости и отношениях с другими учениками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт. Узнайте, нет ли у вашего ребенка навязчивого стремления выйти в интернет с помощью телефона или иных мобильных устройств во время урока.

Как справляться с интернет-зависимостью

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.

2. Не запрещайте ребенку пользоваться интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и

пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети

3. Ограничьте возможность доступа к интернету только своим компьютером или компьютером, находящимся в общей комнате — это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.

4. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий — например, от бездумного обновления странички в ожидании новых сообщений.

5. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибер деятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями — при этом общаясь друг с другом «вживую». Важно, чтобы у ребенка были не связанные с интернетом увлечения, которым он мог бы посвящать свое свободное время.

6. Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без интернета. Важно, чтобы ребенок понял — ничего не произойдет, если он на некоторое время «выпадет» из жизни интернет - сообщества.

7. В случае серьезных проблем обратитесь за помощью к специалисту. Информацию, куда обращаться вы можете найти в разделе Полезная информация [33]

Блокируйте доступ к неподходящим материалам

Один из наилучших способов защиты от нежелательной информации — это блокирование доступа еще до того, как она может быть получена.

Microsoft предлагает несколько таких способов.

Для того чтобы блокировать доступ к нежелательной информации в Internet Explorer® и MSN Explorer, нужно выполнить следующее:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/ Control Panel;
- в панели управления откройте Свойства обозревателя/Internet Options;
- в появившемся окне перейдите на вкладку Содержание/Content;
- в разделе Ограничение доступа/Content Advisor нажмите кнопку Включить/Enable;
- в появившемся окне введите пароль, который будет защищать вводимые вами ограничения от изменения детьми;
- в окне Ограничение доступа/Content Advisor вы можете блокировать доступ к нежелательной информации.

Повысьте уровень безопасности ребенка в электронной переписке.

Для повышения уровня безопасности при работе ребенка с электронной почтой в меню программы Outlook® Express в разделе Сервис/Tools выберите команду Параметры/Options. Перейдите на вкладку Безопасность/Security.

При помощи переключателя выберите зону безопасности для Internet Explorer/Select the Internet Explorer security zone to use вы можете уменьшить вероятность появления вирусов на вашем компьютере. Для этих же целей служит переключатель. Не разрешать сохранение или открытие вложений, которые могут содержать вирусы /Do not allow attachments to be saved or opened that could potentially be a virus. Если же вирус все же попал на ваш компьютер, ограничить его дальнейшее распространение вы можете, установив галочку. Предупреждать, если приложения пытаются отправить почту от моего имени /Warn me when other applications try to send mail as me.

Заблокируйте поступление спама

Чтобы блокировать поступление спама (нежелательной почты), необходимо воспользоваться почтовым сервером, имеющим защиту от спама (например, hotmail.com), или почтовым клиентом, имеющим спам-фильтр (например, Microsoft Outlook). Чтобы настроить спам-фильтр для почтового ящика, размещенного на сервере hotmail.com, необходимо зайти в этот почтовый ящик и перейти по ссылке Options и в вертикальном меню выбрать вкладку Mail.

Перейдя по ссылке Junk Email Filter, вы можете изменить настройки фильтра нежелательной почты.

При помощи ссылки Block Senders, находящейся на вкладке Mail, вы можете добавить любого отправителя в список заблокированных, при этом почта от этого отправителя не будет поступать в ваш почтовый ящик. В случае, если ваш почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться

фильтром, встроенным в Microsoft Outlook. Для настройки этого фильтра в меню Microsoft Outlook выберите Сервис/Tools, в открывшемся меню выберите команду Параметры/Options. В открывшемся диалоговом окне перейдите на вкладку Настройки/Preferences и нажмите кнопку Нежелательная почта/Junk Email.

В появившемся диалоговом окне вы можете внести изменения в настройки фильтра нежелательной почты. Кроме того, вы можете воспользоваться спам-фильтрами других разработчиков.

Повысьте уровень конфиденциальности при общении вашего ребенка в интернете.

Сохранение конфиденциальности личной информации вашего ребенка при его работе в Интернете является важным механизмом безопасности.

Для того чтобы повысить уровень конфиденциальности при общении вашего ребенка в Интернете, выполните следующие действия:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Свойства обозревателя/Internet Options;

- в появившемся окне перейдите на вкладку Конфиденциальность/Privacy;
- при помощи ползунка выберите необходимый уровень конфиденциальности.

Создавайте надежные пароли. Пароли – это ключи, которыми можно разблокировать компьютер и учетные записи в Интернете. Чем надежнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться вашими личными данными в корыстных целях, например, открыть новые счета кредитных карт, обратиться за ипотекой или даже общаться через Интернет от вашего имени. Вы можете не подозревать о таких действиях до тех пор, пока не станет слишком поздно. Создавать надежные пароли несложно. Для укрепления безопасности компьютера достаточно приложить незначительные усилия, с которыми можно познакомиться на сайте Microsoft по адресу <http://www.microsoft.com>

Обычно подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. Ознакомьтесь с этими советами, чтобы защитить компьютеры, которыми вы пользуетесь в школе, от вирусов, хакеров, и других возможных атак.

В настоящее время все большее распространение получают беспроводные сети. Это дает возможность путешествовать по Интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях. Такие сети очень удобны, но их использование сопряжено со снижением уровня безопасности. Если вы устанавливаете беспроводную сеть дома или собираетесь активно использовать беспроводными сетями общего назначения, прочитайте соответствующие разделы брошюры и обратите особое внимание на информацию по безопасности.

Принимайте необходимые меры предосторожности, пользуясь беспроводной связью через программ родительского контроля.

Приложение 1.6.

Примерная тематика открытых мероприятий

1. Родительское собрание «Компьютер и сотовый телефон в жизни обучающегося»
2. Родительское собрание «Механизм обеспечения информационной безопасности учащихся в школе при использовании Интернета»
3. Родительское собрание «Информационная безопасность»
4. Родительское собрание «Безопасность в сети Интернет»
5. Выступление классного руководителя на родительском собрании: «Кибербуллинг и информационная безопасность ребенка»:
6. Лекторий «Современные решения информационной безопасности ребенка при работе в Интернет»
7. Общешкольное родительское собрание «Информационная безопасность семьи и ребенка»

8. Родительский всеобуч, встреча с родительской общественностью: «Актуальные проблемы безопасности образовательной среды: мониторинг, как инструмент выявления проблемных зон»

9. Родительское собрание «Этические нормы общения в социальных сетях».

Памятка педагогам по обеспечению информационной безопасности обучающихся воспитанников.

1. Объясните учащимся правила поведения в Интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.

2. Совместно с учащимися сформулируйте правила поведения в случае нарушения их прав в Интернете.

3. Приучайте несовершеннолетних уважать права других людей в Интернете. Объясните им смысл понятия «авторское право», расскажите об ответственности за нарушение авторских прав.

4. Проявляйте интерес к «виртуальной» жизни своих учеников, и при необходимости сообщайте родителям о проблемах их детей.

5. Научите учеников внимательно относиться к информации, получаемой из Интернета. Формируйте представление о достоверной и недостоверной информации. Наставляйте на посещение проверенных сайтов.

6. Обеспечьте профилактику интернет-зависимости учащихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.

7. Периодически совместно с учащимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернет-зависимости и обсуждайте с родителями результаты своих наблюдений.

8. В случае возникновения проблем, связанных с Интернет-зависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с учащимися и их родителями психолога, социального педагога.

9. Проводите мероприятия, на которых рассказывайте о явлении Интернет-зависимости, ее признаках, способах преодоления.

10. Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровья и сбережения.

11. Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью. Разумно используйте в своей жизни возможности интернета и мобильных сетей.

Материалы родительского собрания

По теме: Профилактика буллинга и кибербуллинга в школьной среде.

Цель: повышение заинтересованности родителей в профилактике

кибербуллинга их детей.

Задачи:

- профилактика буллинга в образовательной среде;
 - предупреждение и преодоление последствий буллинга среди учащихся;
 - систематизировать знания о взаимоотношениях детей и молодежи в учебном заведении;
 - научиться определять группы риска (жертв и булеров);
 - ознакомиться с принципами организации системного противостояния буллинга в молодежном коллективе;
 - приобрести умения асертивного поведения.
- Оборудование:
- мультимедийная установка для показа слайдов;
 - мультимедийная презентация к собранию;
 - памятки для родителей.

Предварительная работа:

В родительском уголке размещены статья о видах буллинга в школьной среде, актуальная статистика по проблеме (выжимка) и меры (советы_ по профилактике. Заранее розданы приглашения родителям с указанием темы собрания.

Аудитория:

- преподаватель;
- родители.

Основная часть:

Добрый день, уважаемые родители! Мы рады встрече с вами. Спасибо, что вы нашли время и пришли на родительское собрание. Тема нашего собрания посвящена проблеме буллинга – в частности, кибербуллинга, то есть в сети Интернет.

Проблема насилия в образовательной среде является, к сожалению, достаточно распространенной проблемой. Очень важно, чтобы ученики, их родители и учителя были проинформированы об этом негативном явлении, как его выявить, и, главное, как его избежать. Оскорбительные прозвища, насмешки, поддразнивание, пинки со стороны одного или группы учащихся в отношении одноклассника или одноклассницы являются признаками нездоровых отношений, которые могут привести к травле – регулярному, повторяющемуся изо дня в день издевательства. Регулярное и целенаправленное нанесение физического и душевного вреда стало объектом внимания ученых и педагогов, начиная с 70-х годов прошлого века, и получило специальное название – буллинг.

Буллинг (от англ. bully – хулиган, задира, грубиян, «tobully» – задираться, издеваться) – длительный процесс сознательного жестокого отношения, агрессивного поведения с целью причинить вред, вызвать страх, тревогу или создать негативную среду для человека.

По данным различных исследований, почти каждый третий ученик, так или иначе подвергавшийся буллингу в школе, страдал от унижений и

смеющихся: 10% - регулярно (раз в неделю и чаще); 55% – частично подвергаются издевательствам со стороны одноклассников; 26% – родителей считают своих детей жертвами буллинга.

В отношении профилактики кибербуллинга в домашней среде родителям следует предложить следующие рекомендации:

1. Не нужно наказывать ребенка, когда он доверился и рассказал о том, что стал жертвой кибербуллинга (или буллинга).
2. Ребенок уже пострадал, и если родители его не поддержат, в следующий раз он может не обратиться за помощью.
3. Полностью запрещая доступ ребенка к интернету (или к другому пространству в реальной жизни) вы добьетесь только того, что ребенок больше вам ничего не будет рассказывать.

В качестве основных мер отметим следующие:

- Важно, чтобы профилактические действия по внедрению правил или действию помощи в случае нападений, чтобы родители оказывали спокойно и уверенно, давая детям положительный эмоциональный ресурс защищенности, поддержки. Свое волнение и тревогу можно обсуждать с другими взрослыми, например другими родителями, дети которых были жертвами буллинга (программа действий школы может включать организацию таких встреч). Следует также поставить в известность педагогов, проинформировать о наличии проблемы, ведь это позволит им более внимательно и целенаправленно отслеживать ситуации традиционного буллинга, сочетание которого с кибербуллингом особенно опасно.

- Постигайте новые знания. Родители должны регулировать пользование ребенка новыми технологиями, чтобы не оставлять ребенка наедине с виртуальной реальностью, родители должны сами овладевать интернетом, учиться пользоваться планшетом или смартфоном и т.д. Вы же рассказываете о правилах дорожного движения и правилах пользования бытовой техникой? Не забывайте о правилах безопасности в Интернете.

- Будьте внимательны к ребенку внимательно выслушивайте ребенка относительно его впечатлений от интернет-среды обращайтесь внимание на тревожные признаки после пользования интернетом, которые могут указывать на то, что ребенок стал жертвой (расстроен чем-то, отказывается общаться и т.д.).

- Поддерживайте доверительные отношения с ребенком доступно расскажите ребенку о кибербуллинге, объясните свою мотивацию: вы заботитесь, а не пытаетесь контролировать частную жизнь подчеркните, что если ребенку поступают обидные письма, эсэмэски или возникают другие проблемы в интернете, он может рассчитывать на помощь родителей не нужно наказанием за посещение нежелательных сайтов лучше объяснить угрозу, которую несут эти сайты.

- Проводите ограниченный контроль. Можно отслеживать события онлайн-жизни ребенка через соцсети, наблюдать время от времени за реакциями ребенка, когда он в интернете. Чтобы предотвратить компьютерную

зависимость, регламентируйте время пользования интернетом, ведь дети часто теряют ощущение времени онлайн. .

- Применяйте технические средства безопасности для защиты от информационных угроз научите ребенка пользоваться специальными безопасными поисковыми системами можно использовать программы-фильтры родительского контроля, которые открывают доступ только к ограниченному перечню безопасных для детей и блокируют вредоносные сайты с недетским контентом (такие фильтры можно установить в операционной системе или в антивирусной программе).

- Формируйте коммуникативную культуру Разъясните ребенку, какое его собственное поведение будет считаться нормальным, а каким опасным или безответственным заметьте, что общение в интернете, как и в реальной жизни, должно быть ответственным: оно может иметь определенные последствия и для самого ребенка, и для людей, с которыми она общается в интернете, не стоит создавать вымышленные образы, негативно реагировать на каждое сообщение провокативного характера.

Советы психолога тем, кто стал жертвой кибер-травли

- Не стесняйтесь обратиться за помощью к людям, которым вы доверяете (ко взрослым, если Вы ребёнок).

- Не следует удалять оскорбительные сообщения. Вы можете не читать, но сохранить их в качестве доказательства травли.

- Не стоит отвечать на оскорбления. Ваши раздражённые ответы возбуждают агрессоров ещё больше и дают им чувство значимости и влияния. Помните: агрессия порождает агрессию.

- Заблокируйте отправителя оскорбительных сообщений.

- Сообщите о проблеме администрации сайта или модератору группы (чата и т. д.).

- Вы не можете контролировать действия тех, кто Вас травит, но Вы можете контролировать свою реакцию. Если они смогут вывести Вас из себя, они победили.

- Нужно быть юридически грамотными, уметь себя защищать и знать, что закон на Вашей стороне. Обидчик не останется безнаказанным.

В противодействии киберпреступности в отношении несовершеннолетних с использованием Сети, предлагаются меры:

- повысить эффективность научного обеспечения деятельности по противодействию киберпреступности в отношении детей и подростков с использованием киберпространства [34]

- совершенствовать систему правоприменения и разработать новые формы и методы борьбы с данным видом кибер-зла;

- с целью формирования у детей, подростков и молодежи духовно-нравственных качеств активизировать информационно-просветительскую работу, раскрывающую ценность семьи, как основы социализации и нормальной жизнедеятельности личности, а также пропаганду здорового образа

жизни в СМИ;

- на законодательном уровне предусмотреть уголовную и административную ответственность организаций провайдеров, за допущение распространения в сети Интернет порнографического контента и текстовых публикаций, пропагандирующих культ жестокости, насилия, наркомании, алкоголизма, сексуальной распущенности и скрытой рекламы проституции;

- в тесты полиграфических исследований лиц, поступающих на работу в государственные учреждения Министерств: образования, здравоохранения, культуры и спорта, в обязательном порядке включать вопросы на выявление склонности к педофилии. При положительном результате, под персональную ответственность осуществляющих проверку должностных лиц, информация должна в обязательном порядке направляться в правоохранительные органы;

- в целях ужесточения предварительной проверки всех категорий лиц, поступающих на работу в государственные учреждения Министерств: образования, здравоохранения, культуры и спорта, от технического персонала до руководителей, создать общедоступную Федеральную базу лиц, ранее судимых за преступления сексуального характера, совершенные в отношении несовершеннолетних;

- Минобрнауки России разработать систему обязательного тестирования учащихся школьными психологами на предмет выявления фактов возможного совершения в отношении несовершеннолетних действий сексуального характера с последующим обязательным информированием правоохранительных органов.

- ограничивать доступность несовершеннолетних к информационным порталам и ресурсам в сети Интернет, чем активно пользуются педофилы, втираясь к ним в доверие и т.д.;

- активизировать работу правоохранительных органов по инициативному выявлению преступлений данной категории не только в специализированных отделах, но и во всех оперативных подразделениях территориальных отделов внутренних дел, а также во всех регионах России;

- оживлять позиции отдельных граждан, сообщающих в правоохранительные органы о совершаемых или выявленных преступлениях.

- усилить законодательный уровень контроля за ранее судимыми, отбывавшими наказание за аналогичные преступления.

- изменить кадровые позиции на местах, как в количественном, так и качественном плане, так как это отражается на эффективности работы;

- наладить взаимодействие между оперативными и другими службами органов внутренних дел, в том числе с оперативными подразделениями;

- проводить эффективные профилактические работы со стороны подразделений полиции общественной безопасности в отношении лиц, ранее судимых, привлекавшихся к административной ответственности, злоупотребляющих алкогольными напитками, ведущих асоциальный образ

жизни, склонных к насилию над детьми;

- в полном объеме использовать возможности МВД;
- осуществлять качественный подбор специализированного аппарата по данной линии;
- организовывать должное оперативное прикрытие детских учреждений;
- проводить рабочие встречи, совещания и совместные научно-практические мероприятия в рамках межведомственного сектора с целью организации совместного контроля за ходом раскрытия киберпреступлений в отношении них с использованием сети Интернет;
- осуществлять работу по организации совместных разработок с региональными подразделениями уголовного розыска при постоянном взаимодействии с оперативными подразделениями
- при выездах в командировки организовывать совместные совещания, рабочие встречи для обеспечения постоянного обмена информацией между службами о нераскрытых киберпреступлениях против половой неприкосновенности несовершеннолетних и лицах, к ним причастных;
- разработать специальный алгоритм действий по использованию кибер-розыскных мероприятий в сети Интернет и их документированию, с целью оказания практической помощи регионам в раскрытии киберпреступлений в отношении детей и подростков и задержании лиц, их совершивших;
- принимать участие в заседании рабочей группы, сформированной в целях выработки мер по совершенствованию механизма выявления, предупреждения, пресечения и раскрытия преступлений, связанных с деятельностью лиц, склоняющих несовершеннолетних к суицидальному поведению посредством оказания психологического воздействия через Интернет и социальные сети

Также хочется отметить, что в настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния киберпреступности в отношении несовершеннолетних в сети Интернет, ни надежных методов сбора таких данных. И дело не только в отсутствии единообразия национального уголовного законодательства стран в сфере борьбы с киберпреступностью в отношении детей и подростков и разной практике его применения, различиях в формировании уголовной статистики и особенностях правоохранительной системы.

Наибольшая часть киберпреступлений в отношении несовершеннолетних с использованием интернет-пространства остается за рамками статистики — можно с уверенностью утверждать, что в официальные отчеты попадает лишь 30, в лучшем случае 40% совершенных преступных деяний. Это объясняется тем, что «потерпевшие — родители детей и подростков» предпочитают не сообщать в правоохранительные органы о совершенных в отношении их детей преступлениях, чтобы не придать огласки общественности и не попасть под обсуждения родственников, близких, друзей и т.д. Другие жертвы

киберпреступлений в отношении детей не сообщают о них, понимая, что найти виновных и компенсировать нанесенный ущерб будет очень сложно.

В настоящее время информационная безопасность в отношении несовершеннолетних рассматривается государствами, как одна из приоритетных задач в сфере национальной безопасности и международной политики, при этом концепция информационной безопасности детей включает как защиту пользователей сетей, так и защиту государства и его критических инфраструктур. Однако, поскольку ни одно государство не может защитить себя, принимая меры только на национальном уровне, для комплексного противодействия кибер- преступности в отношении детей и подростков необходимы:

- гармонизация уголовного законодательства о киберпреступлениях в отношении несовершеннолетних на международном уровне;
- разработка на международном уровне и имплементация в национальное законодательство процессуальных стандартов, позволяющих эффективно расследовать преступления в глобальных информационных сетях, получать, исследовать и представлять электронные доказательства с учетом трансграничности этих преступлений;
- отлаженное сотрудничество правоохранительных органов при расследовании киберпреступлений в отношении детей и подростков на оперативном уровне;
- механизм решения юрисдикционных вопросов в киберпространстве.

Таким образом, международное сотрудничество является ключевым моментом в ликвидации правового вакуума, существующего между развитием киберпреступности в отношении несовершеннолетних в сети Интернет и реагированием на них законодательства. Процесс выработки мер на международном уровне, как показывает опыт, сам по себе является комплексной проблемой. Однако это единственный путь надежной защиты от электронных посягательств и эффективной борьбы с киберпреступлениями данной категории.

Следует отметить, что понятие «вред» в контексте причинения вреда несовершеннолетнему с точки зрения законодательства может включать в себя целый ряд различных действий. Отдельной статьи, которая была бы посвящена исключительно нанесению вреда ребенку или подростку, в УК нет.

Основополагающими направлениями решения этой проблемы являются:

- разработка государственной политики предупреждения кибер правонарушений в отношении несовершеннолетних в сети Интернет, основные положения которых, должны быть закреплены законодательно, а также внести предложения по изменению законодательства по противодействию преступлений, связанных с информационно-телекоммуникационной сетью в отношении несовершеннолетних и педофилии;
- выработать предложения органам власти о создании онлайн-ового центра защиты детей от эксплуатации, который будет заниматься созданием

систем отслеживания сексуального домогательства и криминализированных деяний вне зависимости от страны, откуда они выходят в интернет, и предоставлять информацию властям;

- постоянно осуществлять взаимодействия органов внутренних дел со специалистами виртуального пространства и операторами связи, так как объем и содержание предоставляемых сведений о пользователях услугами интернета и связи, а также порядок обращения к профессионалам виртуального мира и операторам связи, не в полной мере позволяют органам внутренних дел эффективно и мгновенно реагировать, и решать поставленные перед ними задачи в борьбе с киберпреступностью в отношении детей и подростков с использованием Сети;

- поставить вопрос об отнесении применения интернет-технологий при совершении любых киберпреступлений в отношении несовершеннолетних к числу отягчающих обстоятельств, (обстоятельства, отягчающие наказания). Чтобы всякий раз, когда с помощью Интернета совершалось или организовывалось преступление в отношении ребенка либо облегчалось его совершение, это учитывалось при назначении наказания;

- должна быть введена персональная ответственность владельцев сайтов и социальных сетей за размещение информации, пропагандирующей либо облегчающей совершение суицида. При этом ответственность за подстрекательство к самоубийству с использованием Интернета не должна зависеть от наличия конкретных жертв. Напомним, что в настоящее время привлечь виновное лицо к ответственности можно лишь в том случае, когда удалось установить наличие с его стороны подстрекательных действий в отношении жертвы;

- разработать программы пред фильтрации для компьютеров детей и подростков, то есть автоматическое определение в режиме реального времени содержимого запрашиваемой пользователем страницы и ее оценка — если интернет- страница содержит запрещенную информацию, система автоматически ее блокирует.

В рамках основополагающего и комплексного подхода к борьбе с киберпреступностью в отношении несовершеннолетних в киберпространстве должны решаться следующие общие и частные научно-практические задачи:

1. Выявление объективных закономерностей, причин и условий кибернасилия над детьми. Акцент должен быть сделан на фиксацию динамики и прогностическую составляющую познания, так как только такой подход способен реально формировать комплекс профилактических мероприятий и, в конце концов, привести к тому, что основным полем деятельности законодательной власти и правоохранительных органов станет не расследование совершенных киберзлодеяний, а их предотвращение.

2. Создание единого информационно-координационного центра, ведущего сбор, анализ и переработку информации. Данный центр должен работать в тесном контакте и взаимодействии с законодательными, исполнительными, судебными структурами, общественными организациями,

средствами массовой информации и т.д.

3. Разработка и постоянное совершенствование методик выявления и расследования подобных преступлений. Взаимодействие с правоохранительными органами в данном контексте должно осуществляться как в форме непосредственного внедрения методик в аналитическую, оперативно-розыскную и следственную деятельность, так и через создание системы специализированных учебных заведений и курсов переподготовки, повышения квалификации действующих сотрудников.

