Қазақстан Республикасы Ғылым және жоғары білім министрлігі
«Әлкей Марғұлан атындағы Павлодар педагогикалық университеті» КЕАҚ
Қосымша білім беру институты

БЕКІТЕМІН
Басқарма мүшесі – академиялық мәселелер жөніндегі проректор
_____ О.К. Андрющенко
«20» 05 2025 ж.

Педагогикалық кадрлардың біліктілігін арттыру курсының
білім беру бағдарламасы
«Білім беру ортасындағы киберқауіпсіздік және ақпаратты қорғау»

Әзірленді:
PhD, қауымдастырылған профессор
_____Абыкенова Д.Б.
«19» 05 2025 ж.
Пед. ғылымдарының докторы, профессор
_____Жилбаев Ж.О.
«19» 05 2025 ж.
Пед. ғылымдарының кандидаты,
профессор
_____Асаинова А.Ж.
«19» 05 2025 ж.

Келісілді:
ҚББИ директоры:
_____ ф.ғ.к. Р. Жаева
«19» 05 2025 ж.

Павлодар 2025 ж.

I. Жалпы ережелер

Қазіргі білім беру ортасы цифрлық технологияларды қарқынды түрде интеграциялауда, бұл педагогтардан қашықтан оқыту құралдары мен цифрлық ресурстарды меңгерумен қатар, киберқауіпсіздік саласында да хабардар болуды талап етеді. Мұғалімдер мен оқытушылар білім алушылардың цифрлық мәдениетін қалыптастыруда, ақпараттық технологияларды қауіпсіз пайдалануды қамтамасыз етуде және білім беру процесінде дербес деректерді қорғауда маңызды рөл атқарады.

Педагогтардың біліктілігін арттыру бағдарламасы ИРН AP19678646 «Комплаенс-менеджментті пайдалану негізінде мектеп білім беру ортасының киберқауіпсіздігін педагогикалық қамтамасыз ету» жобасы аясында гранттық қаржыландыру арқылы әзірленіп, келесі құжаттар негізінде құрастырылды:

1. Қазақстан Республикасының 2007 жылғы 27 шілдедегі № 319-III «Білім туралы» заңы(2025 жылғы 15 сәуірдегі өзгерістер мен толықтырулармен).
2. Қазақстан Республикасының 2015 жылғы 24 қарашадағы «Ақпараттандыру туралы» заңы (2025 жылғы 8 қаңтардағы өзгерістер мен толықтырулармен).
3. Қазақстан Республикасының 2024 жылғы 1 шілдедегі № 103-VIII ЗРК «Ғылым және технологиялық саясат туралы» Заңы.
4. Қазақстан Республикасы Оқу-ағарту министрінің 2022 жылғы 21 желтоқсандағы № 506 бұйрығымен бекітілген Балаларға қатысты әлімжеттік (буллинг) жағдайының алдын алу қағидалары.
5. Қазақстан Республикасының 2022 жылғы 3 мамырдағы № 118-VII ЗРК «Баланың құқықтарын қорғау, білім беру, ақпарат және ақпараттандыру мәселелері бойынша кейбір заңнамалық актілерге өзгерістер мен толықтырулар енгізу туралы» Заңы.
6. Қазақстан Республикасы Президентінің 2012 жылғы 14 желтоқсандағы «Қазақстан-2050» стратегиясы аясындағы халыққа жолдауы. Білім беру саласындағы басымдықтар: «Біз қашықтан оқыту мен онлайн оқыту секілді инновациялық әдістерді, шешімдер мен құралдарды білім беру жүйесіне жедел енгізуіміз керек».
7. Қазақстан Республикасының 2029 жылға дейінгі ұлттық даму жоспары, Қазақстан Республикасы Президентінің 2024 жылғы 24 сәуірдегі № 611 Жарлығымен бекітілген.
8. Қазақстан Республикасы Оқу-ағарту министрінің 2022 жылғы 3 тамыздағы № 348 бұйрығымен бекітілген мектепке дейінгі, бастауыш, негізгі орта және жалпы орта, техникалық және кәсіптік, орта білімнен кейінгі білім берудің мемлекеттік жалпыға міндетті стандарттары (2025 жылғы 15 сәуірдегі өзгерістермен).
9. Педагог қызметкерлер мен оларға теңестірілген тұлғалардың үлгілік біліктілік сипаттамалары. Қазақстан Республикасы Білім және ғылым министрінің 2009 жылғы 13 шілдедегі № 338 бұйрығы (2020 жылғы 30 сәуірдегі

№ 169 бұйрығы және 2025 жылғы 30 сәуірдегі № 98 бұйрықпен енгізілген өзгерістермен).

10. «Киберқалқан Қазақстан» киберқауіпсіздік тұжырымдамасы, Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген (2023 жылғы 17 наурыздағы өзгерістермен).

11. 2023–2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасы, Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысымен бекітілген.

12. Қазақстан Республикасы Оқу-ағарту министрінің м.а. 2022 жылғы 15 желтоқсандағы № 500 бұйрығымен бекітілген «Педагог» кәсіби стандарты.

13. ҚР СТ IEC/PAS 62443-3-2017 «Өнеркәсіптік байланыс желілері. Желі мен жүйенің қорғалу деңгейі (киберқауіпсіздік)» киберқауіпсіздік стандарты (IEC PAS 62443-3:2008 IDT).

14. Ақпараттық қауіпсіздік бөлімшелерінің басшылары мен қызметкерлерінің құзыреттеріне қойылатын талаптар, соның ішінде ақпараттық қауіпсіздікті қамтамасыз етуге жауапты тұлғалардың біліктілігін арттыру талаптары – Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2020 жылғы 21 қыркүйектегі № 89 қаулысы (2025 жылғы 20 наурыздағы өзгерістермен).

15. Қазақстан Республикасы Үкіметінің 2024 жылғы 13 мамырдағы № 372 қаулысы, 2016 жылғы 20 желтоқсандағы № 832 «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздік саласындағы бірыңғай талаптарды бекіту туралы» қаулысына өзгерістер мен толықтырулар енгізу туралы.

