ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ІШКІ ІСТЕР МИНИСТРЛІГІ

Бәрімбек Бейсенов атындағы Қарағанды академиясы

Е.П. ШУЛЬГИН, Ж.Н. САПАРҒАЛИЕВ,
Е.О. ДОСЫМБЕТОВ, П.А. ТАФИНЦЕВ

КОМПЬЮТЕРЛІК АҚПАРАТ САЛАСЫНДАҒЫ АЛАЯҚТЫҚТЫ ТЕРГЕУДІҢ ЕРЕКШЕЛІКТЕРІ

ОҚУ ҚҰРАЛЫ

ҚАРАҒАНДЫ-2023

Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының оқу-әдістемелік кеңесінің 2023 жылғы 20 шілдедегі № 11 хаттамасымен бекітілген шешімі бойынша жарияланады.

Рецензенттер: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының бастығы полиция полковнигі ***Б.Т. Байсеитов*;** Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының қылмыстық процесс кафедрасының бастығы, заң ғылымдарының кандидаты, полиция полковнигі ***Т.Н. Сулейменов.***

Құрастырушылар: киберқауіпсіздік және ақпараттық технологиялар кафедрасының бастығы з.ғ.к., полиция майоры *Е.П. Шульгин*; киберқауіпсіздік және ақпараттық технологиялар кафедрасының аға оқытушысы з.ғ.м., полиция подполковнигі *Ж.Н. Сапарғалиев*; киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы полиция майоры *Е.О. Досымбетов*; киберқауіпсіздік және ақпараттық технологиялар кафедрасының аға оқытушысы з.ғ.м., полиция майоры *П.А. Тафинцев.*

Шульгин Е.П., Сапарғалиев Ж.Н., Досымбетов Е.О., Тафинцев П.А. Компьютерлік ақпарат саласындағы алаяқтықты тергеудің ерекшеліктері: оқу құралы. – Қарағанды: Қазақстан Республикасы ІІМ Бәрімбек Бейсенов атындағы Қарағанды академиясы, 2023. – 53 б.

Бұл оқу құралы курсанттарға, ақпараттық қауіпсіздік және құқық қорғау саласындағы мамандарға, сондай-ақ компьютерлік ақпарат саласындағы алаяқтық мәселелеріне қызығушылық танытқандарға арналған. Онда мұндай қылмыстарды тергеудің ерекшеліктері, сондай-ақ тергеу кезінде қолданылатын әдістер мен құралдар қарастырылған.

Оқу құралы құқық қолдану қызметін жүзеге асыратын органдардың қызметкерлері, сондай-ақ Қазақстан Республикасы ІІМ жоғары оқу орындарының оқытушылары, докторанттары, магистранттары мен курсанттары үшін қызығушылық тудырады.

МАЗМҰНЫ

КІРІСПЕ

Қазіргі уақытта компьютерлік ақпарат көптеген ұйымдар мен жеке тұлғалар үшін негізгі активке айналды. Алайда, деректердің құндылығының өсуімен бірге көптеген зиянкестер компьютерлік ақпарат саласындағы алаяқтықпен белсенді айналыса бастады. Мұндай қылмыстарды тергеу-бұл ерекше дағдылар мен білімді қажет ететін күрделі және көп қырлы міндет. Бұл оқу құралында компьютерлік ақпарат саласындағы алаяқтықты тергеудің негізгі ерекшеліктерін қарастырамыз.

Компьютерлік қылмыстарды сәтті тергеу үшін киберқауіпсіздік, компьютерлік желі және цифрлық криминалистика бойынша білімі бар мамандандырылған топтар мен сарапшылар болуы керек. Бұл мамандар компьютерлік іздерге талдау жасай алады, осалдықтарды анықтай алады және шабуылдың көзін анықтай алады.

Компьютерлік алаяқтықты тергеудегі негізгі міндеттердің бірі-электронды дәлелдемелерді жинау және сақтау. Бұған компьютерлерді, серверлерді, мобильді құрылғыларды алып тастау, сондай-ақ оларда сақталған деректерді талдау кіреді. Дәлелдемелердің сот процесіне тұтастығы мен жарамдылығын қамтамасыз ету үшін просуалдық нормаларды сақтау маңызды.

Тергеуде зиянкестердің мотивациясын түсіну және оларды анықтау маңызды рөл атқарады. Бұл қаржылық мотивтерді, бәсекелестікті немесе тіпті мемлекеттік кибер тыңшылықты талдауды қамтуы мүмкін. Зиянкестерді анықтау қиын болуы мүмкін, бірақ кінәлілерді жазалау үшін өте маңызды.

Компьютерлік ақпарат әлемінде шабуылдар әр түрлі елдерден келуі мүмкін, ал шабуылдаушылар Интернеттің анонимділігінің артында жасырынуы мүмкін. Сондықтан халықаралық ынтымақтастық және басқа елдермен және ұйымдармен ақпарат алмасу сәтті тергеудің маңызды аспектілері болып табылады.

Компьютерлік ақпарат саласындағы алаяқтықты тергеу болашақта осындай шабуылдардың алдын алу және қорғау шараларын әзірлеуді де қамтиды. Бұл күшейтуді қамтиды киберқауіпсіздік жүйелері, қызметкерлерді оқыту, және киберқауіпсіздік заңнамасын жақсарту.

Мұндай қылмыстарды тергеу мамандандырылған білім мен дағдыларды, сондай-ақ халықаралық ынтымақтастықты қажет етеді. Зиянкестерді анықтау және жазалау ғана емес, сонымен қатар компьютерлік ақпарат саласындағы болашақ шабуылдардан қорғау үшін шаралар қабылдау маңызды.

Киберқылмысқа қарсы іс-қимыл кезінде жоғары Ақпараттық технологиялар саласындағы сотқа дейінгі тергеу компьютерлік жүйелер мен желілерді пайдалану арқылы жасалатын қылмыстарға қарсы күрестің маңызды кезеңдерінің бірі болып табылады. Цифрлық технологиялар өмірдің барлық салаларына енетін қазіргі ақпараттық қоғамда киберқауіптер мен олармен байланысты қылмыстарға тиімді жауап беру қажеттілігі туындайды.

Осы саладағы сотқа дейінгі тергеудің Жалпы сипаттамасы бірқатар ерекшеліктерді қамтиды. Біріншіден, қылмыстың күрделі техникалық аспектілерін тиімді түсіну үшін тергеушілер мен құқық қорғау органдарының

қызметкерлерінің арнайы білімі мен дағдыларының қажеттілігі. Киберқылмыскерлер көбінесе өз әрекеттерін жасыру үшін күрделі алгоритмдер мен әдістерді қолданады, сондықтан тергеушілер үлкен көлемдегі деректерді талдауға және сандық іздерді табуға дайын болуы керек.

Екіншіден, жоғары Ақпараттық технологиялар саласындағы сотқа дейінгі тергеу әртүрлі құқық қорғау органдары мен ақпараттық қауіпсіздік саласындағы мамандар арасындағы ынтымақтастықты талап етеді. Киберқылмыстар көбінесе трансшекаралық сипатқа ие, сондықтан ақпарат алмасу және басқа елдердің әріптестерімен үйлестіру қажет.

Үшіншіден, осы саладағы сотқа дейінгі тергеудің маңызды бөлігі цифрлық дәлелдемелерді жинау және талдау болып табылады. Бұл компьютерлерден, мобильді құрылғылардан, серверлерден алынған мәліметтер, сондай-ақ интернеттен алынған ақпарат болуы мүмкін. Мұндай деректер көбінесе қылмыстарды ашудың және кінәлілерді анықтаудың кілті болып табылады.

Қорытындылай келе, киберқылмысқа қарсы іс-қимыл кезінде жоғары Ақпараттық технологиялар саласындағы сотқа дейінгі тергеу күрделі және жауапты процесс болып табылады. Ол арнайы білім мен дағдыларды, әртүрлі құқық қорғау органдары арасындағы ынтымақтастықты және дәлелдерді жинау және талдау үшін цифрлық технологияларды белсенді пайдалануды талап етеді. Тек осы жағдайда ғана киберқылмыспен күресте табысқа жетуге және ақпараттық кеңістіктің қауіпсіздігін қамтамасыз етуге болады.

Оқу құралында компьютерлік ақпарат саласындағы алаяқтықты тергеудің бастапқы кезеңі, оның барлық элементтерін егжей-тегжейлі талдай отырып, қылмыстың криминалистикалық сипаттамасы қарастырылады. Тергеудің бастапқы кезеңінде туындайтын типтік тергеу жағдайларына және олардың негізінде ұсынылған тергеу нұсқаларына, сондай-ақ жекелеген тергеу әрекеттерінің ерекшеліктеріне талдау жүргізілді (оқиға болған жерді тексеру, жауап алу және бетпе-бет ставка, алу және тінту жүргізу, қажетті сараптамаларды тағайындау). Ситуациялық сипаттаманы және жекелеген тергеу әрекеттерін жүргізуді ескере отырып, тергеудің келесі кезеңінің ерекшеліктері ашылды.

§1. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу ерекшеліктері

Ақпараттық технологиялар кеңінен қолданылатын танымал ақпараттық қоғамда ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар барған сайын өзекті болып, проблемалар туындауда. Мұндай қылмыстарды тергеу осы саланың ерекшеліктерін ескере отырып, ерекше назар аударуды қажет етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу ерекшеліктері, ең алдымен, ақпараттық технологиялардың даму жылдамдығына және электрондық байланыс құралдарының таралуына байланысты. Осыған байланысты жаңа оқиғалар анықталды, компьютерлер, интернет және басқа да цифрлық байланыс құралдары пайдаланылуда.

Осы саладағы қылмыстық құқық бұзушылықтарды тергеу ерекшеліктерінің бірі анықтау мен жолын кесу қиындығы болып табылады. Киберқылмыскерлер көбінесе шетелден операция жасайды және анонимді байланыс құралдарын пайдаланады, бұл оларға қол жеткізуді талап етеді және тергеуді қиындатады. Сонымен қатар, ақпараттандыру саласында техникалық күрделіліктің ерекше жағдайлары және диагностика үшін білім мен дағдыларға деген қажеттілік жиі кездеседі.

Топтар мен жағдайлардың пайда болуы мен таралуына байланысты қылмыстарды анықтаудағы айырмашылық. Полиция, прокуратура, ақпараттық қауіпсіздік мамандары, цифрлық криминалистика мамандары және басқа да мамандар табысты тергеу және пайда табу үшін бірлесіп жұмыс істеуі керек.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеудегі маңызды рөл де көрінеді. Ақпаратты қорғауға және киберқылмыскерлерді қудалауға кепілдік беретін заңнаманы, арнайы нормалар мен ережелерді дамыту мұндай қылмыстарды ашудың көптеген жағдайларының бөлігі болып табылады.

Цифрлық технологияларды дамытудың қазіргі деңгейі қысқа мерзімде бүкіл халықты қамтуды қамтамасыз етуге мүмкіндік береді. Интернет желісі ,т-технологиялар, телекоммуникация желілері және төлем карталарын пайдалану арқылы жасалған алаяқтықтың виртуалды түрлері өзекті сипатқа ие болады.

Интернеттегі алаяқтық механизмінің процедуралық моделі өте үлкен. Бөтеннің мүлкін ұрлау механизмінің моделі немесе алдау немесе сенімге қиянат жасау арқылы бөтеннің мүлкіне құқық алу қылмыстық қол сұғушылық нысанасымен, дәлірек айтсақ, оның нысанымен (электрондық (цифрлық) ақша қаражаты) айқындалады, оған қол жеткізу банктік және кредиттік ұйымдардың цифрлық онлайн платформасымен қамтамасыз етіледі.

Интернет желілерінде жасалатын интернет-алаяқтық жасау механизмінің іс жүргізу моделіне жалпы сипаттама бере отырып, олар құқық

бұзушылықтарды дайындау, жасау және жасыру динамикасына бағытталған мақсатты байланысты әрекеттер жүйесі екенін атап өткен жөн.

Тіркелген интернет-алаяқтық құқық бұзушылықтар бойынша сотқа дейінгі тергеп-тексеру криминалистикалық маңызды цифрлық ақпаратты табуға және тіркеуге және одан әрі қылмыстық істер бойынша материалдардың дәлелі ретінде аударуға бағытталған. Сандық деректер одан әрі тергеу жағдайларын құрудың элементі ретінде бір-бірінен шығады. Оқиға орнын тексеруден бастап әрбір тергеу әрекеті тергеушіге одан әрі нұсқаларын ұсынуға және олар бойынша тергеу жүргізуге мүмкіндік беретін құқық бұзушылық жасау механизмі мен процесі туралы ақпарат беретінін атап өтуге болады.

СДТБТ-да тіркеудің негізін белгілеу және олар бойынша тексеру тергеу әрекеттерін жүргізу үшін шұғыл іс-шаралар жүргізу қажет:

– жеке тұлғаның жазбаша өтінішін іріктеп алу;

– оқиға орнын тексеру ретінде шұғыл тергеу әрекеттерін жүргізу;

– деректер мен қажетті материалдарды алу;

– жедел қызметкерлерге жасырын тергеу әрекеттерін жүргізуге жеке тапсырмалар беру.

Құқық бұзушылық орнын тексеру кезінде тергеу әрекеттеріне қатысу үшін шақыру қажет:

– бағдарламалық жасақтаманы әзірлейтін++, javascript бағдарламашылары;

– компьютерлерді пайдаланатын және жөндейтін бағдарламалық қамтамасыз ету жөніндегі операторлар немесе IT-мамандар;

– жүйелік әкімшілер, бағдарламашылар;

– телекоммуникациялық байланыстар және жабдықтар бойынша инженерлер мамандары;

– киберқауіпсіздікті қамтамасыз ету бойынша специалистов мамандары.

Тәжірибе көрсеткендей, аталған IT мамандары негізінен интернет-алаяқтық жасаған провайдер кәсіпорнының қызметкерлері болып табылады.

Интернет алаяқтық саласындағы құқық бұзушылықтар жоғары кідіріске ие және құқық қорғау органдары цифрлық технологиялар саласындағы арнайы дағдылар мен білімсіз қабылдаудың күрделілігімен байланысты айқын құқық бұзушылықтарды ғана ашады. Сондай-ақ, жәбірленуші тараптың тілегін қайтаратын залалдың шамалы болуы тергеу органдарына жүгінеді. Кейбір жағдайларда аймақтық деңгейдегі жедел бөлімшелердің қызметкерлерінде ұқсас құқық бұзушылықтарды ашуда қолданбалы тәжірибе жоқ. Интернет-алаяқтық бойынша деректерді зерттеу кезінде жәбірленушілерден жауап алу кезінде, ең алдымен, соңғысы ұйыммен байланысып, мәселелерді шешуге тырысатынын көрсету қажет. онлайн платформаларда қызмет көрсеткен.

Азаматтық құқықтық қатынастармен шектесетін құқық бұзушылықтардың ең көп таралған құрамдарының бірі-интернет-алаяқтық.

Интернет - алаяқтық пен азаматтық - құқықтық қатынастардың аражігін ажырату туралы мәселе қандай да бір шарт болған жағдайда басталады. Жазбаша немесе ауызша маңызды емес, бірақ оның қажеттілігі Қажет. Негізгі

мәні екі тараптың өзара қарым-қатынасы болып табылады: бір Тарап ақша қаражатын немесе мүлікті береді, екіншісі қызмет көрсетуге немесе мүлікті беруге (сатуға) міндеттенеді. Осылайша, міндеттемелер қарсы болуы керек.

Интернет алаяқтық кезінде құқық бұзушы мүлікті немесе ақша қаражатын алғысы келеді, шарт тек адамның қылмыстық ниетінің экраны болып табылады.

Азаматтық-құқықтық қатынастардың қалыпты жағдайында адам шарт бойынша өз міндеттемелерін орындау үшін белгіленеді.

Іс-әрекеттерді алаяқтық деп саралау мәселесі келесідей: шартты жасасқанға дейін кінәлінің ақша ұрлау ниетін анықтау және дәлелдеу қажет. Ол үшін кінәлі адам азаматтық құқықтық қатынастарға түскенге дейін де өз міндеттемелерін орындамайтынын анықтау қажет.

Негізгі қиындық-кінәлі адам өзінің шынайы қылмыстық ниетін мұқият жасырады.

Айта кету керек, жай шаруашылық жүргізуші субъектілердің жұмысымен байланысты азаматтық-құқықтық қатынастар және алаяқтық сипаттағы құқық бұзушылықтар жұқа сызықпен бөлінеді.

Сондықтан прокурорлар қадағалау қызметі барысында азаматтық-құқықтық қатынастарды нақты алаяқтықтан нақты ажырата білуі керек.

Қорытындылай келе, дәрістің бірінші сұрағы бізге ақпараттық технологиялар мен коммуникацияларды пайдалануға байланысты қылмыстық құқық бұзушылықтарды тергеудің күрделілігі мен ерекшеліктері туралы құнды ақпарат берілді. Біз қазіргі әлемде ақпараттық технологиялар біздің өмірімізде үлкен рөл атқаратынын білдік, бірақ олар сонымен бірге қоғамның қауіпсіздігіне қауіп төндіреді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу ақпараттық технологияларды қолданумен байланысты қылмыстармен сәтті және тиімді күресу үшін арнайы білім мен дағдыларды қажет етеді.

Дәрісте қарастырылған негізгі аспектілер:

1. Тергеудің техникалық аспектілері: компьютерлік іздер, метадеректер және интернет-трафик сияқты сандық деректерді жинау және талдау үшін арнайы бағдарламалық жасақтама мен әдістерді қолдану.

2. Тергеудің құқықтық аспектілері: ақпараттандыру және байланыс саласын реттейтін заңнаманы түсіну және цифрлық дәлелдемелерді алуға және пайдалануға қатысты ережелер мен процедураларды қолдану.

3. Халықаралық ынтымақтастық: ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар көбінесе трансшекаралық сипатқа ие, сондықтан әртүрлі елдердің құқық қорғау органдары арасындағы тиімді ынтымақтастық мұндай қылмыстарды табысты тергеу мен жолын кесу үшін қажетті шарт болып табылады.

