ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

А.БАЙТҰРСЫНОВ АТЫНДАҒЫ ҚОСТАНАЙ ӨҢІРЛІК УНИВЕРСИТЕТІ

СҰЛТАНҒАЗИН ОҚУЛАРЫ

«ҚАЗІРГІ БІЛІМ БЕРУДІ ДАМЫТУДЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ»
ХАЛЫҚАРАЛЫҚ
ҒЫЛЫМИ-ПРАКТИКАЛЫҚ
КОНФЕРЕНЦИЯ

МАТЕРИАЛДАРЫ

СУЛТАНГАЗИНСКИЕ ЧТЕНИЯ

МАТЕРИАЛЫ

МЕЖДУНАРОДНОЙ
НАУЧНО-ПРАКТИЧЕСКОЙ
КОНФЕРЕНЦИИ
«АКТУАЛЬНЫЕ ВОПРОСЫ
РАЗВИТИЯ СОВРЕМЕННОГО
ОБРАЗОВАНИЯ»

Қостанай, 2023

УДК 378 (094)
ББК 74.58
Қ 22

Қ 22

«Қазіргі білім беруді дамытудың өзекті мәселелері»: «СҰЛТАНҒАЗИН ОҚУЛАРЫ-2023» Халықаралық ғылыми-тәжірибелік конференцияның материалдары, 2023 жылдың 15 наурызы. Қостанай: А.Байтұрсынов атындағы Қостанай өңірлік университеті, 2023. – 427 б.
«Актуальные вопросы развития современного образования»: Материалы международной научно-практической конференции «СУЛТАНГАЗИНСКИЕ ЧТЕНИЯ-2023», 15 марта 2023 года. Костанай: Костанайский региональный университет имени А.Байтурсынова, 2023. – 427 с.

ISBN 978-601-356-257-5

«Сұлтанғазин оқулары-2023» халықаралық ғылыми-тәжірибелік конференциясының «Заманауи білім беруді дамытудың өзекті мәселелері» жинағында жаратылыстану-ғылыми білім берудің мәселелері мен болашағына арналған ғылыми мақалалар жинақталған, жалпы және кәсіптік білім берудің психологиялық-педагогикалық аспектілері қарастырылған, педагогикалық білім берудің ақпараттандыру және дамытудың қазіргі тенденциялары мен технологиялары мәселелері қозғалады.

Осы жинақтың материалдары ғалымдар мен жоғары оқу орындарының оқытушыларына, магистранттар мен студенттерге пайдалы болуы мүмкін.

В сборнике Международной научно-практической конференции «Султангазинские чтения-2023» «Актуальные вопросы развития современного образования»: представлены научные статьи по проблемам и перспективам естественно-научного образования, рассматриваются психолого-педагогические аспекты общего и профессионального образования, затронуты вопросы информатизации и современных тенденций и технологий развития педагогического образования.

Материалы данного сборника могут быть интересны ученым, преподавателям высших учебных заведений, магистрантам и студентам.

ISBN 978-601-356-257-5

УДК 378 (094)
ББК 74.58

достаточно открыто, однако доступ на сайты этих компаний ограничен. В казахстанском же сегменте на электронных платформах достаточно часто встречаются записи объявлений о продаже соответствующего оборудования, причем по довольно низкой цене. Все это говорит о том, что защищенность GSM-сетей несколько преувеличена. [4]

Конечно, представленный в данной статье материал не может охватить абсолютную полноту раскрытия проблемы информационной безопасности в мобильных системах связи, но в нём представлены наиболее значимые аспекты и способы решения данного вопроса.

Список литературы:

1. А.В. Заряев, В.А. Минаев, С.В. Скрыль, В.Ю. Карпычев. Защита информации в мобильных системах связи. Воронеж: Воронежский ин-т МВД России, 2004. 138 с.)
2. А.А. Чекалин, А.В. Заряев, С.В. Скрыль, В.А. Вохминцев. Защита информации в системах мобильной связи. М.: Горячая линия - Телеком, 2005. 171 с.
3. Сетевой ресурс https://detsys.ru/article/bezopasnost_gsm
4. Сетевой ресурс https://www.bibliofond.ru/view.aspx?id=651120

УДК 004.056.2

АҚПАРАТТЫҚ ҚАУІПСІЗДІК МАҢЫЗДЫЛЫҒЫ ЖӘНЕ АЛДЫН АЛУ ШАРАЛАРЫНЫҢ ҚАЖЕТТІЛІГІ

Әлім Әлішер, 2 курс магистранты, Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан, E-mail: alim.alisher@gmail.com

Аңдатпа

Өзектілігі: Ақпараттық қауіпсіздік – бұл ақпаратты, сондай-ақ оның маңызды элементтерін, соның ішінде осы ақпаратты пайдалануға, сақтауға және беруге арналған жүйелер мен жабдықтарды сақтау және қорғау.