Борьба с преступными проявлениями подразумевает различные подходы.

Просматриваются два принципиальных направления:

1) максимально эффективное предупреждение, профилактика, предотвращение самой возможности правонарушений в Сети в отношении детей и подростков;

2) ориентация на выявление и пресечение совершенных преступных кибердеяний в отношении несовершеннолетних.

Данный вид киберпреступности, является тем преступлением, которое можно и нужно пытаться предотвратить. Следовательно, основные усилия в борьбе с этим криминальным злом необходимо направить на создание максимально неблагоприятных условий для совершения киберправонарушений.

Если говорить о видах интернет-преступности в отношении детей, то с точки зрения борьбы с ним следует выделить два уровня противодействия. Первый уровень связан с комплексом мероприятий, всячески сужающих пространство для кибер-насилия и затрудняющих (или делающих невозможным) его осуществление. Этот комплекс мер в большей своей части направлен против всех видов кибернасилия в отношении детей. Второй уровень противодействия связан с учетом специфики конкретных видов кибернасилия и подразумевает направленную детализацию законодательных, правоохранительных и информационно-общественных мер.

Первый уровень мер противодействия может включать в себя следующие крупные направления работы: научно-исследовательское, законодательное, инструктивно-нормативное, правоохранительное, корпоративное, общественно-информационное, индивидуальное.

1. Научно-исследовательское направление. Работа в данной сфере связана с целым рядом задач, включающих в себя сбор информации, ее аналитическую обработку и классификацию, определение на этой основе реальной картины состояния дел и перспективное прогнозирование развития ситуации. Эта работа имеет смысл лишь при четкой интеграции ее результатов в законодательную деятельность и правоохранительную практику. Законодательные предложения, анализ применения действующего законодательства, экспертиза законов и в целом весь круг правового обеспечения противодействия мошенничеству чрезвычайно важно организовать как единый, иерархически выстроенный, компетентный и, в случае необходимости, быстродействующий механизм.

Важно обеспечить также максимально эффективную работу по

взаимоувязыванию различных отраслей законодательства и координацию законотворчества и правоприменения на европейском и мировом уровнях, в рамках двусторонних и многосторонних межгосударственных соглашений, договоров, конвенций и т.д.

Первыми шагами в этом направлении должны стать:

- комплексная экспертиза с участием ученых и практических работников законодательства на предмет максимально возможного сокращения возможностей для кибердеяний в отношении ребенка;
- согласование законодательства с международным (прежде всего, связанным с пресечением трансграничного кибер насилия детей), в том числе проведение мероприятий по реализации в России положений Европейской Конвенций, Доктрин, Деклараций и других правовых законодательств.

Необходимо продумать систему правовой ответственности субъектов сети Интернет (владельцев сайтов, доменов) вне зависимости от их гражданства и страны проживания [35]

Важным результатом научно-исследовательской работы является адаптированный перенос ее результатов в практику работы всей правоохранительной системы. Тесная координация здесь должна осуществляться уже на этапе сбора информации (в частности, регистрации киберпреступлений в отношении детей и подростков, получение оперативной информации, сигналов и т.д.). Отсюда же вытекает настоятельная потребность максимально широкого оповещения общества о результатах изучения феномена кибернасилия через самые разные каналы: средства массовой информации, Интернет, образовательные учреждения, общественные организации и т.д.

2. Законодательное направление включает в себя создание и постоянное совершенствование законодательных норм по борьбе с киберпреступностью в отношении несовершеннолетних с использованием сети Интернет. Здесь также выделяется несколько принципиальных аспектов: унификация и кодификация понятий, определений и терминов, связанных с фиксацией кибер-действий и борьбой с ним; создание норм права и правовых механизмов, в максимальной степени сужающих пространство для кибернасилия в отношении подростков. Гибкость законодательства должна обеспечивать дифференцированный подход к назначению наказания.

3. Инструктивно-нормативное направление представляется наиболее быстродействующим, точечно-направленным инструментом противодействия киберпреступности в отношении несовершеннолетних. Подзаконные акты и различного рода инструктивно-регламентирующие документы в силу своей специфики могут и должны оперативно менять ситуацию в случаях, когда законодатель проявляет медлительность, и в то же время на практическом уровне способствовать максимально эффективному применению законодательных норм. В силу разнородности нормативной базы (государственных учреждений, коммерческих структур, общественных организаций и т.д.) очень важна взаимосогласованность при создании регламентирующей документации. Барьер ведомственности в значительной

степени играет на руку кибернасилие. Именно несогласованность в этой сфере часто порождает возможности для преступных комбинаций. Устранение такого барьера заметно сужает поле для киберпедофильных посягательств.

4. Правоохранительное направление является ведущим элементом реализации мер по пресечению интернет-преступности в отношении детей и подростков. В силу внутренней структуры правоохранительных органов возникает проблема координации, с одной стороны, внутриведомственных подразделений, с другой стороны — межведомственных. Значительное число кибердействий к детям, как указывалось в предыдущих разделах, носит многоэпизодный и трансграничный характер. Однако, зачастую кибернасилие в отношении несовершеннолетних квалифицируется по разным статьям Уголовного кодекса. Сложившаяся практика свидетельствует о том, что киберпедофильные действия выявляются в ходе работы разных территориальных и функциональных оперативных служб.

Из выше сказанного можно сделать вывод, что предупреждение, выявление и профилактика преступлений, совершаемых в отношении несовершеннолетних с использованием сети Интернет, требуют постоянного совершенствования и тщательной коррекции в зависимости, как от общей ситуации, так и в соответствии с частными случаями.

Расследование уголовных дел по данному направлению целесообразно сосредотачивать у наиболее подготовленных, высококвалифицированных сотрудников, что позволит в дальнейшем самосовершенствоваться и специализироваться с учетом их ошибок и недочетов, с целью повышения их квалификации в раскрытии и расследовании киберпреступности в отношении детей и подростков с использованием сети Интернет. [36]

В литературе содержится большое количество работ о буллинге, а также о практических шагах, которые могут быть предприняты родителями и учителями для снижения частоты и распространенности такого поведения. Некоторые работы исходят из англоязычной среды и были разработаны в контексте социальных норм и моделей поведения в западных обществах. Тем не менее, многие из рекомендуемых средств борьбы с издевательствами выходят за рамки культурных границ.

Детям следует привить один принцип, что они не умеют размещать неблагоприятные вещи; Интернет-среда позволяет хулиганам оставаться анонимными. Поскольку они анонимны, они не боятся наказания, потому что им не приходится сталкиваться со своими жертвами. Родители и учителя должны знать об этом аспекте кибербуллинга, поскольку у хулигана мало стимулов прекратить свое поведение. Наилучший подход может заключаться в том, чтобы побудить жертву покинуть онлайн-платформу, используемую агрессором, поэтому родители и учителя должны научиться пользоваться Интернетом и понимать свои возможности.

Другими словами, они должны быть в состоянии обеспечить информированное и компетентное руководство и руководство для детей, которые склонны стать киберхулиганами, а также для тех, кто может стать

жертвой такого поведения; Родители и учителя должны убедиться, что дети и подростки понимают, что они могут обратиться к взрослым в своей жизни, если они подвергаются кибербуллингу. В случае жестокого обращения в Интернете, кибербуллинга, киберпреследования или приближения хищника ребенка предупреждают, чтобы он сообщил об этом своим родителям. Они должны понимать, что на них никто не будет сердиться, а взрослые, занимающие руководящие должности, хотят помочь; Учителя должны внимательно следить за онлайн-отношениями и всегда в социальных сетях. Их также просят помочь учителям искоренить неуважительный и жестокий контент.

Детей следует поощрять документировать любые случаи кибербуллинга, с которыми они сталкиваются, а также прививать один принцип, что они не умеют публиковать неблагоприятные истории, что Интернет-среда позволяет хулиганам оставаться анонимными. Поскольку они анонимны, они не боятся наказания, потому что им не приходится сталкиваться со своими жертвами. Родители и учителя должны знать об этом аспекте кибербуллинга, поскольку у хулигана мало стимулов прекратить свое поведение. Наилучший подход может заключаться в том, чтобы побудить жертву покинуть онлайн-платформу, используемую агрессором; Родители и учителя должны научиться пользоваться Интернетом и понимать свои возможности.

С другой стороны, школа должна быть в состоянии обеспечить информированное и компетентное руководство для родителей и для детей, которые склонны стать киберхулиганами, а также для тех, кто может стать жертвой такого поведения; Родители и учителя должны убедиться, что дети и подростки понимают, что они могут обратиться к взрослым в своей жизни, если они подвергаются кибербуллингу. В случае дома детей и подростков следует поощрять использовать социальные сети среди остальных членов семьи, а не наедине. Он может служить сдерживающей силой злонамеренного поведения и способствовать снижению распространенности кибербуллинга; Родители и учителя должны поощрять детей сообщать о любых ситуациях, когда друг или сверстник подвергается кибербуллингу, чтобы это могло быть расследовано; Родители и учителя должны следить за тем, чтобы дети понимали, что кибербуллинг опасно и может нанести реальный вред жертве. Часто это незаметно из-за «нереального» характера онлайн-взаимодействия;

Хотя дети и подростки имеют право на определенную степень конфиденциальности в Интернете, родители по-прежнему обязаны знать и понимать, что их дети делают в цифровой среде. Крайне важно найти баланс между вмешательством и надлежащим мониторингом участия детей в онлайн-мероприятиях.

Среди образовательных технологий в последние два десятилетия особую актуальность приобрели социально-воспитательные технологии, что напрямую связано с современными вызовами развития государственного образовательного пространства и устойчивым социально-экономическим кризисом в российском обществе, поскольку технологии социального воспитания – это группа социальных технологий, ориентированных на

осуществление важнейшей функции общества – подготовку подрастающих поколений к включению в общественную жизнь, к социально- нормированному функционированию в социуме.

В свою очередь социально-воспитательная технология – это обоснованная на основе педагогической диагностики система, в которой реализуется алгоритм последовательных операций для обеспечения гармоничного взаимодействия личности с социальной средой. Основными компонентами системы являются целеобразование, диагностические процедуры, выбор способов действия и их инструментария, оценка результатов деятельности.

Следует отметить, что на сегодняшний день отсутствует устоявшаяся классификация социально-воспитательных технологий. В научном обращении встречается широкое разнообразие указанных технологий, которые условно можно отнести к следующим группам: технологии семейного воспитания; технологии дошкольного воспитания; технологии социально-педагогических комплексов; технологии дополнительного образования; технологии трудового, профессионального воспитания и образования; технологии работы с трудновоспитуемыми детьми; технологии социально-педагогической реабилитации и поддержки детей с ограниченными возможностями развития; технологии реабилитации детей с нарушением социальных связей и отношений; технологии установления связей с общественностью.

Цели и задачи проекта

Целью проекта является предоставление информации и получение навыков решения существующих проблем старшеклассников, прежде всего явления кибербуллинга, посредством использования методики форум-театра.

Реализация поставленных целей предполагает решение следующих задач:

1. Выбор общеобразовательного учебного заведения, в котором будет внедряться проект.
2. Подбор и разработка диагностического материала для выявления и оценки уровня проявлений буллинга среди старшеклассников.
3. Подготовка сценариев для проведения форум-театра.
4. Информирование учащихся о внедрении проекта.
5. Создание благоприятного социально-психологического климата и установление положительного эмоционального контакта со старшеклассниками для проведения форум-театра.

Ожидаемые результаты проекта

Внедрение проекта будет эффективным в том случае, если:

- уменьшится количество участников буллинга и жертв данного явления;
- у учащихся будет сформировано видение буллинга как негативного явления, они поймут всю суть его деструктивных последствий, как для самого агрессора, так и для жертвы травли.
- старшеклассники осознают то, что только они несут ответственность

за свои действия;

- учащиеся получают опыт разрешения сложных жизненных ситуаций;
- старшеклассники будут осведомлены о том, куда обращаться за помощью в случае школьных издевательств.

Этапы реализации проекта «Стоп кибербуллинг!» табл. 1

Название этапа	Срок этапа	Содержание работы
Подготовительный	Январь- февраль 2022год	Построение плана действий. Накопление материалов, подтверждающих актуальность проблемы. Разработка проекта. Выбор учебного заведения для его внедрения.
Организационный	Март – апрель 2022 год	Обобщение и систематизация собранного материала на предварительном этапе. Планирование деятельности. Выбор наиболее эффективных способов достижения целей. Подбор и разработка диагностического инструментария по изучению уровня проявлений кибербуллинга среди старшеклассников. Создание сценариев для форум-спектаклей.
Процедурный (реализация проекта)	Апрель – май 2022 год	Установление контакта и налаживание взаимодействия с участниками проекта. Проведение лекции по теме: «Что такое кибербуллинг в школе и как с ним бороться». Проведение диагностики уровня распространения кибербуллинга среди старшеклассников. Создание и реализация спектаклей форум-театра. Мониторинг процесса и результатов осуществления проекта.
Аналитический	Сентябрь-ноябрь 2022год	Диагностика и анализ результатов внедрения проекта; планирование дальнейшей работы по организации и популяризации форум-театра среди учащейся молодежи.

Программа реализации социального проекта «Стоп кибербуллинг!»
табл.2

/п	Название	Формы и методы	Срок выполнения
	Исследование уровня распространения буллинга в травля и травля в интернете», среде старшеклассников, Авторская анкета «Буллинг и их проявлений агрессивности среди проявления в учащейся среде». Апрель 2022 год них, воздержания и Методика «Агрессивное поведение» несдержанности, а также (По Е. Ильину и П. Ковалеву). стратегий поведения в «Диагностика склонности к конфликтных ситуациях. конфликтному поведению» (Адаптация Н.В. Гришиной).		

Ознакомление старшекласников с понятием буллинг, его особенностями, причинами и последствиями, сопровождающими данное явление. А также сообщения информации, что делать и куда обращаться, если стали жертвой травли.	Лекция по теме: «Что такое кибербуллинг в школе и как с ним бороться»	Апрель 2022 год
Подготовка форум-спектаклей	Выбор темы спектакля; определение сюжетной линии; распределение ролей и их обсуждение	Апрель 2022 год
Проведение форум-спектаклей	1. Информационная беседа «Форум - театр: возможности и особенности»; 2. Проведение разогрева – упражнения направленные на формирование доброжелательной атмосферы среди зрителей и актеров 3. Показ форум спектакля учащимися 10 класса «Чучело Online»; 4. Показ форума учащимися 11 класса «А могло все быть иначе»; 5. Форум со зрителями	Апрель – май 2022 год
Мониторинг эффективности внедрения проекта и оценка результативности проделанной работы; планирование дальнейшей работы	Проведение опроса среди участников форума по эффективности его деятельности, подведение итогов.	Май 2022 год

Для реализации проекта «Стоп Кибербуллинг» требуется привлечение таких личностных ресурсов как: творческий потенциал старшекласников, материально технические информационные, человеческие (педагоги, классные руководители социальный педагог).

Для повышения эффективности предлагаемых мер необходимо приглашать родителей через просветительскую деятельность. Пример первичного родительского собрания представлен в приложении 1, где обосновывается понятие буллинга и даются общие рекомендации по его профилактике. В отношении школьных мер предлагается составить следующий план на год (приложение 2), а краткий перечень базовых мер возможно обозначить следующим образом:

- Сотрудники школы осуществляют регулярный надзор (мониторинг) в школьных коридорах и зонах совместного пользования (спортивных залах, игровых зонах, рекреациях).
- Использование Интернета в школе максимально управляемо. Установлены фильтры и списки ограниченных сайтов и контента.

- Ученику покидать территорию школы по прибытии и до окончания уроков согласно расписанию занятий можно только при соответствующем заявлении родителей и с согласия администрации школы.

- Школа обучает персонал навыкам ненасильственного общения в виде лекций, тренингов, практических занятий.

- В образовательную программу включены профилактические тренинги, психологически ролевые игры по темам толерантности, профилактики конфликтов и буллинга. Классный руководитель постоянно влияет на социально психологический климат класса.

- Классный руководитель планирует и проводит командо образующие игры, занятия и упражнения среди учащихся.

- Школьный психолог ведет регулярную коррекционную работу в течение учебного периода с классами, отдельными группами детей, отдельными детьми по соблюдению ими толерантности, избеганию проявлений насильственного поведения.

- Школьный психолог, согласно утвержденному плану работы, исследует психологический климат в классе, групповую динамику класса, эмоциональное состояние учащихся, проводит социометрию для получения информации о взаимоотношениях среди детей. Полученную информацию использует для формирования и коррекции работы психолога с классом.

- Школьный психолог путем наблюдения и анализа распознает у учащихся и работников школы проблемы в межличностном общении адаптации к учебному коллективу и оказывает им своевременную социально-психологическую помощь.

- Школа проводит просветительскую работу с родителями по избежанию и распознаванию насильственного поведения к ребенку/ребенку, помочь ребенку в случае проявлений буллинга в рамках «Школы положительного отцовства».

- В начале учебного года каждый классный руководитель проводит 3 занятия, посвященные профилактике буллинга и насилию. На первом – знакомит с Антибуллинговой политикой, на остальных – прорабатывает с детьми разные схемы действий в той или иной ситуации.

- В начале учебного года (в течение августа) для работников школы школьный психолог и заместитель директора школы по воспитательной работе проводят ознакомительную встречу по Антибуллинговой политике школы и дают четкие инструкции и разъяснения относительно противодействия, реагирования и профилактики насильственного поведения в школе.

- В начале учебного года в родительских группах классов в социальной сети размещается для ознакомления краткое извлечение из Антибуллинговой политики школы.

- В октябре в школе проходит просветительский семинар для родителей школы для ознакомления со стратегиями родительского поведения в тех или иных неприемлемых ситуациях.

- Психолог школы постоянно интересуется информацией о возможных

других профилактических мероприятиях, а также методах работы как с обидчиками, так и с жертвами буллинга, проводят самостоятельно или приглашают внешних специалистов для обучения школьного персонала практикам профилактики буллинга и работы со случаями буллинга.

- На сайте школы размещен выписка из Антибуллинговой политики заведения.

Таким образом, нами была составлена программа социальной профилактики кибербуллинга для школьников, которая содержит в себе меры для нескольких целевых аудиторий – школьников, родителей и учителей.

В рамках пробного мероприятия, нами был проведен первичный комплекс просветительского характера, состоящий из лекций по просвещению учителей, родителей и школьников. Для того чтобы оценить привлекательность подобных мер, мы провели социологическое исследование в рамках первичной выборки школьников (50 человек), учителей школы (20 учителей) и родителей учеников (100 человек). Нами были получены следующие результаты.

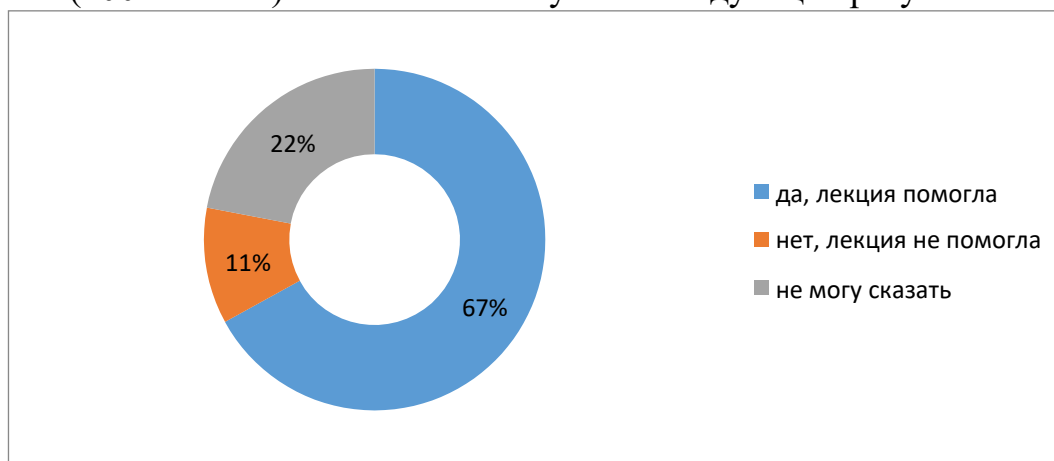


Рисунок 1. – Результаты удовлетворенности обучающихся

На основании рисунка видно, что большинство школьников отметили, что для них проведенные лекции оказались эффективными, где более 65% учеников отметили, что смогли переоценить текущую ситуацию в их классе в отношении одноклассников или же себя самих, а 22% не смогли оценить полезности мероприятий для себя в силу замкнутости, например, или же неготовности поделиться собственным опытом (что в дальнейшем будет передано психологу и классному руководителю для дальнейшего наблюдения). 11% школьников ответили негативно о проведенных мероприятиях, так как либо уже сталкивались с подобной ситуацией либо являлись ее активным участников (наблюдателем, например).

В отношении эффективности мероприятий для учителей нами были получены следующие данные.

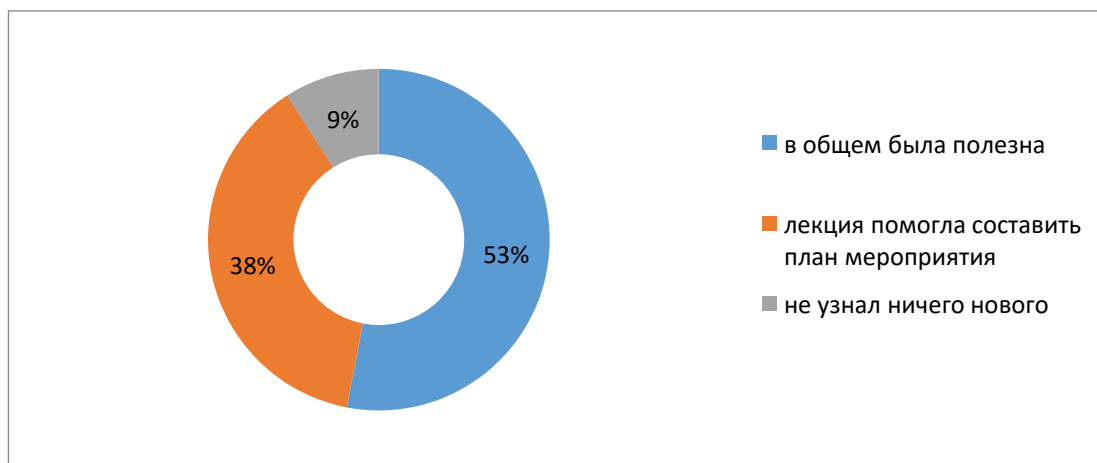


Рисунок 2. – Результаты оценки эффективности мероприятий для педагогов.

На основании рисунка видно, что для большинства учителей подобные меры носят положительный эффект, так как более 50% учителей сказали, что в общем информация носила полезный характер, с которой они были знакомы ранее в теории и практике своей работы. Для практически 40% учителей подобные мероприятия помогли составить конкретный перечень мер в своей работе или же акцентировать внимание на отдельных вопросах в поведении их учеников, что также следует считать положительной стороной, а для менее чем 10% учителей данные мероприятия не соответствовали ожиданиям ввиду уже знакомой для них информации или же отсутствия мер помощи для их практики в профилактике буллинга.

Наконец, рассмотрим результаты исследования по выборке родителей.