4. Кәсіби даму: ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тиімді тергеу үшін білім мен дағдыларды үнемі жаңарту қажет, өйткені қылмыстың технологиялары мен әдістері үнемі дамып отырады. Жалпы, дәріс құқық қорғау органдарының заманауи ақпараттық технологиялар және онымен байланысты қауіптер туралы

хабардар болуының маңыздылығын атап өтті. Тұрақты оқыту мен ынтымақтастық арқылы ғана біз ақпараттандыру және байланыс саласындағы қылмыстармен тиімді күресіп қоғамның қауіпсіздігін қамтамасыз ете аламыз.

Соңғы компьютерлік және ақпараттық-телекоммуникациялық технологиялар ұзақ уақыт бойы қазіргі қоғамның өмірі мен қызметінің ажырамас бөлігіне айналды, оны Ақпараттық деп санауға болады. Мобильді байланыс құралдарының, компьютерлердің, Интернет желісінің, түрлі қосымшалардың және бағдарламалық қамтамасыз етудің кеңінен таралуы қоғам мен мемлекеттің қазіргі даму кезеңінің ерекшеліктерінің бірі болып табылады. Қазіргі және технологиялық жетістіктердің жағымсыз жағы бар-киберқылмыс. Айта кету керек, ақпараттық-телекоммуникациялық технологияларды қолдану арқылы жасалған қылмыстар жеке мемлекеттің емес, дамыған елдердің көпшілігінің проблемасы болып табылады.

Интернет желісін пайдаланушылар ақпараттық кеңістікте жеке өмірі туралы мәліметтерді, төлем карталарының деректерін, электрондық құжаттарды сақтайды, әртүрлі құрылғыларды қолдана отырып қаржылық операциялар мен азаматтық-құқықтық мәмілелер жасайды. Сонымен қатар, қылмыскерлер киберқылмыстардың, соның ішінде компьютерлік ақпарат саласындағы алаяқтықтың іздерін жасыру мен жасырудың жаңа тәсілдерін әзірлеуде. Олар зиянды бағдарламалық жасақтаманы, қосымшаларды, сайттарды және ақша қаражаттарын ұрлаудың басқа құралдары мен құралдарын жасайды, оларға банктердің онлайн-сервистері, онлайн-төлем сервистері, мобильді банктер және т. б. арқылы қол жеткізуге болады.

Қоғамның даму тенденциялары мен қылмыстық саланың жаңа бағытын ескере отырып, ақпараттық-телекоммуникациялық технологиялар саласындағы арнайы білім компьютерлік ақпаратты пайдалануға байланысты қылмыстарды тергеу кезінде сұранысқа ие және қажет бола бастады. Бұдан басқа, мұндай ақпарат барлық құқық қорғау органдарының, оның ішінде сотқа дейінгі тергеу органдарының қызметкерлерінің жұмысында құрал мәртебесіне ие болды. Шынында да, сот-медициналық маңызды компьютерлік ақпаратты алу және талдау дағдылары сотқа дейінгі тергеу органы маманының кәсіби құзыреттерін бекіту үшін маңызды компонент болып табылады, олар білім беру процесінің шеңберінде қалыптасып, одан әрі практикалық қызметте дамуы керек.

Одан әрі тергеу барысы сапалы жүргізілуіне байланысты болатын тергеу іс-қимылдарының алгоритмі маңызды рөл атқарады (оқиға болған жерді қарау, оның ішінде заттар мен құжаттарды қарау, жәбірленушілер мен ықтимал куәгерлерден егжей-тегжейлі сұрау салу; сот сараптамаларын тағайындау және жүргізу; күдіктілерден жауап алу және басқа да бірқатар тергеу әрекеттері, оларды жүргізу қажеттілігі нақты тергеу жағдайына байланысты қылмыстық іс бойынша),

Бүгінгі таңда компьютерлік ақпарат саласындағы алаяқтықты ашу және тергеу проблемаларына байланысты жүргізілген зерттеулерде осы қылмыстық істерді орындау әдістемелеріне кешенді және жан-жақты талдау жоқ екенін атап өтеміз. Қолданыстағы әдіс компьютерлік ақпарат

саласындағы алаяқтықты ашу мен тергеудің қажетті сапасын қамтамасыз етеді. Мұның салдары осы санаттағы ашылған қылмыстық істер санының азаюы және тергелген және соттың қарауына жіберілген қылмыстық істер бойынша елеулі нәтиженің болмауы болып табылады.

Өзін-өзі бақылау мәселелері:

1. Ақпараттандыру мен байланысқа байланысты қылмыстық құқық бұзушылықтардың негізгі түрлері қандай?
2. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеудің қандай ерекшеліктері бар?
3. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеуде қандай әдістер мен әдістер қолданылады?
4. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеуді қандай органдар жүзеге асырады?
5. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеудегі ынтымақтастықты қандай халықаралық келісімдер реттейді?
6. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеуде қандай проблемалар мен сын-қатерлер бар?
7. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеу кезінде қандай бұлтартпау шараларын қолдануға болады?
8. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеу кезінде азаматтардың қандай құқықтары мен бостандықтары шектелуі мүмкін?
9. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеу кезінде ақпаратты қорғаудың қандай құралдары мен әдістері қолданылады?
10. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеуді дамытудың қандай перспективалары бар?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Қазақстан Республикасының қандай заңнамалық актілері ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу мәселелерін реттейді?

a) Қылмыстық кодекс;

b) Конституция;

c) «Ақпарат және коммуникация туралы» заң;

d) Азаматтық кодекс;

e) Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы Кодексі.

2. Ақпараттандыру мен байланысқа байланысты қылмыстық құқық бұзушылықтардың негізгі түрлері қандай?

a) киберқылмыстар;

b) алаяқтық;

c) ұрлық;

d) кісі өлтіру;

e) авторлық құқықты бұзу.

3. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеуді қандай органдар жүзеге асырады?

A) ішкі істер министрлігі;

b) ұлттық қауіпсіздік комитеті;

c) Прокуратура;

d) Әділет министрлігі;

e) барлық аталған органдар.

4. Ақпараттандыру және байланыс саласында қылмыстық құқық бұзушылық жасаған адамдарға қатысты қандай шаралар қолданылуы мүмкін?

a) айыппұл;

b) бас бостандығынан айыру;

c) шартты айыптау;

d) міндетті жұмыстар;

e) барлық аталған шаралар.

5. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде қандай дәлелдер қолданылуы мүмкін?

a) айғақтар;

b) сараптамалық қорытындылар;

c) құжаттар мен материалдар;

d) фотосуреттер мен бейнежазбалар;

e) аталған барлық дәлелдер.

6. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде ақпаратты қорғау үшін қандай шаралар көзделген?

a) ақпараттық тасымалдағыштарды тәркілеу;

b) деректерді шифрлау;

c) физикалық қорғауды орнату;
d) ақпаратқа қол жеткізуді бақылау;
e) барлық аталған шаралар.

7. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу мәселелерін қандай халықаралық келісімдер реттейді?

a) шенген келісімі;
b) қылмыстық істердегі өзара құқықтық көмек туралы келісім;
c) киберқылмыс туралы Еуропалық конвенция;
d) еркін сауда туралы келісім;
e) барлық аталған келісімдер;

8. Қандай органдар ақпараттандыру және байланыс саласындағы заңнаманың сақталуын бақылауды жүзеге асырады?

a) байланыс және ақпараттандыру министрлігі;
b) монополияға қарсы комитет;
c) ұлттық қауіпсіздік комитеті;
d) білім және ғылым министрлігі;
e) барлық аталған органдар.

9. Жәбірленушілердің ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде қандай құқықтары бар?

a) өзінің ар-намысы мен қадір-қасиетін қорғау құқығы;
b) келтірілген залал үшін өтемақы алу құқығы;
c) хат алмасудың құпиялылық құқығы;
d) тергеуге қатысу құқығы;
e) барлық аталған құқықтар.

10. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың алдын алу үшін қандай шаралар көзделген?

a) ақпараттық кампаниялар өткізу;
b) халықты желідегі қауіпсіздік негіздеріне оқыту;
c) техникалық қорғау құралдарын әзірлеу және енгізу;
d) жедел-іздестіру іс-шараларын жүргізу;
e) барлық аталған шаралар.

§2. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар бойынша тергеу іс-қимылдарын жүргізуді ұйымдастыру

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар бойынша тергеу іс-қимылдарын жүргізуді ұйымдастыру тергеушілер мен құқық қорғау органдары тарапынан ерекше назар мен Құзыретті талап ететін күрделі және көп қырлы процесс болып табылады. Бұл дәрісте біз ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеудің негізгі ерекшеліктері мен принциптерін қарастырамыз.

Бірінші маңызды аспект-ақпараттандыру және байланыс саласының ерекшелігін түсіну. Қазіргі заманғы технологиялар мен байланыс құралдары біздің өмірімізде маңызды рөл атқарады, бірақ оларды заңсыз мақсаттарда да қолдануға болады. Сондықтан тергеушілер заманауи ақпараттық технологияларды терең білуі және түсінуі, сондай-ақ цифрлық дәлелдемелерді жинау, талдау және сақтау үшін арнайы бағдарламалар мен құралдарды тиімді пайдалана білуі қажет.

Екінші маңызды аспект-тергеу процесінде заңдылық пен әділеттілік принциптерін сақтау. Ақпараттандыру және байланыс саласындағы тергеу әрекеттерін жүргізу кезінде компьютерлік файлдар, электрондық пошта, әлеуметтік желілер және т.б. сияқты электрондық дәлелдемелермен жұмыс істеу ерекшеліктерін ескеру қажет.

Үшінші маңызды аспект-басқа мамандармен және ұйымдармен ынтымақтастық. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу көбінесе компьютерлік форензика сарапшыларымен, киберқауіпсіздік мамандарымен, байланыс провайдерлерінің өкілдерімен және басқа да мамандандырылған ұйымдармен өзара әрекеттесуді талап етеді. Тек күш біріктіру және ақпарат алмасу арқылы біз киберқылмыспен тиімді күресіп, ақпараттық кеңістіктің қауіпсіздігін қамтамасыз ете аламыз.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу тергеушілерден жоғары құзыреттілікті, заманауи технологияларды білуді және басқа мамандармен ынтымақтастықты талап ететін күрделі және жауапты процесс болып табылады. Осылайша ғана біз киберқылмыспен тиімді күресіп ақпараттандыру және байланыс саласындағы азаматтардың құқықтары мен мүдделерін қорғай аламыз.

Тергеу және сот практикасы компьютерлік ақпарат саласындағы алаяқтықты тергеудің бастапқы кезеңінде жүргізілетін негізгі тергеу әрекеттері мен жедел-іздестіру іс-шараларының шеңберін алдын ала анықтады: жәбірленушілерді (жәбірленуші тарап өкілдерін) анықтау және одан әрі жауап алу; жәбірленуші компьютерді не басқа да портативті құрылғыларды пайдаланған үй-жайда (тұрғын үйде) оқиға болған жерді қарап-тексеруді жүргізу; жедел-іздестіру техникалық байланыс құралдарын алу: ықтимал куәгерлерден немесе куәгерлерден жауап алу, күдікті адамдардан жауап алу: барлық қажетті сараптамаларды тағайындау және жүргізу.

Жәбірленушілерден жауап алу (жәбірленуші тарап өкілдерінен). Тәжірибе көрсеткендей, тергеудің бастапқы кезеңінде жәбірленушілер, әдетте, жанжалсыз жағдайда жауап алынады, өйткені олар күдікті қылмыскерді анықтауға және ұстауға мүдделі адамдар болып табылады. Куәгерлер әртүрлі позицияларды қабылдай алады - тергеуге қолайлы және керісінше, бұл куәгердің кімнің жағында екеніне және оның істің нәтижесіне деген қызығушылығына байланысты.

Белсенді адал жәбірленушілер, әдетте, оң жағынан сипатталады, тергеумен ынтымақтасады, қажетті іс-шараларға өз еркімен қатысады, тергеуге көмектесуге тырысады, оның нәтижелеріне қызығушылық танытады. Белсенді емес адал жәбірленушілер белсенділерден ерекшеленеді, олар пассивті әрекет етеді, тергеу барысына қызығушылық танытпайды, тергеушімен кездесуден аулақ болуға тырысады. Екі жағдайда да жауап алу кезінде жасалған қылмыстың ұмытылған бөлшектері мен мән-жайларын еске түсіруге бағытталған тактикалық әдістер қолданылады (алдыңғысын нақтылау және сабақтас оқиғаларды еске түсіру, құжаттар мен заттай дәлелдемелерді ұсыну, жауап алу кезінде ассоциативті байланыстарды белсенді пайдалану).

Тұрақсыз жәбірленушілер өз айғақтарын өзгертуге, бұрын берілген айғақтардан бас тартуға бейім, қылмыскермен (достық немесе отбасылық) байланысы болуы мүмкін. Жәбірленушінің бұл түрі сыртқы қысымға оңай ұшырауы мүмкін. Оларға көбінесе кәмелетке толмағандар жатады.

Жосықсыз жәбірленушілер, әдетте, жанжалға шынайы куәлік бермейді, агрессивті мінез-құлықпен сипатталады.

Тұрақсыз және жосықсыз жәбірленушілерден жауап алуға дайындық кезінде күдіктілерден жауап алуға, жанжал жағдайында дайындық бойынша тактикалық ұсыныстарды басшылыққа алу және өтірікті жеңуге, кінәні әшкерелеуге бағытталған тактикалық әдістерді қолдану (дәлелдемелер ұсыну, эмоционалдық шиеленісті пайдалану, тергеуді қызықтыратын мән-жайларды баяндаудың әртүрлі тәртібімен еркін баяндау әдісі, нақтылайтын, нақтылайтын мәселелерді белсенді қолдану, жауап алынатын адамның жеке басының жағымды қасиеттерін ынталандыру, ішкі қайшылықтарды қолдану және т. б.).

Мұндай теру жәбірленушілерден алғашқы жауап алуды дайындауда тиімді қолданылуы мүмкін. Сонымен, жәбірленушінің түрін және жауап алу кезінде тиісті тактиканы таңдауды ескере отырып, компьютерлік ақпарат саласындағы алаяқтықты тергеу кезінде жәбірленушілерден келесі ақпаратты анықтау қажет:

– қандай компьютерлік-техникалық құрал қылмыстық шабуылға ұшырады;

– дербес компьютерде немесе басқа техникалық құрылғыда жұмыс істеу дағдысының деңгейі және ұялы телефондарды пайдалану деңгейі;

– компьютерде немесе техникалық жағынан күрделі құрылғыда орнатылған бағдарламалық құралдар туралы білімнің болуы;

– интернет желісін ұсыну бойынша қызметтер көрсетуге қандай операторомен (провайдермен) шарт жасалды және қандай шарттарда;

– жәбірленуші өзіне қатысты алаяқтық әрекеттер жасағаны туралы қалай білді;

– қандай жағдайда қылмыстық оқиға қылмыскерлерді әшкерелеп, қылмыстық оқиға тізбегін белгілей алатын барлық деректерді көрсете отырып өтті;

– қылмыскерлермен визуалды байланыс болды ма, егер солай болса, қандай жағдайда кездесуге кім куә бола алады, сыртқы келбеттің егжей-тегжейлі сипаттамасы.

Көрсетілген мәселелер тізбесі негізінен жеке тұлғалардан анықталады, оларға қатысты компьютерлік ақпарат саласында алаяқтық жасалған заңды тұлғаларға қатысты сұрақтар тізбесі тергеу жүріп жатқан нақты тергеу жағдайына байланысты кеңейтіледі.

Компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша жәбірленуші ретінде заңды тұлға болған жағдайда да анықтау қажет мәселелердің шамамен тізімін береміз. Бұл жағдайда ұйымның қызметкерлері (мысалы, жүйелік әкімшілер, ақпараттық қауіпсіздік қызметкерлері, бухгалтерлер, менеджерлер, ақпараттық-техникалық қызмет көрсету қызметкерлері және т. б.) келесі мәселелер бойынша куәгер ретінде жауап алады:

– заңды тұлғаның орналасқан жері және қызмет түрі;

– ұйым қызметін реттейтін құжаттардың тізбесі, лицензиялардың болуы,

– жұмыс режимі, ішкі тәртіп, өткізу режимінің болуы жұмыс көлемі, жасалған шарттардың сипаты мен болуы, олардың түрлері, мазмұны мен шарттары, контрагенттердің атауы мен орналасқан жері;

– компьютерде сақталған ақпараттың мәні мен көлемі, оған қол жетімділіктің, кодтар мен парольдердің болуы;

– алаяқтық әрекеттермен келтірілген залалдың бар-жоғын, сипаты мен көлемін, оның келтірілу шарттарын құжаттамалық растау;

– қызметкерлердің қайсысы күдіктілермен, қылмыскерлермен байланысқа түсті, мұндай байланыстың сипаты;

– жасалған қылмыстың механизмі, қылмыстық нәтиженің себептері мен жағдайлары туралы жауап алынғандардың әрбір санатының пікірі.

Киберқылмысты тергеудің бастапқы кезеңінде объективті ақпараттың негізгі көзі оқиға болған жерді қарау сияқты тергеу әрекеті болып табылады.

Осы тергеу әрекетін жүргізу кезінде тергеушіде қылмыс белгілерінің болуы, оны жасау механизмі мен мән-жайлары туралы ақпарат жинау мүмкіндігі пайда болады, одан әрі анықталғанды тіркейді.

Киберқылмысты тергеу кезінде оқиға орнын тексеру: 1) қылмыс белгілерін анықтау, тіркеу, алып қою және оларды одан әрі бағалау; 2) қылмыстың анықталған белгілерін зерттеу арқылы оның жасалу мән-жайлары (қылмыскердің жасалу тәсілі, орны, уақыты, жеке басы және т.б.) белгіленеді; 3) қылмыс үшін пайдаланылатын ақпаратты алу мақсатында жүргізіледі. тергеу нұсқаларын құру және жедел-іздестіру іс-шараларын жүзеге асыру.

