Аратұлы Қ., Байғазы Е.

Ақпараттық қауіпсіздік саласындағы қылмыстарды тергеу әдістемесі

Ақпараттық қылмыстар жөніндегі мәліметтер үзілмелі болып келеді. Соған байланысты ақпараттық қылмыстарды толығымен ашып бейнелеп беру криминалистика ғылымы мен тәжірибесі жағынан өте қиын. Осындай шабуылдарға ұшыраған мемлекеттік және коммерциялық ұйымдар өздерінің қорғаныс жүйесі мен келтірілген шығындарын тергеуден жасыратыны белгілі. Сондықтан көп жағдайларда тергеуге қажетті мәліметтер жарыққа шыға бермейді.

Түйін сөздер: ақпараттық қауіпсіздік, ақпараттық қылмыстар, криминалистика, тергеу, тергеу ситуациялары, тактикалық тергеу әрекеттері, компьютерлік-техникалық сот сараптамасы, арнайы білімді қолдану.

Aratuly K., Baigazy E.

Methodology for the investigation of crimes in the sphere of information security

Data on information crimes are most often broken. In this connection, and in terms of forensic science, and practice to fully disclose and describe this perspective is very difficult. We know that public services themselves, and even the state itself, and commercial organizations manage to conceal the true information about the attack in their information system security and the consequences of such an attack on the investigating authorities and the public. For this reason, it is necessary and important information for investigation remains a mystery.

Key words: information security, information crimes, criminalistics, the investigation, the investigation of the situation, tactical actions investigative, computer forensics and technology, using of special knowledge.

Аратулы К., Байгазы Е.

Методика расследования преступлений в сфере информационной безопасности

Данные об информационных преступлениях чаще всего бывают прерывистыми. В связи с чем и с точки зрения науки криминалистики и практики полностью раскрыть и описать данную проблематику очень сложно. Известно, что сами государственные службы, а то и само государство, и коммерческие организации умудряются скрыть достоверную информацию о нападении в их информационную систему безопасности и о последствиях такого нападения от органов следствия и от общественности. И по этой причине необходимая и важная информация для следствия остается в тайне.

Ключевые слова: информационная безопасность, информационные преступления, криминалистика, следствие, следственные ситуации, следственные тактические действия, компьютерно-техническая судебная экспертиза, применение специального знания.

ӘОЖ 343

***Аратұлы Қ., Байғазы Е.**

Әл-Фараби атындағы Қазақ ұлттық университеті,
Қазақстан Республикасы, Алматы қ.
*E-mail: kunya8585@mail.ru

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ ҚЫЛМЫСТАРДЫ ТЕРГЕУ ӘДІСТЕМЕСІ

Ақпараттық қауіпсіздік саласындағы қылмыстарды анықтау және тергеу кезінде бірнеше алғашқы типтік тергеу ситуациялары болады:

1-ситуация – ақпараттық жүйенің немесе желінің (компьютердің) иесі немесе заңды пайдаланушысы өзі ақпараттық құқықбұзушылықты анықтады, күдікті тұлғаны анықтап, ол жөнінде жауапты тұлғаларға және құқыққорғау органдарына хабарлады;

2-ситуация – ақпараттық жүйенің немесе желінің (компьютердің) иесі немесе заңды пайдаланушысы ақпараттық құқықбұзушылықты анықтады, алайда құқықбұзушылықты жүзеге асырған тұлғаны білмеді, осы жөнінде жауапты тұлғаларға және құқыққорғау органдарына хабарлады;

3-ситуация – ақпараттық жүйенің не желінің пайдаланушысы немесе иесі компьютерлік қол сұғуды анықтады, күдікті тұлға құқыққорғау органдарына белгілі және құқыққорғау органдары немесе құзырлы тұлғалар күдіктіні жедел-іздестіру шаралары кезінде ұстады (тұтқындады), нақты кінәлі тұлғалар белгісіз;

4-ситуация – компьютердің не компьютерлік желінің иесі ақпараттық құқықбұзушылық жөнінде білмейді, өзге жауапты тұлғаларға ол жөнінде белгілі, тиісті құқыққорғау немесе құзыретті органдарға ол жөнінде хабарланды. Мұндай ситуация да кездесуі мүмкін, себебі ақпараттық қылмыстардың жасалғандығы субъективті фактормен байланысты болып келеді. Көп жағдайда ақпараттық қылмыстар жәбірленуші жағынан ескерілмеуі мүмкін.