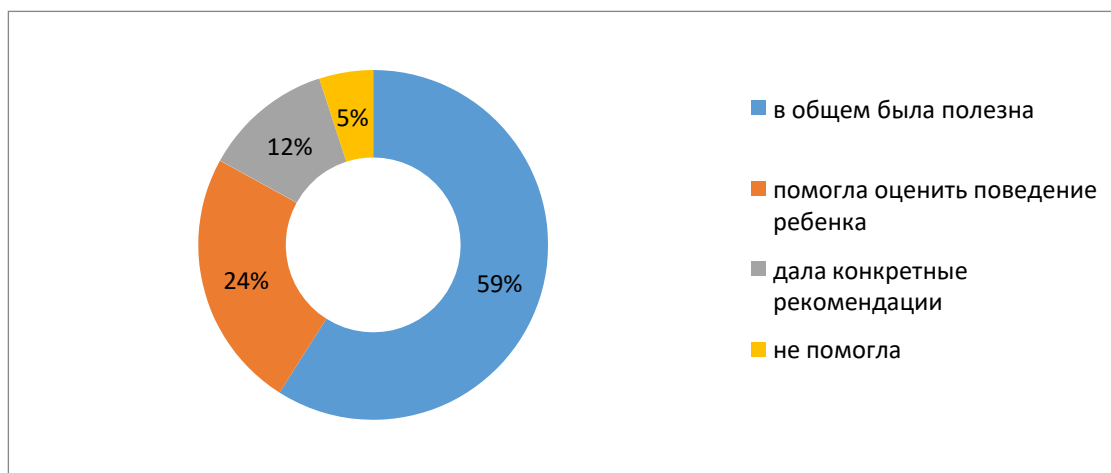


Рисунок 3. – Результаты оценки эффективности мероприятий для родителей

На основании рисунка видно, что для родителей в большинстве случаев проведенные мероприятия также носят положительный эффект, так как родители смогли переосмыслить поведения своего ребенка-подростка (практически четверть выборки – 24%), а для 12% найти определенные инструменты диагностики и профилактики буллинга для их ребенка в кругу семьи. Только 5% родителей отметили, что для них данная тема не носила актуальный характер ввиду уверенности в своем ребенке (3%) или же

уверенности, что это проблема школы (2%). Помимо этого, большинство родителей отметили, что готовы участвовать дальше в подобных мероприятиях.

Таким образом, разработанные нами меры являются эффективными.

Вот 10 базовых приемов информационной безопасности, о которых нужно знать и говорить детям и подросткам. Основные приемы кибергигиены для детей и взрослых включают:

1. Следите за тем, чтобы ваш смартфон не попадал в руки к незнакомцам, которым якобы необходимо сделать срочный звонок. Если у незнакомого человека появится доступ к вашему разблокированному гаджету – это может быть чревато проблемами.

2. Пользуйтесь длинными и надежными паролями, биометрией и двухфакторной аутентификацией при проведении платежей, совершении операций с деньгами. Применение удобных паролей, которые состоят из 3-4 букв, может плохо закончиться.

3. Поменьше распространяйтесь о себе в сети. Не предоставляйте незнакомцам лишней информации. Мошенники могут воспользоваться полученными сведениями и совершить на вас атаку.

4. Отклоняйте запросы на дружбу в соц. сетях. Такая опрометчивость может привести к валу рекламной рассылки и это только один из неблагоприятных сценариев развития событий.

5. Контролируйте установленные на смартфоне приложения, следите за тем, к чему они имеют доступ. Новой игре ни к чему знать ваше местонахождение или обладать доступом к камере.

6. Не забывайте обновлять программы и ПО на всех устройствах. Их создатели не зря трудятся, в обновленных версиях меняется не только дизайн, они становятся менее уязвимыми к атакам злоумышленников.

7. Осторожно открывайте письма, приходящие на электронную почту, если те поступают с незнакомых адресов. Это может быть чревато заражением.

8. Аккуратно пользуйтесь публичными сетями Wi-Fi, когда обращаетесь к мобильному банку. В отелях и прочих местах отдыха часто можно встретить тех, кто стремится к легкой наживе.

9. Не устанавливайте «поломанное» ПО с ненадежных ресурсов.

10. Контролируйте покупки, которые ваш ребенок совершает в интернете. Если в семье есть ребенок, установите на его телефон приложение родительского контроля. При наличии такой программы вы сможете не волноваться за безопасность своего чада, когда тот находится в сети. Такие программы позволяют предотвратить посещение ребенком нежелательных сайтов, ограничит время его пребывания в интернете. Поможет обеспечить цифровую безопасность, защитить персональные данные. Полезные материалы для подготовки уроков и мероприятий, посвященных Интернет-безопасности школьников. (приложение 8)

Заключение

Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Интернет-зависимость — это навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. В частности, некоторые учащиеся настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день.

Задача педагогов в связи с имеющимися рисками состоит в том, чтобы указать на эти риски, предостеречь от необдуманных поступков, сформировать у учащихся навыки критического отношения к получаемой в Интернете информации, воспитать культуру безопасного использования Интернет. Также следует обратить внимание на гигиенические требования, которые необходимо соблюдать при работе с компьютером:

- школьникам среднего и старшего возраста можно проводить перед монитором до двух часов в день, устраивая 10-15-минутные перерывы каждые полчаса;

- ребенок младшего возраста может находиться за компьютером не более 15 минут в день, в условиях классно-урочной деятельности – не более одного урока, а при наличии противопоказаний офтальмолога – только 10 минут, не более 3 раз в неделю;

- лучше работать за компьютером в первой половине дня;

- комната должна быть хорошо освещена;

- при работе за компьютером следить за осанкой, мебель должна соответствовать росту;

- расстояние от глаз до монитора – 60 см;

- периодически делать зарядку для глаз.

В соответствии с федеральными государственными образовательными стандартами общего образования в структуру основной образовательной программы основного общего образования включена программа воспитания и социализации учащихся, которая содержит такое направление, как формирование культуры здорового и безопасного образа жизни. В рамках этой программы может осуществляться информационно-просветительская работа среди школьников, пропагандирующая важность владения навыками безопасной работы в сети Интернет.

Для того чтобы повысить эффективность предложенных мер, нами был составлен план работы в отношении профилактики кибербуллинга в школьной среде для учителей, то есть со стороны школы, которая содержит в себе мероприятия для учителей, родителей и школьников. Основными средствами ее реализации выступают беседы, лекции, вебинары и тренинги.

Список использованных источников

1. Смагулова Ш., Байтугелова Н., Наурызбаев Т. Информационная безопасность детей: Проблемы и пути решения./ Пособие для педагогов, психологов, родителей и всех заинтересованных сторон. Астана, 2010 г. <http://www.balakkk>.
2. <https://factcheck.kz/nauka/media-i-informacionnaya-gramotnost-shkolnikov-kazahstana-rezultaty-issledovaniya>
3. Доклад Объединенной инспекционной группы «Кибербезопасность в организациях системы ООН. Женева 2021 г.
4. <https://factcheck.kz/nauka/media-i-informacionnaya-gramotnost-shkolnikov-kazahstana-rezultaty-issledovaniya>
5. Уголовный кодекс Российской Федерации. ст. 159.6
6. Мишина М. М., Воробьева к. А. Психологические особенности личности участников кибербуллинга в популярных социальных сетях УДК 159.9 Психологические науки. Вестник московского государственного областного университета. № 3.2020г. DOI: 10.18384/2310-7235-2020-3-29-43
7. Шумакова Е. В. Воспитательное пространство социальных сетей интернета // Профессиональное образование. Столица. 2011. № 6. С. 39–40.
8. Лоренц, К. Агрессия / К. Лоренц. – М.: Прогресс. Универс, 1994. – 272 с.].
9. Капиренкова О.Н. Современное понимание буллинга в школе // Евразийский союз ученых (ЕСУ) – 2020 - № 6 (75) – С.58-62].
10. Асмолов А. Г., Семенов А. Л., Уваров А. Ю. Российская школа и новые информационные технологии: взгляд в следующее десятилетие. М., 2010. 84 с.с. 68. <https://factcheck.kz/nauka/media-i-informacionnaya-gramotnost-shkolnikov-kazahstana-rezultaty-issledovaniya>
11. Ефремова Г. Инновационные технологии в современном образовательном пространстве: коллективная монография / Под общ. редакцией Г.Л. Ефремовой. – Сумы: Изд-во СумГПУ имени А. С. Макаренко, 2020. – 444 с.
12. https://www.mindmeister.com/ru/12485180/_?fullscreen=1
13. <https://pyatigorsk.org/22665>
14. © www.pyatigorsk.org
15. <https://www.mindmeister.com/ru>
16. <http://dod-piligrim.ru/wp-content/uploads/METODICHESKIE-REKOMENDATSII-PEDAGOGAM-po-formirovaniyu-informatsionnoj-bezopasnosti-u-detej-i-podrostkov.pdf>
17. <https://namib.online/2023/09/programma-xvii-mezhdunarodnogo-foruma-partnerstvo-gosudarstva-biznesa-i-grazhdanskogo-obshhestva-pri-obespechenii-mezhdunarodnoj-informatsionnoj-bezopasnosti/>
18. Электронный ресурс]. URL: <https://kiberbulling.net/> (дата обращения: 15.04.2020).

19. <https://www.unodc.org/unodc/ru/frontpage/2017/September/how-the-uns-cybercrime-unit-is-helping-to-track-paedophiles-and-protect-children.html>
20. <http://detionline.com> — главная страница,
<http://detionline.com/internet-project/about>
<http://detionline.com/assets/files/research/BookTheorye.pdf> — теория,
http://detionline.com/assets/files/research/Book_Praktikum.pdf — практика
21. www.razbiraeminternet.ru/teacher.
22. https://edu.tatar.ru/upload/images/files/children_health_and_care_in_it.pdf
23. <http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx>,
<http://www.microsoft.com/ru-ru/security/default.aspx>.
24. <http://www.mindmeister.com/ru/12485180/>
25. <http://www.dinkypage.com/ita42>
26. <http://www.oszone.net/6213/>
<http://www.microsoft.com/ruru/security/familysafety/childsafetyinternet.aspx>
<http://sch730.edusite.ru/p158aa1.html>
<http://wiki.pippkro.ru>
<http://lavandamd.ru>
<http://rovit.rxfly.net/stati/seti/69bezopasnyjinternetdljadetejiihroditelej.html>
www.cursedgames.com/vkuszdorovya.ru
www.cifrovik.ru
www.consumerclub.com.ua/demanrus.ru
www.azbykamam.ru
27. <http://www.etiket.ru/contact/email.html>
28. http://rusbatya.ru/index.php?option=com_content&task=view&id=220
ИД «Собеседник» <http://www.sobesednik.ru>
[/archive/sb/39_2008/children_nongrata/](http://archive.sb/39_2008/children_nongrata/)
29. <http://www.nestor.minsk.by/kg/2006/33/kg63308.html>
30. <http://www.microsoft.com/rus/protect/family/guidelines/rules.msp>
31. Сайт «Ребенок в сети» <http://www.detionline.ru/index.html>
32. Сайт пословиц <http://allproverbs.ru/>
33. <http://detionline.com/helpline/rules/parents>
34. Аносов А.В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий. М., 2018.
35. Эффективное предупреждение преступности: в ногу с новейшими достижениями / Материалы Десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями: А/CONF.187/10. Вена.
36. Предварительное следствие. 3-е изд., перераб. и доп. Учебник. Под ред. М.В. Мешкова. 2019 г. 575 с.
37. Гриф МУМЦ «Профессиональный учебник». Гриф НИИ образования и науки.

Список дополнительной литературы, используемый в материалах.

1. Фонд Развития Интернет в рамках выполнил проекта «Поколение Z: информационно-коммуникационные технологии как культурное орудие развития высших психических функций» при поддержке Российского фонда фундаментальных исследований подготовил публикации:
2. Солдатова Г.У., Ярмина А.Н., Темежникова О.Б., Особенности идентичности и социально-психологической адаптации участников буллинга и кибербуллинга, Академический вестник, Государственное бюджетное образовательное учреждение высшего образования Московской области «Академия социального управления», Москва, 2017, 3, 25, 38 — 50.
3. Солдатова Г.У., Трифонова А.В., Медиамногзадачность: стоит ли беспокоиться? Дети в информационном обществе, Фонд Развития Интернет, Москва, 2017, 3, 28, 26 — 37.
4. Солдатова Г.У., Теславская (Олькина) О.И., Видеоигры, академическая успеваемость и внимание: опыт и итоги зарубежных эмпирических исследований детей и подростков, Современная зарубежная психология, МГППУ, Москва, 2017.
5. Солдатова Г.У., Львова Е.Н., Чигарькова С.В., Онлайн-агрессия и подростки: результаты исследования школьников Москвы и Московской области, Международный научно-практический журнал «Эпоха науки», Москва, 2017, 12, 104 — 109.
6. Солдатова Г.У., Ртищева (Журина) М.А., Серёгина В.В., Онлайн-риски и проблема психологического здоровья детей и подростков, Академический вестник, Государственное бюджетное образовательное учреждение высшего образования Московской области «Академия социального управления», Москва, 2017, 3, 25, 29 — 37.
7. Солдатова Г.У., Теславская (Олькина) О.И., Видеоигры в фокусе науки, Дети в 33Отчет о деятельности Фонда Развития Интернет | 20.02.2018 информационном обществе, Фонд Развития Интернет, Москва, 2017, 27, 22 — 35.
8. Солдатова Г.У., Трифонова А.В. Поколение Z в формате многозадачности и вопросы адаптации к цифровой среде, КОМПЛЕКСНЫЕ ИССЛЕДОВАНИЯ ЧЕЛОВЕКА: ПСИХОЛОГИЯ МАТЕРИАЛЫ VII СИБИРСКОГО ПСИХОЛОГИЧЕСКОГО ФОРУМА, Томский государственный университет, Томск, 2017, 208 — 211.
9. Солдатова Г.У., Рассказова Е.И. Мотивация в структуре цифровой компетентности российских подростков, Национальный психологический журнал, Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В. Ломоносова» Факультет психологии, Москва, 2017, 1, 25, 3 — 14.
10. Солдатова Г.У., Теславская О.И. Особенности межличностных отношений российских подростков в социальных сетях. Национальный психологический журнал, 2018, 31 - 3, 12-22
11. Солдатова Г.У., Ртищева М.А., Теславская О.И.. Особенности использования цифровых технологий дошкольниками и младшими

школьниками. Психология человека как субъекта познания, общения и деятельности / Отв. ред. В. В. Знаков, А. Л. Журавлёв., 2018, 2195-2201

12. Солдатова Г.У., Ртищева М.А., Теславская О.И.. Мой электронный друг. Дети в информационном обществе. , 2018, 29, 38-43

13. Солдатова Г.У., Теславская О.И.. Оптимальные родительские стратегии регуляции использования детьми видеоигр. Сборник материалов VI Межрегиональной научно-практической конференции ДИАЛОГ-ONLINE, 2018, 9-12

14. Солдатова Г.У., Вишнева А.Е. Особенности выполнения когнитивных задач детьми с разной интенсивностью использования цифровых устройств. Психическое здоровье и образование: сборник научных статей по материалам II Конгресса «Психическое здоровье человека XXI века », 2018, 315-319

15. Солдатова Г.У., Львова Е.Н., Пермякова И.Д.. Феномены традиционного буллинга и кибербуллинга: сходства и различия. Цифровое общество как культурно-исторический контекст развития человека: сборник научных статей и материалов международной конференции «Цифровое общество как культурно-исторический контекст развития человека» 14–17 февраля 2018, Коломна / под общ. ред. Р.В. Ершовой, 2018, 380-385

16. Солдатова Г.У., Рассказова Е.И., Чигарькова С.В., Львова Е.Н. Цифровая культура: правила, ответственность и регуляция. Цифровое общество как культурно-исторический контекст развития человека: сборник научных статей и материалов международной конференции «Цифровое общество как культурно-исторический контекст развития человека» 14–17 февраля 2018, Коломна/ под общ. ред. Р.В. Ершовой., 2018, 374-379

17. Yarmina A. , Soldatova G., Khrushchev S., Rasskazova E., Tkhostov A.. Online and offline deviant behavior in russian adolescents: Results of population study of parent–child pairs. European Psychiatry, 2018, 48 - 1, 193

18. Солдатова Г.У., Рассказова Е.И.. Неосведомленность родителей о столкновении подростков с рисками в интернете: содержание и психологические факторы. Психологический журнал, 2019, 40 - 1, 71-83

19. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернет. [Электронный ресурс] URL:<http://www.ifap.ru/library/book331.pdf>

20. Безопасность детей в Интернете URL:<http://www.microsoft.com/rus/childsafety>

21. Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт. [Электронный ресурс]. URL: <http://ideti.org/>

22. Безопасный интернет: для кого и от кого? URL: <http://www.mobilereview.com/articles/2012/kidsafeinet.shtml>

23. Безопасный 3G Интернет для учебы. URL:<http://www.chip.ua/novosti/internetiseti/2012/08/bezopasnyi3ginternetdlyaucheb>

24. Борьба с вредоносными программами <http://support.kaspersky.ru/viruses>

25. Горбачева Е. В. Административно-правовое обеспечение информационной безопасности несовершеннолетних. [Электронный ресурс] URL: <http://www.dissercat.com/content/administrativnopravovoeobespechenieinformatsionnoibezopasnostinesovershennoletnikh#ixzz2IZYiXTYN>
26. Грег Шипли. Основы безопасности ИТ. [Электронный ресурс] URL: http://www.ccc.ru/magazine/depot/03_04/read.html?0501.htm
27. Дети и интернет, какие опасности скрывает всемирная паутина. / Методическое пособие для родителей. URL: <http://www.pandia.ru/text/77/115/462.php>
28. Детская безопасность в Интернете. [Электронный ресурс]. URL: <http://www.debotaniki.ru/2012/09/detskayabezopasnostvinternete/>
29. Дети в Интернете: кто предупрежден, тот вооружен. URL: <http://do.znate.ru/docs/index26385.html>
30. Десять фактов, которые нужно сообщить детям ради безопасности в Интернете <http://do.znate.ru/docs/index32759.html>
31. Ежеквартальный журнал для педагогов, психологов и родителей «Дети в информационном обществе» издаётся Фондом Развития Интернет с 2009года. Научная поддержка: факультет психологии МГУ имени М.В. Ломоносова и Федеральный институт развития образования МОНРФ. Информационная поддержка: Министерство образования и науки Российской Федерации. Выпуски №1 11 URL: <http://detionline.com/journal/numbers/11>
32. Журнал "Дети в информационном обществе" новый издательский проект, осуществляемый с 2009 года Фондом Развития Интернет при научной поддержке факультета психологии МГУ имени М.В. Ломоносова и Федерального института развития образования Министерства образования и науки РФ. Периодичность 4 раза в год. Выпуски №1 №7 URL: <http://www.fid.su/projects/journal/>
33. Режим доступа: <http://www.fid.su/projects/journal/>
34. Интерактивный курс “Основы безопасности детей и молодежи в интернете”. [Электронный ресурс] URL: <http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/html/etusivu.htm>
35. Интернет: реальные и мнимые угрозы" (под научной редакцией и с комментариями Антона Серго).[Электронный ресурс]. URL: <http://www.internetlaw.ru/book/index2.htm>
36. Интернетугрозы: троллинг и кибербуллинг. [Электронный ресурс]. URL: <http://internetua.com/internetugrozitrollingikiberbulling>
37. Информационная безопасность детей в мире компьютерных технологий, ИНТЕРНЕТ Орел Инна Юрьевна Муниципальное образовательное учреждение «Ягринская гимназия» (МОУ «Ягринская гимназия»), г. Северодвинск [Электронный ресурс] URL: <http://ito.edu.ru/2010/Arkhangelsk/IV/IV02.html>
38. Конотопов А. Обучающий курс“Гений Интернета” URL: <http://konotopov.com/internet/>
39. Линии помощи «Дети онлайн». <http://www.detionline.com/>

Интернетугрозы и эффективное противодействию им в отношении пользователей. <http://www.saferunet.ru/>

40. Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным.

<http://www.obzh.info/novosti/novoe/bezopasnostdeteivinternete.html>

41. Мельников В.П. Информационная безопасность и защита информации. [Электронный ресурс]. URL: http://www.books.demetri.ws/inf_books_25

42. Общие рекомендации по безопасному использованию интернета и мобильной связи URL: <http://do.znate.ru/docs/index30424>.

О ЛИНИИ ПОМОЩИ «ДЕТИ ОНЛАЙН» <http://do.znate.ru/docs/index30424.html>

43. Ольхова Н.Е. Беседа с родителями «Интернет зависимость». [Электронный ресурс]. //Электронно педагогический журнал Большая перемена. URL: http://www.pomochnikvsem.ru/load/publikacii_pedagogov/klassnoe_rukovodstvo/beseda_s_roditeljami_internet_zavisimost/37102567

44. OS.zone.net Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль». <http://www.oszone.net/6213/>

45. Презентация “Правовое регулирование охраны и защиты прав несовершеннолетних. “Защита детей от информации, причиняющей вред их здоровью и развитию” URL: <http://www.myshared.ru/slide/193722/>

46. Проблема информационной безопасности в содержании школьного образования Мошкин В. Н., Чередниченко А. И.[Электронный документ]//URL: <http://www.unialtai.ru/engine/download.php?id=502>

47. Пырьева В.В. Методическая разработка родительского собрания на тему “Безопасность детей в сети Интернет”URL: <http://www.proshkolu.ru/user/VeraPyryeva/blog/243888/>

48. РЕКОМЕНДАЦИИ ПО ПОЛЬЗОВАНИЮ СОЦИАЛЬНЫМИ СЕТЯМИ И ОНЛАЙНИГРАМ URL:<http://do.znate.ru/docs/index30424.html>

49. Родителям о безопасном интернете. URL: <http://74322s004.edusite.ru/p67aa1.html>

50. Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернетугроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети. URL:<http://www.rgdb.ru/innocuousinternet>

51. Руководящие указания для детей и молодых людей по защите в онлайн-среде. URL: <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/children/glchild2009r.pdf>

52. Смагулова Ш., Байтугелова Н., Наурызбаев Т. Информационная безопасность детей: Проблемы и пути решения./ Пособие для педагогов,

психологов, родителей и всех заинтересованных сторон. Астана, 2010 URL: http://www.balakkk.kz/fileadmin/user_upload/images/Informacija_bezopasnost_rus..pdf

53. Club Symantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля. URL: http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids

54. Тест на выявление Интернет-зависимости. URL: <http://www.psyhelp.ru/internet/test.php>

55. Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета. URL: <http://www.fid.su/>

56. Энциклопедия информационной безопасности. [Электронный ресурс] URL: <http://www.securelist.com/ru/encyclopedia>

Приложения

Приложение 1.

Нормативно правовые акты Республики Казахстан в отношении безопасности детей в информационном пространстве.

Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. «Об утверждении Концепции кибербезопасности» «Киберщит Казахстана»;

Закон Республики Казахстан от 2 июля 2018 года № 169-VI ЗРК. «О защите детей от информации, причиняющей вред их здоровью и развитию».

Нормативное постановление Конституционного Совета Республики Казахстан от 18 мая 2015 года № 3 «Об официальном толковании пункта 1 статьи 27 Конституции Республики Казахстан и о проверке на соответствие Конституции Республики Казахстан Закона Республики Казахстан «О защите детей от информации, причиняющей вред их здоровью и развитию» и Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию».

Распоряжение Премьер-Министра Республики Казахстан от 25 июля 2018 года № 88-р «О мерах по реализации Закона Республики Казахстан от 2 июля 2018 года «О защите детей от информации, причиняющей вред их здоровью и развитию».

Закон Республики Казахстан от 18 марта 2019 года № 237-VI ЗРК. «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам оборонной и аэрокосмической промышленности, информационной безопасности в сфере информатизации».

Постановление Правительства Республики Казахстан от 30 ноября 2021 года № 850. О проекте Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам стимулирования инноваций, развития цифровизации и информационной безопасности».

Закон Республики Казахстан от 14 июля 2022 года № 141-VII ЗРК. «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам стимулирования инноваций, развития цифровизации, информационной безопасности и образования»

Распоряжение Премьер-Министра Республики Казахстан от 25 августа 2022 года № 128-р «О мерах по реализации Закона Республики Казахстан от 14 июля 2022 года "О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам стимулирования инноваций, развития цифровизации, информационной безопасности и образования" и внесении изменения в распоряжение Премьер-Министра Республики Казахстан от 11 февраля 2022 года № 25-р "О мерах по реализации Закона Республики Казахстан от 24 ноября 2021 года "О внесении изменений и

дополнений в некоторые законодательные акты Республики Казахстан по вопросам перераспределения полномочий между уровнями государственного управления».