Киберқылмыстардың басты ерекшелігі-элемент киберкеңістік, ол арқылы шабуылдаушы заңмен қорғалатын құқықтарға, бостандықтар мен

мүдделерге қол сұғады. Тергеу кезінде тергеуші киберкеңістікте географиялық шекаралар болмағандықтан, бастапқы нүкте ретінде әрекет ететін орынды анықтау мәселесіне тап болады. Мәселен, мысалы, біреудің жеке банктік шотынан ақша ұрламақ болған шабуылдаушы кез-келген жерде (үй-жай, көше, саябақ, Көлік, басқа қала, ел және т.б.) орналастыру арқылы осы мақсатқа жету үшін негізгі әрекеттерді жүзеге асыра алады. Тергеуші, өз кезегінде, шабуылдаушының жеке басын анықтау үшін бірқатар тергеу әрекеттерін орындауы керек, бастапқы нүкте-оқиға орны. Айта кету керек, киберқылмыстарда, егер қылмыстық қол сұғушылық шабуылдаушының физикалық сатуынсыз жүзеге асырылса, оқиға орны әрдайым бола бермейді.

Қазіргі заманғы криминалист ғалымдардың ұстанымы бар, олар оқиға орнын «киберкеңістік» деп санау керек деп санайды. Бұл үкім қайшылықты, өйткені киберкеңістік қылмыстың іздері орналасқан жер болса да, дәстүрлі мағынада оқиға орны-бұл сезім мүшелерінің көмегімен анықтауға болатын қылмыс белгілері бар физикалық іске асырылған, материалдық орын. Біз білетіндей, киберкеңістікті сезім мүшелерін емес, техникалық құрылғыларды қолдану арқылы зерттеу мүмкін емес.

Жоғарыда айтылғандардан басқа, киберқылмыстарда оқиға орны әр түрлі болуы мүмкін учаскелер орман алқабынан, көлік құралынан бастап техникалық құрылғыны орнатуға немесе тасымалдауға болатын жерлер. саябақ үй - жаймен немесе бірқатар үй-жайлармен аяқталады. Сапалы тергеу әрекетін жүргізу үшін тергеуші бірқатар дайындық шараларын жүргізуі керек.

Киберқылмыстар бойынша оқиға орнын тексеруге дайындық кезінде тергеуші тергеу әрекетіне қатысатын адамдар туралы мәселені шешуі керек.

Оқиға орнына келген соң тергеушіге ұсынылады:

1) оқиға орнына өзінің келу уақытын белгілеуге және қажет болған жағдайда жәбірленушіге қажетті көмек көрсетілгеніне көз жеткізуге, оқиғаның салдарын жою жөнінде шаралар қабылдауға міндетті. Сондай ақ оқиға орнын тексеру кезінде қалыптасқан жағдайды бекіту үшін бағдарлау және шолу фототүсірілімін жүргізу;

2) құрылғылардың бетінде немесе ішінде болуы мүмкін көрсетілген іздердің сақталуы жөнінде шаралар қабылдау қажет, ол үшін: a) оқиға орнындағы адамдардың ешқайсысына компьютерлік жабдыққа қол тигізуге рұқсат бермеу; b) оқиға орнындағы адамдарға электрмен жабдықтауды өшіруге рұқсат бермеу; d) маманның қатысуынсыз техникамен ешқандай айла-шарғы жасамау егер тәуелсіз іс-әрекеттердің нәтижесінде криминалистикалық маңызды ақпаратқа зақым келтіру мүмкіндігі болса; e) табылған құрылғыларды оқиға орнына келген кезде (күйі Қосулы немесе өшірулі)сол күйінде қалдыру);

3) егер тексеру объектісі жергілікті желімен қосылған стационарлық құрылғылар болып табылса, барлық құрылғылардың жұмысын ұйымдастыратын орталықтандырылған сервердің бар-жоғын анықтау, сондай-ақ жергілікті қосылу арқылы тексерілетін үй-жайдан тыс жабдықпен өзге де қосылыстар орнату;

4) тексерілетін жабдықтың телефон желісімен байланысы бар-жоғын анықтаңыз. Егер байланыс болған жағдайда шабуылдаушының телефон желісін пайдалану фактісінің бар жоғын анықтаған сәтке дейін оны пайдалануды тоқтату қажет;

5) құрылғыда және маманның көмегімен қандай бағдарламалар жұмыс істейтінін анықтаңыз және оларды хаттамада егжей-тегжейлі сипаттаңыз, егер маман ақпаратты жоюға қабілетті зиянды бағдарламаны тапса, онда маманнан осы бағдарламаның жұмыс уақытын, оны өшірген жағдайда қандай салдарлар болатынын нақтылау қажет.

Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар бойынша тергеу әрекеттерін жүргізу кезінде ұйымдық және құқықтық тетіктерді жетілдіруді талап ететін күрделі және көп қырлы процесс болып табылады.

Бүгінгі таңда Ақпараттық технологиялар мен байланыстың даму деңгейі қылмыскерлерге интернет желісін және басқа да электрондық байланыс құралдарын пайдалана отырып қылмыс жасауға мүмкіндік береді. Бұл осы салада тергеу әрекеттерін тиімді ұйымдастыруды қажет етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеудегі негізгі кедергілердің бірі интернет желісінің анонимділігі мен алдамшылығы болып табылады. Қылмыс жасалған жерді және қылмыскердің жеке басын анықтау жиі қиын. Осыған байланысты құқық қорғау органдары жұмысты үйлестіруді және ақпарат алмасуды ішкі деңгейде ғана емес, халықаралық деңгейде де жақсартуы қажет.

Негізгі міндеттердің бірі ақпараттық технологиялар саласындағы құқық қорғау органдары қызметкерлерінің құзыретін арттыру және даярлау болып табылады. Арнайы курстар, тренингтер және оқыту осы салада жұмыс істейтін қызметкерлерді кәсіби даярлаудың міндетті элементтері болуға тиіс.

Сондай-ақ құқық қорғау органдары, сондай-ақ бизнес және азаматтық қоғам өкілдерімен ынтымақтастықты дамыту қажет. Барлық деңгейдегі өзара іс қимыл ақпараттандыру және байланыс саласындағы қылмыстармен тиімді күресуге мүмкіндік береді.

Қорытындылай келе, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар бойынша тергеу іс-қимылдарын жүргізуді ұйымдастыру күрделі және маңызды міндет болып табылатынын атап өткен жөн. Оның табысты орындалуы заңнаманы және ұйымдастырушылық тетіктерді жетілдіруді, қызметкерлердің біліктілігін арттыруды және барлық мүдделі тараптар арасындағы тиімді өзара іс-қимылды қамтамасыз етуді талап етеді. Тек осы жағдайда ғана біз тиімдірек тергеуге және кінәлілерді жазалауға қол жеткізе аламыз.

Өзін-өзі бақылау мәселелері:

1. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеудің қандай ерекшеліктері бар?
2. Осы салада тергеу әрекеттерін жүргізу кезінде қандай әдістер мен құралдар қолданылады?
3. Ақпараттандыру және байланыс саласындағы қылмыстық істерді тергеуде цифрлық дәлелдемелерді алу және қамтамасыз ету қандай ерекшеліктерге ие?
4. Осы салада тергеу әрекеттерін жүргізу кезінде ақпараттың құпиялылығы мен сақталуын қамтамасыз ету үшін қандай шаралар қолданылады?
5. Ақпараттандыру және байланыс саласындағы қылмыстық істерде цифрлық дәлелдемелерді зерттеуді жүргізетін сарапшыларға қандай талаптар қойылады?
6. Тергеушілер мен жедел қызметкерлердің осы саладағы қылмыстық құқық бұзушылықтарды тергеу кезінде қандай құқықтары мен міндеттері бар?
7. Ақпараттандыру мен байланысқа байланысты қылмыстық істерде жедел-іздестіру іс-шараларын жүргізудің ерекшеліктері қандай?
8. Ақпараттандыру және байланыс саласындағы тергеу әрекеттерін жүргізу кезінде алынған ақпаратты рұқсатсыз қол жеткізуден қорғау үшін қандай шаралар қолданылады?
9. Осы саладағы қылмыстық істерді тергеу кезінде сот сараптамасын жүргізудің қандай ерекшеліктері бар?
10. Ақпараттандыру мен байланысқа байланысты қылмыстық істерде тергеуге жататын адамдардың құқықтары мен заңды мүдделерінің сақталуын қамтамасыз ету үшін қандай шаралар қолданылады?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде қандай тергеу әрекеттері жүргізілуі мүмкін?

a) тінту;

b) жауап алу;

c) жауаптар a)және b);

d) сараптама;

e) жоғарыда айтылғандардың барлығы.

2. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар бойынша тергеу әрекеттерін жүргізуге кімнің құқығы бар?

a) тергеуші;

b) прокурор;

c) судья;

d) полиция қызметкері;

e) жоғарыда айтылғандардың барлығы.

3. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде тінту жүргізудің қандай ерекшеліктері бар?

a) сандық құрылғыларды іздеу және алу;

b) мамандандырылған бағдарламалық жасақтаманы пайдалану;

c) ақпараттық қауіпсіздік саласындағы мамандардың қатысуы;

d) жоғарыда айтылғандардың барлығы;

e) ешқандай ерекшеліктері жоқ.

4. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде жауап алу қалай жүргізіледі?

a) кәдімгі жауап алу хаттамалары арқылы;

b) көрсеткіштерді жазу және талдау үшін арнайы бағдарламаларды пайдалана отырып;

c) ақпараттық технологиялар саласындағы мамандардың қатысуымен;

d) жоғарыда айтылғандардың барлығы;

e) ешқандай жолмен жүргізілмейді.

5. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде қандай сараптамалар жүргізілуі мүмкін?

a) компьютерлік сараптама;

b) сот-медициналық сараптама;

c) техникалық сараптама;

d) жоғарыда айтылғандардың барлығы;

e) ешқандай сараптама жүргізілмейді.

6. Ақпараттандыру және байланыс саласындағы тергеу әрекеттерін жүргізу кезінде ақпараттық қауіпсіздікті қамтамасыз ету қалай жүзеге асырылады?

a) деректерді шифрлауды қолдану;

b) антивирустық бағдарламалық жасақтаманы орнату;

c) ақпараттық ресурстарға қол жеткізуді шектеу;

d) жоғарыда айтылғандардың барлығы;

e) ақпараттық қауіпсіздікті қамтамасыз ету талап етілмейді.

7. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде жедел-іздестіру іс-шараларын жүргізудің қандай ерекшеліктері бар?

a) интернет-трафикті бақылау және талдау;

b) мониторинг үшін арнайы бағдарламалық қамтамасыз етуді пайдалану;

c) интернет-провайдерлермен ынтымақтастық;

d) жоғарыда айтылғандардың барлығы;

e) ешқандай ерекшеліктері жоқ.

8. Ақпараттандыру және байланыс саласындағы тергеу әрекеттерін жүргізу кезінде ақпараттың сақталуы мен дұрыстығын қамтамасыз ету үшін қандай шаралар қолданылуы мүмкін?

a) деректердің сақтық көшірмесін жасау;

b) цифрлық қолтаңбаларды пайдалану;

c) ақпаратты қорғалған қоймаларда сақтау;

d) жоғарыда айтылғандардың барлығы;

e) ешқандай шаралар қолданылмайды.

9. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде қандай шектеулер бар?

a) құпиялылық және жеке өмірге қол сұғылмаушылық қағидаттарын сақтау;

b) ақпаратқа қол жеткізу құқығын сақтау;

c) кінәсіздік презумпциясы принципін сақтау;

d) жоғарыда айтылғандардың барлығы;

e) ешқандай шектеулер жоқ.

10. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергеу кезінде басқа мемлекеттермен ынтымақтастық қалай жүзеге асырылады?

a) сұрау салу және ақпарат алмасу бойынша;

b) халықаралық келісімдер мен уағдаластықтар арқылы;

c) мамандандырылған халықаралық ұйымдарды пайдалана отырып;

d) жоғарыда айтылғандардың барлығы;

e) ешқандай жолмен жүзеге асырылмайды.

§3. Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы қазіргі цифрлық әлемдегі өзекті және маңызды тақырып болып табылады. Технологияның дамуымен және компьютерлер мен интернеттің көбірек қолданылуымен компьютерлік ақпарат саласындағы алаяқтық қылмыстық әрекеттің кең таралған түрлерінің біріне айналды. Бұл мәтінде біз компьютерлік ақпарат саласындағы алаяқтықтың сот-медициналық сипаттамасының негізгі аспектілерін, оның ерекшеліктері мен салдарын қарастырамыз.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы киберқылмыспен күресудің маңызды аспектісі болып табылады. Бұл саладағы алаяқтық компьютерлік жүйелер мен желілер арқылы жүзеге асырылатын заңсыз қол жеткізу, бұзу, жеке басын ұрлау, қаржылық алаяқтық және басқа да алаяқтық қылмыстардың кең ауқымын қамтиды.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы келесі аспектілерді талдауды қамтиды:

1. Техникалық аспектілер: криминалистикалық сарапшылар қылмыстың техникалық егжей-тегжейлерін зерттейді, мысалы, бұзу әдістері, зиянды бағдарламалық жасақтаманы пайдалану, анонимді желілерді пайдалану және т.б. олар IP мекенжайлары, журналдар, метадеректер және басқа да техникалық артефактілер сияқты қылмыскерлер қалдырған іздерді талдайды.

2. Психологиялық аспектілері: сот сарапшылары компьютерлік ақпарат саласындағы алаяқтардың мотивтері мен психологиялық сипаттамаларын зерттейді. Олар қылмыскерлердің жәбірленушілерді манипуляциялау үшін қандай стратегияларды қолданатынын, олардың алдау, манипуляциялау және адастыру тәсілдерін талдайды.

3. Қаржылық аспектілер: сот сарапшылары компьютерлік ақпарат саласындағы алаяқтықтың қаржылық іздерін зерттейді. Олар қаржылық операцияларды, ақша аударымдарының іздерін, виртуалды валюталарды пайдалануды және қылмыстың басқа қаржылық аспектілерін талдайды.

4. Әлеуметтік аспектілер: сот сарапшылары компьютерлік ақпарат саласындағы алаяқтықтың әлеуметтік аспектілерін зерттейді. Олар қылмыскерлердің адамдарды алдау және манипуляциялау үшін әлеуметтік инженерияны, фишингті, фармингті және басқа әдістерді қалай қолданатынын талдайды.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы құқық қорғау органдарына киберқылмыстарды ашуға және алдын алуға көмектеседі. Бұл қылмыстың сипаттамаларын анықтауға, қылмыскерлерді анықтауға және оларды жауапқа тарту үшін дәлелдер жинауға мүмкіндік береді. Сонымен қатар, ол кибершабуылдан тиімді қорғаныс шараларын әзірлеуге және компьютерлік ақпарат саласындағы қауіптер туралы хабардарлықты арттыруға көмектеседі.

Компьютерлік ақпарат саласындағы алаяқтық деректердің қауіпсіздігі мен құпиялылығына үлкен қауіп төндіреді. Қылмыстың бұл түрінің

криминалистикалық сипаттамасы оның ерекшеліктерін, әдістері мен белгілерін анықтауға, сондай-ақ оның алдын алу және онымен күресудің тиімді шараларын жасауға мүмкіндік береді. Құқық қорғау органдары мен киберқауіпсіздік мамандарының осындай қылмыстарды ашу және тергеу үшін заманауи әдістер мен технологиялармен ынтымақтасуы және қолдануы маңызды. Тек осылай ғана ақпараттың қауіпсіздігін және компьютерлік ақпарат саласындағы алаяқтықтан қорғауды қамтамасыз етуге болады.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы осы санаттағы қылмыстық істерді тергеу кезінде ескеру қажет бірқатар ерекшеліктерге ие.

Сот-медициналық сипаттаманың негізгі элементтерін қарастырыңыз.

Орын мен уақытты болдырмайтын қылмыс жасау жағдайы. Компьютерлік ақпарат саласындағы алаяқтық орынының сипаттамасы белгілі бір ерекшеліктерге ие. Бір жағынан, қылмыс жасалған жер ақпараттық-Телекоммуникациялық желінің өзі болып табылады, онда қолда бар компьютерлік ақпаратты енгізу, жою, бұғаттау орын алады. Екінші жағынан, қылмыс жасалған Жер нақты техникалық құрылғының орналасқан жері болып табылады.

Телекоммуникациялық желіден басқа алаяқтық жасау орны ақша қаражатын (банкоматтар, интернет-дүкендер және т.б.) «олма-қол ақшаға айналдыру» орны болып табылады.

Қылмыс жасау уақытына келетін болсақ, бұл қылмыскердің қылмыстық жоспарды қай уақытта жүзеге асыра бастағанына және қолма-қол ақшаны қашан алғанына байланысты. Яғни, ақша қаражатын алмаған жағдайда, тек компьютерлік ақпаратты сақтау, өңдеу немесе беру құралдарын енгізу, жою, бұғаттау немесе олардың жұмыс істеуіне өзге де араласу бойынша әрекеттер жасағанда ғана алаяқтыққа дайындалу немесе осындай қылмыс жасауға әрекет жасау белгілері болуы мүмкін.

Компьютерлік ақпарат саласындағы алаяқтыққа байланысты істер бойынша қылмыстық қол сұғушылықтың нысанасы болуы мүмкін:

– ақшалай қаражат: қаскүнемдер адам өмірінің әртүрлі салаларында көрсетілетін кез келген Қызметтер арқылы ақша қаражатын заңсыз ала алады. Айта кету керек, кейбір жағдайларда бағалы қағаздар, төлем тапсырмалары және басқалары да тақырып бола алады;

– жәбірленушіні бұзуы мүмкін жеке сипаттағы ақпарат: мәселен, мысалы, ең көп тарағандары-әртүрлі әлеуметтік желілердегі аккаунттардың парольдері, төлем карталарының нөмірлері және басқа да осыған ұқсас мәліметтер;

– жылжымалы және жылжымайтын мүлікке құқық: әдетте, бұл пәтерлер, үйлер, автомобильдер және зергерлік бұйымдар;

– ақпаратты ұстау: бұл топ аудиовизуалды және электронды ұстау әдістерін қолдану арқылы компьютерлік деректер мен командаларды алуға бағытталған компьютерлік қылмыстарды жасау тәсілдерінен тұрады. Ақпарат алаяқтықты одан әрі жасау үшін бастапқы деректерді, парольдерді, кіру кодтарын, шот нөмірлерін, банктік операцияларды жүргізу тетіктерін алуға қызмет ете алады.