Біліктілікті арттыру курсының білім беру бағдарламасы «Білім беру ортасындағы киберқауіпсіздік және ақпаратты қорғау» жалпы орта білім беру ұйымдарының мұғалімдеріне (бұдан әрі – Тыңдаушылар) арналған. Бағдарлама тыңдаушылардың оқушылар арасында киберқауіптердің алдын алу бойынша құзыреттерін дамытуға бағытталған.

Курс барысында тыңдаушылар киберқауіпсіздіктің негіздерімен, цифрлық білім беру кеңістігінде қауіпсіз жұмыс істеу қағидаларымен, жеке деректерді қорғау әдістерімен, сондай-ақ мектеп оқушылары мен студенттердің цифрлық сауаттылығын қалыптастыру стратегияларымен танысады.

Қазіргі таңда мектеп мұғалімдері заманауи білім беру технологияларын меңгеріп қана қоймай, цифрлық ортадағы ықтимал қауіптерді анықтай білуі, деректердің таралуын болдырмауы және оқушыларды интернетте қауіпсіз әрекет етуге үйрете білуі қажет. Курста киберқауіпсіздік негіздерін оқыту әдістемесіне, ата-аналармен және оқушылармен цифрлық гигиена мәселелері бойынша жұмысты ұйымдастыруға, сондай-ақ киберқауіпсіздік қағидаларын білім беру үдерісіне кіріктіруге ерекше назар аударылады.

Білім берудегі киберқауіпсіздік мәселесі деректерді техникалық қорғаудан бастап, цифрлық мәдениет пен желідегі жауапты мінез-құлықты қалыптастыруға дейінгі кең ауқымды қамтиды. Курстың маңызды міндеттерінің бірі –

мұғалімдердің цифрлық гигиена, жеке деректермен жұмыс істеу, қауіптерді талдау және қорғаныс құралдарын пайдалану бойынша құзыреттерін дамыту, сондай-ақ білім беру ұйымдарындағы ақпараттық қауіпсіздіктің құқықтық негіздерін түсіну.

Курс жалпы білім беретін мектеп мұғалімдеріне арналғанымен, колледждер мен жоғары оқу орындарының оқытушыларына, әдіскерлерге және білім беру ұйымдарының әкімшілік қызметкерлеріне де пайдалы болуы мүмкін. Бағдарлама аяқталғаннан кейін тыңдаушылар алған білімдерін кәсіби қызметте тиімді қолдана алады, оқушыларға, әріптестерге және ата-аналарға арналған киберқауіпсіздік бойынша әдістемелік ұсыныстар әзірлей алады, сондай-ақ білім беру ортасының цифрлық қауіпсіздігін арттыра алады.

Білім беру деңгейі: орта білім беру ұйымдары.

Тыңдаушылар категориясы: жалпы орта білім беру ұйымдарының мұғалімдері.

Оқу көлемі: 80 сағат.

Оқу тілі: қазақ, орыс тілдері.

II. Глоссарий

Ақпараттық қауіпсіздік – жеке тұлғаның, қоғамның және мемлекеттің ақпараттық саладағы сыртқы және ішкі қауіп-қатерлерден қорғалу күйі.

Ақпарат қауіпсіздігі – ақпараттың тиісті субъектілер үшін құпиялылығының бұзылуы (рұқсатсыз жария ету), тұтастығының бұзылуы (өзгертілуі), қолжетімділігінің жоғалуы немесе төмендеуі, сондай-ақ заңсыз таралуынан қорғалу деңгейі.

Ақпараттық технология қауіпсіздігі – ақпаратты өңдеу технологиялық процесінің қорғалу деңгейі.

Ақпаратты қорғау – қорғалатын ақпараттың таралуын, оған санкцияланбаған және кездейсоқ әсерлерді болдырмауға бағытталған іс-шаралар жиынтығы.

Ақпаратқа санкцияланбаған қолжетімділіктен қорғау – заннамалық құжаттармен немесе ақпарат иесінің белгілеген ережелерімен карастырылған құқықтарды бұза отырып, ақпаратқа қол жеткізуді болдырмауға бағытталған іс-әрекеттер.

Қорғалатын ақпарат – меншік нысаны болып табылатын және құқықтық құжаттардың немесе ақпарат иесінің талаптарына сәйкес корғауға жататын ақпарат.

Киберқылмыскер – жеке мүддесі, идеологиялық немесе басқа да себептермен қасақана құқық бұзушылық жасайтын тұлға.

Кибершабуыл – ақпараттық инфрақұрылым объектілеріне, оларды өзара байланыстыратын телекоммуникациялық желілерге бағытталған бағдарламалық және/немесе аппараттық-бағдарламалық құралдардың мақсатты әсері, оның нәтижесінде олардың жұмыс істеуі бұзылады немесе тоқтатылады, сондай-ақ өңделетін ақпараттың қауіпсіздігіне қауіп төнеді.

Киберқауіпсіздік – ақпараттық инфрақұрылым мен оның құрамындағы ақпараттың сыртқы және ішкі қауіптерден қорғалу күйі.

Кибербуллинг – цифрлық технологияларды пайдалану арқылы жүзеге асырылатын қудалау. Кибербуллинг әлеуметтік желілерде, мессенджерлерде, ойын платформаларында және мобильді құрылғыларда орын алуы мүмкін. Бұл – қорқыту, ашуландыру немесе масқаралау мақсатында бағытталған әдейі мінез-құлық үлгісі.

Киберинцидент – ақпараттың құпиялылығына, тұтастығына, шынайылығына, қолжетімділігі мен сақталуына нақты немесе ықтимал қауіп төндіретін оқиға, сондай-ақ қауіпсіздік саясаттарын бұзу (бұзу қаупі) жағдайы.

Кибертерроризм – адамдардың өмірі мен денсаулығына қауіп төндіретін, сондай-ақ аса маңызды нысандардың жұмысында ауыр бұзылулар тудыруы мүмкін ақпараттық жүйелерге жасалатын шабуылдар. Бұл шабуылдар билік органдарының шешімдеріне ықпал ету, саяси немесе басқа да қоғамдық қызметке кедергі жасау, халықты қорқыту немесе қоғамдық тәртіпті тұрақсыздандыру мақсатында жүзеге асырылады.

Ақпараттың құпиялылығы – ақпарат иесінің келісімінсіз немесе Қазақстан Республикасының заңнамалық актілерінде көзделген басқа негіздерсіз оны таратпау және (немесе) ұсынбау талабы.