Закон Республики Казахстан от 11 декабря 2023 года № 44-VIII ЗРК. «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов».

Приложение 2.

Руководство по защите детей в Интернете <https://www.itu-cop-guidelines.com/>

Глобальная программа МСЭ по защите детей в Интернете <https://www.itu-cop-guidelines.com/implementation>

Защита детей в Интернете в спорте https://www.itu.int/hub/publication/s-gen-cop-child_pb-2022/

Что помогает предотвратить насилие над детьми в Интернете? <https://www.who.int/publications/i/item/9789240062061>

Конвенция о правах ребенка <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

Цифровая дезинформация/дезинформация и дети Отчет ЮНИСЕФ за 2022 год <https://www.unicef.org/globalinsight/media/2096/file/UNICEF-Global-Insight-Digital-Mis-Disinformation-and-Children-2021.pdf>

Учебная программа по медийной и информационной грамотности для педагогов и учащихся <https://unesdoc.unesco.org/ark:/48223/pf0000377068>

Измерение цифрового развития - Факты и цифры за 2022 год https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2022-pdf-e.pdf

Безопасное пребывание в Интернете (план занятий для начальной школы) https://www.unodc.org/e4j/en/primary/e4j-tools-and-materials/lesson-plan_staying-safe-online.html

Учет данных: защита конфиденциальности и безопасности учащихся <https://unesdoc.unesco.org/ark:/48223/pf0000381494>

Планы уроков ООН «Безопасность в Интернете», предоставленные на сайте Управления Организации Объединенных наций. https://www.unodc.org/e4j/en/primary/e4j-tools-and-materials/lesson-plan_lets-be-respectful-online.html

Ценности Навыки

Урок по теме: «Интернет-безопасность и предотвращение киберпреступности», для возрастной группы 6–9 лет.
https://www.unodc.org/e4j/en/primary/e4j-tools-and-materials/lesson-plan_lets-be-respectful-online.html

Ключевой вопрос: Как мы можем использовать Интернет безопасно и ответственно, при этом получая при этом удовольствие?

Цели обучения:

- Распознавайте потенциально небезопасные, опасные или рискованные онлайн-ситуации и поведение.
- Определить правила, позволяющие избегать небезопасных, опасных или рискованных ситуаций и поведения в Интернете.
- Определить стратегии, которые следует использовать при столкновении с потенциально небезопасными, опасными или рискованными онлайн-ситуациями и поведением. «Большая проблема с маленьким экраном».

Ценности Навыки

Урок по теме: «Давайте будем уважительны в Интернете»
https://www.unodc.org/e4j/en/primary/e4j-tools-and-materials/lesson-plan_lets-be-respectful-online.html

Урок на «Интернет-безопасность и предотвращение киберпреступности» для возрастной группы 9 – 12

Ключевой вопрос: «Как мы можем уважительно общаться в Интернете?»

Цели обучения: Осознать сходства и различия между онлайн и оффлайн общением.

Демонстрируйте примеры уважительного и неуважительного онлайн-общения. Определите стратегии, соответствующие их возрасту, когда они сталкиваются с тревожной, расстраивающей, опасной или неясной ситуацией в Интернете. Установите правила, обеспечивающие уважительное общение и взаимодействие онлайн и офлайн.

Участвующая организация Организационная стратегия в области информационных и коммуникационных технологий с элементом кибербезопасности.

Специальные документы по политике кибербезопасности:

Секретариат Организации Объединенных Наций. Информационно-коммуникационные технологии в Организации Объединенных Наций (А/69/517) и резолюция 69/262 Генеральной Ассамблеи). Директива о правилах информационной безопасности для Секретариата Организации Объединенных Наций (2013 год);

ЮНЭЙДС Стратегия в области ИКТ (2017–2020 годы) не включает кибербезопасность. ЮНЭЙДС работает над глобальным планом

кибербезопасности, который также будет охватывать правила кибербезопасности;

ЮНКТАД Соответствует стратегии Секретариата Организации Объединенных Наций в области информационно - коммуникационных технологий, соответствует Стратегии кибербезопасности Секретариата Организации Объединенных Наций;

ПРООН Стратегия информационных технологий (на 2020–2023 годы), Правила информационной безопасности (2016 год)

ЮНЕП Соответствует стратегии Секретариата Организации Объединенных Наций в области информационно - коммуникационных технологий, Стратегии кибербезопасности Секретариата Организации Объединенных Наций;

ЮНФПА Стратегия в области информационно- коммуникационных технологий (2018–2021 годы), Правила безопасности информационно-коммуникационных технологий

Хабитат ООН Соответствует стратегии Секретариата Организации Объединенных Наций в области информационно- коммуникационных технологий, соответствует Стратегии кибербезопасности Секретариата Организации Объединенных Наций

УВКБ Стратегия информационных технологий (2020–2022 годы)

ЮНИСЕФ Стратегия информационно- коммуникационных технологий, Стратегический план ЮНИСЕФ по информационной безопасности (2018–2022 годы)

УНП/ЮНОВ Соответствует стратегии Секретариата Организации Объединенных Наций в области информационно - коммуникационных технологий, соответствует Стратегии кибербезопасности Секретариата Организации Объединенных Наций

ЮНОПС Пятилетняя стратегия в области ИКТ

БАПОР Стратегия управления информацией (2019–2020 годы)

ООН-женщины Стратегия в области информационных и коммуникационных технологий (2018–2021 годы) Правила информационной безопасности

ВПП Общеорганизационная стратегия информационных технологий (2016–2020 годы), Общеорганизационные правила безопасности информации и информационных технологий (2015 год)

ФАО Цифровая стратегия информационно- коммуникационных технологий (2017 год), Правила информационной безопасности

МАГАТЭ Стратегический план производственных технологий (2015–2020 годы) Стандарты информационной безопасности

ИКАО Цифровая стратегия информационно- коммуникационных технологий (2017 год) (на рассмотрении), Правила информационной безопасности (2007 год, 2-я редакция)

МОТ Стратегия информационных технологий (2018–2021 годы) Да, Правила информационной безопасности электронных систем (2010 год)

ИМО Стратегический план в области информационно-коммуникационных технологий (2019–2023 годы) Да, Управление рисками информационной безопасности (2015 год)

МСЭ применяет более целостный подход к внедрению системы управления организационной устойчивостью, включая разработку подробного анализа воздействия на деятельность, отображающего стратегические риски и стратегии воздействия на деятельность, а также антикризисное управление, обеспечение бесперебойности деятельности и послеаварийное восстановление ИКТ

ЮНЕСКО Стратегия управления знаниями и информационно-коммуникационных технологий (2018–2021 годы) включена в систему общеорганизационного управления рисками и Сборник должностных инструкций (правила безопасности информации и информационных технологий)

ЮНИДО Стратегия корпоративных информационно-коммуникационных технологий (2029–2021 годы)

ЮНВТО Стратегия информационно-коммуникационных технологий не охватывает кибербезопасность

ВПС Стратегия ВПС в области ИКТ будет подготовлена в декабре 2021 года

ВОЗ Стратегия в области управления информацией и технологий (2019 год), Стратегия кибербезопасности

ВОИС Стратегия информационно-коммуникационных технологий (новая стратегия находится в стадии разработки) Правила и стандарты информационной безопасности и Стратегия информационной безопасности нового поколения;

(2021–2024 годы)

ВМО Стратегия в области информационных и коммуникационных технологий (2020–2023 годы)

Нормативно-правовая база организаций системы ООН в области кибербезопасности. Доклад Объединенной инспекционной группы. Кибербезопасность в организациях системы Организации Объединенных Наций. Женева 2021г.

https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_russian.pdf

Уровни нормативной базы кибербезопасности:

Стратегический уровень. Часто один документ, содержащий указания руководства в общих терминах. Определяет организационное видение, цели и общие принципы, излагает основные принципы управления, организационные роли и обязанности, а также может сформулировать кибербезопасность как организационное решение, включая указания о допустимой степени риска. Относится к общеорганизационному уровню, в основном предназначен для его осуществления высшим руководством

Уровень политики. Серия отдельных документов, содержащих предписывающие, требующие действий формулировки, обычно публикуемых в

виде официальных административных бюллетеней. Определяет организационные принципы, лежащие в основе системы обеспечения информационной безопасности, с обязательными внутренними положениями и правилами, определяющими цели и связанные с ними меры, организованными по темам (например, классификация информации, управление рисками, непрерывность деятельности и восстановление после аварии, а также допустимое использование данных и ресурсов ИКТ) и устанавливающими конкретные функции и обязанности. Относится ко всему персоналу и подразумевает возможность дисциплинарных взысканий в случае несоблюдения.

Процедурный уровень. Серия руководящих указаний или типовых порядков действий, поддерживающих директивы более высокого уровня, с описанием процессов, направленных на установление систематической практики предоставляет подробные инструкции по конкретным шагам, которые следует предпринять, или действиям, которых следует избегать (соблюдение правил использования паролей, регулярное антивирусное сканирование и обновление ПО, сканирование USB-накопителей (с интерфейсом «универсальная последовательная шина»), полученных в подарок, перед их использованием; и т. д.) Может применяться ко всему персоналу или быть ориентированным на определенные роли (например, персонал ИКТ, архивисты и документоведы, а также специалисты по закупкам).

Технический уровень. Серия технических протоколов, направленных на правильное и единообразное исполнение. Излагают подробные пошаговые инструкции, требующие больших познаний в предметной области для применения и реализации. Темы могут включать, среди прочего, конфигурацию базы данных, безопасность сети и безопасность облачной среды. В основном адресованы техническим специалистам.

Стратегии в области информационно-коммуникационных технологий и специальные документы по политике в области кибербезопасности в участвующих организациях. Конвенция о правах ребенка (Distr.: General, 2 March 2021, Russian, Original: English) Комитет по правам ребенка. Замечание общего порядка № 25 (2021) о правах детей в связи с цифровой средой.

Глоссарий терминов кибербезопасности (доклад ООН)

https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_russian.pdf

Ботофермы, ботнет — это большое количество инфицированных компьютеров, которые используются для создания и рассылки спама или вирусов или наводнения сети сообщениями при атаке типа «отказ в обслуживании». Источник: ESCAL Institute of Advanced Technologies, glossary of security terms www.sans.org/security-resources/glossary-of-terms/

Взлом Преднамеренное или непреднамеренное раскрытие информации, которое отрицательно сказывается на ее конфиденциальности, целостности или доступности. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Распределенная атака типа «отказ в обслуживании» Атака, при которой несколько инфицированных систем используются для атаки одной цели. Поток входящих сообщений в атакуемую систему вынуждает ее выключиться и отказывать в обслуживании незлонамеренным пользователям. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Шифрование Математическая функция, которая защищает информацию, делая ее нечитаемой для всех, кроме тех, у кого есть ключ для ее расшифровки. Источник: Национальный центр кибербезопасности (Соединенное Королевство) www.ncsc.gov.uk/information/ncsc-glossary

Оконечное устройство Любое подключенное к сети устройство — такое, как настольные компьютеры, ноутбуки, смартфоны, планшеты, принтеры или другое специализированное оборудование, например, кассовые терминалы в торговых точках, — которое используется как пользовательская оконечная точка в распределенной сети. Источник: Barracuda Networks Inc., Glossary www.barracuda.com/glossary/endpoint-device

Межсетевой экран Устройство обеспечения безопасности сети, контролирующее объем и характер входящего и исходящего сетевого трафика. Защищает локальные системные ресурсы от доступа извне. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Интернет вещей - Сеть разнообразных контролируемых через Интернет устройств, которые могут подключаться друг к другу и обмениваться информацией. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Вредоносное ПО Вредоносное программное обеспечение, предназначенное для инфицирования или повреждения компьютерной системы без согласия владельца. Распространенные формы вредоносного ПО — компьютерные вирусы, черви, трояны, шпионское и рекламное ПО. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Фишинг - Попытка третьей стороны получить конфиденциальную информацию у лица, группы или организации, выдавая себя за конкретного, обычно хорошо известного отправителя сообщений, как правило с корыстными целями. Мошенники пытаются обманом заставить пользователей раскрыть личные данные, такие как номера кредитных карт, параметры доступа в систему банковского обслуживания и другую конфиденциальную информацию, которую они могут затем использовать для совершения мошеннических действий. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Программы-вымогатели Тип вредоносного ПО, которое блокирует пользователю вход в систему или доступ к данным до тех пор, пока не будет выплачена денежная сумма. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Теневая ИТОборудование или ПО, используемые подразделением или сотрудником без ведома группы информационных технологий или

безопасности организации. Источник: Cisco
www.cisco.com/c/en/us/products/security/what-is-shadow-it.html

Социальная инженерия Манипулирование людьми с целью выполнения теми определенных действий или разглашения информации, полезной для злоумышленника. Источник: Национальный центр кибербезопасности (Соединенное Королевство) www.ncsc.gov.uk/information/ncsc-glossary

Целевой фишинг Использование поддельных электронных писем для того, чтобы убедить сотрудников организации раскрыть свои имена пользователя или пароли. В отличие от фишинга, при котором используется массовая рассылка, целевой фишинг узко направлен на четко определенную цель. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Спуфинг - Подделка адреса отправителя передачи с целью незаконного проникновения в безопасную систему. Источник: Комитет по системам национальной безопасности (Соединенные Штаты) <https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf>

Виртуальная частная сети - Частная сеть связи, обычно используемая внутри компании или несколькими разными компаниями или организациями для связи по более широкой сети. В виртуальной частной сети сообщения обычно зашифрованы или инкапсулированы для защиты от перехвата другими пользователями в сети общего пользования, в которой построена виртуальная частная сеть. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Уязвимость Изъян или слабое место в разработке или реализации информационной системы или ее среды, которые могут быть использованы для неблагоприятного воздействия на ресурсы или деятельность организации. Источник: Канадский центр кибербезопасности <https://cyber.gc.ca/en/glossary>

Дополнительные материалы для проведения уроков по интернет- безопасности и внеурочной работы.

Примерные правила поведения в сети для подростков (по версии портала Mel.fm):

1. Говори в Сети только то, что скажешь, глядя в глаза.
2. Не показывай информацию о себе никому, кроме близких друзей.
3. Не трави других.
4. Травят тебя — закрывай аккаунт.
5. Не рассказывай о себе незнакомцам.
6. Важно сказать «нет» предложениям о переписке, звонке, встрече.
7. Троллинг — не повод для нервных потрясений.
8. У шутки могут быть далеко идущие последствия.
9. За экраном такие же люди, как ты, помни об этом всегда.

Вы можете сформулировать собственные правила, используя в работе следующие кейсы.

№ 1. Ученица 5-го класса рассказала своему классному руководителю, что группа ее одноклассников снимает на фото и видео все, что происходит на перемене. Чтобы было, что снимать, они берут чей-нибудь рюкзак, оставленный в коридоре, выбрасывают его в урну для мусора и ждут, когда владелец рюкзака начнет его искать. Фото и видео ученики выкладывают в разные социальные сети.

Может ли подобное произойти с вами? [Методические рекомендации по обеспечению информационной безопасности обучающихся при работе в сети Интернет: [Электронный ресурс]. СПб: ГБУ ДПО «СПбЦОКОиИТ», 2018. URL: <https://umr.rcokoit.ru/pages/methodical-cabinet-is-network.html>.]

№ 2. К психологу школы за советом обратился ученик 8-го класса. Школьник рассказал, что около двух недель назад по электронной почте он получил приглашение от своего друга поиграть в интернет-игру, доступ к которой открывается по прикрепленной ссылке. Перейдя по указанной в письме ссылке, в появившемся окне подросток подтвердил свое участие, нажав какую-то кнопку. Игра оказалась очень увлекательной, но спустя день на электронную почту пришло письмо с незнакомого адреса с требованием оплаты участия. Ученик его проигнорировал, письма, содержащие угрозы благополучию его семьи, стали появляться каждый день. Со слов ребенка, он должен уже около 200 000 тенге. Родителям рассказать боится. Что предпринять, не знает.

Как вы думаете, чего ему не следовало делать? Может ли это произойти с вами?

№ 3. После первой четверти к директору школы обратилась мама новенькой девочки из 10-го класса. Мама сообщила, что в социальной сети появилась группа под названием «Ненавижу новенькую», к которой присоединилось 60% класса. В группе публикуются сведения, порочащие девочку. На телефон ребенку приходят СМС с угрозами и требованиями

покинуть класс. Ребенок уходит из класса и из школы не хочет, однако эмоциональное состояние девочки беспокоит маму. Разговор с классным руководителем не привел к положительному результату.

Какой совет бы дали вы? [Методические рекомендации по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет]

№ 4. Однажды вечером Аня обнаружила, что кто-то взломал ее аккаунт, разместил на стене неприличные изображения и стал рассылать оскорбления ее друзьям в личной переписке. Аня восстановила доступ к аккаунту и поменяла пароль, но было уже поздно. Многие удалили ее из друзей и добавили в черный список, а кто-то даже перестал разговаривать в школе.

Что следует сделать Ане для того, чтобы восстановить свою репутацию? Как предотвратить подобную ситуацию?

№ 5. Вадиму 14 лет, он хорошо учится, занимается карате, живет рядом со школой. Выходя из школы после уроков, он встретил свою бабушку, которая расспросила его о школе, поправила шарф, а на прощание поцеловала. Эту сцену сняли на видео его одноклассники, поместили в социальную сеть и подписали «у Вадима новая подружка!». Когда Вадим узнал, кто это сделал, он сильно избил одноклассника. Из-за этого его отстранили от участия в соревнованиях.

Кто пострадал в этой ситуации? Кто поступил неправильно? Как вы бы поступили в данной ситуации?

№ 6. В 9-м классе школы учились две подруги, Катя и Оля. Под большим секретом Катя рассказала Оле, что ей нравится Игорь из 11-го класса. Оля не удержалась и рассказала об этом одной знакомой в социальной сети, и скоро это стало известно всем. Над Катей стали смеяться, она очень разозлилась и стала писать про Олю всякие гадости в Интернете. Родители Оли обратились к классному руководителю и директору школы. В итоге Катя была вынуждена перейти в другую школу.

Кто пострадал в этой ситуации? Кто поступил неправильно? Как вы бы поступили в данной ситуации?

№ 7. Представьте, что у вашей младшей сестры появился собственный компьютер. Родители разрешили ей пользоваться им самостоятельно, но договорились, что она будет проводить за ним не более 30 минут в день. Вас попросили настроить домашний компьютер так, чтобы она могла им пользоваться максимально безопасно. Какие настройки вы будете использовать? [Интернет: возможности, компетенции, безопасность. Методическое пособие для работников общего образования.]

№ 8. Вы были в гостях у знакомого и немного поработали за его компьютером — искали информацию, заходили в свой почтовый ящик и аккаунт социальной сети. Какие настройки браузера вы можете использовать, чтобы ваша информация осталась конфиденциальной?

№ 9. Вы обнаружили бесплатную точку Wi-Fi и подключились к ней. Что вы можете не опасаясь делать в Интернете? Какие ваши действия могут оказаться опасными? На что нужно обращать внимание при работе в Интернете через общественное Wi-Fi-подключение?

№ 10. Вы искали нужную книгу в Интернете, нашли и решили скачать, но тут возник баннер, заблокировавший весь экран, с надписью Microsoft Security. На баннере также написано, что необходимо пополнить счет, отправив СМС на номер NNNN, чтобы получить код разблокировки.

Что предпринять, чтобы решить проблему? Послать ли СМС на номер? Что нужно сделать, чтобы больше не попадать в такие неприятные ситуации?

№ 11. Паша подготовил доклад об игуанах для выступления на уроке биологии. Для своей презентации ученик скопировал несколько фотографий с сайтов, где искал информацию, а также несколько найденных с помощью поиска Google среди картинок фотографий игуан. Паша дал ссылки на изображения в презентации. Кроме того, мальчик включил в презентацию несколько фотографий домашней игуаны своего друга Васи, которые скопировал из Васиного профиля в социальной сети, попросив у него разрешения на использование фотографий. В презентации школьник использовал книгу известного ученого-исследователя, жившего в XIX веке, а именно: взял отрывки с описанием исследования игуан, живших в неволе, а также процитировал слова ученого. Чтобы соблюсти правила цитирования, Паша указал имя и фамилию ученого, оформил текст кавычками, а книгу добавил в список использованной литературы. Презентация настолько понравилась учителю биологии, что он помог Паше опубликовать ее в школьном журнале

Нарушил ли Паша чьи-то авторские права при подготовке презентации? Если да, то каким образом? В каких случаях Паше стоит быть более внимательным?

№ 12. Маша (14 лет) очень переживала, когда рассталась со своим молодым человеком. Чтобы разобраться в причинах расставания, она искала в Интернете информацию об отношениях и на одном из форумов увидела историю девушки, как две капли воды похожую на то, что произошло с ней. Маша написала этой девушке (ее звали Вика), и Вика ей ответила. Они вместе обсуждали произошедшее, делились чувствами и переживаниями, обсуждали темы, которые больше ни с кем не решались обсудить. В одном из сообщений Вика написала, что, чтобы забыть их несчастную любовь, им нужно найти себе какое-то занятие, увлечение. Вика сказала, что недавно нашла очень хорошую студию танцев, и предложила Маше пойти туда вместе.

Стоит ли Маше согласиться на встречу? Что вас настораживает в ситуации? Доверяете ли вы Вике? Какие могут быть последствия встречи? Какими способами Маша могла бы себя обезопасить?

№ 13. Неделию назад в социальной сети к Наде (12 лет) в друзья добавился Саша, 13 лет. Надя не знала его лично, но видела, что он есть в друзьях у шести ее близких знакомых, поэтому подтвердила заявку Саши. Он написал, что ему

очень понравилась Надя на какой-то из фотографий в профиле их общих друзей, и хотел бы познакомиться с ней поближе. Саша прислал Наде множество сообщений, и она рассказала ему многое о себе: чем она увлекается, про свою школу и семью, где она живет и где любит отдыхать. Они даже обменялись номерами телефонов и несколько раз созванивались. Саша кажется Наде очень внимательным и заботливым молодым человеком, ей нравится, что он в нее влюблен. Вчера Саша наконец пригласил Надю на свидание: предложил сходить в кино на вечерний сеанс. Надя очень обрадовалась.

Стоит ли Наде согласиться на встречу? Что вас настораживает в ситуации? Доверяете ли вы Саше? Какие могут быть последствия встречи? Какими способами Надя могла бы себя обезопасить?

Приложение.

Информационно-аналитический журнал «Дети в информационном обществе» был учрежден в 2009 г. в рамках Года безопасного Интернета.

Информационно-аналитический журнал «Дети в информационном обществе» посвящен темам социализации, образования, личностного и духовного развития детей в эпоху глобальных социально-культурных перемен, вызванных бурным ростом информационно-коммуникационных технологий. Издание ориентировано на тех, кто профессионально работает со школьниками и детьми дошкольного возраста: учителей, воспитателей, менеджеров образования, библиотекарей, семейных и школьных психологов. Выпускается с 2009 года.

Своей главной задачей журнал ставит изучение и осмысление широкого социально-культурного контекста, в котором происходит становление современных детей и подростков. На основе наиболее актуальных российских и зарубежных исследований в издании рассказывается о том, как дети и подростки используют компьютеры и Интернет в школе и дома, какое влияние информационные технологии оказывают на их развитие, творческие способности, образ жизни, как они общаются и познают окружающий мир. Еще одна важная тема — взаимодействие детей и взрослых в информационном обществе. Авторы журнала ищут ответы на вопросы о том, как преодолеть культурный разрыв между поколениями и оказать эффективную помощь детям в виртуальном и реальном мире. В журнале рассматриваются и негативные стороны информатизации, среди которых — компьютерная зависимость, агрессивность в сети и многое другое.

К настоящему времени у издания сложился широкий круг авторов — ученых, педагогов — практиков, психологов, экспертов в области информационно-коммуникационных технологий, права, библиотечного дела, сформировались устойчивые связи с научными изданиями схожей тематики, выходящими в странах ЕС, США, Великобритании. Издатель: Фонд Развития Интернет (www.fid.su, www.detionline.com).