Сонымен қатар компьютерлік қылмыстардың басым бөлігі жасырын жасалады, сол себепті АКЖ-нің пайдаланушысы немесе компьютерлік жүйенің иесі, яғни жәбірленуші тұлғалар қылмыстың жасалғандығы жөнінде беймәлім болуы мүмкін. Сондықтан ақпараттық қылмыстар латентті қылмыстар қатарына жатады. Ал егер АКЖ-ні пайдаланушы, компьютердің иесі немесе оны заңды түрде қолданушысы ақпараттық құқықбұзушылық жөнінде хабардар болмаса, ол туралы ақпарат құқыққорғау органдарына мүлдем жетпеуі мүмкін.

Кінәлі адам белгілі болса, тергеудің басты тапсырмасы жәбірленушіден тиісті дәлелдемелерді процессуалдық жинау болады және оларға мыналар жатады:

а) жүйедегі ақпараттың тұтастылығының және конфиденциялдылығының бұзылуы;

ә) жүйедегі ақпараттың тұтастылығының және конфиденциялдылығының бұзылуынан келтірілген зардап мөлшері;

б) жүйедегі ақпараттың тұтастылығы мен конфиденциялдылығының бұзылуы тәсілдері мен кінәлімен жасалған әрекеттердің сипатын бөлшектеу арқылы құқықбұзушылықтың әдісі мен нәтижесін құрайтын себепті байланыс;

в) кінәлі адамның жасаған іс-әрекеті мен одан келтірілген зиянына қатысы.

Ал егер қылмыскер қылмысты жасау сәтінде немесе қылмысты жасап болғаннан кейінгі сәтте ұсталған болса, ұсталғанды жеке тінту, одан жауап алу және оның тұрғылықты мекен-жайы бойынша тінту алдын-ала тергеу әрекеттері жүзеге асырылуы тиіс.

Бұл қадамдағы типтік тергеу әрекеттеріне ақпараттық жүйені, оның желілерін және электронды тасымалдауыштарды қарау мен тіркеуді, куәлардан және осы электронды жүйелерді жүзеге асыратын және басқаратын өкілетті адамдардан жауап алуды жатқызуға болады. Жұмыстың маңызды элементі болып электронды құжаттарды, қылмыскер заңсыз кірген сәттегі ақпараттық жүйелерді тасымалдауыштарды, құрылғыларды маманның қатысуымен алу әрекеті табылады.

Сонымен қоса тергеу қызметкерлеріне қылмыскер ақпараттық жүйе арқылы кіру әрекеттерін жүзеге асырған орнын ескерген дұрыс, яғни қылмыс орнын тіркеуге алу керек. Себебі қылмыскер әрекеттерін жүзеге асырған кезде өзіне қажетті заттарды қолдану кезінде көптеген іздер қалдырып кетуі мүмкін.

Нәтижесінде алынған дәлелдемелер тұлғаны күдікті немесе тіпті айыпкер ретінде тану шешімін қабылдауға негіз болуы мүмкін.

Егер қылмыстың субъектісі ұсталмаған немесе анықталмаған жағдайда тергеу қызметінің келесі алғашқы тапсырмасы дәлелдемелерді жинау болып табылады. Мысалы, ақпараттық жүйедегі тұтастық және конфиденциалдық талаптарының бұзылуын, зардаптың мөлшерін және әрекет пен келтірілген нәтиженің себепті байланысын нақты анықтау.

Типтік тергеу іс-әрекеттері бірінші типтік жағдайға ұқсас. Алайда сол уақыт ішінде күдіктінің осы ақпараттық жүйеге кіруді жүзеге асырған қылмыс орнын іздеу шараларын атқарған дұрыс. Қылмыс орнын іздеу қызметтік тұлғалар арқылы ақпараттық жүйеге кіру орны мен кіру әдісін, қылмыскердің қолданған тәсілдерін және бағдарламаларын анықтай отырып жүзеге асырылады. Қылмыстың орны көбінесе оның жұмыс орны, үйі, жұмысының және үйінің маңайындағы ғаламтор кафелер, әуежайлар, вокзалдар, қоғамдық жерлер, туыстарының немесе достарының үйі және сәйкес құрылғылары мен қондырғылары бар жоғары жылдамдықты Вай-Фай (Wi-Fi) нүктелері бар планетамыздың кез келген жері болып табылады.