Ақпарат иесі – Қазақстан Республикасының заңнамалық актілерінде белгіленген негіздер бойынша немесе шарт негізінде ақпарат иесі құқығын алған ақпараттық қатынастар субъектісі.

Білім беру парадигмасы – педагогтың әртүрлі білім беру қызметінде нақты әрекеттерін анықтайтын теориялық және әдістемелік алғышарттардың жиынтығы, оның үлгі ретінде басшылыққа алатын негіздері.

Педагогикалық парадигма – ғылыми-педагогикалық көзқарастар жүйесі, педагогикалық қызметтің теориялық ережелері, әдіснамалық негіздері, ұғымдары және құндылық критерийлері жиынтығы.

Жеке деректер – Қазақстан Республикасының заңнамалық актілеріне сәйкес халық тіркеліміне енгізілуге жататын жеке тұлғаның негізгі және қосымша дербес деректері, сондай-ақ оны сәйкестендіруге мүмкіндік беретін басқа да мәліметтер.

Ақпарат пайдаланушысы – ақпаратты алатын, тарататын және (немесе) ұсынатын, оны пайдалануға құқығын іске асыратын ақпараттық қатынастар субъектісі.

Ақпараттық жүйенің және (немесе) ақпараттық желінің пайдаланушысы – ақпараттық жүйеге және (немесе) ақпараттық желіге қол жеткізіп, оларды пайдаланатын ақпараттық қатынастар субъектісі.

Ақпарат ұсыну – белгілі бір адамдар тобының ақпаратпен танысуына бағытталған әрекеттер.

Ақпараттық қауіпсіздік жүйесі – құқықтық (заңнамалық) және әкімшілік сипаттағы арнайы шаралар, ұйымдастырушылық іс-шаралар, физикалық және техникалық (бағдарламалық және аппараттық) қорғаныс құралдары, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз етуге арналған арнайы персонал жиынтығы.

Ақпаратты қорғау құралы – ақпаратты қорғауға арналған немесе пайдаланылатын техникалық, бағдарламалық құрал, зат және/немесе материал.

Скам (Scam) – интернеттегі алаяқтық.

Смишинг (Smishing) – алаяқтықтың бір түрі, оның мақсаты – SMS арқылы жіберілген сілтемеге өту немесе зиянды бағдарламалық жасақтаманы жүктеу. Смишинг-хабарлама әдетте банк, мемлекеттік мекеме, байланыс операторы, танымал дүкен немесе лотерея, акциядағы күтпеген жеңіс туралы хабарлама түрінде келеді.

Қауіп-қатер – объектінің жұмыс істеу режимін әдейі немесе кездейсоқ (қасақана емес) бұзу және қорғалатын ақпараттың немесе объектінің басқа да ресурстарының қасиеттерін бұзу мақсатында қауіпті әсер ететін факторларды жүзеге асыруға бағытталған нақты немесе ықтимал іс-әрекеттер.

Ақпараттық қауіпсіздікке төнетін қауіп – ақпараттың құпиялылығының, тұтастығының, қолжетімділігінің бұзылуына, сондай-ақ оны

заңсыз таратуға әкелуі мүмкін ықтимал оқиға, әрекет, процесс немесе құбылыс, бұл ақпарат иесіне, меншік иесіне немесе пайдаланушысына зиян келтіреді.

Фишинг (Phishing) – алаяқтықтың бір түрі, оның мақсаты – электрондық пошта, әлеуметтік желілердегі парақша, интернет-банкинг және басқа сервистерге қол жеткізу үшін құпия деректерді алу.

Цифрлық гигиена – интернет желісінде ақпараттық қауіпсіздікті (анонимділікті емес, қорғауды) қамтамасыз ету үшін адам сақтауы тиіс ережелер жиынтығы. Бұл сандық қауіпсіздік туралы білім саласына жатады.

III. Бағдарламаның тақырыптық бағыттары

«Білім беру ортасының киберқауіпсіздігі және ақпаратты қорғау» бағдарламасының жаңашылдығы мұғалімдерді білім беру үдерісінде цифрлық қауіпсіздікті қамтамасыз етуге бағытталған практикалық білім мен дағдыларды кешенді түрде оқытумен ерекшеленеді. Қолданыстағы цифрлық сауаттылық курстарынан айырмашылығы, бұл бағдарлама мұғалімдердің жеке құзыреттерін дамытуға ғана емес, сонымен қатар оқушыларға цифрлық қауіпсіздік негіздерін оқытуға дайындығын қалыптастыруға бағытталған.

Ғылыми зерттеулер мен практика көрсетіп отырғандай, білім беру ұйымдарындағы цифрлық қауіпсіздік деңгейі көбінесе мұғалімдердің даярлық деңгейіне байланысты. Осы бағдарлама пән мұғалімдерін, сынып жетекшілерін, әдіскерлер мен білім беру ұйымдарының әкімшілігін ақпаратты қорғау, цифрлық этика және оқушылардың желідегі қауіпсіз мінез-құлқын қалыптастыру негіздеріне оқытудың ғылыми негізделген әдістерін ұсынады.

Бағдарлама киберқауіпсіздікті білім беруде нормативтік-құқықтық реттеуден бастап, цифрлық гигиена мен деректерді қорғау негіздерін оқыту әдістемелеріне дейінгі кең ауқымды мәселелерді қамтиды. Курста цифрлық қауіпсіздік талаптарына бейімделген заманауи білім беру бағдарламаларын әзірлеу әдістері, ақпаратты қорғау тәсілдері, киберқауіптерді талдау және алдын алу технологиялары, сондай-ақ оқушылар мен олардың ата-аналарын киберқауіпсіздік қағидаларына тиімді оқыту стратегиялары қолданылады.

Осылайша, бағдарлама мұғалімдерді киберқауіпсіздік мәселелері бойынша даярлаудағы бар олқылықтарды толықтырып қана қоймай, білім беру ортасындағы жалпы цифрлық мәдениеттің артуына ықпал етеді.

IV. Бағдарламаның мақсаты, міндеттері және күтілетін нәтижелері

Бағдарламаның мақсаты – білім беру ортасында киберқауіпсіздікті тиімді қамтамасыз етуге, цифрлық мәдениетті қалыптастыруға және ақпаратты қорғауға дайын педагог кадрларды даярлау.