Компьютерлік техника құралдарына рұқсатсыз қол жеткізу. Бұл топ ортақ мақсатпен сипатталатын әртүрлі әдістерді біріктіреді – компьютерлік ақпаратқа рұқсатсыз қол жеткізу. Мысалы, «компьютерлік отырғызу» жәбірленушінің компьютерлік жүйесі туралы алдын-ала алынған мәліметтерді кездейсоқ таңдау немесе пайдалану арқылы жүзеге асырылады. «Әлеуметтік инженерия» (ақпараттық қауіпсіздік контекстінде) – белгілі бір әрекеттерді жасау немесе құпия ақпаратты жария ету мақсатында адамдарды психологиялық айла-шарғы жасау. Сондай-ақ, алаяқтар "баяу таңдау" әдісін қолданады, онда қорғаудың әлсіз жақтарын іздейді, содан кейін жүйеде қамтылған ақпаратты зерттеу мүмкіндігі пайда болады.

Деректерді манипуляциялау және басқару топтары. Мысалы, деректерді ауыстыру (жаңа деректерді өзгерту немесе енгізу). Ең көп таралған әдіс – «трояндық ат». Зиянды бағдарламалардың басым көпшілігі осы түрге жатады. Компьютерлік вирустарды үш жалпыланған топқа бөлуге болады: жүктеу (жүйелік) вирустар (машиналық жадтың жүктеу секторларына әсер етеді); файлдық вирустар (орындалатын файлдарға, соның ішінде com-ға әсер етеді. ..exe… sys….) аралас вирустар.

Аралас топтар. Алаяқтық әрекеттерді жасау кезінде жоғарыда аталған екі немесе одан да көп тәсілдер қолданылады.

Қылмыстардың талданатын санатына тән белгілерге, ең алдымен, киберқылмысты анықтаудың, анықтаудың тиімді механизмінің болмауынан туындаған жоғары кідіріс жатады. Ұйымдастырушылық киберқылмыстар, әдетте, бірнеше адамның бөтен мүлікті ұрлау механизмін қажет ететіндігіне байланысты. Трансұлттық екі және одан да көп мемлекеттерге не екі және одан да көп мемлекеттердің заңды немесе жеке тұлғаларының мүдделеріне нұқсан келтіретін белгілі бір кезеңде жасалған қылмыстардың жиынтығында көрінеді. Бұл Интернет желісі арқылы әртүрлі елдерде тұратын қылмыскерлер арасындағы өзара әрекеттесуді қамтамасыз етуге кедергілердің болмауынан, сондай-ақ оларды қылмыстық жауапкершілікке тарту процедурасының белгілі бір қиындықтарынан туындайды, өйткені қылмыскерлер әдетте әртүрлі мемлекеттердің юрисдикциясында болады. Бұл жеке тұлғаны анықтау, қамауға алу және дәстүрлі тәсілдермен қудалау процесін қиындатады. Осы ерекшеліктерді ескере отырып, қылмыскер ұсталудан қорқып, қылмыс орнына оралу мүмкіндігіне ие.

Із түзу механизмі. Компьютерлік ақпарат саласында алаяқтық жасаған кезде із жасау механизмінің өзіндік ерекшеліктері бар. Бұл қылмыстарды жасаған кезде идеалды іздер мүлдем жоқ. Бұл шабуылдаушылардың барлық алаяқтық әрекеттерін жәбірленушімен жеке байланыссыз жасайтындығына байланысты.

Көптеген жағдайларда компьютерлік ақпаратқа тән нақты іздер қалады:

– домендік атауды тіркеу деректері, домендік атауларды тіркеушімен өзара әрекеттесуден логин; осы тіркеушіге төлем жүргізу іздері;

– алаяқтар доменін қолдайтын DNS қызметін орнату кезіндегі іздер;

-орналастыру веб-сайты бар хостинг провайдерімен өзара әрекеттесудің іздері: тапсырыс, төлем, теңшеу, мазмұн шығанағы;

– сайтқа кірген кезде пайдаланушы жабдығы қалдырған іздер (мысалы, cookie файлдары, сессия жазбасының деректері, жарнама трекерлері, IP-мекен-жайы туралы мәліметтер және т.б.).

Алаяқтық құрбандарымен өзара әрекеттесу кезінде алаяқтар келесі іздерді қалдырады: электрондық пошта арқылы, веб-форум арқылы тапсырыстарды қабылдау кезінде пошталық мекен-жай деректері, сайттың диалогтық терезесінде немесе ықтимал құрбандармен қосымшада хат алмасу.

Зиянды бағдарламалық қамтамасыз етуді пайдалана отырып компьютерлік ақпарат саласында алаяқтық жасау барысында мынадай цифрлық іздер қалдырылуы мүмкін:

– файлдар (орындалатын және әртүрлі скриншоттар, динамикалық жүктелетін кітапхана файлдары, лог-файлдар, мұрағаттар, электрондық пошта файлдары);

– жүйені қашықтан немесе жергілікті басқаруға, жүйелік деректерді жоюға, сондай-ақ пайдаланушы деректерін ұрлауға және жүйе туралы мәліметтерді жинауға арналған бағдарламалар;

– жүйелік оқиғалар мен ақпараттық қауіпсіздік оқиғалары журналдарының жазбалары;

– іске қосылған процестер мен қызметтердің тізімі;

– қолданыстағы және жақында орнатылған желілік қосылыстардың тізімі;

– siem-жүйелер экраны, антивирустық бағдарламаның ақпараттық қауіпсіздігі оқиғалары туралы ақпарат;

– жергілікті және домендік пайдаланушылардың тізімі;

– бағдарламаларды іске қосу тізілімінің кілттері;

– тапсырмаларды жоспарлаушының деректері;

– артефактілер және бағдарламаны іске қосу метадеректері (Prefetch, Amcache).

Алаяқтық әрекеттер жасау мақсатында қылмыскерлер интернет желісін пайдаланушылар төлемдер жүргізу кезінде өз құрылғыларында және браузерлерінде қалдыратын цифрлық іздерді (экран және операциялық жүйе туралы деректер; уақыт белдеуі, браузер серверге жіберетін тақырыптар, орнатылған плагиндер, терезе өлшемі және т. б.) және кеңейтілген деректер негізінде жиналатын деректерді пайдаланатынын ескеріңіз. аналитиктер және кеңейтілген оқыту алгоритмдері соның ішінде cookie файлдары және пайдаланушының сандық әдеттері.

Ақша қаражатын алу процесінде іздер қалады: төлем жүйесіне ақша енгізу кезінде(жәбірленушіге көрсетілетін деректемелер), алаяқтар бақылайтын шоттар арасында ақша аудару кезінде ақша қаражатын алу, шоттарды қашықтықтан басқару (ашу және жабу); алаяқтардың ақшаны жуу және қолма-қол ақшамен делдалдармен өзара әрекеттесуі.

Антивирустық және тестілік бағдарламалардың, сондай-ақ зиянды бағдарламалық жасақтаманың компьютерде немесе басқа құрылғыда, мысалы, жәбірленушінің ұялы телефонында жұмыс істеу нәтижесінде қалған іздер туралы ақпарат маңызды сот-медициналық маңызы бар. Құрылғымен қандай да бір әрекеттер жасалмағанын білу керек, оны кім бастағанына және

қай уақытта болғанына қарамастан, жергілікті немесе қосылған интернет желісіне біріктірілген жекелеген құрылғылар арасындағы байланыс арналары арқылы ақпараттың өтуі туралы ақпарат қызығушылық тудырады. Мұндай ақпарат жүргізуді автоматтандырылған жүйе автоматты режимде жүзеге асыратын log-файлдарда сақталады және байланыс уақыты (байланыс сеансының басталу, аяқталу уақыты және ұзақтығы), статистикалық немесе динамикалық IP-мекенжайлар, телефон нөмірлері, хабарламаның берілу жылдамдығы, пайдаланылған хаттамалардың түрін қоса алғанда, байланыс сеансының сипаттамалары, хаттамалардың өзі туралы ақпаратты сақтайды, Пайдаланылған желілік жабдықтың MAC-мекен-жайы, жүйелік уақыт және т.б.

Осы санаттағы істер бойынша қылмыскердің жеке басының өзіндік ерекшеліктері бар. Қылмыстық топтардың ұйымдастырушылары немесе көшбасшылары болып табылатын алаяқтар, әдетте, жоғары білімге ие және компьютерлік технологиялар саласында арнайы білімге ие, егер қарапайым орындаушылар туралы айтатын болсақ, онда олар, әдетте, орташа тұлғалар, орта білімі бар және олардың функциялары топ жетекшілерінің нұсқауларын нақты орындауда.

Компьютерлік ақпарат саласындағы қылмыскерлердің жас критерийі бойынша екі топқа бөлінуі керек екенін атап өткен жөн.

Бірінші топ шамамен 16-22 жастағы адамдардан тұрады. Бұл жоғары сынып оқушылары немесе техникалық бейімділігі бар орта арнаулы оқу орындарында оқитын студенттер, көбінесе жоғары оқу орындарында ақпараттық технологиялармен байланысты мамандықтар бойынша оқитын адамдар. Бұл адамдар әдетте бірінші рет қылмыс жасайды: қылмыстың мәні көбінесе аз ақша болып табылады. Аталған санаттағы адамдарға алаяқтық жасау туралы қылмысты Мұқият дайындаудың және жасырудың жоқтығы да куәландырады.

Беттің екінші тобы – 23 жастан асқан. Осы санаттағы адамдар белгілі бір арнайы білімге ие, компьютерлік технологиялар саласында жоғары білімі бар, сондай-ақ компьютерлік ақпаратты сақтау, өңдеу немесе беру құралдарының жұмысына араласудың көмегімен белгілі бір қылмыстық әсер ету тәжірибесі бар. Олар зейінділікпен және белгілі бір кәсібилікпен ерекшеленеді. Қылмыстық әрекеттер жәбірленушілер шеңберінің болуымен, елеулі материалдық залал келтірумен көп эпизодтық сипатта болады, қылмыс іздерін жасауға және жасыруға мұқият дайындықпен сипатталады. Компьютерлік техника құралдарын пайдалана отырып жасалатын қоғамдық қауіпті қылмыстардың көпшілігі, аса ірі көлемде ақша қаражатын иемдену, алаяқтық осы адамдар тобының үлесіне тиеді.

Қылмыскерлердің жеке басының жоғарыда аталған ерекшеліктерін ескере отырып, қылмыстарды сотқа дейінгі тергеу органдарының алдында тұрған көптеген міндеттердің бірі-оған қарсы әрекетті жеңу немесе бейтараптандыру. Мұндай қарсы іс қимылдың ерекшеліктеріне байланысты құқық қорғау органдары тиісті шаралар қабылдайды.

Қылмыстың осы түрі бойынша жәбірленушілер кез келген жеке тұлғалар болуы мүмкін, бірақ тәуекел тобына ақпараттық технологияларды

білмейтіндер жиі түседі; интернет-дүкендерде жиі сатып алушылар, төлем жүйелерін пайдаланушылар, банк клиенттері болып табылатын тұлғалар; әртүрлі мақсаттарда Интернет желісін пайдаланатын тұлғалар және т. б.

Жеке ақпаратты алаяқтық жолмен алатын жәбірленушілерге қатысты, олар банктердің ескертулеріне, төлем жүйелеріне бөгде адамдарға карта нөмірі, PIN-код және т.б. туралы құпия ақпаратты жібермеу туралы ескертулерге назар аудармайтындығын атап өтуге болады.

Алаяқтық жасауға ықпал ететін негізгі себептер:

– бағдарламалық қамтамасыз етудің жеткіліксіз деңгейі;

– қашықтықтан бірнеше компьютерді автоматтандыру;

– операциялық жүйелерді бұзу кезінде қылмыскерлердің ықтимал мүмкіндіктері;

– бірыңғай базада әртүрлі деңгейдегі және деңгейдегі ақпаратты сақтау;

– пайдаланушылардың компьютермен жұмыс істеу кезінде қауіпсіздік шараларын сақтамауы, оның ішінде қауіп-қатерді көрсететін бағдарламаларды елемеу, мысалы, "Антивирус"жүйелері;

– бірнеше пайдаланушының белгілі бір компьютеріне кіру;

– жәбірленушілердің орын алған қылмыстық оқиға туралы мәлімдемеуіне байланысты қылмыстардың кідірісінің едәуір деңгейі, өйткені бұл лауазымдық міндеттерді орындау кезіндегі немқұрайлылық пен кәсіпқойлықтан не қылмыскерлерді анықтау кезінде компьютерлік жүйеге араласу жөніндегі қылмыстық іс-қимылдардың табылуына байланысты ұйым басшылары тарапынан ақпараттың жария етілуіне мүдделі болмауынан болды іс жүзінде мүмкін емес;

– құқық қорғау органдарының қызметкерлерінде компьютерлік ақпарат саласындағы алаяқтық туралы қылмыстық істерді тергеушілердің, осы салада белгілі бір арнайы білімнің болмауы, соның салдарынан тергеу әрекеттері сауатсыз жүргізіледі, бұл одан әрі тергеудің тиімсіздігіне әкеледі.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы қылмыстық қол сұғушылықтың мәні, жағдай және қылмыс жасау тәсілі туралы әрбір ақпараттың жүйесі тұрғысынан қарастырылады.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы компьютерлік технологияны қолданумен байланысты қылмыстармен күресудің маңызды құралы болып табылады. Осы саладағы алаяқтық адамдардың жеке қауіпсіздігіне, қаржысы мен құпиялылығына, сондай-ақ ақпараттық жүйелердің тұрақтылығы мен сенімділігіне елеулі қауіп төндіреді.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы қылмыскерлер алаяқтық әрекеттерді жасау үшін қолданатын әдістер мен құралдарды талдауды және зерттеуді қамтиды. Бұған бұзу, фишинг, фарминг, вирустар және зиянды бағдарламалық жасақтаманың басқа түрлері сияқты техникалық аспектілерді зерттеу кіреді.

Сот-медициналық сипаттама сонымен қатар компьютерлік ақпарат саласындағы алаяқтықтың психологиялық және социологиялық аспектілерін талдауды қамтиды. Қылмыскерлердің себептері мен мінез құлқын зерттеу

мұндай қылмыстардың алдын алу мен жолын кесудің тиімді стратегияларын жасауға көмектеседі.

Технологияның дамуымен және интернеттің кеңеюімен компьютерлік ақпарат саласындағы алаяқтық барған сайын күрделене түсетінін атап өткен жөн. Сондықтан қылмыскерлерден бір қадам алда болу үшін сот-медициналық сипаттама үнемі жаңарып, дамып отыруы керек.

Компьютерлік ақпарат саласындағы алаяқтықпен күресу мақсатында құқық қорғау органдары, ақпараттық қауіпсіздік жөніндегі мамандар және басқа да мүдделі тараптар арасындағы ынтымақтастықты дамыту қажет. Тек бірлескен күш жігермен ғана қылмыстың осы түрімен тиімді күресуге және қоғамның мүдделерін қорғауға болады.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы қылмыстың іздерін талдауды, қолданылған әдістер мен құралдарды бағалауды, кінәлілерді анықтауды және дәлелдемелерді жинауды қамтиды. Бұл құқық қорғау органдарына қылмыстарды тиімді тергеуге және кінәлілерді жауапқа тартуға мүмкіндік береді.

Алайда, технологияның дамуымен және алаяқтықтың жаңа әдістерінің пайда болуымен сот-медициналық сипаттама үнемі жетілдіріліп отыруы керек. Бұл криминалистердің білімі мен дағдыларын үнемі жаңартып отыруды, сондай-ақ ақпараттық қауіпсіздік саласындағы сарапшылармен ынтымақтастықты қажет етеді.

Қиындықтарға қарамастан, компьютерлік ақпарат саласындағы алаяқтықтың сот-медициналық сипаттамасы киберқылмыспен күресудің ажырамас бөлігі болып табылады. Ол қылмыстардың алдын алуда және жолын кесуде, Ақпараттық жүйелер мен деректердің қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады.

Жалпы, компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасы киберқылмыспен күресудің қажетті құралы болып табылады. Оның дамуы мен қолданылуы компьютерлік технологияларды қолданумен байланысты қауіп-қатерлерге тиімді қарсы тұруға және қоғамның мүдделері мен жеке қауіпсіздігін қорғауға мүмкіндік береді.

Өзін-өзі бақылау мәселелері:

1. Компьютерлік ақпарат алаяқтығының сот-медициналық сипаттамасы дегеніміз не?
2. Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасын жүргізу кезінде қандай негізгі әдістер мен құралдар қолданылады?
3. Компьютерлік ақпарат саласындағы алаяқтықты тергеу кезіндегі тергеу әрекеттерінің ерекшеліктері қандай?
4. Компьютерлік ақпараттық алаяқтықты тергеу кезінде қандай дәлелдер қолданылуы мүмкін?
5. Компьютерлік ақпараттық алаяқтықты тергеу кезінде қандай техникалық зерттеулер жүргізілуі мүмкін?
6. Компьютерлік ақпарат саласындағы алаяқтықты тергеу кезінде сот-сараптамалық бағалаудың қандай ерекшеліктері бар?
7. Компьютерлік ақпарат саласындағы алаяқтықтың алдын алу шараларын қолдануға болады?
8. Компьютерлік ақпарат алаяқтық істері бойынша сот практикасының қандай ерекшеліктері бар?
9. Компьютерлік ақпарат саласындағы алаяқтықты тергеуді қандай заңнамалық актілер реттейді?
10. Компьютерлік ақпарат саласындағы алаяқтықтың криминалистикалық сипаттамасын дамытудың болашағы қандай?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Компьютерлік ақпаратқа заңсыз қол жеткізу үшін қандай термин қолданылады?

a) фишинг;
b) хакерлік;
c) вирус;
d) спам;
e) қарақшылық.

2. Алаяқтықтың қандай түрі пайдаланушыларды алдау және олардың жеке деректерін алу үшін электрондық поштаны пайдалануды қамтиды?

a) фишинг.
b) спам;
c) вирус;
d) хакерлік;
e) қарақшылық.

3. Шабуылдаушыға компьютерге кіруге және басқаруға мүмкіндік беретін бағдарламалық кодты белгілеу үшін қандай термин қолданылады?

a) вирус.
b) фишинг;
c) хакерлік;
d) спам;
e) қарақшылық.

4. Пайдаланушылардың жеке деректерін алу үшін жалған веб-сайттар құруды қамтитын алаяқтықтың қандай түрі?

a) фишинг;
b) хакерлік;
c) вирус;
d) спам;
e) қарақшылық.