Жиі кездесетін типтік болжауларға мыналарды жатқызамыз: қылмыскердің жеке тұлғасына қатысты болжаулар (кімде ақпаратқа, ақпараттық жүйеге кіруге мүмкіндігі болды? Кімнің осындай қылмыс жасауға мақсаты немесе қызығушылығы тууы мүмкін? Қылмыскердің ниеті немен сипатталады және т.б.), ақпараттық шабуылдар мен ақпараттық жүйелерге заңсыз кіру әрекеттері қай жерден жасалуы мүмкін, қылмысты жасау жағдайлары қандай болды, келтірілген шығынның (зардаптың) мөлшері және т.б.

Алғашқы тергеу әрекеттерін аталған типтік тергеу ситуациялары бойынша куәгерлерден жауап алудан, қылмыс жөнінде жан-жақты мәліметтерді жинастырудан бастаған маңызды болып табылады. Мәліметтерді жинастырумен қатар тергеу үшін басты сипатқа ие – оқиға болған жердегі ақпараттық жүйелерді, ақпараттық тасымалдауыштарды, қосалқы және жеке құрылғыларды ұқыпты және толық қарау болып табылады.

Сонымен қатар мәліметтерді жинау кезінде дайындық жұмыстары үлкен рөл атқарады. Куәгер және жәбірленуші тұлғаларды оқиға орнына абайлап қатыстыру немесе мүлдем алшақтату және тиісті алғашқы тергеу әрекеттерін жүргізу, олардан жауап алу. Оқиға болған жерге мүдделі емес ақпараттық технологиялар саласының мамандарын қатыстыру, олармен үлгілерді, заттай дәлелдемелерді алу жұмысын жүзеге асыру.

Дәлелдеуші ақпараттың мәні мен маңызын түсіну үшін қолданатын классикалық жолдардың бәрі электронды ақпаратты тасымалдаушылардан алынған объектілерді және жоғарғы технологияларды пайдалану кезінде пайда болатын процедураларды теориялық құқықтық талдау шегінен тыс қалдырады. Дәлелдемелік ақпараттардың зерттеушілермен келтірілген сұрақтары бәрі-бір де әдетте қолданылатын хаттама, сарапшы қорытындысы, құжаттар, заттай дәлелдемелер негізінде жүзеге асырылады. Әсіресе ақпараттық технологиялар негізінде алынған мәліметтерді дәлелдеме ре-

тінде пайдалану көп жағдайда мүмкін емес. Енді ол объектілерге қолданыстағы Қылмыстық-процестік кодексінің дәлелдемелер жөніндегі нормаларын қолданатын болсақ, ол дәлелдемелік мәлімет бар диск, процессор, флешка, дискета және т.б. тек заттай дәлелдеме ретінде ғана қарастырылады. Басқаша айтқанда, тергеу мен сотты қызықтыратын ақпаратты электронды тасымалдауыш дәлел ретінде тек физикалық объект болып қарастырылады, яғни оның түсі, салмағы, пішіні, қандай материалдан жасалғаны, ол материал жөніндегі мағлұмат және т.б. Бұл дегеніміз оның ішкі мазмұны қарастырылмайды және ашылмайды, ол криминалистикадағы киімдегі қан дақтары, механикалық бұзылымдар, сындыру іздері бар кіретін есік және тағы да басқалары сияқты сырттай ғана зерттеледі. Бұлардың айырмашылығы киімді қарау, есікті, құлыпты тексеру жалпы қылмыстың сипатын және оны жасаудың механизмін көрсететін мәліметтерді береді, ал ақпаратты электронды тасымалдауышты қарау еш жеке, ерекше немесе іс үшін маңызды белгілерді анықтамайды. Мұндай дисктер мен дискеталар, процессорлар мыңдаған, ал қан дағы бар киім қайталанбас біреу ғана болады. Содықтан оларды бір қатарға қоюға болмайды.