Мақсаты: Ақпараттық қауіпсіздікті қамтамасыз ету-ақпараттық деректерді және қолдау инфрақұрылымын кездейсоқ немесе қасақана араласудан қорғау, бұл деректердің жоғалуына немесе олардың рұқсатсыз өзгеруіне әкелуі мүмкін.

Түйінді сөздер: Ақпараттық қауіпсіздік, қолжетімділік, құпиялылық, тұтастық, ақпараттық қауіпсіздік саясаты.

Аннотация

Актуальность: Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации.

Цель: Обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения.

Ключевые слова: Информационная безопасность, доступность, конфиденциальность, целостность, политика информационной безопасности.

Abstract

Relevance: Information security is the preservation and protection of information, as well as its most important elements, including systems and equipment designed to use, save and transmit this information.

Goal:Information security – to protect information data and supporting infrastructure from accidental or intentional interference, which may cause data loss or unauthorized modification.

Keywords: Information security, accessibility, confidentiality, integrity, information security policy.

Ақпараттық қауіпсіздік(ағылш. *Ақпараттық қауіпсіздік*, сонымен қатар-ағылш. InfoSec) - ақпаратқа рұқсатсыз қол жеткізуді, пайдалануды, ашуды, бұрмалауды, Өзгертуді, зерттеуді, жазуды немесе жоюды болдырмау тәжірибесі. Бұл әмбебап ұғым деректер қабылдай алатын формаға қарамастан қолданылады (электронды немесе, мысалы, физикалық). Ақпараттық қауіпсіздіктің негізгі міндеті-қолданудың орындылығын ескере отырып және ұйымның жұмысына ешқандай зиян келтірместен деректердің құпиялылығын, тұтастығын және қол жетімділігін теңдестірілген қорғау. Бұған, негізінен, негізгі құралдар мен материалдық емес активтерді, қауіп көздерін, осалдықтарды, ықтимал әсер ету дәрежесін және тәуекелдерді басқару мүмкіндіктерін анықтауға мүмкіндік беретін

көп сатылы тәуекелдерді басқару процесі арқылы қол жеткізіледі. Бұл процесс тәуекелдерді басқару жоспарының тиімділігін бағалаумен бірге жүреді.

Осы қызметті стандарттау үшін ғылыми және кәсіби қауымдастықтар ақпаратты қорғаудың техникалық шаралары, құқықтық жауапкершілік, сондай-ақ пайдаланушылар мен әкімшілерді оқыту стандарттары саласында базалық әдіснаманы, саясатты және индустриялық стандарттарды әзірлеуге бағытталған тұрақты ынтымақтастықта болады. Бұл стандарттау деректерге қол жеткізу, өңдеу, сақтау және беру тәсілдерін реттейтін көптеген заңнамалық және нормативтік актілердің әсерінен айтарлықтай дамиды. Алайда, ұйымда кез-келген стандарттар мен әдістемелерді енгізу, егер үздіксіз жетілдіру мәдениеті дұрыс егілмеген болса, тек үстірт әсер етуі мүмкін.