5. Бағдарламалық жасақтаманы заңсыз көшіру және тарату үшін қандай термин қолданылады?

a) қарақшылық.
b) фишинг;
c) хакерлік;
d) вирус;
e) спам.

6. Алаяқтықтың қандай түрі электрондық поштаға немесе мобильді құрылғыларға қажетсіз хабарламаларды жіберуді қамтиды?

a) спам;
b) фишинг;
c) взлом;
d) вирус;
e) пиратство.

7. Компьютерді зақымдауы немесе пайдаланушының жеке деректерін ұрлауы мүмкін бағдарламалық кодты белгілеу үшін қандай термин қолданылады?

a) вирус;

b) фишинг;

c) хакерлік;

d) спам;

e) қарақшылық.

8. Алаяқтықтың қандай түрі пайдаланушыларды алдау үшін жалған ақпаратты немесе көріністі пайдалануды қамтиды?

a) фишинг;

b) спам;

c) хакерлік;

d) вирус;

e) қарақшылық.

9. Ақпаратты алу, өзгерту немесе жою мақсатында компьютерлік жүйелерге заңсыз қол жеткізу үшін қандай термин қолданылады?

a) хакерлік;

b) фишинг;

c) вирус;

d) спам;

e) қарақшылық.

10. Алаяқтықтың қандай түрі компьютерлік ақпаратқа заңсыз қол жеткізу үшін басқа біреудің ақпаратын немесе тіркелгі деректерін пайдалануды қамтиды?

a) фишинг;

b) хакерлік;

c) вирус;

d) спам;

e) сәйкестендіру алаяқтық.

§4. Компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша алғашқы тергеу әрекеттерін жүргізу ерекшеліктері

Ғылым мен техниканың қазіргі даму кезеңінде қылмысты цифрландыру криминалистикалық ғылымның алдында тұрған негізгі сын-қатерлердің бірі болып табылады. Бұл жағдайға ғылыми әдебиеттерде де назар аударылды.

Қазіргі уақытта Қазақстан Республикасында бұрын отандық заң ғылымы мен практикасына белгісіз және компьютерлік техника құралдары мен ақпараттық-өңдеу технологияларын пайдалануға байланысты қылмыстық қол сұғушылықтардың жаңа түрінің пайда болуы мен даму фактілері - компьютерлік қылмыстар нарықта жетілуіне қарай совершенам және салыстырмалы түрде арзан дербес компьютерлердің пайда болуына байланысты ерекше дабыл қағуда шағын және үлкен компьютерлер арасындағы шекаралар бұлыңғыр бола бастады, адамдардың шексіз тобына қуатты ақпараттық ағындарға қосылу мүмкіндігі пайда болды. әрине, сонымен бірге ақпаратқа қол жетімділіктің бақылануы, оның сақталуы мен қатерсіздігі туралы мәселе туындады. Бұл ретте ұйымдастыру шаралары, сондай-ақ бағдарламалық және техникалық қорғау құралдары кейде тиімсіз болып шығады. Әсіресе, рұқсат етілмеген араласу мәселесі жоғары дамыған технологиялар мен ақпараттық желілері бар елдерде өзін танытты. Қосымша қауіпсіздік шараларына жүгінуге мәжбүр болған олар құқықтық қорғау құралдарын белсенді қолдана бастады.

Қазақстанда компьютерлік қылмыс жалпы қылмыстық жағдайға және қылмыстық заңнаманың жетілмегендігіне, сондай-ақ арнайы білімді талап ететін компьютерлік саланың өзіндік ерекшелігіне байланысты жасырын сипатқа ие болуы мүмкін. Сондай-ақ, есептеу техникасымен байланысты қылмыстардың белгілі бір ерекшелігін ескеру қажет. Есептеу техникасының өзі қылмыстық қол сұғушылықтың нысаны болуы мүмкін (мүлікке қарсы қылмыстар - ұрлау, жою, зақымдау), сондай-ақ қылмыс жасау құралы, яғни ұрлау, салықтарды жасыру, ақпаратты бұрмалау және т. б. (бұл мағынада компьютерді қару немесе көлік құралы сияқты қылмыс құралдарымен қатар қарастыруға болады).

Компьютерлік қылмыстардың парадоксалдылығы-қылмыстың басқа түрін табу қиын, оны жасағаннан кейін оның құрбаны қылмыскерді ұстауға аса қызығушылық танытпайды, ал қылмыскердің өзі ұсталып, өзінің қызметін компьютерлік хакерлік салада жарнамалайды, құқық қорғау органдарының өкілдерінен аз жасырады. Психологиялық тұрғыдан бұл парадокс түсінікті. Біріншіден, компьютерлік қылмыстың құрбаны оны ашуға кететін шығындар (мысалы, банк өзінің беделін жоғалту нәтижесінде болған шығындарды қоса алғанда) келтірілген залалдан едәуір асып түсетініне сенімді. Екіншіден, қылмыскер, тіпті бас бостандығынан айырудың максималды мерзімін (үш жылға дейін, егер ауыр зардаптар болмаса, бірақ көбінесе шартты мерзім болса), іскерлік және қылмыстық ортада кеңінен танымал болады, бұл болашақта оған алған білімі мен дағдыларын тиімді пайдалануға мүмкіндік береді.

Тергеу және сот практикасы компьютерлік ақпарат саласындағы алаяқтықты сотқа дейінгі тергеп-тексерудің бастапқы кезеңінде жүргізілетін негізгі тергеу әрекеттері мен жедел-іздестіру іс-шараларының шеңберін алдын ала анықтады: жәбірленушілерді (жәбірленуші тарап өкілдерін) анықтау және одан әрі жауап алу; жәбірленуші компьютерді не басқа да портативті құрылғыларды пайдаланған үй-жайда (тұрғын үйде) оқиға орнын қарап-тексеру жүргізу; жедел -тергеу әрекеттерімен қатар іздестіру іс-шараларын жүргізу; техникалық байланыс құралдарын алу; ықтимал куәгерлер мен куәгерлерден жауап алу; күдікті адамдардан жауап алу; барлық қажетті сараптамаларды тағайындау және жүргізу.

Жәбірленушілерден жауап алу (жәбірленуші тарап өкілдерінен). Тәжірибе көрсеткендей, сотқа дейінгі тергеудің бастапқы кезеңінде жәбірленушілер, әдетте, жанжалсыз жағдайда жауап алынады, өйткені олар күдікті қылмыскерді анықтауға және ұстауға мүдделі адамдар болып табылады. Куәгерлер тергеуге қолайлы және керісінше әртүрлі позицияларды қабылдай алады, бұл куәгердің кімнің жағында екеніне және оның істің нәтижесіне деген қызығушылығына байланысты.

Белсенді адал жәбірленушілер, әдетте, оң жағынан сипатталады, тергеумен ынтымақтасады, қажетті іс-шараларға өз еркімен қатысады, тергеуге көмектесуге тырысады, оның нәтижелеріне қызығушылық танытады. Белсенді емес адал жәбірленушілер белсенділерден ерекшеленеді, олар пассивті әрекет етеді, сотқа дейінгі тергеу барысына қызығушылық танытпайды, тергеушімен кездесуден аулақ болуға тырысады. Осы және басқа жағдайларда жауап алу кезінде жасалған қылмыстық құқық бұзушылықтың ұмытылған бөлшектері мен мән-жайларын еске түсіруге бағытталған тактикалық әдістер қолданылады (алдыңғы оқиғаларды нақтылау және еске түсіру, құжаттар мен заттай дәлелдемелерді ұсыну, жауап алу кезінде ассоциативті байланыстарды белсенді пайдалану),

Тұрақсыз жәбірленушілер өз айғақтарын өзгертуге, бұрын берілген айғақтардан бас тартуға бейім, қылмыскермен (достық, тұрмыстық немесе отбасылық) байланысы болуы мүмкін. Жәбірленушінің бұл түрі сыртқы қысымға оңай ұшырауы мүмкін. Оларға көбінесе кәмелетке толмағандар жатады.

Жосықсыз жәбірленушілер, әдетте, шынайы куәлік бермейді, жанжалға барады, агрессивті мінез-құлықпен сипатталады.

Тұрақсыз және жосықсыз жәбірленушілерден жауап алуға дайындық кезінде күдіктілерден жауап алуға, жанжал жағдайында дайындық бойынша тактикалық ұсыныстарды басшылыққа алу және өтірікті жеңуге, кінәні әшкерелеуге бағытталған тактикалық әдістерді қолдану (дәлелдемелер ұсыну, эмоционалдық шиеленісті пайдалану, тергеуді қызықтыратын мән-жайларды баяндаудың әртүрлі тәртібімен еркін баяндау әдісі, нақтылайтын, нақтылайтын мәселелерді белсенді қолдану, жауап алынатын адамның жеке басының жағымды қасиеттерін ынталандыру, ішкі қайшылықтарды қолдану және т.б.).

Сонымен, жәбірленушінің түрін және жауап алу кезінде тиісті тактиканы таңдауды ескере отырып, компьютерлік ақпарат саласындағы

алаяқтықты тергеу кезінде жәбірленушілерден келесі ақпаратты анықтау қажет:

– қандай компьютерлік-техникалық құрал қылмыстық шабуылға ұшырады;

– дербес компьютерде немесе басқа техникалық құрылғыда жұмыс істеу дағдысының деңгейі және смарт құрылғыларды пайдалану деңгейі;

– компьютерде немесе техникалық жағынан күрделі құрылғыда орнатылған бағдарламалық құралдар туралы білімнің болуы;

– интернет желісін ұсыну бойынша қызметтер көрсетуге қандай операторменен (провайдермен) шарт жасалды және қандай шарттарда;

– жәбірленуші өзіне қатысты алаяқтық әрекеттер жасағаны туралы қалай білді;

– қандай жағдайда қылмыстық оқиға қылмыскерлерді әшкерелейтін және қылмыстық оқиға тізбегін құра алатын барлық деректерді көрсете отырып өтті;

– қылмыскерлермен визуалды байланыс болды ма, егер солай болса, қандай жағдайда кездесуге кім куә бола алады; сыртқы келбеттің толық сипаттамасы.

Компьютерлік ақпарат саласында алаяқтық жасалған заңды тұлғаларға келетін болсақ, сұрақтар тізбесі сотқа дейінгі тергеу жүріп жатқан нақты тергеу жағдайына байланысты кеңейтіледі.

Компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша жәбірленуші ретінде заңды тұлға болған жағдайда да анықтау қажет мәселелердің шамамен тізімін береміз. Бұл жағдайда ұйымның қызметкерлері (мысалы, жүйелік әкімшілер, ақпараттық қауіпсіздік қызметкерлері, бухгалтерлер, менеджерлер, ақпараттық-техникалық қызмет көрсету қызметкерлері және т. б.) келесі мәселелер бойынша куәгер ретінде жауап алады:

– заңды тұлғаның орналасқан жері және қызмет түрі;

– ұйымның қызметін реттейтін құжаттардың тізбесі, лицензиялардың болуы;

– жұмыс режимі, ішкі тәртіп, өткізу режимінің болуы;

– жұмыс көлемі, жасалған шарттардың сипаты мен болуы, олардың түрлері, мазмұны мен шарттары, контрагенттердің атауы мен орналасқан жері;

– компьютерде сақталған ақпараттың мәні мен көлемі, оған қол жетімділіктің, кодтар мен парольдердің болуы;

– алаяқтық әрекеттермен келтірілген залалдың бар-жоғын, сипаты мен көлемін, оның келтірілу шарттарын құжаттамалық растау;

– қызметкерлердің қайсысы күдікті қылмыскерлермен байланысқа түсті, мұндай байланыстың сипаты;

– жауап алынғандардың әрбір санатының жасалған қылмыс тетігі, қылмыстық нәтиженің туындау себептері мен шарттары туралы пікірі.

Жәбірленуші компьютерді немесе басқа да портативті құрылғыларды пайдаланған үй-жайда (тұрғын үйде) оқиға орнын тексеру.

Оқиға орнын тексеру маңызды тергеу әрекеттерінің бірі болып табылады: қылмыстық іс бойынша одан әрі тергеу көбінесе оның сапалы, жан-жақты және кәсіби жүргізілуіне байланысты.

Компьютерлік ақпарат саласындағы қылмыстарды тергеу кезінде оқиға орны жасалған компьютерлік қылмыстың іздері табылған жер учаскесі немесе үй-жай болып табылады; барлық желілік орта, оның ішінде ғаламдық желілерге кіру және шығу нүктелері. Компьютерлік ақпаратты пайдалана отырып, алаяқтықты тергеу кезінде оқиға орнын тексерудің ерекшелігі, мысалы, тұрғын үйді ұрлаудан айырмашылығы, үй-жай ғана емес, сонымен қатар құрылғы да тексеріледі.

Осыған байланысты, стационарлық компьютер, ноутбук және басқа да техника табылған оқиға орнында жұмыс істеген кезде жедел-тергеу тобы мен өзге де қатысушылар бірқатар ұсыныстар мен ережелерді сақтауы қажет:

– оқиға орнында табылған компьютерлермен және өзге де техникалық құрылғылармен алдын ала белгісіз салдарлар туындауы мүмкін кез келген әрекеттерді жасауға үзілді-кесілді тыйым салынады;

– тергеу барысында пайдалануды шектеу керек немесе компьютерлік ақпаратты зақымдауы мүмкін техникалық құралдарды пайдаланудан бас тарту керек, мысалы, жұмысы электромагниттік сәулеленудің, магнит өрісінің, рентген сәулесінің және т. б. әсеріне негізделген әдістер.;

– маман тек техникалық құралдармен ғана емес, сонымен қатар ұнтақтар мен химиялық реактивтермен де жұмыс істегенде абай болу керек;

– компьютерлік жүйелер мен компьютерлік ақпараттың сипаттамалары мен жұмыс істеу процесін тіркеу кезінде арнайы терминологияны қолдану;

– машиналық тасығышта сақталатын компьютерлік ақпаратты қарау кезінде қарап шығу мен сипаттаудың жалпы ережелерін: жалпыдан жекеге, каталогтардан жеке файлдарға, файл қасиеттерінің жалпы сипаттамаларынан оның нақты мазмұнына дейін ұстану;

– сот-медициналық маңызы бар немесе болуы мүмкін компьютерлік техниканың құралдары ғана алынуы керек-ақпарат.

Сонымен қатар, оқиға болған жерді сапалы тексеру мақсатында жоғарыда көрсетілген ережелерден басқа, оқиға болған жерді тексеру өндірісінің ұйымдастырушылық-тактикалық негіздерін сақтау қажет.

Оқиға орнын тексеру туралы шешім қабылданғаннан кейін келесі әрекеттерді орындау қажет:

– оқиға орнын уақтылы келгенге дейін қорғауды қамтамасыз ету бойынша шаралар қабылдау (мысалы, осы санаттағы қылмыстарды тергеудегі өте жағымсыз сәт зардап шеккен тараптың компьютерлік жүйелерді жедел-тергеу тобы келгенге дейін апатты қалпына келтіру үшін ақпараттық технологиялар саласындағы мамандарды шақыруы болады), өйткені абайсызда немесе білместен дәлелді маңызы бар маңызды деректер жойылуы мүмкін;

– келген кезде оқиға туралы қажетті ақпаратты бере алатын адамдардың болуын қамтамасыз етіңіз, мысалы, желі әкімшісі, кәсіпорынның қауіпсіздік қызметкері, талдаушылар, ұйымның бухгалтерлік қызметкерлері, егер олар белгілі болса, куәгерлер және т. б.;

– ЖТТ нұсқамасында мамандардың болуын қамтамасыз ету. Бұл ретте оқиға орнын тексеруге қатысатын адамдарға бірлескен нұсқама беруге ерекше назар аударылсын және мамандарға бағдарламалық-техникалық құралдардың дайындығын тексеруді тапсырылсын;

– мамандармен өзі кеңесіп, мамандарды оқиға болған жерді тексеруге қатысатын барлық адамдарға оқиға болған жерді қарау тәртібі туралы нұсқау беруге міндеттеу;

– куәгерлердің қатысуын қамтамасыз ету. Тексеруге байланысты тергеу әрекеттерінде компьютерлік ақпарат саласындағы қылмыстарды тергеу кезінде. бағдарламалық жабдықтармен, компьютерлік жабдықтармен өзге де манипуляциялармен компьютерлік жабдықтарды, машиналық тасымалдағыштарды, бағдарламалық жабдықтарды алып қою арқылы тергеу әрекетіне әсер ететін салада ең аз білімге ие болу үшін куәгерлерге қосымша талаптар қою қажет.

Оқиға орнына келген кезде тергеуші келесі әрекеттерді орындауы керек:

– оқиға орнынан барлық бөгде адамдарды алып тастау және кейіннен тексеру жүргізу кезінде мұндай адамдардың пайда болуының алдын алу;

– ЖТТ келгенге дейін оқиға орнында болған адамдарды анықтау, ал олардың жағдайға енгізген өзгерістерін анықтау. Мұндай ақпаратты оқиға орнына полиция шақырылғаннан кейін жәбірленушімен бірге болған куәгерлер мен адамдар, сондай-ақ жәбірленушінің өзі бере алады;

– жәбірленуші ұйымның немесе жәбірленушінің қызметкерлерімен (егер бар болса) әңгімелесу арқылы қарау кезінде ескерілуі және ескерілуі тиіс ұсынылған мәліметтерді жинау;

– пайдаланылатын телекоммуникациялық жабдықтың атауын, оның сипаттамаларын, пайдаланылатын электрондық пошта құралдарының өзгеруін белгілеу. Жәбірленуші тергеушіні қызықтыратын жабдыққа құжаттама бере алады. Сонымен қатар, жабдықты визуалды тексеру шеңберінде техниканы сәйкестендіруге мүмкіндік беретін жапсырмаларды, техникалық сипаттамалары, атауы, моделі және сериялық нөмірі бар жапсырмаларды табу сирек емес;

– үй-жайда орналасқан компьютерлердің жергілікті есептеу желісіне жалғанғанын анықтау және компьютердің қаралатын үй-жайдан тыс жабдықпен немесе есептеу техникасымен байланысы бар-жоғын, компьютер телефон желісіне жалғанғанын анықтау;

– бағдарламалардың компьютерде жұмыс істейтінін және қайсысы екенін анықтаңыз.