Бағдарлама педагогтердің цифрлық қауіпсіздік саласындағы кәсіби құзыреттерін дамытуға, деректер мен ақпараттық жүйелерді қорғау бойынша практикалық дағдыларды меңгеруге, сондай-ақ киберқауіпсіздіктің негіздерін оқыту әдістемелерін қалыптастыруға бағытталған. Бұл әдістемелер оқушылардың жас ерекшеліктері мен қажеттіліктерін ескере отырып әзірленеді.

Бағдарлама аясында цифрлық гигиена, интернет-қауіптердің алдын алу, деректерді қорғау стратегиялары, цифрлық этика және білім беру ұйымдарындағы киберқауіпсіздіктің құқықтық аспектілеріне ерекше назар аударылады.

Курстың міндеттері:

1. Тыңдаушыларды киберқауіпсіздік негіздерімен, өзекті қауіп-қатерлермен және білім беру ортасындағы оларды алдын алудың табысты мысалдарымен таныстыру.

2. Ақпараттық қауіпсіздік, цифрлық гигиена және білім беру ұйымдарындағы жеке деректерді қорғау салаларындағы терминология мен негізгі ұғымдарды үйрету.

3. Оқушылар мен педагогтердің интернеттегі қауіпсіз мінез-құлқын, цифрлық мәдениетін және киберқауіптерге қарсы тұру дағдыларын қалыптастыру әдістерін зерделеу.

4. Деректерді қорғаудың заманауи технологияларымен, шифрлау құралдарымен, қолжетімділікті басқару жүйелерімен және бұлтты сервистерді қауіпсіз пайдалану тәсілдерімен таныстыру.

5. Жеке деректерді қорғау мен авторлық құқық саласындағы заңнаманы қоса алғанда, киберқауіпсіздіктің құқықтық және этикалық аспектілерін қарастыру.

6. Тыңдаушыларды оқушылардың жас және психологиялық ерекшеліктерін ескере отырып, киберқауіпсіздік бойынша сабақтар өткізудің әдістемелерімен қамтамасыз ету.

7. Оқу материалдарын бейімдеуді және қауіпсіз цифрлық білім беру ортасын ұйымдастыруды қоса алғанда, білім беру үдерісіне киберқауіпсіздік қағидаларын кіріктіру бойынша ұсынымдар әзірлеу.

Бағдарлама аяқталғаннан кейін қатысушылар:

-Білім беру үдерісін киберқауіпсіздік қағидаттарын ескере отырып тиімді ұйымдастыру, білім беру ортасында жеке деректер мен цифрлық ақпараттың қорғалуын қамтамасыз ету.

- Білім беру ұйымдарында ақпаратты қорғаудың заманауи технологиялары мен әдістерін, оның ішінде аутентификация, шифрлау және қолжетімділікті бақылау құралдарын қолдану.

-Киберқауіпсіздік бойынша оқу материалдарын әзірлеу және бейімдеу, оқушылардың жас ерекшеліктері мен когнитивтік даму деңгейін ескеру.

-Оқушылардың цифрлық сауаттылығын, интернеттегі жауапты мінез-құлық мәдениетін және киберқауіптерге қарсы тұру дағдыларын қалыптастыру.

- Қауіпсіз цифрлық білім беру ортасын құру мақсатында әріптестерімен және техникалық мамандармен өзара әрекеттесу, сондай-ақ оқушылар мен ата-аналарға ақпараттық қауіпсіздік мәселелері бойынша кеңес беру.

Курсты меңгеру нәтижелеріне қойылатын талаптар:

- Түсіну – Тыңдаушылар киберқауіпсіздік қағидаттарын, білім беру ортасындағы негізгі қауіптер мен тәуекелдерді терең түсініп, жеке деректер мен цифрлық ақпаратты қорғаудың маңыздылығын сезінуі тиіс.

- Қабілеттілік – Цифрлық сауаттылықты арттыру бағдарламаларын әзірлеу және бейімдеу, ақпаратты қорғау әдістерін қолдану және цифрлық білім беру ортасының қауіпсіз жұмысын қамтамасыз ету қабілетіне ие болуы қажет.

- Командалық жұмыс дағдылары – Ақпараттық қауіпсіздікті кешенді қорғауды қамтамасыз ету мақсатында әріптестермен, IT-мамандармен, білім беру ұйымдарының әкімшілігімен, сондай-ақ оқушылар мен олардың ата-аналарымен тиімді өзара әрекеттесу қабілеті.

- Цифрлық технологияларды пайдалану – Деректерді қорғау, білім беру платформаларының киберқауіпсіздігін қамтамасыз ету және киберқатерлердің алдын алу үшін заманауи құралдар мен бағдарламалық қамтамасыз етуді меңгеру.

- Бағалау және кері байланыс – Білім беру мекемесінің ақпараттық қауіпсіздігіне аудит жүргізу, осал тұстарын анықтау және оларды жою бойынша ұсыныстар әзірлеу, сондай-ақ цифрлық қауіпсіздік мәселелері бойынша конструктивті кері байланыс беру қабілеті.

- Зерттеу дағдылары – Киберқауіпсіздік саласындағы заманауи үрдістерді талдау, деректерді қорғаудың жаңа әдістері мен тәсілдерін зерттеу, сондай-ақ осы салада өз бетінше зерттеулер жүргізу қабілетіне ие болуы қажет.

- Контекстке бейімделу – Цифрлық білім беру ортасының өзгермелі шарттарына, заңнамалық талаптарға және білім беру мекемесінің техникалық мүмкіндіктеріне сәйкес киберқауіпсіздік шараларын икемді түрде бейімдеу дағдыларын көрсетуі тиіс.

- Кәсіби даму – Киберқауіпсіздік саласындағы біліктілігін үнемі арттыруға, жаңа технологиялар мен әдістерді меңгеруге, кәсіби қауымдастықтар мен конференцияларға белсенді қатысуға ұмтылуы қажет.

- Тиімділікті көрсету – Киберқауіпсіздікті қамтамасыз етудің тиімді стратегияларын әзірлеп, енгізу, нәтижелерін талдау және білім беру мекемесіндегі цифрлық қауіпсіздік деңгейін арттыру қабілетіне ие болуы тиіс.

