ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Қуаныш АРАТҰЛЫ

АҚПАРАТТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРМЕН КҮРЕСУ АСПЕКТІЛЕРІ

Монография

Алматы
«Қазақ университеті»
2019

ӘОЖ 343
КБЖ 67.408
А 75

Баспаға әл-Фараби атындағы Қазақ ұлттық университетінің Ғылыми Кеңесі (№5 хаттама, 28.01.2019) және Редакциялық-баспа кеңесінің (№3 хаттама, 06.02.2019) шешімімен ұсынылған

Пікір жазғандар:
заң ғылымдарының докторы, профессор **А.Е. Жатқанбаева**
PhD **А. Алтынбекқызы**

Аратұлы Қ.

А 75 Ақпараттық құқық бұзушылықтармен күресу аспектілері: монография / Қ. Аратұлы. – Алматы: Қазақ университеті, 2019. – 196 б.

ISBN 978-601-04-3986-3

Бұл монографиялық еңбекте ақпараттық қылмыстармен күресудің қылмыстық саясаты қарастырылады. Компьютерлік қылмыстылық ұғымына және онымен сабақтас терминдер мен ағымдарға түсінік және анықтама беріле отырып аса өзекті қоғамдық мәселелер жан-жақты қозғалады әрі талқыланады. Сонымен қатар аталған мәселенің халықаралық деңгейдегі жағдайы ескеріліп қылмыстық-құқықтық заңшығару үдерістері негізге алынады.

Аталған ғылыми еңбек автордың ардақты да құрметті ғылыми жетекшісі заң ғылымдарының докторы, профессор Рима Еренатқызы Джансараеваға арналады.

ӘОЖ 343
КБЖ 67.408

ISBN 978-601-04-3986-3

МАЗМҰНЫ

АНЫҚТАМАЛАР, БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

Бұл жұмыста келесі терминдерге сәйкес анықтамалар қолданылған:

Ақпаратты бөгеу дегеніміз – компьютерлерді пайдалануышылар үшін ақпаратпен қатынау мүмкіндігін жасанды түрде қиындатып қою немесе сол әрекеттер үшін тосқауыл жасау

Ақпаратты жою дегеніміз – компьютерлік ақпаратты оның қалыпқа келуінсіз физикалық түрде ликвидациялау немесе ақпаратты сақтағыш заттан оны түбегейлі жойып жіберу

Ақпаратты көшіру – компьютерлік ақпаратты басқа сақтағышқа немесе тасымалдағышқа ауыстыру арқылы репродукциялау

Жаңарту (өзгерту немесе модификациялау) – ЭЕМ-де, ЭЕМ жүйесінде және желілерінде ақпараттың мазмұнын кез келген қалыпта өзгерту және сонымен қатар ақпараттың бағыттық маршрутын немесе жүру жолын өзгеріске ұшырату

Интернет – халықаралық глобалды байланыс желісі

ИК-порт, WI-FI – инфра-қызыл сымсыз жалғану

«К» басқармасы – компьютер қылмыстарымен айналысатын тергеу бөлімі

Компьютерлік вирус – арнайы жазылған шағын көлемді (кішігірім) программа. Ол өздігінен басқа программалар соңына немесе алдына қосымша жазылады да, оларды бүлдіруге кіріседі, сондай-ақ компьютерде тағы басқа келеңсіз әрекеттерді істейді. Ішінен осындай вирус табылған программа «ауру жұққан» немесе «бүлінген» деп аталады

Қылмыстық саясат – бұл қылмыстылықты қысқартуға, келтірілетін зардап мөлшерін азайтуға бағытталған қылмыстық-құқықтық, қылмыстық іс жүргізулік, сондай-ақ криминологиялық және басқа да шаралардан тұратын мемлекетпен жасалатын және ары қарайғы қадағаланатын қылмыстылықпен күресу шараларының мемлекеттік стратегиясы және тактикасы

Құрттар – жүйелік программалаушылардың информациялық-есептеу желілерінің бос тұрған ресурстарын анықтау программаларына кіріп алып, сол бос құрылғыларды тектен тек жұмыс істеуге мәжбүр етеді. Мысалы, оларды шексіз циклге енгізіп, құрдан-құр жүргізіп кояды немесе қажетсіз мәліметтерді баспаға шығартады

Мәліметтер базасы дегеніміз – бұл ЭЕМ арқылы табылуы және барлануы мүмкін болатындай жүйеленген мәліметтер (мысалы: мақалалар, есептеулер, кестелер) жиынтығының объективті формада ұсынылған және ұйымдастырылған түрі

Персоналды компьютерлер (ПК) – үстел үстіне орнатылады, көп функциялы, көптеген перифериялық қосымша құрылғылары бар, мүмкіндіктері мол, кеңселік жұмыстарда және басқа да мақсаттарда қолданылатын құрал

ЭЕМ желісі – бір-бірімен электрбайланыс сымдарымен немесе сымсыз портпен біріктірілген компьютерлер жиынтығы, немесе байланыс каналдарының не құралдарының әр компьютердің оның орналасқан жеріне қарамастан есептеу және ақпарат ресурстарын пайдалануға мүмкіндік беретін жиынтығы

ЭЕМ жүйесі – компьютерлердің біреуі жүйенің элементі болып саналатын немесе бірнеше ЭЕМ жүйесінен тұратын компьютерлік кешен немесе компьютерлік сервер

CD – компактілі диск

CD-ROM, DVD-ROM – лазерлі дисктерді оқитын құрылғылар

Ctrl-C, **Ctrl-Break** – пернетақта батырмаларының комбинациясы

DVD – компактілі видео диск

e-gov – электронды Үкімет

HD – hard disc, қатты диск

IMEI – ұялы байланыстың абоненттік құрылғысының сәйкестендіру (идентификациялық) коды (ағылш. International Mobile Equipment Identity) мобильді құрылғыларды анықтайтын халықаралық стандарт

MIT – Массачусетс технологиялық институты

SIM (ағылш. Subscriber Identification Module) абонентті идентификациялау модулі – мобильді байланыс түрлерінде қолданылатын абонентті сәйкестендіру және анықтау модулін жүзеге асыратын құрал. Кейпі физикалық пластикалық шағын карта

WWW – (World Wide Web) Әлемдік Ғаламтор

АКТ – Ақпараттық-коммуникациялық технологиялар

АҚШ – Америка Құрама Штаттары

АЭС – Атом электр станциясы

БАҚ – Бұқаралық ақпарат құралдары

БҚО – Батыс Қазақстан облысы

БҰҰ – Біріккен Ұлттар Ұйымы

ВЗУ – (внешнее запоминающее устройство) сыртқы сақтау құрылғысы

ДОС (DOS) – Операциялық жүйесі
ЖИТ – Жаңа информациялық технологиялар
ІІБ – Ішкі істер басқармасы
ІІМ – Ішкі істер министрлігі
КТҚ – Компьютерлік техника құралдары
ҚР – Қазақстан Республикасы
ҚІЖК – Қылмыстық іс жүргізу кодексі
МБ – Мәліметтер базасы
ОЖ – Операциялық жүйе
ОЗУ – (оперативное запоминающее устройство) жедел түрде сақтаушы құрылғы
РФ – Ресей Федерациясы
ТМД – Тәуелсіз мемлекеттер достастығы
ФТБ (ФБР) – Федералды тергеу бюросы
ЭЕМ – Электронды есептеу машинасы
ЭҮ – Электронды Үкімет
***.com,*.exe** – түрлі кеңейтілулі файлдар
0 және 1 – нөл және бір сандарынан тұратын екілік (бинарлы) сандар жүйесі

КІРІСПЕ

Қоғамның тарихында XIX ғасырдың соңы мен XX ғасырдың басынан бастап технологиялық революция феномені бастамасын тауып міне осы күнге дейін зымыраған қарқынмен дамып, адамзаттың өмірін таңғаларлық өзгеріске салып келеді. Бұл революция көптеген салдарға алып келді, ғылым сан түрлі бағыттарға ыдырап жаңа ғылым және ілім салалары туындады, осы сәттерден бастап автоматтандырылған технологиялар тоқтаусыз дамып өзгеріске түсе бастады. Соның ішінде байланыс құралдары мен есептеу машиналары пайда болды.

Есептеу машиналары бастамасын XX ғасырдың 50-60 жылдары алады. Алғашында ешбір қатер қауіпсіз әлеуметтік технологиялар қоғамға еніп кетті, бірақ тәжірибе көрсеткендей, кез келген жаңалық адамзат үшін тек пайдасын тигізе қоймай, кері әсерін де қалдырады. Пайда табу көзі бар жерде адамдар пайданы көптеп, кейде шексіз көргісі келеді, соның салдарынан заң нормаларын кесіп өту де туындайды.

Жаңа технологиялар тарихы өте ауқымды, соның ішінде қазіргі қоғамның міндетті қосалқы бөлшегі ол компьютерлік технологиялар. Компьютерлер қоғамның абсолютті түрде барлық салаларында бар десек аса қосып айтушылық болмас. Кез келген баспанада, қоғамдық орындарда, оқу орындарында, кітапханаларда, мемлекеттік мекемелерде, мұрағаттарда, жерде, әуеде, суда, жер астында болсын, космоста да, тіпті жеке адамның қалтасында, автокөліктерде, жалпы айтатын болсақ барлық жерде компьютерленген технологиялар кездеседі.

Компьютерлік қылмыстар ұғымы немесе қазіргі кезде айтатындай «киберқылмыстар» салыстырмалы түрде жаңа ғасырда пайда болды. Адамзат өмірі күнделікті үйреншікті жай өмір мен виртуалды өмірге бөлініп кетті. Адамдар арақашықтықты қысқартып үйренді, үйден шықпай-ақ жер көру, сөйлесу, көрісу, құжаттар жіберу, құпияларын айту, тіпті сатып алуды орындау қиынға түспеді. Осының барлығы жаңа азаматтық қатынастарды

алып келді, ал адам қатынасқа түскен жерде әрдайым қылмыс орнын тауып өтеді.

Ешкім компьютерлік сауаттылыққа теңдей ие емес, біреулер жаңа технологияларды жетік білсе, екіншілер базалық дәрежеде ғана пайдалана алады, үшіншілер мүлдем олардан алшақ. Сондықтан күштілер жоғарыда, ал әлсіздер төменде болады, біреулер осы қатынастардың субъектілері, екіншілері қолсұғушылықтың объектісі болады. Оларды қолсұғушылықтан тек «заң» қорғай алады. Ал заңның дамуы мен әмірі ғылымға тікелей тәуелді. Сол себепті біз ғылыми тұрғыдан осы мәселені қолға алып болашақта мемлекеттік органдармен заңнаманы жетілдіруге қатысты біріге жұмыс атқаруды тамамдаймыз. Ақпараттық қылмыстардың өзектілігі қазіргі таңда сөзсіз маңызды.

Қазақстан басқа мемлекеттер сияқты ғылыми техникалық революцияның жаңа келесі қадамына ауысып келеді, яғни техникалардың даму темпі өрбіген, ақпаратты автоматты түрде өңдеу, жаңа интеллектуалдық технологияларды жасау негіз болған ақпараттық қоғам орнап келеді. Аталған факторлар әлеуметтің, қоршаған ортаның мәдениеттік, саяси, құқықтық өмірінің түбегейлі өзгеруіне сөзсіз ықпал етеді. Соңғы жылдары көптеген мемлекеттер өздерінің басты мақсаты ретінде ақпараттық қоғамға көшу бағдарламаларын жасау мен концепцияларын жүзеге асыруды қойып отыр. Бұл осы мәселенің шындығында жер жүзін дүрсілкіндіріп отырғанын көрсетеді.

Тәуелсіз Қазақстан Республикасында саяси, экономикалық, жаһандық ғаламторлық әлемнің және әлеуметтік тұрғыдан дамуы, өркендеу процесі берік орын алды. Елімізде жылма-жыл алға өрлеушілік, дүниежүзілік деңгейге көтерілуге қадам басқандық айқын көрініс беруде. Мемлекетімізде құқықтық негіз берік орын алды. Осы аз уақыт ішінде Қазақстан Республикасы көптеген жетістіктерге жеткені бәрімізге анық, бірақ мемлекетімізде орын алып жатқан осындай оңды жетістіктерімізбен бірге қоғамның одан әрі серпінді дамуына кедергі келтіріп жатқан теріс құбылыстар да бар. Сондай қоғамға жат құбылыстардың бірі – қылмыстылық. Жалпы ақпараттық қылмыстылық басқа қылмыстарға қарағанда соңғы жиырма жылдыққа дейін көп кездесе бермеген факторлардың бірі, уақыт өте келе бұл мәселе қауіптілік дәрежесі жоғары қылмыстар қатарына бірте-бірте жақындап келеді. Бірақ та бұл тұрғыдағы қылмыстардың қоғамға қауіптілігі оның

латенттігіне байланысты, яғни мұндай қылмыстардың ашылуы, ресми тіркелуі көп қиындықтарды туғызады. Компьютерлік қылмыстардың ішіндегі көп кездесетіні компьютерге, оның құрылғыларына, компьютерлік жүйеге және желіге заңсыз кіру, зиянды бағдарламаларды шығару, енгізу және тарату заңсыз әрекеттері, ақпараттық-коммуникациялық жүйелерді, ондағы мәлімет пен ақпаратты талан-таражға салу, өзгерту, көшіру және жойып жіберу.

Алғашында батыс елдерінде дамуын алған бұл қылмыстар ТМД елдерінде де көрініс таба бастады, әлемдік елдермен қатар біздің мемлекетіміз де бұл мәселеге тойтарыс көрсету амалдарын жетілдіруге дайындық үстінде. Бұл қылмыстың өрбуі еліміздің экономикасына, сонымен қатар әлеуметтік факторларына теріс ықпалын тигізуде. Осы мәселемен күресуде мемлекетіміздің тәжірибесі жетіңкіремей, құқықтық мәселесі толыққанды жетілмей отыр. Бұл проблемамыздың бірден-бір себебі халқымыздың ақпараттық сауаттылығының төмендігі, құқыққорғау органдарымыздың тәжірибесі мен біліми дәрежесінің төмендігі, бұл мәселенің елімізге жаңадан келуі, глобалды желі субъектілері мен объектілері әлемнің кез келген нүктесінде болуы. Осы себептермен байланысты ақпараттық қауіптілік кез келген жерден төнуі мүмкін.

Жоғарыда айтып кеткендей, жаңа қоғамды ақпараттандыру жоғары ақпараттық технологиялар негізінде жасалатын жаңа қылмыс түрлерінің пайда болуына әкеп соқты. Бұл қылмыс құралдарының спектрі кең, ол жай үйдегі персоналды компьютерлерден бастап жоғары дәрежелі есептеу жүйелеріне дейін тараған. Мұндай саладағы қылмыстармен күресу мәселесі үлкен қиындық тудырып отыр, сол себепті бұл тақырып ашық тақырып және өте өзекті болып отыр.

Компьютерлік қылмыстарды жасаудың ерекшелігін ескере отырып, олардың аса латенттілігін атап кету керек. Олай дейтініміз, аталған қылмыстардың өздеріне тән ерекшеліктері бар. Біріншіден, ол қылмыстардың жасырын жасалуында, екіншіден, бір ғана компьютерлік (ақпараттық) қылмыстың өзі үлкен материалдық шығын келтіруі мүмкін. Үшіншіден, мұндай қылмыстар жоғары дәрежелі, жоғары білікті, білімді, тәжірибелі өз саласының мамандарымен жасалады.

Елбасымыз халыққа арнаған жолдауында экономикалық қылмыстылықпен күресуге көңіл бөлуге талап қойды. Біздің мақсатымыз қазіргі таңдағы ғылым мен қоғамның басты және өзекті аспектісі ретіндегі компьютерлік ақпараттық қылмыстармен күресудің криминологиялық және қылмыстық саясатты кешенді зерттеу және ұйымдастыру, сонымен қатар осы топтағы қылмыстардың криминогендік, жалпы және ерекше белгілерін қарастыру, шетелдіктердің тәжірибесі мен теориясын пайдалана отырып, зерттеулер жасап, өз еліміздің жағдайын саралап мүмкіндігінше жаңа тәсілдер енгізіп, қылмыстармен күресу, алдын алу амалдарын шығару, жалпы халықтың осы саладағы қылмыстарға қатысты көзін ашуға, ақпараттық сауаттылығын жоғарылату, мұндай қылмыстардан алшақ болу және қорғана білуді үйрету, құқық қорғау органдарына белгілі бір дәрежеде көмегімізді тигізу, қылмыстардан сақ болуды және аталған мәселелерді шешуге септігін тигізер басқа да сұрақтарды көтеру болып табылады.

1. АҚПАРАТТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРМЕН КҮРЕСУДЕГІ ҚЫЛМЫСТЫҚ САЯСАТ

1.1. Компьютерлік қылмыстылық пен киберқылмыстардың түсінігі және олардың жалпы сипаттамасы

Бүгінгі таңда Қазақстан қоғамы есептеу техникасы арқылы жасалатын аса қауіпті қылмыстармен кездеспеген.

Қазіргі заманның қоғамын информатизациялау, компьютеризациялау жаңа қылмыс түрін «киберқылмыстарды» тудырды. Олардың осылай аталу себебі қылмыскерлер қылмыс жасайтын кезде есептеу жүйелерін, байланыс және телекоммуникацияның жаңа құралдарын, ақпаратты алудың дыбыссыз электронды түрлерін, компьютерлерді және т.б. пайдаланады.

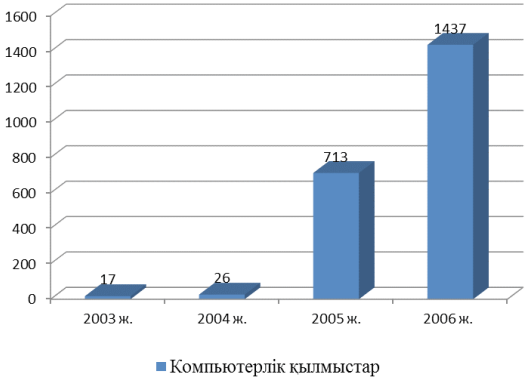
Қазақстан Республикасының Президенті Қазақстан халқына жолдауында «Киберщит» бағдарламасын қалыптастыруды және сандық Қазақстан саясатын жүргізуді Үкімет басшыларына тапсырған болатын [1].

Қоғам мен мемлекеттің әлеуметтік-экономикалық және мәдениеттік өміріндегі ақпараттық технологиялардың дамуының динамикасы ақпараттық қауіпсіздік мәселесін шешуге жоғары талаптарды қояды. Мемлекеттің ақпараттық қауіпсіздігін қамтамасыз ету ақпаратты алу, пайдалану саласындағы адам мен азаматтың конституциялық құқығы мен бостандығын жүзеге асыратын ұйымдастырушылық, техникалық, бағдарламалық, әлеуметтік механизмдері кешенді әдістерді қажет етеді, сонымен қатар ақпараттық қауіпсіздік саласындағы халықаралық қатынастарды дамытуды, саяси, экономикалық және әлеуметтік тұрақтылықты, заңдылықты және құқықтық тәртіпті, ҚР аумақтық тұтастылықты, конституциялық құрылымды, егеменділікті қажет етеді [2].

Біраз статистикаға көз салатын болсақ, ҚР Ішкі істер министрлігінің 2003 жылдың сәуір айында құрылған, құзыреттігі бойынша жоғары технологияларды қолданылып жасалған кибер-

қылмыстарды анықтау, жазалау және ашу болып табылатын «К» басқармасының қызметкерлерінің айтуынша, электронды есептеу техникаларын және ақпараттық технологияларды пайдалана істелетін қылмыстар саны өсіп келеді. Мысалы, егер 2003 жылда Республикамыздың ішкі істер органдарымен осы категорияға жататын 17 қылмыс пен құқық бұзушылық тіркелсе, 2004 жылда олардың саны – 26, 2005 – 713, ал 2006 жылда мұндай 1437 факті тіркелген (1-сурет).

Мұндай тенденцияның құрылуы, мамандардың пікірінше, адамдардың интернет желісін пайдаланумен, бұрынғы ТМД елдері мен Қытайдан келетін контрафакті өнім ағымының өсуімен, электронды техникаларға қондырғы ретінде пайда болып жатқан әртүрлі технологиялардың шығып, ел арасында тез тарауымен байланысты. Киберқылмыстардың өсуінің тағы бір себеп факторы адамдардың есепайырысуының ақшасыз түрінің дамып кетуі. Қылмыскерлер осы электронды түрде қаражат мөлшерін ұрлауды көңілсіз қалдыра алмайды, себебі жеңіл ақша табудың бір мүмкіндіктері пайда болып жатыр.



1-сурет – Статистикалық көрсеткіш (компьютерлік қылмыстардың динамикасы)

Киберқылмыскерлердің объектісі белгілі бір адам немесе тіпті белгілі бір адамдар тобы болуы мүмкін. Қылмыскерлер әртүрлі сайттар, көп жағдайда нәпсіқұмарлық сипаттағы сайттар жасап, жеңіл қылықты әйелдер ретінде суреттер мен телефон не ме-

кен-жайды көрсетіп адамнан керекті ақпаратты шығарып алады. Белгілі адамдар тобына қарсы жасалатын қылмыстарға төлеммен немесе басқа да бухгалтерлік операциялармен, қағаздармен автоматизацияланған компьютерлік жүйені пайдалана жұмыс жасайтын ұйымдар мен мекемелерге қатысты жасалатын киберқылмыстар жатады.

Ал кейбір лауазымды тұлғалардың айтуынша, Қазақстан үшін киберқылмыстардың зияны айтарлықтай төмен, себебі біздің қоғамда бұл мәселе шетелдегідей аса дамымаған. Бірақ аса бір маңызды мәселе ол сайттарда саясаткерлердің, нақты жеке тұлғалардың немесе басқалардың атын қорлау, жала жабу, атына кір келтіру. Барлық сайттар бізде бұқара ақпараттық құралдарға жатады, сондықтан мұндай сайттар шын мәнінде заңмен қудалануы мүмкін.

Бұрынғы Мәдениет және ақпарат министрінің айтуынша, оның ведомствосында болашақта Интернет сайттарды қадағалайтын концепция жүзеге асырылып жатыр. Жалпы халықаралық аренада 45 ірі елде Глобалды Интернет желісіне тотальды мемлекеттік бақылау жүйесі ұйымдастырылған. Ал Қазақстан бұл жолды таңдаған жоқ, себебі бұл авторитарлық мемлекеттің белгісі болып тұр, ал Қазақстан өзін, барлығымыз білетіндей, демократиялық, зайырлы мемлекет деп таниды. Бірақ мемлекет өз халқын Интернеттің жағымсыз жақтарынан қорғап қалу үшін оны қадағалап отырғаны дұрыс. Біз білетіндей, Интернет порнографиялық, қылмыстық, террористік және экстремистік байланыстар үшін жақсы ресурс болып табылады. Бұл мемлекеттер үшін Интернетті қадағалаудың бірден-бір басты себебі болған-мыс.

Прогресті ештеңемен тоқтату мүмкін емес. Адамзат қазір үлкен қарқынмен дамып жатыр. Кейде тіпті заңнама қоғамның дамуын реттеу үшін нормаларын қарастырып та үлгермейді. Компьютерлік ақпаратты Қазақстанның қылмыстық заңнамасында қылмыстық-құқықтық қорғау ҚР Қылмыстық кодексінің 7-тарауының 205-213 баптарында айтылған [3]. Ол «Ақпараттандыру және байланыс саласындағы қылмыстық құқықбұзушылықтар».

Компьютерлік қылмыстылықтың шегі жоқ. Ол халықаралық деңгейдегі ұғым болып табылады. Адам өміріне жаңа технологиялардың енуінен бастап, ақпараттармен алмасу тез, арзан және тиімді болды, сәйкесінше ақпарат саласындағы қылмыстар да

адам ұғымының шегінен асып барады, тіпті белгілі қылмыс түріне анықтама беру мүмкін емес.

Ғылыми-техникалық революция ағымы қоғамда маңызды әлеуметтік өзгерістер әкелді, соның ішінде басты қоғамдық қатынастар мен ресурстардың жаңа түрі – ақпараттық қатынастар. Олардың алғашқыда болған ресурстардан бірқатар ерекшеліктері бар: 1) олар тұтынылмайды және физикалық емес, моральдік қабылдауға жатады; 2) олар өз мәні бойынша материалды емес және белгілі физикалық кейіпті ала алмайды, тек арнайы физикалық тасығыштарда сақталады; 3) оларды пайдалану басқа ақпарат көздерін пайдалануды азайтады, соның арқасында уақыт пен құралдарды үнемдеуге жақсы мүмкіндік береді; 4) оларды жасау және пайдалану процесі ерекше жолмен, яғни компьютерлік техникамен жүзеге асырылады.

Ақпарат қазіргі заман қоғамының негізі болды, қоғам қызметінің пәні мен нәтижесі, ал оны жасау, жинау, сақтау, беру және жетілдіру процесі өз кезегінде оның өндірісінің құралдарын жетілдіру (электронды есептеу техникасы, телекоммуникация құралдары және байланыс жүйелері) прогресін тудырды.

Жалпы осының бәрі «жаңа информациялық технология» ұғымына кіріп кетеді. ЖИТ адам қызметінің әртүрлі саласындағы ақпараттық процестерді жүзеге асыру тәсілдері мен құралдарының, яғни адамның ақпараттық қызметін (оны басқаша ақпараттық жүйе ретінде қарастыруға болады) жүзеге асыру әдістерінің жиынтығы болып табылады. Басқаша айтқанда, ақпарат қоғамдық ақпараттық қатынастардың өнімі болады, сәйкесінше тауарлық белгілерге ие болып сату-сатыпалудың пәніне айналады [4].

Қоғамдағы жүріп жатқан ақпараттық процестердің нәтижесі болып жаңа әлеуметтік қатынастардың пайда болуы мен қалыптасуы немесе өзгеруі табылады. Мысалы, тіпті қазір дайындаумен, берумен және шарттық қатынастар көлемімен байланысты әртүрлі шарттық қатынастарды ғылыми-техникалық құжаттау жөнінде, бағдарламалық қамтамасыз ету, мәліметтер базасы және олармен жұмыс жасайтын басқару жүйесі жөнінде айта кетсе болады.

1974 жылы нарықта компактілі және салыстырмалы қымбат емес персоналды компьютерлердің пайда болуы шексіз тұлғалар шеңберіне мықты ақпараттық ағымдарға қосылуына мүмкіндік берді [5, 3 б.].

Бұл жерде ақпаратқа, оның сақталуына және сапалылығына қатысты қолжетімділікті бақылау туралы мәселе туындады. Ұйымдастырушылық шаралар және де қорғаудың бағдарламалық және техникалық құралдары толыққанды тиімді болмады.

Қазақстандық социумда компьютерлік техниканы қолдану арқылы жасалатын қылмыстар қоғамға беймәлім жат қылық, олар тек шетелдіктерге таным әрекет деген стереотиптік ой қалыптасқан. Бұл ойды жарым-жартылай дұрыс десек де болады, себебі еліміздің кейбір түпкірлерінде компьютеризация тұрмақ коммуникация түрлері, тіпті жай ғана ауыз су жүргізілмеген. Мүмкін сол себептен осы мәселеге қатысты ғылыми жұмыстардың тапшылығы түсіндіріледі. Бірақ соған қарамастан компьютерлік қылмыстар бізде оларға жеткілікті мөлшерде көңіл бөлетіндей дәрежеде кездесіп те жатады.

Осыдан 15-20 жыл бұрын компьютерлік қылмыстылықты Қазақстанда жоққа шығарса келісуге болатын-ды. Ал қазір ақпараттық жағдай мүлдем өзгеше, оған төменде бірнеше мысал келтіріп кетуге болады.

Мысалы, 2005 жылы шілде айында Қарағанды қаласының оқушылары «Нурсат» компаниясының серверіне хакерлік шабуыл жасаған. Шығын шамамен 260 млн. теңге көлемін құраған [6].

2011 жылдың 27 тамызында белгісіз хакер ҚР Батыс-Қазақстан облысы Ішкі істер басқармасының сайтын бұзған, хакердің жалған аты Ахмдаса (латын әріптерімен жазылған) немесе 2010 жылы түріктердің «Соғыс» атты хакерлік тобы Қазақстан Республикасы БҚО-ның ІІБ-ның, Облыстық соты және Облыстық прокуратурасының сайттарын бұзған екен [7].

Кез келген мемлекеттің ұлттық инфрақұрылымы бүгінгі күні жаңа компьютерлік технологиялармен тығыз байланысты. Банктік және энергетикалық жүйелердің күнделікті қызметі, көлік жүйелері, әуе қозғалысы тіпті медициналық жәрдем мен адамға қажетті күнделікті мұқтаждық қызметтері мен сервисі автоматтандырылған электронды есептеу жүйелерінің дұрыс және қауіпсіз жұмысына толық тәуелді. Қазіргі таңда жалпы қылмыстардың басты бөлігін жаңа технологиялармен байланысты жасалатын қылмыстар саны қамтып келеді. Оның тез дамып өсуіне тікелей қазіргі жаңа заманның негізгі бастамасы Интернет ғаламторымен тікелей байланысты және өнымен тең дәрежеде

күресуді жүзеге асыра алмай келе жатқан өкілетті органдармен және тиісті шаралардың жетіспеуімен байланысты.

Компьютерлік қылмыстар қазіргі кездің аса өзекті мәселелерінің бірі. Бұл мәселенің өзектілігі жылдан жылға адамдарды аса қауіппен мазалап отыр. Осыдан тіпті 3 жыл бұрын бұл мәселенің жағдайы басқа болды, 5 жыл бұрын одан өзгеше болды, ал 10 жыл бұрын компьютерлік қылмыстар адамзат баласын қазіргі кездегідей толғандырмаған десек артық болмас.

Болашақта жай ғана қатардағы адамның күнделікті өмірін компьютерлік технологияларсыз елестетіп көру де мүмкін емес, жаңа қоғамға жат құбылыс секілді. Мемлекеттердің компьютерлік қылмыстылықпен күресуге бағытталған шараларына қарамастан әлемдегі оның саны күрт өсіп келеді. Ресми емес мәліметтер бойынша Кеңес билігі кезінде ең алғашқы компьютерлік қылмыс 1979 жылы жасалған, зардап мөлшері 80 мың рубльге шыққан. 1997 жылға Ресей Федерациясында жоғары технологиялар саласында қылмыстар саны 300-ге жетеді, ал 2000 жылы тіркелген қылмыс саны 1300-ге барады. Украинада 2002 жылы 31 қылмыстық іс қозғалады, ал Қазақстанда 2000 жылдан 2008 жыл аралығында шамамен 2 мыңға жуық осы тектес қылмыстар тіркеледі [8].

Өзекті мәселе болып осы түрлі жай қолданыстағы персоналды компьютерлер мен телефондардан бастап қиын технологияларды пайдалану арқылы, техникалық құралдар мен әдістәсілдерді білетін жоғары білікті мамандардың қызметіне жүгіне отырып ұйымдасқан қылмыстарды жасайтын тұлғалармен күресу келеді. Қазіргі кезде жалған құжаттар мен жасанды ақша белгілері компьютерлік өңдеу мен перифериялық құралдардан шығару арқылы дайындалады. Бұның себебі жаңа техникалар мен технологиялардың кез келген тұлғаға қолжетімді болуы және жеңіл оларды пайдалануда. Жаңа техникалардың тез дамып, қоғамға енуінің жылдамдығына және адамдардың оларды теріс мақсатта пайдалану айласын табуы ағымына, қылмыспен күрес жүргізу сатыларының әрқашан бірнеше қадам арта қалуы жаңа ғасырдың үлкен кетігі болып отыр және бұл екі үрдістің осы жылдамдықта қозғалуы ұзақ уақыт өзгеріссіз болып тұр. Уақыт өте келе арақашықтық алшақтап келеді, оның пайдасы тек қылмыскерлердің қанжығасына байлануда. Компьютерлерді немесе желілерді пайдалану арқылы жасалатын қылмыстардың қаупі соншалықты

адам баласы оны көз алдына елестете алмайды. Жай ғана Интернет арқылы таратылатын ақпараттар мен зияткерлік шығармалар, авторлық және сабақтас құқық иегерлері зиян шегетін мөлшерді елестеткеніміз жеткілікті. Жасөспірім балалар порнографиясы мен лицензиялы өнімдердің контрафактілі көшірімдері қоғамға моральді және материалды шығын келтіреді. Бұл зиян мөлшері миллиондаған не миллиардтаған қаражат мөлшерінде есептеледі. Мұндай жағдайда қылмыскерді жауапқа тарту мүлдем мүмкін емес, себебі заңсыз ұсыныс жасаушы жердің нақты белгісіз бір нүктесінде орналасса, мысалға Бразилияның бір жерінде болсын, ал тұтынушы Казақстанда болуы мүмкін. Жаңа технологиялар мен глобалды Интернет желісі адам баласының қадағалауына және бақылауына бағынбайтын XXI ғасырдың, қоғамның, жеке тұлғаның іштей құртатын үлкен бір жауы. Мұндай зиянкестермен күресудің бір амалы болып барлық мемлекеттердің бірдей болып бірігіп, ынтымақтастық білдіре білгені болады. Қазіргі таңда көріп отырғанымыздай мемлекеттер арасында тек қана жанжал мен саяси қақтығыстар орын тауып отыр, оның бірден бір себебі терроризм мен экстремизм, саяси тұрақсыздық, бүкіләлемдік дағдарыс пен халықаралық аренада жер қойнауына күресу, сыбайлас жемқорлық, діни араздықтың дамуы, ал осының барлығының дамуының ең тиімді құралы – ол ИНТЕРНЕТ желісі.

Компьютерлік технологияларды экономикалық қылмыстар мақсатында пайдалану ол ақиқаттың тек бергі жағы. Сөзсіз компьютерлік қылмыскерлер қомақты қаржы соммаларын ұрлап жәбірленушіге аса үлкен шығын келтіреді. Бірақ, біздің ойымызша компьютерлік технологияларды пайдаланатын қылмыскерден туындайтын қауіп ол мемлекеттік қауіпсіздік. Хакерлер, яғни компьютерлік қылмыскерлер, соңғы кездерде жиі-жиі мемлекеттік органдарға, нақтырақ осы органдардың қызметтік сайттары мен мәліметтер базасын сақтайтын серверлерге ғаламтор арқылы немесе желіге жалғану арқылы жасырын шабуыл жасап келеді. Қылмыскерлердің ниеті экономикалық сипаттан саяси мәнге ие болды. Егер бұрын хакерлердің объектісі жеке тұлғалар, кәсіпорындар мен банктер болса, қазір олар жаңа қадамға ауысты. Бұл қылмыскерлердің мемлекеттік құзырлы органдардан бір бас жоғары тұрғанын және бір қадам алдыға ойлайтынын көрсетеді.

Ақпараттық революция мемлекетімізге қиын экономикалық және саяси кезеңде күрт басып кірді. Мемлекет тарапынан қолға

алынған шаралар тым кеш болғандай, қоғамдық қатынастарды реттейтін шаралар жүйесі әсерсіз қалды, енді дегенде жаңа нормалар кешені қажет болды. Қоғамның қатынасы жаңа технологиялық қатынастар аясына өтті, қатынастар арасында ақпаратық өнім пайда болды, түрлі қызмет түрлері пайда болды, ақпараттық қатынастар геометриялық прогрессия түрінде жан-жақта тарады. Ақпараттық қатынастар арқылы біз сауда-саттыққа түсеміз, ақысыз түрде (MP3, MP4, doc., vav, exe., adobe, avi, mkv, wmv, 3GP, JPG және т.б. форматтағы) шығармалар мен туындылар аламыз, зияткерлік қатынастар бұзылады, авторлық және сабақтас құқықтар бұзылады, порнографиялық өнімдер таратылады, жасөспірім балалардың психикасы бұзылады, террористер және экстремистер ешбір бақылаусыз сөз байласады, ұлтаралық және нәсілдік қақтығыстар интернет арқылы өрбіп барады, контрабанда жүзеге асырылады, наркотикалық тауарлар сатылады, мемлекетке опасыздық жасалады, қыздар тәнін сатады, алаяқтық еш кедергісіз жүріп жатады, ақпарат талан-таражға салынады, адамдардың ар-намысы мен абыройына кір келтіріледі, жалған ақпарат таратылады және осылар сияқты сан түрлі қылмыс түрлері ерікті түрде орындалып жатады.

Әсіресе заңсыз ақпараттық іс-әрекеттер мәселесі технологиялық және ақпараттық желілер жағынан жоғары дамыған мемлекеттер ішінде тез дамып келеді. Қосымша шараларға мәжбүр болған олар құқықтық және соның ішінде қылмыстық құқықтық қорғау шараларын қолданбақшы болды. Мысалы, шетел тәжірибесіне келетін болсақ, Францияның 1992 жылғы Қылмыстық кодексінде меншікке қатысты қылмыстар тарауы «автоматизациялаудан өткен мәліметтер жүйесін талан-таражға салу туралы» нормамен толықтырылған, онда автоматизациялаудан өткен мәліметтер жүйесіне толығымен немесе бір бөлігіне заңсыз кіру, осындай жүйенің дұрыс жұмыс істеуіне кедергі келтіру немесе жұмысын бұлдіру немесе алдау арқылы жалған мәліметтер енгізу, мәліметтер базасын өзгерту не жою туралы айтылған [9].

Бұл мәселеден халықаралық ұйымдар шет қалмады, әсіресе Европа Кеңесі компьютерлік ақпарат саласындағы құқықбұзушылықтар мәселесіне арнап, арнайы конвенция жобасын қарастырып оны ұйымдастыруды қажет деп тапты. Мәселен, Ресей құқықтанушылары ақпаратты автоматты түрде ұйымдастыру тәсілдерін қолдану саласына қатысты сауалды көтеру туралы

мәселені бұрыннан көтеріп келеді. Сөйтіп, Ресейде 1992 жылы «Электронды-есептеу машиналарының және мәліметтер базасының бағдарламаларын құқықтық реттеу туралы» заңы қабылданды [10].

Бұл заңда ЭЕМ үшін бөтен бағдарламаларды немесе мәліметтер базаларын өз атынан шығару не заңсыз тарату немесе айналымға шығару қылмыстық жауапкершілік тудыратыны туралы айтылған. 1994 жылы компьютерлік ақпаратпен байланысты бірқатар нормалардан тұратын Азаматтық кодекс, ал 1995 жылы «Ақпарат, ақпараттандыру және ақпаратты қорғау туралы» Федералды заң қабылданды. Компьютерлік ақпараттың қауіпсіздігін тудыратын құқықтық шарттар жүйесінің логикалық дамуын 1996 жылы дайындалған компьютерлік қылмыстар үшін жауапкершілік тудыратын бірқатар баптар тобы түсіндіреді.

