ӘОЖ 347/9
DOI: 10.54649/2077-9860-2024-3-80-87

Н.Д. Тлешалиев [1]
[1] Ph.D, қауымдастырылған профессор,
Каспий қоғамдық университеті
Қазақстан Республикасы , Алматы қ.
E-mail: nurlan.tleshaliev@mail.ru

Б.С. Утаев[2]
[2]Каспий қоғамдық университеті
Қазақстан Республикасы, Алматы қаласы

ЭЛЕКТРОНДЫҚ ДӘЛЕЛДЕМЕЛЕРДІ ТІРКЕУ ЖӘНЕ АЛЫП ҚОЮ

Аңдатпа

Мақалада қазіргі заманғы қылмыстық, азаматтық және әкімшілік сот өндірісінің маңызды бөлігі болып табылатын электрондық дәлелдемелерді тіркеу және алу әдістері қарастырылады. Автор электрондық дәлелдемелерді пайдалануды реттейтін негізгі нормаларын, сондай-ақ оларды жинау, сақтау және сотта ұсыну тәсілдерін талдайды. Мұндай дәлелдемелермен жұмыс істеудің құқықтық аспектілері мен практикалық аспектілеріне, соның ішінде құқық қорғау органдары мен сот сарапшыларының жұмысына ерекше назар аударылады.

Түйінді сөздер: автоматтандыру, ақпараттандыру, қылмыстар, қылмыстық құқық бұзушылық, азаматтық талап, кінәні мойындау, электрондық мемлекеттік қызмет интеграторы, электронды дәлелдемелер, дәлелдемелерді тіркеу, дәлелдемелерді алу, цифрлық іздер, құқықтық аспектілер, сот сараптамасы, ақпараттық қауіпсіздік, цифрлық сот сараптамасы, электрондық пошта , блокчейн, сот тәжірибесі.

Н.Д.Тлешалиев[1]
[1] PhD, ассоциированный профессор,
Каспийский общественный университет,
Республика Казахстан, г. Алматы
E-mail: nurlan.tleshaliev@mail.ru

Б.С. Утаев[2]
[2]Каспийский общественный университет,
Республика Казахстан, г. Алматы

ФИКСАЦИЯ И ИЗЪЯТИЕ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ

Аннотация

В статье рассматриваются методы фиксации и изъятия электронных доказательств, которые являются важной частью современного уголовного, гражданского и административного процесса. Автор анализирует основные нормы, регулирующие использование электронных доказательств, а также подходы к их сбору, хранению и представлению в суде. Особое внимание уделено правовым аспектам и практическим аспектам работы с такими доказательствами, включая работу правоохранительных органов и судебных экспертов.

Ключевые слова: автоматизация, информатизация, преступления, уголовный проступок, гражданский иск, признание вины, сервисный интегратор "электронного правительства, элек-

тронные доказательства, фиксация доказательств, изъятие доказательств, цифровые следы, правовые аспекты, судебная экспертиза, информационная безопасность, цифровая криминалистика, электронная почта, блокчейн, судебная практика.

N.D. Tleshaliyev[1]
[1]Ph.D, Associate Professor,
Caspian Public University,
Republic of Kazakhstan, Almaty
E-mail: nurlan.tleshaliev@mail.ru

B.S. Utaev[2]
[2]Caspian Public University
Republic of Kazakhstan, Almaty

RECORDING AND SEIZURE OF ELECTRONIC EVIDENCE

Annotation

The article examines the methods of recording and seizing electronic evidence, which is an important part of modern criminal, civil and administrative proceedings. The author analyzes the main rules governing the use of electronic evidence, as well as approaches to its collection, storage and presentation in court. Particular attention is paid to the legal aspects and practical aspects of working with such evidence, including the work of law enforcement agencies and forensic experts.

Key words: automation, informatization, crimes, criminal offense, civil claim, admission of guilt, e-government service integrator, electronic evidence, recording of evidence, seizure of evidence, digital traces, legal aspects, forensic examination, information security, digital forensics, e-mail, blockchain, judicial practice.

Заңды түрде алынған, олардың негізінде анықтау органы, анықтаушы, тергеуші, прокурор, сот осы Кодексте айқындалған тәртіппен Қазақстан Республикасының Қылмыстық кодексінде көзделген іс-әрекеттің бар екенін немесе жоқ екенін, күдіктінің, айыпталушының немесе сотталушының бұл әрекетті жасағанын немесе жасамағанын, оның кінәлілігін не кінәсіздігін, сондай-ақ істі дұрыс шешу үшін маңызы бар өзге де мән-жайларды анықтайтын нақты деректер қылмыстық іс бойынша дәлелдемелер болып табылады.