Техникалық құрылғылардағы қылмыстық әрекеттің криминалистикалық маңызды іздерін дұрыс бекіту тергеушіден осындай ақпаратты тасымалдаушылармен іздеу, алу және одан әрі жұмыс істеу бойынша терең білім мен дағдыларды талап етеді.

Тексерудің жұмыс кезеңі саусақ іздерінің, аяқ киімнің іздерінің, ықтимал бұзу құралдарының, қолжазба жазбаларының және т. б. дәстүрлі дәлелдерін жинаудан басталады.

Оқиға болған жерді қарау кезінде ең маңызды объект (желілік сервер объектілері, серверлер) орналасқан шеткі аймақтан орталыққа тексеру тәртібі түсінілетін тексерудің концентрлік әдісін қолдану қажет.

Компьютерлік жүйелерді, олардың желілерін және перифериялық жабдықтарды егжей-тегжейлі қарап-тексеруді жүргізу не аталған құрылғыларды оқиға орнында тікелей былайша зерттеуге болады. Маман куәгерлердің қатысуымен жүйені антивирустық тестілеу үшін ноутбукты желіге немесе машиналық тасымалдағышқа қосады.

Аталған қосылымды жүзеге асыра отырып, маман зиянды (немесе вируспен зақымдалған) бағдарламаларды анықтау үшін дербес компьютерлер мен желілерді тестілеуді жүргізеді. Оларды анықтау үшін тиісті антивирустық және вирусты анықтайтын бағдарламалық жасақтама қолданылады.

Оқиға орнын тексеру кезінде компьютерлік ақпаратпен жұмыс істеудің негізгі принциптерін бөліп көрсету керек:

– қылмыс орнында табылған іздердің сақталуы қамтамасыз етіледі (бөгде адамдарды алып тастау, компьютерлік жабдықтың үздіксіз жұмысын бақылау);

– тиісті маманның қатысуынсыз қосылған компьютерлік құрылғыда файлдарды іздеуге және олармен жұмыс істеуге жол берілмейді;

– компьютерлік жабдықты алып қою қажет болған жағдайда жұмысты дұрыс аяқтау жүзеге асырылады, маршрутизатор немесе модем ажыратылады;

– егер зиянды бағдарламалық қамтамасыз етумен қылмыстың электрондық-цифрлық іздерін рұқсатсыз жою қаупі бар болса, компьютерді электрмен жабдықтау желісінен шұғыл ажырату шаралары қабылданады;

– аккумуляторлық батареядан жұмыс істейтін құрылғымен, мысалы, ноутбукпен жұмыс істеген жағдайда, оны ажырату шаралары қабылданады;

– алынған жабдықты орау мен тасымалдауды мұқият бақылау жүзеге асырылады;

– компьютерді тексеру өндірісі оның сыртқы түрін, монитор экранын және оған қосылған құрылғыларды фотофиксациялаумен қатар жүреді;

– фотофиксация және компьютерлік құрылғыға жақын жағдайдың толық сипаттамасы жасалады;

– өшірілген компьютерді жұмыс күйіне келтіруге тыйым салынады;

– алынатын әрбір объект (кабель, flesh-диск және т. б.) жеке таңбалауға жатады;

– қаптама тәркіленген заттардың бүліну мүмкіндігін болдырмауы тиіс;

– магниттермен және басқа да ықтимал қауіпті құрылғылармен жанасуды болдырмайтын жағдайларда тасымалдау және одан әрі сақтау қамтамасыз етіледі;

– алынатын жабдықтың кез келген құжаттамасы, мысалы, логиндері/парольдері бар жазбалар және өзге де криминалистикалық маңызы бар ақпарат міндетті түрде алынуға тиіс;

– ұялы телефонмен немесе планшетпен жұмыс істегенде экранды өшіруге немесе құлыптауға болмайды. Қайта қосу құпия сөзді сұрауға әкелуі

мүмкін, бұл деректермен жұмыс істеуді қиындатады. Бұл жағдайда батареяны оңтайлы күйде зарядтау қажет;

– егер қандай да бір себептермен құрылғы батареяның қосымша зарядынсыз ұзақ уақыт бойы батареяның қызмет ету мерзімін сақтай алмаса және зарядтағыш болмаса, онда ол зарядсызданғанға дейін маманның қатысуымен осы құрылғымен жұмысты дереу ұйымдастыру қажет;

– оқиға орнын тексерудің тиісті хаттамасында жүргізілген барлық іс-әрекеттерді егжей-тегжейлі құжаттау жүзеге асырылады.

Кейінгі салыстырмалы зерттеу (файлдар) үшін үлгілерді алу, осы және кейінгі әрекеттерді сәтті жүргізу және жүйеге зиян келтірмеу үшін желілік орта файлдарының сыртқы ақпарат тасымалдағыштарына немесе маманның ноутбугына толық резервтік көшірмесін жасау қажет.

Деректердің толық көшірмесі одан әрі заттай дәлел ретінде егжей-тегжейлі зерттеу үшін қылмыстық іске қосу үшін алынады. Тергеуші зертханалық жағдайда кейінгі сараптамалық зерттеу үшін алдыңғы көшірмелерін (егер бар болса) талап етеді. Содан кейін антивирустық тестілеу жүргізіледі. Айта кету керек, маман тексеру кезінде және жұқтырған файлдарды анықтаған кезде оларды ешқандай жағдайда "емдеуге" немесе қалпына келтіруге болмайды, анықталған зиянды бағдарламалар тек жазылады. Содан кейін зиянды бағдарламалар мен вирус жұққан файлдар электронды тасымалдаушымен бірге осы саладағы сарапшыға әрі қарай зерттеуге беріледі. Сарапшы ақпаратты жан-жақты зерттегеннен кейін тергеушіге тергеудің одан әрі барысын анықтауға мүмкіндік беретін белгілі бір қорытынды береді.

Маңызды компьютерлік ақпаратты тергеу іс-әрекетін жүргізу кезінде тергеуші ғана емес, сонымен қатар машиналық тасымалдаушыларға, олардың жүйелеріне, олардың желілері мен машиналық тасымалдаушыларына сараптамалық зерттеу жүргізу кезінде сарапшы да анықтай алады.

Оқиға орнында Microsoft Windows негізіндегі жабдықпен жұмыс істеген кезде пайдаланушының Интернет желісіндегі жұмысы туралы криминалистикалық маңызды ақпаратта тізілім және жүйелік оқиғалар файлдары, белсенді қосылымдардың тізімі мен параметрлері бар файлдар, модемдердің жұмыс хаттамалары, Index файлдары болуы мүмкін екенін ескеріңіз.пайдаланушы кіретін интернет-ресурстар туралы мәліметтерді қамтитын dat: каталогтарда орналасқан файлдар: documents and Settings username cookies); пайдаланушының Интернет желісінде жұмыс істеуіне арналған бағдарламалардың параметрлері мен жұмыс хаттамалары бар файлдар.

Жеке айта кетейік, оқиға болған жерді тексеру шеңберінде техниканы сапалы тексеру әрдайым мүмкін емес, мысалы, мұқият және егжей-тегжейлі зерттеуді қажет ететін техникалық күрделі жабдықтар табылған жағдайда, тиісті білім саласында маман болмаған кезде және басқа объективті себептер мен жағдайларға байланысты. Мұндай жағдайда криминалистикалық техника қағидалары бойынша (сондай-ақ жоғарыда көрсетілген ұсынымдарға сәйкес) жабдықты алып қою және маманды шақыра отырып, тергеушінің

кабинетінде затты қарап-тексеруді жүргізу және (немесе) компьютерлік сараптама тағайындау қажет.

Затты қарау кезінде (мысалы, ноутбук немесе ұялы телефон) сыртқы белгілерді, функционалды күйді және мүмкін болса, құрылғының ақпараттық мазмұнын мұқият және егжей-тегжейлі сипаттап, жазып алу қажет.

Маманмен бірге компьютерлік техниканың саны мен түрін, бағдарламалық жасақтаманың түрін және құрылғылардың өзара әрекеттесу сипатын, рұқсатсыз кіруден қорғайтын аппараттық және бағдарламалық құралдардың болуын анықтап, іс бойынша дәлелдемелерді жою мақсатында қылмыскерлер қабылдаған қауіпсіздік шараларын анықтаған жөн.

Компьютерді тексеру кезінде сізге:

– тексеру хаттамасында және оған қоса берілген схемада желінің барлық компьютерлерінің, олардың перифериялық құрылғыларының орналасуын, сервердің, кабельдерді, телекоммуникация құрылғыларын (модемдерді, факс-модемдерді) төсеу орнының болуын, олардың орналасуын және телефон байланысы арналарына қосылуын орнату және бекіту;

– хаттамада атауын (әдетте алдыңғы жағында көрсетіледі), сериялық нөмірін, жинақтамасын (диск жетектерінің, желілік карталардың, қосқыштардың және басқалардың болуы және типі), жергілікті есептеу желісімен және телекоммуникация желілерімен байланысының болуын және құрылғылардың жай-күйін (ашу іздері бар және оларсыз)көрсету;

– жабдықтың сыртқы күйін сипаттаңыз, сонымен бірге қосылу орындарына назар аударыңыз (мысалы, принтердің байланыс порттары мен компьютердің перифериялық құрылғыларының жүйелік блогы, корпустың қақпақтарын бекіту бұрандалары, жүйелік блоктың астындағы беттер, монитор және басқа құрылғылар. Әдетте бұл жерлерде шаң жиналады, яғни іздер қалуы мүмкін, олардың болуы немесе болмауы хаттамада көрсетілуі керек. Сондай-ақ, компьютер құрылғыларының корпустарына салынған барлық белгілердің, пломбалардың, әртүрлі белгілер мен жапсырмалардың (түгендеу нөмірлері, жадқа арналған жазбалар, сатушы фирмалардың бақылау маркерлері және басқалары) болуы мен жай-күйін, ластанудың, механикалық зақымданудың болуын және олардың локализациясын атап өту қажет;

– осы құрылғылардың өзара қосылу тәртібін дәл сипаттаңыз, (қажет болған жағдайда) қосылатын кабельдер мен оларды қосу порттарын белгілеңіз, содан кейін компьютер құрылғыларын ажыратыңыз;

– қандай файлдар мен бағдарламалардың көшірілгенін және қайдан, көшірудің басталу және аяқталу уақытын, көшірмелер санын жазып алыңыз. Ақпарат көшірілген физикалық тасымалдағыштар, олардың қаптамасы, компьютерлік ақпаратты басып шығару үшін пайдаланылған принтердің техникалық сипаттамалары көрсетіледі.

Портативті компьютерлік құрылғыларды, планшеттерді, ұялы телефондарды және т. б. қарау кезектілігін үш кезеңге бөлуге болады: сыртқы тексеру, оның шеңберінде тергеуші жалпы белгілерді (құрылғының түрі мен күйін) зерттейді және тіркейді; конструктивті, онда аппараттың дизайны тексеріледі(корпус, аккумулятор, флэш-карта, SIM-карта); тексеру

құрылғының жадында қамтылған мәліметтер флэш-тасымалдағышта немесе SIM-картада зерттелетін және жазылатын ақпараттық орта. Затты тексеру хаттамасында табылған құрылғы туралы мәліметтер ғана емес (IMEl, SIM картасының нөмірі, маркасы, моделі, формасы, дизайн ерекшеліктері, сериялық нөмірі, IP нөмірі және т. б.), сонымен қатар құрылғымен жүргізілетін барлық манипуляциялар (жад карталарының мазмұнын, телефон кітапшасын, ашылатын файлдарды қосу, қарау және т. б.) ашылатын файлдардың толық сипаттамасы және атауы бар.

Кейбір тактикалық және криминалистикалық ұсыныстар ретінде, тергеушінің қарамағында алғашқы тергеу әрекеттерін жүргізу кезінде бірден бірнеше құрылғылар (планшеттер, ұялы телефондар, Ноутбуктер) алынған жағдайлар жиі кездесетінін қосу керек. Бұл жағдайда тексеруден бұрын оларды өшіру, батареяны, SIM картасын алу мүмкін емес, өйткені кейіннен қосу кезінде құлыптау кодтары, қауіпсіздік парольдері, PIN кодтары қажет болуы мүмкін. Бұл жағдайда сындарлы тексеру оның ақпараттық ортасын зерттегеннен кейін ғана жүргізілуі керек екенін атап өтейік.

Егер нақты пайдаланушылардың телефон аппараттарын қосудың кіріс және шығыс сигналдары туралы деректер қылмыстық іс үшін маңызды болса, онда ұялы телефонның заңды иесінің келісімі болмаған жағдайда тергеуші мұндай ақпаратты тек сот шешімі бойынша тексере алатынына назар аудару өте маңызды болып көрінеді.

Сондай-ақ, анықталған байланыс құрылғысының ақпараттық ортасын тексеруге егжей-тегжейлі тоқталу қажет, өйткені дәл осы тексеру кезеңінде криминалистикалық маңызды ақпаратты тіркеуге болады, ақпараттық ортаны тексеру хаттамада құрылғының құлпын ашу процедурасын көрсетуден, графикалық және мәтіндік элементтерді тізімдеуден басталады. ол құлыпты ашқаннан кейін оның экранында пайда болды. Ұялы телефонды тексерген жағдайда ұялы телефонның IMEI-нөмірін *#06# пернелер тіркесімін басу арқылы (он бес таңбалы нөмір телефон экранында көрсетілуі тиіс) немесе ұялы телефон параметрлерінде тексеру жүзеге асырылады.

Егер құрылғы парольмен қорғалмаған жағдайда, тексеру хаттамасында ақпараттық мазмұн – контактілер, хабарламалар тізімі, суреттердің, фотосуреттердің, бейнероликтердің болуы, жұмыс үстелінің қалталары мен файлдарының тізімі, орнатылған бағдарламалар және т. б. ретімен көрсетіледі.

Ақпараттық ортаны тексеру барысында құрылғының экранын қылмыстық іс үшін маңызы бар ақпаратпен кезең-кезеңмен егжей-тегжейлі суретке түсіру жүргізіледі. Ақпараттық ортадағы ақпараттың үлкен көлемін визуалды түрде түсіру үшін бейнетүсірілім қолданылуы керек. Бұл ретте тергеуші жабдықпен айла-шарғы жасау арқылы қандай да бір ақпаратты алуға бағытталған барлық іс-әрекеттерге міндетті түрде түсініктеме береді.

Электрондық-цифрлық іздерді неғұрлым сапалы және жылдам алуға осы қажеттіліктерге арналған арнайы заманауи аппараттық-бағдарламалық кешендер (мысалы, "мобильді криминалист, UFED, Belkasoft, secure View 3, MOBILedit, MicroSystemation, XRY және т.б.) ықпал ете алады. Аталған бағдарламалық қамтамасыз ету мен аппараттық-бағдарламалық кешендер

оқиға болған жерді тексеру, затты қарау және компьютерлік сараптама жүргізу шеңберінде пайдаланылуы мүмкін, оларды қолдану қылмыстық істі тергеу үшін маңызы бар техникалық құрылғылардан қажетті ақпаратқа мүмкіндік береді.

Тергеу тексеру барысында аппараттық-бағдарламалық кешендерді қолданудың орындылығы күмән тудырмайды. Компьютерлік ақпарат саласындағы алаяқтық бойынша оқиға орнын тексеру кезінде қылмыс жасалуы мүмкін барлық техникалық құрылғылар міндетті түрде алынып тасталуға тиіс.

Техникалық құрылғылардан криминалистикалық маңызды ақпаратты жоғалту мүмкіндігін азайту үшін қылмысты сапалы ашу және тергеу мақсатында аппараттық-бағдарламалық кешендерді оқиға болған жерді тексеру процесінде тікелей қолданған жөн. Кешіктіру электронды-цифрлық іздердің жоғалуына әкелуі мүмкін. Егер оқиға орнында аппараттық-бағдарламалық кешенді қолдану мүмкін болмаса (мысалы, ақпараттың үлкен көлемі. электрондық-цифрлық іздердің жоғалуын болдырмау үшін сақтық шараларын сақтай отырып, аталған техникалық құрылғыны маманның көмегімен алып қою ұсынылады. Кейіннен тергеу іс-әрекетін жүргізу шеңберінде маманды шақыра отырып және аппараттық-бағдарламалық кешендерді пайдалана отырып, затты тексеру техникалық құрылғыдан қажетті ақпаратты алып тастау керек. Бұл алгоритм өте тиімді, бірақ практикалық тергеу және сараптамалық қызметте белгілі бір қиындықтарға ие. Аппараттық-бағдарламалық кешені бар маманның оқиға орнын тексеруге және техникалық құрылғыларды пайдалана отырып жасалған әрбір қылмыс бойынша затты тексеруге қатысуының нақты мүмкіндігі әрдайым бола бермейді.

Осылайша, жоғарыда аталған аппараттық-бағдарламалық кешендер қылмыстық істі ашу және одан әрі тергеу үшін маңызы бар қажетті электрондық-цифрлық іздерді дәлірек анықтауға және алуға мүмкіндік береді. Оларды алып қою міндетті түрде маманның қатысуымен ұйымдастырылуы керек. Оларды қолданудың орындылығы күмән тудырмайды. Оқиға орнын тексеру процесінде аппараттық-бағдарламалық кешендерді пайдалану криминалистикалық маңызды ақпаратты тез және сапалы алуға және қылмыскерлерді «ыстық ізбен» іздестіру бойынша одан әрі іс-қимыл жасауға мүмкіндік береді.

Техникалық байланыс құралдарын және электрондық ақпарат тасығыштарды алу, кейіннен мамандардың қатысуымен заттарды қарау. Компьютерлік ақпарат саласындағы алаяқтықты тергеу үшін маңызы бар техниканың әртүрлі түрлерін тексеру ерекшеліктері.

Алып қоюға жататын техникалық байланыс құралдары мен электрондық ақпарат тасығыштарға кейіннен маманның қатысуымен тексеріле отырып, ақпаратты пайдалануға жарамды электрондық есептеу машиналарында тұрақты немесе уақытша сақтауға, сондай-ақ оны ақпараттық-телекоммуникациялық желілер немесе өңдеу және ақпараттық жүйелер арқылы беруге арналған конструктивті түрде арналған кез келген құрылғыларды жатқызуға болады. Мұндай құрылғыларға мыналар жатады:

ұялы және Интернет желілерінде (ұялы телефондар, смартфондар, смарт-сағаттар, ноутбуктер, планшеттер, дербес компьютерлер, нетбуктар, скринингтік құрылғылар) мүмкіндік беретін барлық құрылғылар, Құрылғылар, геопозитивтілік (GPS-навигация) туралы ақпарат алу модулін пайдалану жұмысы, мысалы, трекерлер, навигаторлар, және сондай-ақ, машиналық ақпарат құралдары: қатты және икемді магниттік дискілер флэш-карталар, SIM карталар және басқа құрылғылар, төлем пластикалық карталары және т.б.