Бұл заңда компьютерлік ақпарат ұғымына жақсы анықтама берілген. Ол бойынша, компьютерлік ақпарат болып ұсыну нысанына қарамай тұлғалар, заттар, фактілер, оқиғалар, құбылыстар және процестер туралы мәліметтер табылады. Бірақ компьютерлік ақпарат дегеніміз мәліметтің өзі емес, оның машина оқитын түріндегі формасы, ал біз білетіндей компьютерлерде мәліметтің барлығы екілік сан, яғни 0 және 1 сандары арқылы жүреді. Ол мәліметтер компьютердің сақтау бөлімінде, не тасымалдау құрылғысында (дискеттер, оптикалық, магниттік-оптикалық дискіде, магниттік лентада немесе басқа да материалдық құрылғыда) орналасады.

Электронды есептеу машиналарының бағдарламасы ЭЕМ және басқа компьютерлік құрылғылардың функционалды түрде жұмыс жасау үшін арнайы нәтижеге жеткізетін мәліметтер мен командалар жиынтығы. ЭЕМ (компьютер) – ақпаратты енгізу, онымен жұмыс жасау және шығару үшін арналған (бірнеше біріктірілген құрылғылар қосындысы) құрылғы немесе жүйе [11, 14 б.].

ЭЕМ желісі – компьютерлер жиынтығы, немесе байланыс каналдарының не құралдарының әр компьютердің оның орналасқан жеріне қарамастан есептеу және ақпарат ресурстарын пайдалануға мүмкіндік беретін жиынтығы.

Мәліметтер базасы дегеніміз – бұл ЭЕМ арқылы табылуы және барлануы мүмкін болатындай жүйеленген мәліметтер (мысалы: мақалалар, есептеулер, кестелер) жиынтығының объективті формада ұсынылған және ұйымдастырылған түрі.

Қылмыстың сан жағынан жылдам өсуі және сапасы жағынан өзгеріп отыруы қоғам өмірінің әртүрлі салаларындағы қарама-қайшылықтардың қозуы салдарынан болады. Оған бірден-бір себеп болатын құқыққорғау органдарындағы өзгерістер, заңнамадағы кемшіліктер, заңнаманың тұрақсыздығы, құқық-қолдану тәжірибесіндегі жетілмеген қателіктер, осының барлығы компьютерлік қылмыстылықтың әлеуметтік құбылыс ретіндегі даму процесін жылдамдатуға әсерін тигізеді.

Ақпаратпен жұмыс жасау технологиялар саласында заңнама көп жағдайда техниканың даму процесінен бірнеше қадам артта қалып отырады. Ал құқыққорғау органдарында осыған қатысты мамандарды дайындау мүлдем артта қалып және осы таңда жаңа қылмыс түрлерін табу мен ашуда ешбір септігін тигізе алмай отыр. Ұйымдасқан қылмыс әлемі мен олардың кәсіби өсуінің арасындағы байланыс пен оларға қарсы күрес жүргізетін ішкі істер органдарының қызметкерлерінің біліктілігі және дайындық дәрежесі қылмыспен күресуде нәтижеге және сапалы сипатқа әсерін тигізеді. Компьютерлік қылмыстармен күресудің тиімділігін көтеретін факторлардың бірі оперативті-тергеу қызметкерлердің кадрлік құрамының жағдайы, яғни олардың ішкі кәсіби ядросы, жоғары дәрежелі мамандардың жетіспеуін толтыру.

Соған қарамастан, мамандардың қазіргі заманғы прогрестің дамуымен байланысты электрондық, компьютерлік қылмыстың өсуі және дамуы жөніндегі пікірі бойынша қылмыс және қылмыс түрлері өте жоғары қарқынмен өсуде. АҚШ-тың ФТБ (ФБР) мәліметтері бойынша компьютерлік қылмыскерлерге АҚШ территориясында ғана қылмыспен айналысып отырғандарға осы күні көпұлтты ұйымдардың кез келген кодтары мен коммерциялық құпияларына кодтарын бұзып заңсыз кіруіне қиынға түспейді. Осының салдарынан бізде, Ресейде және басқа шет елдерде компьютерлік технологияларды пайдалану арқылы банкілік транзакциялар жүзеге асырылады, яғни көптеген миллион долларлар қылмыскерлермен арнайы күні бұрын жасалатын шоттарға үлкен ұйымдардан аударылады. Мысалы, сонау 1991 жылы ғана Кипр аралына Ресейден 2,6 млрд. АҚШ доллары осындай жолмен келіп түскен. Мамандардың айтуынша, не ФБР, не басқа арнайы қызмет түрлері байқамай қалатын ай сайын мұндай мыңдаған операциялар жүргізіледі [12, 5 б.].

Тұтас алғанда қазіргі заманғы ақпараттық технологияларды криминалдық пайдалану компьютерлік қылмыстылықты тек пайдалы ғана емес, тіпті қауіпсіз іс ретінде көрсетеді. Сол себептен БҰҰ-ның қылмыстылық жөніндегі комитеті бұл мәселені терроризм және есірткі бизнесі сияқты аса ауыр қылмыстар қатарына қояды.

Ақпараттық қылмыстар жөніндегі мәліметтер үзілмелі болып келеді. Соған байланысты қазіргі кезде ешкім ақпараттық қылмыстарды толығымен ашып бейнелеп бере алмайды. Осындай шабуылдарға ұшыраған мемлекеттік және коммерциялық ұйымдар өздерінің қорғаныс жүйесі мен келтірілген шығындарын тергеуден жасыратыны белгілі. Сондықтан көп жағдайларда тергеуге қажетті мәліметтер жарыққа шықпайды.

Мысалға, Италияда 1993 жылы компьютер арқылы банктерден 20 млрд. лира ұрланған екен. Францияда жылына осы қылмыстардан келтірілетін шығын 1 млрд. евро шамасында болады және жыл сайын осындай қылмыстар саны 30–40 пайызға өсуде [13, 12 б.].

Германияда компьютерлік мафия жылына 4 млрд. дейін ақша соммасын ұрлап отырған. Американдық компьютерлік қылмыстар жөніндегі ұлттық ақпараттық орталықтың мәліметтері бойынша тіпті сол 1988 жылдың өзінде компьютерлік қылмыстардан американдық фирмаларға 500 млн. доллар көлемінде шығын келтірілген. Сонда қазіргі кезде материалдық шығын бірнеше есеге өсіп отыр. Ал жалпы алғанда (ең төменгі есеп бойынша) компьютерлік қылмыстардан Европа мен Америка елдерінде келтірілген шығын ондаған миллиард долларды құрайды. Соның өзінде осындай қылмыстардың тергеушілерге мәлім болатыны тек 10%, қалған 90%-ы жасырын түрде қалады. Бұл компьютердің дамыған елі болып табылатын, мұндай қылмыстармен күресуге тәжірибесі мол Американың өзінде. Ең алғаш осындай сипаттағы қылмыс Америкада 1966 жылы байқалған болатын. Ал Ресейде «электронды тәсілдерді пайдалану арқылы жасалатын талан-таражбен күресу жөніндегі бөлімше» тек 1997 жылы Ресей Федерациясының Ішкі істер министрлігінің экономикалық қылмыстар бойынша бас басқармасында құрылған болатын. Онда бар-жоғы 4 адам ғана жұмыс істейтін.

1991 жылы Ресейдің Сыртқыэкономбанкінен 125,5 мың АҚШ доллары ұрланған екен. Қылмыскерлер сол банктің есеп-

теу орталығының қызметкерлері болып шығады. Олар жасанды құжаттарды жасап, жалған паспорт бойынша жеке шоттар ашып, қаражат мөлшерін аударып отырған [14, 156 б.].

Ақпараттық қылмыстарға тек ақша-қаражат мөлшерін ұрлау ғана жатпайды, оған құпия болып табылатын немесе жәбірленушіге, оның жұмысына зиян тигізетін кез келген ақпарат түрін жасырын көшіру, бүлдіру немесе көшіріп алу да жатады. Мысалы, 1992 жылдың жазында бір шетелдік алмаз концерннің өкілі өз дискетілеріне Ресейдің алмаз өндіру ұйымының компьютерлер желісінен қызметтік құпия болып бағаланған мәліметті көшіріп алған.

Ресей Федерациясы Орталық банкі шабуылдардың санының өсуіне байланысты қорғану әрекеттерін күшейтіп, 1994-1996 жылдары арасында компьютерлік жүйеге қаражат мөлшерін алу үшін 300 заңсыз енуді және шабуылдарды анықтап алдын алған болатын.

1996 жылдың көктемінде қылмыскерлер Москваның банктік компьютерлік жүйесіне Москваның жинақтаушы банкі реквизиттерімен жасанды вексельдерді енгізіп, 375 млрд. ресей рублі мен 80 млн. АҚШ долларын талан-таражға салмақшы болған [15, 1-тарау].

Компьютерлік қылмыстылық – ол тек қана ақша ұрлау емес, ол электронды вирустармен байланысты заңсыз әрекеттер, яғни пайда көру мақсатынсыз біреуге қомақты зиян келтіру мақсатындағы іс-әрекеттер. Ай сайын зиянкестермен вирустың 2-10 жаңа түрі шығарылып отырады екен.

Вирустардың қауіптілік дәрежесінің жоғарылығын дәлелдеудің бірден бір дәлелі Литва прокуратурасы қозғаған қылмыстық іс. Ол кезде электрондық вирус Игналинсктің Атомдық электро жүйесінің компьютеріне енген болатын, сол себептен бүкіл қорғау жүйесі бұзылған еді. Сәл болғанда АЭС-сы екінші Чернобыль атағына ие болатын еді.

90-жылдардың аяғында Америка Құрама Штаттарында Компьютерлерді қорғау Институтымен бірге ФБР (федералды тергеу бюросы) зерттеу жүргізді. Оған 428 ұйым қатысты. Олардың 42% ақпараттық шабуылдың қандай да бір түрін немесе басқа да компьютерлік жүйелерді заңсыз пайдалануды 12 ай ішінде байқаған екен.

Мәліметтерді санкциясыз өзгерту көбіне медициналық және қаржылық ұйымдарда кеңінен байқалған екен (37% – мед. ұйымдар, 21% – қаржылық ұйымдар).

Жүргізілген сауалдан мынаны байқаймыз:

Ұйымдардың 50%-нан астамында желі арқылы шабуыл кезінде қорғануды жүргізетін жобасы мүлдем жоқ;

60%-дан астамында азаматтық немесе қылмыстық істер бойынша соттық қарауды ары қарай жүргізу үшін дәлелдемелерді сақтап қалу стратегиясы жоқ.

70%-да олардың коммуникациялық және ақпараттық жүйесіне шабуыл жасауды ескертетін құрылғылары жоқ.

17%-ы ақпараттық жүйеге шабуыл жасалғанда құқық қорғау органдарына хабардар ететіні жайлы айтқан.

70%-дан астамы құқыққорғау органдарына жүгінбеу себебін антижарнама деп көрсетті, яғни олардың атағына кері әсерін тигізетінін айтты [16].

Келтірілген мәліметтер компьютерлік қылмыстардың өсу тенденциясын сипаттайды және осыған қатысты мемлекеттің тез арада әрекет етуінің қажеттілігін көрсетеді.

Осы уақытқа дейін компьютерлік қылмыстарды біз тек батыс елдерінде болатын құбылыс ретінде қабылдадық. Компьютеризацияның біздің қоғамда төмен болуы ақпараттық қылмыстарға күдікпен қарауға қажет емес көзқараспен қабылданды. Тек соңғы жылдары ғана компьютерлік қылмыстармен күресу проблемаларына қатысты жұмыстар пайда бола бастады. Негізінен ол ресейлік жұмыстар қылмыстық-құқықтық, криминологиялық және криминалистикалық аспектілер жағынан қарастырылып келеді.

Алғаш компьютерлік қылмыстылықпен күресу мәселелері туралы Ресейдегі құқықтық ғылым ресми түрде тек 1992 жылы «Криминалистика және компьютерлік қылмыстылық» семинарларын ашу сәтінен бастап жариялаған болатын.

Компьютерлік қылмыстылықтың нақты анықтамасының болмауы осындай қылмыстармен айналысатын құқық қорғау органдарына олармен толыққанды күресуіне мүмкіндіктерін азайтады.

Компьютерлік қылмыстарды шартты түрде екі үлкен категорияларға бөліп көрсетуге болады: біріншісі – компьютерлердің жұмысына араласумен байланысты жасалатын қылмыстар, екін-

шісі – компьютерлерді және олардың қосалқы перифериялық бөлшектерін қылмысты жасаудың қажетті техникалық құралы ретінде пайдалану немесе қылмыс жасаудың амалы және қылмыстың жалпы құралы ретінде қолдану арқылы жасалатын қылмыстар.

Бұған біз компьютерлер маңында жасалатын қылмыстарды киргізбейміз, олар мысалы, програмистердің авторлық құқығын бұзу, есептеу техникасы арқылы жасалатын заңсыз бизнес, компьютерлерді мүлік ретінде жою және т.б.

Компьютер жұмысына араласумен байланысты істелетін қылмыстардың өзін бірнеше түрге бөліп көрсетуге болады, олар:

1) компьютерде сақталған ақпаратқа заңсыз кіру. Заңсыз кіру әдетте, бөтен атты, техникалық мекендерді өзгертіп, пайдалану арқылы жүзеге асырылады. Кейде біреу жұмыс жасап кеткеннен кейін сақталған мәліметке кіру, мәліметтерді тасымалдаушы құрылғыларды ұрлау, тасымалдау операциялары жүріп жатқан кезде қосымша аппаратураларды жалғау арқылы да жүзеге асырылады.

Мұндай жағдайда заңсыз кіруші өзін заңды пайдаланушы ретінде көрсетіп компьютерлік жүйеге кіреді. Адамды физиологиялық сипаттамалары бойынша, саусақ іздері байынша, көз сетчаткасы немесе даусы бойынша және т.б. ерекшеліктер бойынша анықтай алмайтын жүйелер бұл әдіске қарсы төтеп бере алмайды. Оның ең оңай жолы заңды пайдаланушылардың кодтарына немесе идентификациялық сандар жүйесіне ие болу.

Заңсыз кіру компьютерлік жүйенің бұзылуы нәтижесінде де жүргізілуі мүмкін. Мысалы: жүйе істен шыққан сәтте кейбір файлдар ашық қалған болса, ол файлдар кез келген жүйені пайдаланушыға желі арқылы ашық болғаны. Желіде ол былай көрінеді: банк клиенті өзінің сақталған бөлмесіне кіргенде оның бір қабырғасы жоқ болып шығады, сол жоқ қабырға арқылы ол көрші орналасқан бөлмедегі барлық бөтен құндылықты ұрлай алады;

2) бағдарламалық қамтылған жүйелерге логикалық бомбаларды енгізу, олар белгілі бір шарттарды орындаған кезде іске қосылып, компьютерлік жүйені бөлшектеп немесе толығымен істен шығарады;

3) компьютерлік вирустарды жасау және оларды тарату.

Троялық ат. Оның мәні осы программаның барлық мәліметтерін жойып, келесі бағдарламаға ауысу, содан соң оның мәліметтерін жою, сөйтіп келесісіне көшу. Бұл вирус нақ кәдімгі вирус

сияқты жұқпалы түрде тарайды, яғни ол коммуникациялық желілер арқылы бір жүйеден екінші жүйеге ауысу қасиетіне ие;

4) бағдарламалық есеп жүйелерін жасау, дайындау, ұйымдастыру, орнату кезіндегі ауыр салдарға әкелген қылмыстық салақтық.

Бұл жерде абайсыздық мәселесі орын алып тұр. Компьютерлік техника саласындағы абайсыздық салдар басқа техника, көлік құралдарын пайдалану кезіндегі абайсыз келтірілген зардаптар құрамымен, оның кінәсімен сәйкес келеді.

Компьютерлік абайсыздықтың басқа абайсыздықтардан ерекшелігі жалпы қатесіз компьютерлік бағдарламалар болмайды. Егер кез келген техника саласындағы жобаны үлкен сенімділікпен орындауға болса, программалау саласындағы мұндай сенімділік тек шартты түрде не болмаса мүлдем болмайды;

5) компьютерлік жалған ақпаратты жасау.

Бұл компьютерлік қылмыстың түрі басқаларына қарағанда кейінірек шыққан. Ол заңсыз кірудің ерекше түрі болып табылады, өйткені заңсыз кіруде пайдаланушы бөтен адам болса, ал бұл жерде пайдаланушы жоғары біліктілігі бар осы бағдарламаны жасаушы адам болады.

Қылмыстың негізі жалған мәліметтер, бағдарламалар жасап тапсырушыға оны сату, өндіру немесе дұрыс істемейтін өнімді өткізу. Кей кезде жалған мәліметті сайлау, дауыс беру, компьютермен белгілі нәтижелерді шығару және көптеген басқа есептеу технологияларымен жұмыс істеу кезінде кездестіруге болады;

6) компьютерлік ақпаратты ұрлау.

Компьютерлік ақпаратты ұрлауды қылмыстық кодекстегі басқа ұрлау құрамдарымен ұқсастыруға болмайды.

Егер де жай талан-таражға салу қылмыстары қолданыстағы қылмыстық заңнамамен толыққанды шешілсе, ал ақпаратты ұрлауға қатысты туындайтын мәселелер жағдайы өте күрделі. Бізде бағдарламалық қамсыздану шын мәнінде тәжірибеде ақпараттарды ұрлау немесе ұрланған бағдарламалармен алмасу арқылы жүзеге асып жатыр. Кімде кім лицензиялы бағдарламаларды арнайы фирмаларға барып рұқсатпен сатып алып жатқан жоқ, оның бәрі бір-бірінен көшіріп алу, сұрап алу т.б. жолдармен тарауда. Ол дегеніміз қылмыстық жауаптылық туғызады, сәйкесінше барлық көшіріп алғандарды жауапқа тарту, ол мүмкін емес жағдай екені бізге түсінікті. Сондықтан компью-

терлік ақпаратты қылмыстық құқықтық қорғалу объектісі екенін біз халық санасына жеткізуіміз керек және қылмыстық құқық ғылымында оған жеке пән ретінде қарауымыз керек.

Қоғамның компьютеризациялануы компьютерлік қылмыстар санының жылдам өсуіне әкеліп соғады, сонымен қатар уақыт өте компьютер арқылы ұрланып отырған ақша соммасы жай ақша ұрлау, тонау және т.б. қылмыстардан барған сайын асып барады. Бір ғана мемлекетті алып оған компьютер арқылы келтірілген шығынын қарасақ, бір минут ішінде ғана шығын қомақты болуы мүмкін. Мысалы, жоғарыда бір айтылып кеткендей, Мәскеулік сотпен қарастырылған қылмыстық іс бойынша Кеңес Одағының Сыртқыэкономбанкінен 125,5 мың АҚШ доллары ұрланған және сонымен қоса 500 мың доллар әлі де ұрланбақшы болған.

Осы қылмыстарды сипаттама беретін тағы бір мысал, 1995 жылдың қыркүйек айында аса ірі көлемде ақша-қаражат мөлшерін Ресей Орталық банкінің (Центральный банк России) Бас есепкассалық орталығынан ұрлауға оқталу болған, олар 68 309 768 000 ресей рублін алмақшы болған [17].

АҚШ-тың Бақылау Палатасының (Government Accountability Office) мәліметтері бойынша 2005 жылы компьютерлік қылмыстар АҚШ-тың экономикасына $67.2 млрд. шығын келтірді. Салыстыру үшін АҚШ-тың заңды және жеке тұлғалары бір жылда Интернетке кетірген ақша соммасын келтірейік. Бір ғана 2006 жылы ол сомма $102 млрд. құрады. Компьютерлік криминал барған сайын қауіпті болып келеді.

АҚШ-та «компьютерлік қылмыс» (cybercrime) ұғымы көп мағыналы. Ол бөтен компьютерді немесе компьютерлік желіні бұзу болуы мүмкін (көбінесе хакерлер айналысады). Ол Интернетті қолдану арқылы алаяқтық жасау не құнды ақпаратты ұрлау болуы мүмкін, ол зияткерлік меншікті талан-таражға салу (мысалы: әуендер мен видеоларды заңсыз көшіру), компьютерлік вирустарды, спамды тарату және т.б. болуы мүмкін. Компьютерлік қылмыстардың категориясына тағы да педофильдер және басқа да тән құмар қылмыскерлер санаты жатады.

Федералды Тергеу Бюросының (ФБР/FBI) бағалауы бойынша компьютер қылмыскерлерді күштірек жасайды. Компьютер арқылы олар мысалы, жәбірленуші жақпен тікелей байланысқа шықпайды, мемлекет аралық шекараны қысқартады. Информациялық технологиялардың дамуы біруақытта мыңдаған

және миллиондаған адамдарға шабуыл жасауға мүмкіндік береді және ең бастысы қылмыскерлер анонимді болып қала береді.

Бақылау Палатасының айтуынша, компьютерлік қылмыстар әртүрлі мақсатқа ие, сондықтан шын мәнінде шығындарды есептеу қиынға түседі. Мысалы, түрлі террористік, экстремистік топтар осындай әдістерді өздерінің қаржылық операцияларын жүргізу үшін пайдаланады.

Бақылау Палатасының бағалауы бойынша, АҚШ-та компьютерлік қылмыстармен күрес белсенді түрде жүріп жатыр, бірақ күрес өте ауырға түсіп жатыр. Бұл мәселенің бір проблемасы кадрлік мәселе: жоғары дәрежелі мамандар материалдық себептерге байланысты көбінесе мемлекетке емес жеке компанияларға жұмыс істейді [18].

Компьютерлік қылмыстардың бір қызығы зардап шеккен жәбірленуші қылмысты ашуда және қылмыскерді ұстауда өзінің ынтасын, қызығушылығын білдірмейді, ал қылмыскер, егер ұсталса, қылмысты жасағанын сол мезеттен мойындайды, яғни өзін жарнама (PR) ретінде ұсынады, қылмысты кім жасағаны ел құлағына жетсін дейді. Қылмыстық кодексте осындай ерекшелігі бар басқа қылмыс түрлері кездеспейді. Оның себебі неде? Қылмыскер мен жәбірленушінің бұл әрекеттері немен түсіндіріледі?

Біріншіден, компьютерлік қылмыстың жәбірленушісі қылмысты ашуға және оның жариялы болуынан кететін шығын оған қылмыс барысында келтірілген шығыннан асып кететініне сенімді.

Екіншіден, қылмыскер максималды бас бостандығынан айыру мерзімін (кейде шартты түрде) алғанның өзінде бизнес немесе қылмыстық ұйымдар арасында аты тарап, сұраныс иесі болады, немесе бас бостандығын айыру орнынан шыққаннан кейін ұрланған қаражатты пайдаланбақшы боламын деген оймен болады.

Соған қарамастан қазіргі кезде ғылымда компьютерлік қылмыстың ұғымына, түсінігіне қатысты нақты анықтама жоқ, тек оны топтастыруға қатысты әртүрлі пікір ойлар бар.

Бұл ұғымдарды беруде қиын жағы, біздің ойымызша, осы қылмыстардың бір объектісін көрсету мүмкін еместігінде, сонымен қоса қылмыстың құқықтық қорғау жағынан алғандағы заттардың көп еместігінде болып отыр.

Шын мәнінде екі негізгі ғылыми ой ағымы бар. Зерттеушілердің бір бөлігі компьютерлік қылмыстарға компьютер не объект, не қылмыс құралы болатын әрекеттер түрін жатқызады. Ал екінші топтағы ғалымдар компьютерлік қылмыстарға тек ақпаратты автоматизациялық өңдеу саласындағы заңға қайшы әрекеттерді жатқызады. Олар саралау үшін басты белгі ретінде ерекшеленген топқа жатқызуға мүмкіндік беруді, әдістердің, құралдардың, объектілердің жалпылығын жатқызады. Басқаша айтқанда, қол сұғудың объектісі болып компьютерлік жүйеде өңделетін ақпарат саналады да, ал компьютер қол сұғудың құралы болады. Көп елдердің заң шығару қызметі осы жолмен дами бастады.

Қылмыстық құқық, криминалистика ғылымдарында қылмыс материалдық тұрғыдан қаралғандықтан, кез келген қылмыстың мәні материалдық, әлеуметтік, идеологиялық құндылықтарға қатысты адамдардың байланысын, қылмыстық-құқықтық нормалармен қорғалатын қоғамдық қатынастарын өзгертуде, бөлуде көрініс табады.

Сәйкесінше, қылмыстық қол сұғушылықтың объектісіне қатысты екі пікірдің болуы мүмкін емес. Әрине бұл жерде объект болып, мүлтіксіз, ақпарат танылады, ал қылмыскердің іс-әрекетін қоғамның ақпараттық қарым-қатынастарына қол сұғу деп таныған жөн.

Бұл қылмыстардың субектісі жалпы да және арнайы да болуы мүмкін. Негізінен компьютерлік, ақпараттық қылмыстар қасақаналық кінәмен жасалады, бірақ абайсыздық қылмыстарын да жоққа шығаруға болмайды. Осы жөнінде зерттеу жұмысының нақты осы тақырыпқа қатысты бөлінген бөлімінде толығырақ айта кетеміз. Ал қазір компьютерлік қылмыстардың ұғымына қайта оралсақ, осы саланы зерттеген ғалымдардың пікірлерін қарастырайық.

Мысалы, А.В. Дуловтың пікірінше, компьютерлік қылмыстарға компьютерлердің жұмысын бұзумен байланысқан компьютерлердің көмегімен жасалатын түрлі қылмыстық әрекеттер [19, 3-4 б.].

Біздің ойымызша бұл анықтама компьютерлік қылмыстылықты нақты түсіндіре алмайды, өйткені компьютерлік қылмыстың жасалуына олардың жұмысының істен шығуы немесе бұзылуы міндетті шарт емес, қоғамға қауіпті нәтиже компьютерлердің немесе олардың бағдарламалық қамтамасыз ету жүйесі мен желіле-

рінің дұрыс жұмыс жасау кезінде де туындауы мүмкін. Мысалы, компьютерлік алаяқтық, мәліметтер жиынтығын ұрлау, жасырын көшіру, заңсыз кіру және т.б. қылмыстар кезінде компьютерлердің қызметі бұзылмайды.

Ал Н.А. Селиванов компьютерлік қылмыстар ретінде қылмыстың пәні ретінде компьютерлік ақпаратты немесе қылмыстың құралы болып табылатын электронды есептеу техникасын пайдаланатын басқа объектілерге заңсыз қол сұғу мақсатындағы әрекетті таниды [20, 37 б]. Бұл пікірге қарсы ой айтқан В.В. Крылов «жалпы компьютерлік қылмыстар ұғымын шектемей, компьютерлік техника құралдарымен байланысты ақпараттық қатынастар аясында жасалатын қылмыстық әрекеттердің жиынтығын криминалистік тұрғыдан компьютерлік қылмыстар деп түсіне білген дұрыс» деп көреді [21, 50-64 б.]. Оның ойынша, компьютер ол ақпараттық қатынастардың тек құралы ғана, және бұл құралды қылмыс жасау кезінде қолдану немесе қолданбау құпиялы құжаттандырылған ақпаратты ұрлауда, көшіруде және бұзуда ешқандай рөл атқармайды.

В.В. Крылов компьютерлік қылмыстардың базалық ұғымы ретінде ақпараттық қызмет саласындағы құқықтық қатынастар жүйесін нақты бір техникалық құралдардан бөліп көрсету нұсқасын қарастыруды ұсынады. Ол мынадай қорытындыға келеді: Қылмыстық кодекстің ерекше бөліміндегі компьютерлік ақпарат саласындағы қылмыстар ақпаратты өңдеудің ортақ құралымен, яғни компьютермен, біріктірілген ақпараттық қылмыстардың бір бөлігі болып табылады.

Ю.М. Батурин компьютерлік шабуылдың объектілерін үш категорияға бөліп көрсетеді: бірінші, компьютерлердің өзі, екіншісі, компьютерлер шабуыл құралы болып қолданылатын қылмыс объектілері және соңғысы компьютерлердің айналасындағы болатын объектілер [22, 9 б.]. Бірақ осы топтастыру бойынша бірінші категориядағы объектілерді компьютерлік қылмыстардың объектілері қатарына кіргізбеген жөн болады, себебі бірінші жағдай бойынша, компьютерлер тек мүлік ретінде, азаматтық құқықтық қатынастардың кез келген объектісі сияқты тек материалдық зат, игілік, мүлік сияқты қабылдануы тиіс. Біз материалдық құндылықты тек қана оның атауы бойынша ғана басқа бір ерекше категория ретінде көрсетпеуіміз керек.

Сол сияқты классикалық көзқарасты Н.Ф. Ахраменка ұстанады, яғни компьютерлік қылмыстардың шегін электронды есептеу машиналарын қылмыстың қаруы немесе құралы ретінде және қылмыстық шабуылдың пәні ретінде пайдаланумен көрсетуге болады. Соны айта тұра, компьютерлердің өздерін компьютерлік қылмыстардың заты ретінде қарастыруға болмайтынын көрсетеді. Себебі осындай қылмыстарды жасау барысында қылмыстың заты не пәні болып техника немесе техникалық құрал табылмайды, шын мәнінде зиян келтірілетін оның ішіндегі сақталатын, өңделетін немесе көшірілетін ақпараттық мәліметтер қылмыстың заты болып есептеледі. Зиян компьютерге емес компьютердің ішіндегі интеллектуалды мәліметтер жиынтығына келтіріледі.

Осыдан байқайтынымыз, компьютерлік қылмыстардың пәнін кең мағынада қарастыру керек: ақпараттан басқа пәннің ішіне есептеу машиналарының және ақпараттық үдеріс ағымдарының дұрыс жұмыс істеуін кіргізу керек.

Аталған бұл пікірлердің барлығы сөзсіз орынды, бірақ біз компьютерлік қылмыстар мен жоғары ақпараттық технологиялар саласындағы қылмыстар арасындағы байқалмайтын шағын ғана шекараны айыра алуымыз керек. Көптеген қазақстандық, ресейлік және басқа шетелдік ғалымдар компьютерлік қылмыстар деген терминді осы жоғарыда аталған ұғымдардың барлығына теңдей қолданып, өзге тұлғаларды да сол талқылаумен келістіріп қойды. Бірақ бұл жалған ойлар компьютерлік қылмыс атты ұғымды жекеден жалпылыққа итермелеп, оны тек шартты сипаттағы ұғым ретінде қалыптастырып келеді.

Қоғамда жаңа көптеген ағымдар мен ұғымдар пайда болып жатыр, ал отандық заңнама мен ғылым өзгеріссіз сол бір компьютерлік қылмыстардың айналасында жүр. Социумда жаңа қауіп түрі оның мәнін, түсінігін ашатын терминологиялар мен анықтамалардан жат.

Ал бұл дегеніміз құбылыстарды дұрыс ұғынбау және нәтижесінде оларды әдістемелік дұрыс қолданбау көптеген жағымсыз салдарға алып келеді. Ал заң кез келген салада немесе ортада болсын тек нақты анықтаманы, нақты шектілікті, нақты саралауды және нақты орындалуды қажет ететін феномен, егер осы шарттар орындалмаса, қоғам, мемлекет, жеке адамдар және заң шығару мен заң қолдану институттары үлкен зиян мен шығын шегеді.

Біздің ойымызша, жоғарыда аталған терминдердің ортақ мәселесі ол ақпараттық қауіпсіздік, сол себепті осы екі ұғымды басқа да ақпараттық қауіпсіздіктің құрамына кіретін ұғымдармен бірге бір үлкен біртектес қылмыстық заңнаманың бөліміне немесе тіпті тарауына шоғырландырған дұрыс. Ал кейін қоғамдық талаптарға сай жаңа ғылыми-технологиялық жетістіктердің пайда болуына орай тиісті қоғамға қауіптілік туындаған кезде осы тарауға қосымша ретінде енгізіп отыруға болады.

Ақпараттық қауіпсіздік мәселесі шын мәнінде көкейтесті мәселелер арасынан орын тауып отыр және уақыт өте келе қоғамның мәліметтерді өңдеу мен таратуға қатысты барлық салаларына терең еніп бара жатыр. Қорғаныс алаңынан қылмыстық-құқықтық объектілер ішінен басқа да қорғаныс пәндерін ұмытпауымыз жөн. Сол себепті компьютерлік қылмыстылықты құрайтын ақпараттық қылмыстар жиынтығына компьютерлік ақпараттық қылмыстар мен компьютерлік техника құралдарының ішіндегі ақпараттар мен мәліметтерден басқа компьютерлерде сақталатын мәліметтердің авторларының құқығы, түрлі компьютерлік бағдарламалардың жұмысы мен олардың авторлары, және лицензияны қажет ететін (яғни, оны сатып алатын тұлғаның материалдық шығыны немесе нақты қаражат мөлшері) жүйелік бағдарламалар, бағдарламалық қамтамасыз ету, операциялық жүйелер, видео-, аудио-ойнаушылар және өнімдер, компьютерлік лицензиялы ойындар, серверлік басқару жүйелері және т.б. кіруі тиіс, себебі бұл компьютерлердің барлық қоғамдық қарым-қатынас шегіне тарауымен шартталады.

Тәжірибеде компьютерлік ақпараттың қауіпсіздігіне қарсы жасалатын қылмыстар мен компьютерлерді қылмысты жасаудың құралы ретінде қолдану арқылы жасалатын қылмыстарды айыру қиынға түсуі мүмкін. Олардың басты ерекшелігі қылмыстың объектісінде болып табылады. Компьютерлік ақпаратқа қарсы жасалатын қылмыстардың объектісі болып машиналық аппаратта, ақпаратты сақтағышта, ЭЕМ-де, ЭЕМ жүйесі мен желісінде, серверде сақталатын немесе операциялық жұмыс жасайтын қорғалатын ақпарат не мәлімет табылады. Ал компьютерлерді пайдалану арқылы жасалатын қылмыстардың объектісі болып нақты қылмыстық шабуыл бағытталған қоғамдық қатынас табылады. Мысалы, компьютерлік техниканы пайдалану арқылы жасалатын алаяқтық кезінде қылмыстың тікелей объектісі мен-

шік қатынасы немесе құқығы болады, электронды тыңшылық (шпионаж) кезінде қылмыстың объектісі мемлекеттің қауіпсіздігі, оның егемендігі мен тәуелсіздігі болады. Алайда екі жағдайда да қылмыс жасау кезінде қылмыстың пәніне әсер ету байқалады, яғни екі жағдайда да компьютерлік ақпаратқа қандай әсер немесе зиян келтіріледі немесе зиян келтірілу арқылы аяқталады. Сол себепті осындай деликатты қылмыстар жөнінде ғалымдардың бірі былай деген болатын: «Жалпы ғылымда қылмыстардың осы күнге дейін ортақ бір шектеу моделі жасалмаған, оны жасау қиынға түседі, өйткені мұндай топтастырулардың көпбағыттылығы және түрліқұрылымдылығы сияқты аспектілер толық ескеріліп жанжақты қарастырылуы керек» [23].

Осыдан байқайтынымыз, компьютерлік қылмыстарды жасау кезінде міндетті түрде компьютерлік сақтағыштағы компьютерлік ақпаратқа қандай да әсер болатынын айтуға болады.

Сонымен, компьютерлік қылмыстылық деп қылмыстық заңнамамен анықталатын, машиналық ақпараттық қылмыстық қол сұғушылықтың объектісі болатын, ақпараттық қылмыс жасау кезінде компьютерлік сақтағыштағы немесе операциялық жадыдағы мәліметке немесе ақпаратқа қандай да заңсыз әсер ететін қоғамға қауіпті іс-әрекеттер жиынтығын айтамыз. Бұл жағдайда қылмыстың заты мен құралы болып компьютерлік ақпарат, компьютер, компьютерлік желілер мен жүйелер, техникалық құралдар және қосалқы бөлімдер табылады.

1.2. Жоғары ақпараттық технологияларды пайдалану салаларындағы қылмыстармен күресудегі мемлекеттің қылмыстық-құқықтық саясаты

Қылмыстық саясат – бұл қылмыстылықты қысқартуға, келтірілетін зардап мөлшерін азайтуға бағытталған қылмыстық-құқықтық, қылмыстық іс жүргізушілік, сондай-ақ криминологиялық және басқа да шаралардан тұратын мемлекетпен жасалатын және ары қарай қадағаланатын қылмыстылықпен күресу шараларының мемлекеттік стратегиясы және тактикасы [24].

Мамандардың ойынша, алғаш рет «қылмыстық саясат» түсінігі 1804 жылы белгілі неміс криминалисі Ансельм Фейербахтың еңбегінде көрініс тапты, одан кейін ғылыми айналымда кеңі-

нен қолданыла бастады. 1888 жылы Франц Фон Лист өзінің «Қылмыстық саясаттың мақсаты» атты еңбегінде «қылмыстық саясатқа» кеңірек анықтама беріп көрді. Оның ойынша қылмыстық саясат үш мағынада түсіндіріледі: 1) қылмыстылықпен күресудің мақсаттары, міндеттері және қағидалары анықталған нормативтік актілер арқылы көрініс табатын мемлекеттің қызметі (құзыреті); 2) қылмыстылықпен күресуді жүзеге асыратын мемлекеттік қызметтің ерекше бір тәжірибелік түрі; 3) қылмыстылықпен күресудің стратегиясы мен тактикасы туралы ғылыми теория [25, 110 б.].

Алайда қазіргі ғылымда «қылмыстық саясат» терминіне нақты қысқаша анықтама берілмеген. Себебі бұл ұғым өте ауқымды, өте кең әсерлі, жалпы мағыналы және көп тармақты ұғым. Қылмыстық саясат туралы бір ауыз сөзбен айтып, оның түсінігін толық мөлшерде ашып айту мүмкін емес.

Қылмыстық-құқықтық саясат түсінігіне бір мезетте бірнеше негізгі ұғымдар кіреді және олар жекелеп қарастырылады: «саясат», «құқықтық саясат», толықтай алғанда «қылмыстық саясат» және нақтылау алғанда «қылмыстық-құқықтық саясат». Алғашқы екі түсінік саясаттанушылармен және құқық теоретиктерімен жеткілікті деңгейде талданады. «Қылмыстық саясат» және «қылмыстық-құқықтық саясат» ұғымына көптеген белгілі қылмыстық құқық және криминология салаларының ғалымдары тоқталып өткен [26].