Интернет-ресурсы для педагогических работников:

<http://www.fid.su/projects/deti-v-internete> сайт Фонда Развития Интернет.

<http://content-filtering.ru/> сайт «Ваш личный интернет», советы, рекомендации для детей и родителей по безопасной работе в Интернет.

<http://www.ligainternet.ru/> Лиги безопасного Интернета.

<http://ppt4web.ru/informatika/bezopasnyjj-internet.html> презентации о безопасном Интернете.

<http://www.microsoft.com/ru-ru/security/default.aspx> сайт Центра безопасности Майкрософт.

<http://www.saferunet.org/children/> Центр безопасности Интернета в России.

https://edu.tatar.ru/upload/images/files/909_029%20Orangepdf Безопасно и просто: родительский контроль. — Буклет

Урок в 9–10 классах. Профилактика интернет-зависимости «Будущее начинается сегодня» <http://festival.1september.ru/articles/612789/> Материал разработан для учащихся 9-11 классов, но может модифицироваться и для учащихся среднего звена школы.

Материалы (буклет, презентация и текст) для бесед профилактике игровой и интернет-зависимости у детей и подростков на сайте Министерства образования и науки Республики Татарстан: http://mon.tatarstan.ru/prof_internet_zavisimosti.htm

<http://www.nachalka.com/node/950> Видео «Развлечение и безопасность в Интернете»

<http://i-deti.org/> портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы

<http://сетевичок.рф/> сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности

<http://www.igra-internet.ru/> — онлайн интернет-игра «Изучи Интернет — управляй им»

<http://www.safe-internet.ru/> — сайт Ростелеком «Безопасность детей в Интернете, библиотека с материалами, памятками, рекомендациями по возрастам

Информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников:

<http://www.ligainternet.ru/news/> мероприятия Лиги безопасного интернета. Лига безопасного интернета — крупнейшая и наиболее авторитетная в России организация, созданная для противодействия распространению опасного контента во всемирной сети. Лига безопасного интернета была учреждена в 2011 году при поддержке Минкомсвязи РФ, МВД РФ, Комитета Госдумы РФ по вопросам семьи женщин и детей. Попечительский совет Лиги возглавляет помощник Президента Российской Федерации Игорь Щеголев.

<http://xn--b1afankxqj2c.xn--p1ai/partneram-o-proekte> мероприятия проекта «Сетевичок». Проект представляет собой группу онлайн-мероприятий:

Статистика киберпреступлений.

2023

- Интерпол арестовал 3500 человек и \$300 млн в 34 странах по делу о глобальной сети киберпреступников.
- Как хакеры взламывают отели на Booking.com и требуют деньги у клиентов
- 4 порта в Австралии остановили работу из-за кибератаки. 30 тыс. контейнеров зависли.
- Кого и как атакуют хакеры на Ближнем Востоке, и почему там закладывают миллиарды долларов на кибербезопасность.
- У аргентинского финрегулятора похитили 1,5 Тбайт данных. Хакеры требуют выкуп \$500 тыс. и обещают уничтожить банковскую систему.
- Обновлённый пакистанский троян ReverseRAT нацелен на госучреждения Индии
- Хакеры атаковали одну из крупнейших в Канаде энергетических компаний
- АРТ-группировка Dark Pink наносит киберудары по азиатским правительственным и военным структурам.
- Раскрыта одна из самых сложных цепочек заражения компьютеров в истории

2022

- Хакеры начали массово атаковать операторов связи по всему миру, чтобы завладеть чужим телефонным номером.
- Северокорейская хакерская группировка Kimsuky атакует политические и дипломатические организации Южной Кореи.
- Волна кибератак Killnet разбилась об эстонские системы защиты
- Албания ушла в оффлайн после кибератаки
- Русскоязычные хакеры из Killnet парализовали работу нескольких госструктур Литвы
- Банда Killnet объявила о масштабной атаке на Италию
- Российских хакеров заподозрили в кибератаках на немецкие компании по возобновляемой энергетике.
- Закрыт RaidForums-хакерский форум по торговле краденными базами данных

2021

- Интерпол провел крупнейшую операцию по задержанию киберпреступников
- Южная Корея стала мировым центром цифрового секс-шантажа

2020

- Group-IB помогла Интерполу выявить преступников из Нигерии, атаковавших компании по всему миру.
- В Киргизии взломан сайт парламент;

- Взлом крупнейших баз данных ДНК, кража генеалогических профилей;
- Германия объявила международный розыск россиянина, обвинённого в кибератаках на бундестаг;
- Выявлено 1,3 тыс. вредоносных программ с названием сервисов видеоконференций;
- Как киберпреступники зарабатывают миллионы на коронавирусе
- В Индонезии задержаны киберпреступники, заразившие сотни онлайн-магазинов по всему миру;
- Сексуальное вымогательство через умные камеры

2019

- Число атак на роутер стало в десятки раз больше
- 27% компаний в мире столкнулись с кибератаками на смартфоны сотрудников
- Хакеры атакуют бензоколонки и крадут банковские данные автомобилистов
- Рассекречена самая большая хакерская группировка в истории
- У посетителей воруют данные кредиток
- Белорус украл у банков 630 тысяч евро и вернул деньги биткоинами
- Чиновники во всём мире атакованы через Whats App
- Fortinet 2019 Operational Technology Security Trends Report
- Цена хакерского взлома
- Мошенник выманил у Google и Facebook \$123 млн
- Массовые задержания пользователей теневого интернета
- В номерах десятков гостиниц встроили мини-камеры.

Подглядывать за гостями можно было за \$50 в месяц.

- Мошенники, представляясь техподдержкой Microsoft, устанавливали вирусы

2018

- Секс-шантаж в интернете набирает популярность
- Киберпреступники похитили около \$1,2 млрд в криптовалюте
- Технологическое соглашение по кибербезопасности (Cybersecurity Tech Accord)
- Microsoft Security Intelligence Report
- Cisco Annual Cybersecurity Report
- Обвинение членов группы Infraud
- Интернету грозит фрагментация из-за кибератак
- Клиника заплатила \$55 тыс. кибервымогателям

2017

- Тренды от PandaLabs
- Итоги года и прогнозы от Positive Technologies
- Прогнозы Trend Micro
- Спецслужбы США: «Исламское государство» «ушло» в виртуальный мир

- PwC: Российские компании сравнялись с американскими по уровню кибербезопасности.
 - Данные "Лаборатория Касперского"
 - Как мошенник нагрел авиакомпанию на 32 млн. долл и сел на 5 лет
 - Российские хакеры получили возможность для промышленного шпионажа с эксплойтами АНБ.
 - Крупнейшая киберсхема на финансовом рынке
 - Кибервымогатели требуют с жертв почти вчетверо больший выкуп
 - Интерпол: кибермошенничество в Западной Африке стало источником богатства и объектом поклонения.
 - Датские депутаты испугались брать гаджеты в командировку в Россию
 - Positive Technologies: в 2017 году число кибератак на банки возрастет на треть
- 2016
- Kaspersky Cybersecurity Index
 - 2016 год побил рекорд по количеству киберугроз
 - Ernst & Young: готовность защищаться растет, а инвестировать - нет
 - Интернет-пропаганда в составе значимых киберугроз 2017 года
 - Panda Security: прогноз на 2017 год
 - Исследование IBM и Ponemon Institute: компании все еще не готовы противостоять кибератакам.
 - Check Point отметил рост количества кибератак и вредоносных программ на 5%
 - Fortinet о тенденциях в сфере кибербезопасности
 - 3,2 млн ПК уязвимы, 0,002 млн имеют средства защиты
 - Europol назвал восемь основных тенденций киберпреступлений
 - 9-кратный рост неизвестных зловредов за десятилетие
 - Киберпреступники нацелились на добывающую промышленность
 - Cisco: программы-вымогатели наступают
 - Цены взлома аккаунтов соцсетей и почтовых сервисов
 - Balabit: ТОП-10 самых популярных хакерских методов
- 2015 год
- Gemalto: Breach Level Index 2015 Индекс критичности потери данных
 - Gemalto: только шифрование поможет защититься от потери данных
 - Trend Micro Security Predictions
 - HP Cyber Risk Report
 - CyberEdge Group Cyberthreat Defense Report: Более половины компаний опасаются успешных кибератак против них в 2015 году.
 - Positive Technologies: основные тенденции кибератак 2015 года
 - 84 миллиона новых образцов вредоносных программ, на 9 миллионов больше, чем в 2014 году.

- Самые мощные угрозы в 2015 году: трояны и ПНП
- Самые крупные инфекции вызваны троянами
- Китай остается одной из самых зараженных стран мира
- Скандинавские страны показали самый низкий уровень заражения

2014 год

- Лучше платить, чем защищать?
- Gemalto: Обзор утечек и краж данных
- Global Cyber Executive Briefing «Делойт Туш Томацу Лимитед»

2013 год

- Zurich: 2013 год стал самым удачным для кибер-преступников
- Кибератаки на IT-корпорации и СМИ
- Социальные сети под ударом
- Фишинговые атаки на интернет-мессенджеры
- Поимка киберпреступников
- Угрозы для TOR
- Мобильные угрозы
- Программы-вымогатели

2012 год

- WatchGuard: Поставщики облачных сервисов пострадают от масштабных сетевых атак.

- Symantec: Киберконфликты станут нормой

2011 год

- Увеличение числа утечек данных, потери устройств и как позаботиться о будущем

- Мобильные угрозы подвергают удару бизнес и индивидуальных пользователей

- Kaspersky Security Bulletin: Рейтинг стран по уровню безопасности интернет-серфинга

- Топ-20 стран по количеству размещенного на ресурсах вредоносного ПО

- Рейтинг стран по готовности к кибер угрозам

2010: Данные Symantec

- Год направленных атак
- Социальные сети: плодородная почва для кибер-преступности
- Готовые инструменты для осуществления атак сфокусировались на Java;

- Проясняется схема действий злоумышленников в мобильном пространстве;

- Ландшафт угроз – Основные цифры и факты

<https://www.tadviser.ru/index.php>

Авторская анкета «Кибербуллинг и его проявления в учащейся среде»

2. Твой возраст:
3. Твой пол: ☐ мужской ☐ женский
4. В каком классе ты обучаешься? .
5. Какова твоя средняя успеваемость обучения? ☐ 5 ☐ 4 ☐ 3 ☐ 2
6. Знаете ли вы, что такое кибербуллинг?
 - да;
 - нет;
 - затрудняюсь ответить.
7. Присутствует ли насилие в вашей школе?
 - да;
 - нет;
 - затрудняюсь ответить.
8. Были ли вы участниками кибербуллинга (в роли жертвы, агрессора или наблюдателя)?
 - да;
 - нет.
9. Как вы относитесь к явлению кибербуллинга?
 - положительно;
 - отрицательно;
 - мне все равно, главное, чтобы меня не касалось.
10. Сталкивались ли вы с унижением в школе?
 - да;
 - нет;
 - затрудняюсь ответить.
11. Какие издевательства вы испытывали в школе?
 - оскорбление/обзывание;
 - распространение слухов;
 - физические угрозы в сети;
 - распространение фото/изображений-мемов издевательского характера;
 - распространение фото без согласия;
 - другой буллинг.
12. Где чаще всего можно столкнуться с проявлением кибербуллинга?
 - мессенджеры (внутренние группы в WA, например);
 - в Тик Ток;
 - в Инстаграмм;
 - на внешних сайтах в сети Интернет;
 - другие ресурсы.
13. Причины, по которым некоторые ученики становятся жертвами издевательств?

- внешний вид;
- физические ограничения;
- поведение человека;
- само провоцирование агрессии;
- человек не может за себя вступить;
- материальный статус.

14. Чаще всего агрессорами являются:

- ребята;
- девушки.

15. Как вы реагировали на кибербуллинг, когда становились его свидетелями?

- не обращал внимания;
- пассивно наблюдал/ла;
- поддерживал/ла агрессора;
- стал/ла в защиту жертвы травли;
- сообщил/ла взрослым.

16. К кому бы вы обратились за помощью, если бы стали жертвой издевательств?

- решал/ла бы проблему самостоятельно;
- к друзьям;
- к психологу;
- к родителям;
- к классному руководителю;

17. Как учителя реагируют на случаи кибербуллинга?

- требуют прекращения ссоры;
- возлагают решение проблем на самих учащихся, не вмешиваются в их отношения;
- вообще не обращают внимания на такие случаи.

18. Встречались ли вы проявления буллинга к школьникам со стороны учителей?

- да, постоянно;
- да, редко;
- нет, не встречал/ла.

19. Рассказывают ли вам в школе о том, как предотвратить насилие и кто может в этом помочь?

- да;
- нет;

20. В каком виде в вашей школе проводится работа по предупреждению кибербуллинга?

- классные часы;
- встречи со специалистами;
- консультации психолога/социального педагога;
- вообще не производится.

21. Как часто в вашей школе проводится работа по предупреждению кибербуллинга?

- часто;
- периодически;
- Очень редко.

«Диагностика склонности к конфликтному поведению»

Адаптация Н.В. Гришиной

Цель: определение преобладающего способа поведения человека в конфликтных ситуациях.

Инструкция. В каждой из представленных пар выберите то суждение, которое наиболее типично для вашего поведения. Отведенное время – не более 15-20 минут.

1.

А. Иногда я предоставляю возможность другим взять на себя ответственность за разрешение спорного вопроса.

Б. Вместо того чтобы обсуждать то, в чем мы расходимся, я стараюсь обратить внимание на то, с чем мы оба не согласны.

2.

А. Я стараюсь найти компромиссное решение.

Б. Я стараюсь уладить дело с учетом интересов другого и моих собственных.

3.

А. обычно я настойчиво стараюсь добиться своего.

Б. Я стараюсь успокоить другого и главным образом сохранить наши отношения.

4.

А. Я пытаюсь найти компромиссное решение.

Б. Иногда я жертвую своими интересами ради интересов другого человека.

5.

А. Улаживая спорную ситуацию, я все время стараюсь найти поддержку у другого.

Б. Я стараюсь сделать все, чтобы избежать напряженности, от которой нет никакой пользы.

6.

А. Я стараюсь избежать возникновения неприятностей для себя.

Б. Я стараюсь добиться своего.

7.

А. Я стараюсь отложить решение спорного вопроса с тем, чтобы впоследствии решить его окончательно.

Б. Я считаю необходимым в чем-то уступить, чтобы добиться другого.

8.

А. обычно я настойчиво стараюсь добиться своего.

Б. Я прежде всего стараюсь ясно определить то, в чем состоят все затронутые интересы и вопросы.

9.

А. Думаю, что не всегда следует волноваться из-за каких-то возникающих разногласий.

Б. Я прилагаю усилия, чтобы добиться своего.

10.

А. Я твердо стремлюсь достичь своего.

Б. Я пытаюсь найти компромиссное решение

11.

А. Я прежде всего стараюсь ясно определить то, в чем состоят все затронутые интересы и вопросы.

Б. Я стараюсь успокоить другого и, главным образом, сохранить наши отношения.

12.

А. Часто я стараюсь не занимать позицию, которая может вызвать споры.

Б. Я даю возможность другому в чем-то остаться при своем мнении, если он тоже идет мне навстречу.

13.

А. Я предлагаю среднюю позицию.

Б. Я настаиваю, чтобы было сделано по-моему.

14.

А. Я сообщаю другому свою точку зрения и спрашиваю о его взглядах.

Б. Я стараюсь показать другому логику и предпочтение моих взглядов.

15.

А. Я стараюсь успокоить другого, и главным образом сохранить наши отношения.

Б. Я стараюсь сделать все необходимое во избежание напряженности.

16.

А. Я стараюсь не задеть чувства другого.

Б. Я стараюсь убедить другого в преимуществах моей позиции.

17.

А. обычно я упорно стараюсь добиться своего.

Б. Я стараюсь сделать все, чтобы избежать напряженности, от которой нет никакой пользы.

18.

А. Если это сделает другого счастливым, я дам ему возможность настоять на своем.

Б. Я даю возможность другому в чем-то остаться при своем мнении, если он тоже идет мне навстречу.

19.

А. Я, прежде всего, стараюсь ясно определить то, в чем состоят все затронутые интересы и спорные вопросы.

Б. Я стараюсь отложить решение спорного вопроса с тем, чтобы впоследствии решить его до конца.

20.

А. Я стараюсь немедленно преодолеть наши разногласия.

Б. Я стараюсь найти лучшее сочетание выигрышей и потерь для нас обоих.

21.

А. Ведя переговоры, я стараюсь быть внимательным к желаниям другого.

Б. Я всегда склоняюсь к прямому обсуждению проблемы.

22.

А. Я пытаюсь найти позицию, которая находится посередине между моей позицией и точкой зрения другого человека.

Б. Я отстаиваю свои желания.

23.

А. Как правило, я озабочен тем, чтобы удовлетворить желание каждого из нас.

Б. Иногда я предоставляю возможность другим взять на себя ответственность за разрешение спорного вопроса.

24.

А. Если позиция другого кажется ему очень важной, я постараюсь пойти навстречу его желаниям.

Б. Я стараюсь убедить другого прийти к компромиссу.

25.

А. Я стараюсь показать другому логику и предпочтение моих взглядов.

Б. Ведя переговоры, я стараюсь быть внимательным к желаниям другого.

26.

А. Я предлагаю среднюю позицию.

Б. Я почти всегда озабочен тем, чтобы удовлетворить желание каждого из нас.

27.

А. Часто избегаю занимать позицию, которая может вызвать споры.

Б. если это сделает другого счастливым, я дам ему возможность настоять на своем.

28.

А. обычно я настоятельно стараюсь добиться своего.

Б. Улаживая ситуацию, я обычно стараюсь найти поддержку у другого.

29.

А. Я предлагаю среднюю позицию.

Б. Думаю, что не всегда стоит волноваться из-за возникающих разногласий.

30.

А. Я стараюсь не задеть чувства другого.

Б. Я всегда занимаю такую позицию в спорном вопросе, чтобы мы совместно с другим заинтересованным человеком могли добиться успеха.

Ключ по расшифровке:

прос	Во	Борьба	Сотрудничес	Компромисс	Избеган	Уступчивос
		тво		ие	ть	
1				А	Б	
2		Б	А			
3	А					
4			А		Б	
5	Б	А		Б	Б	
6				А		
7	А		Б	А		
8	Б	Б				
9	А			А		
10			Б			
11		А			Б	
12	Б		Б	А		
13	Б		А			
14		А				
15				Б	А	
16	Б				А	
17	А			Б		
18			Б		А	
19		А		Б		
20		А	Б			
21		Б			А	
22	Б		А			
23		А		Б		
24					А	
25	А		А		Б	
26		Б				
27				А	Б	
28	А	Б				
29			А	Б		
30		Б			А	

Доклад Объединенной инспекционной группы «Кибербезопасность в организациях системы ООН. (Женева 2021 г.)

I. Введение

1. Дети, с которыми проводились консультации в ходе подготовки настоящего замечания общего порядка, сообщили, что цифровые технологии имеют жизненно важное значение для их нынешней жизни и для их будущего: «с помощью цифровых технологий мы можем получать информацию со всего мира»; «[цифровые технологии] познакомили меня с основными аспектами моей идентичности»; «когда тебе грустно, Интернет может помочь увидеть что-то, что приносит радость».

2. Цифровая среда постоянно развивается и расширяется, охватывая информационно-коммуникационные технологии, в том числе цифровые сети, контент, услуги и приложения, подключенные устройства и среды, виртуальную и дополненную реальность, искусственный интеллект, робототехнику, автоматизированные системы, алгоритмы и аналитику данных, биометрию и технологию имплантации.

3. Цифровая среда становится все более важной в большинстве аспектов жизни детей, в том числе и в период кризиса, поскольку общественные функции, включая образование, государственные услуги и торговлю, все больше опираются на цифровые технологии. Она открывает новые возможности для реализации прав детей, но в то же время создает опасность их нарушения или ущемления. В ходе консультаций дети высказали мнение о том, что цифровая среда должна поддерживать, поощрять и защищать их безопасное и равноправное участие: «мы бы хотели, чтобы правительство, технологические компании и учителя помогали нам контролировать недостоверную информацию в Интернете»; «я хотел[а] бы получить четкое представление о том, что на самом деле происходит с моими данными... Зачем их собирают? Как их собирают?»; «меня... беспокоит распространение моих данных».

4. Необходимо соблюдать, защищать и осуществлять права каждого ребенка в цифровой среде. Инновации в сфере цифровых технологий оказывают на жизнь детей и их права широкомасштабное и взаимозависимое воздействие даже в тех случаях, когда сами дети не имеют доступа к Интернету. Полноценный доступ к цифровым технологиям может помочь детям реализовать весь спектр их гражданских, политических, культурных, экономических и социальных прав. Однако, если цифровые технологии не являются общедоступными, высока вероятность усиления существующих форм неравенства и возможно появление его новых форм.

5. В основу настоящего замечания общего порядка положен опыт Комитета в деле рассмотрения докладов государств-участников и проведения им дня общей дискуссии по вопросу о цифровых средствах массовой информации и правах детей, практика договорных органов по правам человека, рекомендации Совета по правам человека и специальных процедур Совета, два

раунда консультаций с государствами, экспертами и другими заинтересованными сторонами по концептуальному документу и предварительному проекту, а также международные консультации с 709 детьми, живущими в самых различных условиях в 28 странах в нескольких регионах мира.

6. Настоящее замечание общего порядка следует рассматривать вместе с другими соответствующими замечаниями общего порядка Комитета и его руководящими принципами, касающимися осуществления Факультативного протокола к Конвенции, касающегося торговли детьми, детской проституции и детской порнографии.

II. Цель

7. В настоящем замечании общего порядка Комитет разъясняет, каким образом государствам-участникам следует осуществлять Конвенцию применительно к цифровой среде, и дает руководящие указания относительно соответствующих законодательных, политических и других мер по обеспечению полного соблюдения ими своих обязательств по Конвенции и факультативным протоколам к ней в свете возможностей, рисков и вызовов, связанных с поощрением, соблюдением, защитой и осуществлением всех прав детей в цифровой среде.

III. Общие принципы

8. Следующие четыре принципа служат своего рода призмой, через которую следует рассматривать осуществление всех других прав, предусмотренных Конвенцией. Ими следует руководствоваться при определении мер, необходимых для обеспечения реализации прав детей в связи с цифровой средой.

A. Недискриминация

9. Право на недискриминацию требует, чтобы государства-участники обеспечивали всем детям равный, эффективный и реальный доступ к цифровой среде. Государствам-участникам следует принимать все необходимые меры для преодоления цифровой эксклюзии. Это включает в себя обеспечение бесплатного и безопасного доступа для детей в специально отведенных для этого общественных местах и инвестирование в стратегии и программы, которые содействуют обеспечению недорогого доступа всех детей к цифровым технологиям и их грамотного использования в образовательных учреждениях, общинах и дома.

10. Дети могут подвергаться дискриминации в силу того, что они лишены возможности пользоваться цифровыми технологиями и услугами или получают сообщения, содержащие ненавистнические высказывания, или сталкиваются с несправедливым отношением к ним при использовании этих технологий. Другие формы дискриминации могут возникнуть в случае, если автоматизированные процессы, приводящие к фильтрации информации,

профилированию или принятию решений, основаны на предвзятых, частичных или незаконно полученных данных о ребенке.

11. Комитет призывает государства-участники принимать упреждающие меры для предотвращения дискриминации по признаку пола, инвалидности, социально-экономического положения, этнического или национального происхождения, языка или по любым другим признакам, а также дискриминации в отношении детей из числа меньшинств и коренных народов, детей — просителей убежища, детей-беженцев и детей-мигрантов, детей из числа лесбиянок, гомосексуалов, бисексуалов, трансгендеров и интерсексов, детей — жертв торговли людьми или сексуальной эксплуатации, детей, находящихся в учреждениях альтернативного ухода, детей, лишенных свободы, и других групп детей, находящихся в уязвимом положении. Потребуется конкретные меры для ликвидации связанного с гендерными факторами цифрового разрыва в интересах девочек и обеспечения уделения особого внимания таким аспектам, как доступ, цифровая грамотность, неприкосновенность частной жизни и безопасность в Интернете.