Қылмыстық істі дұрыс шешу үшін маңызы бар нақты деректер: күдіктінің, айыпталушының, жәбірленушінің, куәнің, қорғалуға құқығы бар куәнің, сарапшының, маманның айғақтарымен; сарапшының, маманның қорытындысымен; заттай дәлелдемелермен; процестік әрекеттердің хаттамаларымен және өзге де құжаттармен белгіленеді [1], [2].

Тергеушінің дұрыс әрекет алгоритмін таңдауға және жүйеге минималды әсер ететін әдістерді қолдануға көмектесетін қажетті білімі мен тәжірибесі болуы керек. Барлық әрекеттеріңізді оларды жүзеге асыру уақытын көрсете отырып жүзеге асыру өте маңызды.

Нақты уақыт режимінде компьютерлік деректерді анықтау мен алудың әмбебап схемасын ұсыну қиын. Әр жағдай өзінше ерекше және тәжірибелі тергеуші белгілі бір жағдайда қалай жақсы әрекет ету керектігін білуі керек.

Ақпараттың қолжетімділігі ақпараттық жүйенің тиісті өкілеттіктері бар субъектілерге ақпаратқа дер кезінде бөгетсіз рұқсат беру қабілетімен анықталады. Ақпаратты жою немесе бұғаттау (қателіктің немесе қасақана іс-әрекеттің нәтижесінде) қолжетімділіктің жойылуына алып келеді.

Қолжетімділік – ақпараттық-коммуникациялық қызметтерді беру (теміржол және авиациялық билеттерді сатудың, банктік қызметтердің ақпараттық жүйелері, интернетте өнімдерді интернет-ресурстармен және электрондық БАҚ-пен тарату) жолымен клиенттерге қызмет көрсетуге бағытталған ақпараттық жүйелердің жұмыс істеуі үшін маңызды белгі. Уәкілетті пайдаланушы белгілі бір қызметтерге (көбінесе желілік) рұқсат ала алмайтын жағдайды қызмет көрсетуден бас тарту деп атайды[3].

Коммуникациялық (желілік) технологиялардың дамуына байланысты ақпараттық жүйені немесе басқарушы электрондық ақпараттық ресурсты алыстан

пайдаланушы адамның жеке басына байланысты ақпараттық қауіпсіздіктің қосымша тағы екі ерекшелігін бөліп көрсетеді: аутенттілік және дәлелдегіштік [3].

Аутенттілігі – ақпараттық-коммуникациялық қызметтер көрсету саласында ақпаратқа немесе хабарға қатысты заңдық тұрғыдан маңызды іс-әрекеттің авторын дұрыс анықтау мүмкіндігі, мысалы, электрондық коммерцияда электрондық-цифрлық қолтаңба немесе түпнұсқаландырудың өзге тәсілі пайдаланылған кезде.

Дәлелдегіштік (бас тартпаушылық) – авторлықтан бас тартқан кезде жасалған іс-әрекеттерді тіркеу жолымен ақпараттық жүйедегі немесе ресурстағы ақпаратқа қатысты іс-әрекет жасаған автор басқа ешкім емес, осы пайдаланушы болып табылатындығын дәлелдеу мүмкіндігі [3].

Киберқауіпсіздік – бұл қолданушыларды, олардың ақпараттық жүйелерін, желілері мен бағдарламаларын сандық шабуылдардан қорғауды қамтамасыз етуге бағытталған қызмет.

Мұндай кибершабуылдардың басты мақсаты әрі хакерлердің жеке мақсаттары үшін осы ақпаратты одан әрі пайдалану үшін пайдаланушының құпия ақпаратын алу, әрі бүкіл бизнес-процестің жұмысын бұзу болуы мүмкін. Сондықтан, әсіресе мемлекеттік департаменттер мен ірі жеке ұйымдардың жағдайында, Қазақстан үшін, сондай-ақ әлемнің басқа елдері үшін Интернетте тиімді және қауіпсіз болу үшін басты міндеттердің бірі дәл осы киберқауіпсіздік саласын дамыт уболып табылады [4].

Компьютерлік деректерді криминалистикалық талдау үшін сізде тиісті дайындық, практикалық тәжірибе, сондай-ақ бекітілген криминалистикалық құралдардың арнайы жиынтығы болуы керек. Егер тінту орнында жоғарыда аталған дағдылар мен құралдарға ие маман болмаса, дереу мамандандырылған бөлімге, біздің жағдайда ішкі істер министрлігі Криминалдық полиция департаментінің "киберқылмыстарға қарсы күрес" басқармасының аумақтық бөлімшелеріне, Экономикалық тергеу департаментінің мамандарына, Қазақстан Республикасы Әділет министрлігінің Сот сараптамалары институтының сарапшыларына жүгіну керек.