И.А. Исмаилов қылмыстық саясатты қылмыстылықпен күресудің белгілі мақсаттағы шаралары бойынша тапсырмаларын, нысандарын және мазмұндарын анықтау және жүзеге асыру ретінде нақты шешімдерді қабылдау және жүзеге асыру, басқару және саяси жетекшілік ету дәрежесінде мемлекет қызметінің бағыты, өзге әлеуметтік жүйелермен қарым-қатынас ету және ресурстық, идеологиялық, құқықтық, ақпараттық базада осы жүйелерді оптималды түрде жүргізуді және жетілдіруді ұйымдастыру және қамтамасыз ету деп сипаттап берді [27, 124 б.].

Келтірілген нысан қылмыстық саясаттың түсінігіне толығымен жауап береді деп айтуға келмейді, сол себепті Г.М. Миньковскийдің пікірімен келісуге тура келеді: қылмыстылықпен күресумен байланысты мемлекет пен қоғам қызметінің бағыттары қалай аталса да, не ол қылмыстық саясат деп аталсын, не қылмыстылықпен күресу саясаты деп аталсын, сөз бұл жерде эко-

номикалық, идеологиялық және әлеуметтік саясаттың эффективтілі қызмет етуін қамтамасыз ететін ішкі саясаттың маңызды құрамдас бөлігі туралы болып отыр [28, 7 б.].

Ең бастысы, бұл жерде қылмыстық саясатқа максималды нақты және толық анықтама беру емес, біріншіден, бұл анықтама шегінде қылмыстық саясат салаларының мемлекет тарапынан функциялары қарастырылуы керек, яғни мемлекеттің идеялары, қағидалары, саясаты, стратегиясы және тактикасы; екіншіден, қылмыстылықпен күресу бағытының ең ұшына құқықтық мемлекеттің құндылықтарын (тұлғаның, қоғамның және мемлекеттің қауіпсіздігі, адам мен азаматтың құқықтары мен бостандықтары, заңдылық, ізгілік және әділеттік) жүзеге асырушы ерекше құрал болып табылатын, қылмыстық саясаттың негізі болып келетін «құқық» тұруы тиіс; үшіншіден, қылмыстық саясаттың түсініктемесін беруде кешенді, көпаспектілі сипаттама қолданылып және жеткілікті мөлшерде оның концептуалдық, заңшығарушылық және құқыққолданушылық дәрежелері сипатталуы керек.

Қылмыстық құқықтық саясат қылмыстық саясаттың бір бөлігі болып табылады және келесідей бағыттарда жұмыс істейді:

- қылмыстық-құқықтық реттеудің негізгі қағидалары мен бағыттары анықталады;
- криминализация (іс-әрекетті қылмыстық деп тану) және декриминализация жүреді;
- пенализация (белгілі қылмыстық іс-әрекет жасалғаны үшін нақты жазалау шарасын анықтау) және депенализация (қылмысты жасаумен байланысты мәжбүрлеу шараларды қолдануды жоққа шығаратын шарттарды анықтау) жүреді;
- қылмыстық-құқықтық сипаттағы баламалы (альтернативті) және жазамен қатар қолданылатын басқа да шаралар анықталады;
- қылмыстық құқықтың қолданыстағы нормаларына олардың қазіргі тарихи контекстегі мәнін, мағынасын нақтылау үшін түсініктеме беріледі;
- құқыққорғау органдары қылмыстық құқықтың институттары мен нормаларды тәжірибелік қолдануға сүйенеді.

Қылмыстық саясаттың теориясы мемлекеттің белгілі бір тарихи кезеңінде қылмыстық сипаттағы іс-әрекеттердің даму заңдылықтарын зерттеуге әмсе анықтауға, қылмыстылыққа әсер етудің

және заңдылықты қамтамасыз етудің қазіргі заман талаптарына сай моделін ұсынуға бағытталған.

Қылмыстық саясаттың мәселелері салалық ғылымдар теориясында фундаментальды болып табылады, әсіресе қылмыстық құқық, қылмыстық іс жүргізу және криминология салалары ішінде.

«Саясат» (politike) термині грек тілінен аударғанда «мемлекетпен басқару өнері» дегенді білдіреді. Саясат қоғамдық өмірдің белгілі салаларын басқару бойынша мемлекеттің функцияларын айқындайды. Әлеуметтік саясаттың бір бағыты ретіндегі қылмыстық саясат ол мемлекеттің қылмыстылықпен күресу аясындағы саясаты. Сөз бұл жерде мемлекеттің қызметінің бағыты, яғни қылмыстылықпен және қылмыстармен тығыз байланысты қоғамға кері өзге де жүріс-тұрыс нысандарымен күрес бойынша мемлекеттік органдардың осы ерекше сала бойынша нысандарын, мақсаттары мен міндеттерін, мазмұндары мен құрылымдарын анықтауы туралы жүріп жатыр.

Қылмыстық саясат екі негізгі бөлімнен: жеке бөлімдерден және өзінің мазмұны мен көлемі жағынан тең емес категориялардан тұрады. Оның басты ядросын бүкіл қылмыстық саясаттың нормативтік базасына ие, оның құрылымдық элементі қылмыстық-құқықтық саясат құрайды. Қылмыстық саясат қылмыстылықпен күресудің құқықтық базасын құрайтын салалар кешені, институттар мен нормалар жүйесінің негізі болып табылатын қылмыстық құқықпен тығыз байланысты. Криминология ғылымында саясат құқықтың соңынан өзінің даму үдерісін жүргізбейді, керісінше құқық саяси құрылымдардың соңынан, олардың жүзеге асырылуын қамтамасыз етуде қатысып дамиды. Кейбір жағдайда қылмыстық саясат аяқ астынан жетіледі, бірінші кезекте заң қабылданады да, кейін оның қабылдану себептері түсіндіріледі. Қылмыстық саясат әлеуметтік саясаттың бір бөлігі болып табылады және қылмыстың құрамына сәйкес түрлі бағыттарды білдіретін бірнеше элементтерден тұрады: адам өмірі мен денсаулығына қарсы қылмыстармен, терроризммен, экономикалық сипаттағы қылмыстармен, рецидивтік қылмыстылықпен, кәмелеттік жасқа толмағандардың қылмыстарымен және т.с.с. күресу.

Қылмыстық саясат қылмыстылықпен күрес жүргізу және күресті ұйымдастыру бойынша күнделікті ағымдағы қызметте ғана кездесе бермейді, сонымен бірге қылмыстық-құқықтық саладағы

заңнамалық анықталған мемлекеттік билікпен жүргізілетін шектеулерде, қоғамның тұтыну бағыттарына қатысты адекватты приоритеттерде, қылмыстық-құқықтық реттеуді жүзеге асырудың маңызды тапсырмаларында, жолдарында және амалдарында да орын табады. Қылмыстық саясаттың мазмұны болып біршама көлемде қылмыстылықтың себептеріне әсер ететін және сол арқылы оның көзін жоюға үлесін қосатын әлеуметтік экономикалық және идеологиялық шаралар кешенін жүзеге асыру табылады [29, 6-7 б.].

Қылмыстық саясат туралы, жоғарыда айтылғандай, көптеген ғылыми трактаттар жазылып кеткен, алайда, өткен ғасырдың тоқсаныншы жылдарында осы мәселеге қатысты құқықтанушы ғалымдар негізгі акцентті теориялық жағына көп аударып кетті [30]. Тек санаулы ғылым өкілдерінің ғана қылмыстық саясаттың мемлекет пен қоғам өмірінің қазіргі тәжірибесіндегі көрінісін сипаттауға батылы барады. Осындай ғалымдардың ішінен Ресейлік С.С. Босхоловты және Э.Ф. Побегайлоны атап өтуге болады.

Сөйтіп, қылмыстық саясатқа арналған С.С. Босхоловтың жұмысында Ресейдің қазіргі саяси жағдайы жалпы әлемдік кризистік жүйеге кірумен байланысты. Бұл кризиске Ресейдің конституциялық-құқықтық жүйесі де шалдықты. Кризистің мәні қажетті уақытта өз алдына қойылған мақсаттарын жеткілікті дәрежеде орындай алмайтын биліктің конституциялық-құқықтық институттарының дезинтеграциясында. Қандайда бар демократиялық даму жолынан авторитарлыққа ауысу қаупі шынайы болып барады [31, 16 б.].

Ал профессор Э.Ф. Побегайло Ресейдің қылмыстық құқықтық саясатының кризистік жағдайын ғана көрсете қоймай, жеткілікті дәрежеде оған дәлелдер келтіреді [32]. Қылмыстық саясаттың мазмұны енді тек санаулы адамдар тобымен айқындалады. Алғашындай ғалымдар мен қоғам қайраткерлері және жалпы социум арасындағы талқылауға салынбай, кейде тіпті саяси сипаттағы қандай да халықаралық ықпал мен әсердің лезде нәтижесімен анықталып отырады. Зерттеушілер көрсеткендей, «қайта құрылу» (перестройка) кезеңі деп шартты түрде аталатын уақытқа дейінгі Кеңестік қылмыстық саясаттың бағыттарын коммунистік партия және оның басқарушы органдары мен тұлғалары анықтайтын. Осыдан мынадай қорытындыға келуге болады: қылмыстық саясат алқалы органмен жасалатын және басқа барлық

мемлекеттік органдармен, қоғамдық ұйымдармен және ғылыммен мүлтіксіз жүзеге асырылатын функционалды қызмет [33].

Профессор С.В. Бородин, И.М. Гальперин, В.И. Курляндский, А.С. Сенцов, Н.А. Стручков қылмыстық саясаттың мазмұнына қылмыстық құқықтың, қылмыстық іс жүргізу және қылмыстық атқару құқығының нормаларымен регламенттелген қылмыстылықпен күресудің арнайы шараларын жатқызады.

Кеңес дәуірі кезеңі мен ТМД кезеңіндегі қылмыстық құқық теориясындағы қылмыстық саясаттың қалай анықталғанын көру үшін атақты зерттеуші-ғалымдардың осы мәселеге қатысты жазылған еңбектерінен пікірлерін келтіруге болады. Сөйтіп, Н.И. Загородников пен Н.А. Стручковтың жұмыстарында былай делінген: «Қылмыстық саясат кеңестік саясаттың қылмыстылықпен күресудегі мәжбүрлеу шаралары шеңберін жасау және жүзеге асыру, мүмкін болатын мемлекеттік мәжбүрлеу шаралары шеңберін анықтау, материалдық, іс жүргізулік және қылмыстық атқару құқықтарының құқықтық нормаларын жасау және қолдану бастапқы шарттары қалыптасатын бағытын білдіреді» [34, 4 б.].

Осы тектес анықтаманы Л.Д. Гаухман мен Ю.И. Ляпунов берген еді: «Кеңестік қылмыстық саясат – бұл әлеуметтік қоғамдық қатынастарды белгілі тарихи кезеңдегі әлеуметтік-экономикалық формацияның мәніне сәйкес қоғамның объективті даму заңдылықтарының ілімдеріне негізделген қылмыстық қолсұғушылықтардан (қылмыстылықпен күрес жүргізу) қорғау бағыттары мен перспективалары» [35, 4 б.].

Н.А. Беляевтың пірінше, қылмыстық саясат қылмыстық қолсұғушылық жасаған тұлғаларға қатысты жазаларды қолдану немесе әкімшілік не қоғамдық әсер ету шараларын ауыстыру жолымен жүзеге асырылады [36, 15 б.].

Кейбір ғалымдар қылмыстық саясат саласын оған тек соңғы нәтиже кезінде толығымен қылмыстылықпен күресуге жәрдемдесетін әлеуметтік шараларды кіргізу арқылы кеңейтуге қарсы болды. Олар өз бетінше қажетті негіздемеге ие болмады [37, 100-101 б.]. Осы сияқты қылмыстық саясатты әлеуметтік саясатқа тікелей жататынын жоққа шығаратын пікірді П.Н. Панченко да айтып өткен [38, 90 б.].

90-жылдарға келетін болсақ, оған қылмыстық саясат туралы С.С. Босхоловтың көзқарасын айтуға болады. Ол бойынша қылмыстық саясат дегеніміз: біріншіден, тиісті директивті актілер-

де (заңдар, Президент жарлықтары, Үкімет қаулылары) орын тапқан қылмыстылықпен күрестің мемлекеттік саясаты (доктринасы); екіншіден, сәйкесінше саяси, әлеуметтік және құқықтық білімдердің ғылыми теориясы мен синтезі; үшіншіден, қылмыстылыққа және басқа да құқықбұзушылықтарға белсенді қарсы бағытталған әлеуметтік қызметтің ерекше түрі [39, 32 б].

В.П. Ревиннің анықтағаны бойынша, қылмыстық саясат дегеніміз қоғамды қылмыстылықтан қорғау бойынша, оптималды стратегияны ұйымдастыру және жүзеге асыру бойынша, қылмыстылықтың дәрежесін шектету және орнықтыру мақсатында қамтамасыз ету жұмысы бойынша мемлекеттің нақтыланды-рылған белсенді қызметі [40, 7 б.].

Қылмыстық саясатты жүзеге асыру деп оның субъектілерінің әлеуметтік жүріс-тұрысын түсіну керек: мемлекет азаматтық қоғам институттарымен бірге қылмыстық саясат қағидаларын саяси және саяси-құқықтық алғышарттарды, қылмыскерлерді қайта әлеуметтендіру, қоғамға адаптациялау бағдарламаларын құқықтық тәртіпті қамтамасыз ету үшін, қылмыстылықтың алдын алу және онымен күресу жұмыстарын жүзеге асырады.

Қылмыстық-құқықтық саясаттың мазмұны тек заңшығарушымен ғана шектеліп қоймайды, сонымен бірге оған құқық-қолдану қызмет тармақтары да кіреді. Оның мазмұнындағы басты бағыттары қылмыстық-құқықтық құралдар арқылы жағымсыз құбылыстармен күресу, қоғамға қауіпті іс-әрекеттердің қылмыстық жазаланушылығын анықтау, қылмыстылықтың шеңберін шектеу, жазаланушылықтың сипатын анықтау, қылмыстық жауаптылық шаралары мен олардан босату шарттарын белгілеу болып табылады. Теорияда қылмыстық-құқықтық саясатты ұйымдастыру мен жүзеге асырудың орталық бағыты ретінде әділдікпен жобаланатын және қолданыстағы қылмыстық-құқықтық нормалардың криминалдық және әлеуметтік шартталғандығын анықтау және негіздеу үдерісі саналады.

А.Л. Дзигарьдің пікірінше, жаңа заңнамаларды жасауға тартылған тұлғалар Карл Маркстің: «қоғам заңға негізделмеуі керек... Керісінше, заң қоғамға негізделуі керек, ол жеке индивидуумның еркіне қарсы қоғамның мүдделері мен тұтынуларының жалпы материалдық қажеттілігінен шығатын көрініс болуы керек», – деген ілімін білмейді не есепке алмайды [41, 126-127 б.].

Қазақстан Республикасының қазіргі кездегі қылмыстық құқықтық саясаты мемлекетіміздің 2010 жылдан 2020 жылдар аралығын қамтитын құқықтық саясат тұжырымдамасына сәйкес келесідей бағыттарды көздейді. Біріншіден, қоғамға аса қауіп туындатпайтын қылмыстарды декриминализациялауды жүзеге асыру көзделуде. Екіншіден, бас бостандығынан айырумен байланысты емес жазаларды қолдану аясы кеңейеді. Үшіншіден, жекелеген қылмыстар бойынша бас бостандығынан айырудың жоғары мерзімдерін жеңілдету қарастырылуда. Төртіншіден, маңызы шамалы кейбір қылмыстар үшін бас бостандығынан айыру түріндегі жазалар тағайындалмайтын болады. Бесіншіден, мемлекетке қылмыспен келтірілген зиянды толық өтеген жағдайда қылмыстық жауаптылықтан босатудың жаңа негіздері қарастырылады. Алтыншыдан, қылмыстардың қайталануы барысында жаза тағайындаудың тәртібін реттейтін нормаларды Қылмыстық кодекстен алып тастау мәселесі қарастырылуда. Жетіншіден, кәмелетке толмағандардың қылмыстық жауаптылығы және жазасын жеңілдету көзделуде.

Әлем XXI ғасырда түбегейлі өзгерістерге түсуде. Өзінің маңызы жөнінен аталған ғасыр ұлы географиялық ашулар мен колониялды жүйенің ыдырауы және ұлттық мемлекеттердің құрылу дәуірімен салыстыруға болады. Ол жаһандану дәуірі. Жаһандану – қазіргі кездегі экономика, саясаттану, құқық, халықаралық қатынастар және басқа да пәндер бойынша неғұрлым көп талқыланатын проблемалардың бірі болып қалуда [42, 17 б.].

Аталған мәселеге қатысты түрлі көзқарастар кездеседі. Зерттеуші ғалымдардың бірі жаһанданудың экономикалық аспектілеріне тоқталса, келесі көзқарастағылар бірыңғай ақпараттық кеңістікті қалыптастыруды көздейді, үшінші көзқарасты ұстанушылар стандартты компьютерлік бағдарламаларды пайдалануға негізделген бірыңғай стандарттардың дамуына арнаған. Француз зерттеушісі Б. Бади жаһанданудың үш өлшемінің болатындығын атап кетеді:

1) Жаһандану тұрақты келе жатқан тарихи үдеріс;

2) Жаһандану әлемді әмбебаптандыру;

3) Жаһандану ұлттық шекараларды жою [43, 8-9 б.].

Ақпараттық-коммуникациялық технологиялардың бір түрі болып компьютеризация табылады. Б.Х. Толеубекованың айтуынша, әлемдік компьютеризацияның бастамасы болып сис-

тематизацияны, жиналған білімдерді тәртіпке келтіруді, мәліметтер банкін (базасын) жасауды, адам өмірінің сан алуан түрлі салаларынан кеңейіп жиналып жатқан мәліметтерді сақтауды қажет еткен XX ғасырдың ортасындағы ақпараттық жарылыс табылды. Осы жұмыстың ауқымды бөлігін өзіне алар техникаға деген объективті қажеттілік пайда болды. Яки сол техника компьютерлер түрінде, не бастапқыда аталғандай электронды-есептеу машиналары түрінде (ЭЕМ) жасалды [44, 10 б.].

Қазіргі кезде әйгілі Ақпараттық-коммуникациялық технологиялар сөз байланысын немесе жай ғана АКТ-ны кез келген жерде кездестіруге болады. Осы АКТ-ның бір жағы болып келетін виртуалды желілік қауымдастықтар қазір тек әлеуметтанушылар мен философтарды ғана емес көптеген елдердің арнайы қызметшілерін де мазалап отыр.

Сөзсіз АКТ-ның жалпы алғанда жақсы пайдалы жақтары да көп. Келіссеңіз, үйден шықпай креслода отырып керек анықтамаңызды не басқа да құжаттарыңызды «Электронды үкіметке» (e-gov) кіріп алып жатсаңыз жақсы емес пе, осы органдарға немесе мекемелерге барып, кезекте тұрғанша немесе үйіңізде шай не кофе ішіп отырып ұшаққа билет алсаңыз қаншама уақыттыңызды үнемдейсіз [45, 10 б.].

Психологтар көп адамдардың (әсіресе жасөспірімдер арасында) тез қарқынмен өсіп жатқан ғаламтордың алаяқтық айлаларына тәуелді болып жатқанын айтады: жер шары тұрғындарының үлкен бөлігі виртуалды кеңістікте, тек ұйықтауға ғана үзіліс жасап (кейбіреулердің пікірінше, мұндай адамдар мүлдем ұйықтамайды) өмір сүре бастады [46, 10 б.].

Ғалымдар мен саясаткерлердің осындай көзқарастарынан кейін компьютерлік қылмыстар мәселелері ұлттық қылмыстық саясаттың басты приоритетті көкейтесті шеңбері болғаны сөзсіз. Төменде біз Қазақстан Республикасының компьютерлік құқық бұзушылықтар мен Ғаламторда болып жатқан мәселелерге қатысты қылмыстық-құқықтық саясат ұстанымдары, бағыттары мен бағдарламалары, алға қойған мақсаттары мен міндеттері, осы уақытқа дейін істелген жұмыстары, мәселелерді реттеу мақсатында қабылданған ұлттық заңнамалар мен халықаралық шарттар кешені бойынша категориялы функционалды көрсеткіштерін жан-жақты қарастыруға бел буамыз.

XX жүзжылдықтың 90-жылдарының басы Қазақстанда да, кеңес кезеңінен кейінгі кеңістікте де адамзат өмірінің салаларын жаппай компьютеризациялаумен сипатталды. Алғашында компьютерлер банк қызметі салаларында қолданыла бастады, кейін толық қадаммен оқу мекемелерін компьютеризациялау жүзеге асырыла бастады, сонымен бірге мемлекеттік органдардың, әсіресе ауқымды құжаттармен және іс-қағаздармен, кеңсе мен мұрағаттармен жұмыс жасайтын құқыққорғау органдарында компьютеризация жүргізіліп, компьютерлерінде мәліметтер базасы қалыптастырылды. Алайда жаңа ақпараттық технологиялар, бастапқыда айтылғандай, мемлекет пен қоғам ішінде дамуға, жетілдірілуге итермелеп қоймай, жаңа жағымсыз үдерістерді тудырды. Ақпараттық технологияларды қоғам өмірінің түрлі салаларына енгізу салдарымен қатар компьютерлік қылмыстылықпен күресу мәселелері қиындап барады.

Компьютеризацияның жоғары дәрежесі басым батыстық елдерде бұл мәселе алғашқылардың бірі болып отыр. Отандық және шетелдік басылымдар мен бұқаралық ақпарат құралдары соңғы жылдары ақпараттық салада қылмыстылықты сипаттайтын жаңа көріністердің түрлі ұғымдары мен құбылыстарын көтерумен жанталасуда. Бұл әлеуметтік құқықтық феноменнің анық қырларының болуына қарамастан теорияда осы қылмыстарды орнықты сипаттайтын ортақ бір құқықтық дефиниция әлі күнге дейін жоқ. Әдебиеттерде осыған байланысты түрлі ұғымдар мен көріністерді кездестіруге болады. Мысалы, жоғары технологиялар саласындағы қылмыстар, коммуникациялық қылмыстар, компьютерлік қылмыстар, киберқылмыстар, компьютерлік ақпарат саласындағы қылмыстар, ақпараттық қылмыстар, жоғары ақпараттық технологиялар саласындағы қылмыстар, интернеттік қылмыстар, глобалды компьютерлік желілер саласындағы қылмыстар және т.б. Ал шетелдік әріптестер мынадай сөз тіркестерін қолданады: high-tech crime, cyber crime, network crime, computer crime және басқалары, сәйкесінше олардың тікелей аудармасы мынадай болады: «жоғары технология қылмысы», «киберқылмыс», «желі жұмысындағы қылмыс» және «компьютерлік қылмыс».

Біз білетіндей, мемлекет өз тарапынан компьютерлік қылмыстарға қатысты жүйелі құқықтық және криминологиялық шаралар шеңберін айқындап қылмыстың жеке түрінің, тобы-

ның қылмыстық маңызды белгілерін сипаттау жүйесін, қылмыс туралы, оның субъектісінің сипатын беретін, қылмысты жасаудың механизмін, әдістерін, мақсатын және онымен күресудің кешенді әдістерін көрсететін, қылмысты ашу мен алдын алуға алдына мақсат қоятын тапсырмалар мен сипаттамалар жүйесін ұйымдастырады.

Компьютерлік ақпараттар саласындағы қылмыстар, басында ескерткеніміздей, салыстырмалы жас қылмыстар қатарына кіреді. Отанымызда мұндай қылмыстарды тергеу тәжірибесі төмен, себебі еліміз жас болғаннан кейін, ғылыми-техникалық құралдардың тез дамуынан және компьютерлік сауаттылықтың төмендігі сияқты себептерден бұл саладағы қылмыстылықпен күресу ісі жоғары сатыға өте алмай жатыр.

Аталған саладағы қылмыстық әрекеттердің қоғамдық қауіптілігі ашық түрде арта түсуде және заңшығару қызметіміздің компьютерлік қылмыстылыққа қатысты негізінен шет елдердің криминализациялық тәжірибесін формализациялау біздің көз алдымызда жүріп жатыр.

2006 жылдың 10 қазанында шығып, күшіне еңген ҚР Президентінің «Қазақстан Республикасының ақпараттық қауіпсіздік концепциясы туралы» Жарлығында бұрын-соңды ешбір әдебиетте, еңбекте, қолданыстағы Қылмыстық Кодексте берілмеген осы саладағы ұғымдар мен әдіс-әрекеттер және қылмыстық әрекеттер түрлерінің тізімі берілген. Соның ішінде, біздің ойымызша, Қылмыстық кодекстегі қылмыс құрамдарына қосып бірқатар қылмыстық әрекеттерді атап өткен дұрыс [47].

Олар:

- ақпараттық алмасуды уақытылы жасамау және ақпараттық мекен-жайға қатысты қателік жасау, ақпаратты заңсыз жинау және пайдалану;
- ақпаратқа және ақпараттық ресурстарға заңсыз кіру, заңға қайшы ақпараттық салада мәліметтерді жою, модификациялау (түрлендіру) және көшіру;
- ақпаратты заңсыз манипуляциялау немесе әсер ету (дезинформация, ақпаратты өзгерту не жасыру);
- ақпараттық жүйелерде мәліметтерді заңсыз көшіру;
- бұқаралық ақпарат құралдарын адамдардың, қоғамның және мемлекеттің мүдделеріне қарсы тұрғыдан пайдалану;

– кітапханалардан, мұрағаттардан және мәліметтер базасынан ақпаратты талан-таражға салу;
– ақпаратты өңдеудің технологиясын бұзу;
– вирустарды кіргізу;
– бағдарламалық және аппараттық қосалқы құрылғы орнату;
– ақпаратты және байланысты өңдеу құралдарын жою және бұзу;
– машиналық немесе басқа ақпаратты тасымалдауыштарды жою, бұзу және ұрлау;
– бағдарламалық не аппараттық кілттерді және ақпаратты криптографиялық қорғау құралдарын талан-таражға салу;
– мәліметтерді беру желілерінде және байланыс линияларында жалған ақпаратты жіберу, дешифрлеу және бұрып алу;
– тұтынушыларға жалған, толық емес және бұзылған ақпаратты қасақана түрде немесе олқылықпен ұсыну;
– және т.б. заңға қайшы іс-әрекеттер.

Бұл концепция жөнінде толығырақ төменде тоқталып кетеміз.

Криминологиялық тұрғыдан ақпараттық жүйеде сақталған бағдарлама, басқа да кез келген ақпарат мөлшері сияқты жоғарыда айтылған әрекеттердің (жою, модификациялау, көшіру, бұзу, дешифрлеу, блок қою және т.б.) кезіне шалдығуы мүмкін. Компьютерге арналған бағдарламалар да құжаттандырылған ақпараттарға жататын белгілер жиынтығына ие және сол ақпараттарды қорғайтын заң нормаларымен қорғалады.

Сөйтіп, кейбір авторлардың пікірі бойынша, компьютерлік ақпарат – ол машиналық тасымалдауышта бекітілген және ЭЕМмен (компьютерлік құралдармен) қабылдауға болатын телекоммуникациялық арналар арқылы жіберілетін ақпарат. Яғни компьютерлік ақпарат белгілі бір жерлерде сақталады және қажетті жағдайда белгілі арақашықтықта қозғалады, ол дегеніміз осы екі іс-әрекет кезінде ақпарат қандай да бір әсерге, яки заңсыз қолсұғушылыққа шалдығуы мүмкін. Сол себепті бірінші кезекте компьютерлік ақпарат салаларындағы басты объект, басты қорғаныста қажет ететін пән және негізгі элемент рөлін компьютерлік ақпарат атқарады. Жалпы жоғары технологиялар салаларындағы кез келген мәселе, олардың жұмысы болсын, олардың мазмұны болсын барлығы тек екілік сандардан тұратын 0 және 1 ақпараттардан

тұрады, осы ақпараттарды түрлі комбинацияда алмастыру арқылы белгілі ақпараттық операциялар немесе іс-әрекеттер жүзеге асырылады. Ол дегеніміз компьютерлік қылмыстардың тамырлы пәні немесе заты осы екілік сандардан тұратын ақпараттар. Мысалы, банктік шоттан ақша қаражат соммасын ұрлау үшін қылмыскер алдымен ақпараттарды ұрлайды және оларды қажетті операциялар жасау үшін толықтырады, өзгертеді, алмастырады, көшіреді және жасырады, содан кейін ақша электронды түрде операциялық өзгеріске түседі (шоттан шотқа ауысады, электронды төлем арқылы қолданылады немесе қолданбалы ақшаға ауысады). Отандық және шетелдік ғалымдар мемлекетпен қатарласа, ең бастысы, осы компьютерлік ақпараттарды мейлінше қорғау жөнінде шаралар жиынтығын ойластыруы керек дейді.

Осы салалардағы қылмыстылықпен күресу барлық елдерді ойландырып отыр, әсіресе өзектілікті осы мәселе бұрынғы ТМД елдері арасында алып отыр. Қазақстан Республикасында соңғы жылдарда компьютерлік қылмыстар байқалмады, оның себебі компьютерлік қылмыстарды анықтау құқыққорғау органдарына қиынға түсіп отыр. Компьютерлік қылмыстар із қалдырмайды десек ол жалған мәлімет болады, жалпы кез келген қылмыс із қалдыруы тиіс, бұл жерде үлкен мәселе құқыққорғау органдарының осындай сипаттағы қылмыстарды анықтау тәжірибесінің жетілмегендігі болып отыр.

Ал енді «Ақпараттық қауіпсіздік туралы Концепцияға қайта оралсақ.

2011 жылдың 14 қарашада қайта қабылданып, күшіне енген ҚР Президентінің «Қазақстан Республикасының ақпараттық қауіпсіздік Концепциясы туралы» Жарлығы осы саладағы көптеген ұғымдарға түсінік беріп, бірталай мәселелерді шешіп отыр. Онда қолданыстағы Қылмыстық кодексте берілмеген осы саладағы ұғымдар мен әдіс-әрекеттер және мүмкін болар қылмыстық әрекеттер түрлерінің тізімі берілген.

ҚР-дың ақпараттық қауіпсіздік Концепциясы Қазақстан Республикасының Конституциясы (1995 жылдың 30 тамызында Референдумда қабылданған) негізінде және Қазақстан Республикасының 1998 жылдың 26 маусымында қабылданған «ҚР Ұлттық қауіпсіздігі туралы» Заңы, 1999 жылдың 15 наурызындағы «Мемлекеттік құпиялар туралы», 1999 жылдың 13 шілдесіндегі «Терроризммен күресу туралы», 2003 жылдың 7 қаңтарындағы

«Электронды құжат және электронды сандық жазба туралы», 2007 жылдың 11 қаңтарындағы «Информатизация туралы» және 2005 жылдың 18 ақпанындағы «Экстремизмге қарсы әрекет туралы» Заңдары негізінде, сонымен қатар Қазақстан Республикасының Президентінің 2006 жылдың 18 тамызында №163 Жарлығымен мақұлданған Қазақстан Республикасының 2006 – 2009 жылдарға арналған ақпараттық аумақтағы бәсекелік қабілеттілікті дамыту концепциясы негізінде құрастырылған.

Тағы да, осы Концепцияны ұйымдастыру кезінде бұрынғы ТМД қатысушы мемлекеттерінің 1999 жылғы 4 маусымдағы әскери саладағы ақпараттық қауіпсіздік Концепцияларының ережелері және осы саладағы халықаралық тәжірибесі ескерілген.

Бұл Концепция Қазақстан Республикасының ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай мемлекеттік саясатты ұйымдастыруда және жүзеге асыруда негіз болып табылады. Оның ережелері болашақта Қазақстанның ақпараттық кеңістіктегі мемлекеттік саясатын жүзеге асыруда ескеріледі. Мемлекеттік саясат жеке және заңды тұлғалардың заңға қайшы емес тәсілдермен ақпаратты ерікті түрде жасау, іздеу, алу және тарату құқықтарын қамтамасыз етуге негізделген.

Мемлекет ақпараттық ресурстарды меншік объектісі ретінде таниды және оларды шаруашылық айналымға жібереді, егер ақпараттық ресурстардың иелерінің, пайдаланушыларының және басқарушыларының заңды мүдделері дұрыс ескеріліп отырса. Мемлекеттік саясат ақпараттық қауіпсіздікті қамтамасыз ету саласында мемлекеттік органдар мен ұйымдардың монополизміне жол бермейді.

Қазақстан Республикасының ақпараттық қауіпсіздік жағдайы. Қазіргі кезде Қазақстанның саяси және экономикалық өзгерістеріне байланысты болып жатқан үдерістер оның ақпараттық қауіпсіздік жағдайына тікелей әсерін тигізеді. Соған қоса, ақпараттық қауіпсіздіктің жағдайын бағалау кезінде туындайтын жаңа факторларын ескерген қажет. Ол факторларды саяси, экономикалық және ұйымдастырушылық-техникалық деп бөлуге болады.

Ақпараттық қауіпсіздіктің қазіргі кездегі жағдайын зерттеу оның Қазақстандағы дәрежесі адамның, қоғамның және мемлекеттің қажеттіліктеріне, сұраныстарына сай келмейді. Мемлекеттік органдарды толық, жетімді, уақытылы және түсінікті

ақпаратпен қамтамасыз ету үшін, соның ішінде мемлекеттік ақпараттық ресурстарды қорғау, талаптарға сай техникалық құралдардың сәйкестігін нақтылау жүйесін және отандық қорғау тәсілдерін жетілдіру үшін негізделген шешімдер қабылдау қажет. Ақпараттық қауіпсіздікті ұйымдастыруға кері әсерін осы саладағы кәсіби мамандардың аз болуы тигізеді. Ақпараттық қарудан қорғану, техникалық барлауға қарсылық көрсету және осы саладағы нормативтік құқықтық базаны жетілдіру және басқа да көптеген мәселелерді ары қарай ұйымдастыру қажеттілігі туындап отыр.

Интернеттің ақпараттық кеңістікте өсуі және тарауы салдарынан адам мен қоғамның құқықтарын қатігездік пен қанаушылықты білдіретін ақпараттан, жастарды, жаңа ұрпақты теріс тәрбиелейтін жалған және бұрыс ақпараттардан қорғау қажеттігі туындайды. Сонымен қатар, бұл қауіптердің сыртқы қайнар көздері Қазақстан Республикасының заңнамасының юрисдикциясы шеңберіне кірмей де қалуы мүмкін, сол себепті осы әрекеттерге құқықтық шаралар жүйесін қолдану қиын болып отыр.

Осы айтылып отырған саладағы өзекті мәселелердің бірі отандық ақпараттық технологиялардың болмауы, адамдар бұл технологиялардың ақпараттық қауіпсіздік талаптарына сай келетінін білмей, тәуекелге барып импорттық тауарды алады. Біз шетелдік өндірушілер ұсынып отырған техниканы алуымызға тура келеді, мүмкін олар техника арқылы барлық бақылау әрекеттерін, мүмкін тіпті операцияларын жүргізіп отырғанын білмейміз. Осының бәрі ақпараттық қауіпсіздікке, мәліметтер базасына және банкіне қауіп төндіреді және шетелдік өндірушілер алдында телекоммуникация, ақпарат және басқа көптеген маңызды салалар жағынан тәуелділікке алып келеді.

Ақпараттық саладағы құқықтық қатынастар субъектісі болып меншік нысанына қарамай заңды және жеке тұлғалар табылады. Ал меншік иегері болып мемлекет (мемлекеттік органдар мен ұйымдар және лауазымды тұлғалар түрінде), жеке тұлға және заңды тұлға табылады.

Ақпаратты жасау және пайдалану тұрғысынан ақпараттық қатынастардың субъектілері автор, меншік иесі, пайдаланушы және билік етуші ретінде танылуы мүмкін. Ақпарат және ақпараттық ресурстар заттай және интеллектуалдық меншік

ретінде танылуы мүмкін. Сондықтан ақпаратты өңдеу кезінде ақпараттық жүйелерде тек конфиденциалдықты ғана қамтамасыз ету емес, сонымен қоса оның тұтастылығын және қолжетімділігін қамтамасыз ету қажет. Электронды құжаттар үшін олардың әрқайсысының шынайылығы электронды әріптік жазбамен дәлелденуі тиіс. Ал мемлекеттік құпиядан тұратын ақпараттарға қатысты қатынастардың барлық субъектілері үшін ерекше анықталған құпиялық режим әрекет етеді. Бұл ақпараттардың меншік иесі болып мемлекет танылады. Бұл субъектілерге қатысты ақпараттарды мемлекеттік ақпараттық қорғау жүйесі қадағалайды.

Қазіргі кездегі қоғамның сәтті қызметі ондағы ақпараттық үрдістердің қалыпты, ұйымдасқан түрде жүру дәрежесіне байланысты. Сол себепті Қазақстан Республикасы үшін осы үрдістердің мемлекет шегіндегі ақпараттық кеңістікте бірігуі зор маңыздылыққа ие.

Қазақстан Республикасын ақпараттық кеңістікте біріктіру «Электрондық үкіметтің» рөлін жоғарылатады. «Электрондық үкімет» («e-government» немесе жай «e-gov») Қазақстан Республикасы үшін алғашында 2005-2007 жылдарға арналған Мемлекеттік ұйымдастыру бағдарламасымен жүзеге асырылып және ҚР Президентінің 2004 жылғы 10 қарашадағы №1471 Жарлығымен бекітілген. «Электронды үкімет» биліктің барлық тармақтары үшін олардың қызметтерін ақпараттық көмекпен қамтамасыз ету арқылы қызметтің эффектілігін көтеруге, олардың арасындағы ақпараттық қарым-қатынастардың динамикасын қамтамасыз етуге және экономика саласындағы субъектілер мен халықпен қарым-қатынасын жасауға мүмкіндік береді. ЭҮ-нің құзыреті мен функциялары ҚР-дың «Электронды құжат және электронды сандық жазба туралы», «Информатизация туралы» Заңдарында анықталған.

Қазақстан Республикасының 2005-2007 жылдарға арнаған «Электрондық үкіметті» мемлекеттік ұйымдастыру бағдарламасы шегінде «жеке тұлғалар», «заңды тұлғалар», «қозғалмайтын мүлік регистрі», «мекен-жай регистрі» мемлекеттік мәліметтер базасы құрылды. Олардың қауіпсіздігі ақпараттық қатынастардың субъектілері арасындағы қауіпсіз ақпараттық қарым-қатынастардың нәтижесінде қамтамасыз етіледі.