V. Бағдарламаның құрылымы мен мазмұны

Бағдарламаның құрылымы
(80 академиялық сағат)

№	Тақырып	Дәріс (сағат саны)	Практикалық сабақтар (сағат саны)	Өзіндік жұмыс (сағат саны)	Барлығы
1-модуль. Білім беру саласындағы киберқауіпсіздік негіздері					
1.1	Киберқауіпсіздікке кіріспе: негізгі терминдер, қауіптер және заманауи сын-қатерлер. Білім беру мекемелеріндегі ақпараттық қауіпсіздікті қамтамасыз етуге қатысты нормативтік-құқықтық актілерге шолу.	1	2	3	12
1.2	Мектептер мен жоғары оқу орындарындағы ақпараттық қауіпсіздіктің негізгі аспектілері. Мұғалімнің цифрлық сауаттылық пен желідегі қауіпсіз мінез-құлық мәдениетін қалыптастырудағы рөлі.	1	2	3	
2-модуль. Киберқауіптер және оларды болдырмау әдістері					
2.1	Киберқауіптердің түрлері: фишинг, зиянды бағдарламалар, деректердің таралып кетуі, әлеуметтік инженерия және т.б. Жеке деректерді қорғау әдістері: оқушылар мен педагогтердің	1	2	3	12

	ақпараттық қауіпсіздігін қамтамасыз ету.				
2.2	Білім беру ортасындағы қауіптерді басқару: шабуылдарды талдау және алдын алу. Практикалық кейстер мен нақты кибершабуыл оқиғаларын талдау: білім беру мекемелеріне жасалған шабуылдардың мысалдары.	1	2	3	
3-модуль. Деректерді қорғау және цифрлық гигиена					
3.1	Жеке және корпоративтік ақпаратты қорғаудың негізгі қағидаттары. Білім беру мекемесінің қауіпсіздік саясаты: әзірлеу және енгізу.	1	2	2	10
3.2	Мектептер мен жоғары оқу орындарында қауіпсіз интернетке қол жеткізуді орнату. Цифрлық гигиенаның негіздері: құрылғылар мен бұлттық сервистерді қауіпсіз пайдалану.	1	2	2	
4-модуль. Оқушылар мен педагогтердің ақпараттық қауіпсіздігі					
4.1	Құпиясөздер мен тіркелгілермен жұмыс: көпфакторлы аутентификация және шифрлау. Буллинг пен онлайн-қатерлерге қарсы іс-қимыл: оқушылардың	1	2	3	12

	киберқауіпсіздігін қамтамасыз ету.				
4.2	Әлеуметтік желілер мен мессенджерлердегі қауіпсіздік: жеке деректерді қорғау. Ата-аналармен интернет-қауіпсіздік мәселелері бойынша жұмыс ұйымдастыру.	1	2	3	
5-модуль. Қауіпсіз білім беру процесін ұйымдастыру					
5.1	Білім беру платформалары мен цифрлық ресурстарды қорғаудың негіздері. Қауіпсіз бұлттық сервистермен және оқу үдерісін басқару жүйелерімен (LMS) жұмыс істеу.	1	2	3	12
5.2	Мектеп оқушыларына киберқауіпсіздік негіздерін үйретудің интерактивті әдістері. Киберқауіпсіздік бойынша сабақтар, тренингтер және практикалық жаттығулар өткізу.	1	2	3	
Модуль 6. Инциденттерге шара қолдану және дағдарысты басқару					
6.1	Кибершабуыл немесе деректердің таралуы жағдайында іс-қимыл жоспары. Оқытушы мен әкімшінің инциденттің салдарын жоюдағы рөлі.	1	2	2	10
6.2	Құқық қорғау органдары және IT-мамандарымен қауіптер кезінде өзара	1	2	2	

	әрекеттесу. Білім беру ортасындағы кибершабуылдардың нақты жағдайларын талдау.				
7-Модуль. Киберқауіпсіздіктің болашағы және кәсіби дағдыларды дамыту					
7.1	Киберқауіпсіздік және цифрлық технологиялар саласындағы заманауи үрдістер. Педагогтар мен білім алушыларды этикалық хакерлік және қауіпсіз бағдарламалау негіздеріне оқыту.	1	2	3	12
7.2	Киберқауіпсіздік саласындағы кәсіби даму мүмкіндіктері. Білім беру ортасындағы цифрлық қауіпсіздікті арттыруға арналған жеке іс-қимыл жоспарын әзірлеу.	1	2	3	
	Барлығы	**14**	**28**	**38**	**80**

Бағдарламаның мазмұны

1-модуль. Білім беру саласындағы киберқауіпсіздіктің негіздері

Киберқауіпсіздікке кіріспе: негізгі терминдер, қауіптер және заманауи сын-қатерлер. Білім беру мекемелеріндегі ақпараттық қауіпсіздікті қамтамасыз етуге қатысты нормативтік-құқықтық актілерге шолу. Мектептер мен жоғары оқу орындарындағы ақпараттық қауіпсіздіктің негізгі аспектілері. Мұғалімнің цифрлық сауаттылық пен қауіпсіз онлайн-мәдениетті қалыптастырудағы рөлі.

2-модуль. Киберқауіптер және оларды болдырмау әдістері

Киберқауіптердің түрлері: фишинг, зиянды бағдарламалар, деректердің таралып кетуі, әлеуметтік инженерия және т.б. Жеке деректерді қорғау әдістері: оқушылар мен педагогтердің ақпараттық қауіпсіздігін қамтамасыз ету. Білім беру ортасындағы қауіптерді басқару: шабуылдарды талдау және алдын алу. Практикалық кейстер мен нақты кибершабуыл оқиғаларын талдау: білім беру мекемелеріне жасалған шабуылдардың мысалдары.

3-модуль. Деректерді қорғау және цифрлық гигиена

Жеке және корпоративтік ақпаратты қорғаудың негізгі қағидаттары. Білім беру мекемесінің қауіпсіздік саясаты: әзірлеу және енгізу. Мектептер мен жоғары оқу орындарында қауіпсіз интернетке қол жеткізуді орнату. Цифрлық гигиенаның негіздері: құрылғылар мен бұлттық сервистерді қауіпсіз пайдалану.