Кез келген заттай дәлелдемеге жататын материалдық объект қылмыстың іздерін ашу үшін, басқа материалдық объектілерді анықтау үшін, басқа да іске маңызды жағдайларды анықтау үшін тергеу қарауына жатуы тиіс.

Электронды тасымалдауыш заттарын қарау іске маңыздылығы бар ең төменгі минималды мәліметтерді береді. Қарастырылып отырған материалдық объектінің спецификасы оны заттай дәлелдемелерге жатқызу кезінде оның тек іске қатыстылығын факт ретінде процессуалдық фиксация жасау болып табылады.

Заттай дәлелдемені қарау көптеген қылмыстық істер бойынша басқа да криминалистикалық процессуалдық тергеу іс-әрекеттерін жүргізуге қажеттілік тудырады. Мысалы: қараудан кейін сот сараптамасы тағайындалуы мүмкін немесе тану әрекеті жүргізілуі мүмкін. Егер тану әрекеті бұрын қаралған объектінің ұқсастығын немесе айырмашылығын анықтауға бағытталса, сараптама әрекеті істің жағдайлары жөніндегі мәліметтерді арнайы білімге негізделген әдістер арқылы объектіні зерттеуге бағытталады.

Арнайы білімді қолдану және сараптама тағайындау. Заңгер-тергеуші осы саладағы барлық технологиялық өзгерістерді бақылап игеріп отыруы мүмкін емес. Сол себепті арнайы мамандардың тінту, қарау және алу шараларына қатысуы аса маңызды және қажет.

Бұл жерде «тиісті мамандарды қайдан алуға болады» деген сұрақ туындайды. Мұндай маман иелерін компьютерлік және коммуникациялық техника құралдарымен жұмыс жасайтын және орнататын, жөндейтін ұйымдардан және мекемелерден, жоғары оқу орындарынан, арнайы білім беру қызметтерінен, ғылыми-зерттеу ұйымдары мен ұжымдарынан іздеген дұрыс.

Электронды ақпараттық саласындағы арнайы мамандар мысалға тергеу кезінде мына мәселелер бойынша көмегін тигізуі мүмкін:

1. Компьютерлік құралдардың құрамы мен конфигурациясы қандай және олар арқылы айыптыға тиісті әрекеттерді жүзеге асыруға бола ма?

2. Бұл электронды ақпараттық құралында ақпараттық ресурстың қай түрі бар?

3. Табылған файлдар басқа компьютерлік құралдың ақпаратының бір көшірмесі болып табылмайды ма?

4. Бұл файлдар мен бағдарламаларда вирус бар ма, бар болса нақты қандай вирус?

5. Табылған қағаз бетіндегі жазбалар бұл бағдарлама бойынша код болып табылмайды ма және бұл бағдарлама мақсаты мен бағыты неде?

6. Белгілі компьютерлік ақпарат жойылуға, көшіруге және модификациялауға ұшырады ма?

7. Анықталып отырған ақпараттық жүйеде компьютерді эксплуатациялаудың қандай ережелері бар және олар бұзылды ма?

8. Эксплуатациялау ережелерін бұзу ақпаратты, мәліметті, белгілі бағдарламаны жою, көшіру және модификациялау әрекеттерімен себепті байланыста бар ма?

Сот сараптамасына келетін болсақ қарау да, тану да ғылыми білім базасында тергеу ісін жүргізу үшін негіз бермейді. Соған қоса бұл жерде сот сараптамасын тағайындау мен жүргізу үшін себеп болатын сыртқы фактор орын алмайды. Себеп те, негіз де факт туралы басқа да мәліметтерден құрылуы мүмкін.

Ақпаратты электронды тасымалдауыштың қай тергеліп жатқан іске жататынын анықтау сол объектіде орналасқан ақпаратқа қол жеткізу, кейін оған баға беру және ақпаратты шешу мен іс бойынша дәлел ретінде оны қолдану мәселесін шешу мақсатына ие.

Сөйтіп, ақпаратты электронды тасымалдауышты заттай дәлел ретінде қарау мен тану нәтижелері бойынша сот сараптамасын тағайындауға және жүргізуге нақты негіздердің болмауы қарастырылып отырған мәселе бойынша құқықтық қарым-қатынастарды реттейтін арнайы қыл-

мыстық-процестік нормасын ескеру өзектілігіне әкеледі.