Ақпараттық қауіпсіздікті қамтамасыз етудің мақсаты және тапсырмасы. Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі мақсаттарына жатады:

– ұлттық ақпараттық қорғау жүйесін жасау және күшейту, соның ішінде әсіресе мемлекеттік ақпараттық ресурстарда;
– ақпараттық салада мемлекеттік ақпараттық ресурстарды, сондай-ақ адам және қоғамның құқықтары мен мүдделерін қорғау;
– Қазақстанның ақпараттық тәуелділікке ұшырауына жол бермеу, Президенттің, Парламенттің, Үкіметтің және басқа мемлекеттік органдар мен ұйымдардың ақпараттық изоляциясын, басқа мемлекеттер жағынан ақпараттық экспансия мен блокадаға жол бермеуді қамтамасыз ету.

Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз етудің негізгі тапсырмалары болып табылады:

– ақпараттық қауіпсіздік саласындағы Қазақстан Республикасының ұлттық заңнамасын жетілдіру;
– ақпараттық қауіпсіздіктің қатерінің қайнар көздерін анықтау, бағалау және болжамдау, қорғаныстағы объектілердің қорғану параметрлерін анықтау;
– мемлекеттік ақпаратты қорғауды қамтамасыз ететін саясатты ұйымдастыру, оны жүзеге асырудың шаралары мен әдістерін жүйелеу;
– мемлекеттік органдар мен ұйымдар іс-әрекетінің координациясын жасау;
– глобалды ақпараттық желілер мен жүйелерді жасау мен пайдалану үдерістерінде Қазақстанның белсенді қатысуын қамтамасыз ету;
– нормативтік құқықтық және әдістемелік базаны жетілдіру арқылы техникалық барлауларға (разведкалар) қарсылық көрсету жүйесін дамыту.

Ақпараттық қауіп төндіретін қылмыстық әрекеттер әртүрлі тәсілдермен жүзеге асырылуы мүмкін. Ол тәсілдерге ақпараттық, бағдарламалық-математикалық, физикалық, радиотехникалық және ұйымдастырушылық-құқықтық тәсілдер жатады. Енді осы тәсілдерді, біздің ойымызша, рет-ретімен бір тізімге келтіріп көрсеткен дұрыс.

Олар:

- ақпараттық алмасуды уақытылы жасамау және мекенжайға қатысты қателік жасау, ақпаратты заңсыз жинау және пайдалану;
- ақпаратқа және ақпараттық ресурстарға заңсыз кіру, заңға қайшы ақпараттық салада мәліметтерді жою, модификациялау және көшіру;
- ақпаратқа заңсыз манипуляция жасау немесе әсер ету (дезинформация, ақпаратты өзгерту не жасыру);
- ақпараттық жүйелерде мәліметтерді заңсыз көшіру;
- бұқаралық ақпарат құралдарын адамдардың, қоғамның және мемлекеттің мүдделеріне қарсы тұрғыдан пайдалану;
- кітапханалардан, мұрағаттардан және мәліметтер базасынан ақпаратты талан-таражға салу;
- ақпаратты өңдеудің технологиясын бұзу;
- вирустарды кіргізу;
- бағдарламалық және аппараттық қосалқы құрылғы орнату;
- ақпаратты және байланысты өңдеу құралдарын жою және бұзу;
- машиналық немесе басқа ақпаратты тасымалдауыштарды жою, бұзу және ұрлау;
- бағдарламалық не аппараттық кілттерді және ақпаратты криптографиялық қорғау құралдарын талан-таражға салу;
- персоналға әсер ету;
- мәліметтерді беру желілерінде және байланыс линияларында жалған ақпаратты жіберу, дешифрлеу және бұрып алу;
- парольдік-кілттік жүйеге әсер ету;
- байланыс және басқару жүйесін радиоэлектронды түрде төмендету;
- техникалық құралдар мен информатизациялау құралдарына сәйкестікті өтпеген не ескірген немесе толық жетпеген сатып алынған заттар;
- тұтынушыларға жалған, толық емес және бұзылған ақпаратты қасақана түрде немесе олқылықпен ұсыну;
- жеке және заңды тұлғалар үшін маңызды ақпараттардан тұратын құжаттарға кіруге заңсыз шектеу қою;
- және т.б. заңға қайшы іс-әрекеттерден тұратын амал-тәсілдер.

Сонымен мемлекеттің әр саладағы ақпараттарды қорғауды қамтамасыз етудің өз ерекшеліктері болады. Оның себебі әр саланың өз ерекшелігіне байланысты ақпараттық кемістіктері және бәсеңді элементтері болады.

Сондықтан әр сала үшін оның жағдайына әсер ететін спецификалық арнайы факторлар есебімен ақпараттық қауіпсіздікті қамтамасыз ететін нысандар мен тәсілдерді пайдалану және арнайы жұмыстар кешені қажетті.

Осы Концепцияға негізделе ақпараттық қауіпсіздікті қамтамасыз етудің негізгі бағыттарын атап өтуге болады:

- нормативтік құқықтық базаны жетілдіру;
- әдістемелік және техникалық құжаттарды дайындау;
- ақпаратты қорғау саласындағы біртұтас саясатты жасап жетілдіру;
- мемлекеттік құпиялардың қорғауын қамтамасыз ету;
- техникалық шпионажға қарсылық көрсету;
- ақпараттық қарудың әсерінен қорғану;
- ақпараттық ресурстарды, ақпараттық-телекоммуникациялық жүйелерді және ақпараттық инфрақұрылымды ұйымдастырушылық-техникалық қорғау;
- ақпараттық жүйелерді және информатизация объектілерін ақпарат және ақпаратты қорғау саласындағы стандарт талаптарына және нормативтік құқықтық актілерге сәйкестендіру;
- техникалық құралдардың ақпараттық қауіпсіздіктің талаптарына сәйкестігін дәлелдеу;
- ақпараттық қауіпсіздікте қауіпті төндіретін қайнар көздерді анықтау, бағалау және болжамдау;
- техникалық қауіп құралдарына қарсы адекватты шараларды оперативті (жедел) түрде қабылдау;
- ақпаратты қорғау мен ақпараттық қауіпсіздікті қамтамасыз ету бағыттары бойынша ғылыми-зерттеулік қызмет және ғылыми-техникалық қамту;
- ақпараттық технологиялар және ақпаратты қорғау саласындағы кадрларды дайындау;
- халықаралық достастыққа ұмтылу.

Компьютерлік ақпараттық қылмыстардың объектілерін ақпараттық қорғау мемлекеттік жүйеде ақпараттық қауіп, оның объектілері және тәсілдері деп бөліп қарастырылады. Соның

ішінде осы элементтерді ескере отырып ақпараттық қауіпсіздікті қамтамасыз ету саяси салада, экономика саласында, мемлекеттік қорғаныс саласында, төтенше жағдай кезінде, жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелерде, ғылым және техника саласында, жеке тұлғаның рухани өмірі мен ақпараттық қауіпсіздігі саласында және халықаралық достастық саласында өз ерекшеліктерімен жүзеге асырылады деп бөліп көрсетуге болады. Осы салалардағы ақпараттық қауіпсіздіктің жүзеге асырылу ерекшеліктерін толығырақ «Қазақстан Республикасының ақпараттық қауіпсіздік Концепциясынан» көруге болады [48].

Соның ішінде, біз ғылыми жағынан қызығушылық танытқан мына салалардағы мемлекет саясатының ақпараттық қауіпсіздік мәселелерін қарастырған жөн деп таптық. Біріншісі, «жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелердегі» ақпараттық қауіпсіздікті қамтамасыз ету, екіншісі, «ғылым және техника» саласындағы ақпараттық қауіпсіздік, үшіншісі – «жеке тұлғаның рухани өмірі мен ақпараттық қауіпсіздігі», төртіншісі – «халықаралық достастық».

Жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелердегі ақпараттық қауіпсіздікті қамтамасыз етудің негізгі объектілері болып: мемлекеттік құпияларға жататын мәліметтерден тұратын ақпараттық ресурстар, құжаттандырылған ақпараттық массивтер мен мәліметтер базасы түрінде көрсетілген конфиденциалды ақпараттар және мемлекеттік және нарықтық басқарудың ақпараттық жүйелері, ақпарат жүйелері мен құралдары (есептеуіш техника құралдары, ақпараттық-есептеуіш кешендері, желілер және жүйелер), бағдарламалық құралдар (операциялық жүйелер, мәліметтер базасымен басқару жүйелері, басқа да программалық қамтамасыз ету жалпыжүйелік немесе қосалқы құралдар), басқарудың автоматтандырылған жүйелері, мәліметтер байланысы мен тасымалы жүйелері, ақпаратты қабылдау, тасымалдау және өңдеу техникалық құралдары, олардың ақпараттық физикалық жолдары, мемлекеттік құпиялармен жұмыс жасайтын бөлмелер, құпия жұмыстарын жүргізу және құпия сұхбаттарын өткізу жерлері, құралдары және техникалық жүйелері, мемлекеттік құпиядан тұратын мәліметтері бар ақпараттық ресурстар, әскери басқару органдарының, ұлттық қауіпсіздік, ішкі істер органдарының оперативті және стратегиялық

дайындық пландары жөніндегі әскери әрекеттері, олардың сандық және кадрлық құрамы туралы, қызмет бағыттары, мобилизациялық дайындығы туралы, әскермен және қарумен басқару және байланыс жүйесі туралы, ақпараттық қамту және инфрақұрылым туралы мәліметтер бар ақпараттық ресурстар, «Электронды үкіметтің» ақпараттық инфрақұрылымы табылады.

Жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелердегі ақпараттық қауіпсіздікті қамтамасыз етудің негізгі бағыттарына мыналар жатады:

– мемлекеттік басқару органдарының ақпараттық жүйелерінің тоқтаусыз жұмыс істеуін қамтамасыз ету;
– техникалық шпиондық құралдардан арнайы қорғаныс;
– өңделіп жатқан немесе ақпараттың техникалық құралдарында сақталынған ақпаратқа заңсыз кіруді болдырмау;
– өңделіп жатқан ақпараттардың электромагниттік сәулелену арқылы шығып кетуінің алдын алу;
– ақпараттың бұзылуын, жойылуын, өзгеруін келтіретін және ақпараттық құралдардың жұмысында ауытқулар келтіретін әрекеттердің алдын алу;
– электронды құрылғылардың объектілері мен техникалық құралдарына енгізілген ақпаратты бұрып алу қондырғыларын анықтап табу;
– мекемелер мен объектілерде жүрген сөйлесу мәліметтерін техникалық құралдармен бұрып алуға жол бермеу.

Жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелердегі ақпараттық қауіпсіздікті қорғаудың негізгі ұйымдастырушылық-техникалық шаралары мыналар:

– ақпаратты техникалық қорғау саласындағы ұйымдардың қызметін лицензиялау;
– мемлекеттік құпияларға жеке және заңды тұлғалардың рұқсатының және кіруінің жүйелік шешімін жасау;
– ақпараттық қауіпсіздікті қамтамасыз етудің талаптарын орындау бойынша информатизация объектілерін аттестациялау;
– информатизация және байланыс құралдарының, ақпаратты техникалық қорғау құралдарының ақпараттық қауіпсіздік талаптарына сәйкестігін дәлелдеу және эффектілігін қадағалау;

– қорғалған орындалудағы ақпараттандырылған және автоматтандырылған басқару жүйелерін жасау және қолдану;
– ақпаратты техникалық қорғаудың құралдарын және оның эффектілігін қадағалау тәсілдерін жасау және пайдалану;
– телекоммуникациялық-ақпараттық жүйелерде және локалды есептеуіш желілерде компьютерлік вирустардың жұғуынан, заңсыз кіру әрекеттерінен ақпаратты қорғауды ұйымдастыру;
– локалды есептеуіш желілерін ақпаратқа заңсыз кіруден қорғау эффектілігін қадағалауды жүргізу;
– ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарды компьютерлік ақпараттың қауіпсіздігі саласында ұйымдастыру, координациялау және қаржыландыру;
– ақпараттық қауіпсіздіктің қауіп төндіретін қайнар көздерін анықтау, бағалау және болжамдау;
– мемлекетаралық келісулер шегінде ақпараттық қылмыстармен күресу мәселелері бойынша тәжірибемен алмасу қатынастарын кеңейту;
– ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мамандарды дайындау жөніндегі оқу-әдістемелік және материалдық базаны жасау;
– мемлекеттік органдар мен ұйымдардың өзіндік қауіпсіздігін күшейту, ақпараттық құпиялық пен қорғау режимін қамтамасыз ету.

Ғылым және техника саласында ақпараттық қауіпсіздіктің негізгі объектілеріне мемлекеттің технологиялық, ғылыми-техникалық, әлеуметтік-экономикалық дамуына маңызды мәлімет пен білімді келтіретін фундаменталды, ізденіс және қосалқы ғылыми зерттеулер, патенттелмеген технологиялар, ноу-хау, модельдің өндірістік жобалары және зерттеулік құрылғылар (бұлар патенттелмеген және ҚР-дың заңнамасына кірмегендіктен, конфиденциалдық мәртебе алмағандықтан шет елге сатылып кетуі, талан-таражға салынуы және тарап кетуі мүмкін), зияткерлік меншіктің объектілері (жаңалықтар, ашулар, шығармалар, олардың патенттері, өндірістік жобалар, бағдарламалық өнімдер және т.б.) жатады.

Мемлекет жағынан қауіптерге қарсылық жолы ретінде осы саладағы заңнаманы және оны жүзеге асырудың механизмдерін

үнемі жетілдіріп отыру табылады. Осы саладағы қауіптің алдын алудың және нейтрализациялаудың (бейтараптандырудың) көптеген шаралары, әсіресе, ғылыми кадрлерге қатысты мемлекеттің әлеуметтік және экономикалық саясаты саласына жатады.

Жеке тұлғаның рухани өмірі мен ақпараттық қауіпсіздігі саласында. Осы саладағы ақпараттық қауіпсіздікті қамтамасыз етудің объектісі ретінде адамдардың көзқарасы, олардың өмірлік құндылықтары және идеалдары, әсіресе мемлекет пен қоғамға маңыздылардың бірі патриотизм, азаматтық парыз, этникалық және діни шыдамдылық және т.с.с., тұлғаның әлеуметтік және жеке ориентациясы, мәдениеттік және эстетикалық сұранымдары, тұлғаның психикалық денсаулығы табылады.

Рухани өмір саласы басқаларына қарағанда бұқаралық ақпарат құралдары арқылы көбінесе жүзеге асырылатын ақпараттық-пропагандалық әрекеттерге, идеологиялық қысымға, мәдениеттік экспансияға өте сезімтал келеді. Осыған байланысты бұқаралық ақпараттық құралдар (БАҚ) тұлғаның рухани өмірінің қалыптасуында анықтаушы рөл атқарады. Ол БАҚ қоғам алдында үлкен жауапкершілікке ие дегенді білдіреді. Соның ішінде ерекше орынды Интернет алып отыр, ол өзінің ашықтығы мен қол жетімділігі арқылы халықаралық терроризм мүддесі үшін, яғни теріс ақпарат арқылы адамдарға әсер ету құралы ретінде, қатыгездікке, ұлтаралық бөлініске, діни экстремизмге итермелейтін құрал ретінде пайдалануы мүмкін.

Рухани өмір саласындағы қауіптің алдын алу және нейтрализациялау, ең басты, елімізде қоныстанған көптеген этностардың тарихи және мәдени салт-дәстүрлерін, мүдделерін ескеретін мемлекеттік идеологияны қажет етеді. Осындай идеология негізінде ақпараттық қауіпсіздіктің қауіптерін бағалаудың нақты критерийлері, негізгі приоритеттері және осы саладағы мемлекеттік саясат жасалуы мүмкін.

Зиянды және теріс ақпарат трафигін қадағалау мақсатында ұйымдастырушылық-құқықтық шараларды жүзеге асыру, Интернет саласын құқықтық реттеу жұмыстары қажеттілік тудырып отыр.

Тарихи-мәдениеттік ғұрыптарды құрайтын ақпараттық ресурстардың сақталуын және дамуын қамтамасыз ететін, сонымен қоса мәдениеттің коммерциализациялауына қарсылық көрсететін құқықтық және ұйымдастырушылық шараларды жасау қажет.

Уақыт өте келе қылмыстық аренада халықаралық компьютерлік қылмыстар фактісі кең таралып келеді. Көптеген ғылыми зерттеулерден байқайтын болсақ, соңғы жылдары қылмыспен күресуде халықаралық байланыстың ұғымы, мақсаты және сипаты біршама өзгеріске ұшыраған.

Қазіргі кезде халықаралық байланыстың қажеттілігі ұлттық құқыққорғау органдарының тәжірибелік қызметінен, яғни шет ел мемлекетінің территориясында дәлелдемелерді алу мүмкіндігінен, заңда көрсетілген қылмыстық іс жүргізу әрекеттерін жүргізу мүмкіндігін қамтамасыз етуден, әділ соттылықты жүргізуден байқалады.

Ол, бір жағынан, халықаралық құқықтық нормалармен, екінші жағынан, еліміздің қылмыстық және қылмыстық іс жүргізу заңдарымен реттеледі.

Сол себепті бұл бағдарламадан халықаралық достастық саласында ұсынылатын жағдайларды қарастырып өтейік. Ақпараттық қауіпсіздік саласындағы халықаралық достастық саяси, әскери, экономикалық, мәдени және басқа да дүниежүзілік достастықтың қатысушы елдері арасындағы қарым-қатынас түрінің ажырамас құрамдас бөлігі болып табылады.

Қазақстан Республикасының мүдделеріне жауап беретін достастықтың негізгі бағыттарына мыналар жатады:

– трансшекаралық ақпаратпен алмасу және алмасу регламентінің ақпараттық қауіпсіздігін қамтамасыз ету, сонымен қоса осы ақпараттарды телекоммуникациялық арналар арқылы өткізу барысында мәліметтің бұзылмауын және сақталуын қамтамасыз ету;
– халықаралық қарым-қатынастардың қатысушы мемлекеттердің компьютерлік қылмыстармен күресумен байланысты қызметтерін координациялау;
– ақпараттық алмасудың жаңа жүйелерін жасау бойынша халықаралық жобаларды біріге жасау, технологиялық базаларды жетілдіру, ақпараттық жүйелерді және ақпараттық ресурстардың қауіпсіздік жүйелерін ұйымдастыру және т.б.

Ерекше назар бұрынғы Тәуелсіз Мемлекеттер Достастығына кірген қатысушы-мемлекеттермен, Ұйымдық қауіпсіздік туралы шарттың ұйымдарымен, Шанхай достастық ұйымының мемле-

кеттерімен, Еуразиялық экономикалық бірлестіктің қатысушы-мемлекеттерімен қарым-қатынас жасауға бөлінеді.

Достастықтардың аталған бағыттарда мақсаттарын жүзеге асыру үшін мыналарды басшылыққа алуға тиіс:

– Қазақстанның ақпараттық қауіпсіздікті қамтамасыз ету саласындағы жұмыс жасайтын халықаралық ұйымдарда белсенділік танытып қатысуы;
– осы саладағы тәжірибелермен алмасу, соның ішінде әсіресе халықаралық және отандық шығармалар мен басылымдарды алмастыру арқылы және мемлекеттер арасында тиісті өкілдерді тәжірибеге жіберу арқылы.

Жоғарыда қарастырылған мәселенің барлығы Қазақстан Республикасы қылмыстық саясатының теориялық тұрғыдағы бір бөлігі ғана. Қылмыстық саясат теорияға негізделген бағдарламалар мен бағыттардан басқа міндетті түрде тәжірибелік сипатқа ие жүзеге асыру жұмыстарынан және олардың нәтижелерінен тұруы тиіс. Сол себепті ендігі біздің қарастыратынымыз осы уақытқа дейін көрініс тапқан тәжірибелік аспектілер.

Қазақстан Республикасы қылмыстарды тергеу тәжірибесінде осыған қатысты XXI ғасырдың басында біраз шаралар қолданған болатын. Құқыққорғау органдарында, әсіресе халық тығыздығы жоғары, даму дәрежесі қарқынды мегаполистер мен қалаларда компьютерлік қылмыстар мен оларға тектес немесе қатарлас қылмыстарды тергеумен айналысатын арнайы бөлімшелер құрылды. Кейбір қалаларда немесе елді мекендерде мұндай инициатива, біз білетіндей, Қылмыстық іс жүргізу кодексі негізінде жергілікті құқыққорғау органдарының басшыларымен ұйымдастырылады. Мысалы, тергеу бөлімінің бастығы мұндай тапсырманы бермес бұрын, қызметкердің жаңа технологияларға деген икемділігін, қызығушылығын, білімін, тәжірибесін және басқа да ерекшеліктерін, жұмысқа деген ынтасын ескереді.

Кейбір жағдайда құқыққорғау қызметкерлерінің арасында тергеу жұмысын қолайлы жүргізу үшін арнайы техникалық білімі бар азаматтардың да кездесіп жатуы мүмкін. Компьютерлік техниканы жастар арасында жоғары техникалық білімсіз де жақсы игеру тәжірибелері кездесіп жатады, ондай тұлғаларды біз «делитант» деп атаймыз, оның әрине жағымды да, жағымсыз да жақтары болуы ықтимал.

Қазақстан Республикасында 2003 жылы «ҚР ІІМ ақпараттық технологиялар саласындағы қылмыстармен күресуді ұйымдастыру бойынша басқармасы» құрылған болатын және оның мақсаты мына бағыттарда қызмет жасау болатын:

– компьютерлік ақпарат саласындағы қылмыстармен күресу (ЭЕМ, олардың жүйелері мен желілері, соның ішінде меншік иесінің құқықтары қылмыстық қолсұғушылықтың объектісі болып табылады);
– телекоммуникациялар саласындағы қылмыстармен күресу (ЭЕМ, олардың жүйелері мен желілері қылмысты жасаудың құралы болып табылады);
– азаматтардың конституциялық құқықтарына қол сұғатын қылмыстармен күресу (жеке өмірге қол сұғылмаушылық, жазба құпиялығы, телефондық, пошталық, телеграфтық және басқа да хабарлар мен мәліметтер құпиялығы);
– адамгершілікке қарсы қылмыстармен күресу (порнографияны тарату, Интернет женгетайшылығы, балалар порнографиясы);
– экономикалық қызмет саласындағы қылмыстармен күресу (тауарлық белгіні заңсыз пайдалану, лицензиялы өнімдерді жалған түрде жасау, жалған төлем карталарын дайындау және өндіру және т.б.);
– жоғары технологиялар саласындағы қылмыстармен күресу аясындағы халықаралық міндеттемелерді тікелей жүзеге асыру (трансұлттық компьютерлік және телекоммуникациялық қылмыстар туралы мәліметтер бойынша шетелдік құқыққорғау органдарымен жедел қарым-қатынас іс-әрекеттерін жүзеге асыру, кейінге қалдырылмайтын ақпараттармен алмасу, «Үлкен Сегіздік» мүше елдері және Интерпол форматында іздестіру тапсырмаларын орындау және сұраныстармен алмасу);

Бүгінгі таңда «К» басқармасы өзіне жүктелген тапсырмаларды жүзеге асыра отырып қылмыспен күресудің маңызды нәтижелеріне жетті. Олардың ішінде зияткерлік меншік нарығындағы құқықбұзушылықтарды анықтау және алдын-алу, авторлық және сабақтас құқықтардың объектілерін заңсыз шығару, тарату және пайдаланумен байланысты қылмыстарды уақытылы ескерту және тергеу. Құқыққорғау органдарының қызметкерлері лицензиялы өнімдерді жалған түрде (пираттық DVD, CD-дискілер,

бағдарламалық қамтамасыз ету, жүйелік бағдарламалар, компьютерлік бағдарламалар) жасаумен айналысатын тұлғаларды анықтаумен айналысып келеді. Сонымен қатар олар телекоммуникация желілерінде, банктік салада және ақша операцияларын жүзеге асыратын басқа да салаларда болатын қылмыстармен күреседі.

Компьютерлерді байланыстыратын желі ИНТЕРНЕТ қысқа уақыт ішінде жалпы жер шары бойынша жаһанды ақпараттық жүйеге айналды. Сонымен қатар Интернет желісінің мүмкіндіктері барған сайын жиі-жиі заңға қайшы іс-әрекет жасаудың құралына айналып барады. Компьютерлік қылмыстылық – бұл компьютерлік ақпарат қылмыстық қолсұғушылықтың пәні болып табылатын компьютерлік қылмыстардың жиынтығы, сонымен бірге компьютерлік ақпарат қоғамға қауіпті іс-әрекеттердің объектісі болатын басқа да қылмыстардың жиынтығы. Бұл компьютерлік ақпарат саласындағы заңға қайшы іс-әрекеттер қазіргі әлемнің ең зиянды құбылыстарының бірі болып отыр [49].

Адам өміріне қазіргі заман ақпараттық технологиялардың енуі қоғамды ақпараттандыру барысының нәтижесі. Бұл іс материалдық өндірісті және әлеуметтік қызмет пен саланы басып алып, өзіне ақпаратты жасауды, өңдеуді, және таратуды қамтамасыз ететін ақпараттық техника мен технологияларды жасауды; ақпараттандыру құралдары мен істерін пайдалануға және дамытуға үлесін қосатын инфрақұрылымды ұйымдастыруды; ақпаратты, ақпараттық өнімдерді және ақпараттық қызмет түрлерін жасауды кіргізеді.

Ақпараттандыру (информатизация) үдерістерінің объектілері болып табылады: ақпараттық технологиялар; кез келген құрылғының жадысында хабарламалар, құжаттар немесе мәліметтер базасының массивтері түрінде сақталатын немесе жұмыс жасайтын машинамен өңделетін ақпарат; бағдарламалық өнімдер; ақпараттық-есептеу жүйелері не желілері; ақпараттық қызметтер.

Ал ақпараттандыру саласындағы қарым-қатынас субъектілері болып: жеке және заңды тұлғалар; мемлекеттік органдар және ақпараттық жүйелердің, технологиялар мен қызметтердің, бағдарламалық өнімдердің, машинамен өңделетін ақпараттың авторлары, сақтаушылары, иеленушілері немесе тұтынушылары болып келетін әкімшілік-аумақтық құрылымдар табылады. Ақпараттандырудың инфрақұрылымына коммуникация жүйеле-

рі, ақпараттық объектілер мен технологиялардың өз арасында қарым-қатынасын қамтамасыз ететін есептеу құралдары мен желілердің жүйелері кіреді; аппараттық және есептеу жүйелерінің жұмысын демеп тұратын бағдарламалық құралдар; ақпараттық құралдар және мәліметтер базасы; ақпараттандыру ісінің әсерлі дамуына үлесін тигізетін экономикалық және құқықтық механизмдер [50].

Сонымен, ақпараттандыру қоғам мен оның әр мүшесінің ақпараттандырылуының дәрежесін көрсетеді, тіпті адамдар санасында әлемнің ғылыми негізделген және жеткілікті суреттелген негізін, сәйкесінше материалдық және рухани құндылықтарын қалыптастырады. Қоғамды ақпараттандыруда маңызды рөлді компьютеризациялау атқарады. Компьютеризациялаусыз ақпараттандыру мүлдем жүзеге асырылмас еді немесе өте аз мөлшерде ғана көрініс табатын еді. Бірақ ақпараттандырудың мөлшеріне компьютеризацияның сапалық және сандық қасиетті үлкен ықпал етеді. Көп жағдайда қоғамға не компьютерлік техниканың саны жетпей қалуы мүмкін, бұл жағдайда адамдарға жұмысын кезектесіп істеуге тура келеді, яғни бірін-бірі күту керек болады, нәтижесінде жұмысқа үлкен залал келтіріледі, үлкен ұйымдарда үлкен шығын болады, не техника сапалық жағынан жиі істен шығып тұруы мүмкін, яғни тағыда жұмыста ауытқулар мен тоқтап қалулар орын табады, оларды іске қосу үшін арнайы білімі бар мамандарды шақыруға тура келеді, яғни тағы уақыт кетеді, нәтижесінде жұмыс бабында үлкен қатер туындайды. Компьютеризация белгілі пәндік саладағы адам қызметінің (өндірістік немесе басқарушылық) нақты түрлерін автоматты түрде техникалық жүзеге асыруды білдіреді.

Жалпыадамдық ақпараттандырудың жағымсыз құбылысы болып компьютерлік қылмыстылықтың пайда болу фактісі болып отыр. Ақпараттандыру ісі соншалықты жылдам, қоғам оның жағымсыз салдарын болжай алмай, оның кейінгі нәтижелерін жою үшін немесе күрес жүргізу үшін шаралар кешенін ойластыра алмады. Сөйтіп, есептеу техникалары мен персоналды компьютерлердің қолжетімдігі компьютерлік білімнің оның мүмкіндіктерімен бірге тұрғындардың кең бөлігінде тарауына қадам алды. Ақпараттық технологиялардың мұндай мүмкіндіктері мен осы мүмкіндіктерді жүзеге асыру үшін жауапкершілік мөлшерінің төмендігі немесе мүлдем болмауы компьютерлерді қолдану-

шыларға барған сайын мүмкіндіктерін жаңартып отыруға, оларды басқа қылмыс аяларында тексеріп көруге түрткі болды.

Өз кезегінде, ақпараттық алмасу саласындағы қатынастарды реттеу заңнамасының қоғам мүмкіндіктерінен артта қалуы осы компьютерлік қылмыстардың тез арада тарап кетуіне әсер етеді.

Ақпараттық технологиялардың ілгері қарай дамуы пайда болған компьютерлік қылмыстардың жетік дамуына және жаңа немесе қосымша қылмыс түрлерінің пайда болуына немесе ол қылмыстардың жаңа әдістермен, тәсілдермен, мүмкіндіктермен жасалуына негіз болады. Сол қалыпта ортақ пайдаланылатын ресурстарға алшақтанған ақпараттық байланыс жүйесі арқылы жалғану туралы мәселе де болды. Осындай жүйелердің бірі болып қазіргі таңда «Интернет» танылады. Оның пайдалану аясы жылдан жылға кеңейіп барады. Сол алпысынша жылдары пайда болған сәтінде Интернет тек әскери мақсаттағы байланыс түрі болатын және тек санаулы адамдардың ғана оған рұқсаты болатын [51, 224 б.]. Ол таңғаларлық жағдай емес, адамзат үшін жалпы жаңа технологиялар «гаджет» түрінде алғаш арнайы қызметтер үшін шығарылып кейін пайда табу мақсатында социумға таратылады. Ал гаджеттерді біз бірінші кезекте материалдық және тәжірибелік кейпін алмай тұрып қиял-ғажайып фильмдерде, шытырман оқиғаларда көреміз, содан кейін бұл қиялдық идеялар қолданыста жүзеге асырылады. Жалпы өмірде осы фактор үлкен ғылыми-техникалық прогрестің түрткісі және механизмі болып табылады.

Ал аталып кеткен қылмыстылық пен қоғамдағы жағымсыз көріністерді ескерту және жою үшін мемлекет өзінің қызметінің бағыттары, нысандары және әдістері бойынша жүзеге асырылатын саясатты қалыптастырады. Аталған әдістемелік талаптарды есепке алып осы мәселеге қатысты қылмыстық саясат ұғымы ретінде түсіну керек:

а) тиісті басқарушылық актілерде орын тапқан компьютерлік қылмыстылықпен күресудің мемлекеттік саясатын;

б) ғылыми теорияны және сәйкес саяси, әлеуметтік және құқықтық ілімдердің синтезін (бірігуін);

в) компьютерлік қылмыстылықпен белсенді, ынталы күресу іс-әрекеттеріне бағытталған әлеуметтік қызметтің ерекше түрін.

Компьютерлік қылмыстармен күресуде мемлекеттің, жалпы социумның жиі кездесетін белгілі идеялары немесе қағидалары

бар. Ал осы саладағы қылмыстармен күресу саласында қылмыстық саясатты түсіну немесе ұғыну үшін осы идеялар мен қағидаларды құрастыратын білімдерді анықтаусыз мүмкін емес, себебі осы қағидаларды біріктіру арқылы біз саясаттың өзін айқындаймыз.

Компьютерлік қылмыстармен күресу саласындағы қылмыстық саясаттың қағидалары қатарына келесілерді кіргізуге болады: теңдік қағидасы, демократиялылық, әділдік қағидасы, ізгілік, адамгершілік қағидасы, жауапкершілік қағидасы, заңдылық қағидасы, ғылымилық және т.б.

Теңдік немесе теңқұқықтылық қағидасы дегеніміз кез келген адам заң мен сот алдында абсолютті түрде тең, оның нәсіліне, діни нанымына, жынысына, түріне, жасына, тіліне, ұлтына, еліне, көзқарастарына, тәндік қасиеттеріне, материалдық жағдайына, шығу тегіне, туған жеріне, тұрғылықты жеріне, қызмет бабына, қанына, түсіне, дене бітіміне және басқа да адамды өзге адамнан ерекшелейтін қасиеттеріне және жағдайларына қарамастан жауапкершілігі, міндеттері мен құқықтары жағынан тең екенін білдіреді. Нақ осы ерекшеліктер компьютерлік қылмыстылық қатынастар арасында да негіз болады.

Демократиялылық дегеніміз компьютерлік қылмыстылық саласындағы мәселелерді реттеу барысында қоғамның, жеке адамның және мемлекеттің мүдделері, құқықтары мен бостандықтары ескеріле отырып тиісті дирекциялық іс-шаралар жүзеге асырылады, яғни қылмыстық саясатты жүзеге асыруда бірінші орында жеке адамдардың ерік-ықтиярынан көрініс табатын қоғамның жалпылық мүддесі болады. Мемлекеттің құқықтық негіздерін бекіту мен ұйымдастыру кезінде адамдардың тікелей немесе жанама да қатысуы қажет. Халықтың мемлекеттік аппарат қызметіне әсер етуі, қоғамдық пікірдің үнемі есепке алынуы, азаматтық қадағалау мен бақылаудың жетілуі демократиялылық қағидасының түпнегізін сипаттайды. Мемлекет компьютерлік қылмыстармен күресудің негізгі бағыттарын анықтағанымен, жеке адамның немесе азаматтың, халықтың, азаматтық қоғам институттарының қатысуымен ғана қажетті іс-шаралар сәттілікке душар болады.

Әділдік қағидасы қылмыс жасаған тұлғаға қатысты қылмыстық-құқықтық сипаттағы жазалау және басқа да шаралары істелген қылмыстың қоғамға қауіптілігі дәрежесі мен сипатына, кел-

тірілген залал мөлшеріне және жаза мөлшеріне әсер ететін басқа да жағдайлар мен белгілерге сәйкес әділетті түрде тура тағайындалған болуы керек. Ешкім де бір қылмыс үшін екі немесе одан көп рет, әлде қайта жауапқа тартылмауы тиіс. Сот жазаны тағайындау кезінде эмоция, жек көрушілік немесе кек алу сезімдерімен емес, тек жасалған қылмыстың объективті бағасы мен кінәлінің тұлғалық қасиеттеріне сүйене отырып жүзеге асыруы тиіс.

Ізгілік қағидасы қылмыстық заңнама адамның қауіпсіздігін қамтамасыз ету керек дегенді білдіреді және қылмыстық-құқықтылық жаза мен жазалау институттары қылмысты жасаған тұлғаға тәндік зорлық-зомбылық келтіруді және адамның арнамысын жерге таптауды мақсат қылып қоймайды. Ізгілік дегеніміз – адамның ар-намысын, қадірін сыйлауды, қоғам ісі мақсаты ретінде адамның игіліктеріне талпынуды, адамның жеке тұлға ретіндегі құндылықтарын білдіретін адамгершілік ұстаным.

Жауапкершіліктен құтыла алмау қағидасы қылмысты жасаған кез келген тұлға қылмыс үшін жауапкершілікті міндетті түрде тартуы тиіс дегенді білдіреді. Бұл қағида арқылы мазмұны жағынан жалпылық сипаттағы заңдылық пен теңдік қағидалары нақтыландырылады немесе тура мағынаға ие болады.

Заңдылық қағидасы қылмыс жасаудың қылмыстық іс-әрекеті, оның белгілері, жазаланушылығы және басқа да нәтижелері сәйкесінше әдетте тек заңмен анықталады деген идеясы ретінде түсіндіріледі. Ешкім де қылмыстық жазаға заңсыз тартылмауы тиіс, заңдылық қағидасы бойынша тұлға жауаптылыққа тек сот үкімі, шешімі бойынша және тек заң негізінде тартылуы керек. Адам заңмен тыйым салынғанның барлығынан алшақ болу тиіс. Заңдылықтың өзінің функциялары бар – заң тыйым салады, рұқсат береді, өкілеттік береді, бағыт береді, реттейді, жазалайды және қорғайды.

Бұл қағиданың тағы бір мағынасы оның басқа құқықтық реттеу түрлерінен қарағанда заң билігі мен құқық билігі ісінде басты жүзеге асыру қабілетінде.

Ғылымилық қағидасы компьютерлік қылмыстылықпен күрес жүргізу стратегиясын және тактикасын ұйымдастыру кезінде қылмыстылықпен күресуде максималды мүмкін болатын нәтижелерге жетуді қамтамасыз ететін ғылыми объективті заңдылықтардан, фактілі ережелерден, шынайы мүмкіндіктерден бастама алу керек екендігін білдіреді.