4-модуль. Оқушылар мен педагогтердің ақпараттық қауіпсіздігі

Құпиясөздер мен тіркелгілермен жұмыс: көпфакторлы аутентификация және шифрлау. Буллинг пен онлайн-қатерлерге қарсы іс-қимыл: оқушылардың киберқауіпсіздігін қамтамасыз ету. Әлеуметтік желілер мен мессенджерлердегі қауіпсіздік: жеке деректерді қорғау. Ата-аналармен интернет-қауіпсіздік мәселелері бойынша жұмыс ұйымдастыру.

5-модуль. Қауіпсіз білім беру үдерісін ұйымдастыру

Білім беру платформалары мен цифрлық ресурстарды қорғаудың негіздері. Қауіпсіз бұлттық сервистермен және оқу үдерісін басқару жүйелерімен (LMS) жұмыс істеу. Мектеп оқушыларына киберқауіпсіздік негіздерін үйретудің интерактивті әдістері. Киберқауіпсіздік бойынша сабақтар, тренингтер және практикалық жаттығулар өткізу.

6-модуль. Инциденттерге шара қолдану және дағдарысты басқару

Кибершабуыл немесе деректердің таралуы жағдайында іс-қимыл жоспары. Оқытушы мен әкімшінің инциденттің салдарын жоюдағы рөлі. Кибершабуыл немесе деректердің таралуы жағдайында іс-қимыл жоспары. Оқытушы мен әкімшінің инциденттің салдарын жоюдағы рөлі.

7-модуль. Киберқауіпсіздіктің болашағы және кәсіби дағдыларды дамыту

Киберқауіпсіздік және цифрлық технологиялар саласындағы заманауи үрдістер. Педагогтар мен білім алушыларды этикалық хакерлік және қауіпсіз бағдарламалау негіздеріне оқыту. Киберқауіпсіздік саласындағы кәсіби даму мүмкіндіктері. Білім беру ортасындағы цифрлық қауіпсіздікті арттыруға арналған жеке іс-қимыл жоспарын әзірлеу.

Күтілетін нәтижелер:

Курс аяқталғаннан кейін қатысушылар:

– Оқушылар мен педагогтердің деректерін киберқауіптерден тиімді қорғай алады.

– Білім беру мекемелерінде ақпараттық қауіпсіздік саясаттарын әзірлеп, енгізе алады.

– Мектеп оқушылары мен студенттерге киберқауіпсіздік негіздерін оқыта алады.

– Киберинциденттерге уақытылы шара қолданып, олардың салдарын барынша азайта алады.

– Қауіпсіз цифрлық ортаны қалыптастыру үшін ата-аналармен және әріптестерімен тиімді өзара іс-қимыл жасай алады.

VI. Оқу процесін ұйымдастыру

Оқу үдерісінің негізгі бірлігі – сабақ. Оқу материалы тыңдаушыларға бейімделген түрде ұсынылады: түсіндіру, демонстрация, бейнематериалдар, иллюстрациялар және консультациялар арқылы. Курс бірнеше аптаға бөлініп, жалпы көлемі – 80 академиялық сағатты құрайды.

Оқыту үдерісінің ерекшеліктері ретінде белсенді оқыту әдістері мен цифрлық технологияларды қолдануға бағытталған ұйымдастырушылық формалар, әдістер мен тәсілдер қарастырылады. Сабақтарда тыңдаушылардың белсенді қатысуына мән беріледі: топтық жұмыс, кейстерді талдау, проблемалық жағдаяттарды шешу, өзіндік бағалау және кері байланыс ұйымдастырылады.

Ағымдағы бақылау – тапсырмалардың орындалу барысын бақылау және тыңдаушылардың өз бетінше жүзеге асыруы арқылы жүргізіледі.

Тақырыптық бақылау – әр модуль аяқталған соң өткізіледі.

Қорытынды бақылау – курс аяқталғаннан кейін, барлық материалдар жобаның сайтына (https://cyberacademy.ppu.edu.kz/) жүктелгеннен кейін жүргізіледі.

Тыңдаушылар курсты аяқтау үшін киберқауіпсіздік бойынша сабақ әзірлеп, мектеп оқушыларымен жеке жұмыс істеуге арналған шағын жобасын дайындап, оны сайтқа жүктеуі тиіс. Барлық тапсырмалар мазмұны мен рәсімделуі бойынша бейімделген сипатта болады.

VII. Оқу-әдістемелік қамтамасыз ету

Курсты ұйымдастыру барысында қосымша төмендегі материалдар ұсынылады:

– Курста қолдануға арналған дайын оқу материалдары мен оқу презентациялары ұсынылады.

– Онлайн-ресурстар: Электрондық ресурстарға, веб-сайттарға, онлайн-курстарға және цифрлық технологиялармен жұмыс істеуге арналған білім беру платформаларына шартты түрде тегін қолжетімділік беріледі.

– Интерактивті оқу материалдарын жасауға, веб-конференциялар өткізуге, тестілеу және басқа да онлайн-іс-әрекеттерге арналған қосымшаларға шартты түрде тегін қолжетімділік ұсынылады.

– Білім беру технологиялары: Оқытушыларды Learning Management Systems (LMS) сияқты білім беру технологияларын қолдануға үйретуге арналған ақпарат пен ресурстар беріледі.

– Әдістемелік материалдар: Сабақтар мен таратпалық материалдарды әзірлеуге арналған нұсқаулықтар ұсынылады.

– Үздік тәжірибе үлгілері: Балаларға киберқауіпсіздікті оқытуда қолданылатын интерактивті әдістер мен психологиялық-педагогикалық тәсілдер туралы ақпарат ұсынылады.

VIII. Оқу нәтижелерін бағалау

Курсты сәтті аяқтағаннан кейін тыңдаушылар өз сабақ беретін сыныптарында киберқауіпсіздік бойынша жеке сабақтар өткізеді. Барлық оқу материалдары ашық қолжетімділік үшін https://cyberacademy.ppu.edu.kz/ сайтына жүктеледі.

Күтілетін нәтижелер: Бағдарламаны меңгеру нәтижелеріне қойылатын талаптар (жалпы мәдени және кәсіби құзыреттіліктердің қалыптасуы).