В.А. Номоконов пікірінше, электрондық дәлелдемелерді анықтауға және жинауға бағытталған алғашқы тергеу әрекеттерін жүргізу барысында деректерге немесе құрылғыларға — жабдықтың өзіне де, бағдарламалық қамтамасыз етуге де өзгерістер енгізуге болмайды. Қылмыс орнының сақталуына және дәлелдемелер жинауға жауапты адамдар іріктелген материалдың тұтастығын және оның берілу тарихының сақталуын қамтамасыз етуге міндетті. Жұмыс істейтін құрылғының деректеріне білікті маман қол жеткізуі керек және бұл деректердің өзіне минималды әсер ететіндей болуы керек[5, 46 б.].

Тергеу әрекетінің тиісті хаттамасын жасау барысында қажет болған жағдайда үшінші тарап бұл әрекеттерді қайталай алуы үшін адамдардың барлық іс-әрекеттерін дәл сипаттау қажет. Іздеу және алу процесінің, сақтау шарттарының және электрондық деректерді жылжыту тәртібінің толық сипаттамасын қамтамасыз ету және тексеру жағдайында осы ақпаратты сақтау қажет.

Интернет-бұл бүкіл әлем бойынша миллиондаған компьютерлерді құрылғылар мен хаттамалар арқылы байланыстыратын ғаламдық желі және оның жұмысының ережелері мен стандарттарын белгілейтін бірнеше ұйымдар бар. Сонымен қатар, ғаламдық желінің әрбір жеке түйіні құрылымы мен мазмұны басқа ұйымдарға тәуелді емес тәуелсіз ішкі желі ретінде жұмыс істей алады. Интернетке қол жетімділіктің көптеген технологиялары бар, Бұл онлайн қызметтердің ауқымын едәуір кеңейтеді[6].

Интернеттегі дәлелдермен жұмыс істеу кезінде сіз виртуалды және физикалық әлемді нақты ажыратып, бір тілден екінші тілге аудара білуіңіз керек. Виртуалды әлем тілінде "орналасу" әдетте URI/URL деп аталады (бірыңғай ресурс идентификаторы (Uniform Resource Identifier, socr. URI) немесе бірыңғай ресурс көрсеткіші (Uniform Resource Locator, сокр. URL)-бұл желідегі орынның атауы немесе мекен-жайы ретінде жұмыс істейтін таңбалар тізбегі Интернет) немесе IP мекенжайы [6].

Интернет протоколы-бұл Интернет желісі арқылы деректерді жіберу немесе алу үшін қолданылатын стандарттар мен ережелердің белгіленген жиынтығы. IP мекенжайы-интернеттегі ақпарат көзінің ең негізгі түрі. Бұл деректер пакеттерінің қайда жеткізілетінін көрсетеді.

Интернет-провайдерлерге IP мекенжайын беру процесі өте қарапайым. IANA аймақты құйымға өз аймағындағы өтініш берушілер

үшін қандай IP мекенжайлары бар екенін хабарлайды. Содан кейін интернет-провайдер (Internet service Providers, қысқ. ISP) IP мекенжайларын алу үшін аймақтық ұйымға жүгінеді. Интернет-провайдер IP мекенжайларының белгілі бір ауқымын алғаннан кейін, оларды өз клиенттеріне (соңғы пайдаланушыларға) таратадыжәне жауапты желіні құрады [6].

Екі бірдей жалпыға ортақ IP мекенжайлары бір уақытта интернетке қосылмайды. Хаттарды (деректерді) жіберу және алу үшін қала көшесіндегі үйге ұқсас әр компьютердің өзіндік ерекше мекен-жайы болуы керек. Үй компьютерін Интернетке қосқан кезде, интернет-провайдер бұл компьютерге уақытша пайдалануға бірегей IP мекенжайын ұсынады. Бұл дегеніміз, осы компьютерден белгілі бір уақыт ішінде жүзеге асырылатын Интернеттегі барлық әрекеттер осы IP-мекен-жаймен байланысты болады. Интернеттен ажыратылғаннан кейін IP мекенжайы басқа компьютерлердің пайдасына қайта бөлінеді [7].

Әрбір интернет-провайдердің белгілі бір IP-мекен-жайы бар. Кейде интернет-провайдердің клиенттерінің саны олардың IP-мекенжайларының санынан асып түседі. Қолжетімді мекен-жайлардың жетіспеушілігінен клиенттерді жоғалтпау үшін арнайы технологиялар мен хаттамалар жасалды. Ең көптаралған хаттама-бұл түйінді динамикалық конфигурациялау протоколы (Dynamic Host Configuration Protocol, қысқ. DHCP) [7].