Ең алғаш Қазақстан тәуелсіздік алғаннан кейін фактілі және заңи түрде компьютерлік немесе ақпараттық құқықбұзушылықтарға қарсы шараларды жүзеге асыру саласындағы мемлекеттің саясаты Қазақстан Республикасының қолданыстан шыққан 1997 жылғы Қылмыстық кодексінің нормаларында көрініс тапқан. ҚР 1997 жылғы Қылмыстық кодексінің 227-і және 227-1-і баптарында келесі қылмыстық іс-әрекеттер үшін қылмыстық жауаптылық қарастырылған еді:

1) Заңмен қорғалатын компьютерлік ақпаратқа, яғни машиналық сақтағыштағы, электронды есептеу машинасындағы (ЭЕМ), ЭЕМ жүйесіндегі немесе олардың желісіндегі ақпаратқа заңсыз кіру, сол сияқты ЭЕМ-ге, ЭЕМ жүйесіне немесе олардың желісіне кіре алатын адамның ЭЕМ-ді, ЭЕМ жүйесін немесе олардың желілерін пайдалану ережелерін бұзуы, егер бұл әрекеттер ақпаратты жоюға, бөгеуге, жаңартуға (өзгеріске) не көшіруге, ЭЕМ жұмысын, ЭЕМ жүйесін немесе олардың желісін бұзуға әкеп соқса;

2) Ақпаратты санкциясыз жоюға, бөгеуге, өзгертуге не көшіруге, ЭЕМ жұмысын, ЭЕМ жүйесін немесе олардың желісін бұзуға көпе-көрінеу әкелетін ЭЕМ-ге арналған бағдарламалар жасау немесе қолда бар бағдарламаларға өзгерістер енгізу, сол сияқты осындай бағдарламаларды немесе осындай бағдарламалары бар машиналық сақтағыштарды пайдалану немесе тарату;

3) Жасап шығарушының немесе заңды иесінің келісімінсіз ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын құқыққа сыйымсыз өзгерту, ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын құқыққа сыйымсыз жасау;

4) Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын өзгертуге немесе ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын жасауға мүмкіндік беретін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату [52, 81 б.].

Бұл баптар сөзсіз дұрыс және қолданыста жүзеге асырылған, бірақ заман талабына онша келіңкіремейді. Бұл қылмыс әрекеттер шеңбері өте кең, енді осы қылмыстық әрекеттерді қазіргі заман талаптарымен, қазіргі адамдар сөз айналысымен, жастар слэнгтерімен, жаңа ақпараттық ғылыми терминдермен алмастыра, жаңа тәсілдерді пайдалана атап көрейік.

1) Ең бірінші, ең жиі кездесетін қылмыс түрі ол бөтен біреудің компьютеріне, компьютерлік техникаға немесе ақпараттық жаңа технология түріне заңсыз кіру, оның өзі бірнеше тәсілмен жүзеге асырылуы мүмкін: а) компьютерлік техникаға тікелей кіру; б) локалды желі арқылы басқа нүктеден қосылу арқылы кіру; в) интернет желісі арқылы кіру (оның өзі сым арқылы және сымсыз жалғану әдістерімен жасалады).

2) Бөтен біреудің компьютеріне кіру әрдайым қылмыс бола бермейді, ол үшін басты талап, яғни кіру заңға қайшы болуы керек немесе компьютерлік құрал иесінің рұқсатынсыз болуы керек және қылмыстық кодекстің гипотезасында көрсетілгендей компьютердегі ақпарат немесе мәлімет жойылу, бұзылу, көшірілу, бөгелу, өзгеру керек. Ал Қылмыстық кодекстегі «жаңарту» әрекеті онша түсінікті емес.

Бұл әдістердің әрқайсысы жеке қылмыс түрлерін тудырады:

а) жою, көшіру, бұзу тек компьютерлік техника құралдарында ғана емес, қазіргі заманның жаңа туындыларына қарсы жасалуы мүмкін, яғни бұл қылмыстық әрекеттердің басты объектілері болуы мүмкін: ұйымдық жұмыс жасау компьютерлері, үйдегі персоналды компьютерлер, ноутбуктер, нетбуктер, макбуктер, персоналды планшеттер, ұялы телефондар, жады карталары (карта памяти), смартфондар, симкалар (sim-карталар), USB флешкалар, сыртқы қатты дисктер (hard disk), дискеталар, DVD, CD дискілер, тіпті MP3 ойнағыштар және электронды цифрлі видеокамералар мен фотоаппараттар, себебі қазіргі технологиялардың көбінде немесе барлығында десек қателеспейміз, компьютерлік бағдарламалар мен бағдарламалық қамтамасыз етулер қолданылады;

б) компьютерлік құралдың жұмысын бұзуды, бөгеуді жүзеге асыратын басты амал ол компьютерлік вирустық бағдарламаларды енгізу және тарату. Вирустық бағдарламалар жоғарыда аталып кеткен барлық жаңа технологиялар түрлеріне қарсы жасалуы мүмкін. Осыдан біз оның әсер ету аясы өте үлкен екенін көреміз. Компьютерлік ВИРУСТАР мәселесі өте үлкен тақырып, ол жөнінде біз зерттеу жұмысымыздың келесі бөлімдерінде нақтырақ тоқталып өтеміз.

3) Компьютерлік ақпараттық техника құралдарындағы мәліметті ұрлау ерекше көңіл бөлетін қылмыс түріне жатады. Көп жағдайда компьютерлік қылмыстар электронды техникада

сақталатын ақпаратты, мәліметті ұрлау мақсатында жасалады. Компьютерлік ақпаратты ұрлау түрлі ниеттермен жасалуы мүмкін: пайда көру мақсатында, кек алу, жек көрушілік мақсатымен, бұзақылық, кәсіби қызығушылық мақсатында, біреудің әсерімен, сөз беру мақсатында, мүмкіндігін тексеру үшін, кейде тіпті жай уақыт өткізу үшін. Алғашқыда айтқандай компьютерлік қылмыстардың объектілері персоналды компьютерден басқа түрлі нано-технологиялар болуы ықтимал, сол себепті қылмыскерлер ақпаратты не мәліметті ұрлау кезінде мәлімет сақталатын техникалық құралды да қоса ұрлауы мүмкін. Тергеу органдары қылмысты бірнеше құрам бойынша саралауы мүмкін немесе тек техниканы ұрлау деп қарастыруы мүмкін, бірақ бұл жерде басты объект болып компьютерлік ақпарат болуы тиіс. Электронды сақтағыштағы немесе компьютерлік гаджеттегі мәлімет олардың өзінен бірнеше мәрте қымбат болуы мүмкін. Мысалы, егер планшет шамамен 100 мың теңге көлемінде тұрса, ондағы ақпарат миллиондаған соммамен бағалануы мүмкін немесе ақпарат оның иесіне құны жоқ қазынамен тең болуы мүмкін.

2. АҚПАРАТТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫҢ ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ ЖӘНЕ КРИМИНОЛОГИЯЛЫҚ СИПАТТАМАСЫ

2.1. Компьютерлік технологияларды пайдалану және байланыс саласындағы құқық бұзушылықтардың қылмыстық-құқықтық сипаттамасы

Қылмысты түбегейлі жоюға бағытталған, осы саладағы басқа ойларды қолдамайтын мемлекеттің біржақты саясаты объективті түрде әлеуметтік конформизмге әкеледі.

Қылмыспен күресу доктринасына қатысты қазіргі кездегі талаптарға сай осы қызметтен басқа біройлы пікір жоқ. Т.Э. Караевтың пікірінше, қылмыспен күресудің саясаты жөнінде жаңа сапалы концепциялар керек, соған қарамастан Т.Э. Караевтың өзі қылмысты түбегейлі жоюға бағытталған ескі доктринаның өкілі болып отыр. Компьютерлік техниканы пайдаланумен байланысты жасалатын қылмысқа қатысты функционалды сипаттамамен анықталынатын құқықтық бақылаудың әдіс-құралдардарының негізінде оны екі түрге бөліп көрсетуге болады: 1) позитивті құқықтық бақылау; 2) репрессивті құқықтық бақылау.

Компьютерлік техниканы пайдаланумен байланысты қылмыстылықты позитивті құқықтық бақылауға компьютерлік техника мен оның қосалқы элементтерін заңды және заңсыз қолдану мен пайдалану және қылмыстық жауаптылық тудырмайтын мақсаттағы оларды тікелей қолдану нәтижесінде алынған өнімдерді заңды және заңсыз пайдалану барысында жинақталатын құқықтық қатынастарды реттейтін нормалардың жиынтығы кіреді [53]. Дүние жүзі бойынша компьютерлік программалар, компьютерлердің математикалық қамтылуы авторлық құқықтың объектісі болып табылады. Ю.М. Батуриннің айтуынша: «Авторлық құқықтың объектілеріне ЭЕМ мен мәліметтер базасына арналған бағдарламалар жатады. Сонымен қоса

бағдарламаларды авторлық құқықпен қорғау шектеулі сипатта болады. Авторлық құқық шығарманың нысаны мен мазмұның бірқалыпта сақтайтыны бізге мәлім. Егер оның нысаны мен мазмұны өзгеріп кететін болса, онда авторлық құқықта жеке құқықтық қорғауды иеленетін жаңа объект пайда болады. Бірақ авторлық құқық тәуелсіз (объективті) ұқсастыққа қарсы қорғау құқығын бере алмайды, әсіресе бағдарламалық қамтуларды шығару кезінде, себебі бағдарламаларды жасау кезінде жалпыға ортақ бір ережелер мен формулаларды, әдістерді қолданады. Компьютерлік бағдарламаларды авторлық құқық қорғайды, тек егер олар объективті нысанға (әдетте ол қолжазба) ие болса және тек осы нысанда қолдану кезінде болса. Алайда, ЭЕМ жұмыс істеп тұрғанда бағдарлама қолжазбаға қарағанда өзгерген түрде пайдаланылады, сол себептен авторлық құқық мәні бойынша ешқандай қорғаушылық функциясын атқара алмайды. Бағдарламаларды авторлық құқықпен қорғау толық көлемде оны таралудан, ойнатылудан қорғай алмайды. Автордың келісімісіз тарату не ойнату сипатталған пән бойынша оны пайдалануға ешбір кедергісіз жүзеге асырылады» [54, 115 б.].

Аса маңыздылығы ойнатылудың көрініс табу нысаны материалды тасымалдауышпен байланысты болуы [55]. Авторлық құқықта суретті, мүсінді, қолжазбаны және т.б. анықтауда пішіні, нысаны, бейнесі ойнатылуы маңызды болса, компьютерлік бағдарламаларда жағдай мүлдем өзгереді. Егер бағдарлама қағаз бетіне бейнеленген болса, компьютерлік бағдарлама авторлық құқықтың кәдімгі әдеттегі объектісі бола алады. Бірақ оның құндылығы, бағалығы объективті түрде бағалануы мүмкін, егер де оны сәйкес техникалық тасымалдауышқа (флешка, диск, дискета, HD және т.с.с.) ауыстыру арқылы тікелей мақсатта пайдаланса ғана. Техникалық тасымалдауыш – кез келген не жеке дара сипаттағы түпнұсқалы мәліметті, бағдарламаны, ақпаратты, бейнені, фотоны фиксация жасауға жарамды унифицирленген объект [56].

Құқықтық қадағалаудың осы бөліміне қатысты құқықтық жүйеде ҚР-дың 1992 жылдың 15 қаңтарында қабылданған «ҚР ғылым және мемлекеттік ғылыми-техникалық саясаты туралы» Заңы қызығушылықты танытады [57].

Тауар өндірушінің меншігі болып табылатын компьютерлік бағдарлама қылмыскермен заңсыз жолмен өңделуі, шығарылуы мүмкін, меншік иесінің фирмалық белгісін білдіретін жалған

тауар белгісімен қамтылуы мүмкін, сауда айналымына жіберілуі мүмкін, нәтижесінде меншік иесі материалдық зиян шегеді, ал құқықбұзушы заңсыз материалдық пайда шығарады.

Бұл мәселе тек құқыққорғау органдарына ғана емес, арнайы қызмет қызметкерлеріне де, банктердің қауіпсіздік қызметіне де, информатика саласындағы мамандар мен сарапшыларға да, оқу және ғылыми-зерттеу мекемелерінің өкілдеріне де қатысты, соның ішінде компьютерлік вирустар, компьютерлік техника және бағдарламалық қамту бойынша сарапшыларға да қатысты.

Көп елдердің қылмыстық өрісінде ақпараттық технологиялардың дамуы және оларды қолдану жоғары қарқынмен өсіп келеді, сол себепті ғалымдарға осы саланы, осы саладағы қылмыстарды үнемі бақылап зерттеуге тура келеді.

Көптеген елдердің құқыққорғау органдарына бұл мәселе қылмыстылықтың жаңа түрі ретінде көрінеді. Сондықтан бұл қылмыстарға қарсы күресуге олар әрдайым дайын бола бермейді. Ең басты оның себебі осы саланы реттейтін заңнаманың болмауы, құқыққорғау органдарының қызметкерлерінің дайындығының төмен болуы не мүлдем болмауы және осындай құқықбұзушылықтарды тіркеу, қарау, сәйкес сот сараптамасын жүргізу технологиялары мен техникалық құралдарының болмауы. Бұл дегеніміз өз кезегінде компьютерлік қылмыстармен күресу жөнінде заңнаманы ұйымдастыру, полиция, прокуратура, сот органдары және сараптама мекемелері жүйесінде мамандарды дайындайтын арнайы курстарды жасау қажеттілігін тудырады.

Қазіргі кезде халықаралық компьютерлік қылмыстар фактісі кең тарауда. Әсіресе көп кездесетін компьютерлік алаяқтық, қылмыспен табылған ақшаны заңдастыру үшін компьютерлік техниканы пайдалану, хакерлердің (компьютерлік желіге заңсыз кіретін тұлға) халықаралық ақпараттық жүйелерге кіруі және ақпаратты ұрлауы. Осы мәселеден көріп отырғандай, халықаралық қылмыстарды тергеу кезінде көмек болатын халықаралық процедуралар қажеттілігі және Интерпол шегінде жұмыс істейтін органды ұйымдастыру ұсынысы туындайды.

Жоғары ақпараттық технологиялар саласындағы қылмыстарды тергеуде туындайтын мәселелерді шешу қылмыстарды тергеудің жаңа әдістерін іздеу мен оларды пайдалануға ғана емес, ол үшін арнайы білімді де пайдалануға да тура келеді. Аса жоғары

маңыздылыққа бұл жерде компьютерлік қылмыстарды тергеу барысын реттейтін құқықтық нормалардың жиынтығы ие [58].

Қазақстан Республикасы Конституциясының 20-бабында «әркім заңмен тыйым салынбаған кез келген жолмен ақпаратты алуға құқылы» делінген [59]. Сонымен қатар, Интернет желісі арқылы берілетін ақпараттың ашықтығы тек жеке және заңды тұлғалардың ақпараттық қорғалатындығы туралы мәселені ғана емес, жалпы мемлекеттің де қауіпсіздігі мәселесін көтереді. Ақпараттық саладағы Қазақстан Республикасының Ұлттық мүддесі Қазақстанның әлемдік ақпараттық жүйеге кіруімен шартталып тұр. Сол себепті ақпараттық салада қоғамдық қатынастарды реттейтін нормативтік-құқықтық актілерді қабылдауға тура келді. Сөйтіп, «ҚР Ұлттық қауіпсіздігі туралы» Заңы Қазақстанның ұлттық қауіпсіздігінің бір бөлігі ретінде «ақпараттық қауіпсіздік» ұғымын енгізді [60]. Соған сәйкес, ақпараттық қауіпсіздік дегеніміз ақпараттық саладағы тұлғаның және қоғамның құқықтары мен мүдделерінің және ақпараттық ресурстардың қорғаныстағы жағдайы.

Салыстыру үшін Ресей Федерациясының 1995 жылдан бері әрекет ететін «Информация, информатизация және информацияны қорғау туралы» Заңын қарастырайық. Бұл заң нақты осы салаға қатысты жұмыс жасайды. Ресейден кейін сегіз жылдан соң Қазақстан Республикасының «Информатизация туралы» Заңы күшіне енді [61]. Ол Заң негізінде ақпараттық ресурстар, оларды қолданушылар мен қорғау ұғымын анықтап бекітті және ақпараттық қатынастардың дамуына заңшығарушының уақытылы реакциясы болып табылды.

Информатизация осы уақытта Қазақстан аумағында жаңа негативті (жағымсыз) құбылыстардың пайда болуына, соның ішінде осы саладағы қылмыстарға алып келді.

1998 жылдың 1 қаңтарында алғашқы күшін жойған Қазақстан Республикасының Қылмыстық кодексінде компьютерлік техника мен оның құрылғыларына қатысты тұрақты шешім қарастырылған. Ол Қылмыстық кодекс (ҚР ҚК-нің 7-тарауы 227-бабы) осы салаға қатысты мынадай қылмыс құрамдарын анықтаған еді:

– «заңмен қорғалатын компьютерлік ақпаратқа, яғни машиналық сақтағыштағы электронды есептеу машинасындағы (ЭЕМ), ЭЕМ жүйесіндегі немесе олардың желісіндегі ақпаратқа заңсыз кіру, сол сияқты ЭЕМ-ге, ЭЕМ жүйесіне немесе олардың желісі-

не кіре алатын адамның ЭЕМ-ді, ЭЕМ жүйесін немесе олардың желілерін пайдалану ережелерін бұзуы, егер бұл әрекеттер ақпаратты жоюға, бөгеуге, жаңартуға не көшіруге, ЭЕМ жұмысын, ЭЕМ жүйесін немесе олардың желісін бұзуға әкеліп соқса»;

– «ақпаратты санкциясыз жоюға, бөгеуге, жаңартуға не көшіруге, ЭЕМ жұмысын, ЭЕМ жүйесін немесе олардың желісін бұзуға көпе-көрінеу әкелетін ЭЕМ-ге арналған бағдарламалар жасау немесе қолда бар бағдарламаларға өзгерістер енгізу, сол сияқты осындай бағдарламаларды немесе осындай бағдарламалары бар машиналық сақтағыштарды пайдалану не тарату».

Бұл кодекстің соңғы өзгерістері мен толықтырулары бойынша 227-бапқа 227-1-бабы қосылды, ол да ресми түрде компьтерлік қылмыстар қатарына жатқан, қазір де ақпараттық қылмыстар тарауының қатарына кіреді, оның себебі түсінікті, оны атауынан да көруге болады. Баптың атауы және мазмұны:

– «ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын, абоненттің сәйкестендіру құрылғысын құқыққа сыйымсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгерту үшін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату» [62].

Қазір бұл нақты заңға қайшы әрекеттер үлкен өзгеріске түсе қойған жоқ, бірақ тарихи және саяси тұрғыдан маңызды қадам жасалды, яғни ҚР қолданыстағы Қылмыстық заңнамасында ақпараттық қатынастарды реттейтін және тиісті қылмыстық жауаптылықты қарастыратын «жеке» тарау пайда болды. Бұл сөзсіз заңшығару саласында басты және қажетті қадам болып есептеледі.

Өзіміздің ғалым Т.Б. Сеитов ескергендей, «компьютерлік қылмыстылықтан төніп тұрған қауіп бүгін көптеген елдермен объективті шындық ретінде қабылданып отыр. Оның себебін осы елдердің бұл мәселеге қатысты жүргізіп жатқан ғылыми жұмыстарынан, заңнамаларындағы сәйкес нормаларынан байқаймыз» [63, 14 б.]. Мысал ретінде Т.Б. Сеитов бұрынғы ТМД елдерінің заңнамасына ұсыныс ретінде шығарылған Модельдік қылмыстық кодекстегі құқықтық нормаларды келтіреді. Осы құжаттың 12-ші «Ақпараттық қауіпсіздікке қарсы қылмыстар» тарауындағы баптардың құрамында келесідей қылмыс түрлері кездеседі:

1) компьютерлік ақпаратқа заңсыз кіру;

2) компьютерлік ақпаратты модификациялау [64, 359 б.];

3) компьютерлік саботаж;

4) компьютерлік ақпаратты заңсыз иелену;

5) компьютерлік жүйеге немесе желіге заңсыз кірудің арнайы тәсілдерін дайындау және тарату;

6) зиянды программаларды жасау, пайдалану және тарату;

7) компьютерлік жүйелер мен желілерді эксплуатациялаудың ережелерін бұзу.

Осыған қатысты Т.Б. Сеитовтың пікірі: «ҚР Қылмыстық кодексін дайындау кезінде Қазақстанның заңшығарушылары ұсынылған құрамдардың екеуін ғана таңдап алған» [65, 14 б.]. Қазақстандық заңшығарушылардың ұстанымы толық жетілмеген, заңнамада қылмыскермен жасалатын әрекеттердің барлығы көрініс таба алмаған, ол дегеніміз көптеген қылмыстар үшін қылмыскер жауапкершіліктен босатылады дегенді білдіреді. Мысалы, Ресейлік заңнамада біздің қылмыс құрамдарымыздан басқа «ЭЕМ-ді, ЭЕМ жүйесі немесе желілерін эксплуатациялау ережелерін бұзу» құрамы бар [66]. Оның себебі Ресей Федерациясының құқыққорғау органдары өз жұмыстарында бұл қарама-қайшылықтармен жиі кездеседі.

Ақпараттандыру саласындағы қылмыстарды ескертудің ерекшеліктері тек заңшығарушы органдармен ғана емес, сонымен қатар атқарушы билікпен де қарастырылады. Сөйтіп, Қазақстан Республикасының Мемлекеттік құпияларды қорғау жөніндегі Агенттігінде Үкіметтің қаулысымен 2000 жылы Ақпаратты техникалық қорғау орталығы пайда болды, оның мақсаты мемлекеттік органдардың қызметіне ақпаратты техникалық қорғау құралдарын енгізу және жаңа түрлерін ойластыру. Тағы да ҚР-дың Үкіметі құрамында қазіргі кезде Ақпаратты қорғау жөніндегі мемлекеттік комиссия жұмыс атқарады, оның қызметін оның атауының өзі айтып тұр. Үкіметтің бұл саладағы экономикалық қызметі де байқалады, мысалы, Қазақстан Республикасының Ұлттық банкінің ақпаратқа қатысты конфиденциалдығы мен қауіпсіздігін қамтамасыз ететін бірқатар ережелер мен нұсқаулар дайындалған, мақсаты банктің бөлімшелері мен басқа екінші дәрежелі банктермен электронды төлемдер жүргізу операциялары туралы қауіпсіздік пен жасырындықты қамтамасыз ету. Атқарушы биліктің құқыққорғау қызметі де шетте қалған жоқ, жедел-

іздестіру қызметтері арқылы ҚР-дың электрбайланыс желілерінде арнайы жедел-іздестіру шараларын қамтамасыз ету қарастырылған [67].

Ғылыми-техникалық прогресс қылмыстың мазмұнын күрделі өзгертті, сол себепті қылмыспен күресудің механизмі құрамында да өзгерістерге алып келді. В.А. Мазуровтың айтуынша, компьютерлік технологияларды пайдалана жасалатын қылмыстар тек электронды болмыста ғана емес, сонымен қатар қандай да болсын электронды құрылғылар бар тәндік өмірде де жасалып жатады [68].

Кез келген мемлекеттің ұлттық инфрақұрылымы бүгінгі күні жаңа компьютерлік технологиялармен тығыз байланысты. Банктік және энергетикалық жүйелердің күнделікті қызметі, көлік жүйелері, әуе қозғалысы тіпті медициналық жәрдем мен адамға қажетті күнделікті мұқтаждық қызметтері мен сервисі автоматтандырылған электронды есептеу жүйелерінің дұрыс және қауіпсіз жұмысына толық тәуелді. Қазіргі таңда жалпы қылмыстардың басты бөлігін жаңа технологиялармен байланысты жасалатын қылмыстар саны қамтып келетінін сан алуан рет айттық. Оның тез дамып өсуіне тікелей қазіргі жаңа заманның негізгі бастамасы Интернет ғаламторымен тікелей байланысты және онымен тең дәрежеде күресуді жүзеге асыра алмай келе жатқан өкілетті органдармен және тиісті шаралардың жетіспеуімен байланысты десек те болады.

Компьютерлік қылмыстар қазіргі кездің аса өзекті мәселелерінің бірі. Бұл мәселенің өзектілігі жылдан жылға адамдарды аса қауіппен мазалап отыр. Осыдан тіпті үш жыл бұрын бұл мәселенің жағдайы басқа болды, бес жыл бұрын одан өзгеше болды, ал он жыл бұрын компьютерлік қылмыстар адамзат басшыларын қазіргі кездегідей толғандыра қойған жоқ.

Болашақта жай ғана қатардағы адамның күнделікті өмірін компьютерлік технологияларсыз елестетіп көру де мүмкін емес, жаңа қоғамға жат құбылыс секілді. Мемлекеттердің компьютерлік қылмыстылықпен күресуге бағытталған шараларына қарамастан әлемдегі оның саны күрт өсіп келеді.

Өзекті мәселе болып, осы түрлі, жай ғана қолданыстағы персоналды компьютерлер мен Смартфондардан (ұялы телефондардан) бастап қиын технологияларды пайдалану арқылы, техникалық құралдар мен әдіс-тәсілдерді білетін жоғары білік-

ті мамандардың қызметіне жүгіне отырып, ұйымдасқан қылмыстарды жасайтын тұлғалармен күресу келеді. Казіргі кезде жалған құжаттар мен жасанды ақша белгілері компьютерлік өңдеу мен перифериялық құралдардан шығару арқылы дайындалады. Бұның себебі жаңа техникалар мен технологиялардың кез келген тұлғаға қолжетімді болуы және оларды адамдардың жеңіл пайдалануында.

Жаңа техникалардың тез дамып, қоғамға енуінің жылдамдығына және адамдардың оларды теріс мақсатта пайдалану айласын табуы ағымына, қылмыспен күрес жүргізу инстанцияларының әрқашан бірнеше қадам артта қалуы жаңа ғасырдың үлкен кетігі болып отыр және бұл екі үрдістің осы жылдамдықта қозғалуы ұзақ уақыт өзгермей келеді. Уақыт өте келе ара-қашықтық алшақтап келеді, оның пайдасы тек қылмыскерлердің қанжығасына. Компьютерлерді немесе желілерді пайдалану арқылы жасалатын қылмыстардың қауіптілігі соншалықты адам баласы оны көз алдына елестете алмайды. Жай ғана Интернет арқылы таратылатын ақпараттар мен зияткерлік шығармалар, авторлық және сабақтас құқық иегерлері зиян шегетін мөлшерді елестеткеніміз жеткілікті. Жасөспірім балалар порнографиясы мен лицензиялы өнімдердің контрафактілі көшірімдері қоғамға моральді және материалды шығын келтіреді. Бұл зиян мөлшері миллиондаған не миллиардтаған қаражат мөлшерінде есептеледі. Мұндай жағдайда қылмыскерді жауапқа тарту мүлдем мүмкін емес, себебі заңсыз ұсыныс жасаушы жердің нақты белгісіз бір нүктесінде орналасса, мысалға Бразилияның бір жерінде болсын, ал жәбірленуші Қазақстанда болуы мүмкін. Жаңа технологиялар мен жаһанды Интернет желісі адам баласының қадағалауына және бақылауына бағына бермейтін XXI ғасырдағы қоғамның, жеке тұлғаның маңызды серігі болмастан, басты әрі жасырын бір жауы. Мұндай зиянкестермен күресудің бір амалы болып барлық мемлекеттердің бірдей болып бірігіп, ынтымақтастық білдіре білгені болады. Қазіргі таңда көріп отырғанымыздай, мемлекеттер арасында тек қана жанжал мен саяси қақтығыстар орын тауып отыр, оның бірден бір себебі терроризм мен экстремизм, саяси тұрақсыздық, бүкіләлемдік дағдарыс пен халықаралық аренадағы жер қойнауы үшін күресу, сыбайлас жемқорлық, діни және ұлтаралық араздықтың өрбуі және қарқынды дамуы, ал осының барлығының дамуының ең тиімді құралы – ол, әрине, Интернет желісі.

Компьютерлік қылмыстарды біз жеке қарастырамыз, бұл үлкен қателік, жоғарыда айтқанымыздай кез келген қылмыс, тіпті кез келген іс-әрекет электронды техникаларды, олардың бағдарламаларын пайдалану, оларды байланыстыратын локалды және глобалды желілерді пайдалану арқылы жасалады. Қылмыс саны мен қылмыс түрі тоқтамай өсіп келеді. Ал компьютерлік қылмыстармен күресу үшін шығарылған заң нормалары екінші онжылдықтың соңына таяп қалды ешбір өзгеріссіз сол қалыпта тұр. Осыдан көретініміз, қылмыстардың дамуы мен олармен күрес жүргізу арасындағы арақашықтық қандай қарқынмен өсіп бара жатқаны, екеуі салыстыруға да келмейді.

Қазақстан Республикасының Қылмыстық кодексін қарастыратын болсақ, жиырмасыншы ғасырдың соңында компьютерлік қылмыстарға қатысты қолданысқа енгізілген құқық нормалары сипаты мен мазмұны еш өзгеріссіз және толықтыруларсыз тұр. Бұл нормалардың дұрыстығында күмән жоқ, бірақ заман талабына сай бұл нормаларды жетілдіргеніміз, яғни жаңа нормалармен толықтырғанымыз жөн. Жетілдірмес бұрын заңнамадағы бар нормаларымызды қарастырып, қылмыстық құқық ғылым саласы тұрғысынан, құрылымы, сипаты жағынан толық талқылап көрелік.

Бірінші қарастыратынымыз, қолданыстан шығып қалған Қазақстанның Қылмыстық кодексінің 7-тарауының 227-бабы [69].

Компьютерлік ақпаратқа заңсыз кіру, ЭЕМ үшін зиянды бағдарламаларды жасау, пайдалану және тарату (227-бап).

Компьютерлік ақпаратты қылмыстық-құқықтық нормамен қорғау Қазақстан Республикасының жаңа және соңғы Қылмыстық кодексінде тұңғыш рет көрсетіліп отыр. Бұрынғы Қылмыстық кодексте мұндай арнаулы норма болмаған. Компьютерлік ақпаратқа заңсыз кіру, ЭЕМ үшін зиянды бағдарламаларды жасау, пайдалану және тарату негізінен қоғамның экономикалық саладағы қоғамдық катынастарында орын алған. Осыған орай заң шығарушы, сол кезде көрсетілген норманы Қылмыстық кодекстің 7-тарауына, яғни экономикалық қызмет саласындағы қылмыстар санатына қосқан еді. Ал қазір бұл норма, заңға қайшы немесе жаңа редакцияда айтылғандай, құқыққа сыйымсыз әр әрекет түрінде жеке-жеке 8 бапқа бөліп қарастырылып отыр.

Заңмен қорғалатын компьютерлік ақпаратқа, яғни машиналық сақтағыштағы, электронды есептеу машинасындағы (ЭЕМ),

ЭЕМ жүйесіндегі немесе олардың желісіндегі ақпаратқа заңсыз кіру, егер бұл әрекет ақпаратты жоюға, бөгеуге, жаңартуға не көшіруге, ЭЕМ жұмысын, ЭЕМ жүйесін немесе олардың желісін бұзуға келіп соқса – компьютерлік ақпаратқа зансыз кіру, ЭЕМ үшін зиянды бағдарламаларды жасау, пайдалану және тарату деп танылып, кінәлі тұлға Қылмыстық кодекстің 227-бабымен жауапқа тартылатын еді.

Ақпарат ресурстарының, жүйелерінің, технологияларының меншік иесі болып осы объектілерге толық көлемде иелену, пайдалану және билік ету құқығын жүзеге асыруға құқылы субъектілер танылады. Ақпарат ресурстарының, жүйелерінің, технологияларының иеленушілері болып осы объектілерге иелену, пайдалану және заңда белгіленген шекте билеу құқығын жүзеге асыруға құқылы субъектілер танылады. Компьютерлік ақпаратқа заңсыз кіру тәсілдері сан алуан болуы мүмкін: компьютерлік ақпаратқа кіруге құқық беретін жалған құжат көрсету; техникалық құрылымның кодын немесе мекен-жайын өзгерту, ақпаратты қорғау жүйелерін немесе құралдарын өзгерту, ақпарат көздеріне жазу ақпаратын қосу және т.б. Компьютерлік қылмыстардың, бастапқыда айтып кеткендей, міндетті шарттары болып компьютерлерге заңсыз кіру, оларды істен шығару немесе жұмысын бұзу, ақпаратты жою, ақпаратты жаңарту (біздің ұсынысымыз бойынша орыс мәтініндегі «модификация» сөзін жаңарту дегеннің орнына «өзгерту» немесе сол күйінде «модификациялау» деген дұрыс), бөгеу, көшіру әрекеттері табылатын. Бұл әрекеттердің шегі мен мәні, сипаты мен ұғымы түсінікті. Бірақ осы туралы шектеулі мағынада А.Н. Ағыбаев қысқаша кейбір ұғымдарға түсінік берген.

Мысалы, ол «компьютерлік ақпаратқа заңсыз кіру деп заңмен қорғалатын ақпаратты, оның заңды меншік иесінің немесе оның иеленушісінің рұқсатынсыз өз бетімен алуды немесе көшіруді айтамыз; ақпаратты бөгеу деп ақпарат көздері толық сақталғанымен оны пайдалану және оған еркін кіруге кедергі келтіру тәсілдерін айтамыз; ақпаратты жаңарту деп меншік немесе заңды иеленушінің билігінде болған ақпаратқа олардың келісімінсіз кез келген тұрғыдағы өзгерістерді енгізуді айтамыз; ақпаратты көшіру деп ақпарат көздерінің түпнұсқасын сақтай отырып, ондағы файлдардың немесе диск жүйелерінің, көшірмесін алу арқылы немесе басқадай тәсілдермен көбейтуді немесе оның мазмұнын жариялауды айтамыз» деген [70].

ЭЕМ жұмысын, ЭЕМ жүйесін немесе олардың желісін бұзуға – ЭЕМ-нің жекелеген жүйелерінің жұмыс қабілетінің төмендеуі, компьютер желісінің элементтерінің істен шығуы, компьютер жүйелерінің өз қызметін толық орындамауы жатады.

Қылмыс компьютерлік ақпаратқа заңсыз кіру, егер бұл әрекет ақпаратты жоюға, бөгеуге, жаңартуға немесе көшіруге, ЭЕМ жұмысын, ЭЕМ жүйесін немесе олардың желісін бұзуға әкеліп соққан уақыттан бастап аяқталған деп танылады.

Қылмыстық кодекстің 227-бабының 2-тармағында осы қылмыс құрамының ауырлататын түрі көрсетілген: олар адамдар тобының алдын ала сөз байласуы бойынша жасалған немесе ұйымдасқан топ не өз қызмет бабын пайдалана отырып, сондайақ ЭЕМ-ге, ЭЕМ жүйесіне немесе олардың желісіне кіре алатын адам жасаған әрекеттер. Алдын ала сөз байласып жасалған қылмыс пен ұйымдасқан топ жасаған қылмыстың түсінігі Қылмыстық кодекстің 31-бабының тиісінше 2-ші және 3-ші тармақтарында айтылған.

Өз қызметін пайдалана отырып қылмыс жасаудың түсінігі Қылмыстық кодекстің өзге баптарында және Мемлекеттік қызмет түрлерін реттейтін НҚА-де берілген.

Компьютерлерге, олардың жүйесіне немесе олардың желісіне кіре алатын адамға осы жүйеде заңды түрде жұмыс істейтін, бірақ өзінің атқаратын жұмысы бойынша нақты белгіленген міндеттерінің шегінен шығып, компьютерлік ақпараттағы өзіне жүктелмеген басқа міндетті атқаруға қол сұғып, араласқандар жатады.

ҚР ҚК 7-тарауында көрсетілген қылмыстық құқықбұзушылықтардың субъектісі – 16 жасқа толған, есі дұрыс адам болып табылады [71].

Ал енді қазіргі қолданыстағы Қылмыстық кодекстегі 7-тарауды жеке қарап көрейік. Атауы «Ақпараттандыру және байланыс саласындағы қылмыстық құқықбұзушылықтар», баржоғы жеке қарастырылған 9 бап (205–213 аралығындағы баптар). Бір қарағанда жаңадан 7 өз бетінше дара норма қосылған секілді, алайда мұқият қарасаңыздар, баяғы жартас, сол жартас, ешбір мағыналы өзгеріс жоқ. Жаңалығы аз, бірақ бар. ЭЕМ желілері мен жүйелері, сәйкесінше, ақпараттық жүйелер мен телекоммуникациялық желілер деп өзгертілген, яғни ұғымдар заман талабына сай келетін атаулармен өзгертілген не алмастырылған.

Жұмыста санкция жағы салыстырылып отырған жоқ, себебі ҚР Жаңа қылмыстық заңнамасында (3 шілде 2014 жылғы) қылмыстық жауаптылық мәселесі үлкен реформаға ұшырады.

Атап өтетін болсақ,

205-бап. Ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялық желісіне құқыққа сыйымсыз қол жеткізу;

206-бап. Ақпаратты құқыққа сыйымсыз жою немесе түрлендіру;

207-бап. Ақпараттық жүйенің немесе телекоммуникациялар желісінің жұмысын бұзу;

208-бап. Ақпаратты құқыққа сыйымсыз иеленіп алу;

209-бап. Ақпаратты беруге мәжбүрлеу;

210-бап. Зиян келтіретін компьютерлік бағдарламалар мен бағдарламалық өнімдер жасау, пайдалану немесе тарату;

211-бап. Қолжетімділігі шектелген электрондық ресурстарды құқыққа сыйымсыз тарату (мәні мен сипаты жағынан жаңа норма ретінде қабылдауға болады);

212-бап. Құқыққа қайшы мақсаттарды көздейтін Интернет-ресурстарды орналастыру үшін қызметтер ұсыну;

213-бап. Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын, абонентті сәйкестендіру құрылғысын құқыққа сыйымсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгертуге арналған бағдарламаларды жасау, пайдалану, тарату.

Енді компьютерлік қылмыстардың қылмыстық-құқықтық сипаттамасын ғылыми тұрғыдан кең мағынада жан-жақты аспектілерді көтере отырып тоқталып өтелік. Қылмыстардың белгілеріне және элементтеріне жеке-жеке тоқтайтын болсақ бірінші кезекте компьютерлік қылмыстардың объективті белгілерін қарастырайық.

Компьютерлік қылмыстардың қоғамға қауіптілігі сипаты мен дәрежесін белгілеу кезінде олардың әлеуметтік табиғатын анықтау үшін маңызды теоретикалық сипатқа осы қылмыстардың объектілерін белгілеп алған дұрыс. Қылмыстық іс-әрекеттің қоғамға қауіптілігі қоғамдық игіліктің құндылығы мен маңыздылығына және сол игілікке қылмыстан келтірілетін зардаптың мөлшеріне байланысты. Қарастырылып отырған қылмыстардың объектісін жан-жақты зерттеу осы қолсұғушылықтардың құқықтық және

әлеуметтік мәнін анықтауға, қылмыстық-құқықтық норманың әсер ету шегін анықтауға, қоғамға қауіпті нәтижелерді белгілеуге мүмкіндік береді. Оның пайдасы осы қылмыстарды басқа қылмыстардан айыруға және дұрыс саралау қызметін жүзеге асыруға мүмкіндік береді.