Пәнді меңгеру деңгейін бағалау критерийлері

"Қабылданды" бағасы келесі қатысушыларға қойылады:

– курс бағдарламасының негізгі материалын келесі оқуға және болашақ мамандығы бойынша жұмыс істеуге жеткілікті көлемде меңгергендерге.

– бағдарламалық тапсырмаларды толық орындағандарға.

– қажетті білімге ие, ауызша жауап беру немесе жазбаша тапсырма орындау кезінде жол берілген қателіктері рұқсат етілетін деңгейде болғандарға.

– оқыған материалдың көп бөлігін көрсете алған және оқытушының түсіндіруінен кейін жіберілген қателіктерді саналы түрде түсініп, түзете алғандарға.

"Қабылданбады" бағасы келесі жағдайларда қойылады:

– тыңдаушы негізгі материал бойынша айтарлықтай олқылықтарды көрсетсе, бағдарлама аясында тапсырылған міндеттерді орындау барысында принципті қателер жіберсе; Қатысушы оқыған материалдың көп бөлігін меңгермеген болса, практикалық тапсырмаларды шеше алмаса және қосымша сұрақтарға жауап бере алмаса.

Аралық бақылау практикалық сабақтар барысында интерактивті сұрақ-жауап талқылауы және қатысушылардың өзіндік жұмыс (ҚӨЖ) аясында тапсырмаларды орындауын тіркеу арқылы жүргізіледі. Аралық бақылау бойынша максималды балл – 60 балл.

Қорытынды бақылау аралық бақылау бойынша ең жоғары балл мөлшерінде – 40 балл түрінде жүзеге асырылады. Курсты сәтті аяқтау үшін қатысушы 100 баллдан кемінде 50 балл жинауы қажет.

Курсты аяқтағаннан кейін қатысушылар білуі тиіс:

– Білім беру ортасындағы киберқауіпсіздіктің негізгі қағидаттары, мақсаттары және нормативтік талаптары.

– Мектептегі ақпараттық қауіпсіздікке төнетін қазіргі заманғы қауіп-қатерлер: фишинг, деректердің таралуы, әлеуметтік инженерия, зиянды бағдарламалық қамтамасыз ету.

– Оқушылар мен педагогтердің дербес деректерін қорғауды қоса алғанда, мектепте қауіпсіз цифрлық ортаны ұйымдастыру әдістемесі.

– Педагогтер, оқушылар және ата-аналар үшін цифрлық гигиена мен ақпараттық қауіпсіздік қағидаттары.

– Киберэтика негіздері. білім беру саласындағы ақпарат пен дербес деректерді қорғаудың құқықтық аспектілері.

– Әр түрлі жас топтарындағы оқушылар үшін киберқауіпсіздік материалдарын бейімдеу әдістері.

Істей алуы тиіс:

– Әр түрлі жас ерекшеліктеріне және цифрлық сауаттылық деңгейіне сәйкес киберқауіпсіздік бойынша оқу материалдары мен оқыту әдістерін бейімдеу.

– Қолжетімді, қауіпсіз және ынталандырушы оқу ортасын құру үшін цифрлық технологиялар мен интерактивті құралдарды пайдалану.

– Киберқауіпсіздік саласында тиімді оқыту ұйымдастыру мақсатында командалық жұмыс дағдыларын дамыту, әріптестермен, ассистент-педагогтермен және IT-мамандармен өзара әрекеттесу.

– Оқушылардың цифрлық қауіпсіздік деңгейін бағалау, цифрлық қауіптерді диагностикалау және жеке ұсыныстар әзірлеу.

– Киберқауіпсіздік бойынша жобалық тапсырмалар әзірлеу және бейімдеу, оның ішінде практикалық кейстер, киберинцидент сценарийлері және цифрлық гигиена бойынша тапсырмалар жасау.

Курсты аяқтағаннан кейін қатысушылар білім беру ортасындағы киберқауіпсіздік бойынша кешенді түсінікке ие болып, оқушылар мен педагогтердің цифрлық қауіпсіздігін тиімді қамтамасыз ету үшін қажетті арнайы дағдыларды меңгереді. Олар қауіпсіз цифрлық тәжірибелерді енгізе алады, киберқауіпсіздік бойынша оқу материалдарын бейімдеп, мектепте ақпараттық қауіпсіздік мәдениетін қалыптастыра алады.

IX. Курстан кейінгі қолдау

Курстан кейінгі қолдау келесі бағыттарды қамтиды:

– Қатысушыларға жобаларды жүзеге асыру барысында менторлық қолдау көрсету.

– Білім беру саласындағы киберқауіпсіздік жөніндегі сарапшылармен вебинарлар мен семинарлар өткізу.

– Тәжірибе мен ресурстармен алмасу үшін топтық талқылаулар мен форумдар ұйымдастыру.

– Қатысушылардың оқу портфолиосы, өзіндік бағалау және жобалар арқылы бағалануы.

Бұл бағдарлама тыңдаушыларға білім беру саласындағы киберқауіпсіздік бойынша алған білімдері мен дағдыларын сенімді түрде енгізуге мүмкіндік беріп, білім сапасын арттыруға ықпал етеді.

X. Негізгі және қосымша әдебиеттер тізімі

Негізгі әдебиеттер:

1. Қазақстан Республикасының 2007 жылғы 27 шілдедегі № 319-III «Білім туралы» Заңы, 2025 жылғы 15 сәуірдегі өзгерістер мен толықтырулармен.

2. Қазақстан Республикасының 2015 жылғы 24 қарашадағы «Ақпараттандыру туралы» Заңы, 2025 жылғы 8 қаңтардағы өзгерістер мен толықтырулармен.

3. Қазақстан Республикасының 2024 жылғы 1 шілдедегі № 103-VIII ЗРК «Ғылым және технологиялық саясат туралы» Заңы.

4. Балаларға қатысты буллингтің (қудалау) алдын алу қағидалары, Қазақстан Республикасы Оқу-ағарту министрінің 2022 жылғы 21 желтоқсандағы № 506 бұйрығы.

5. Қазақстан Республикасының 2022 жылғы 3 мамырдағы № 118-VII ЗРК «Баланың құқықтарын қорғау, білім беру, ақпарат және ақпараттандыру мәселелері бойынша Қазақстан Республикасының кейбір заңнамалық актілеріне өзгерістер мен толықтырулар енгізу туралы» Заңы.