DHCP-бұл IP мекенжайларының ауқымын құрылғылар тобына автоматты түрде тарату үшін қолданылатын протокол (яғни, бір-бірімен байланыс орнатуға арналған құрылғыларға арналған ережелер жиынтығы). Бұл хаттаманың жұмыс принципі өте қарапайым. Құрылғы интернетке қосылғысы келгенде, ол интернет провайдерінен бос IP мекенжайын сұрайды; интернет провайдері қолжетімді IP мекенжайларының тізімін тексереді (яғни, қазіргі уақытта басқа құрылғыларға қандай IP мекенжайлары берілмегенін көреді) және Сұраусалушы клиентке (құрылғыға) бос IP мекенжайларының бірін бөледі – мекен-жайлары. Бұл реттe интернет-қызметтерді жеткізуші пайдаланушының күнін, уақытын және идентификаторларын тіркейді. Клиент интернеттен ажыратылғаннан кейін, пайдаланылған IP мекенжайы басқақұрылғылар арасында тарату үшін қолжетімді IP мекен жайларының тізіміне қайтарылады. Бұл Интернетке қосылған сайын пайдаланушы немесе құрылғы әртүрлі IP мекенжайларын ала алатынын білдіреді. Кейде IP мекенжайы бір сессия барысында бірнеше рет өзгереді [7].

Нақты әлемде, егер сізде поштамекен-жайы үнемі өзгеріп отырса, онда сізге хат жазу өте қиын болар еді, өйткені пошта оларды қайда жеткізетінін білмейді. Интернетте үнемі бірдей IP мекенжайы болуы керек құрылғылардың белгілі бір түрлері бар. Бұл жағдайларда статикалық IP-мекен-жайлар қолданылады, яғни интернет – провайдер құрылғыға (клиентке) белгілі бір IP-мекен-жайды оның клиенті болып қалғанға дейін тағайындайды [8].

Интернет-провайдерлердің көпшілігінде статикалық және динамикалық IP мекенжайлары бар. Бірінші және екінші жағдайда, интернет-провайдерлер белгілі бір уақытта белгілі бір IP – мекен-жайды кім қолданғанын біледі. Назар аударыңыз, Интернетке қолжеткізу қызметтерін ұсыну шарттары әдетте жеке немесе заңды тұлғалармен жасалғанымен, IP мекенжайлары Жеке тұлғаларға емес, құрылғыларға беріледі [8].

Егер интернет-тергеу кезінде белгілі бір IP-мекенжай пайда болса, онда интернет-қызметтерді жеткізушіден Интернетке қолжетімділікті қамтамасыз ету туралы келісімшарттың егжей-тегжейін және белгілі бір уақытта осы IP-мекен-жай берілген құрылғы туралы ақпаратты білуге болады. Әдетте, мұндай ақпаратқа тергеу соты санкциялаған алу туралы қаулы негізінде қол жеткізуге болады (жекелеген жағдайларда қылмыстық қудалау органының талабы бойынша). Тиісті IP мекенжайы зерттелетін әрекеттер контекстінде пайдаланылған сәтті мүмкіндігінше дәл анықтау керек екенін ескеріңіз [8].

"UTC — 10" уақыт белдеуін көрсетеді, бұл жағдайда "Дүниежүзілік үйлестірілген уақыт 10 сағат" (Гавайи). Интернет-провайдерге IP – мекен-жайларды пайдалану туралы ақпарат беру туралы сұраныстар жібере отырып, уақыт белдеуін көрсетуқажет [8].

Осы диссертациялық зерттеушеңберінде электрондық дәлелдемелерді егжей-тегжейлі анықтау және оны кейіннен зерделеу тәртібіне тоқталудың қажеті жоқ деп санаймыз.

Осы зерттеуде қылмыстық қудалау органы электрондықдәлелдемелерді табу және алукезінде кездесетін мәселелерге баса назар аударылады [8].

Е.Р. Россинская ойынша, жалпы қылмыстық құқықбұзушылықтарды тергеу кезінде

қылмыстық істің тағдыры көбіне байланысты болатын негізгі тергеу әрекеттері тексеру, алу және тінту болып табылады. Аталған тергеу әрекеттерінде олардың негізінде кейіннен айыптаукұрылатыннемесеқылмыстыққудалауды тоқтату туралы шешімдер қабылданатын заттар бейнеленеді және сипатталады. Заттай дәлелдемелерді алу барысында іс-әрекеттер сипатталатын және белгілі бір дәлелдемелерді табу орны белгіленетін тұрақты алгоритм пайдаланылады [9, 87 б.].