В. Наилучшие интересы ребенка

12. Наилучшие интересы ребенка — развивающаяся концепция, которая требует проведения оценки сообразно конкретному контексту. Изначально цифровая среда не предназначалась для детей, однако она играет значительную роль в их жизни. Государствам-участникам следует обеспечить, чтобы в любой деятельности, касающейся создания, регулирования, дизайна и использования цифровой среды и управления ею, первоочередное внимание уделялось наилучшим интересам каждого ребенка.

13. Государствам-участникам следует привлекать к такой деятельности национальные и местные органы, осуществляющие надзор за соблюдением прав детей. При рассмотрении вопроса о наилучших интересах ребенка они должны учитывать все права детей, включая их право искать, получать и передавать информацию, быть защищенными от причинения вреда и на должный учет их мнений, а также обеспечивать прозрачность оценки наилучших интересов ребенка и применяемых критериев.

С. Право на жизнь, выживание и развитие

14. Возможности, предоставляемые цифровой средой, играют все более важную роль в развитии детей и могут иметь решающее значение для их жизни и выживания, особенно в кризисных ситуациях. Государствам-участникам следует принимать все необходимые меры для защиты детей от рисков нарушения их права на жизнь, выживание и развитие. Риски, связанные с контентом, контактами, поведением и контрактами, касаются, среди прочего, материалов насильственного и сексуального характера, киберагрессии и домогательств, азартных игр, эксплуатации и посягательств, в том числе сексуального характера, а также поощрения самоубийств или деятельности, угрожающей жизни, или подстрекательства к ним, в том числе со стороны преступников или вооруженных групп, включенных в списки террористических

и экстремистских организаций. Государствам следует выявлять и устранять новые риски для детей, возникающие в различных контекстах, в том числе путем заслушивания их мнений о характере конкретных рисков, с которыми они сталкиваются.

15. Использование цифровых устройств не должно наносить вреда, равно как и не должно подменять собой личное общение детей или детей и родителей или лиц, осуществляющих уход за детьми. Государствам-участникам следует уделять особое внимание воздействию технологий в первые годы жизни ребенка, когда пластичность мозга максимальна, а социальная среда, в частности отношения с родителями и лицами, осуществляющими уход за детьми, имеет решающее значение для их когнитивного, эмоционального и социального развития. В первые годы могут потребоваться меры предосторожности в зависимости от дизайна, назначения и видов использования технологий. Следует организовать подготовку для родителей, лиц, осуществляющих уход за детьми, педагогов и других соответствующих субъектов и дать им рекомендации по надлежащему использованию цифровых устройств с учетом результатов исследований влияния цифровых технологий на развитие детей, особенно в критические периоды неврологического развития в младшем детском и подростковом возрасте.

D. Уважение мнения ребенка

16. Дети сообщили, что цифровая среда предоставляет им важнейшие возможности, для того чтобы их мнения по затрагивающим их вопросам были услышаны. Использование цифровых технологий может способствовать обеспечению участия детей на местном, национальном и международном уровнях. Государствам-участникам следует содействовать повышению осведомленности о цифровых средствах выражения детьми своего мнения и обеспечению доступа к ним, а также организовывать подготовку для детей и оказывать им поддержку для их участия наравне со взрослыми, при необходимости анонимно, с тем чтобы они могли эффективно отстаивать свои права как индивидуально, так и в качестве группы.

17. При разработке законодательства, стратегий, программ, услуг и учебных курсов по вопросам прав детей в связи с цифровой средой государствам-участникам следует привлекать всех детей, прислушиваться к их потребностям и должным образом учитывать их мнения. Им следует обеспечить активное взаимодействие поставщиков цифровых услуг с детьми, с предоставлением соответствующих гарантий, и должный учет ими мнений детей при разработке продуктов и услуг.

18. Государствам-участникам рекомендуется использовать цифровую среду для проведения консультаций с детьми по вопросам соответствующих законодательных, административных и других мер и обеспечить, чтобы их мнениям уделялось серьезное внимание и чтобы участие детей не приводило к ненадлежащему контролю или сбору данных, нарушающим их право на неприкосновенность частной жизни, свободу мысли и убеждений. Им следует

обеспечить, чтобы процессы консультаций включали детей, не имеющих доступа к технологиям или навыков их использования.

IV. Развивающиеся способности

19. Государствам-участникам следует уважать развивающиеся способности ребенка как правообразующий принцип, предусматривающий процесс, в ходе которого дети постепенно приобретают профессиональные знания, понимание сути вещей и способность к действиям. Этот процесс имеет особое значение в цифровой среде, где дети могут участвовать более независимо с точки зрения надзора со стороны родителей и лиц, осуществляющих уход за ними. Риски и возможности, связанные с участием детей в цифровой среде, меняются в зависимости от их возраста и этапа развития. Государствам-участникам следует руководствоваться этими соображениями всякий раз при разработке мер по защите детей в этой среде или по облегчению их доступа к ней. При разработке мер, учитывающих возраст, следует опираться на наилучшие и современные исследования по целому ряду дисциплин.

20. Государствам-участникам следует принимать во внимание меняющееся положение детей и их роль в современном мире, опыт и знания детей, которые приобретаются неравномерно в разных областях навыков и занятий, а также различный характер связанных с этим рисков. Эти соображения должны уравниваться важностью осуществления их прав в поддерживаемой среде и разнообразием индивидуального опыта и обстоятельств. Государствам-участникам следует обеспечить, чтобы поставщики цифровых услуг предлагали услуги, соответствующие развивающимся способностям детей.

21. В соответствии с обязанностью государств оказывать надлежащую помощь родителям и лицам, осуществляющим уход за детьми, в выполнении ими своих обязанностей по воспитанию детей, государствам-участникам следует содействовать осознанию родителями и лицами, осуществляющими уход, необходимости уважать растущую самостоятельность детей, их развивающиеся способности и неприкосновенность частной жизни детей. Им следует оказывать родителям и лицам, осуществляющим уход за детьми, поддержку в овладении цифровой грамотностью и осознании рисков для детей, чтобы они смогли помочь детям реализовать их права в связи с цифровой средой, включая право на защиту.

V. Общие меры по осуществлению, принимаемые государствами-участниками

22. Для обеспечения возможности реализации прав детей и их защиты в цифровой среде требуется широкий спектр законодательных, административных и иных мер, включая меры предосторожности.

A. Законодательство

23. Государствам-участникам следует пересмотреть, принять и обновить национальное законодательство в соответствии с международными стандартами в области прав человека для обеспечения совместимости цифровой среды с правами, закрепленными в Конвенции и факультативных протоколах к ней. Законодательство должно оставаться актуальным в контексте технического прогресса и новых видов практики. Им следует предусмотреть обязательное использование оценок воздействия на права детей для учета прав детей в законодательстве, при выделении бюджетных ассигнований и принятии других административных решений, касающихся цифровой среды, а также содействовать их применению государственными органами и предприятиями, имеющими отношение к цифровой среде.

В. Комплексная политика и стратегия

24. Государствам-участникам следует обеспечить, чтобы национальные стратегии, касающиеся прав детей, конкретно затрагивали вопросы цифровой среды, и выполнять соответствующие нормативные акты, отраслевые кодексы, проектно-конструкторские стандарты и планы действий, которые должны регулярно оцениваться и обновляться. Такие национальные стратегии должны быть направлены на предоставление детям возможности пользоваться преимуществами цифровой среды и обеспечение их безопасного доступа к ней.

25. Защита детей в Интернете должна быть интегрирована в национальную политику защиты детей. Государствам-участникам следует осуществлять меры по защите детей от рисков, включая киберагрессию и сексуальную эксплуатацию детей и сексуальные посягательства с использованием цифровых технологий и в Интернете, обеспечить расследование таких преступлений и предоставлять средства правовой защиты и поддержку пострадавшим детям. Им следует также удовлетворять потребности детей, находящихся в неблагоприятном или уязвимом положении, в том числе путем предоставления адаптированной для детей информации, при необходимости с переводом на соответствующие языки меньшинств.

26. Государствам-участникам следует обеспечить функционирование эффективных механизмов защиты детей в Интернете и соответствующих стратегий обеспечения их безопасности при соблюдении других прав детей везде, где дети имеют доступ к цифровой среде, включая дом, учебные заведения, интернет-кафе, молодежные центры, библиотеки, а также медицинские учреждения и учреждения альтернативного ухода.

С. Координация

27. Для охвата всеобъемлющих последствий цифровой среды для прав детей государствам-участникам следует назначить государственный орган для координации политики, руководящих указаний и программ, касающихся прав детей, между центральными и местными органами власти. Такому национальному координационному механизму необходимо взаимодействовать со школами и сектором информационно-коммуникационных технологий и сотрудничать с бизнесом, гражданским обществом, научными кругами и

организациями в целях реализации прав детей в связи с цифровой средой на межотраслевом, национальном, региональном и местном уровнях. Он должен опираться, по мере необходимости, на технологические и другие соответствующие экспертные знания государственных и иных органов и подвергаться независимой оценке на предмет эффективного выполнения своих обязанностей.

Д.Выделение ресурсов

28.Государствам-участникам следует мобилизовывать, выделять и осваивать государственные ресурсы для выполнения законодательства, стратегий и программ, направленных на полное осуществление прав детей в цифровой среде и повышение общедоступности цифровой среды, что необходимо для решения проблемы растущего воздействия цифровой среды на жизнь детей и для содействия обеспечению равного доступа к услугам и возможностям подключения к Интернету и их финансовой доступности.

29.В тех случаях, когда ресурсы поступают от предпринимательского сектора или по линии международного сотрудничества, государствам-участникам следует обеспечить, чтобы осуществление их собственных полномочий, процессы мобилизации их доходов, выделения и расходования бюджетных средств не подвергались вмешательству или подрыву в результате действий третьих сторон.

Е.Сбор данных и исследования

30.Регулярно обновляемые данные и исследования имеют решающее значение для понимания последствий цифровой среды для жизни детей, анализа ее воздействия на их права и оценки эффективности государственных мер. Государствам-участникам следует проводить обеспеченный достаточными ресурсами сбор надежных, всеобъемлющих данных в разбивке по возрасту, полу, инвалидности, географическому местоположению, этническому и национальному происхождению и социально-экономическому положению. Такие данные и исследования, включая исследования, проводимые с участием детей и самими детьми, должны быть положены в основу законодательства, политики и практических мер и находиться в публичном доступе. При сборе данных и проведении исследований, касающихся цифровой жизни детей, необходимо соблюдать неприкосновенность их частной жизни и самые высокие этические стандарты.

Ф.Независимый мониторинг

31.Государствам-участникам следует обеспечить, чтобы мандаты национальных правозащитных учреждений и других соответствующих независимых учреждений охватывали права детей в цифровой среде и чтобы они могли получать и расследовать жалобы детей и их представителей и принимать надлежащие меры. При наличии независимых надзорных органов, контролирующей деятельность, связанную с цифровой средой, национальные

правозащитные учреждения должны тесно сотрудничать с такими органами в деле эффективного выполнения ими своего мандата в отношении прав детей.

G.Распространение информации, повышение осведомленности и обучение

32.Государствам-участникам следует распространять информацию и проводить кампании по повышению осведомленности о правах ребенка в цифровой среде, уделяя особое внимание тем субъектам, чьи действия оказывают прямое или косвенное воздействие на детей. Государствам-участникам следует содействовать организации образовательных программ для детей, родителей и лиц, осуществляющих уход за детьми, широкой общественности и лиц, ответственных за разработку политики, в целях расширения их знаний о правах детей в связи с возможностями и рисками, имеющими отношение к цифровым продуктам и услугам. Такие программы должны включать информацию о том, каким образом дети могут получить пользу от цифровых продуктов и услуг и развивать свою цифровую грамотность и навыки, как обеспечить неприкосновенность частной жизни детей и предотвратить их виктимизацию, а также как определить, что ребенку причинен вред онлайн или офлайн, и принять надлежащие меры. Такие программы должны основываться на результатах исследований и консультаций с детьми, родителями и лицами, осуществляющими уход за детьми.

33.Специалисты, работающие с детьми и в их интересах, а также в предпринимательском секторе, в том числе технологической отрасли, должны проходить подготовку, включающую изучение того, как цифровая среда воздействует на права ребенка в различных контекстах, каким образом дети осуществляют свои права в цифровой среде и каким образом они получают доступ к технологиям и используют их. Они должны также пройти обучение по вопросам применения международных стандартов прав человека в цифровой среде. Государствам-участникам следует обеспечить организацию начальной профессиональной подготовки и повышения квалификации по вопросам цифровой среды для специалистов всех уровней системы образования в целях развития их знаний, навыков и практики.

H.Сотрудничество с гражданским обществом

34.Государствам-участникам следует на систематической основе привлекать гражданское общество, в том числе возглавляемые детьми группы и неправительственные организации, работающие в области защиты прав детей, а также организации, занимающиеся вопросами цифровой среды, к разработке, осуществлению, мониторингу и оценке законов, стратегий, планов и программ, касающихся прав детей. Им следует также обеспечить условия для осуществления организациями гражданского общества своей деятельности, связанной с поощрением и защитой прав детей в связи с цифровой средой.

I.Права детей и предпринимательский сектор

35.Предпринимательский сектор, включая некоммерческие организации, прямо и косвенно воздействует на права детей при предоставлении услуг и продуктов, связанных с цифровой средой. Предприятия должны соблюдать права детей и предотвращать и устранять нарушения их прав в связи с цифровой средой. Государства-участники обязаны обеспечить выполнение предприятиями этих обязательств.

36.Государствам-участникам следует принимать меры, в том числе путем разработки, мониторинга, осуществления и оценки законодательства, правил и стратегий, для обеспечения соблюдения предприятиями своих обязательств по недопущению использования своих сетей или онлайн-услуг таким образом, чтобы это приводило к нарушениям или ущемлению прав детей, включая их право на неприкосновенность частной жизни и защиту, или способствовало таким нарушениям или злоупотреблениям, а также по предоставлению детям, родителям и лицам, осуществляющим уход за детьми, оперативных и эффективных средств правовой защиты. Им следует также призывать предприятия предоставлять открытую информацию и доступные и своевременные рекомендации в поддержку безопасной и полезной цифровой деятельности детей.

37.Государства-участники обязаны защищать детей от нарушений предприятиями их прав, включая право на защиту от всех форм насилия в цифровой среде. Хотя предприятия могут не принимать непосредственного участия в совершении наносящих вред действий, их деятельность может стать причиной нарушений права детей на свободу от насилия или способствовать им, в том числе посредством разработки и предоставления цифровых услуг. Государствам-участникам следует принимать законы и нормативные акты, направленные на предотвращение нарушений права на защиту от насилия, а также законы и акты, направленные на расследование нарушений, вынесение судебных решений и устранение нарушений, совершаемых в связи с цифровой средой, и контролировать и обеспечивать их соблюдение.

38.Государствам-участникам следует требовать от предпринимательского сектора соблюдения должной осмотрительности в отношении прав детей, в частности проведения оценок воздействия на права детей и предоставления общественности полной информации об их результатах с уделением особого внимания дифференцированному, а порой и серьезному воздействию цифровой среды на детей. Им следует принимать соответствующие меры для предупреждения, мониторинга и расследования нарушений прав ребенка со стороны коммерческих предприятий и наказания за них.

39.Помимо разработки законов и стратегий государствам-участникам следует требовать от всех предприятий, оказывающих воздействие на права детей в связи с цифровой средой, соблюдения нормативно-правовых положений, отраслевых кодексов и условий предоставления услуг, которые соответствуют самым высоким стандартам этики, обеспечения неприкосновенности частной жизни и безопасности, в связи с дизайном, проектированием, разработкой, предоставлением, распределением и

маркетингом их продуктов и услуг. К ним относятся предприятия, которые непосредственно ориентированы на детей, имеют их среди своих конечных пользователей или иным образом воздействуют на детей. Им следует требовать от таких предприятий соблюдения высоких стандартов прозрачности и подотчетности и рекомендовать им принимать меры по наилучшему обеспечению интересов ребенка при внедрении инноваций. Кроме того, им следует требовать от таких предприятий предоставления учитывающих возрастную специфику инструкций для детей или родителей либо лиц, осуществляющих уход за маленькими детьми, по поводу условий предоставления ими своих услуг.

J. Коммерческая реклама и маркетинг

40. Цифровая среда включает предприятия, которые зависят в финансовом плане от обработки персональных данных для определения целевой аудитории приносящего прибыль или платного контента, и такие процессы преднамеренно и непреднамеренно воздействуют на цифровой опыт детей. Многие из этих процессов предполагают участие нескольких коммерческих партнеров, создание цепочки коммерческой деятельности и обработку персональных данных, которые могут привести к нарушениям или ущемлению прав детей, в том числе посредством рекламы элементов дизайна, которые предугадывают действия ребенка и направляют их в сторону более экстремального контента, автоматических уведомлений, которые могут прервать сон, или использования личной информации ребенка или информации о его местонахождении для направления потенциально опасного коммерчески ориентированного контента.

41. При регулировании рекламы и маркетинга, предназначенных для детей и доступных им, государствам-участникам следует уделять первоочередное внимание наилучшим интересам ребенка. Спонсирование, продакт-плейсмент и все другие формы коммерческого контента не должны увековечивать гендерные и расовые стереотипы, и между ними и всем остальным контентом должно существовать четкое разграничение.

42. Государствам-участникам следует законодательно запретить профилирование или таргетинг детей любого возраста в коммерческих целях на основе цифровой записи их фактических или предполагаемых характеристик, включая групповые или коллективные данные, таргетинг посредством профилирования по ассоциации или сходству интересов. Должно быть также запрещено прямое или косвенное соприкосновение детей с видами практики, основанными на нейромаркетинге, анализе эмоций, иммерсивной рекламе и рекламе в виртуальной и дополненной реальности для продвижения продуктов, приложений и услуг.

K. Доступ к правосудию и средствам правовой защиты

43. Дети сталкиваются с особыми трудностями при доступе к правосудию в связи с цифровой средой по целому ряду причин. Эти трудности обусловлены, в частности, отсутствием законодательства, устанавливающего

санкции за нарушение прав детей конкретно в связи с цифровой средой, сложностью получения доказательств или установления личности нарушителей или тем, что дети и их родители или лица, осуществляющие уход за ними, не знают о своих правах или о том, что является нарушением или ущемлением их прав в цифровой среде. Дополнительные проблемы могут возникнуть, если от детей требуется раскрыть информацию о действиях деликатного или конфиденциального характера в Интернете или если они опасаются возмездия со стороны сверстников или социальной изоляции.

44. Государствам-участникам следует обеспечить широкое распространение информации о надлежащих и эффективных судебных и внесудебных механизмах правовой защиты в связи с нарушениями прав детей в цифровой среде и беспрепятственный доступ к ним для всех детей и их представителей. Механизмы подачи жалоб и представления сообщений должны быть бесплатными, безопасными, конфиденциальными, предусматривать меры реагирования, быть адаптированы для детей и в доступных форматах. Государствам-участникам следует также предусмотреть возможность подачи коллективных жалоб, в том числе групповых исков и судебных разбирательств в общественных интересах, а также оказания правовой или иной соответствующей помощи, в том числе через специализированные службы, детям, права которых были нарушены в цифровой среде или посредством цифровой среды.

45. Государствам-участникам следует создать механизмы передачи таких дел на рассмотрение и оказания эффективной поддержки детям, ставшим жертвами таких нарушений, координировать их деятельность и проводить на регулярной основе ее мониторинг и оценку. Эти механизмы должны предусматривать меры по выявлению детей, ставших жертвами нарушений, лечению и последующему уходу за ними и их социальной реинтеграции. Подготовка кадров по вопросам выявления детей, ставших жертвами нарушений, должна стать элементом механизма передачи дел, в том числе для поставщиков цифровых услуг. Меры, предусмотренные такими механизмами, должны быть межучрежденческими и адаптированными для детей, с тем чтобы не допустить повторной и вторичной виктимизации ребенка в контексте следственных действий и судебных процессов. В этой связи могут потребоваться специальные меры защиты конфиденциальной информации и возмещения вреда, связанного с цифровой средой.

46. Надлежащее возмещение ущерба включает реституцию, компенсацию и сатисфакцию и может предусматривать принесение извинений, меры по исправлению положения, удаление незаконного контента, предоставление доступа к службам психологической реабилитации или принятие других мер. В отношении нарушений в цифровой среде механизмы правовой защиты должны учитывать уязвимость детей и необходимость оперативно прекратить причинение ущерба в настоящее время и предотвратить будущий ущерб. Государствам-участникам следует гарантировать недопущение повторных

нарушений, в том числе путем реформирования соответствующих законов и стратегий и их эффективного осуществления.

47. Цифровые технологии дополнительно усложняют расследование преступлений в отношении детей, которые могут иметь трансграничный характер, и судебное преследование за них. Государствам-участникам следует рассмотреть вопрос о том, каким образом использование цифровых технологий может облегчить или затруднить расследование преступлений в отношении детей и судебное преследование за них и принять все доступные превентивные и правоприменительные меры и меры судебной защиты, в том числе в сотрудничестве с международными партнерами. Им следует организовать специализированную подготовку для сотрудников правоохранительных органов, прокуроров и судей по вопросам нарушений прав детей, непосредственно связанных с цифровой средой, в том числе в рамках международного сотрудничества.

48. Дети могут сталкиваться с определенными трудностями в получении средств правовой защиты в случае нарушения их прав в цифровой среде предприятиями, в частности в контексте их глобальной деятельности. Государствам-участникам следует рассмотреть возможность принятия мер для обеспечения уважения, защиты и осуществления прав детей в контексте экстерриториальной предпринимательской деятельности и деловых операций при условии, что существует разумная связь между государством и соответствующим поведением. Им следует обеспечить создание предприятиями эффективных механизмов подачи жалоб; однако такие механизмы не должны препятствовать доступу детей к государственным средствам правовой защиты. Кроме того, им следует обеспечить, чтобы органы, обладающие надзорными полномочиями в отношении прав детей, в том числе органы, занимающиеся вопросами здравоохранения и безопасности, защиты данных и прав потребителей, образования и рекламы и маркетинга, проводили расследование в связи с жалобами и предоставляли надлежащие средства правовой защиты в случае нарушения или ущемления прав детей в цифровой среде.

49. Государствам-участникам следует предоставлять детям учитывающую их интересы и соответствующую их возрасту информацию с использованием адаптированных для детей формулировок об их правах, а также о механизмах представления сообщений и подачи жалоб, услугах и средствах правовой защиты, имеющихся в их распоряжении в случае нарушения или ущемления их прав в связи с цифровой средой. Такая информация должна также предоставляться родителям, лицам, осуществляющим уход за детьми, и специалистам, работающим с детьми и в их интересах.

VI. Гражданские права и свободы

A. Доступ к информации

50. Цифровая среда предоставляет детям уникальную возможность реализовать право на доступ к информации. В этой связи важную функцию

выполняют средства массовой информации и коммуникации, включая цифровой и онлайн контент. Государствам-участникам следует обеспечить доступ детей к информации в цифровой среде и ограничение осуществления этого права только в тех случаях, когда это предусмотрено законом и необходимо для целей, зафиксированных в статье 13 Конвенции.

51. Государствам-участникам следует обеспечить и поддерживать создание цифрового контента для детей, учитывающего их возраст и способствующего расширению прав и возможностей детей в соответствии с их развивающимися способностями, и гарантировать их доступ к разнообразной информации, включая информацию о культуре, спорте, искусстве, здоровье, гражданско-правовых и политических вопросах и правах детей, которой располагают государственные органы.