Қылмыстық құқық ғылым саласының теориясы әдетте қылмыстың объектісі ретінде заңмен қорғалатын, қылмыстық іс-әрекет кезінде зардап шегетін қоғамдық қатынастарды немесе қатынастар жиынтығын таниды. Әдебиеттерде осы нұсқа жалпыға ортақ немесе жалпылықпен танылған болып саналады.

Біздің ойымызша, әдістемелік жағынан дұрыстықты танытатын талпыныс қылмыстың объектісін жүйелік позиция тұрғысынан қарастыру. Ол бойынша қылмыстың объектісі белгілі типтегі жүйе ретінде қабылданады, содан кейін, осы жүйенің элементтері арасында қарым-қатынас орнатылады.

Енді осы қоғамдық қатынастардың қайсысымен объектіге зардап келтірілетінін анықтап алу үшін қылмыстық құқық теориясында ең басты жалпы объектіні, кейін топтық объектіні және тікелей объектіні белгілеп алу қажет. Жүйелік тұрғыдан қарағанда, бұл жүйелер әртүрлі дәрежелі жүйелер, оларда әртүрлі мақсаттағы функциялар бар және олар бір-бірімен тығыз байланысты, сол себепті олар ортақ мәндік сипатқа ие және бірбіріне тәуелді.

Барлық қылмыстық іс-әрекеттердің, соның ішінде компьютерлік қылмыстардың да, жалпы объектісі қылмыстық заңның жалпы бөліміне сәйкес қылмыстық қолсұғушылықтан қылмыстық заңнама негізінде қорғалатын қоғамдық қатынастардың жиынтығы болып табылады.

Топтық объект, біз білетіндей, ол жалпы объектінің бір бөлігі және ол біртектес қылмыстық әрекеттер арқылы біртоптық қоғамдық қатынастарға қол сұғуды білдіреді. Қылмыстық заңнаманың Ерекше бөлімін тарауларға бөлу осы біртектес қоғамдық қатынастардың топтастырылуы негізінде жүзеге асып отыр.

Компьютерлік (ақпараттық) қылмыстар ҚР Қылмыстық кодексінің «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» атты 7-тарауында (ҚР ҚК 205-, 213-баптары) белгіленген.

Компьютерлік қылмыстардың топтық объектісі болып нарықтық экономиканы дамытуға, сандық немесе цифровизациялау саясатын жүзеге асыруға бағытталған, қоғамның ақпараттандыру саласындағы туындайтын мемлекетпен қорғалатын қоғамдық қатынастар жүйесі табылады.

Компьютерлік қылмыстардың тікелей объектісіне тар мағынада компьютерлік ақпаратты қорғау, ақпараттық қауіпсіздік саласындағы қоғамдық қатынастар жатады.

Кең мағынада компьютерлік қылмыстардың тікелей объектісі – ол компьютерлер мен компьютерлерде сақталатын ақпараттардың қауіпсіздігі, ақпараттық сақтағыштардағы ақпараттың қорғаныстық жағдайы, компьютер жүйесі мен желілерінің қауіпсіздігі, олардың техникалық пайдалану ережелерінің бұзылуы, жағымсыз зиянды бағдарламалардан қорғану жағдайы.

Сонымен қатар, ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодының қауіпсіздігі, абоненттің сәйкестендіру құрылғысын құқыққа сыйымсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгерту үшін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату әрекеттерінің жағдайы.

Қосымша объектінің түрлері көп, мысалы, бала асырап алу құпиясына құқықтары, жеке құпиялар және т.с.с.

Келесі қарастырылып өтетін, қылмыстардың объектілерімен қатар қарастырылатын компьютерлік қылмыстардың құрылымдық элементі болып саналатын мәселе – қылмыстың пәні немесе заты. ҚР Қылмыстық кодексінің 205-бабы 1-тармағында және өзге нормаларында көрсетілген компьютерлік қылмыстардың заты ретінде машиналық сақтағыштарда, ақпараттық немесе телекоммуникациялық жүйелерде немесе желісінде сақталатын компьютерлік ақпарат есептеледі.

Қылмыстың заты ретінде қарастырылып отырған компьютерлік ақпараттың өзіндік ерекшеліктері бар:

1) компьютерлік ақпарат өте үлкен көлемді және тез өңделетін болады;

2) мұндай ақпараттар өте жеңіл болады және оларды тез жойып жіберуге болады. Мысалы, 500 беттен тұратын үлкен мәтінді жойып жіберу үшін не бары тышқанның оң жақ мәзірінің тиісті сөзін басқаны жеткілікті не одан да тез операция пернетақтаның батырмасының комбинациясын басу арқылы кез келген көлемде-

гі ақпаратты жоюға болады, ал баяғы заманда 500 беттен тұратын құжатты жою үшін оны өртеу керек болатын және оған қаншама уақыт керек екенін елестетіп көріңіз;

3) компьютерлік ақпарат нақты түрсіз және түссіз болады және өзіне тән ерекше белгілері болмайды, сол себепті ақпарат пен ақпараттың иесі арасында тиесілі байланыс бар немесе жоқ екенін айтуға мүмкін емес;

4) осы түрдегі ақпарат тек машиналық сақтағыштарда немесе тасығыштарда (дискеталарда, магниттік ленталарда, лазерлік дисктарда, флешкаларда, жартылай өткізгіштік схемаларда, цифрлік ойнағыштарда, электронды құрылғыларда, сыртқы қатты дисктерде), ЭЕМ-нің өзінде (операциялық жадыда – ОЗУ) орналасуы мүмкін;

5) қарастырылып отырған ақпараттың түрі тек аталған электронды есептеу техникалары мен перифериялық құрылғылары көмегімен (диск енгізуші, лазерлі дисктерді оқитын құрылғы, CD-ROM, DVD-RAM, USB порт, электр сымдары, диск шешуші, тышқан, пернетақта, цифрлі пернетақта, стриммер, экранды пернетақта және т.б.) ғана жасалуы, өзгертілуі, көшірілуі, пайдалануы, қайта жасалуы және қолданылуы мүмкін;

6) бұл ақпараттар компьютер желілерінің барлық байланыс түрлерімен және барлық коммуникациялық арналарымен алмасуы мүмкін және сол арқылы кез келген үлкен көлемді ақпаратты жердің кез келген нүктесіне жылдам уақытта жіберуге болады.

Компьютерлік ақпаратты бірнеше ерекше белгілері бойынша, сипаттары бойынша топтарға бөліп қарастыруға болады.

Компьютерлік ақпарат оларды тасымалдаушы құрылғыларына байланысты: магниттік лентада сақталған ақпарат, дискеталарда, лазерлік дисктерде, қатты дисктерде, компьютердің қатты дискінде, ақпараттық жүйенің жадысында, желісінде немесе жүйесінде сақталған ақпараттар деп бөлінеді.

Ақпараттың түріне байланысты: мәтіндік, сандық, графиктік, символдық, суреттік, бейнелік (видео) және дыбыстық (аудио) болып бөлінеді.

Ақпараттың орналасқан жеріне байланысты: уақытша орналасқан жерін көрсететін, үнемі сақталған жерін көрсететін, желідегі орнын көрсететін және қасиеттерімен бірге орналасқан жерін сипаттайтын деп бөлінеді.

Компьютерлік ақпараттың файлдық атауы бойынша: түрлі таралымдағы (расширениядағы) мәлімет, атаудың символдық белгілік сипаттамасы бойынша ақпарат деуге болады.

Ақпараттың көлемі бойынша: парақтар саны көрсетілген, жолдар саны көрсетілген, символдар көлемі көрсетілген ақпарат деп бөлуге болады.

Уақыты бойынша: жасалған уақытты көрсететін және өзгерген уақытты көрсететін деп бөлінеді.

Ақпараттың атрибуттары бойынша: архивтік, жасырын, жүйелік, жалпыға, тек оқу үшін, ярлыктік және т.б. деп бөлінеді.

Осы жоғарыда аталған ұғымдар негізінде компьютерлік қылмыстардың заты ретінде ақпаратты тасымалдағыштар, компьютерлер, ақпараттандыру және телекоммуникация желілері және жүйелері және электронды ақпаратты өзінде сақтайтын осылар сияқты басқа құрылғыларды қабылдау керек, өйткені компьютерлік ақпарат аталған құрылғылармен өте тығыз байланысты және оларсыз ақпараттың болуы мүлдем мүмкін емес.

Ақпараттық (машиналық) тасымалдағыштарға жатқызуға болады:

– құрылғылардың ішіндегі қатты магниттік немесе магниттік-оптикалық дисктерде жинақтаушы;

– сыртқы қатты магниттік диск;

– ақпаратты жинақтайтын сыртқы құрылғы;

– магниттік немесе арнайы металлдық лентада жинақтаушы ішкі құрылғы;

– жұмсақ магниттік диск;

– оптикалық немесе магнитті оптикалық диск;

– қағаз, пластик немесе металл карталары;

– жадының интегралды микросхемалары немесе микрочиптері;

– флэшкарталар, чиптер, электронды мобильді құрылғылар;

– түрлі нысандағы және көлемдегі сақтау карталары және т.б.

Бағанадан ЭЕМ, яғни электронды есептеу машинасы деп айтып келеміз, біреуге ол түсінікті, біреуге түсініксіз болуы мүмкін, ал басқаларға бұл баяғыда ұмтылған, қолданыстан алынап тасталған архаизмдік сөз, термин болуы мүмкін, ал жаңа ұрпаққа мүлдем жаңа сөз сияқты көрінуі мүмкін, себебі бұл сөз айналымда жүргенде олар дүниеде болмаған болуы мүмкін. Сол себепті Элект-

ронды есептеу машинасы деген ұғымды ашып талқылап көрейік, содан кейін осы анықтамаға басқа заманға сай атау берейік.

Электронды есептеу машинасы (ЭЕМ) бұл – операциялық рет бойынша берілген бағдарламаның орындауы арқылы ақпаратты керекті қалыпқа, нысанға, керекті есептеулерге келтіретін құрылғы. ЭЕМ-нің ата-тегін біз есеп-шоттардан және математикалық калькуляторлардан көреміз.

ЭЕМ қатарына қазіргі таңда келесі аппараттар мен құрылғыларды жатқызуға болады:

– персоналды компьютерлер (үстел үстіне орнатылады, көп функциялы, көптеген перифериялық қосымша құрылғылары бар, сәйкесінше мүмкіндіктері мол, кеңселік жұмыстар үшін өте ыңғайлы);

– ноутбуктер немесе алғашқы атауы laptop (диск енгізетін құрылғысымен, мүмкіндіктері көп), нетбуктер немесе subnotebook (диск енгізетін, оқитын құрылғысы жоқ, тек USB қондырғысы бар, жеңіл және арзанырақ тұрады);

– қалталы персоналды компьютерлер (функциялары шектелген);

– планшеттер (жалғыз экранды, бір бөлімнен тұратын портативті компьютерлер, CD немесе DVD құрылғылары жоқ, сенсорлы не тачскриндік экранмен, ойындармен және қызығушылық бағдарламаларымен қолдану ыңғайлы);

– қалталы электронды кітапшалар (тек жұмыс жасау мақсатында ыңғайлы);

– электронды аудармашылар (шектеулі тілдерді аударады, тілмаш, алфавитті және тілді үйренуге болады, дыбыстық қосымшасы бар);

– коммуникаторлар (ағылш. communicator) (қалталы персоналды компьютер, мобильдік телефон қызметі бар және мобильдік телефондарда бар барлық қосымша мүмкіндіктерімен бірге) [72];

– смартфондар (керісінше мобильді телефон, қосымша компьютерлік бағдарламалық мүмкіндіктері жеткілікті, салыстырмалы бағасы қымбат).

Сонымен қатар ЭЕМ қатарына бағдарламалық ортақ жүйелерді жатқызуға болады (интегрированные системы). Мысалы өрт қауіпсіздігін қадағалайтын бағдарламалық жүйелі құрылғылар, су немесе газ құбырындағы қысымды көрсететін және

қауіпсіздікті қамтамасыз ететін электронды аппараттар, электронды есіктер, банкоматтар, атракциондар, электронды кассалық аппараттар және т.б.

ЭЕМ жүйесі – компьютерлердің біреуі жүйенің элементі болып саналатын немесе бірнеше ЭЕМ жүйесінен тұратын компьютерлік кешен немесе компьютерлік сервер.

ЭЕМ желісі – бір-бірімен электрбайланыс сымдарымен немесе сымсыз портпен біріктірілген компьютерлер жиынтығы. Жүйелі бағдарламалық жұмыс кезінде орнатушының немесе пайдаланушының еркімен кез келгенін, әсіресе жоғары сапалы немесе жоғары операциялық жылдамдықта жұмыс жасайтынын сервер ретінде пайдалануға болады [73].

ЭЕМ сөзінің мағынасы ашылған секілді, бірақ XX ғасырдың 90-жылдары ЭЕМ орнына қарапайым «компьютер» сөзі келеді. Ендеше компьютер дегеніміз бұл – операциялық рет бойынша берілген бағдарламаның орындауы арқылы ақпаратты керекті қалыпқа, нысанға, керекті есептеулерге келтіретін құрылғы, сонымен қатар мультимедиялық ойнауларды жүзеге асыратын универсалды аппарат, адамдар арасында қарым-қатынасты байланыстыратын, ақпаратпен алмасуды жүзеге асыратын кешендік құрылғы, ғылыми зерттеулер жүргізу бағдарламаларын пайдалану құралы, күнделікті өмірде адамдардың жұмысын қамтамасыз ететін, қолдану шегі кең адамзат ғылыми еңбегінің нәтижесі.

«Компьютер» сөзі ағылшын тілінің «computer», яғни есептеу, есептеуші немесе есептеуіш сөздерінен шығады. Өз кезегінде ағылшындар ол сөзді латын тілінен алған «computo» есептеймін дегенді білдіреді [74].

Сол себепті ҚР Қылмыстық кодексінің келесі редакциясында 227-баптың мазмұнында ЭЕМ терминін «компьютер» сөзіне ауыстырған жөн болады.

Қылмыстың затына қайта оралатын болсақ, ҚР Қылмыстық кодексінің 7-тарауында компьютерлік қылмыстардың затына заңмен қорғалатын ақпараттан тұратын машиналық сақтағыштар, электронды есептеу машиналары, яғни компьютерлер, ақылды құрылғылар, СМАРТ технологиялар, компьютер жүйелері мен желілері жатады.

Заңмен қорғалатын компьютерлік ақпаратқа жатады:

1) Мемлекеттік құпиялар – мемлекеттік және қызметтік құпияны құрайтын, эффектілі әскери, экономикалық, ғылыми-тех-

никалық, сыртқы экономикалық, сыртқы және ішкі саясаттық, барлаулық, контрбарлаулық, жедел іздестірушілік және басқа да қызмет түрлерін жүзеге асыру мақсатында таралуы мемлекетпен шектелетін және мемлекетпен қорғалатын мәліметтер тізімі [75];

2) Қызметтік және сауда-саттықтық (коммерциялық) құпия – үшінші тұлғаларға белгісіз шынайы немесе потенциалды саудалық құндылыққа иелі ақпарат, ол ақпаратқа заң негізінде қол сұғуға рұқсат жоқ және оның иесі конфиденциалдылықты сақтау үшін тиісті шараларды қолданады [76, 128 б.];

3) Банктік құпия – банк клиенттері және банктің бөлімшелері мен филиалдарының кез келген қызмет түрін пайдаланатын барлық адамдардың жеке мәліметтері мен ақпараттары, олардың шоттары мен шоттарындағы қаражат туралы, депозиттер және олардың нөмірлері туралы, ақша қозғалысы мен ақша қалдығы туралы, банктің өзінің шоттары мен операциялары туралы, клиенттердің мүлкі туралы, қарыздары туралы, несиелері мен микронесиелері туралы, кодтары мен парольдері туралы, банк сейфтерінің құрамы туралы, кеңсе жиһазының құрамы туралы, құжаттардың мазмұны туралы мәліметтер [77];

4) Салықтық құпия – салық төлеушілер туралы салық органдарымен алынған кез келген мәлімет, төмендегілерден басқа:

– салық төлеушінің тіркеу нөмірі;

– салық төлеушінің жеке нөмірі (кейіннен енгізілген);

– салық жылы бойынша салық төлеушінің бюджетке төлеген салық және басқа төлемдер сомасы (жеке тұлғалардан басқасы);

– салықтық қылмыстар және басқа да қылмыстар жасаған тұлғаларды заң бойынша тергеу мақсатында құқық қорғау органдарына берілетін мәліметтер;

– соттың талап етуі бойынша салықтық дауларды қарастыру істері бойынша қажетті мәліметтер;

– Қазақстан Республикасының ратификацияланған халықаралық шарттары бойынша шет елдердің құқық қорғау органдарына және халықаралық ұйымдарға келісім-шарт бойынша берілетін тиісті мәліметтер [78];

5) Жеке және отбасы құпиясы;

6) Хат жазысу, телефондық сөйлесу құпиясы, пошталық, телеграфтық және басқа да хабарламалардың құпиялылығы;

7) Дәрігерлік (медициналық) құпия – пациенттің науқастығы туралы немесе медициналық куәландыру нәтижелері туралы мәліметтер; ҚР азаматының психиатриялық ауытқулары туралы мәліметтер немесе психиатриялық көмекке жүгіну туралы, емделу жөнінде фактілер туралы және адамның психикалық жағдайы туралы басқа да мәліметтер [79];

8) Адамның иммун тапшылығы вирусын жұқтырған тұлғалар туралы және соз, ВИЧ / ЖҚТБ (СПИД) ауруымен ауратындар туралы мәліметтер [80];

9) Ұл баланы немесе қыз баланы асырап алу туралы құпиясы;

10) Адвокаттық құпия – адвокатқа жүгіну фактісі, көмек сұрап өтініш жасаған адаммен және басқа да адамдармен жасалған ауызша және жазбаша келіссөздердің мазмұны туралы, көмек сұрап өтініш жасаған адамның мүдделерінде жасалатын әрекеттердің сипаты мен нәтижелері туралы мәліметтер, сондай-ақ заң көмегін көрсетуге қатысты өзге де ақпарат. Адвокаттардың, адвокаттар алқасы төралқасы, заң консультациясы, адвокат кеңсесі қызметкерлерінің заң көмегін көрсетуге байланысты алынған мәліметтерді жария етуге, сондай-ақ өз мүдделері немесе үшінші бір адамдардың мүдделері үшін пайдалануға құқығы жоқ. Адвокат құпиясына жататын мәліметтерді көмек сұрап өтініш жасаған адамның келісімінсіз жария еткен адвокат заңға сәйкес жауапты болады (18-бап) [81];

11) Нотариалдық іс-әрекеттердің құпиясы (Мысалы: мұрагерлік өсиетнаманың мазмұнын жарияламау);

12) Судья мәжілісінің құпиялығы;

13) Зейнетақылық жинақтардың құпиялығы – салымшылар туралы мәліметтер, алымшылар туралы мәліметтер, шоттар туралы, ағымдағы шоттардың қозғалысы туралы, қаржылық операциялар туралы мәліметтер;

14) Жекелік қасиеттерге ие ашылмаған мәліметтер – техникалық, ұйымдастырушылық, өндірістік, коммерциялық ақпараттар, үшінші тұлғаларға белгісіз жаңалық ашу жөніндегі ақпараттар, ғылыми зерттеу кезінде туындаған жаңалықтар (толығымен патенттелмеген, авторлық құқық жарияланбаған, лицензия алынбаған өнімдер), сонымен қатар өндіріс құпиялары (ноу-хау);

15) Алдын ала тергеу мен анықтау іс-әрекеттерінің мәліметтері;

16) Қылмыстық іс жүргізуде қорғаныста қажет ететін тұлғалар туралы конфиденциалды мәліметтер;

17) Конфиденциалды мәліметтер – мемлекеттік құпиялар қатарына жатпайтын, мәліметті білетін тараптар жағынан заң негізінде қорғалатын, келісім бойынша тұлғалардың еркімен жасырындық қасиетке ие болатын мәліметтер;

18) Конфиденциалды кедендік ақпарат – кедендік іс саласындағы сыртқы экономика және басқа да қызмет түрлерінің қатысушыларына қатысты ақпарат.

ҚР Қылмыстық кодексінің 210-бабы бойынша қылмыс құрамының затына компьютерлерге қарсы зиянды бағдарламалардан тұратын тасымалдағыштар немесе сақтағыштар жатады.

Сол сияқты ҚР Қылмыстық кодексінің 213-бабы бойынша қылмыстың заты болып ұялы байланыстың абоненттік құрылғысының сәйкестендіру (идентификациялық) коды және ұялы байланыс абонентінің сәйкестендіру (идентификациялық) картасы (SIM-карта) танылады.

Ұялы байланыстың абоненттік құрылғысының сәйкестендіру (идентификациялық) кодын басқаша IMEI-код деп те атайды. IMEI – (ағылш. International Mobile Equipment Identity) мобильді құрылғыларды анықтайтын халықаралық стандарт, GSM стандартындағы ұялы телефондар үшін уникалды 15 дәрежелі код. GSM алғашқы атауы Groupe Special Mobile болған, кейін халықаралық стандарттардың өзгеруіне байланысты GSMC (Global System for Mobile Communications) мобильді коммуникациялар үшін глобальді жүйе деп өзгертілді. Ұялы телефонның моделі және шығу ерекшелігі IMEI-кодтың алғашқы 8 санымен (TAC/Type Allocation Code) анықталады да, қалған сандар телефонның сериялық нөмірін және бақылау санын білдіреді [82].

Ұялы байланыс абонентінің идентификациялық картасын адамдар арасында және қолданыста SIM-карта деп атайды. SIM (ағылш. Subscriber Identification Module) абонентті идентификациялау модулі – мобильді байланыс түрлерінде қолданылатын абонентті сәйкестендіру және анықтау модулін жүзеге асыратын құрал. Кейіпі физикалық пластикалық шағын карта. Картаның негізгі функциясы аккаунт туралы идентификациялық ақпаратты сақтау. Сонымен қатар сол арқылы абонент аккаунтты өзгертпей, картасында сақтаулы тұрған басқа абоненттердің нөмірлерін көшірмей, қайта жазбай, есте сақтамай тек қана өзі-

нің SIM-картасын ұялы телефоннан басқа телефонға лезде ауыстыру арқылы абоненттік операцияларды жүзеге асыра алады. SIM-карта шифрлеуді қамтамасыз ететін жады микросхемасынан тұрады. Карталар түрлі стандартты және түрлі жады көлемімен болады. Бірақ карталардың нысаны бір стандарт бойынша жасалады.

ҚР Қылмыстық кодексінің 213-бабы бойынша қылмыс құрамының заты ұялы байланыстың абоненттік құрылғысының сәйкестендіру (идентификациялық) кодын өзгертетін не жоятын және ұялы байланыс абонентінің сәйкестендіру (идентификациялық) картасын (SIM-картасын) жасайтын бағдарламалардан тұратын машиналық тасымалдағыштар және сақтағыштар болады.

Компьютерлік қылмыстардың объективтік жағы. Кез келген қылмыстың жалпы белгілері және тек өзіне тән ерекше белгілері болады. Сол белгілердің бір бөлігі қылмыстың объективті жағының элементтерінен тұрады. Қылмыстың объективті жағы дегеніміз – қылмыстық заңмен қорғалатын объектілерге қол сұғатын, қоғамға қауіпті іс-әрекеттің сыртқы көрінісі.

Іс-әрекеттің объективтік жағынсыз қылмыстық объектінің өзіне қол сұғу мүмкін емес және қылмыс құрамын айқындайтын элементтердің басқалары да болуы мүмкін емес, яғни қылмыстық іс-әрекетсіз (әрекет немесе әрекетсіздік) қылмыстың субъектісі де, сол субъектінің қылмыстың объектісі мен объективтік іс-әрекетке деген қатынасынан туындайтын субъективтік жағы да бола алмайды. Яғни қылмыстың элементтері немесе белгілері қылмыс құрамының нысанына қарай бір-бірінсіз көрініс табуы мүмкін емес.

Заң шығарушы Қылмыстық кодекстің баптарында қылмыстың объективтік жағын қалай құрған, соған байланысты құқықтық теорияда да қылмыс құрамдарын бөлу керек. Заңнама бойынша қылмыс құрамдары негізінен материалдық немесе ресми (формальдық) болып бөлінеді. Егер қылмыстың объективтік жағы өз құрамына қылмыстық іс-әрекетпен (әрекет немесе әрекетсіздік) қатар, сол іс-әрекеттен туындайтын нәтижелерді кіргізетін болса, мұндай қылмыстар материалдық қылмыс құрамдары болып саналады. Егер қылмыстың құрамына міндетті белгі ретінде тек қылмыстық іс-әрекеттің бар болуы жеткілікті болса, мұндай қылмыс құрамдары формальды құрам болып табылады.

Қылмыстың объективтік жағы қылмыстық-құқықтық норманың диспозициясында сипатталады.

Қылмыстың объективтік жағы ақпаратты санкциясыз жоюға, бөгеуге, жаңартуға не көшіруге, компьютерлік құрылғылардың жұмысын, жүйесін немесе олардың желісін бұзуға көпе-көрінеу әкелетін телекоммуникациялық немесе ақпараттық құралдарға арналған бағдарламалар жасау немесе қолда бар бағдарламаларға өзгерістер енгізу, осындай бағдарламаларды пайдалану, осындай бағдарламалары бар машиналық сақтағыштарды пайдалану не тарату арқылы көрінеді.

Объективтік жағынан қылмыс мынадай әрекеттермен сипатталады: заңмен қорғалатын компьютерлік ақпаратқа заңсыз кіру немесе компьютерлік құралдарға зиянды бағдарламаларды жасау, пайдалану және тарату арқылы заңды немесе жеке тұлғалардың, қоғамның, мемлекеттің заңмен қорғалатын мүдделеріне мүліктік немесе басқа да зиян келтіру.

Қылмыстың объективтік жағының міндетті белгісі – Қылмыстық кодекстің 7-тарауында көрсетілген зардаптың орын алуы болып табылады. Ақпаратты жою – ақпарат көздерін құрту, файлды, дискілер мен флешкаларды, ондағы мәліметтерді немесе басқадай машиналық жазу деректерін мүлдем жою, сөйтіп ақпаратты қайта қалпына келтіру мүмкіндігін толық істен шығару болып табылады.

Компьютер үшін зиянды бағдарламалар жасау және тарату деп ақпаратты санкциясыз жоюға, бөгеуге, жаңартуға не көшіруге, компьютер жүйесін, жұмысын, олардың желісін бұзуға көпе-керінеу әкелетін компьютерге арналған бағдарламалар жасау немесе қолда бар бағдарламаларға өзгерістер, яғни зиянды вирустар енгізу әрекеттерін айтамыз.

Зиянды бағдарламаларды көбейту, тарату немесе (яғни оның көшірмесін белгісіз адамдарға беру), сондай-ақ оны айналымға енгізетін басқа да әрекеттерді істеу осындай бағдарламаны пайдалану деп танылады.

Компьютер жұмысына, жүйесіне немесе олардың желісіне зиянды бағдарламаларды енгізу, сондай-ақ оларды сату, сыйға беру немесе басқаларға тегін үлестіру осындай бағдарламаларды немесе осындай бағдарламалары бар машиналық сақтағыштарды тарату деп танылады. Бұл қылмыстық құқық теориясы бойынша

жалпы белгілер, ал егер ҚР Қылмыстық кодексінің компьютерлік қылмыстарға бөлген нақты нормаларын қарастыратын болсақ, ол төмендегідей болады.

Компьютерлік ақпаратқа заңсыз кіру дегеніміз компьютерге, оның жүйесіне және желісіне, ақпаратты сақтайтын немесе тасымалдайтын құрылғыға компьютерлік ақпараттың иесінің немесе заңды пайдаланушысының рұқсатынсыз немесе рұқсатын теріс пайдалану арқылы қол сұғу.

Заңмен қорғалатын компьютерлік ақпаратқа заңсыз кіру әдістері жоғарыда айтылғандай алуан түрлі болады:

1) компьютерлік ақпаратқа жасырын тыңдау құрылғыларын қолдану арқылы кіру;

2) компьютерлік ақпаратқа компьютердің өзіне тікелей кіру арқылы;

3) желі арқылы қосылу және кіру тәсілі арқылы;

4) желілік немесе электрлік сымсыз жалғану арқылы;

5) қашықтықтық фотобейнелеу тәсілімен;

6) электронды сәулелерді бұрып алу арқылы;

7) мистификация (жүйені сұрау ретінде көріну амалын қолдану) әдісі арқылы;

8) акустикалық сәулелерді бұрып алу және принтер мәтінін қайта қалпына келтіру амалымен;

9) ақпараттық тасымалдауыштарды және өндірістік шығыстарды (қоқыстарды жинау арқылы) ұрлау жолымен;

10) бөтен пайдаланушылардың массивтерінен мәліметтерді санап алу арқылы;

11) қорғаныс шараларын өтіп ақпараттық тасымалдауыштарды көшіріп алу жолымен;

12) тіркеліп қойған немесе тіркеуден өткен пайдаланушы ретінде кіру;

13) программалық қақпандарды қолдану жолымен;

14) аппаратура мен байланыс желілеріне заңсыз қосылу арқылы;

15) қорғаныс механизмдерін жұмыс қалпынан шығарып тастау сияқты басқа да тәсілдермен ақпаратқа заңсыз кіру.

Тәжірибеде осы тәсілдердің өзіндік ерекшеліктері бар және осылардың ішінде ең жиі кездесетін әдістерге әлеуметтік атаулар тіркелген. Мысалы, «компьютерлік абордаж» бөтен ақпараттық желілерге заңды пайдаланушылардың сәйкестендіру белгіле-

рін (көбінесе пайдаланушылардың аттарын, логиндерін және парольдерін) алмастыру арқылы заңсыз кіру. Аталған компьютерлік қылмыс жасау тәсілі қылмыскермен жәбірленуші компьютерінің абоненттік нөмірін кездейсоқ таңдау арқылы немесе алдын ала алынған абоненттік мекен-жай арқылы жүзеге асырылады. Мысалы, жай ғана телефондық аппаратты пайдалану арқылы шабуыл жасау, әрине, виртуалды шабуыл.

Кейде қылмыскерлер мұндай жағдайда арнайы жасалған парольдерді автоматты түрде теретін бағдарламаларды пайдаланады (көбінесе шетелдік зауыттық немесе қолданбалы қолдан жасалған парольдерді іздейтін бағдарламалар). Бұл бағдарламаның жұмыс алгоритмі қазіргі заман компьютерлерінің жұмыс істеу жылдамдығында, бағдарлама пернетақтада бар барлық мүмкін болатын, әрине ең жиі кездесетіндерінен бірінші бастап, сандар мен әріптердің комбинацияларын және варианттарын қосымша символдармен алмастыра отырып сәйкестендіріп көреді. Оның іздеу жылдамдығы адам санасынан бірнеше есеге тез болады және егер ұқсас пароль кездескен жағдайда ол бағдарлама автоматты түрде абоненттік байланысты жүзеге асырады.

«Баяу таңдау» ағылш. browsing, яғни қарастыру деген сөзінен шыққан компьютерлік ақпаратқа заңсыз шабуыл жасау тәсілі. Қылмыскер компьютерлік жүйеге заңсыз шабуыл жасауды оның қорғаныс жүйесіндегі әлсіз жерлерді анықтау арқылы жүзеге асырады. Қосулы тұрған компьютерге қылмыскер кедергісіз кіреді. Кез келген компьютерді қолданушы жұмыс барысында уақытты үнемдеу үшін компьютерді қосып кетеді, яғни компьютерлік құрал таңертең жұмыстың басында қосылады да, кешкі жұмыс уақыты аяқталғанша қосулы тұрады, шамамен стандартты кеңсе компьютері күніне орта есеппен 7-8 сағат қосылып тұрады. Біз білетіндей, компьютерді толығымен қосу және толығымен сөндіру үшін біраз уақыт кетеді. Сол себепті көптеген жұмысшылар жұмыс уақытын үнемдеу үшін компьютерлерді әрдайым қосып немесе өшіріп жүрмейді. Осы уақыт ішінде қылмыскер қолайлы уақытты пайдаланып өзінің әрекеттерін жүзеге асырады. Бір заңсыз кіру әрекеті арқылы қылмыскер компьютерлік жүйедегі ақпаратты көшіріп алуы, оқып алуы, басқа қайнар көздеріне таратып жіберуі және керек жағдайда осы жерге қайтып келуі мүмкін. Көп жағдайда жәбірленушілер оларға қатысты қылмыс жасалғанын білмеуі де мүмкін.

Бұл тәсілдің баяу таңдау деп аталуы бұл процесс ұзақ уақытты және ұқыптылықты қажет етеді. Мұндай шабуылды болдырмаудың ең қолжетімді және тиімді шарасы компьютердің қорғаныс жүйесін үнемі жаңартып отыру, компьютердегі ұсақ өзгерістерге үлкен көңіл бөлу және қосулы тұрған компьютерлік құралды қараусыз қалдырмау немесе желіден ажыратып қою.

Апаттық әдіс. Бұл компьютерлік қылмыс жасаудың тәсілі сол компьютерде болатын бағдарламаларды заңсыз кіру үшін пайдалану арқылы жасаумен ерекшеленеді. Әдетте бұл компьютердің дұрыс жұмыс жасауына жауап беретін бағдарламалар болады.

Мұндай бағдарламалар компьютерлерде болатын ауытқулар мен басқа да теріс әсерлерді жою үшін қолданылады. Сондықтан компьютерлердің жұмысы үшін олардың қажеттілігі мол, ал қысмыскерлер осыны пайдаланып компьютерлік жүйеге бағдарламалармен бірге кіріп кетуі мүмкін [83, 58-59 бб.].

Айта кететін жәйт, бұл аталған компьютерлік жүйелерге және желілерге тәжірибе жағынан заңсыз кіру әдістері қылмыстың объективтік жағының белгісі ретінде қылмысты саралауға әсерін тигізбейді.

Бірнеше рет атап өткендей, компьютерлік ақпаратқа заңсыз кіру қылмыс құрамдарының қоғамға қауіпті салдары ҚР Қылмыстық кодексінің 7-тарауында көрсетілген. Олар: ақпаратты жою, көшіру, бөгеу, өзгерту және компьютер жұмысын бұзу, ақпараттық және телекоммуникациялық жүйені немесе желісін бұзу.

Ақпаратты жою дегеніміз – компьютерлік ақпаратты оның қалыпқа келуінсіз физикалық түрде ликвидациялау немесе ақпаратты сақтағыш заттан оны түбегейлі жойып жіберу.

Жаңарту (өзгерту немесе модификациялау) – компьютерде, оның жүйесінде және желілерінде ақпараттың мазмұнын кез келген қалыпта өзгерту және сонымен қатар ақпараттың бағыттық маршрутын немесе жүру жолын өзгеріске ұшырату.

Ақпаратты көшіру – компьютерлік ақпаратты басқа сақтағышқа немесе тасымалдағышқа ауыстыру арқылы репродукциялау.

Ақпаратты бөгеу дегеніміз – компьютерлерді пайдаланушылар үшін ақпаратпен қатынау мүмкіндігін жасанды түрде қиындатып қою немесе сол әрекеттер үшін тоскауыл жасау.

Ақпаратты бөгеудің белгілері ретінде ақпараттың тұтастылығы (оның алғашқы сақталған қалпы), компьютерлік ақпаратты пайдаланудың уақытша немесе ұдайы мүмкін еместігі жатады.

Компьютерлік құрылғылардың жұмысының бұзылуы дегенді ЭЕМ-нің жұмысындағы ауытқулардың жиынтығын, дисплейде бұрыс мәліметтердің шыға беруін, компьютердің ақпаратты көрсетуге тыйым салуын немесе көрсетуден бас тартуын, компьютерлік жүйенің немесе оның элементтерінің істен шығуын және аяқ астынан сөніп қалуын түсіну керек. Алайда осы жерде компьютердің физикалық тұтастылығын сақтап қалуы басты шарт болады.

Қолданыстағы заңнаманың нормаларына сәйкес компьютер жүйесі және желілерін қолдану ережелері тек заңға бағынышты қосымша нормативтік-құқықтық актілермен реттеледі. Мысалы, ол актілерге мыналарды жатқызуға болады:

– Қазақстан Республикасы Ұлттық Банкі Басқармасының 2000 жылы 21 сәуірде қабылданған №146 «Қазақстан Республикасында төлемдер мен ақша аударымдарын жүзеге асыру кезінде электронды құжаттармен алмасу ережелерін қабылдау туралы» Қаулысы;

– Қазақстан Республикасы Ұлттық Банкі Басқармасының 1995 жылы 19 қазанда қабылданған №177 Қаулысы негізіндегі «Ұлттық Банктің бөлімшелері арасында, сонымен қатар Қазақстан Республикасының банктері арасында электронды төлемдерді алмастыру кезінде бағдарламалық-криптографиялық қорғаныс жүйесін пайдалану тәртібі туралы Ережесі»;

– Сол кездегі Қазақстан Республикасының мемлекеттік кірістер Министрінің 2000 жылы 18 мамырдағы «Қазақстан Республикасы мемлекеттік кірістер Министрлігінің электронды мониторинг жүйесінің ақпаратты беру және қорғау тәртібі туралы Ережені қабылдау туралы» Бұйрығы.

Осы нормативтік-құқықтық актілердің ережелерін бұзу аталған қылмыстық іс-әрекетті қалыптастырады, мысалы, субъектінің қорғаныс жүйесінде вирустық бағдарламалардан қорғайтын және заңсыз ақпараттық кіруге жол бермейтін ақпараттық қорғаныс жүйесінің немесе операциялық бағдарламалық ортаның болмауы.

Осы аталып кеткен компьютерлік қылмыстардың нысандарының объективтік жағын қарастырмас бұрын, олардың барлығының

өз спецификасы бойынша зиянды компьютерлік бағдарламамен байланысты екенін айта кеткен жөн. Себебі виртуалды өмірде кез келген әрекет, әрекетсіздік, операция, мәтін, дыбыс, видео, презентация, форма, кейіп, нышан, түс, бояу – ол қылмыс болсын, қылмыс болмасын барлығы тек бағдарламалар жасау арқылы ғана жүзеге асады.

ҚР Қылмыстық кодексінің 210-бабының диспозициясы бойынша зиянды бағдарлама өнімдері компьютер үшін жасалған, компьютердің жұмысын бұзатын, компьютер жүйесін және желісін бұзатын немесе арнайы түрде компьютерлік ақпаратты заңсыз жою, бөгеу, өзгерту және көшіру салдарына әкелетін компьютерлік ақпараттық бағдарламаны білдіреді.