Кәсіпорында ақпараттық қауіпсіздік жүйелерін сәтті енгізу үшін үш негізгі қағиданы ұстану қажет:

- Құпиялылық.Бұл қажетсіз немесе рұқсатсыз жария етудің алдын алу үшін кәсіпорын деректерімен, активтерімен және іскерлік операциялардың әртүрлі кезеңдеріндегі ақпаратпен қауіпсіздіктің жеткілікті деңгейіне кепілдік беру үшін бақылауды іске қосуды білдіреді. Құпиялылық ақпаратты сақтау кезінде, сондай-ақ оның форматына қарамастан қатардағы ұйымдар арқылы транзит кезінде сақталуы керек.
- Тұтастық. Тұтастық корпоративтік ақпараттың ішкі және сыртқы дәйекті болуын қамтамасыз етумен байланысты басқару элементтерімен айналысады. Тұтастық сонымен қатар ақпараттың бұрмалануын болдырмауға кепілдік береді.
- Қол жетімділік. Қол жетімділік уәкілетті тұлғалардың ақпаратына сенімді және тиімді қол жеткізуді қамтамасыз етеді.қажет болған жағдайда ақпарат пен деректерге қол жеткізу үшін желілік орта болжамды түрде әрекет етуі керек. Ақаулыққа байланысты жүйені қалпына келтіру ақпараттың қол жетімділігіне қатысты маңызды фактор болып табылады және мұндай қалпына келтіру жұмысына теріс әсер етпейтіндей етіп қамтамасыз етілуі керек.

Ақпараттық қауіпсіздікке төнетін қауіптер әр түрлі формада болуы мүмкін. 2018 жылы "қызмет ретінде қылмысқа" байланысты қауіптер ең ауыр болып саналады (ағылш. Crime-as-a-Service), Заттар интернеті, жеткізу тізбектері және реттеушілер талаптарының күрделенуі[. "Қызмет ретінде қылмыс" - бұл жетілген қылмыстық қауымдастықтардың киберқылмыскерлерге қол жетімді бағамен қараңғы веб-нарықта қылмыстық қызмет пакеттерін ұсыну моделі. Бұл соңғысына киберқылмысты жаппай құбылысқа айналдырып, техникалық күрделілігі немесе қымбаттығы жоғары болғандықтан бұрын қол жетімсіз хакерлік шабуылдар жасауға мүмкіндік береді. Ұйымдар заттар интернетін белсенді түрде енгізуде, олардың құрылғылары көбінесе қауіпсіздік талаптарын ескермей жасалған, бұл шабуыл үшін қосымша мүмкіндіктер ашады. Сонымен қатар, заттар интернетінің қарқынды дамуы мен күрделенуі оның ашықтығын төмендетеді, бұл анық емес анықталған құқықтық нормалар мен шарттармен бірге ұйымдарға өз клиенттерінің құрылғылар жинаған дербес деректерін өздері білмей-ақ өз қалауы бойынша пайдалануға мүмкіндік береді. Сонымен қатар, ұйымдардың өздері үшін Интернет құрылғылары жинаған деректердің қайсысы сыртқа жіберілетінін бақылау қиынға соғады. Жеткізу тізбегінің қауіптілігі мынада: ұйымдар өз жеткізушілеріне әртүрлі құнды және құпия ақпаратты беруге бейім, бұл оны тікелей бақылауды жоғалтады. Осылайша, бұл ақпараттың құпиялылығын, тұтастығын немесе қолжетімділігін бұзу қаупі айтарлықтай артады. Реттеушілердің жаңа және жаңа талаптары ұйымдардың өмірлік маңызды ақпараттық активтерін басқаруды едәуір қиындатады. Мысалы, 2018 жылы Еуроодақта қолданысқа енгізілген дербес деректерді қорғаудың жалпы регламенті (ағылш. General Data Protection Regulation, GDPR), кез келген ұйымнан кез келген уақытта өз қызметінің немесе жеткізу тізбегінің кез келген учаскесінде қандай жеке деректердің бар екенін және қандай мақсатта бар екенін, олардың қалай өңделетінін, сақталатынын және қорғалатынын көрсетуді талап етеді. Сонымен қатар, бұл ақпарат тек уәкілетті органдардың тексерулері барысында ғана емес, сонымен қатар жеке тұлғаның — осы деректердің иесінің бірінші талабы бойынша ұсынылуы керек. Мұндай сәйкестікті сақтау айтарлықтай бюджет қаражаты мен ресурстарды ұйымның ақпараттық қауіпсіздігінің басқа міндеттерінен алшақтатуды талап етеді. Дербес деректерді өңдеуді ретке келтіру ұзақ мерзімді перспективада ақпараттық қауіпсіздікті жақсартуды көздесе де, қысқа мерзімді жоспарда ұйымның тәуекелдері айтарлықтай артады.