52. Государствам-участникам следует содействовать производству и распространению такого контента с использованием различных форматов и многообразия национальных и международных источников, включая новостные средства массовой информации, вещательные компании, музеи, библиотеки, а также образовательные, научные и культурные организации. Им следует, в частности, стремиться к расширению предоставления разнообразного, доступного и полезного контента для детей с инвалидностью и детей, принадлежащих к этническим, языковым, коренным и другим меньшинствам. Возможность доступа к соответствующей информации на понятных детям языках может оказать существенное позитивное воздействие на обеспечение равенства.

53. Государствам-участникам следует обеспечить, чтобы все дети были осведомлены о наличии в Интернете разнообразной и качественной информации, в том числе контента, не зависящего от коммерческих или политических интересов, и могли легко ее найти. Им следует обеспечить, чтобы автоматизированный поиск и фильтрация информации, включая системы рекомендаций, не отдавали приоритет платному контенту, имеющему коммерческую или политическую подоплеку, перед выбранным детьми контентом или за счет права детей на информацию.

54. Цифровая среда может включать материалы, содержащие гендерные стереотипы, дискриминационные и расистские высказывания, сцены насилия и эксплуатации и порнографию, а также ложные сведения, дезинформацию и недостоверную информацию, а также информацию, побуждающую детей к незаконной или вредной деятельности. Такая информация может поступать из множества источников, включая других пользователей, создателей коммерческого контента, лиц, совершающих преступления сексуального характера, или вооруженных групп, внесенных в списки террористических или экстремистских организаций. Государствам-участникам следует защищать детей от вредного и сомнительного контента и обеспечить, чтобы соответствующие предприятия и другие поставщики цифрового контента разрабатывали и применяли руководящие принципы, гарантирующие безопасный доступ детей к разнообразному контенту, признавая их право на

информацию и свободу выражения мнений, и при этом защищая их от таких вредных материалов в соответствии с их правами и развивающимися способностями. Любые ограничения на функционирование любых основанных на интернет-технологиях, электронных или других систем распространения информации должны соответствовать положениям статьи 13 Конвенции. Государства-участники не должны умышленно препятствовать или разрешать другим субъектам препятствовать подаче электроэнергии, подключению к сетям сотовой связи или к Интернету в любом географическом районе, будь то частично или полностью, что может привести к затруднению доступа ребенка к информации и коммуникации.

55. Государствам-участникам следует побуждать поставщиков цифровых услуг, используемых детьми, применять краткую и понятную маркировку контента, например о соответствии контента возрасту или о его надежности. Им следует также призывать их к предоставлению доступных руководящих указаний, подготовки, образовательных материалов и механизмов обратной связи отчетности для детей, родителей и лиц, осуществляющих уход за детьми, педагогов и соответствующих профессиональных групп. Системы рекомендаций с учетом возраста или контента и предназначенные для защиты детей от несоответствующего их возрасту контента, должны применяться с соблюдением принципа минимизации данных.

56. Государствам-участникам следует обеспечить соблюдение поставщиками цифровых услуг соответствующих руководящих принципов, стандартов и кодексов и соблюдение правил законной, необходимой и пропорциональной модерации контента. Контроль контента, школьные системы фильтрации и другие технологии, ориентированные на обеспечение безопасности, не должны использоваться для ограничения доступа детей к информации в цифровой среде; их следует использовать только для предотвращения попадания к детям вредных материалов. Модерация и контроль контента должны быть сбалансированы с правом на защиту от нарушений других прав детей, в частности их права на свободу выражения мнений и на неприкосновенность частной жизни.

57. Профессиональные кодексы поведения, устанавливаемые новостными СМИ и другими соответствующими организациями, должны включать руководящие указания о методах сообщения о цифровых рисках и возможностях в отношении детей. Такие указания должны привести к созданию отчетности, основанной на фактах, без раскрытия личности детей, ставших жертвами нарушений, и в соответствии с международными стандартами в области прав человека.

В. Свобода выражения мнений

58. Право детей на свободу выражения мнений включает право искать, получать и распространять всякого рода информацию и идеи, используя любые средства по своему выбору. Дети сообщили, что цифровая среда открывает широкие возможности для выражения их идей, мнений и политических

взглядов. Для детей, находящихся в неблагоприятном или уязвимом положении, взаимодействие с использованием современных технических средств с другими людьми, которые делятся своим опытом, может помочь им выразить свои мысли.

59. Любые ограничения права детей на свободу выражения мнений в цифровой среде, такие как фильтры, включая меры безопасности, должны быть законными, необходимыми и пропорциональными. Обоснование таких ограничений должно быть прозрачным и доводиться до сведения детей в формулировках, адаптированных для соответствующего возраста. Государствам-участникам следует предоставлять детям информацию и возможности обучения по вопросам эффективного осуществления этого права, в частности по вопросам создания цифрового контента и его безопасного распространения при уважении прав и достоинства других лиц и без нарушения законодательства, например законодательства, касающегося подстрекательства к ненависти и насилию.

60. Когда дети выражают свои политические или иные взгляды и проявляют свою индивидуальность в цифровой среде, они могут подвергнуться критике, враждебному отношению, угрозам или наказанию. Государствам-участникам следует защищать детей от киберагрессии и угроз, цензуры, утечки данных и наблюдения с использованием цифровых технологий. Дети не должны привлекаться к ответственности за выражение своих мнений в цифровой среде, если только они не нарушают ограничений, предусмотренных уголовным законодательством и совместимых со статьей 13 Конвенции.

61. Учитывая наличие коммерческих и политических мотивов для продвижения конкретных мировоззрений, государствам-участникам следует обеспечить, чтобы использование автоматизированных процессов фильтрации информации, профилирования, маркетинга и принятия решений не подменяло и не ограничивало способность детей формировать и выражать свои мнения в цифровой среде и не препятствовало ей.

С. Свобода мысли, совести, убеждений и религии

62. Государствам-участникам следует уважать право ребенка на свободу мысли, совести и религии в цифровой среде. Комитет рекомендует государствам-участникам принять или обновить положения о защите данных и стандарты дизайна для выявления, определения и запрещения практик, которые манипулируют правом детей на свободу мысли и убеждений в цифровой среде или вторгаются в него, например путем анализа эмоций или мнения. С помощью автоматизированных систем можно делать выводы о внутреннем состоянии ребенка. Государствам-участникам следует обеспечить, чтобы автоматизированные системы или системы фильтрации информации не использовались для негативного воздействия или влияния на поведение или эмоции детей или для ограничения их возможностей или развития.

63. Государствам-участникам следует обеспечить, чтобы дети не подвергались наказанию в связи с их религией или убеждениями и чтобы их

будущие возможности не ограничивались каким-либо иным образом. На осуществление права детей исповедовать свою религию или убеждения в цифровой среде могут распространяться только законные, необходимые и пропорциональные ограничения.

Д.Свобода ассоциации и мирных собраний

64.Цифровая среда может дать детям возможность формировать свою социальную, религиозную, культурную, этническую, сексуальную и политическую идентичность и участвовать в жизни соответствующих сообществ и в общественной жизни в целях обсуждения, культурного обмена, социальной сплоченности и разнообразия. Дети сообщили, что цифровая среда предоставляет им ценную возможность встречаться, обмениваться мнениями и обсуждать их со сверстниками, лицами, принимающими решения, и другими лицами, разделяющими их интересы.

65.Государствам-участникам следует обеспечить посредством законов, правил и стратегий защиту права детей на участие в организациях, которые осуществляют свою деятельность частично или исключительно в цифровой среде. Не допускается никаких ограничений на осуществление детьми своего права на свободу ассоциации и мирных собраний в цифровой среде, за исключением законных, необходимых и пропорциональных. Такое участие не должно само по себе приводить к негативным последствиям для этих детей, таким как исключение из школы, ограничение или лишение будущих возможностей или постановка на учет в полиции. Такое участие должно быть безопасным, конфиденциальным и свободным от наблюдения со стороны государственных или частных организаций.

66.Присутствие в общественном пространстве и возможности сетевого взаимодействия в цифровой среде также могут содействовать активной деятельности детей и расширению их прав и возможностей в качестве защитников прав человека. Комитет признает, что цифровая среда позволяет детям, в том числе детям-правозащитникам, а также детям, находящимся в уязвимом положении, общаться друг с другом, отстаивать свои права и создавать ассоциации. Государствам-участникам следует оказывать им поддержку, в том числе путем содействия созданию специальных цифровых пространств, и обеспечивать их безопасность.

Е.Право на неприкосновенность частной жизни

67.Неприкосновенность частной жизни имеет жизненно важное значение для свободы действий, достоинства и безопасности детей, а также для осуществления их прав. Персональные данные детей обрабатываются с целью предоставления им образовательных, медицинских и других услуг. Угрозы неприкосновенности частной жизни детей могут возникать в результате сбора и обработки данных государственными учреждениями, предприятиями и другими организациями, а также в результате такой преступной деятельности, как кража персональных данных. Угрозы могут также исходить от собственной

деятельности детей, а также от деятельности членов их семьи, сверстников или других лиц, например когда родители размещают фотографии онлайн или неизвестное лицо размещает информацию о ребенке.

68. Данные могут включать информацию, в частности, о личности детей, их деятельности, местонахождении, общении, эмоциях, здоровье и взаимоотношениях. Определенные комбинации персональных данных, включая биометрические данные, могут однозначно идентифицировать ребенка. Цифровые методы, такие как автоматизированная обработка данных, профилирование, поведенческий таргетинг, обязательная проверка личности, фильтрация информации и массовое наблюдение, становятся обычным делом. Такая практика может привести к произвольному или незаконному ущемлению права детей на неприкосновенность частной жизни; она может иметь неблагоприятные последствия для детей, которые способны продолжать сказываться на них на более поздних этапах жизни.

69. Вмешательство в частную жизнь ребенка допустимо только в том случае, если оно не является ни произвольным, ни незаконным. Поэтому любое вмешательство должно быть предусмотрено законом, преследовать законную цель, осуществляться в соответствии с принципом минимизации данных, быть пропорциональным и направленным на обеспечение наилучших интересов ребенка и не должно противоречить положениям, целям или задачам Конвенции.

70. Государствам-участникам следует принимать законодательные, административные и другие меры для обеспечения уважения и защиты частной жизни детей всеми организациями и во всех средах, которые обрабатывают их данные. Законодательство должно предусматривать надежные гарантии, транспарентность, независимый надзор и доступ к средствам правовой защиты. Государствам-участникам следует требовать включения в цифровые продукты и услуги, затрагивающие детей, встроенного алгоритма конфиденциальности. Им следует пересматривать законодательство о неприкосновенности частной жизни и защите данных на регулярной основе и обеспечить, чтобы процедуры и практические меры способствовали предотвращению преднамеренных или случайных нарушений неприкосновенности частной жизни детей. В тех случаях, когда шифрование считается надлежащим средством, государствам-участникам следует рассмотреть вопрос о принятии надлежащих мер, позволяющих выявлять случаи сексуальной эксплуатации детей и сексуальных надругательств над ними или материалы, содержащие сцены сексуального надругательства над детьми, и сообщать о них. Такие меры должны быть строго ограничены в соответствии с принципами законности, необходимости и пропорциональности.

71. В тех случаях, когда запрашивается согласие на обработку данных ребенка, государствам-участникам следует обеспечить, чтобы согласие было информированным и свободно дано ребенком или, в зависимости от возраста и развивающихся способностей ребенка, родителем или лицом, осуществляющим уход за ним, и получено до обработки этих данных. В тех случаях, когда

собственное согласие ребенка считается недостаточным и для обработки личных данных ребенка требуется согласие родителей, государствам-участникам следует требовать, чтобы организации, занимающиеся обработкой таких данных, проверяли, является ли такое согласие информированным, осмысленным и дано ли оно родителем ребенка или лицом, осуществляющим уход за ним.

72. Государствам-участникам следует обеспечить, чтобы дети и их родители или лица, осуществляющие уход за ними, могли легко получать доступ к хранимым данным, исправлять неточные или устаревшие данные и удалять данные, незаконно или без необходимости хранимые государственными органами, частными лицами или другими органами, с учетом разумных и законных ограничений. Им следует также обеспечить право детей отозвать свое согласие и возражать против обработки персональных данных в тех случаях, когда контролер данных не может доказать наличия законных и веских оснований для такой обработки. Кроме того, им следует предоставлять детям, родителям и лицам, осуществляющим уход за детьми, информацию по таким вопросам с использованием адаптированных для детей формулировок и в доступных форматах.

73. Персональные данные детей должны быть доступны только органам власти, организациям и лицам, уполномоченным законом обрабатывать их с соблюдением таких процессуальных гарантий, как регулярные проверки и меры подотчетности. Данные о детях, собираемые в определенных целях, в любом учреждении, включая досье преступников в цифровом формате, должны быть защищены и собираться исключительно в этих целях и не должны храниться незаконно или неоправданно или использоваться в иных целях. В тех случаях, когда информация предоставляется в одном учреждении и может на законных основаниях принести пользу ребенку в результате ее использования в другом учреждении, например в контексте школьного и высшего образования, использование таких данных должно быть прозрачным, подотчетным и осуществляться с согласия ребенка, родителя или лица, осуществляющего уход за ребенком, в зависимости от обстоятельств.

74. Законодательство и меры, касающиеся неприкосновенности частной жизни и защиты данных, не должны произвольно ограничивать другие права детей, такие как их право на свободу выражения мнений или защиту. Государствам-участникам следует обеспечить, чтобы законодательство о защите данных предусматривало соблюдение неприкосновенности частной жизни детей и защиту персональных данных в цифровой среде. Благодаря непрерывным технологическим инновациям сфера охвата цифровой среды расширяется и включает в себя все больше услуг и продуктов, таких как одежда и игрушки. Поскольку места, в которых дети проводят время, становятся «подключенными к Интернету» благодаря использованию встроенных датчиков, подключенных к автоматизированным системам, государствам-участникам следует обеспечить, чтобы на продукты и услуги, способствующие созданию таких условий, распространялось действие надежных мер защиты

данных и других норм и стандартов, касающихся неприкосновенности частной жизни. К ним относятся общественные места, такие как улицы, школы, библиотеки, спортивные и развлекательные центры и офисы, в том числе магазины и кинотеатры, а также дом.

75. Любое наблюдение за детьми с использованием цифровых технологий вместе с любой связанной с этим автоматизированной обработкой персональных данных должно производиться с соблюдением права ребенка на неприкосновенность частной жизни и не должно осуществляться на регулярной основе, неизбирательно или без ведома ребенка или в случае детей младшего возраста без ведома их родителей или лиц, осуществляющих уход за ними; а также без права возражать против такого наблюдения в коммерческих и образовательных учреждениях и учреждениях, занимающихся уходом, при этом для достижения желаемой цели всегда следует рассматривать имеющиеся средства, которые в наименьшей степени нарушают неприкосновенность частной жизни.

76. Цифровая среда создает определенные проблемы для родителей и лиц, осуществляющих уход за детьми, в плане соблюдения права детей на неприкосновенность частной жизни. Технологии, которые контролируют деятельность в Интернете в целях безопасности, такие как устройства и услуги отслеживания, если не применяются с осторожностью, могут помешать ребенку получить доступ к «горячей линии» или искать важную информацию. Государствам-участникам следует объяснить детям, родителям и лицам, осуществляющим уход за ними, а также общественности важность права ребенка на неприкосновенность частной жизни и то, каким образом их собственные действия могут угрожать этому праву. Им следует проинформировать их о методах соблюдения и защиты неприкосновенности частной жизни детей в связи с цифровой средой при обеспечении при этом их безопасности. Контроль родителей и лиц, осуществляющих уход за ребенком, за цифровой деятельностью ребенка должен быть соразмерным и соответствовать его развивающимся способностям.

77. Многие дети используют онлайн-аватары или псевдонимы, которые защищают их личность, и такая практика может быть важна для защиты частной жизни детей. Государствам-участникам следует требовать избрания подхода, предусматривающего интеграцию встроенного алгоритма безопасности и встроенного алгоритма конфиденциальности с анонимностью, обеспечивая при этом, чтобы практика анонимности не использовалась в обычном порядке для сокрытия вредных или незаконных действий, таких как киберагрессия, ненавистнические высказывания или сексуальная эксплуатация и сексуальные надругательства. Защита частной жизни ребенка в цифровой среде может быть жизненно важной в обстоятельствах, когда родители или лица, осуществляющие уход за ребенком, сами представляют угрозу для безопасности ребенка или они находятся в конфликте по поводу ухода за ребенком. В таких случаях может потребоваться дополнительное

вмешательство, а также консультации по семейным вопросам или другие услуги для обеспечения права ребенка на неприкосновенность частной жизни.

78.Поставщики профилактических или консультативных услуг для детей в цифровой среде должны быть освобождены от требования о получении ребенком согласия его родителей для доступа к таким услугам. Такие услуги должны соответствовать высоким стандартам конфиденциальности и защиты детей.

Г.Регистрация рождения и право на идентичность

79. Государствам-участникам следует поощрять использование систем цифровой идентификации, которые позволяют регистрировать рождения всех новорожденных детей и которые официально признаются национальными органами власти, с тем чтобы облегчить доступ к услугам, включая здравоохранение, образование и социальное обеспечение. Отсутствие регистрации рождения способствует нарушению прав детей в соответствии с Конвенцией и факультативными протоколами к ней. Государствам-участникам следует использовать современные технологии, включая передвижные пункты регистрации, для обеспечения доступа к регистрации рождения, в частности детей в отдаленных районах, детей-беженцев и детей-мигрантов, детей из группы риска и детей, находящихся в маргинализированном положении, а также для охвата детей, рожденных до внедрения систем цифровой идентификации. Для того чтобы такие системы приносили пользу детям, им следует проводить кампании по повышению осведомленности, создавать механизмы контроля, поощрять участие общин и обеспечивать эффективную координацию между различными субъектами, включая специалистов, занимающихся вопросами гражданского состояния, судей, нотариусов, работников здравоохранения и сотрудников учреждений по защите детей. Государствам-участникам следует также обеспечить наличие надежной системы обеспечения неприкосновенности частной жизни и защиты данных.

ВII.Насилие в отношении детей

80.Цифровая среда может открыть новые пути для совершения насилия в отношении детей, способствуя ситуациям, в которых дети подвергаются насилию и/или могут быть подвергнуты влиянию с целью причинения вреда себе или другим. Кризисы, такие как пандемии, могут привести к повышенному риску причинения вреда онлайн, учитывая, что в таких обстоятельствах дети проводят больше времени на виртуальных платформах.

81.Лица, совершающие преступления сексуального характера, могут использовать цифровые технологии, для того чтобы склонять детей к действиям сексуального характера и участвовать в сексуальных посягательствах на детей в Интернете, например посредством потокового видео в прямом эфире, производства и распространения материалов, содержащих сцены сексуального надругательства над детьми, а также посредством принуждения их к совершению действий сексуального характера. Насилие, сексуальная эксплуатация и сексуальные посягательства с использованием цифровых технологий также могут совершаться в кругу доверия ребенка,

членами семьи или друзьями или в случае подростков сексуальными партнерами и могут включать киберагрессию, в том числе запугивание и угрозы репутации, создание или распространение текстов или изображений сексуального характера без согласия, таких как созданный самим ребенком контент путем подстрекательства и/или принуждения, а также поощрение поведения, причиняющего вред самому себе, например порезов, суицидального поведения или расстройств пищевого поведения. В тех случаях, когда такие действия совершаются детьми, государствам-участникам следует, по мере возможности, применять в отношении соответствующих детей подходы, предусматривающие профилактику, обеспечение безопасности и восстановительное правосудие.

82.Государствам-участникам следует принимать законодательные и административные меры для защиты детей от насилия в цифровой среде, включая регулярный пересмотр, обновление и обеспечение соблюдения прочной законодательной, нормативной и институциональной базы, которая защищает детей от общепризнанных и новых рисков всех форм насилия в цифровой среде. Такие риски включают физическое или психологическое насилие, увечья или издевательства, пренебрежительное или грубое обращение, эксплуатацию и надругательства, в том числе сексуального характера, торговлю детьми, насилие по признаку пола, киберагрессию, кибератаки и информационную войну. Государствам-участникам следует осуществлять меры безопасности и защиты в соответствии с развивающимися способностями детей.

83.Цифровая среда может открыть новые возможности для вербовки и эксплуатации детей негосударственными группами, в том числе вооруженными группами, включенными в списки террористических или экстремистских организаций, для участия в насильственных действиях. Государствам-участникам следует обеспечить законодательный запрет вербовки детей террористическими или прибегающими к насилию экстремистскими группами. С детьми, обвиняемыми в соответствующих уголовных преступлениях, следует обращаться в первую очередь как с жертвами, однако в случае предъявления обвинений должна применяться система правосудия в отношении детей.

VIII.Семейное окружение и альтернативный уход

84.Многие родители и лица, осуществляющие уход за детьми, нуждаются в поддержке для развития своих технических знаний, возможностей и навыков, необходимых для оказания детям помощи в связи с цифровой средой. Государствам-участникам следует обеспечить возможность для родителей и лиц, осуществляющих уход за детьми, овладеть цифровой грамотностью, узнать, каким образом технологии могут содействовать правам детей, а также определять, что ребенок стал жертвой вреда в Интернете, и принимать надлежащие меры. Особое внимание следует уделять родителям детей, находящихся в неблагоприятном или уязвимом положении, и лицам, осуществляющим уход за ними.

85. При оказании поддержки и консультативной помощи родителям и лицам, осуществляющим уход за детьми, в связи с цифровой средой государствам-участникам следует содействовать осознанию ими необходимости уважать растущую самостоятельность детей и потребность в неприкосновенности частной жизни в соответствии с их развивающимися способностями. Государствам-участникам следует учитывать, что дети часто пользуются возможностями цифровых технологий и экспериментируют с ними и могут сталкиваться с рисками, в том числе в более молодом возрасте, чем могут предвидеть родители и лица, осуществляющие уход за детьми. Несколько детей сообщили о том, что они нуждаются в большей поддержке и поощрении своей цифровой деятельности, особенно в тех случаях, когда, по их мнению, подход родителей и лиц, осуществляющих уход за детьми, является карательным, чрезмерно ограничительным или не учитывающим их развивающиеся способности.

86. Государствам-участникам следует учитывать, что поддержка и консультативная помощь, оказываемые родителям и лицам, осуществляющим уход за детьми, должны основываться на понимании специфики и уникальности отношений между родителями и детьми. Такая консультативная помощь должна помогать родителям поддерживать надлежащий баланс между защитой ребенка и формирующейся самостоятельностью на основе взаимного сопереживания и уважения, а не запрета и контроля. Для того чтобы помочь родителям и лицам, осуществляющим уход за детьми, поддерживать баланс между родительскими обязанностями и правами ребенка, необходимо руководствоваться наилучшими интересами ребенка в сочетании с учетом его развивающихся способностей. Рекомендации родителям и лицам, осуществляющим уход за детьми, должны включать поощрение социальной, творческой и учебной деятельности детей в цифровой среде и подчеркивать, что использование цифровых технологий не должно подменять собой непосредственное, отзывчивое взаимодействие между самими детьми или между детьми и родителями или лицами, осуществляющими уход за ними.

87. Важно, чтобы дети, разлученные со своими семьями, имели доступ к цифровым технологиям. Имеющиеся данные свидетельствуют о том, что цифровые технологии способствуют поддержанию семейных отношений, например в случае раздельного проживания родителей, когда дети находятся в учреждениях альтернативного ухода, для установления отношений между детьми и будущими усыновителями или приемными родителями, а также для воссоединения детей, оказавшихся в кризисных гуманитарных ситуациях, со своими семьями. Таким образом, в случае разлученных семей государствам-участникам следует поддерживать доступ детей и их родителей, лиц, осуществляющих уход за детьми, или других соответствующих лиц к цифровым услугам с учетом соображений безопасности и наилучших интересов ребенка.