Осы жерде ақпаратты электронды түрде тасымалдауыштар өзінің физикалық қасиеттеріне байланысты қылмыстың қаруы, құралы бола алмайды. Олар жайдан жай компьютерлік қылмыстық әрекеттің объектісі бола алмайды, қылмыстың объектісі ретінде тек оның ішіндегі ақпарат саналады. Сарапшыға осы ақпараттық құралдардың ішіндегі зерттелетін объектіге қатысты сұрақтар қойылады.

Олар өз кезегінде өзінде ақпаратқа байланысы бар іздерді сақтай алмайды, себебі ақпарат із қалдыруы мүмкін емес. Ал сыртқы іздер, мысалы, саусақ іздері мұндай қылмыстарда тек жанама дәлел болады, ол адамның бұл ақпаратқа тек қандай да қатысты болуы мүмкін екенін ғана көрсете алады. Бұл іздерге қатысты дактилоскопиялық сараптама және іздердің ерекшеліктеріне байланысты басқа да сараптама түрлері тағайындалуы мүмкін.

Тікелей дәлелдерге ақпаратты электронды түрде тасымалдауыштағы мәлімет және ол мәліметтің мазмұны жатады. Жалпы заттар әлемінің объектісі болып табылатын электронды тасымалдауыштар шын мәнінде компьютерлік қылмысты анықтаудың тәсілі бола алмайды. Бұл мақсаттарға тек осы мәліметтерді зерттеген кезде ғана жетуге болады. Сол себепті тиісті кешенді сараптамалық зерттеулер жүзеге асырылуы тиіс.

Ақпаратқа қатысты сараптамалық зерттеулер – ол азаматтық және қылмыстық істер бойынша дәлелдеуге маңызды болып саналатын жағдайлардан туындайтын, арнайы мамандардың зерттеу объектісі болып табылатын ақпараттық, бағдарламалық, компьютерлік желі мен жүйелік қауіпсіздік саласындағы тәжірибелік ілім тармағы.

Осындай зерттеулердің объектісіне жатады:

– персоналды компьютерлік құралдар;

– ақпараттық-коммуникациялық желілер және жүйелер;

– түрлі нысандағы компьютерлік қамтамасыз ету бағдарламалары, өзге де ақпараттық бағдарламалар;

– ақпараттық және ақпараттық жүйеге қатысты құжаттар;

– электронды құралдар, блокноттар, кітапшалар;

– компьютердің қосалқы құралдары (тышқан, пернетақта, кабельдер, сымдар, енгізу және шығару құралдары, монитор, модем және т.б.);

– ноутбуктер, планшеттер, смартфондар, түрлі бағдарламалары бар электронды құралдар;

– электронды пошталар, ғаламтор сілтемелері мен парақшалары және т.б.

– ақпаратты тасымалдауыштар (CD, DVD, USB тасымалдауыштар, микрокарталардың сан түрі, MP3 ойнағыштар, сыртқы жадылар, дискеталар, мини дисктер және т.б.).

Зерттеу объектілерінің ерекшеліктеріне байланысты оларды келесі нақты топтық түрлерге бөлеміз:

1) Компьютерлік-техникалық сот сараптамасы – компьютерлік құралдардың өздерін, олардың қосалқы бөлшектері мен техникалық құралдарын, электронды тасымалдауыштарын олардың техникалық дәрежесі мен қасиетін анықтау мақсатында жасалатын сараптама түрі;

2) Компьютерлік-бағдарламалық сот сараптамасы – компьютерлік жүйедегі бағдарламалық қамтамасыз ету және өзге де ақпараттық бағдарламаларды сараптамалық зерттеуді жүзеге асыру үшін тағайындалатын сараптама түрі;

3) Ақпараттық-техникалық сот сараптамасы – заңмен қорғалатын электронды мәліметтерге қол сұғу фактісімен ұштасатын сұрақтарды шешуге бағытталған сараптамалық зерттеулер;

4) Ақпараттық-желілік сот сараптамасы – жоғарыда аталған сараптама түрлерінен осы үшеуінің объектілерінің бірлесіп істеуі арқылы ақпараттық желіге шығу функцияларын жаңжақты зерттеуді білдіреді. Желілер жергілікті және жаһанды болып бөлінеді, сол себепті зерттеу көлемі де жергілікті желі шегінде немесе аса ауқымды жаһандық ғаламтор көлемінде сипатталуы мүмкін.