Қауіп-бұл қорғалатын ақпараттық ресурстарды иемденудің мүмкін немесе жарамды әрекеттері.

Құпия деректердің сақталу қаупінің көздері бәсекелес компаниялар, зиянкестер, басқару органдары болып табылады. Кез-келген қауіптің мақсаты-деректердің тұтастығына, толықтығына және қол жетімділігіне әсер ету.

Қауіптер ішкі немесе сыртқы болып табылады. Сыртқы қауіптер деректерге сырттан қол жеткізу әрекеттерін білдіреді және серверлерді, желілерді, жұмысшылардың аккаунттарын бұзумен және техникалық ағып кету арналарынан ақпаратты оқумен (қателер, камералар, аппараттық құралдар арқылы акустикалық оқу, терезелер мен архитектуралық конструкциялардан діріл-акустикалық ақпаратты алу) бірге жүреді.

Ішкі қауіптер қызметкерлердің, жұмыс бөлімінің немесе фирма әкімшілігінің заңсыз әрекеттерін білдіреді. Нәтижесінде құпия ақпаратпен жұмыс істейтін жүйені пайдаланушы бөгде адамдарға ақпарат бере алады. Іс жүзінде мұндай қауіп басқаларға қарағанда жиі кездеседі. Қызметкер бірнеше жылдар бойы бәсекелестерге құпия деректерді "ағыза" алады. Бұл оңай жүзеге асырылады, өйткені қауіпсіздік әкімшісі уәкілетті пайдаланушының әрекеттерін қауіп ретінде көрсетпейді.

Ішкі АҚ қауіптері адам факторымен байланысты болғандықтан, оларды бақылау және басқару қиынырақ. Қызметкерлерді тәуекел тобына бөлу арқылы оқиғалардың алдын алуға болады. Бұл тапсырманы психологиялық профильдер жасауға арналған автоматтандырылған модуль – "Serchinform ProfileCenter" жеңе алады.

Рұқсатсыз кіру әрекеті бірнеше жолмен жүруі мүмкін:

- құпия деректерді бөгде адамдарға бере алатын, физикалық медианы ала алатын немесе баспа құжаттары арқылы қорғалатын ақпаратқа қол жеткізе алатын қызметкерлер арқылы;
- бағдарламалық жасақтаманың көмегімен шабуылдаушылар "логин-пароль" жұптарын ұрлауға, деректерді транскрипциялау, ақпаратты рұқсатсыз көшіру үшін криптографиялық кілттерді ұстауға бағытталған шабуылдар жасайды.
- автоматтандырылған жүйенің аппараттық компоненттерінің көмегімен, мысалы, тыңдау құрылғыларын енгізу немесе ақпаратты қашықтықтан оқудың аппараттық технологияларын қолдану (бақыланатын аймақтан тыс).

Көптеген адамдар қандай да бір жолмен ақпараттық қауіпсіздікке қауіп төндіреді. Мысалы, олар зиянды бағдарламалардың (вирустар мен құрттар, трояндық бағдарламалар, төлем бағдарламалары), фишингтің немесе жеке басын ұрлаудың құрбаны болады. Фишинг (ағылш. Phishing) құпия ақпаратты (мысалы, тіркелгі, құпия сөз немесе несие картасы деректері) иелену үшін алаяқтық әрекетті білдіреді. Әдетте, Интернет пайдаланушылары кез-келген ұйымның (банк, интернет-дүкен, әлеуметтік желі және т.б.) бастапқы сайтынан ерекшеленбейтін алаяқтық веб-сайтқа азғыруға тырысады. Әдетте, мұндай әрекеттер жалған сайттарға сілтемелері бар ұйымның атынан жалған электрондық хаттарды жаппай жіберу арқылы жүзеге асырылады. Браузерде осындай сілтемені ашқаннан кейін, күдікті пайдаланушы алаяқтардың меншігіне айналатын тіркелгі деректерін енгізеді. Identity Theft термині ағылш. — "жеке тұлғаны ұрлау" 1964 жылы ағылшын тілінде біреудің жеке деректері (мысалы, аты-жөні, банк жүйесіндегі шоты немесе несие картасының нөмірі, көбінесе фишинг арқылы алынған) алаяқтық және басқа қылмыстар жасау үшін қолданылатын әрекеттерді көрсету үшін пайда болды. Қылмыскерлер заңсыз қаржылық артықшылықтар, несиелер алған немесе басқа қылмыстар жасаған адам көбінесе айыпталушыға айналады, бұл оған ауыр қаржылық және заңды әсер етуі мүмкін. Ақпараттық қауіпсіздік жеке өмірге тікелей әсер етеді, оның анықтамасы әр түрлі мәдениеттерде әр түрлі болуы мүмкін.