Электрондық ақпарат құралдарынан дәлелдемелер алу оларды алуды және алуды бірнешеретқиындатады.Алынғанэлектрондық дәлелдемелердің тұтастығы сотта дауланатынын ескере отырып, қылмыстық қудалау органы электрондық дәлелдемелердің бастапқы деректерін жазып алуы қажет. Көрсетілген тіркеу электрондық дәлелдемелерді зерттеуді жүргізген мамандарға немесе сарапшыларға қандай да бір электрондық дәлелдемелердің қайдан және қалай алынғанын түсіндіру үшін қажет. Сотталушылар мен олардың қорғауы электрондық дәлелдемелерді алудың заңсыздығы туралы әртүрлі нұсқаларды ұсынады,табылғанэлектрондықдәлелдемелер мен олардыңшығу тегіне күмән келтіреді.

Заттай дәлелдемелерді табу және алып қою барысында қылмыстық қудалау органы заттар мен құжаттарды толық сипаттайды, айрықша белгілерге назар аударады, әрбір бөлшекті сипаттайды, буып-түйеді, тігеді және түсіндірме түсініктемелерді биркаларда қалдырады. Алайда, электрондық ақпарат тасығыштарды табу және алып қою барысында дәстүрлі заттай дәлелдемелерге қолданылатын бекіту әдістері жеткіліксіз. Электрондық медианың жады биттерден петабайтқа дейінгі ақпарат көлеміне байланысты әртүрлі болады. Тиісінше, электронды тасымалдағышта табылған құжаттардың әрқайсысының қасиеттерін сипаттау мүмкін емес. Алайда, сотты электронды дәлелдемелерді алудың заңдылығына сендіру үшін электронды ақпарат тасығыштың оны алып қойғаннан бастап электронды дәлелдемелер табылғанға дейін сыртқы және ішкі өзгерістерге ұшырамағанын дәлелдеу қажет.

Электрондық ақпарат тасығыштарды табу және алу орнын сипаттау кезінде мынадай ақпаратты жазу қажет (дәлелдемелерді жинау сатысында қосымша деректер пайда болуы мүмкін):

Объектілердің физикалық орналасуы: жүйенің эскизін жасау, яғни оның құрамдас бөліктерінің орналасуы (тышқандар, перне тақталар және т.б.); бөлменің фото және бейне түсірілімін жасау (мүмкіндігінше дөңгелек); жүйелер мен электрондық компоненттердің / құрылғылардың/жабдықтардың орналасқан жерін белгілеу және олардың өзара байланысын сипаттау [10].

Тергеуге қатысты барлық анықталған құрылғылар туралы толық ақпарат, олардың маркасын, моделін және сериялықнөмірін көрсету; компьютердің қандай күйде екендігі туралы ақпаратты (қосулы, өшірулі, ұйқы режимінде) қоса алғанда, электрондық дәлелдемелерді қамтитын немесе білдіретін барлық компьютерлік жүйелердің жай-күйі мен орналасуы туралы деректер; компьютерлік жүйелер мен өзге де құрылғылардың кабельдік және сымсыз қосылуы туралы ақпарат; Барлық порттар мен кабельдерді, сондай-ақ перифериялық құрылғылармен байланыстарды белгілеңіз: болашақта бұл жүйенің нақты конфигурациясын қалпына келтіруге көмектеседі. Пайдаланылмаған порттарды белгілеу; деректер тасымалдаушыларын анықтау үшін ноутбуктің түйісу түйіндерін табу; монитордың сипаттамаларын көрсету; компьютердің алдыңғы бөлігін, мониторды және басқа компоненттерді суретке түсіру; монитор экранының суретін сипаттау; қосылған бағдарламаларды бейнеге түсіру немесе экранда суреттің толық сипаттамасын жасау; тергеуге қатысы бар, бірақ зерттеуге жатпайтын электрондық құрылғылар мен компоненттерді сипаттау ойық; тінту, алу, қарап-тексеру жүргізілетін жердегі адамдар туралы ақпарат; тінту жүргізілетін жердегі адамдар мен сұхбаттасуға және олардың жауаптарын тиісті нысандарға енгізуге міндетті [11].

Электрондық ақпарат тасығыштарта былғанжәнеалынған жердегі барлық тұлғалардың дербес деректері; компьютерлік жүйелер мен жабдықтарды пайдаланған барлық тұлғалардың дербес деректері; компьютерлік құрылғылардың куәгерлері мен пайдаланушылары/иелері ұсынған ақпарат пен түсініктемелер; тінту жүргізілетін жерде жүзеге асырылған барлық іс-қимылдардың сипаттамасы; барлық іс-әрекеттер мен уақыттарды сипаттай отырып, тиісті тергеуіс-қимылының хаттамасын жасау оларды жүзеге асыру.