6. Қазақстан Республикасы Президентінің Қазақстан халқына Жолдауы – «Қазақстан-2050» стратегиясы аясындағы мемлекеттің жаңа саяси бағыты, 2012 жылғы 14 желтоқсан. Білім беру саласындағы басымдықтар: «Біз заманауи білім беру жүйесіне қашықтан оқыту мен онлайн оқытуды қоса алғанда, инновациялық әдістерді, шешімдер мен құралдарды жедел енгізуіміз қажет. Бұл әрбір азамат үшін қолжетімді болуы тиіс».

7. Қазақстан Республикасының 2029 жылға дейінгі Ұлттық даму жоспары. Бұл құжат Қазақстан Республикасы Президентінің 2024 жылғы 24 сәуірдегі № 611 Жарлығымен бекітілген.

8. Мектепке дейінгі тәрбиелеу мен оқытудың, бастауыш, негізгі орта және жалпы орта, техникалық және кәсіптік, орта білімнен кейінгі білім берудің мемлекеттік жалпыға міндетті стандарттары, Қазақстан Республикасы Оқу-ағарту министрінің 2022 жылғы 3 тамыздағы № 348 бұйрығы, 2025 жылғы 15 сәуірдегі өзгерістер мен толықтырулармен.

9. Педагог қызметкерлер мен оларға теңестірілген тұлғалардың үлгілік біліктілік сипаттамалары, Қазақстан Республикасы Білім және ғылым министрінің 2009 жылғы 13 шілдедегі № 338 бұйрығы – Қазақстан Республикасы Білім және ғылым министрінің 2020 жылғы 30 сәуірдегі № 169 бұйрығының редакциясында және Қазақстан Республикасы Оқу-ағарту министрінің 2025 жылғы 30 сәуірдегі № 98 бұйрығымен енгізілген өзгерістермен.

10. Киберқауіпсіздік тұжырымдамасы («Киберқалқан Қазақстан»), Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген (2023 жылғы 17 наурыздағы өзгерістермен).

11. 2023–2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасы, Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысымен бекітілген.

12. «Педагог» кәсіби стандарты, Қазақстан Республикасы Оқу-ағарту министрінің міндетін атқарушының 2022 жылғы 15 желтоқсандағы № 500 бұйрығымен бекітілген.

13. Киберқауіпсіздік стандарты – ҚР СТ IEC/PAS 62443-3-2017 «Өнеркәсіптік коммуникациялық желілер. Желі мен жүйенің қорғалуы (киберқауіпсіздік). 3-бөлім. Өнеркәсіптік процестерді өлшеу және басқарудың қорғалу деңгейі (киберқауіпсіздік) (IEC PAS 62443-3:2008, IDT).

14. Ақпараттық қауіпсіздік бөлімшелерінің басшылары мен қызметкерлерінің құзыреттеріне қойылатын талаптар, оның ішінде ақпараттық қауіпсіздікті қамтамасыз етуге жауапты тұлғалардың біліктілігін арттыру талаптары – Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі басқармасының 2020 жылғы 21 қыркүйектегі № 89 қаулысы, 2025 жылғы 20 наурыздағы өзгерістермен.

15. Қазақстан Республикасы Үкіметінің 2024 жылғы 13 мамырдағы № 372 қаулысы, 2016 жылғы 20 желтоқсандағы № 832 «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздік саласындағы бірыңғай талаптарды бекіту туралы» қаулыға өзгерістер мен толықтырулар енгізу туралы.

Қосымша әдебиеттер:

1. Yusif S., Hafeez-Baig A. Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework //Journal of Applied Security Research. – 2023. – Т. 18. – №. 2. – С. 267-288.

URL: https://doi.org/10.1080/19361610.2021.1989271 (на англ.).

2. Harris M. A., Martin R. Promoting cybersecurity compliance //Cybersecurity education for awareness and compliance. – IGI Global, 2019. – С. 54-71. URL: https://www.igi-global.com/chapter/promoting-cybersecurity-compliance/225917 (на англ.).

3. Vasileiou I., Furnell S. (ed.). Cybersecurity education for awareness and compliance. – IGI Global, 2019. – 305 с. (на англ.).

4. Sadiku M. N. O., Chukwu U. C., Sadiku J. O. Cybersecurity for Education //European Journal Of Innovation in Nonformal Education. – 2023. – Т. 3. – №. 6. – С. 182-188. URL: http://www.inovatus.es/index.php/ejine/article/view/1828/1831 (на англ.).

5. Kitchenham B., Charters S. Guidelines for performing systematic literature reviews in software engineering. – 2007. URL: https://www.elsevier.com/data/promis_misc/525444systematicreviewsguide.pdf (на англ.).

6. Belastock E. Our Biggest Nightmare Is Here //Education Next. – 2022. – Т. 22. – №. 2. URL: https://go.gale.com/ps/ (на англ.).

7. Torres M., Mullins A., Thompson N. Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector // ACIS 2022 Proceedings. 96. – 2022. – С. 1-10. URL: https://aisel.aisnet.org/acis2022/96/ (на англ.).

8. Richardson M. D. et al. Planning for Cyber Security in Schools: The Human Factor //Educational Planning. – 2020. – Т. 27. – №. 2. – С. 23-39. URL: https://eric.ed.gov/?id=EJ1252710 (на англ.).

9. Ulven J. B., Wangen G. A systematic review of cybersecurity risks in higher education //Future Internet. – 2021. – Т. 13. – №. 2. – С. 1-40. URL: https://doi.org/10.3390/fi13020039 (на англ.).

10. White T. About the K12 Security information exchange: Annual report. – 2022. – 30 с. URL: https://info.identityautomation.com/hubfs/PDFs/StateofK12Cybersecurity2022.pdf (на англ.).

11. Diana I., Ismail I. A., Zairul M. Cyber Risk among High School Students: A Thematic Review //Malaysian Journal of Social Sciences and Humanities (MJSSH). – 2023. – Т. 8. – №. 4. – С. 1-19. URL: https://doi.org/10.47405/mjssh.v8i4.2251 (на англ.).

12. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832. URL: https://adilet.zan.kz/rus/docs/P1600000832.