Мемлекеттік органдар, Қарулы Күштер, корпорациялар, қаржы институттары, Денсаулық сақтау мекемелері және жеке кәсіпкерлер өз қызметкерлері, клиенттері, өнімдері, ғылыми зерттеулері және қаржылық нәтижелері туралы құпия ақпараттың едәуір көлемін үнемі жинақтап отырады. Мұндай ақпараттың бәсекелестердің немесе киберқылмыскерлердің қолына түсуі ұйым мен оның клиенттері үшін ауқымды құқықтық салдарға, орны толмас қаржылық және беделді шығындарға әкелуі мүмкін. Бизнес тұрғысынан ақпараттық қауіпсіздік шығындарға қатысты теңдестірілген болуы керек; Гордон-Лобтың экономикалық моделі осы мәселені шешуге арналған математикалық аппаратты сипаттайды.Ақпараттық қауіпсіздік қатерлеріне немесе ақпараттық тәуекелдерге қарсы тұрудың негізгі әдістері:

- төмендету-осалдықтарды жою және қауіптердің алдын алу үшін қауіпсіздік және қарсы іс-қимыл шараларын енгізу;
- беру-қауіптерді іске асыруға байланысты шығындарды үшінші тұлғаларға: сақтандыру немесе аутсорсингтік компанияларға ауыстыру;
- егер қауіпсіздік шараларын іске асыру құны қатерді іске асырудан болатын ықтимал залалдан асып кеткен жағдайда, қаржылық резервтерді қабылдау-қалыптастыру;
- бас тарту-тым қауіпті әрекеттерден бас тарту.

Аппараттық және бағдарламалық АҚ

Барлық заманауи операциялық жүйелер бағдарламалық жасақтама деңгейінде кіріктірілген деректерді қорғау модульдерімен жабдықталған. MAC OS, Windows, Linux, iOS дискілердегі деректерді шифрлау және басқа құрылғыларға тасымалдау процесінде өте жақсы жұмыс істейді. Дегенмен, құпия ақпаратпен тиімді жұмыс жасау үшін қосымша қорғаныс модульдерін пайдалану маңызды.

Пайдаланушы ОЖ деректерді желі арқылы беру кезінде қорғамайды, ал қорғаныс жүйелері корпоративтік желі арқылы айналатын ақпараттық ағындарды және солтүстікте деректерді сақтауды бақылауға мүмкіндік береді.

Аппараттық-бағдарламалық қорғаныс модулі әдетте топтарға бөлінеді, олардың әрқайсысы сезімтал ақпаратты қорғау функциясын орындайды:

Сәйкестендіру деңгейі-стандартты немесе көп деңгейлі аутентификацияны, биометрияны (бетті тану, саусақ ізін сканерлеу, дауысты жазу және басқа әдістерді) пайдалана алатын пайдаланушыларды танудың кешенді жүйесі.

Шифрлау деңгейі жіберуші мен алушы арасында кілттермен алмасуды қамтамасыз етеді және жүйенің барлық деректерін шифрлайды/шифрын ашады.

Ақпараттық қауіпсіздіктің құқықтық негізін мемлекет қамтамасыз етеді. Ақпаратты қорғау халықаралық конвенциялармен, Конституциямен, федералдық заңдармен және заңға тәуелді актілермен реттеледі.

Қазақстанда киберқауіпсіздік саласын дамыту мәселелеріне жіті көңіл бөлінуде. Мемлекеттік органдармен, ҮЕҰ және бизнеспен бірлесіп жүргізілетін жұмыстың нәтижесінде біздің еліміз киберқауіпсіздіктің жаһандық индексіндегі өз позициясын қарқынды жақсарта түсті. Қазір Қазақстанкиберқауіпсіздік саласы бойынша 40-шы орында. Айта кету керек, өткен жылы біздің еліміз 82 орында болған еді.