Қаптама:электрондықдәлелдемелердіорау алдындасипаттаңызжәнетаңбалаңыз;алынған дәлелдемелерді түп нұсқалық қаптамада тасымалдау; егер түп нұсқа қаптама сақталмаса,

антистатикалық материалдарды (яғни қағаз немесе антистатикалық полиэтилен пакеттерін) қолданыңыз. Статикалық электр энергиясын жасай алатын материалдарды пайдаланбаңыз (яғни қарапайым полиэтилен пакеттер); сақтау құралдарын (скиам дискілерді) бүктемеңіз, майыстырмаңыз немесе сызатпаңыз; сақтау құралдарының бетіне ештеңе жапсырмаңыз. Мүмкіндігінше оларды конверттерге немесе қораптарға салыңыз; Дәлелдері бар барлық қораптар мен конверттерге қол қойыңыз; Егер бірнеше компьютерлік жүйелер тәркіленсе, бастапқы конфигурацияны одан әрі қалпына келтіру үшін тиісті белгілер жасаңыз.

Смартфондар, ұялы телефондар сол режимде қалуы керек (қосулы/ өшіру), онда олар табылды:

Смартфондар мен ұялы телефондарды орау үшін Фарадей оқшаулағыш пакеттерін (олар сигналдарды блоктайды), радио оқшаулағыш материалдарды немесе алюминий фольганы пайдалану керек: бұл хабарламалардың жіберілуіне және қабылдануына жол бермейді. Егер құрылғы дұрыс оралмаған болса немесе қорғаныс орамынан шығарылса, онда ол хабарламалар жібере және қабылдай алады. Назар аудару керек: оқшаулағыш қаптамада құрылғы тезірек таусылу мүмкін. Егер батарея заряды таусылса, құрылғыны "ұшақ режиміне" ауыстыруға болады.

Тасымалдау: электрондық дәлелдерді магниттік сәулелену көздерінен алыс ұстаңыз. Радио таратқыштар, микрофондар және қыздырылған орындықтар электрондық деректерді зақымдауы мүмкін; тәркіленген жабдықты физикалық факторлардың әсерінен (соққылардан, ылғалдылықтан және жоғары температурадан) қорғау; тасымалдау кезінде қораптарға салынбаған. Компьютерлер мен құрылғылар зақымданудан және шамадан тыс дірілден қорғау үшін жақсы бекітілуі керек. Атап айтқанда, компьютерлер еденге, ал мониторлар көліктің отырғышына экран төмен қаратып орналастырылады. Мониторлар қауіпсіздік белдіктерімен бекітіледі; үлкен, ауыр заттарды кішкентайларға салмаңыз; мүмкіндігінше жабдықтар мен құрылғыларды машинада қажет болғаннан ұзағырақ ұстамаңыз.

Сақтау: жиналған дәлелдемелердің тізімдемесін Қазақстан Республикасының 2014 жылғы 4 шілдедегі №231-V ҚРЗ қылмыстық іс жүргізу кодексіне [1] және "заттай дәлелдемелерді, алынған құжаттарды, ақшаны ұлттық және шетел валютасында алу, есепке алу, сақтау, беру және жою қағидаларын бекіту туралы" Қазақстан Республикасы Үкіметінің №1291 қаулысына сәйкес жүргізу сот, прокуратура, қылмыстық құдалау және сот сараптамасы органдары" 2014 жылғы 9 желтоқсандағы [26]; "Заттай дәлелдемелерді, алынған құжаттарды, ұлттық және шетел валютасындағы ақшаны, есірткі құралдарын, қылмыстық істер бойынша психотроптық заттарды алып қою, есепке алу, сақтау, беру және жою қағидаларын бекіту туралы" Қазақстан Республикасы Үкіметінің №1291 қаулысында көрсетілген қағидаларға сәйкес дәлелдемелерді ылғал көздерінен және жоғары температурадан алыс сенімді жерде сақтау, прокуратура, қылмыстыққұдалаужәне сот сараптамасы органдарымен " 2014 жылғы 9 желтоқсандағы; Дәлелдерді магниттік сәулеленуден, ылғалдан, шаңнан және басқа да зиянды бөлшектер мен заттардан қорғауды қамтамасыз ету; дәлелдемелерді сақтау үшін: қол жетімділікті бақылау; өрт қауіпсіздігі (дабыл беру, өрт сөндіргіштер, сақтау аймағында және іргелес аймақтарда темекі шегуге тыйым салу); температура мен ылғалдылықты бақылау; магнит өрістерінен қорғау деңгейі жеткілікті қауіпсіз үй-жайларды пайдалану (радио құрылғылардың бағытталған әсерінен оқшаулау).