Компьютерлік құралдар үшін бағдарлама деген ұғымға түсінікті ҚР заңнамалары береді. Соның ішінде компьютерлік бағдарламаға анықтама ҚР «Авторлық құқық және сабақтас құқықтар туралы» Заңында былай делінген: Электронды есептеуіш машинасына арналған бағдарлама – ол алдыға қойған мақсаттарға жету немесе алғышарттар мен тапсырмаларды орындау үшін, сонымен қатар ЭЕМ үшін бағдарламаны жасау үшін дайындық материалдарын және аудиовизуалдық ойнау нышанын қоса есептегенде қажетті нәтижелерге жету үшін сөздермен, сандармен, кодтармен, символдармен, белгілермен, рәміздермен, диаграммалармен немесе басқа да нысандармен көрініс тапқан ережелер мен қағидалар жиынтығы.

Көптеген авторлар өз еңбектерінде зиянды бағдарламаларды анықтау үшін көп жағдайда «Компьютерлік вирус» деген сөз тіркесін пайдаланады.

Ресми түрде «компьютерлік вирус» деген терминді ең алғаш 1984 жылы Америка Құрама Штаттарының қызметкері Фред Коэн сол Құрама штаттарында ақпараттық қауіпсіздікке қатысты өткен конференцияда қолданған деп есептеледі.

Компьютерлік вирус деп өзінің көптеген көшірмелерін жасай алатын және сол көшірмелерін компьютерлердің және есептеу жүйелерінің аясына немесе олардың ішіндегі жеке файлдарға ендіре алатын бағдарламаны (немесе кодтарды жүзеге асыратын жиынтықты) айтады. Сонымен қоса тек қана көшіріліп қана қоймай, көшірмелердің өзі де басқа көшірмелерді тудырып нақ сол әрекеттерді қайта қайталап жүзеге асырып отырады [84, 172 б.].

Шынына келетін болсақ «компьютерлік вирус» деген терминмен зиянды бағдарламаларды теңдестіру дұрыс бағыт емес. Себебі бұл салада өзінің әсер ету әрекеті принциптері мен салдарына қарай компьютерлік вирустардан ерекшеленетін зиянды бағдарламалар бар. Мысалы, «Трояндық ат» – бұл бағдарлама ойдағы күткен нәтижені жасамай басқа әрекеттерді орындайды. Яғни бұл бағдарламалар өзінің мақсаты ретінде файлдарды реттеу деп көрсетеді және бағдарламалық қамтамасыз етуді белсендіргендей болып, ал шын мәнінде олардың жүзеге асыру кезінде файлдар жойылады. Сол сияқты «Құрт» – червь, бір жүйеден басқа жүйеге тез арада ауысу арқылы ерекшеленетін бағдарлама.

Зиянды бағдарлама деген ұғым ретінде, біріншіден, оның жүзеге асуына немесе аспауына байланысты емес кез келген зиянды бағдарламаның пайда болуына әкеліп соққан әрекетті жасауды түсіну керек;

Екіншіден, зиянды бағдарлама жасаудың бір нұсқасы ретінде компьютер үшін арнайы жасалған зиянды емес бағдарламаға қандай да өзгерістер енгізу арқылы, яғни модификациялау арқылы оны зиянды бағдарламалар қатарына ауыстыру әрекетін түсінеміз;

Үшіншіден, компьютерлік қылмыстардың бір нысаны болып есептеуіш құралдарға зиянды бағдарламаларды қолдану табылады. Компьютерлер үшін зиянды бағдарламаларды қолдану дегеніміз оларды компьютерлік құралдарды эксплуатациялау кезінде жүзеге асыруды білдіреді;

Төртіншіден, зиянды бағдарламаларды компьютер үшін тарату дегеніміз кез келген материалдық формада компьютер үшін, мәліметтер базасына, сонымен қатар желілерге және басқа әдістермен өндіріске мүмкіндік беру түсініледі. Таратуға тағы да осы бағдарламаларды сату, жалға беру, пайдалануға беру, несиеге беру, шетелге шығару арқылы өз мақсаттарына қол жеткізуді жатқыза береміз.

Компьютерлік қылмыстардың негізгілерінің бірі «компьютерлік вирустарды» тарату болып табылады. Сол себепті вирустарды тереңірек зерттеуге талпыныс жасап көрелік.

Компьютермен жұмыс істегенде көптеген жағымсыз жағдайлар болады. Мысалы, мәліметтерді жоғалту, компьютер программаларының қызметтен шығуы, компьютердің өздігінен

әрекет етуі т.с.с. Осы жағдайлардың себебі компьютерге еніп кеткен вирустардың әрекеттері болуы мүмкін.

Вирустар – компьютердің негізгі жаулары болып табылады. Олар биологиялық вирустар сияқты өздігінен көбейе алады, жағымсыз әрекеттер жасайды, соның салдарынан үлкен зардап тигізеді.

Вирустарды мүмкіндіктері бойынша келесі түрлерге бөлуге болады:

– зиянсыз – компьютердің жұмысына ешбір әсерін тигізбейді, тек көбею салдарынан дискідегі орынды азайтады;

– қауіпсіз – дискідегі орын азаяды, графиктік және дыбыстық ақаулар байқалады;

– қауіпті вирустар – компьютер жұмысында қатерлі зардаптар туғызады;

– өте қауіпті – жадының жүйелік бөлігінде орналасқан бағдарламалардың, құжаттардың жойылуына, компьютер жұмысына қажетті ақпараттың жоғалуына алып келеді. Қатты дискіні форматтап шығатын әрекеті де болады.

Осыдан бірнеше жыл бұрын DOS және DOS-бірегей программалар қолданыстан шыққаннан кейін осылармен бірге паразит вирустар да жойылды деп ойлағанбыз. Себебі, DOS жүйесіндегі *.com және *.exe файлдарына жұғатын вирустарды жазу кез келген программалауды білетін адамның қолынан келеді, ал Windows-қа арналған вирус күрделі және оны жазу қиынға түседі. Бірақ оған қарамастан вирустар өмірін тоқтатпады, олардың тек түрі өзгеріске түсті.

Вирустарды кімдер және неліктен жазады деген үлкен сұрақ туындауы мүмкін.

Біздің ойымызша, вирустардың көп бөлігін және қарапайым түрлерін «ассамблер» тілін жаңа үйреніп, өз мүмкіндіктерін білгісі келген студенттер мен оқушылар жазады. Ондай вирустар көп өмір сүрмейді, себебі оны тек өз мүмкіндігін тексеру үшін ғана жазады, ол таралмай жазылған дискіде қалады.

Екінші топ жастар (көбінесе студенттер) – олар программалауды толығымен меңгерместен вирустарды жазып, таратады. Олар компьютер әлеміндегі бұзақылар болып табылады.

Уақыт өте бұзақылар тәжірибелі вирус жазғышқа айналады. Олар кәсіби вирустар жазып, «профессионал» аталатын топқа жатады. Бұл топқа көбінесе талантты программистер жатады.

Олар көбінесе «стеилс» немесе полиморфтық вирустар түрін жазады. Бұл вирустар тек файлдарды ғана емес, дискінің жүктелу секторларын, жүйелік файлдарын бүлдіреді және т.б. зиянды әрекеттер істейді.

Ал соңғы топ вирустарды зерттеу үшін жазады. Олар вирустарды таратпайды, бірақ оны қалай жазу керектігі туралы шығармалар жасайды.

Вирустардың көптеген таралу жолдары белгілі. Вирус қолданушы компьютеріне дискеттен, компакт дискілерден немесе электронды почтадан келуі мүмкін. Вирустардан сақтану үшін әрбір қолданушы вирустан қорғануды білуі керек. Себебі, болашақта вирустар толығымен жойылады деген ешқандай сенім жоқ.

Кез келген ауруға ерте не кеш болса да ем табылатыны ертеден белгілі болған. Компьютерлік әлемде сондай емдік программалар антивирустар деп аталады.

MS-DOS ОЖ-де ақпаратты қорғаудың тиімді жабдығы жоқ. Сондықтан да қазіргі уақытта MS-DOS ОЖ-де вирусты іздеп табу және жою үшін вирусқа қарсы программалар көптеп шыға бастады. Сондай антивирустар Aidstest, Adinf, MicroSoft AntiVirus, Norton Antivirus, Kaspersky Anti-Virus, Doctor Web программалары [85].

Вирустар және олардың түрлері. Компьютерлік вирус – арнайы жазылған шағын көлемді (кішігірім) бағдарлама. Ол өздігінен басқа бағдарламалар соңына немесе алдына қосымша жазылады да, оларды «бүлдіруге» кіріседі, сондай-ақ компьютерде тағы басқа келеңсіз әрекеттерді істеуі мүмкін. Ішінен осындай вирус табылған бағдарлама «ауру жұққан» немесе «бүлінген» деп аталады. Мұндай бағдарламаны іске қосқанда алдымен вирус жұмысқа кірісіп, оның негізгі функциясы орындалмайды немесе қате орындалады. Вирус іске қосылған бағдарламаларға да кері әсер етіп, оларға да «жұғады» және басқа да зиянды іс-әрекеттер жасай бастайды (мысалы, файлдарды немесе дискідегі файлдардың орналасу кестесін бүлдіреді, жедел жадыдағы бос орынды жайлап алады, толтырады және т.с.с.).

Өзінің жабысқанын жасыру мақсатында вирустың басқа программаларды бүлдіруі және оларға зиян ету әрекеттері көбінесе сырт көзге біліне бермейді. Оның кері әсері белгілі бір шарттарды орындағанда ғана іске асады. Вирус өзіне қажетті бүлдіру әрекеттерін орындаған соң, жұмысты басқаруды негізгі

программаға береді, ал ол программа алғашында әдеттегідей жұмыс істей береді. Сөйтіп ол программа бұрынғы қалпынша жұмысын жалғастырып, сырт көзге «вирус жұққандығы» бастапқы кезде байқалмай қалады.

Вирустың көптеген түрлері ЭЕМ жадысында DOS-ты қайта жүктегенше тұрақты сақталып, оқтын-оқтын өзінің зиянды әсерін тигізіп отырады.

Вирустың зиянды іс-әрекеттері алғашқы кезде жұмыс істеп отырған адамға байқалмайды, өйткені ол өте тез орындалып әсері онша білінбеуі мүмкін, сондықтан көбінесе адамдардың компьютерде әдеттегіден өзгеше жағдайлардың болып жатқанын сезуі өте қиынға соғады.

Компьютерде «вирус жұққан» программалар саны көбеймей тұрғанда, онда вирустың бар екені сырт көзге ешбір байқалмайды. Бірақ біраз уақыт өткен соң, компьютерде әдеттегіден тыс, келеңсіз құбылыстар басталғаны білінеді, олар, мысалы, мынадай іс-ерекеттер істеуі мүмкін:

– кейбір программалар жұмыс істемей қалады немесе дұрыс жұмыс істемейді;

– экранға әдеттегіден тыс бөтен мәліметтер, символдар, т.б. шығады;

– компьютердің жұмыс істеу жылдамдығы баяулайды;

– көптеген файлдардың бүлінгені байқалады және т.с.с.

Компьютерге вирус жұққанын байқаған кезде кейбір файлдар мен каталогтар, дискідегі мәліметтер бұзылып үлгереді, оның үстіне пайдаланылған дискеттер арқылы немесе жергілікті байланыс желілері бойымен компьютердегі вирус басқа компьютерлерге таралып кеткені байқалмай да қалады.

Вирустардың кейбір түрлерінің кері әсері тіпті одан да терең болады. Олар бастапқы кезде өзінің жұққанын ешбір әсерімен білдіртпей, көптеген программалар мен дискілерге үнсіз таралып кетеді де, сонан соң бірден бел шешіп зиянкестік жасауға кіріседі, мысалға, компьютерден қатты дискіні өздігінен қайта форматтап шығады. Ал зиянкестік әсерін программаларға өте аз тигізіп, бірақ қатты дискідегі мәліметтерді іштен «мұжып», құртып жататын вирустарға не істеуге болады?!

Осының бәрі вирустан дер кезінде қорғанбасақ, оның келешектегі әсері керекті мәліметтерді жоғалтуға душар ететіні талас тудырмаса керек.

Вирус программасының байқалмау себебі олардың көлемі кішігірім ғана болады да, өздері ассемблер тілінде жазылады. Кез келген жағдайда вирус программасы қай компьютерге арналып жазылса да, ол мәлімет алмасып жұмыс істейтін басқа компьютерлерге де тез тарап кетеді және өздігінен вирус өте көп зиянкестік әрекеттер жасауы да мүмкін.

Қазіргі кездегі вирустар негізгі екі топқа бөлінеді:

– резиденттік (компьютер жадында тұрақты сақталатын) вирустар;
– резиденттік емес вирустар.

Вирус жұққан программа іске қосылғанда резиденттік вирустар әсерлене әрекет етеді, олар жедел жадыға көшіріліп жазылып, алғашқы бірсыпыра уақытта әсері сезілмегенмен, соңынан бірден іске қатты кіріседі. Бұл вирустарды тез анықтау ісін қиындатады.

Дискілерге мәлімет жазу кезінде вирус өзінің жабысуына қолайлы сәт іздеп негізгі операциялар орындалып жатқанда солармен қосылып дискіге жазылып алады да, оның қалай жұққанын адамдар білмей де қалады. Ал, резиденттік емес вирус жедел жадыға тұрақты күйде жазылмайды, бірақ вирустың әсері тиген программа іске қосылғанда ол екпіндене түседі де, өзі жұмыс істеп тұрған каталогтан немесе «PATH» командасында көрсетілген каталогтардан өзі ішіне байқаусыз еніп кететін файл іздейді. Ондай файлды тауып, оның ішіне кіріп алып, ол кейін жұмыс істейтін кезде соған зиянды әрекетін тигізеді.

Компьютерлік вирустар дегеніміз бұл сонда не? Бәрінен бұрын бұл – өзінен-өзі көбейіп кететін бағдарламалар. Міне, компьютерлік вирустарға дәл осындай анықтама берген, құбылысты алғашқы зерттеушілердің бірі Фред Коэн.

Бұл өзінің дара еркі бойынша бола беретін бағдарламалар пайдаланушының қалауынсыз, оның еш қатысынсыз өзінің көшірмелерін жасап алады да, оларды басқа компьютерлерге таратады.

Бұл – вирустың қызметінің бір жағы. Сонымен қатар, ең қорқынышты емесі, егерде вирус бағдарламаның жұмысына кедергі келтірмей жай ғана көбейген жағдайда, онда онымен, бәлкім байланысудың қажеті де шамалы. Әйтсе де, кіріп кеткен вирустардың айтарлықтай бөлігі, дәлірек айтқанда, осынау салыстырмалы еш зиянсыз категорияға жатады.

Алайда, көбеюден басқа вирустың тағы бір қызметі «хобби» бар – ол бүлдіру, былғап тастау. «Былғаудың» дәрежесі әр түрлі болуы мүмкін – біреулері сіздің жұмысыңызға кедергі келтіретін экранға мезі еткен суреттерді шығаруымен шектелсе, басқалары ерекше ойланып жатпастан-ақ мәліметтерді қатты дискіден де құртып жібереді. Шындықтың қоспасы, жарым шындық, ойдан құрастырылған қорқыныш – «компьютерлік вирустар» туралы біздің білетіндеріміз небәрі осы ғана. Біреулері кез келген бағдарламаларды қоюға үрейлене қорқады, басқалары электрондық почтадан жалтарады...

Қажет болса, өзінің компьютеріне сәнді антивирус қойып алған осындай пайдаланушылар нағыз қауіппен бетпе-бет келгенде мүлде қорғаусыз қалады.

Компьютердегі кез келген антивирустық бағдарламаның көлемі вирустан қорғауға кепілденген. Сөз жоқ, жақсы антивирустық бағдарлама – бұл вирусты құрту немесе жою мүмкіндігін жоғарылатудың бір ғана тәсілі.

Антивирустық бағдарлама өзімен-өзі не жасай алар еді: бұл бар болғаны қабыршығы ғана, ең маңызды бөлігін құру мәліметтер базасы. Осының арқасында ғана бағдарлама залалды нәрсені тауып алып, кәдімгі бағдарламаны файлдан немесе құжаттан айырып алуы мүмкін.

Алайда жаңа вирустар әр күн сайын пайда болады және егер пайдаланушы өзінің антивирусының мәліметтер базасын жаңартуды күн сайын қадағалап отырмаса, оның бүкіл қуаты пайдаға жарамай қалуы да мүмкін. Осыдан шығатын қорытынды мынау: мәліметтердің антивирустық базасын бір аптадан кешіктірмей жаңартып тұру қажет, ал керек болған жағдайда күн сайын жаңартқан жөн. Антивирустық база неғұрлым жаңартылған сайын, сіз сенімді түрде компьютермен, тасымалдауыштармен және желімен жұмыс істей аласыз, яғни, компьютеріңіз мүмкіндігінше зиянды бағдарламалардан қорғалған болып саналады.

Бүлінген және вирус жұққан файлдар. Вирус дискідегі кез келген файлды бүлдіре алады, бірақ кейбір файлдарға ол бірден жабысады, яғни ол файлдың ішкі көлемінен орын алып, оның қызметін түрлендіріп, қолайлы жағдай туғанда, зиянды әрекетін бастап кетеді. Дегенмен, көптеген программалар мәтіні мен құжаттарға, мәліметтер базасының ақпараттық файлдарына, электрондық кестелердегі мәліметтерге вирустар онша әсерін

тигізе алмайды, тек оларды аздап қана зақымдауы мүмкін. Вирустар мынадай файлдарға жұғуы мүмкін.

Бірден орындалатын файлдар, белгілі бір іс-әрекет істейтін кеңейтілулері (заты) .com және .exe болып келген файлдар, сондай-ақ басқа программаларға қажет кезінде қосылатын оверлейлік файлдар. Файлдарды зақымдайтын мұндай вирустарды *файлдық* деп атайды. Вирус жұққан файлдар өздерінің кері әсерін жұмыс істейтін, іске қосылған сәттерде жасайды. Ең қауіпті вирустарға резиденттік түрде жедел жадыда сақталып, орындалатын әрбір программаны зақымдап отыратындары жатады. Ал егерде олар AUTOEXEC.BAT және CONFIG.SYS арқылы іске қосылатын программаларға жұқса, онда компьютер өшіріліп қайта іске қосылған сайын вирустар өз әсерлерін тұрақты қайталап жүргізіп отырады.

Операциялық жүйенің жүктеуіші мен қатты дискінің ең басты мәлімет жүктеу жазбасы. Бұл аумақтарды зақымдайтын вирустар «жүктегіш» (загрузочный) немесе Boot - вирустар деп аталады.

Мұндай вирустар өз қызметін компьютерді іске қосқанда, яғни операциялық жүйені жүктегенде бірден бастайды және әрдайым компьютердің жедел жадында тұрақты сақталады. Бұлардың таралу тәсілі – компьютерге салынған дискеттердің алғашқы жолдарына жазылған жүктегіш мәліметіне зақым келтіру болып табылады. Әдетте мұндай вирустар екі бөліктен тұрады, өйткені дискеттің жүктеуіш жазбасы мен операциялық жүйенің басты жазбасы өте шағын көлемнен тұрады, сондықтан вирус бірден түгелдей олардың ішіне орналаса алмайды. Вирустың екінші бөлігі дискінің түпкі каталогының соңына немесе мәліметтер кластерлеріне жазылып қалады.

Құрылғылар драйверлері, яғни CONFIG.SYS файлының шеткері құрылғылар көрсетілетін «Devise» деген сөз тұрған жолында жазылған файлдар. Ондай файлдағы вирус сол құрылғыны іске қосқан сайын қызметке кіріседі. Бірақ драйверді бір компьютерден екінші компьютерге көшіру өте сирек болатындықтан, мұндай вирустар көп тарала қоймаған. DOS жүйелік файлдарына (MS DOS.SYS және IO.SYS) да вирус жұқтырылуы теория жүзінде мүмкін болғанымен, олардың таралуы іс жүзінде өте сирек кездеседі.

Әдетте әрбір вирус түрі файлдың бір немесе екі типіне (түріне) ғана «жұғады». Көбінесе бірден орындалатын файлдарға

«жұғатын» вирустар жиі кездеседі. Дискінің жүктегіш аймағын зақымдайтын вирустар екінші орында деп айтуға болады. Шеткері құрылғылар драйверлерін зақымдайтын вирустар сирек кездеседі, әдетте олар бірден орындалатын файлдарға да зиянын тигізеді.

Файлдық жүйені өзгертетін вирустар. Соңғы кезде вирустың жаңа түрлері – дискідегі файлдық жүйені өзгертетін вирустар көбейіп таралуда, оларды қысқаша DIR-вирустар деп атайды. Мұндай вирустар өз мәтінін дискінің белгілі бір бөлігіне (әдетте дискінің соңғы кластеріне) жасырын жазып қояды да, оны дискінің файлды орналастыру кестесіне (FAT) файлдың соңы ретінде белгілейді.

Барлық .COM және .EXE типті файлдар үшін – каталогтағы файлдың алғашқы мәліметі көрсетілген орынға вирус жазылған қате орын көрсетіліп, ал дұрыс көрсеткіш – таңбаланған (кодталған) түрде каталогтың пайдаланылмайтын бөлігіне жасырылады. Сол себепті кез келген бағдарламаны іске қосқанда дискіден бірінші вирус оқылады да, ол тұрақты компьютер жедел жадында сақталып файлдарды өңдейтін DOS бағдарламаларына жабысады. Бірақ жалпы көрініс каталог дұрыс жұмыс атқарған сияқты болып сырт көзге мұның әсері білінбей тұрады. Тек вирусы бар дискеттерден программалық файл оқитын сәттерде оның нақты көлемі қысқарып небәрі 512 не 1024 байт қана болып қалады. Бірақ атқарылуға тиіс вирусы бар әрбір программа іске қосылғанда оның дұрыс емес екендігі байқалмайды. Міне осылай «ауырған» дискілерді дұрыс қалпына келтіру үшін тек арнайы антивирустік программалар қажет (мысалы, Aidstest бағдарламасының соңғы нұсқалары).

Мұндай компьютерлерде ChkDsk, ScanDisk бағдарламаларының көмегімен тексеріс жүргізуге болады.

Бұл бағдарламалар жұқтырылған файлдар туралы, жоғалған кластерлер туралы көптеген хабарлар бере алады.

DIR-вирустың қауіптілігі мынада: мұндай вирустарды ScanDisk текті бағдарламалардың көмегімен түзетудің қажеті жоқ, өйткені дискіні бүлдіріп алуы мүмкін. Бұл вирусқа тек қана вирусқа карсы бағдарламаларды қолдану қажет.

Екінші түрі БҰЛДІРГІ (ЗАРАЗА) – IO.SYS жүйелік файлын жұқтырады.

Мұндай вирустар файлдық жүктеуші вирус болып табылады. DOS бастапқы жүктеуші механизмі мен файлдармен жұмыс-

тың қарапайым механизмі арасында келіспеушілік әрекеттерді орындайды.

Осылайша түпкі каталогта IO.SYS атты екі элемент пайда болады.

Бұл вирустың кауіптілігі: компьютерді таза жүйелік дискетадан SYS C: командасын енгізу арқылы жүктеген жағдайда вирус дискіден жойылмайды.

«Көрінбейтін» және «өздігінен өрбитін вирустар». Өзін жай көзге сездірмес үшін кейбір вирустар жасырынудың қилы-қилы тәсілдерін пайдаланып жүр. Осындайлардың екі түрін – «көрінбейтін» және «өздігінен өрбитін вирустарды» қарастырайық.

«Көрінбейтін вирустар». Көптеген резиденттік вирустар былай жасырынуды әдетке айналдырған, олар DOS жүйесінің вирус жұққан файлдарды шақыруын өзгертпей дұрыс күйінде қалдырады. Бірақ бұл эффект тек вирус жұққан компьютерде ғана байқалады, ал вирус жұға қоймаған компьютерлерде файлдар мен дискілерді жүктеуіш аймақтарының өзгеруін байқау қиын емес.

«Өздігінен өрбитін вирустар». Вирустардың жасырыну жолының екінші тәсілі – өзін-өзі аздап өзгертіп, өрбіп толықтырылып отыруы. Көптеген вирустар жасайтын кері әсерін байқатпас үшін өз көлемінің бірсыпырасын жасырын күйде сақтайды. Бірте-бірте өрби отырып, олар таңбалану тәсілін де, таңбаланбаған алғашқы бөлігін де аздап өзгертіп отырады. Осының арқасында вирусты іздеп табатын тұрақты байттар тізбегі болмай, оларды ұстайтын детектор-программалар жұмысы қиындайды [86, 440 б.].

Компьютерлік вирустардың қысқаша жіктелуі. Қазіргі кезде 50 000 шамасында компьютерлік вирустар белгілі. Оларды әдетте мақсатына, жұмыс логикасына, көлеміне және жұмыс істеу аумағына қарай топтарға жіктейді (1-кесте).

Жұмыс логикасына және мақсатына қарай оларды шартты түрде төмендегідей жіктеуге болады:

«Ұстауыш-вирустар» – бағдарламалық құралдар кешеніндегі қателіктер мен дәлсіздіктерді пайдаланады. Көлемді бағдарламаларды түзету кезінде белсенділік көрсетіп бағдарламаға жабысады. Әртүрлі зияндық әрекеттері бар вирус.

«Логикалық бомбалар» (баяу әсер ететін «бомбалар»)

– қарапайым бағдарламаларға кіріп алып білінбей тұрады. Тек белгілі бір шарттар (көрсетілген күн-ай мерзімінде немесе уақытта, бағдарлама орындалуының белгілі кезеңінде) орындалғанда ғана әсер ете бастайды. Сол шарт орындалар мезетке дейін неғұрлым көп бағдарламаларға «жұғуға» тырысады.

1-кесте

Компьютерлік вирустардың жіктелуінен мысал

Мөлшері бойынша	Жұмыс істеу логикасы бойынша	Жұмыс істеу аумағы бойынша	Мақсаты бойынша
«A» 648 байт «B» 1701байт	«ұстауыштар»	дербес электронды есептеу құралдарында	бейсауат
«C» 1808 байт	«логикалық бомбалар»	көп машиналы кешендерде	шантаж
«D» n байт	«құрттар»	информациялық есептеу желілерінде	аралас мақсатты
«E» 1800 байт	«троялық аттары»	есептеу желілерінде	мағынасыз
«N» n байт «Z» n байт	«жолбарыстар»	электронды есептеу машиналарының желілерінде	насихатшы

«Құрттар» – жүйелік программалаушылардың ақпараттық-есептеу желілерінің бос тұрған ресурстарын анықтау бағдарламаларына кіріп алып, сол бос құрылғыларды тектен тек жұмыс істеуге мәжбүр етеді. Мысалы, оларды шексіз циклге енгізіп, құрдан-құр жүргізіп кояды немесе қажетсіз мәліметтерді баспаға шығартады және т.с.с.

«Троян аттары» – қарапайым қолданбалы бағдарламаларға еніп алып, соларға рұқсат етілмеген әрекеттерді (жасырын ақпаратты оқып жария етеді, жедел жадыдағы ақпараттарды

«басқа жаққа» жіберуге дайындайды) орындатады. Жасалу құрылымы мен көбею жолы оңай болғандықтан, көбінесе компьютер желілерін жаулап алады.

Мақсаттарына қарай вирустар мынадай 4 бөлікке бөлінеді (1-кесте, 4-бағана):

1. «Бейсауат» (гуманды) – онша қатты зиянын тигізбейтін вирустар.

2. «Шантаж жасаушы» – мысалы, белгілі төлемақы берсе, вирус әсері жоғалатынын анонимді түрде хабарлайтын «баяу әсер ететін бомбалар».

3. «Насихатшы» – «өзін көрсету» мақсатында жасалған.

4. «Мағынасыз» – атынан-ақ әсері түсінікті.

Бізде кең тараған Aidstest антивирустік бағдарламаларының авторы Д. Лозинскийдің ұсынысы бойынша, вирустарды көлеміне қарай жеті топқа жіктеуге болатыны белгілі, олар l-кестеде керсетілген.

Сонымен компьютерлік вирустардың түрлері мен топтары туралы біраз сауатымызды ашқан секілдіміз, ендігі кезекте вирустардың пайда болуы және даму тарихы аясынан пайдалы ақпараттарды қарастырып өтсек болғаны.

Вирустар тарихынан. Бұл жағдай көп те емес, аз да емес шамамен қырық жыл бұрын басталған еді. Міне сол кезде, 60-шы жылдардың соңында «персоналкалар» туралы тек қана фантастикалық романдардан оқуға тура келгенде, АҚШ-тың ірі зерттеу орталығындағы бірнеше «үлкен» компьютерлерде өте үйреншікті емес бағдарламалар табылды. Қалыпты бағдарламалардан ерекшелігі «структура бойынша» айтқанмен жүретін, әрі адамның барлық талап-тілектерін орындайтын, киплингтік мысықтар тәрізді бұлар өзімен-өзі серуендеп жүреді. Компьютердің қыртыстарында қандай да бір өздеріне ғана түсінікті іспен айналысатын еді, іс барысында компьютердің жұмысын қатты жылдамдатады. Бір жақсысы әлгілер мұның өзінде де ештеңе бүлдірмеді, әрі көбейе де қоймады.

Алайда бұл ұзаққа созылмады. 70-ші жылдардың өзінде-ақ көбеюге бейім және өздерінің жеке атауларына ие болған алғашқы нағыз вирустар тіркеледі: Univac 1108 үлкен компьютерлері Pervading Animal вирусымен ауырып қалады, ал әйгілі отбасылық IBM-360/370 компьютерінде Christmas tree вирустары ұя салады.

1980 жылы белсенді вирустар саны тіпті жүздеген мөлшерге жетеді [87].

Дербес компьютерлердің көрінуі мен таралуы нағыз эпидемияны туындатты, вирустардың есебі мыңдаған санға барды. Шынында да, «компьютерлерлік вирус» термині тек 1984 жылы ғана көріне бастады. Бірінші рет оны, жоғарыда бірнеше рет айтып кеткендей, ақпараттық қауіпсіздік туралы өзінің баяндамасында АҚШ-тың Лекай университетінің қызметкері Ф. Коэн пайдаланды.

Алғашқы «персоналдық» вирустар қарапайым әрі көнбіс тіршілік етті және пайдаланушылардан айрықша жасырына алмады, өзінің бүлдіретін іс-әрекетін (файлдарды шығарып жіберуде, дискінің логикалық құрылымын бұзуда) ажарлап атқарды. Экранға суреттерді және «Килиманджаро тауының тура биіктігін миллиметріне дейін атаңдар! Дұрыс жауап енгізілмеген кезде сіздің винчестеріңіздегі барлық мәліметтер жойылып кетеді!», – деген арам ниетті «қалжың ысқақты» ақпаратты шығаратын. Мұндай вирустарды анықтау қиынға соқпады.

Классикалық вирустың «алтын ғасыры» он жылға дейін созылды. Бүгін олардың саны күрт қысқарып кетті және де олар «Касперский лабораториясының» бағалауы бойынша барлық вирустардың жалпы санының бірнеше пайызын ғана құрайды. Вирустардың бірқатар типтері мынадайлары: қатты дискінің тиейтін секторын жойып жіберетін boot-вирус тәрізділері бүгін іс жүзінде құртылған. Бір қарағанда ақыр аяғында stealth-вирустарына қарсы ем табылды. Бірақ компьютерлердің хәлін жеңілдететін ғалымда басты қадамдар жасалғанымен вирустар әлемі енді ғана басталған еді...

1995 жылы 6.0 және 7.0 версиясы үшін Word құжаттарына жұқтырылатын вирустар шыға бастайды. Құжаттар орындалатын файл болмағандықтан мамандар бұл мәтіндік редакторлардың жазылған құжаттарында вирустың болуы мүмкін емес деп санаған. Бұл ой теріске шықты. Вирус жұқтырылған құжатты ашқан кезде жұмысты бастайтын болды.

Вирус бар кезде бұл құжаттарды SAVE AS арқылы сақтауда, вирус өзінің макрокомандаларын дискіге көшіріп, сол арқылы жұқтыру әрекетін орындап отырды. Бұл вирустар макровирустар деп аталады [88, 12-22 б.].

1998 жыл мен 1999 жылдың аралығында әлем бірнеше шын мәніндегі тас-талқан ететін вирустар шабуылынан өтті, BIOS жүйелілік платаларын жойып жіберген Win95.CIH вирусының қызметі нәтижесінде дүниежүзінің барлық елдерінде 100 миллионға жуық компьютерлер істен шығып қалды. Ал тіпті жақында ғана 2003 жылдың ортасында жаһандық желі электрондық хаттарға салыну арқылы тарайтын жаңа «SoBig құртынан» зардап шекті.

Біз өз тарапымыздан, компьютерлік вирустарды талдай отырып, қоғамда ақпараттандыру қатынастарды жүзеге асыру барысында салауатты болуына шақыра отырып қандай да бір мөлшерде виртуалды қауіпсіздікке атсалысып, өзіміздің байқауларымызбен және ұсыныстарымызбен бөліспекпіз.

Компьютерлік вирустардан сақтанудың негізгі тәсілдерін атап өтуге болады. Компьютерлік вирустар «таза» компьютерге вирус жұққан иілгіш дискеттер, дисктер, флештасымалдауыштар және т.б. арқылы таратылады. Егер компьютер жергілікті желіге қосылған болса, онда вирустың таралуына бұрынғыдан да кең жол ашылады.

Айта кететін жайт, вирустардың кейбір түрлері компьютерге келісімен зиянды ісіне кірісіп кетеді, ал олардың кейбірі файлдар құрамына енсе де іске кіріспей, біраз уақыт тым-тырыс жасырынып жатады, бұл уақытты «инкубациялық мезгіл» деп атайды. Бұл мезгіл аралығында олар екпінді күйде файлдар арасына таратылып, зақым келтіруді белгілі бір уақыт мөлшері өткен соң немесе ол өзін-өзі белгіленген мөлшерде көбейтіп болған соң ғана бастайды.

Вирустардан сақтану үшін мынадай шаралар қолдануға болады:

– ақпаратты қорғаудың жалпы шаралары – дискіні физикалық зақымданудан сақтау, дұрыс жұмыс істемейтін бағдарламаларды қолданбауға және жұмыс істеп отырған адам қателіктер жібермеуге тырысуы;
– профилактикалық шараларды пайдалану, яғни вирусты жұқтыру мүмкіндігін азайту тәсілдерін қарастыру;
– вирустан сақтайтын арнайы бағдарламаларды пайдалану.

Жалпы ақпаратты қорғау тәсілдері тек вирустан сақтануда ғана емес, басқа жағдайда да пайдалы болатынын есте сақтаған жөн. Ондай тәсілдің негізгі екі түрі белгілі.

1. Ақпараттың көшірмесін алып отыру – файлдарды және дискінің жүйелік мәліметтерін көшіріп сақтау.

2. Керекті ақпаратты басқалардың жиі пайдалануына тосқауыл қою – ол ақпаратты рұқсатсыз (санкциясыз) көшіріп алуды, яғни бағдарламамен дұрыс жұмыс істемейтіндерден және қателігі бар бағдарламалардан қашық жүруді және мәліметтерді өзгертуді, вирустар енгізуді болдырмауды қамтамасыз етеді.

Вирустардың жаңа түрлері күнбе-күн пайда болып жатыр, сондықтан антивирустық бағдарламалардың да тексеру-емдеу қабілеттері жоғары соңғы шыққандарын қолданған дұрыс болатыны түсінікті шығар.

Компьютерге вирус енген жағдайларда, мына ережелерді мұқият орындаған абзал:

1. Алдымен аспай-саспай, ойланып іске кіріскен жөн екенін ұмытпаңыз.

2. Дегенмен, бір әрекет бірден орындалуы керек – вирустың зиянды әрекеттерін әрі жалғастырмас үшін компьютерді бірден өшіру қажет.

3. Егер компьютерге «жұққан» вирус түрін емдей алатын детектор-программаларыңыз болса, дискілерді тексеру мақсатында соларды дереу іске қосыңыз.

4. Біртіндеп вирус жұғуы мүмкін болған барлық дискілерді тексеріп шығу қажет.

5. Егер дискідегі барлық файлдарыңыздың архивтік көшірмелері болса, онда дискіні қайта форматтап, мәліметтеріңізді бұрынғы қалпына келтіруге тырысыңыз.

Енді компьютерге вирус жұқтыру мүмкіндігін азайтатын және жұққан жағдайда оның зиянкесті әрекеттерін барынша азайтатын шараларды қарастырайық, оларды бірнеше топтарға жіктеуге болады:

1) Ақпаратты әркімнің жиі пайдалануын шектеу және оның көшірмесін сақтау.

2) Сырттан келген мәліметтерді мұқият тексеруден өткізу.

3) Вирустан «емдеу аспаптарын» дайындап қою.

4) Белгілі бір уақыт сайын компьютерді вирусқа тексеріп отыру.

Компьютерлік вирустарды іздеп табу және оларды жою. Жалпы ақпаратты сақтаудың ортақ тәсілдерінің қажеттілігіне қарамастан, қазіргі кезде тіпті олардың өзі жеткіліксіз болып отыр.

Вирустан сақтану үшін арнайы бағдарламалар қажет және оларды тұрақты түрде қолдана бастау керек. Мұндай бағдарламаларды бірнеше түрлерге бөлуге болады:

– детекторлар;

– докторлар (фаг-бағдарламалар);

– ревизорлар (файлдардағы және дискінің жүйелік аумақтарындағы өзгерістерді бақылайтын бағдарламалар);

– доктор-ревизорлар;

– сүзгі-программалар (вирустан сақтайтын резиденттік бағдарламалар) жеке вакциналар (иммунизаторлар).

Вирустардың әсерін жоятын антивирустық бағдарламаларды үш негізгі топқа бөлуге болады:

– файл мәліметтерінің бақылауға арналған олардың қосындыларын есте сақтауға негізделген бағдарламалар;

– бағдарламаға немесе операциялық жүйеге вирус жұққан сәтте оларды анықтайтын резиденттік бағдарламалар;

– вирустар жұқтырылғаннан кейін олардың бар екенін анықтайтын бағдарламалар.