Байланыс ақпаратының техникалық құралдары мен электрондық тасымалдаушыларын алудың кейбір ерекшеліктері бар. Сонымен, қазу кезінде келесі міндеттерді шешкен жөн:

– желілерді, қосылымдарды, соның ішінде WI-FI қосылымын ажырату;

– желілік құрылғылардың, пайдаланушыларды авторизациялау жүйелерінің, желілік трафиктің және т. б. жұмыс хаттамаларын алып қою.;

– флэш-карталар сияқты электронды ақпарат құралдарын қауіпсіз түрде шығарып алу арқылы дұрыс;

– құрылғыны электр қуатынан қауіпсіз ажыратыңыз;

– қуат көздері мен жұмыс істеу үшін қажетті кабельдері бар құрылғыны алыңыз;

– тергеу әрекетінің бейнежазбасы бар файлды (егер ол жүргізілген болса) конвертке орналастырылатын, мөрленетін және қатысушылардың қолымен бекітілетін қайта жазылмайтын электрондық тасығышқа көшіру;

– алынатын электрондық ақпарат тасымалдағыштарды буып-түю және мөрлеу.

Қаптама электрондық ақпарат тасығышпен жұмыс істеу мүмкіндігін, сондай-ақ ондағы ақпаратты физикалық зақымдау, бөлшектеу және бүлдіру мүмкіндігін болғызбауға тиіс. Осыған байланысты қаптама клапандары мөрлерге зақым келтірместен қаптаманы ашу мүмкін болмайтындай етіп мөрленеді. Электрондық тасымалдаушының өзін экрандайтын контейнерге («Фарадей қапшығы») араластырған жөн.

Алу хаттамасында ұялы телефондарды, смартфондарды, планшеттерді және басқа да мобильді құрылғыларды алу кезінде объект туралы Сәйкестендіру мәліметтерінен басқа, батарея алынып тасталғанын немесе алынбағанын, түймелерді, пернелерді басу, сенсормен өзара әрекеттесу болғанын көрсету қажет. Егер ноутбукты күту күйінде («ұйқы режимінде») алып тастау элементі болса, онда қаптама басқару пернелерімен, экранмен және қосқышпен кез-келген әрекеттің мүмкіндігін болдырмауы керек.

Қажет болған жағдайда жұмыс істеп тұрған құрылғының жад бейнесін алып тастау немесе алып қоюға жататын тасымалдағыштардан Электрондық ақпаратты көшіру.

Куәгерлерден жауап алу. Айта кету керек, мұндай қылмыстар көбінесе идеалды іздер болмаған кезде жүзеге асырылады: куәгерлердің айғақтары жанама болып табылады және жалпы мәліметтерге дейін азаяды. Әдетте, болған оқиға туралы белгілі бір білімі бар немесе жәбірленушінің бағдарламалық және (немесе) бағдарламалық-аппараттық құралдарға, компьютерге, оның ішінде ноутбуктерге, планшеттік компьютерлерге,

жәбірленушінің өзі жүзеге асырмаған смартфондарға бөгде әсерлері анықталған сәтте жәбірленушінің жанында болуы мүмкін деп аталатын адамдар куә болады. Жеке тұлғаларға қатысты алаяқтық жағдайында, әдетте, жәбірленушінің туыстары немесе жақындары, сондай-ақ жұмыс жөніндегі әріптестері куә болып табылады. Жоғарыда айтылғандай, егер жәбірленуші заңды тұлға болса, онда директор, жүйелік әкімші, техник, бухгалтер, менеджер және т.б. лауазымын атқаратын қызметкерлер куә бола алады. жанжалсыз жағдайда куәгерлерде олардың жасалған алаяқтық туралы хабардар болуына қатысты мәселелер анықталады және тергеу үшін пайдалы болуы мүмкін барлық мәліметтер белгіленеді. Жанжал жағдайында күдіктіден жауап алу кезінде қолданылатын тактикалық әдістердің көпшілігін қолдану қажет.

Күдіктілерден жауап алу. Компьютерлік ақпарат саласындағы алаяқтық бойынша қылмыстық істерді тергеу кезінде компьютерлік ақпарат саласындағы мамандармен тұрақты және үздіксіз өзара іс-қимыл орнатқан жөн, олар оқиға болған жерді тексеру сияқты көптеген тергеу әрекеттерін жүргізуге тартылуы мүмкін; күдіктілерді іздеу және іздеу, жауап алу, тергеу эксперименті және, әрине, сот сараптамаларын жүргізу.

Мамандар тарапынан консультацияларға қарамастан, сотқа дейінгі тергеп-тексеруді жүзеге асыратын тұлға алдын ала тергеуді жүзеге асыруға уәкілетті лауазымды тұлға болып табылатынын және сотқа дейінгі тергеп-тексерудің барысы мен нәтижесі оның біліміне, тәжірибесі мен кәсібилігіне байланысты екенін атап өткен жөн. Сондықтан аталған тергеу әрекеттері жүргізілгенге дейін мұқият алдын ала дайындық жүргізілуі керек. Күдіктілерден жауап алу сияқты тергеу әрекетін жүргізудің тактикалық ерекшеліктеріне толығырақ тоқталғым келеді, өйткені дәл осы тергеу әрекеті компьютерлік ақпарат саласындағы алаяқтықтарды тергеу кезінде 100% жағдайда жүзеге асырылады және алынған ақпарат көлемі оның сапасына байланысты. Бұдан басқа, егер сотқа дейінгі тергеп-тексеруді жүзеге асыратын адам бірінші жауап алу кезінде өзінің қабілетсіздігін көрсетсе, онда күдікті жанжалды позицияны ұстанады және шынайы айғақтар бермейді, бұл бүкіл тергеудің барысына теріс әсер етеді.

Интернет-алаяқтық саласындағы қылмыстық істер бойынша күдіктіден жауап алудың қылмыстың осы түрінің ерекшеліктеріне байланысты өзіндік ерекшеліктері бар. Мұндай жауап алу кезінде ескеру қажет кейбір негізгі аспектілер:

1. Техникалық білім: интернеттегі алаяқтықты тергеу құқық қорғау органдарынан интернет пен компьютерлік жүйелерді қолданумен байланысты техникалық аспектілерді жақсы түсінуді талап етеді. Жауап алушы желідегі алаяқтар қолданатын негізгі ұғымдар мен әдістермен таныс болуы керек.

2. Виртуалды анонимділік: интернеттегі алаяқтар әдетте өздерінің жеке басын жасырады және сәйкестендіруді айналып өту үшін анонимді есептік жазбаларды немесе бағдарламаларды пайдаланады. Осыған байланысты, жауап алушы күдіктінің қылмысқа қатысы бар екенін жоққа шығаруға немесе дұрыс емес ақпарат беруге дайын болуы керек.

3. Электрондық дәлелдемелер: интернеттегі алаяқтық туралы жауап алудың маңызды аспектісі-электронды дәлелдемелерді жинау және талдау. Жауап алушы дәлел ретінде пайдаланылуы мүмкін орналасқан жері, пайдаланылған бағдарламалық құралдар, шоттар және басқа деректер туралы ақпарат алуға бағытталған дұрыс сұрақтар қоя алуы керек.

4. Интернет технологиясын түсіну: жауап алушы алаяқтық схемаларда қолданылатын негізгі интернет технологиялары мен әдістерін жақсы түсінуі керек. Бұған фишинг әдістері, зиянды бағдарламалар бойынша Алаяқтық, Электрондық төлемдерді манипуляциялау және басқа да осыған ұқсас әдістер туралы білім кіруі мүмкін.

5. Психологиялық тәсіл: интернеттегі алаяқтық туралы күдіктіден жауап алу кезінде күдіктімен сенімді қарым-қатынас орнатуға және оның іс-әрекетінің себептерін анықтауға бағытталған психологиялық әдістерді қолдану маңызды. Күдіктінің манипуляция мен алдауға байланысты ерекше сипаттамалары болуы мүмкін, сондықтан мұндай жағдайларға дайын болу маңызды.

Жалпы, интернет-алаяқтық саласындағы қылмыстық істер бойынша күдіктіден жауап алу жауап алушыдан техникалық аспектілерді жақсы білуді, сондай-ақ қылмыстың осы түрінің ерекшеліктерін түсінуді талап етеді. Бұл дәлелдемелерді тиімді жинауға және істің барлық жағдайларын анықтауға көмектеседі.

Таңдау нақты тергеу жағдайына және тексеру мен тінту барысында табылған материалдық іздерге байланысты болатын сараптамаларды тағайындау және жүргізу.

Компьютерлік сараптама жүргізу тактикасы ерекше қызығушылық тудырады, өйткені бұл мәселе компьютерлік ақпарат саласындағы алаяқтықты тергеу кезінде әрқашан орталық болып табылады.

Компьютерлік сараптаманың негізгі міндеттері:

– қылмыстық құқық бұзушылықты тергеу үшін маңызы бар ақпаратты техникалық байланыс құралының жадында немесе электрондық жеткізгіште табу;

– құрылғымен немесе компьютерлік ақпаратпен жүргізілген манипуляцияларды көрсететін жағдайларды анықтау (құру өзгерту, жою, шифрлау және т.б.);

– сараптамаға ұсынылған құрылғы мен бағдарламалық жасақтаманың қасиеттері мен функционалдығын анықтау;

– жадтан жасырын, жойылған ақпаратты алу, деректерді қалпына келтіру.

Компьютерлік сараптаманы тағайындау кезінде ең көп тарағандары белгілі бір критерийлерге сәйкес келетін электрондық тасымалдағыштардағы компьютерлік ақпаратты зерттеу бойынша ақпараттық-іздестіру міндеттері болып табылады. Бұл ретте сарапшының алдына мынадай сұрақтар қойылады:

1. Зерттеуге ұсынылған машиналық тасымалдағыштарда мынадай түйінді сөздерді қамтитын ақпарат бар ма (тізбе беру)... (кілт сөздердің тізімін беріңіз)?

2. Зерттеуге ұсынылған машиналық тасымалдағыштарда (тізбе беру) туралы ақпарат бар ма (нақты не туралы екенін көрсету)?

Компьютерлік ақпараттан, бағдарламалық жасақтамадан, компьютерлерден және басқалардан басқа, қазіргі уақытта ұялы телефондар (смартфондар), бұлтты сақтау, ұялы телефондар мен басқа құрылғылардың суреттері компьютерлік сараптама объектілеріне айналуда. Мұның бәрі компьютерлік сараптаманың өзгеруін және жаңа бағдарламалық жасақтаманы пайдалану қажеттілігін және қолданыстағы бағдарламалық жасақтаманы үнемі жаңартып, жетілдіруді көрсетеді. Сонымен, компьютерлік сараптама жүргізу тәжірибесінде келесі бағдарламалар қолданылуы мүмкін:

– AXIOM;
– UFED;
– Belkasoft;
– Intella;
– Encase Forensic;
– X-Ways Forensic;
– Мобильді криминалист.

Компьютерлік сараптама жүргізу шеңберінде компьютерлік техника, ұялы желі мен Интернет желісінің жұмысы мен құрылысы, бағдарламалық инженерия, электроника және ақпараттық технологиялар саласында арнайы білім пайдаланылады. Сараптаманың бұл түрі ең күрделі және ерекше болып табылады, оның ішінде техника мен ақпараттық-телекоммуникациялық технологиялардың қарқынды дамуына байланысты.

Осыған байланысты сарапшының алдына қойылған мәселелер бірқатар талаптарға сай болуы керек. Мысалы, сұрақ қою кезінде тек арнайы тұжырымдамалық аппарат қолданылуы керек (ұялы телефон Абоненттік байланыс құрылғысы, логин пайдаланушы аты және т.б.). Егер объектіні анықтайтын арнайы термин болмаса, әзірлеуші берген және құжаттамада бекітілген атауды басшылыққа алу керек. Сұрақтар нақты, нақты тұжырымдалған болуы керек, түсініксіз түсіндіруді болдырмауы керек. Бұл ретте Қазақстан Республикасының ҚІЖК сарапшыға қылмыстық іс үшін маңызы бар ақпараттың неғұрлым кең көлемін ұсына отырып, сұраққа жауапты кеңейтуге мүмкіндік береді. Сұрақтар құқықтық сипатта болмауы керек, белгілі бір арнайы білімі бар адам ретінде сарапшының құзыретінен тыс болуы керек.

Зерттеу процесі сараптамаға ұсынылған объектінің қаптамасын тексеруден, оның тұтастығын, түсіндірме жазбалардың сәйкестігін және қолтаңбалардың болуын тексеруден басталады. Қаптаманы ашқаннан кейін объект суретке түсіріледі, өлшемдік сипаттамалары, түсі, конструктивтік ерекшеліктері, дараландырушы ерекшеліктері (оның ішінде зақымданулар, сандық және әріптік белгілер және т.б.), индикаторлар, қосқыштардың, құлыптау түймелерінің және басқа пернелердің орналасуы көрсетіледі.

Зерттеудің басында сараптамаға ұсынылған объект арнайы жабдыққа қосылады, оның көмегімен файлдық жүйенің құрылымы мен ақпараттың

орналасуы орнатылады. Осылайша, сарапшы файлдардың саны, атауы, өлшемдері және т. б. туралы ақпарат алады.

Содан кейін зерттелетін объектілерден (электрондық тасығыштардан) қосымша тасығыштарға ақпаратты секторлық көшіру жүргізіледі. Келесі сараптамалық іс-әрекеттер алынған көшірмелермен жүргізіледі. Бұл ретте, егер бұл сарапшының алдына қойылған мәселелер шеңберіне кірсе, жойылған ақпарат қалпына келтірілуі, деректердің шифрын ашу және парольдердің құлпын ашу, вирустық инфекциялардың бар-жоғын тексеру жүргізілуі мүмкін.

Зерттеудің негізгі сәттерінің бірі-зерттеу объектісінде бар бағдарламалық жасақтаманы қарау немесе эксперименттік іске қосу, оның функционалдық сипаттамаларын анықтау үшін эксперименттік іске қосу тек сарапшының аппараттық-бағдарламалық кешенінде жүзеге асырылады. Зерттеудің бұл түрін көбінесе құқық қорғау органдарының компьютерлік сараптамасы саласындағы сарапшылар емес, жұмыста мамандандырылған мәліметтер базасын, арнайы бағдарламалық жасақтаманы және сараптамалық зерттеу әдістерін қолданатын және тиісті лицензиясы бар үшінші тарап мамандары жүргізетініне назар аударайық.

Айта кетейік сарапшы зерттеу объектісін, ондағы ақпаратты және іс материалдарын сақтауға міндетті, осыған байланысты зерттеу объектісіне қандай да бір өзгерістер енгізу ұсынылмайды. Дегенмен, қазіргі уақытта олардың мазмұнына, мысалы, ұялы телефондарға немесе SSD дискілеріне өзгертулер енгізбестен сараптамалық зерттеу арқылы қол жеткізу мүмкін емес ақпарат тасымалдаушылары бар. Мұндай жағдайда тергеушінің немесе соттың объектіні немесе оның бір бөлігін бүлдіруге әкеп соқпайтын өзгерістер енгізуге жазбаша рұқсаты талап етіледі. Бұл рұқсат компьютерлік сараптама тағайындау туралы қаулыда көрсетілуі немесе сот тергеушінің өтінішін қанағаттандыру арқылы алынуы мүмкін.

Табылған ақпарат мүмкіндігінше іздеуге және қарауға жарамды форматқа келтіріледі және іздеу аймағына қосылады. Ақпаратты қарауды аппараттық-бағдарламалық кешенде бар сарапшының бағдарламалық қамтамасыз етуінің көмегімен де, зерттеу объектілерінде бар бағдарламалық қамтамасыз етудің көмегімен де жүзеге асыруға болады.

Егер ізделген ақпараттың көлемі елеулі болса және сарапшының қорытындысына қосымшаны қағаз тасығышта қалыптастыруға мүмкіндік берсе, онда ақпарат ішінара басып шығарылуы мүмкін. Осыдан кейін ақпаратты бір жазбаның CD - және DVD-дискілеріне көшіру жүргізіледі, ол туралы сарапшының қорытындысы көрсетіледі. Дискіге ақпаратты жазу форматты, қасиеттерді және метадеректерді өзгертпестен жүргізілуі тиіс, содан кейін CD-немесе DVD-дискінің жұмыс істемейтін бетінде арнайы маркердің көмегімен сараптаманың нөмірі мен күні, қосымшаның нөмірі көрсетіле отырып, сарапшының қолымен расталған түсіндірме жазба орындалады.

Сарапшының алдына сұрақтар қойылуы мүмкін:

1. Сараптамаға ұсынылған абоненттік құрылғыда бар ма. онда орнатылған SIM-карта мен жад картасында оны пайдалану барысында

жасалған ақпарат: белгілі бір тұлғалардың немесе абоненттік нөмірлердің контактілерінің тізімі, белгілі бір мазмұндағы жіберілген және қабылданған SMS-хабарламалар, аудио, бейне және графикалық файлдар, соңғы шығыс және кіріс қоңыраулар, абоненттік құрылғының белгілі бір жерде екенін көрсететін геолокация бағдарламаларының деректері белгілі бір уақытта және т.б.

2. Зерттеуге ұсынылған абоненттік құрылғының IMEI мәні қандай?

3. Абоненттік құрылғының жадында белгілі бір әрекеттерді жасауға (тізбе беруге) мүмкіндік беретін бағдарламалық қамтамасыз ету бар ма, мысалы, пайдаланушыдан жасырын SMS-хабарламалар алу, пайдаланушыдан жасырын түрде белгілі бір абоненттік нөмірге SMS-хабарламалар жіберу, пайдаланушыны ескертусіз абоненттік құрылғы туралы мәліметтерді алу және беру?

4. Абоненттік құрылғыда пайдаланушыдан жоспарланбаған функцияларды жасырын орындауға қабілетті бағдарламалық жасақтама іске қосылды ма.