Электрондық дәлелдемелері бар бір бөлмеде жанғыш заттар мен заттарды (мысалы, жуғыш заттар немесе қағаз) сақтамаңыз; дәлелдерді статикалық электр энергиясын тудыратын еден жабыны бар бөлмелерде сақтамаңыз; электронды дәлелдемелерді су құбырлары өтетін бөлмелерде, әсіресе құбырлар төбенің бойымен жүрсе, сақтамаңыз; назар аударыңыз: уақыт өте келе мұндай жүйенің күні, уақыты және конфигурациясы сияқты ықтимал дәлелдер жоғалуы мүмкін. Сонымен қатар, батарея заряды таусылған жағдайда ақпарат жоғалып кетуі мүмкін. Әріптестеріңізге ең алдымен батареямен жұмыс істейтін құрылғыларға (ДК/CMOS) назар аудару керектігін үйретіңіз. (CMOS батареясы немесе комплементарлы металл-оксидті жартылай өткізгіш технологиясына негізделген батарея (Mmplementary metal-oxide-semiconductor, socr. CMOS) BIOS (basicinputoutputsystem – негізгі енгізу-шығару жүйесі) іске қосу үшін пайдаланылады, ол өз кезегінде компьютерлік жүйені іске қосады).

Электрондық ақпарат тасығыштарды пайдалана отырып, қылмыстық істерді тергеу тәжірибесінен тәжірибеде бір бағытты

хэш-функцияларды пайдалану тасығыштағы деректердің тұтастығы мен өзгермейтіндігін куәландыру үшін ұсынылады.

Хэш математикалық мәннің қандай да бір түріне әкелетін деректерге қолданылатын алгоритмді қолданады. Хэш екі нақты деректер жиынтығына қолданылған кезде, күтілетін нәтиже бірдей хэш функциясының мәні болады. Егер бір деректер жиынтығы басқа деректер жиынтығынан сәл өзгеше немесе өзгеше болса, күтілетін нәтиже хэш функциясының басқа мәні болады

Хэш функциясы алгоритмді қолдана отырып және кілтсіз шифрлауды қамтамасыз етеді. Олар "біржақты хэш функциялары" деп аталады, өйткені шифрлауды болдырмау мүмкін емес. Айнымалы ұзындықтағы ашық мәтін (әдетте) тұрақты ұзындықтағы хэш мәніне "хэштеледі" (көбінесе "хабарлама дайджесті" немесе жай "хэш"деп аталады). Хэш функциялары негізінен тұтастықты қамтамасыз ету үшін қолданылады: егер ашық мәтіннің хэш коды өзгертілсе, ашық мәтіннің өзі де өзгереді. Жалпы ескі хэш функцияларына қауіпсіз хэштеу алгоритмдері кіреді [9].

Мысалы, маман оқиға орнында дискінің суретін түсірген кезде хэш функциясы есептеледі, оның мәні хаттамаға енгізіледі. Сарапшы зерттеуге көшірмесін алғаннан кейін одан хэш функциясын есептейді. Егер оның мәні хаттамаға енгізілген мәнге сәйкес келсе, сарапшы және басқа адамдар зерттелетін көшірменің түпнұсқаға бит дәлдігі мен сәйкес келетініне сенімді болады. Сол сияқты, хэш функциясы жеке файлдардың тұтастығын бақылау үшін қолданылады. Мысалы, үйлерді алу кезінде. Журнал файлынан хэш функциясы есептеледі, олхаттамағаенгізіледі. Хаттамадағы хэш функциясының мәні файлды көшіру және сақтау кезінде өзгермейтіндігін қамтамасыз етеді. Хэш функциясының мәндерінің сәйкестігі файлдардың толық сәйкестігіне кепілдік береді [5].

Төменде көрсетілген бөлімде электрондық дәлелдемелердің ерекшелігін ескере отырып, электрондық ақпарат тасығыштарды табу және алу ерекшеліктері сипатталады, жоғарыда сипатталған барлық ұсыныстарды нақты ұстану қажет. Электрондық дәлелдер нәзік, температураға, ылғалға, механикалық зақымға, статикалық электр қуатына, магниттік сәулеленуге және тіпті операциялық командаларға сезімтал болғандықтан, оларды орау, тасымалдау және сақтау кезінде тиісті сақтық шараларын сақтау қажет. Электрондық дәлелдемелерді алу мен сақтаудың ерекшелігінен басқа, қылмыстық құдалау органы мен сот электрондық дәлелдемелердің бастапқы деректерін дәлелдеуі қажет. Алынған сәттен бастап электрондық ақпарат тасымалдаушыларының деректерінің тұтастығы мен өзгермейтіндігін растау үшін Америка Құрама Штаттарының мысалында дайджесттер құрылған сәттен бастап хабарламалардың өзгертілгенін анықтау үшін пайдаланылуы мүмкін "қауіпсіз хэштеу стандартын" анықтау ұсынылады.