Өткен жылдар ішінде еліміздің киберқауіпсіздік саласын дамытудың негізгі тұжырымдамалық тәсілдері әзірленді. 2022 жылға дейін әрекет ететін "Қазақстанның киберқауіпсіздігі" тұжырымдамасы әзірленіп бекітілді. Осымен бірге, бірқатар заңнамалық актілер мен көптеген салалық бұйрықтар қолданысқа енді. Бұдан басқа, зиянды кодты зерттеу бойынша АҚ саласында сынақ зертханалары құрылып, ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы (компьютерлік инциденттерге жеке әрекет ету қызметі (CERT), 7 жедел ақпараттық қауіпсіздік орталығы (SOC)) жұмысын бастады, аталған мамандық бойынша білім гранттарының саны көбейді және т. б.

Ақпараттық қауіпсіздік және жеке деректерді қорғау саласындағы ахуалды одан әрі жақсарту үшін ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі Ақпараттық қауіпсіздік комитетіне азаматтардың жеке басына қатысты деректер өңделетін ақпараттық жүйелердің иелеріне аудит және тексеру жүргізу үшін жеке деректерді қорғау функциясын беру туралы мәселе көтерді.

Қорыта келе, ақпарат-бұл басқа маңызды іскери активтер сияқты ұйымның бизнесі үшін үлкен маңызға ие, сондықтан жеткілікті түрде қорғалуы керек актив. Ақпараттық қауіпсіздік-ақпараттың иелеріне немесе пайдаланушыларына, сондай-ақ ақпараттық саладағы адам мен азаматтың, қоғам мен мемлекеттің құқықтары мен мүдделеріне орнықты даму және ақпараттық тәуелсіздік қамтамасыз етілетін нақты және әлеуетті қатерлерден зиян келтіруге әкеп соғатын табиғи немесе жасанды сипаттағы кездейсоқ немесе қасақана әсерлерден ақпарат пен қолдау инфрақұрылымының қорғалуы. Ақпараттық қауіпсіздікті немесе ақпаратты қорғауды қамтамасыз ету деп оның құпиялылығын, тұтастығын және қолжетімділігін сақтау түсініледі. Ақпараттық қауіпсіздікке бағдарламалық және аппараттық қамтамасыз етудің саясатын, рәсімдерін, процестерін, ұйымдық құрылымдары мен функцияларын қоса алғанда, бақылау шараларының тиісті жиынтығын іске асыру арқылы қол жеткізіледі. Ақпараттық қауіпсіздік саясаты (бұдан әрі – саясат) - ақпаратты, оның ішінде таралуы шектеулі ақпаратты (қызметтік ақпарат), ақпараттық процестерді қорғау жөніндегі алдын алу шараларының кешені және өз қызметінде Қазақстан Республикасы Энергетика министрлігінің, оның ведомстволары мен ведомстволық бағыныста ұйымдарының ақпараттық жүйелерін пайдаланушылардың атына қойылатын талаптарды қамтиды.

Әдебиеттер тізімі:

1. Сингх, Саймон. Книга шифров : Тайная история шифров и их расшифровки. — М. : Издательство «АСТ», 2009. — 448 с..
2. СёрчИнформ КИБ,ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ //Защита информациис помощью DLP-системы. 2019.№ 7. URL: https://searchinform.ru/informatsionnaya-bezopasnost/ (дата обращения: 09.12.2022).
3. Gorodyansky, David. Internet privacy and security : A shared responsibility : [англ.] // wired.com. — 2013. — 10. — Дата обращения: 04.02.2023.
4. Алексей Лукацкий. Триада \"конфиденциальность, целостность, доступность\": откуда она? // SecurityLab.ru. — 2012. — 20 сентября.
5. Үмбетәлі Қ.Н.,Информационная безопасность Республики Казахстан. 2017. URL: https://articlekz.com/article/19962 (дата обращения: 09.02.2022).
6. ҚР ЦДИАӘМ, Ақпараттық қауіпсіздік // Киберқауіпсіздікті қамтамасыз ету мәселелері. Ұсынымдар.20 қаңтар 2023. URL: https://www.gov.kz/memleket/entities/mdai/activities/6?lang=kk (дата обращения: 07.02.2022).