5. Абоненттік құрылғыда Интернетке қосылу функциясы бар ма? Олай болса, белгілі бір интернет-ресурстарға жүгіну туралы деректер бар ма?

Сараптамалық зерттеу процесінде ақпаратты іздеу және зерттеу мынадай ретпен жүргізіледі:

1. «Хгу», «мобильді криминалист», сондай-ақ арнайы бағдарламалық қамтамасыз ету сияқты құралдарды пайдалана отырып, абоненттік құрылғының жадының физикалық қоқысын алу.

2. Сарапшының алдында тұрған міндеттерге байланысты мамандандырылған бағдарламаларды (R-studio, UFS Explorer, Belkasoft AccessData) пайдалана отырып жүзеге асыруға болады. EnCase және т.б.) жойылған ақпаратты қалпына келтіру.

3. Орнатылған, сондай-ақ орнатылмаған, бірақ құрылғыда бар бағдарламалық жасақтама мен қосымшаларды талдау.

4. Барлық қолда бар ақпаратты антивирустық бағдарламалық қамтамасыз етумен тексеру.

5. Істің мән-жайлары мен сарапшының алдына қойылған мәселелерге сүйене отырып, қызығушылық тудыратын ақпаратты іздеу. Бұл ретте іріктемеден штаттық бағдарламалық қамтамасыз ету, стандартты қосымшалар, бұрын белгіленген күннен бастап жасалған ақпарат алынып тасталады.

6. Қызығушылық тудыратын файлдар сарапшының қорытындысында функционалдық мүмкіндіктерден, белсендірілген функциялардан (мысалы, Интернет желісіне кіруге рұқсат беру, SMS-хабарламаларды жіберу, қабылдау және жою, телефон нөмірі, Сериялық нөмір, Қоңыраулар туралы ақпарат алу, байланыс деректеріне, медиа-файлдарға,камераға қол жеткізу, микрофонға, фотосуреттерге, терезелердің үстіндегі хабарламаларды көрсетуге рұқсат және т.б.).

7. Терең зерттеу үшін бағдарламалық файлды java сияқты тиісті бағдарламалау тілінде қабылдауға болатын кодқа түрлендіруге болады. Ол үшін Dex2 Jar немесе Android SDK бағдарламасын пайдалануға болады.

8. Істің мән-жайына байланысты бағдарламалық қамтамасыз етудің статикалық динамикалық талдауы жүргізілуі мүмкін. Соңғы жағдайда ол сарапшының аппараттық-бағдарламалық кешенінде іске қосылады. Бұл ретте оның пайдаланушы деректерін жинау және жіберу, криптографиялық операциялар, жасалған және Жойылған файлдар және т. б. деректерді жіберу және алу мүмкіндіктері тіркеледі.

9. Статикалық және динамикалық зерттеу нәтижелерін бағалау негізінде бағдарлама туралы анықталған ақпараттың істің мән-жайларына сәйкестігі, сондай-ақ құрылғыда, атап айтқанда, қажетті ақпараттың болуы (болмауы) туралы қорытынды жасалады:

– мобильді құрылғының каталогында (атауы) мыналарды жүргізуге мүмкіндік беретін қамтамасыз ету (атауы) бар (іс-қимылдар тізбесі: SMS-хабарламалар алу, нөмірге SMS-хабарламалар жіберу желілік қосылыстарды басқару, мекенжаймен қосылуды ұйымдастыру, пайдаланушының хабарламаларын мобильді құрылғыға алу және беру. Мобильді құрылғының жадында оның жүктелуі туралы келесі мәліметтер бар (мәліметтер тізімін беріңіз);

– мобильді құрылғының жадында мәліметтер бар (мәліметтер тізбесін беріңіз: нөмірден SMS-хабарламаларды алу туралы .... мәтінмен ... және т.б.; мәтіні бар нөмірден SMS-хабарламалар жіберу туралы... интернет-ресурстарға жүгіну туралы және т. б.);

– мобильді құрылғының жадында пайдаланушының ескертуінсіз келесі әрекеттерді (әрекеттер тізімін беруге) мүмкіндік беретін бағдарламалық жасақтама табылған жоқ;

– мобильді құрылғының жадында мәліметтер... (тізім беру) табылмады.

Киберқылмыстардың, оның ішінде компьютерлік ақпарат саласындағы алаяқтықтардың едәуір өсуі жағдайында компьютерлік сараптаманың өзектілігі, қажеттілігі мен тиімділігі күмән тудырмайтынын атап өткен жөн. Алайда, бүгінгі таңда компьютерлік сараптаманың сапалы өндірісі қысқа мерзімде кейбір жағымсыз жағдайлармен күрделене түседі. Осылайша, қылмыстар санының күрт артуына және техникалық байланыс құралдары мен электрондық ақпарат тасымалдаушыларын алып қою және тексеру үшін маман ретінде жиі тартуға байланысты олардың жүктемесіне тиісті рұқсаты бар сарапшылардың жетіспеушілігі проблемасы бар.

Қазіргі уақытта компьютерлік ақпарат саласындағы алаяқтықтарды сәтті және жедел тергеу үшін құқық қорғау органдары жеке компанияларға сараптама жүргізу үшін компьютерлік ақпарат саласында өз қызметін жүзеге асыратын бөгде мамандардың көмегін пайдалануға жүгінуге мәжбүр.

Осылайша, компьютерлік ақпарат саласындағы алаяқтықты тергеу кезінде тергеу әрекеттерін жүргізу белгілі бір ерекшеліктерге ие, олар іздеудің нақты механизмімен, әсіресе цифрлық іздермен жұмыс істеу қажеттілігімен, қылмыс жасау тәсілімен, қылмыскердің жеке басының сипаттамасымен анықталады. Тергеудің оң нәтижесі және белгілі бір тергеу әрекетін тиімді жүзеге асыру үшін тергеуші жоспарды ойластырып, қазіргі тергеу жағдайын жан-жақты талдай отырып, тактикалық әдістер мен мамандардың мүмкіндіктерін қолдана отырып, мұқият дайындалуы керек.

Өкінішке орай, қазіргі уақытта құқық қорғау органдары ақпараттық-телекоммуникациялық технологияларды қолданумен байланысты қылмыстарды тергеуге мамандандырылған кадрлардың жетіспеушілігін сезінуде, бұл тергеудің сапасы мен мерзіміне әсер етеді.

Компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша алғашқы тергеу әрекеттерінің ерекшеліктерін зерттеу барысында келесі негізгі аспектілер анықталды.

Біріншіден, мұндай істер тергеу органдары тарапынан ерекше назар мен құзыреттілікті талап етеді, өйткені олар заманауи ақпараттық технологияларды қолданумен және қылмыс жасаудың нақты әдістерімен байланысты. Технологияның қарқынды дамуын және алаяқтықтың жаңа тәсілдерінің үнемі пайда болуын ескеру қажет, бұл тергеушілерден өз білімдері мен дағдыларын үнемі жаңартып отыруды талап етеді.

Екіншіден, компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша алғашқы тергеу әрекеттерін жүргізу арнайы әдістер мен техникалық құралдарды қолдануды талап етеді. Бұған цифрлық дәлелдемелерді алу және талдау, компьютерлік сараптама жүргізу, мамандандырылған бағдарламалық қамтамасыз етуді пайдалану және т.б. сот процесінде пайдаланылуы үшін алынған дәлелдемелердің сақталуын және дұрыстығын қамтамасыз ету маңызды.

Үшіншіден, компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша алғашқы тергеу әрекеттерін жүргізудің маңызды аспектісі басқа мамандандырылған органдармен және сарапшылармен ынтымақтастық болып табылады. Мұндай істер көбінесе халықаралық сипатқа ие және ақпарат алмасу және басқа елдердің әріптестерімен ынтымақтастық қажет. Істің күрделі техникалық аспектілерін анықтау және талдау үшін ақпараттық қауіпсіздік және киберкриминалистика саласындағы сарапшыларды тарту да маңызды.

Жалпы, компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша алғашқы тергеу әрекеттерін жүргізу арнайы білімді, дағдыларды және басқа мамандармен ынтымақтастықты қажет етеді. Ақпараттық қауіпсіздіктің заманауи қатерлеріне тиімді қарсы тұру үшін мұндай істерді тергеудің әдістері мен тәсілдерін үнемі жетілдіріп отыру қажет.

Өзін-өзі бақылауға арналған сұрақтар:

1. Компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша алғашқы тергеу әрекеттерін жүргізудің негізгі кезеңдері қандай?
2. Компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша алғашқы тергеу әрекеттерін жүргізу кезінде қандай құжаттарды тексеру қажет?
3. Алаяқтық істер бойынша алғашқы тергеу әрекеттерін жүргізу кезінде компьютерлік ақпаратты зерттеудің қандай әдістері қолданылады?
4. Алаяқтық туралы істер бойынша алғашқы тергеу әрекеттері шеңберінде компьютерлік ақпараттың сақталуын қамтамасыз етудің қандай ерекшеліктері бар?
5. Алғашқы тергеу әрекеттерін жүргізу кезінде компьютерлік ақпарат саласындағы алаяқтықтың қандай негізгі белгілерін ескеру қажет?
6. Алғашқы тергеу әрекеттерін жүргізу кезінде компьютерлік ақпарат саласындағы алаяқтықтың электрондық іздерін зерттеудің негізгі әдістері қандай?
7. Компьютерлік ақпарат алаяқтық істерін тергеу кезінде виртуалды ақша ағындарын талдау қалай жүзеге асырылады?
8. Компьютерлік ақпарат саласындағы алаяқтық істер бойынша алғашқы тергеу әрекеттерін жүргізу кезінде метадеректерді жинау мен талдаудың қандай ерекшеліктері бар?
9. Бастапқы тергеу әрекеттері шеңберінде компьютерлік ақпарат саласындағы алаяқтықтың әлеуетті қатысушыларын анықтау және оқшаулау қалай жүзеге асырылады?
10. Компьютерлік ақпарат алаяқтық істері бойынша алғашқы тергеу әрекеттерін жүргізу кезінде қандай негізгі қиындықтар туындауы мүмкін және оларды қалай жеңуге болады?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Компьютерлік ақпарат саласындағы алаяқтық істерді тергеу кезінде қандай алғашқы тергеу әрекеттері жүргізілуі мүмкін?

a) құжаттар мен материалдарды тінту және алып қою;

b) күдіктіні қамауға алу;

c) жедел-іздестіру іс-шараларын жүргізу;

d) куәгерлердің сауалнамасы;

e) жоғарыда айтылғандардың барлығы.

2. Компьютерлік ақпарат саласындағы алаяқтық туралы істерді тергеу шеңберінде тінту жүргізу кезінде қандай ерекшеліктер бар?

a) сот санкциясының болуы қажет;

b) тінту тек күндізгі уақытта жүргізілуі мүмкін;

c) күдікті тінту кезінде болуы керек;

d) тінту тек адвокаттың қатысуымен жүргізілуі мүмкін;

e) жоғарыда айтылғандардың барлығы.

3. Тергеу әрекеттерін жүргізу кезінде компьютерлік ақпараттың сақталуын қамтамасыз ету үшін қандай шараларды қолдануға болады?

a) сыртқы тасымалдағышқа ақпараттың көшірмесін жасау;

b) компьютерге кіруге тыйым салу;

c) ақпаратты жоюға, өзгертуге немесе жасыруға тыйым салу;

d) компьютерлік ақпаратқа сараптама жүргізу;

e) жоғарыда айтылғандардың барлығы.

4. Компьютерлік ақпарат саласындағы алаяқтық туралы істерді тергеу шеңберінде жедел-іздестіру іс-шараларын жүргізу кезінде қандай ерекшеліктер бар?

a) олар тек тергеушінің шешімі бойынша жүргізілуі мүмкін;

b) олар соттың санкциясы болған жағдайда ғана жүргізілуі мүмкін;

c) олар тек адвокаттың қатысуымен жүзеге асырылуы мүмкін;

d) олар тек күндізгі уақытта жасалуы мүмкін;

e) жоғарыда айтылғандардың барлығы.

5. Компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша тергеу әрекеттерін жүргізу кезінде қандай құжаттар мен материалдар алынуы мүмкін?

a) компьютерлер мен ақпарат тасымалдаушылар;

b) қылмыс жасағаны туралы куәландыратын құжаттар;

c) серверлер және желілік жабдық;

d) қорғалған ақпараттың кілттері мен парольдері;

e) жоғарыда айтылғандардың барлығы.

6. Компьютерлік ақпарат саласындағы алаяқтық туралы істерді тергеу шеңберінде куәгерлерден сұрау кезінде қандай ерекшеліктер бар?

a) куә айғақтар беруден бас тарта алады;

b) сұрау салу кезінде куә болу керек;

c) куәгерге сауалнама тек адвокаттың қатысуымен жүргізілуі мүмкін;

d) куә жалған айғақтар үшін қылмыстық жауапкершілікке тартылуы мүмкін;

e) жоғарыда айтылғандардың барлығы.

7. Компьютерлік ақпарат саласындағы алаяқтық туралы істерді тергеу шеңберінде күдіктіні тұтқындау кезінде қандай ерекшеліктер бар?

a) қамауға алу тек тергеушінің шешімі бойынша жүзеге асырылуы мүмкін;

b) қамауға алу тек соттың санкциясы болған жағдайда ғана жүргізілуі мүмкін;

c) қамауға алу тек адвокаттың қатысуымен жүзеге асырылуы мүмкін;

d) қамауға алу тек күндізгі уақытта жасалуы мүмкін;

e) жоғарыда айтылғандардың барлығы.

8. Алаяқтық туралы істерді тергеу шеңберінде компьютерлік ақпаратқа сараптама жүргізу кезінде қандай ерекшеліктер бар?

a) сараптама тергеушінің шешімі бойынша ғана жүргізілуі мүмкін;

b) сараптама соттың санкциясы болған кезде ғана жүргізілуі мүмкін;

c) сараптама адвокаттың қатысуымен ғана жүргізілуі мүмкін;

d) сараптама тек күндізгі уақытта жүргізілуі мүмкін;

e) жоғарыда айтылғандардың барлығы.

9. Тергеу әрекеттерін жүргізу кезінде компьютерлік ақпаратты жоюдың, өзгертудің немесе жасырудың алдын алу үшін қандай шараларды қолдануға болады?

a) компьютерді физикалық құлыптау;

b) интернет желісінен ажырату;

c) мамандандырылған бағдарламалық жасақтаманы пайдалану;

d) компьютерге кіруге тыйым салу;

e) жоғарыда айтылғандардың барлығы.

10. Компьютерлік ақпарат саласындағы алаяқтық туралы істерді тергеу шеңберінде күдіктінің құқықтары мен заңды мүдделерін қорғау үшін қандай шаралар қолданылуы мүмкін?

a) адвокатқа қол жетімділікті қамтамасыз ету;

b) іс материалдарымен танысу мүмкіндігін беру;

c) заңда белгіленген мерзімде сот талқылауын жүргізу;

d) ұстау себебі мен айыптау туралы хабарлама;

e) жоғарыда айтылғандардың барлығы.

ҚОРЫТЫНДЫ

«Компьютерлік ақпарат саласындағы алаяқтықты тергеу ерекшеліктері» тақырыбындағы оқу құралын зерделеу нәтижесінде келесі тұжырымдар жасауға болады.

Компьютерлік ақпарат саласындағы алаяқтық туралы істер бойынша алғашқы тергеу әрекеттерінің өзіндік ерекшеліктері бар, олар тергеу қызметінің жалпы принциптерімен ғана емес, сонымен бірге қылмыстың осы саласының ерекшеліктерімен де анықталады.

Қазіргі ақпараттық қоғамда компьютерлік ақпарат саласындағы алаяқтық барған сайын кең таралған және күрделі қылмысқа айналуда. Фишинг, хакерлік, банктік карточкалық алаяқтық және басқалары сияқты қылмыстардың түрлері тергеушілердің ерекше назары мен құзыреттілігін қажет етеді.

Компьютерлік ақпарат саласындағы алаяқтықты тергеудің негізгі ерекшеліктерінің бірі-жедел әрекет ету және заманауи әдістер мен технологияларды қолдану қажеттілігі. Тергеушілер дәлелдерді сәтті анықтау және жинау үшін компьютерлік жүйелермен, сандық іздермен және желілік протоколдармен жұмыс істеу дағдыларына ие болуы керек.

Сондай-ақ, компьютерлік ақпарат саласындағы алаяқтықты тергеу пәнаралық тәсілді қажет ететінін атап өткен жөн. Жұмыс барысында тергеушілер Ақпараттық технологиялар, банк,, құқықтану және басқа да байланысты салалардағы сарапшылармен ынтымақтасуы керек. Тек осындай тәсіл осы саладағы қылмыстық әрекеттерді тиімді анықтауға және жолын кесуге мүмкіндік береді.

Қорытындылай келе, «компьютерлік ақпарат саласындағы алаяқтықты тергеу ерекшеліктері» тақырыбындағы оқу құралымен танысу осы салада жұмыс істейтін тергеушілер үшін пайдалы білім мен дағдыларды қамтамасыз ететіндігін атап өтуге болады. Алғашқы тергеу әрекеттерін дұрыс және сауатты жүргізу тергеудің маңызды кезеңі болып табылады және бүкіл процестің тиімділігі мен заңдылығын қамтамасыз етуге мүмкіндік береді.

ШУЛЬГИН *ЕВГЕНИЙ ПЕТРОВИЧ,*
САПАРҒАЛИЕВ *ЖАНДОС НУРБЕКОВИЧ,*
ДОСЫМБЕТОВ *ЕСЕН ОРАЗБЕКОВИЧ,*
ТАФИНЦЕВ *ПАВЕЛ АНАТОЛЬЕВИЧ*

КОМПЬЮТЕРЛІК АҚПАРАТ САЛАСЫНДАҒЫ АЛАЯҚТЫҚТЫ ТЕРГЕУДІҢ ЕРЕКШЕЛІКТЕРІ

ОҚУ ҚҰРАЛЫ

Басуға қол қойылды 21.07.2023 ж. Пішімі 60х90/16
Есептік баспа табағы 3,9. Таралымы 50 дана. Тапсырыс 75.
«Гласир» ЖШС баспаханасы. Қарағанды, Ермеков к., 112/5.