88. Необходимо поддерживать баланс между мерами, принимаемыми для повышения общедоступности цифровых технологий, и необходимостью

защиты детей в тех случаях, когда родители или другие члены семьи или лица, осуществляющие уход за детьми, будь то физически присутствующие или находящиеся на расстоянии, могут подвергать их риску. Государствам-участникам следует учитывать, что возникновение таких рисков может быть обусловлено разработкой и использованием цифровых технологий, например вследствие раскрытия информации о местонахождении ребенка потенциальному нарушителю. Признавая эти риски, они должны требовать применения подхода, предусматривающего встроенный алгоритм безопасности и встроенный алгоритм конфиденциальности, и обеспечивать, чтобы родители и лица, осуществляющие уход за детьми, были полностью осведомлены о рисках и имеющихся стратегиях поддержки и защиты детей.

IX. Дети с инвалидностью

89. Цифровая среда открывает детям с инвалидностью новые возможности для налаживания социальных отношений со сверстниками, получения доступа к информации и участия в процессах принятия решений на государственном уровне. Государствам-участникам следует использовать эти возможности и принимать меры для предотвращения создания новых и устранения существующих барьеров, с которыми сталкиваются дети с инвалидностью в связи с цифровой средой.

90. Дети с различными видами инвалидности, включая физическую, интеллектуальную, психосоциальную, слуховую и зрительную инвалидность, сталкиваются с различными барьерами в доступе к цифровой среде, такими как контент в недоступных форматах, ограниченный доступ к недорогим ассистивным технологиям дома, в школе и в общине, а также запрет на использование цифровых устройств в школах, медицинских учреждениях и других местах. Государствам-участникам следует обеспечить доступ детей с инвалидностью к контенту в доступных форматах и отменить меры, которые имеют дискриминационные последствия для таких детей. Им следует обеспечить доступ к недорогим ассистивным технологиям, в случае необходимости, в частности для детей с инвалидностью, живущих в нищете, и проводить информационно-просветительские кампании, организовывать обучение и выделять ресурсы для детей с инвалидностью, их семей и персонала образовательных и других соответствующих учреждений, с тем чтобы они обладали достаточными знаниями и навыками для эффективного использования цифровых технологий.

91. Государствам-участникам следует поощрять технологические инновации, отвечающие потребностям детей с различными видами инвалидности, и обеспечить, чтобы при разработке цифровых продуктов и услуг предусматривалась их универсальная доступность, с тем чтобы ими могли пользоваться все дети без исключения и без необходимости адаптации. Дети с инвалидностью должны участвовать в разработке и реализации мер, продуктов и услуг, которые влияют на осуществление их прав в цифровой среде.

92. Дети с инвалидностью могут быть в большей степени подвержены рискам в цифровой среде, включая киберагрессию и сексуальную эксплуатацию и сексуальные надругательства. Государствам-участникам следует выявлять и устранять риски, с которыми сталкиваются дети с инвалидностью, принимая меры по обеспечению безопасности цифровой среды для них, борясь при этом с предрассудками, с которыми сталкиваются дети с инвалидностью и которые могут привести к чрезмерной защите или исключению из жизни общества. Информация по вопросам безопасности, стратегии защиты, а также общественная информация, услуги и форумы, касающиеся цифровой среды, должны быть в доступных форматах.

Х. Медицинское обслуживание и социальное обеспечение

93. Цифровые технологии могут облегчить доступ к медицинским услугам и информации и способствовать улучшению диагностики и лечебных услуг в интересах физического и психического здоровья и надлежащего питания матерей, новорожденных, детей и подростков. Они открывают также широкие возможности для охвата детей, находящихся в неблагоприятном или уязвимом положении или в отдаленных общинах. В чрезвычайных ситуациях, а также в условиях кризиса в области здравоохранения или гуманитарного кризиса доступ к медицинским услугам и информации может быть возможен только с помощью цифровых технологий.

94. Дети сообщили, что они придают важное значение поиску информации в Интернете и поддержке, касающейся здоровья и благополучия, в том числе по вопросам физического, психического и сексуального и репродуктивного здоровья, полового созревания, сексуальности и зачатия. Подростки, в частности, хотят иметь доступ к бесплатным, конфиденциальным, соответствующим их возрасту и недискриминационным услугам в области психического здоровья и сексуального и репродуктивного здоровья в Интернете. Государствам-участникам следует обеспечить детям безопасный, надежный и конфиденциальный доступ к достоверной информации и услугам в области здравоохранения, включая услуги по психологическому консультированию. В отношении этих услуг обработка данных о детях должна ограничиваться той информацией, которая необходима для их предоставления, и они должны предоставляться специалистами или лицами, имеющими надлежащую подготовку, при наличии регулируемых механизмов надзора. Государствам-участникам следует обеспечить, чтобы цифровые медицинские товары и услуги не создавали и не увеличивали неравенство в доступе детей к очному медицинскому обслуживанию.

95. Государствам-участникам следует поощрять научные исследования и разработки, направленные на удовлетворение конкретных потребностей детей в области охраны здоровья и способствующие достижению положительных результатов в области охраны здоровья детей благодаря техническому прогрессу, и инвестировать в них. Цифровые услуги должны использоваться для дополнения или улучшения очного оказания медицинских услуг детям.

Государствам-участникам следует ввести или обновить нормативные акты, требующие от поставщиков медицинских технологий и услуг учитывать права детей в рамках их функций, контента и распространения.

96. Государствам-участникам следует применять законодательные меры для защиты детей от известных форм вреда, и активно изучать новые исследования и данные в секторе общественного здравоохранения в целях предотвращения распространения дезинформации, а также материалов и услуг, которые могут нанести ущерб психическому или физическому здоровью детей. Могут также потребоваться меры по предотвращению вредного для здоровья участия в цифровых играх или социальных сетях, такие как регулирование разработки цифровых систем, подрывающих развитие и права детей.

97. Государствам-участникам следует поощрять использование цифровых технологий для пропаганды здорового образа жизни, включая физическую и социальную активность. Им следует регулировать адресную или несоответствующую возрасту рекламу, маркетинг и другие соответствующие цифровые услуги, чтобы предотвратить воздействие на детей рекламы нездоровых продуктов, включая определенные продукты питания и напитки, алкоголь, наркотики, табак и другие никотиносодержащие продукты. Такие правила, касающиеся цифровой среды, должны быть совместимы с правилами, действующими в офлайн-среде, и соответствовать им.

98. Цифровые технологии открывают для детей многочисленные возможности для улучшения своего здоровья и благополучия, при условии что они сбалансированы с их потребностями в отдыхе, физических упражнениях и непосредственном взаимодействии со сверстниками, семьями и общинами. Государствам-участникам следует разработать руководство для детей, родителей, лиц, осуществляющих уход за детьми, и педагогов о важности здорового баланса между цифровыми и нецифровыми видами деятельности и достаточным отдыхом.

XI. Образование, досуг и культурная деятельность

A. Право на образование

99. Цифровая среда может в значительной степени обеспечить и расширить доступ детей к высококачественному инклюзивному образованию, включая надежные ресурсы для формального, неформального, неофициального, взаимного и самостоятельного обучения. Использование цифровых технологий может также укрепить взаимодействие между учителем и учеником и между учащимися. Дети подчеркнули важность цифровых технологий для улучшения их доступа к образованию и содействия их обучению и участию во внеклассных мероприятиях.

100. Государствам-участникам следует поддерживать образовательные и культурные учреждения, такие как архивы, библиотеки и музеи, в обеспечении доступа детей к различным цифровым и интерактивным учебным ресурсам, включая ресурсы коренных народов, а также к ресурсам на понятных детям языках. Эти и другие ценные ресурсы могут способствовать тому, что дети

будут заниматься творческой, гражданской и культурной деятельностью, и дать им возможность познакомиться с деятельностью других людей. Государствам-участникам следует расширять возможности детей для онлайн-обучения и обучения на протяжении всей жизни.

101. Государствам-участникам следует на справедливой основе инвестировать в технологическую инфраструктуру школ и других учебных заведений, обеспечивая наличие и финансовую доступность достаточного количества компьютеров, высококачественной и высокоскоростной широкополосной сети и стабильного источника электроэнергии, подготовку преподавателей по вопросам использования цифровых образовательных технологий, доступность и своевременное техническое обслуживание школьного оборудования. Им следует также содействовать созданию и распространению разнообразных цифровых образовательных ресурсов хорошего качества на понятных детям языках и препятствовать усугублению существующего неравенства, например неравенства, с которым сталкиваются девочки. Государствам-участникам следует обеспечить, чтобы использование цифровых технологий не наносило ущерб очному обучению и было оправдано в образовательных целях.

102. Для детей, физически не посещающих школу, или живущих в отдаленных районах или находящихся в неблагоприятном или уязвимом положении, цифровые образовательные технологии могут обеспечить возможность дистанционного или мобильного обучения. Государствам-участникам следует обеспечить наличие надлежащей инфраструктуры, позволяющей всем детям иметь доступ к основным услугам, необходимым для дистанционного обучения, включая доступ к устройствам, электричеству, Интернету, учебным материалам и профессиональной поддержке. Им следует также обеспечить, чтобы школы располагали достаточными ресурсами для предоставления родителям и лицам, осуществляющим уход за детьми, рекомендаций по дистанционному обучению на дому и чтобы цифровые образовательные продукты и услуги не создавали и не усугубляли неравенство в доступе детей к услугам очного обучения.

103. Государствам-участникам следует разработать основанные на фактических данных стратегии, стандарты и руководящие принципы для школ и других соответствующих органов, отвечающих за приобретение и использование образовательных технологий и материалов, в целях повышения эффективности предоставления образовательных услуг. Стандарты для цифровых образовательных технологий должны обеспечивать, чтобы использование этих технологий было этичным и соответствующим образовательным целям и не приводило к насилию и дискриминации в отношении детей, неправомерному использованию их персональных данных, их эксплуатации в коммерческих целях или к другим нарушениям их прав, таким как использование цифровых технологий для документирования деятельности ребенка и сообщения о ней родителям или лицам, осуществляющим уход за ребенком, без ведома или согласия ребенка.

104.Государствам-участникам следует обеспечить преподавание цифровой грамотности в школах в рамках учебных программ базового образования начиная с дошкольного уровня и на протяжении всего обучения в школе, а также оценку таких методик преподавания на основе их результатов. Учебные программы должны включать знания и навыки, необходимые для безопасной работы с широким кругом цифровых инструментов и ресурсов, в том числе связанных с контентом, творчеством, сотрудничеством, участием, социализацией и гражданской активностью. Кроме того, учебные программы должны включать такие элементы, как критический анализ, руководство по поиску надежных источников информации и выявлению дезинформации и других форм контента, содержащего необъективные или ложные сведения, в том числе по вопросам сексуального и репродуктивного здоровья, прав человека, включая права ребенка в цифровой среде, а также доступных форм поддержки и средств правовой защиты. Они должны способствовать осознанию детьми возможных негативных последствий подверженности рискам, связанным с контентом, контактами, поведением и контрактами, включая киберагрессию, торговлю людьми, сексуальную эксплуатацию и сексуальные надругательства и другие формы насилия, а также стратегиям преодоления стресса, направленным на уменьшение вреда, и стратегиям защиты их персональных данных и данных других лиц, а также стратегиям, направленным на формирование у детей социальных и эмоциональных навыков и устойчивости.

105.Все большее значение приобретает важность понимания детьми цифровой среды, в том числе ее инфраструктуры, деловой практики, стратегий убеждения, способов использования автоматизированной обработки, персональных данных и наблюдения, а также возможных негативных последствий цифровизации для общества. Преподаватели, в частности те, кто занимается обучением цифровой грамотности и просвещением в области сексуального и репродуктивного здоровья, должны пройти подготовку по вопросам гарантий, связанных с цифровой средой.

В.Право на культуру, досуг и участие в играх

106.Цифровая среда способствует реализации права детей на культуру, досуг и участие в играх, что крайне важно для их благополучия и развития. Дети всех возрастов сообщили, что для них использование широкого спектра цифровых продуктов и услуг по своему выбору связано с удовольствием, интересом и отдыхом, но при этом они опасаются, что взрослые могут не понять, насколько важны цифровые игры и как их можно разделить с друзьями.

107.Цифровые формы культуры, развлечений и игр должны помогать детям и приносить им пользу, а также отражать и поощрять различную идентичность детей, в частности их культурную самобытность, языки и наследие. Они могут способствовать развитию у детей социальных навыков, обучению, самовыражению, творческой деятельности, такой как музыка и искусство, а также развитию чувства принадлежности и формированию общей

культуры. Участие в культурной жизни в Интернете способствует творчеству, самобытности, социальной сплоченности и культурному разнообразию. Государствам-участникам следует обеспечить возможность для детей использовать свое свободное время для экспериментов с информационно-коммуникационными технологиями, самовыражения и участия в культурной жизни в Интернете.

108. Государствам-участникам следует регулировать и направлять усилия специалистов, родителей и лиц, осуществляющих уход за детьми, а также сотрудничать с поставщиками цифровых услуг, в зависимости от обстоятельств, для обеспечения того, чтобы цифровые технологии и услуги, предназначенные для детей, доступные им или оказывающие влияние на их досуг, разрабатывались, распространялись и использовались в целях расширения возможностей детей в области культуры, развлечений и игр. Сюда можно отнести поощрение инноваций в области цифровых игр и связанных с ними видов деятельности, которые способствуют самостоятельности детей, их личностному развитию и приносят удовольствие.

109. Государствам-участникам следует обеспечить, чтобы содействие созданию возможностей для культуры, досуга и игр в цифровой среде уравнивалось предоставлением привлекательных альтернатив в местах «физического» проживания детей. В частности, в раннем возрасте дети приобретают языковые и социальные навыки, навыки координации и эмоциональный интеллект в основном посредством игры, которая включает физическое движение и непосредственное личное общение с другими людьми. Для детей старшего возраста игры и развлечения, включающие физические упражнения, командный спорт и другие виды активного отдыха на свежем воздухе, могут принести пользу здоровью, а также позволят освоить функциональные и социальные навыки.

110. Досуг, проводимый в цифровой среде, может подвергать детей риску причинения вреда, например посредством малопонятной или вводящей в заблуждение рекламы или посредством крайне убедительных или похожих на азартные игры элементов дизайна. Посредством введения и использования подходов и других мер регулирования, предусматривающих защиту данных, встроенный алгоритм конфиденциальности и встроенный алгоритм безопасности, государствам-участникам следует обеспечить, чтобы предприятия не выбирали в качестве целевой аудитории детей, используя те или иные методы, которые созданы отдавать приоритет коммерческим интересам, а не интересам ребенка.

111. В тех случаях, когда государства-участники или предприятия предоставляют руководящие указания, возрастную классификацию, маркировку или сертификацию в отношении определенных форм цифровых игр и развлечений, они должны быть сформулированы таким образом, чтобы избежать ограничения доступа детей к цифровой среде в целом и не препятствовать их возможностям для досуга или реализации других прав.

ХII. Специальные меры защиты

А. Защита от экономической, сексуальной и других форм эксплуатации

112. Дети должны быть защищены от всех форм эксплуатации, наносящих ущерб любым аспектам их благополучия в связи с цифровой средой. Эксплуатация может принимать различные формы, такие как экономическая эксплуатация, включая детский труд, сексуальная эксплуатация и сексуальные надругательства, продажа, торговля детьми и похищение детей, а также вербовка детей для участия в преступной деятельности, включая формы киберпреступности. Создавая и распространяя контент, дети могут стать экономическими субъектами в цифровой среде, что может привести к их эксплуатации.

113. Государствам-участникам следует пересмотреть соответствующие законы и стратегии для обеспечения защиты детей от экономической, сексуальной и других форм эксплуатации и защиты их прав, касающихся работы в цифровой среде и связанных с ней возможностей получения вознаграждения.

114. Государствам-участникам следует обеспечить наличие соответствующих правоприменительных механизмов и оказывать поддержку детям, родителям и лицам, осуществляющим уход за детьми, в получении доступа к применимым мерам защиты. Они должны принять законодательство для обеспечения защиты детей от приносящих вред товаров, таких как оружие или наркотики, или услуг, таких как азартные игры. Для предотвращения получения детьми доступа к продуктам и услугам, которыми они не могут законно владеть или пользоваться, необходимы надежные системы проверки возраста. Такие системы должны соответствовать требованиям о защите и охране данных.

115. Учитывая обязательства государств по расследованию дел о торговле людьми и судебному преследованию и наказанию за нее, включая составные элементы этого преступления и связанное с ним поведение, государствам-участникам следует разработать и обновить законодательство о борьбе с торговлей людьми, с тем чтобы оно запрещало вербовку детей преступными группами с использованием технологий.

116. Государствам-участникам следует обеспечить наличие соответствующего законодательства для защиты детей от преступлений, совершаемых в цифровой среде, включая мошенничество и кражу персональных данных, а также выделять достаточные ресурсы для обеспечения расследования преступлений, совершаемых в цифровой среде, и судебного преследования за них. Государствам-участникам следует также требовать соблюдения высоких стандартов кибербезопасности, обеспечение интеграции встроенного алгоритма конфиденциальности и встроенного алгоритма безопасности в цифровые услуги и продукты, которыми пользуются дети, с тем чтобы свести к минимуму риск совершения таких преступлений.

В. Отправление правосудия в отношении детей

117. Дети могут подозреваться и быть обвинены или признаны виновными в нарушении законов о киберпреступности. Государствам-участникам следует обеспечить, чтобы лица, ответственные за разработку политики, учитывали воздействие таких законов на детей, уделяли особое внимание профилактике и прилагали все усилия для создания и использования альтернатив мерам уголовного правосудия.

118. Не должно устанавливаться уголовной ответственности за материалы сексуального характера, созданные самими детьми, которыми они владеют и/или которые они распространяют со своего согласия и исключительно для собственного частного пользования. Следует создать учитывающие интересы детей каналы, позволяющие им безопасно обращаться за советом и помощью в тех случаях, когда речь идет о самосоздаваемом откровенном сексуальном контенте.

119. Государствам-участникам следует обеспечить, чтобы цифровые технологии, механизмы наблюдения, такие как программное обеспечение для распознавания лиц, и профилирование рисков, которые используются для предупреждения и расследования преступлений и уголовного преследования за них, не использовались для несправедливого преследования детей, подозреваемых или обвиняемых в совершении уголовных преступлений, и не использовались в нарушение их прав, в частности права на неприкосновенность частной жизни, достоинство и свободу объединений.

120. Комитет признает, что в тех случаях, когда перевод судебных разбирательств в цифровой формат приводит к отсутствию личного контакта с детьми, это может негативно сказаться на мерах реабилитационного и восстановительного правосудия, основанных на налаживании отношений с ребенком. В таких случаях, а также в тех случаях, когда дети лишены свободы, государствам-участникам следует обеспечить личный контакт с детьми, с тем чтобы содействовать их конструктивному участию в работе судов и их реабилитации.

С. Защита детей в условиях вооруженного конфликта, детей-мигрантов и детей, находящихся в других уязвимых ситуациях

121. Цифровая среда может предоставить детям, находящимся в уязвимом положении, в том числе детям в условиях вооруженного конфликта, внутренне перемещенным детям, детям-мигрантам, детям — просителям убежища и детям-беженцам, несопровождаемым детям, детям в условиях улицы и детям, пострадавшим от стихийных бедствий, доступ к жизненно важной для их защиты информации. Цифровая среда может также помочь им поддерживать контакты со своими семьями, обеспечить им доступ к образованию, здравоохранению и другим основным услугам, а также дать им возможность получить продукты питания и безопасное убежище. Государствам-участникам следует обеспечить безопасный, надежный, конфиденциальный и необходимый доступ таких детей к цифровой среде и защищать их от всех форм насилия, эксплуатации и надругательств.

122.Государствам-участникам следует препятствовать вербовке детей и их использованию в конфликтах, включая вооруженные конфликты, посредством цифровой среды. Эти усилия включают предотвращение и криминализацию различных форм домогательства к детям и их склонения к действиям сексуального характера с использованием технологий, например посредством платформ социальных сетей или чатов в онлайн-играх, и меры наказания за них.

XIII.Международное и региональное сотрудничество

123.Трансграничный и транснациональный характер цифровой среды требует активного международного и регионального сотрудничества для обеспечения эффективного соблюдения, защиты и осуществления всеми заинтересованными сторонами, включая государства, предприятия и другие субъекты, прав детей в связи с цифровой средой. Исходя из этого крайне важно, чтобы государства-участники сотрудничали на двусторонней и многосторонней основе с национальными и международными неправительственными организациями, учреждениями Организации Объединенных Наций, предприятиями и организациями, специализирующимися в области защиты детей и прав человека в связи с цифровой средой.

124.Государствам-участникам следует поощрять международный и региональный обмен опытом и передовой практикой и содействовать такому обмену, а также разрабатывать и продвигать меры наращивания потенциала, ресурсы, стандарты, нормативные положения и меры защиты невзирая на национальные границы, что позволяет всем государствам осуществлять права детей в цифровой среде. Им следует способствовать выработке общего определения того, что представляет собой преступление в цифровой среде, а также взаимной правовой помощи и совместному сбору доказательств и обмену ими.

XIV.Распространение информации

125.Государствам-участникам следует обеспечить широкое распространение настоящего замечания общего порядка, в том числе с использованием цифровых технологий, среди всех соответствующих заинтересованных сторон, в частности в парламенте и государственных органах, включая структуры, отвечающие за комплексные и отраслевые цифровые преобразования, а также работников судебной системы, коммерческие предприятия, средства массовой информации, гражданское общество и население в целом, педагогов и детей, в различных форматах и на разных языках, включая адаптированные к потребностям конкретных возрастных групп версии.
https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_russian.pdf

Перечень полезных сайтов для подготовки занятий.

1. https://xn--b1aew.xn--p1ai/Internet_for_kids — Официальный портал МВД России «Безопасный Интернет – детям».
2. <https://www.saferunet.ru/> — Центр безопасного Интернета в России.
3. <http://i-deti.org/> — Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт.
4. <http://www.fid.su/> — Фонд развития Интернет.
5. <http://www.ifap.ru/library/book099.pdf> — «Безопасность детей в Интернете», компания Microsoft.
6. <http://www.oszone.net/6213/> «Обеспечение безопасности детей при работе в Интернет».
7. <https://www.google.ru/safetycenter/families/start/basics/> — Центр безопасности Google.
8. <http://shperk.ru/sovety/avtoritet.html> — Как отличить фейк от настоящего материала?
9. <http://habrahabr.ru/company/mailru/blog/252091/> «Безопасность в интернете: готовы ли пользователи противостоять киберугрозам?».
10. <https://pandia.ru/text/78/639/36613.php> — Урок безопасности «Правила общения в Интернете!» (для подростков 12-15 лет).
11. https://lenvhtl.edumsko.ru/uploads/2000/1188/doc_norm/perechen_meropriyatij_bezopasnost_v_internete.pdf — Программа мероприятий по безопасности в сети Интернет.
12. <https://proshkolu.ru/user/litvinatm59/blog/144290/> — Тренинг «Безопасность в сети Интернет»

Содержание

Введение.....	209
1 Теоретическое обоснование и анализ текущей ситуации кибербезопасности, кибергигиены и киберкультуры детей	212
2 Международный и отечественный опыт по формированию полезных привычек в отношении кибербезопасности, кибергигиены и киберкультуры детей.....	247
3 Методические рекомендации по формированию полезных привычек в отношении кибербезопасности, кибергигиены и киберкультуры детей.....	274
Заключение.....	352
Список использованной литературы.....	353
Приложение.....	360

Балалардың киберқауіпсіздігі, кибергигиенасы және кибермәдениетіне қатысты жағымды әдеттерді қалыптастыру бойынша әдістемелік ұсынымдар

Методические рекомендации по формированию полезных привычек в отношении кибербезопасности, кибергигиены и киберкультуры детей

Басуға 24. 12.2023. ж. қол қойылды. Пішімі 60×84 1/16.
Қағазы офсеттік. Офсеттік басылыс.
Қаріп түрі «Times New Roman». Шартты баспа табағы 25.

Печать была подписана 24.12.2023 г. Формат 60×84 1/16.
Бумага офсетная. Офсетная печать.
Тип шрифта «Times New Roman». Усл. п.л. 25.