Тәжірибеде компьютер саласындағы сараптамалар көбіне кешенді түрде жүргізіледі. Себебі бір зерттеуден екінші зерттеу қажеттігі туындайды, сол себепті сарапшыға сұрақтар туындауы мүмкін реттігі бойынша кешенді түрде қойылады және сараптама ортақ атаумен «компьютерлік-техникалық сот сараптамасы» деп аталады. Осындай сараптама кезінде келесідей негізгі сұрақтар қойылуы мүмкін:

1) Көрсетілген техникалық құрал компьютерлік жүйеге жатады ма?

2) Зерттеуге ұсынылып отырған бөлшек компьютерлік техникалық жүйенің құрамына кіреді ме немесе құрамдас бөлігі болып табылады ма?

3) Компьютерлік жүйенің маркасы, моделі, типі және т.б. ерекшеліктері қандай?

4) Компьютерлік құралдың жиналу әдісі, құрастыру ерекшелігі қандай?

5) Компьютерлік-ақпараттық құралдың негізгі қызметтік мақсаты қандай және қылмыскер қандай мақсатта қолданған?

6) Компьютерлік құрал жұмыс істейді ме?

7) Компьютерлік жүйеде өзінің типтік параметрлерінен өзгеше дефектілері бар ма?

8) Құралды эксплуатациялау режимі қандай?

9) Зерттелетін ақпараттық құралда, жүйеде рұқсат етілмеген немесе сырттан келген бағдарламалар бар ма? Бұл бағдарламалардың мақсаты неде?

10) Ақпараттық жүйеде кездесетін ақпараттар саны және ерекшеліктері?

11) Аталған компьютерлік желіде қауіпсіздік немесе қорғаныс құралдары бар ма, бар болса қандай?

12) Компьютерді пайдаланушылар қорғаныс парольдерін қолданған ба?

13) Қылмыскерде ол парольдерге рұқсаты немесе оларды алу (білу) мүмкіндігі болды ма?

14) Бұл компьютерлік желінің қорғаныс және қауіпсіздік кілттері немесе кодтары бұзылған ба, бұзылса қандай жолмен жүзеге асырылған?

15) Компьютерлік құралдың бағдарламалық қамтамасыз етілуі қандай?

16) Бағдарламалық құралдың типі, түрі, нұсқасы қандай?

17) Бағдарлама лицензиялы өнім бе, әлде заңсыз немесе қылмыскердің қолымен жасалған ба?

18) Бағдарламалық құралдың қауіпсіздік және қорғаныс мүмкіндіктері қандай, қалай жасалған?

19) Ақпараттық тасымалдауыштар кездеседі ме?

20) Электронды тасымалдауыштар жұмыс күйінде ме? Олардың ішінде ақпарат бар ма, жоқ мүлдем бос па?

21) Ақпаратты электронды түрде тасымалдайтын құралдар қорғаныс құралымен қамтамасыз етілген бе?

22) Мәліметтер қандай физикалық жолмен және әдіспен тасымалданған, табылған мәліметтер түпнұсқасы көшірілген бе?

23) Тасымалдауышта анықталған мәлімет қасиеті қандай, сипаттамасы мен параметрлері, яғни файл, папка түрі, көлемі, жасалған немесе өзгертілген мерзімі, уақыты, атрибуттары және т.б.?

24) Файлдың түрі, типі қандай (мұрағаттық (архивтік), жасырын, анық, жалпы рұқсат етілген және т.б.)?

25) Файлдың кеңейтуі (расширение файла) қандай, қайда жиі кездеседі?

26) Электронды мәліметтің мазмұны қандай?

27) Компьютердің ғаламтормен байланысы қандай? Ғаламторға байланыс бар ма?

28) Компьютердің ғаламторда көрініс табатын IP-мекен-жайы қандай?

29) Қылмыскердің не жәбірленушінің логин-парольдері бар ма, қалай қолданылған?

30) Компьютерлік жүйеге жалғану қалай жасалған (желі арқылы, желісіз, әлде портпен)?

Тергеу және зерттеу барысында өзге де санқилы сұрақтар туындауы мүмкін.