Пайдаланылған кайнар көздерінің тізімі:

1. Қазақстан Республикасының Қылмыстық-процестік кодексі Қазақстан Республикасының Кодексі 2014 жылғы 4 шілдедегі № 231-V ҚРЗ.
2. Қазақстан Республикасының Қылмыстық кодексіҚазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ.
3. Киберқауіпсіздік тұжырымдамасын ("Қазақстанның киберқалқаны") бекіту туралыҚазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы.
4. Ақпараттандыру саласындағы ақпараттық қауіпсіздікhttps://egov.kz/cms/kk/cyberspace
5. Номоконов В.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. - 2012. - № 1 (24). – С. 45-55.
6. Байланыс саласындағы "Қолжетімді Интернет" ұлттық жобасын бекіту туралыҚазақстан Республикасы Үкіметінің 2023 жылғы 27 қазандағы № 949 қаулысы
7. Ақпараттандыру туралы Қазақстан Республикасының Заңы 2015 жылғы 24 қарашадағы № 418-V ҚРЗ.
8. Доклад Управления Организации Объединённых Наций по Наркотикам и Преступности “Всестороннее исследование проблемы киберпреступности” февраль 2013 г.
9. Россинская Е.Р. Современные способы компьютерных преступлений и закономерности их реализации // LexRussica. 2019. № 3. С. 87-99.

10. О ратификации Соглашения между Правительством Республики Казахстан и Центральноазиатским региональным информационным координационным центром по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров об условиях его пребывания в городе Алматы Закон Республики Казахстан от 25 ноября 2011 года № 498-IV. www.adilet.kz
11. Постановление Правительства РК от 12 декабря 2017 года №827 «Об утверждении Государственной программы «Цифровой Казахстан». (с изменениями и дополнениями по состоянию на 01.10.2020 г.). www.adilet.kz

References:

1. Қazaқstan Respublikasy`ny`ң Qy`lmy`sty`қ-procestik kodeksi Қazaқstan Respublikasy`ny`ң Kodeksi 2014 zhy`lғy` 4 shildedegi № 231-V ҚRZ.
2. Қazaқstan Respublikasy`ny`ң Qy`lmy`sty`қ kodeksiҚazaқstan Respublikasy`ny`ң Kodeksi 2014 zhy`lғy` 3 shildedegi № 226-V ҚRZ.
3. Kiberқauipsizdik tұzhy`ry`mdamasy`n ("Қazaқstanny`ң kiberқalқany`") bekitu turaly`Қazaқstan Respublikasy` Ykimetinің 2017 zhy`lғy` 30 mausy`mdaғy` № 407 қauly`sy`.
4. Aқparattandy`ru salasy`ndaғy` aқparatty`қ қauipsizdikhttps://egov.kz/cms/kk/cyberspace
5. Nomokonov V.A. Kiberprestupnost` kak novaya kriminal`naya ugroza // Kriminologiya: vchera, segodnya, zavtra. - 2012. - № 1 (24). – S. 45-55.
6. Bajlany`ssalasy`ndaғy` "Қolzhetimdi Internet" ұltty`қzhobasy`nbekituturaly`ҚazaқstanRespubli kasy`Ykimetinің 2023 zhy`lғy` 27 қazandaғy` № 949 қauly`sy`
7. Aқparattandy`ruturaly`ҚazaқstanRespublikasy`ny`ңZaңy` 2015 zhy`lғy` 24 қarashadaғy` № 418-V ҚRZ.
8. Doklad Upravleniya Organizacii Ob``edinyonny`x Nacij po Narkotikam i Prestupnosti “Vsestoronnee issledovanie problemy` kiberprestupnosti” fevral` 2013 g.
9. Rossinskaya E.R. Sovremenny`e sposoby` komp`yuterny`x prestuplenij i zakonomernosti ix realizacii // LexRussica. 2019. № 3. S. 87-99.
10. O ratifikacii Soglasheniya mezhdu Pravitel`stvom Respubliki Kazaxstan i Central`noaziatskim regional`ny`m informacionny`m koordinacionny`m centrom po bor`be s nezakonny`m oborotom narkoticheskix sredstv, psixotropny`x veshhestv i ix prekursorov ob usloviyax ego preby`vaniya v gorode Almaty` Zakon Respubliki Kazaxstan ot 25 noyabrya 2011 goda № 498-IV. www.adilet.kz
11. Postanovlenie Pravitel`stva RK ot 12 dekabrya 2017 goda №827 «Ob utverzhdenii Gosudarstvennoj programmy` «Cifrovoj Kazaxstan». (s izmeneniyami i dopolneniyami po sostoyaniyu na 01.10.2020 g.). www.adilet.kz