Файлдардағы мәліметтердің белгілі бір сипаттамаларын есте сақтайтын антивирустік бағдарламалардың (программалардың) негізгі жұмысы – сол файлдардың жаңа сипаттамаларын бұрын белгіленіп жазылып қойылған мәндермен салыстыру. Егер файл ішіне вирус енсе, онда олар бір-біріне сай келмейді де, бағдарлама ол туралы экранға ескертпе хабар шығарады. Осы тәсілмен бұрын белгісіз жаңадан шыққан вирус түрін де анықтауға болады. Бірақ бұрын белгіленіп жазылып қойылған сипаттамаларды вирустан мұқият сақтау қажет. Ал кейде сол сипаттамалардың өзгеруі вирустың әсерінен емес, тексергеннен кейін өзіңіздің өзгертуіңізден де болуы ықтимал. Оның үстіне, сіз тексеру сипаттамаларын жазу кезінде компьютерде вирус жоқ екеніне сенімді күйде болуыңыз қажет, әйтпесе бұл тәсіл дұрыс нәтиже бере алмайды.

Сондай-ақ, бұл программалардың тағы бір кемшілігіне тексеруге көп уақыттың кетуі мен бақылау сипаттамаларының файл көлемін шектен тыс үлкейтетінін жатқызуға болады. Оған қоса, ол мәліметтерді көшіру немесе аттарын өзгерту қажет болса, тағы да сипаттамаларын өзгертіп жазу керектігі түсінікті болар.

MS DOS ОЖ-де ақпаратты қорғаудың тиімді жабдығы жоқ. Сондықтан да қазіргі уақытта MS DOS ОЖ-де вирусты іздеп

табу және жою үшін вирусқа қарсы программалар көптеп шыға бастады.

Aidstest, DrWeb, Adinf, Norton Antivirus программалары.

Вирусқа қарсы тіркелген программалары бар ОЖ-лер де кездеседі. Мысалы: UNIX ОЖ-сі.

Жұқтырылған файлдармен вирусқа қарсы бағдарламалар жұмыс істеген кезде бағдарлама файлды қайтадан қалпына келтіруге тырысады.

Файлды қалпына келтіру мүмкін болмаған жағдайда, ол файл әрі қарай жұмысқа жарамсыз деп саналып, жойылуы керек.

Вирус файлға жұқтырылғанын білудің тағы бір айғағы файлдың көлемінің өзгеруі.

Вирус жұқпайтын файлдар: **.**BMP, **.**PCX, **.**GIF, **.**WMF форматты графиктік файлдар тек қана суреттер сақтайды. Вирус қанша әсер еткенімен де көріністі сол қалпында көруге болады. Бұл файлдарды жұмысқа қосқанда вирус күш ала алмайды.

Вирусқа қарсы бағдарламаларды орындалатын функцияларына байланысты жіктеуге болады.

Детектор-программалар тек бұрыннан белгілі вирус түрлерінен ғана қорғай алады, жаңа вирусқа олар дәрменсіз болып келеді.

Доктор-программалар немесе «фагтар» вирус жұққан бағдарламалар мен дискілерден «вирус» әсерін алып тастау, яғни «жұлып алу» арқылы емдеп, оларды бастапқы қалпына келтіреді.

Ревизор-программалар да алдымен бағдарламалар мен дискінің жүйелік аймағы туралы мәліметтерді есіне сақтап, содан соң оны кейінгісімен салыстыра отырып сайкессіздікті анықтаса, оны дереу бағдарлама иесіне хабарлайды.

Доктор-ревизорлар – доктор-программа мен ревизорлар арасынан шыққан гибрид. Бұлар тек файлдағы өзгерістерді, анықтап қана қоймай, оларды автоматты түрде емдеп бастапқы қалыпты жағдайға түзеп келтіреді.

Сүзгі программалар – компьютердің оперативтік (жедел) жадында тұрақты (резиденттік) орналасады да, вирустардың зиянды әрекетіне әкелетін операцияны ұстап алып, бұл туралы жұмыс істеп отырған адамға дер кезінде хабарлап отырады. Одан әрі шешім қабылдау әркімнің өзіне байланысты болады.

Вакцина-программалар (немесе иммунизаторлар) компьютердегі бағдарламалар жұмысына әсер етпей, оларды вирус

«жұққан» сияқты етіп модификациялайды да, вирус әсерінен сақтайды, бірақ бұл программаларды пайдалану онша тиімді емес [89, 25 б.].

Компьютерлік қылмыстардың объективтік жағының негізгі белгілері аталып, қарастырылып кетті, ал қосымша белгілері аса ерекшелікпен де, жалпы белгілермен де көрініс табады, олар қылмыс жасаудың орны, уақыты, қылмыс құралы, жағдайы және қымыстың ерекшелігіне байланысты басқа да элементтері болуы мүмкін.

Компьютерлік қылмыстардың орны басқа кез келген қылмыспен салыстырғанда шындығында өте ерекше. Қылмыс жасауды нақтырақ айтсақ қылмыскердің орны жер шары бойынша кез келген нүкте болуы мүмкін. Ол тіпті жер бетінде, әуеде, жер астында, су астында, жүріп келе жатқан көлік ішінде, орман ішінде, тіпті космоста болуы мүмкін.

Ал қылмыстың жәбірленуші жағы, зардап шеккен жағы немесе жалпы объектісі қылмыскерге қарама-қарсы бағытта, әлемнің кез келген жерінде болуы мүмкін. Мысалы, қылмыскер Қазақстанның азаматы болып Алматыдан қылмыстық әрекетті жасаса, оның объектісі Австралияда болуы мүмкін.

Компьютерлік қылмыстардың осы ерекшелігі олардың шекараға, арақашықтыққа бағынбауы және тәуелсіз болуы.

Компьютерлік қылмыстардың уақыты да үлкен мәселе, себебі киберқылмыстар уақыты айтылып кеткен қылмыс орны сияқты ауқымды, кең деген ассоциациялармен байланысты, яғни қылмыс жасау уақыты белгілі шектеулерге тәуелді емес, қылмыс кез келген жерде, кез келген уақытта жасала береді және ол ешкімге де мәлім болмауы мүмкін.

Компьютерлік қылмыстарды жасаудың жағдайы. Қылмыстың жағдайына қылмысқа дейін және қылмыс уақытында өз арасында әрекет ететін әртүрлі объектілер, құбылыстар және процестер кіреді. Олар қоршаған ортаның жерін, уақытын, заттай, табиғи, климаттық, өндірістік, тұрмыстық және басқа да шарттарын сипаттайды, заңға қайшы оқиғаның тікелей емес қатысушыларының мінез-құлқының ерекшеліктерін, олар арасындағы психологиялық байланысты және қылмысты жасаудың мүмкіндігін, шартын, жағдайын анықтайтын объективтік шындықтың басқа да факторларын сипаттайды.

Компьютерлік ақпарат саласындағы қылмыстың жағдайы бірқатар факторлармен сипатталады.

Ең алғаш бұл қылмыстар кәсіби қызмет саласында жасалатынын ескерген жөн. Қылмыскерлер ЭЕМ-ді және оның құрылғыларын басқару саласында ғана арнайы тәжірибеге ие емес, тұтас алғанда ақпараттық жүйелерде ақпаратты өңдеу шегінде арнайы білімге де ие. Сонымен қоса қаржы, банк және толық ақпараттық технологиялар саласында арнайы түсініктер болуы қажет.

Міне компьютерлік қылмыстардың объективтік жағының жалпыланған қылмыстық-құқықтық сипаттамасы осындай. Келесі қарастыратынымыз аталған қылмыс тобының субъективтік белгілері.

Қылмыстық құқықтағы қылмыстың субъектісі – бұл қоғамға қауіпті іс-әрекетті жүзеге асырған және сол үшін заңға сәйкес қылмыстық жауаптылықты атқаратын тұлға. Қылмыстық жауапты болу қабілеті субъектінің белгілі талаптарға сай келуінде, олар: есі дұрыс жеке тұлғалығы, қылмыстық жауапкершілік жасына келгендігі.

Осы қылмыстардың барлық субъектілерінің мәнді белгілері жалпы қылмыстың субъектісінің ғылыми анықтамасын құрайды. Кейбір жағдайларда осы негізгі белгілермен қатар қылмыстың субъектілері нақты қылмыстарды сипаттайтын қосымша белгілерге ие. Мұндай субъект арнайы субъект деп аталады. Заңда арнайы субъектінің ұғымы және анықтамасы берілмеген, арнайы субъект түсінігін біз қылмыстық құқық теориясында кездестіреміз. Б.А. Куриновтың пікірі бойынша: «арнайы субъект болып қылмыстық құқықтағы жалпы субъектінің белгілеріне сай келетін ғана емес, сонымен қатар қосымша өзіне тән ерекше белгілері бар тұлға танылады. Ерекше белгілер көбінесе субъектінің кәсібіне, қызметтік жағдайына, жұмысына және мамандығына қатысты болады» [90, 103 б.].

Осыған ұқсас анықтаманы өз еңбегінде Р. Орымбаев та береді [91, 2 б.].

Қылмыстың жалпы субъектісіне қатысты аталған белгілер қылмыстық құқық ғылымы мен қылмыстық заңнамадағы субъектіге ортақ танылған болып келеді және өз реттеуін Қазақстан Республикасы Қылмыстық кодексінің 14-бабында көрініс табады.

Аталған қылмыстық субъект белгілерінің ішінде субъектінің жасына тоқталып кеткен дұрыс болады. Қолданыстағы

заңнамаға сәйкес (ҚР Қылмыстық кодексінің 15-бабы) қылмыстық жауапкершілікке қылмыс жасалған уақытта жасы 16 жасқа толған тұлға тартылады. Тек кейбір жағдайда, яғни нақты тізімін негіздеп көрсеткен жағдайларда қылмыстық жауапкершілік жасы 14 деп анықталады. Ал бұл тізім ішінде компьютерлік қылмыс құрамдары кездеспейді. Сондықтан компьютерлік ақпаратқа заңсыз кіру қылмысы үшін, қауіпті бағдарламаларды жасау, пайдалану және тарату үшін қылмыстық жауапкершілікке, сонымен қатар ұялы байланыстың абоненттік құрылғысының идентификациялық кодын, абонентті идентификациялау құралын немесе құрылғысын заңсыз өзгерту және ұялы байланыстың абоненттік құрылғысының идентификациялық кодын өзгерту үшін бағдарлама жасау, пайдалану және тарату әрекеттері үшін қылмыстық жауапкершілікке тұлға тек 16 жасқа толған фактісі бойынша тартылады.

Қылмыстық кодекстің 227-бабы 2-тармағы бойынша субъект арнайы субъект болады. Бұл субъектіге компьютерлік ақпаратқа немесе құралға өзінің қызметтік бабын пайдаланып заңсыз кіру әрекетін жүзеге асырған тұлғалар жатады. Бұл қандай тұлғалар болуы мүмкін, соны анықтап алайық. Біздің ойымыз және талқылауымыз бойынша бұл адамдар санатына, әрине, жоғары қызметтік дәрежесі бар және қандайда қырымен компьютерлік құралдарға қатысы және әрекет ету не әсер ету мүмкіндігі бар тұлғалар жатады. Оларды келесідей тізіп көрсетсек:

- лауазымды тұлғалар;
- жауапты мемлекеттік қызметті атқаратын тұлғалар;
- басқарушы немесе әкімшілік тұлға;
- шенеуніктер (шартты түрде);
- мемлекеттік функцияларды жүзеге асыруға өкілетті адамдар және оларға теңестірілген тұлғалар;
- операторлар;
- серверге қол жетімді адамдар;
- бір салада қызмет жасайтын, бірақ компьютерге рұқсаты жоқ адамдар;
- компьютерлерді пайдалануға шектеулі мүмкіндіктері бар, бірақ заңмен қорғалатын әрекеттерді жасауға тыйым салынғандар, мысалы, өзіне қатысты құжаттармен жұмыс жасауға рұқсаты бар, алайда басқа құжаттарды алуға,

көшіруге, жоюға немесе орнын ауыстыруға құқығы жоқ адамдар немесе т.с.с.;
– қылмыстық әрекеттерді жасауға мүмкіндігі мол басқа да тұлғалар.

Бұл біздің топтастыруымыз, ал заңға негізделетін болсақ, нақтырақ айтсақ, Қазақстан Республикасының Мемлекеттік қызмет туралы заңнамасына сәйкес мемлекеттік функцияларды жүзеге асыруға немесе атқаруға өкілетті тұлғаларға қызметтік тұлғалар, ҚР Парламент және мәслихат депутаттары, ҚР Сот жүйесінің судьялары, барлық мемлекеттік қызметкерлер (әкімшілік және саяси) жатады. Осы тұлғалар Қылмыстық заңнама негізінде арнайы субъект ретінде танылады және ҚР Қылмыстық кодексінің арнайы субъектісі талаптарына толығымен жауап береді.

Аталған тұлғалардың мәртебесі ҚР Қылмыстық кодексінің 307-бабының «ескертуінде» анықталған.

Мемлекеттік функцияларды орындауға құзыретті тұлғаларға теңестірілгендерге жатады:
– жергілікті өзін-өзі басқару органдарына тағайындалған немесе сайланған тұлғалар;
– заңда бекітілген тәртіп бойынша ҚР Президенттігіне талапкер ретінде тіркелген азаматтар, ҚР Парламенті мен мәслихатына депутаттыққа үміткер ретінде тіркелген азаматтар, сонымен қатар жергілікті өзін-өзі басқару органдарының сайлау мүшелері;
– ҚР мемлекеттік бюджет есебінен еңбегі қаржыландырылатын жергілікті өзін-өзі басқару органдарында қызмет ететіндер, үнемі немесе уақытша негізде жұмыс істейтіндер;
– мемлекеттік ұйымдарда басқару функцияларын атқаратын тұлғалар немесе жарғы капиталының 35%-дан кем емес мөлшері мемлекет есебінен айырысатын ұйымдардың басқарма бөлімінде қызмет атқаратын тұлғалар.

Лауазымды тұлғалар деп үнемі уақытта, уақытша немесе биліктің өкілі ретінде функцияларды арнайы құзырет бойынша жүзеге асыратын немесе мемлекеттік органдарда және ҚР Қарулы күштерінде немесе басқа да әскерінде, әскери құрамдарында ұйымдастырушылық-шаруашылық не әкімшілік-шаруашылық функцияларды орындайтын мемлекеттік қызметкерлер танылады.

Осы норма тағы да ерекше тұлғаларды көрсетеді, олар жауапты мемлекеттік лауазымда отырған тұлғалар. Аталған баптың екінші ескертуіне сәйкес «жауапты мемлекеттік лауазымды» атқаратын тұлғаларға ҚР-дың Конституциясымен, конституциялық және басқа да нормативтік актілермен мемлекеттік функцияларды тікелей орындау үшін бекітілген лауазымдарды атқаратын тұлғалар жатады.

«Мемлекеттік билік өкілі» деген ұғым ҚР Қылмыстық кодексінің 15-тарауының баптарына қатысты ескертулерінде көрсетілген, оған сәйкес билік өкілі ретінде өзіне тиесілі қызметтік тәуелділікте болмайтын тұлғаларға қатысты заңда көрсетілген тәртіп негізінде басқару өкілеттіктері бар мемлекеттік органның лауазымды тұлғасы танылады. Билік өкілдеріне жатады: құқыққорғау және қадағалау органдарының лауазымды тұлғалары, ҰҚК қызметкерлері, ІІМ қызметкерлері, қаржы полициясы және прокуратура қызметкерлері және басқа да тұлғалар.

Жоғарыда аталған тұлғалардың кез келгені Қазақстан Республикасының Қылмыстық кодексі Ерекше бөлімінің 15-тарауындағы баптар бойынша қылмыс жасаған жағдайда сол норманың санкциясы бойынша қылмыстық жауаптылыққа тартылады.

Осы саладағы қылмыс құрамдарының арнайы субъектілерінің тағы бір санатына мемлекеттік функцияларды орындау үшін құзыретті тұлғаларға, жергілікті өзін-өзі басқаратын органдар мен басқа мемлекеттік органдарға жатпайтын тұлғалар жатады. Бұл топтағы адамдарға өз жұмысы ерекшелігіне байланысты ақпараттық-коммуникациялық технологиялардың пайдалану дағдылары мен білімдеріне қатысты қылмыс субъектісі болатын тұлғалар жатады. Мысалы, оларға жатады: компьютерлік серверлік немесе юзерлік класстардың операторлары, программистер, IT-мамандар, техникалық персонал, компьютерлік каталогтар мен картотекалармен жұмыс жасайтын кітапханашылар, архивариустар, кеңсе қызметкерлері, мәліметтер базаларымен жұмыс жасайтындар, компьютерге қатысы бар іс жүргізу қызметкерлері, хатшылар, компьютерлік жүйемен жұмыс істейтіндер (системщики), Интернет-кафелердің қызметкерлері және т.б.

Аталған қылмыстардың арнайы субъектісі ретінде саралану үшін тізімдегі тұлғалар қылмысты өзінің жұмыс бабын пайдаланып жасау керек.

Бұл қолданыстағы заңнамада көрсетілген компьютерлік қылмыстардың субъектісінің жалпыланған қылмыстық-құқықтық сипаттамасы. Келесі қарастыратынымыз компьютерлік қылмыстардың субъективтік жағы.

Субъективтік жақ дегеніміз – бұл кез келген қылмыстың міндетті элементі және қылмыстық іс-әрекетке дұрыс баға берудің басты және қажетті шарты болып табылады.

Егер қылмыстың объективтік жағы ол қылмыстың сыртқы көрінісі болса, қылмыстың субъективтік жағы ол қылмыстың ішкі сипаттамасы болады. Ішкі сипаттамасы дегеніміз қылмысты жасаған тұлғаның қылмысқа деген психикалық қатынасы. Қылмыстың субъективтік жағының мазмұны кінә, ниет және мақсат сияқты белгілердің сипаты арқылы анықталады.

Кінә субъективтік жақтың негізі болып табылады. Кінә дегеніміз қылмыс субъектісінің жасаған қоғамға қауіпті іс-әрекеті мен сол әрекеттен туындаған қылмыстың салдарына деген қатынасы, психикалық қарасы.

Заңдық анықтамаға сүйене қылмыстық құқық ғылымы қылмыстық іс-әрекеттің (әрекет немесе әрекетсіздік) келесідей белгілерін көрсетеді:

а) қоғамға қауіптілігі;

б) заңға қайшылық;

в) кінәлілік;

г) қылмыстық жазаланушылық.

Сөйтіп, кінәлілік (яғни кінә – қасақана немесе абайсызда) – қылмыстық құқық бойынша қылмыстың қажетті конститутивті белгісі. Субъективтік жақ пен кінәнің арақатынасы жөніндегі сұрақ бойынша екі көзқарасты көрсетуге болады. Біріншісі және неғұрлым дұрысырағы бойынша, кінә ол қылмыстың субъективтік жағы; кінә мен субъективті жақтың ұғымы мағынасы жағынан бір болып келеді. Ал екінші көзқарас бойынша, қылмыстың субъективті жағына кінәнің қасақаналық және абайсыздық түрлерімен қатар ниет, мақсат және басқа да психикалық моменттер кіреді. Кінәні субъектінің психикалық қатынасы, яғни тұлғаның жасалған қылмыстағы шынайы қасақаналығы немесе шынайы абайсыздығы ретінде және қылмыстың құрамы болып келетін субъективтік жақтың белгісі ретінде ерекшелеп көрсеткен жөн. Шынайы қасақаналық пен шынайы абайсыздық белгілі ниетке негізделе, белгілі мақсатқа жетуге бағытталған әрекет есебінен

пайда болады. Басқаша айтқанда, ниет, мақсат және эмоция кінәні толықтыратын психикалық қатынастың міндетті компоненттері болып табылады. Бұл психологиялық элементтер әртүрлі заңдық мағынаға ие. Қылмыстық зардапқа жетуді білдіретін мақсат тікелей қасақаналықтың белгісі болып табылады; ал құрамның шегінен тыс нәтижеге бағытталған мақсат қасақаналықтың бағыттылығын айқындауы мүмкін; ниет пен эмоция қасақаналықтың мазмұнын білдіреді және т.с.с. Кінәнің мазмұнына кіретіннің бәрі оның нысанына әсер ете бермейді және оның нысанының анықтамасына кіре бермейді. Сондықтан ниет пен мақсатты кінәнің мазмұнына кіргізуге қарсылық кінәнің мазмұны мен нысаны ұғымдарының араласуына негізделген.

И.Г. Филановскийдің айтуынша: «Жеке тұлғаның психологиялық құрылымы ниет, мақсат және эмоциямен шектеліп қоймайды. Оған жасалған қылмыстық әрекетті сипаттайтын басқа да психологиялық категориялар (темперамент, мінез-құлық ерекшеліктері және т.б.) кіреді. Бірақ егер осының бәрін кінәнің құрамына кіргізсек, кінә өзінің спецификасынан, яғни қылмыскердің қылығының элементтерін білдіретін тұрақты формуласынан айрылатын еді» [92, 19 б.]. Мұнда екі жағдай қызықтырады, біріншісі, іс-әрекеттің субъективтік жағын тұлғаның психологиялық құрылымымен араластыру; екіншісі, кінәні формула ретінде сипаттау.

Сөйтіп кейбір ғалымдардың айтуынша, кінә мен қылмыстың субъективтік жағының ұғымдары ұқсас ұғымдар ретінде қарастырылуы мүмкін.

Қылмыстың психологиялық мазмұнындағы субъективтік жақ (кінә) біріншіден, субъектінің қоршаған шынайылық пен жасалатын іс-әрекетке деген психикалық қатынасы, екіншіден, ол өзінің динамикасына ие уақыт шегінде басы мен аяғы бар психикалық процесс.

Психикалық қатынас жалпы басқа да қатынастар сияқты байланыс болып табылады. Бұл субъект пен объект (субъектіні қоршаған орта, шынайылық немесе оның жеке жақтары: табиғат, басқа адамдар, әлеуметтік жағдайлар, қоғам, олардың мүдделері және т.б.) арасындағы байланыс. Адам осы қатынас бойынша байланысты және сол арқылы болатын нәтижені түсіне және таңдай алады.

Әр психологиялық актке қандайда бір дәрежеде үш компонент кіреді – интеллектуалдық, еріктілік және эмоционалдық.

Тұрғылықты өмірде бұл компоненттер бір-бірімен тығыз байланыста болып, бір психикалық қатынастың әртүрлі жақтары болып табылады; оларды жеке-жеке тек теориялық анализ кезінде қарастыруға болады.

Интеллектуалдық кезең. Ойлау – заттар мен құбылыстарды олардың белгілерімен бейнелейтін және оларда, олардың арасында болатын әртүрлі байланыстарды ашатын адамның ой-санасындағы психикалық процесс. Адамның ойы оның ақыл-өрісіне сәйкес емес және ол сезіммен, қабылдаумен және есте сақтаумен бірге оның қаруы болып табылады. Ой-сана ойлаумен бірге адамның психикалық қатынасының интеллектуалдық құрамын құрайды.

Еріктілік кезең. Ерік ой-сананың практикалық жағын білдіріп, адамның практикалық қызметін қалыптастырудан тұрады. Мінез-құлықты ерікті реттеу – ол ақыл-ой мен физикалық күштерді мақсатқа жету немесе белсенділіктен бас тартуға бағыттау. Еріктілік күші арқылы адам өзінің мінез-құлқын қадағалап, өз іс-әрекеттеріне басшылық ете алады, белгілі қоғамдық нормаларға қайшы әрекеттерге барудан бас тартады, мақсатына жету үшін жолындағы кедергілерден өтеді немесе жояды.

Сонымен ерік адам санасының практикалық жағын білдіргендіктен, еріктілік қатынас тек нақты әрекет немесе әрекетсіздікте болады.

Эмоционалдық кезең. Адамның әр әрекетінің, сонымен қатар қылмыстық әрекеттің қажетті элементін білдіреді. Эмоционалдық кезең заңшығарушымен кінә нысандарының анықтамасына кіргізілмеген. Бірақ эмоция кінәнің психикалық қатынасының мазмұнына кіреді.

Эмоция:

1) кенеттен пайда болатын жағдайлардан туындайтын эмоция ретінде;

2) жүйке-психикалық тонустың өзгеруінен болатын эмоционалдық күй ретінде;

3) белгілі бір объектіге бағытталған эмоционалдық (жағымды немесе жағымсыз) қатынастардың таңдаулы түрі ретінде көрініс табады.

Осыған байланысты эмоция қылмыс жасау кезінде әртүрлі рөл атқарады. Біріншіден, эмоция қылмыс жасау кезінде ниет ре-

тінде (махаббат сезімі, жек көрушілік, қорқыныш, үрей, қатыгездік және т.б.) орын табуы мүмкін. Екіншіден, ол кінәнің интеллектуалдық және еріктілік процестеріне әсер етіп, қылмыс жасауға түрткі болуы мүмкін. Үшіншіден, эмоция қылмысқа аффект әсерінен апаруы мүмкін.

Аффект дегеніміз – (лат. affectus ішкі толқу, қобылжу деген сөзінен шыққан) қысқа уақытты күшті және толқулы жүретін эмоционалдық ішкі ағым: ашулану, ызалану, қорқу, торығу және т.б. Көбінесе жылаумен, айқаймен, анық әрекеттермен айқындалады.

Қылмыстар өздерінің психологиялық механизмдері бойынша әртүрлі және әртүрлі нұсқаларда интеллектуалдық, еріктілік және эмоционалдық бөлімдер әртүрлі рөл атқарады.

Шынайы өмірлік ситуацияларда адамда әдетте мінез-құлық әрекетінің бірнеше нұсқасы болады. Субъект осы нұсқаларды бағалайды, яғни мінез-құлықтың әлеуметтік нормаларын ескереді, өзінің қылығымен пайда болуы мүмкін әртүрлі нәтижелерді бағалайды. Осы бағалаудың негізінде іс-әрекеттің жасалуына кедергі болатын кері ниет (контрниет) пайда болуы мүмкін. Мысалы, жауаптылықтан қорқу, зардаптың болуын тілемеу және т.б. – яғни бұл жерде ниеттер арасында психикалық күрес жүреді. Осы күрестің нәтижесінде субъект белгілі әрекетті жасауға шешім қабылдайды. Шешімді қабылдау кезеңі қылмыстық қасақаналық немесе қылмыстық абайсыздықтың туу кезеңі болып табылады.

Келесі қадам әрекетті жоспарлау, яғни кезеңдерді анықтау, мақсатқа жету құралдарын таңдау, ойлағанын жүзеге асыру және шешімді орындау болып келеді.

Бұл келтірілген схематика қылмыстық әрекеттің көптеген жағдайларын көрсете алмайды; қылмыс жасаудың психологиялық механизмі жай ғана мөлшерлі немесе өте күрделі болып келе береді. Кей жағдайларда еріктілік актінің ашық этаптары кездеспеуі мүмкін, мысалы: ниеттердің күресі немесе әрекеттерді жоспарлау, адам өзін-өзі сақтап қалу үшін немесе басқа да көптеген себептерден кенеттен қылмысқа баруы мүмкін және т.б.

Бірақ қылмыс көп жағдайда адам мінез-құлқының саналы еріктілік актісін білдіреді, соған қарамастан бұл ережеден тыс ерекшелік жоқ деп айтуға болмайды. Себебі кей кезде тұлға өз мінез-құлқын ұмытшақтық немесе шашыраңқылықтық, жаңғалақтық нәтижесінен түсіне және бағалай алмайды. Қылмыс импульс арқылы жасалуы мүмкін. Егер қылмыс терең физиоло-

гиялық мастық нәтижесінен, қатты физиологиялық аффект немесе күнделікті автоматизм нәтижесінен жасалынса, ол саналы еріктілік бақылаудан айрылуы мүмкін. Бірақ саналы еріктілік бақылау қабілетінен айрылған барлық жағдайларда адамда сәйкесінше саналы еріктілік акт мүмкіндігі болады, субъектіде өз мінез-құлқын реттейтін қабілеті негізінде ерік бостандығы болады, міне сол себепті адам осы жасаған ісіне жауапты болады.

Кінә мазмұны – бұл қылмыс құрамының объективті белгілері, және де кінәлінің жазасын ауырлататын және жеңілдететін қылмыстың объективті жағдайлары. Кінә мазмұны тек қылмыстың нақты объективті белгілеріне ғана тәуелді емес, сонымен бірге заңдағы қылмыс құрамының құрылымына да тәуелді.

Нақты құрамдар бойынша кінә мазмұны кінә нысанына сілтеу арқылы; қылмыстың субъективті жағының белгілері арқылы; субъектінің психикалық қатынасын білдіретін ауырлататын және жеңілдететін қылмыстың объективті белгілері арқылы анықталады.

Кінә нысаны. Нысан – бұл мазмұнның ішкі құрылысы, олардың байланысы, оның элементтерінің қатынасы. Кінә нысаны мемлекеттің заңшығарушыларымен анықталады және құқықтық ұғым болып табылады. Кінә нысандарын анықтай отырып заңшығарушы екі психикалық элементті пайдаланады, олар: интеллектуалдық (алдын ала болжау, білу, сезіну, ойлау, ұғыну) және қылмыстың объективті жағының екі элементімен (әрекет және нәтижемен) байланысы бар еріктілік (қылмысты тілеу, қылмысқа, қылмыстық зардапқа жол беру немесе жол бермеу) кезеңдер.

Ендеше, осыдан біз кінә нысанын анықтауда кінә мазмұнына кіретін элементтердің бәрі қатыса бермейтінін байқаймыз. Бұл материалдық қылмыс құрамдары үшін қалып болып келсе, формальды, яғни нәтиже объективті жақтың элементі болмайтын, қылмыс құрамдары үшін еріктілік кезеңі тек іс-әрекетке қатысты айтылғандықтан өзгеше болады. Нәтиже кінә нысанына әсер етпейді. Қасақаналық та, абайсыздық та формальды құрамдарда қоғамға қауіпті әрекет немесе әрекетсіздікке қатысты анықталады.

Сонымен, кінә нысаны кінә мазмұнына қарағанда мағынасы жағынан терең, бірақ белгілері жағынан кедейлеу болып келді.

В.В. Люциктің айтуы бойынша, кінә нысандарын және интеллектуалдық еріктілік кезеңдерінен құралған мазмұнын төмендегі схема түрінде көрсетуге болады (2-кесте) [93]:

ҚР қылмыстық кодексінің жалпы бөлімінің баптарына сәйкес кінәнің нақты екі нысаны бар: қасақаналық және абайсыздық. Қасақана немесе абайсызда әрекет жасаған адам ғана қылмысқа кінәлі деп танылады.

Қасақана жасалған қылмыс болып тікелей немесе жанама ниетпен жасалған әрекет танылады. Егер адам өз іс-әрекетінің (әрекетсіздігінің) қоғамға қауіпті екенін ұғынып, оның қоғамдық қауіпті зардаптары болуының мүмкін екенін және болмай қоймайтынын алдын ала білсе және осы зардаптардың болуын тілесе, қылмыс тікелей ниетпен жасалған деп танылады. Егер адам өз іс-әрекетінің (әрекетсіздігінің) қоғамға қауіпті екенін ұғынып, оның қоғамдық қауіпті зардаптары болуы мүмкін екенін алдын ала білсе, осы зардаптардың болуын тілемесе де, бұған саналы түрде жол берсе, қылмыс жанама ниетпен жасалған деп танылады.

2-кесте

Кінә нысандары

Қасақана кінә		Абайсызда кінә	
Тікелей қасақаналық	Эвентуалды (жанама) қасақаналық	Қылмыстық менмендік	Қылмыстық немқұрайдылық
Зардаптың болатынын алдын ала білді, осы зардаптың болуын тіледі	Зардаптың болатынын алдын ала білді, зардаптың болуын тілемеді, бірақ саналы түрде жол берді	Зардаптың болатынын алдын ала білді, бірақ жеңілтектікпен болғызбау мүмкіндігіне сенді	Зардаптың болуын тілемеді, болжап білуге тиіс және мүмкін еді, бірақ зардаптың болатынын алдын ала болжап біле алмады

Абайсызда жасалған қылмыс болып менмендікпен немесе немқұрайдылықпен жасалған әрекет танылады. Егер адам өз іс-әрекетінің (әрекетсіздігінің) қоғамға қауіп туғызуы мүмкін екенін алдын ала білсе, бірақ бұл зардаптарды жеткілікті негіздерсіз жеңілтектікпен болғызбау мүмкіндігіне сенсе, қылмыс менмендікпен жасалған қылмыс деп танылады. Егер адам қажетті ұқыпты-

лық пен сақтық болғанда ол зардаптарды болжап білуге тиіс және болжап біле алатын бола тұра өз іс-әрекетінің (әрекетсіздігінің) қоғамдық қауіпті зардаптарының болуы мүмкін екенін болжап білмесе, қылмыс немқұрайдылықпен жасалған деп танылады.

Компьютерлік қылмыстар қасақана қылмыстар санатына жатады. Себебі компьютерлік қылмыстар абайсызда жасалады деп ҚР қылмыстық кодексінде айтылмаған. Қылмыс абайсызда жасалған деп танылады, егер ол туралы тікелей заңнамада ескерілсе (ҚР ҚК 21-бап), сол сияқты абайсыздық үшін жауапқа да тек Қылмыстық кодекстің ерекше бөлімінде нақты көрсетілген жағдайда ғана тартуға болады. Қолданыстағы заңнамадағы компьютерлік қылмыстар үшін абайсыздықта жауапқа тарту ескерілмеген.

Қылмыстық кодекстегі 205-, 213-баптардағы кінәнің мазмұндарын қарастырып көрелік. Заңмен қорғалатын компьютерлік ақпаратқа заңсыз кіру қолданыстағы заңнама бойынша тікелей қасақаналықпен де және жанама қасақаналықпен де жасала береді. Екі жағдайда да интеллектуалдық кезең бірдей, яғни қылмыскер жасайтын қылмыстық әрекеттің қоғамға қауіптілігі дәрежесі мен сипатын ұғынады және сол әрекеттен туындайтын нәтиженің туындауын және оның мөлшерін сезінеді. Тікелей қасақаналық бойынша тұлға компьютерлік қылмыстар бойынша барлық теріс әсерлердің болуын алдын ала ұғынуы, ал жанама қасақаналық бойынша осы салдардың болуын емес, мүмкін болуын ұғынуы түсіндіріледі.

Тікелей қасақаналықтың еріктілік кезеңі ҚР Қылмыстық кодексінің 205-213-баптарының негізгі тармақтарында көрсетілген қоғамға қауіпті салдардың бірінің тілегенімен шектеледі. Тілеу тұлғаның қоғамға қауіпті салдардың болуын заңсыз кіру әрекетін жасау арқылы жүзеге асыруын білдіреді. Ал жанама қасақаналық бойынша еріктілік кезеңі тұлғамен саналы түрде немесе немқұрайлы қатынасы арқылы қылмыстың салдарына жол берілуі. Осының бәрінен көретініміз компьютерлік ақпаратқа заңсыз кіру қылмысы жасалу кезінде тек тікелей қасақаналық орын табатынын байқаймыз. Нақ осы жағдай компьютерлік ақпаратты жою, тосқауылдау, өзгерту, көшіру немесе компьютер, компьютер жүйесі не олардың желілерінің жұмысын бұзу қылмыстық әрекеттеріне қатысты қолданылады. Неге десеңіз, компьютерлік қылмыстардың спецификасы бойынша, барлық компьютерлік

қылмыстар пернетақтаны басу арқылы және кейде бір пернені басу кезінде бағдарламалық қамтамасыз ету жүйесі мақұлдау терезі арқылы өз әрекетіңізді нақтылауды сұрау ақпаратын шығару арқылы жасалуымен ерекшеленеді. Ол дегеніміз қылмыскер қылмыстық әрекетті жасауды және оның салдарының тууын анық саналы ниетпен тілейді, яғни бұл тікелей қасақаналықтың тікелей белгілері болғаны. Компьютерлік қылмысты жасау үшін тұлға алдын ала қылмысқа дайын болу керек, абайсызда компьютерлік операцияларды қаншалықты пернетақтаны ретсіз бассаңыз да жүзеге асыру мүмкін емес.

Егер ҚР Қылмыстық кодексінің 210-бабы 1-тармағын, яғни «ЭЕМ үшін зиянды бағдарламаларды жасау, пайдалану және тарату» қылмыс құрамын қарастырсақ, мұндағы кінә нысаны тікелей қасақаналық болып табылады. ЭЕМ үшін зиянды бағдарламаларды (вирустарды) жасау, пайдалану және тарату кезінде тұлға өзінің әрекеті арқылы келтірілген зиян мөлшерін қоғамға өте қауіпті екенін түсіну керек, себебі қауіпті бағдарлама сөзсіз компьютерлік ақпаратқа, компьютердің жұмысына, компьютерді пайдаланушыларға, компьютерлік құралдың өзіне елеулі зиян келтіреді, оны кез келген жаңа ғасырда өмір сүріп жатқан саналы адам білуі тиіс және біледі десек артық айтылған болмас. Зиянды бағдарламаларды жасау, пайдалану және тарату формальды қылмыс құрамына жатады, себебі зиянды бағдарламаны жасау кезінде зиянды салдар болмауы да мүмкін және болуы да міндетті емес. Пайдалану және тарату кезінде де біз үлкен бір нәтижені күтпейміз, вирусты пайдалану немесе тарату фактісі формальды түрде қылмыс ретінде қабылдана береді. Қылмыстың интеллектуалдық кезеңі басты рөл атқармайды, бірінші кезекте еріктілік кезең тұрады. Вирусты жасау, тарату ұғынусыз-ақ барлық адамзатқа мәлім қатерлі қауіп, шешуші фактор бұл жерде еріктілік, яғни осы қылмыстық әрекеттерді жасау мақсатында нақты шешім қабылдау және оны саналы түрде тілеу. Бұл да тікелей қасақаналықтың белгілері.

Сол сияқты ҚР Қылмыстық кодексінің 213-бабының барлық тармақтары бойынша қылмыс құрамдары, яғни жасап шығарушының немесе заңды иесінің келісімінсіз ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын құқыққа сыйымсыз өзгерту, ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын құқыққа сыйымсыз жасау, сонымен

қатар ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын өзгертуге немесе ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын жасауға мүмкіндік беретін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату тікелей қасақаналық бойынша жасалады. Аталған қылмыстардың құрамы формальды құрам болып есептеледі.

Компьютерлік қылмыстар субъектілерінің кінәсінің мазмұны мен бағытын анықтаудан басқа, заңнама құқыққорғау органдарын әр нақты қылмыстық жағдай бойынша субъектілердің қылмысты жасауға итермелеген мақсаты мен ниетін анықтауды талап етеді. Қылмыстың мақсаты дегеніміз қылмыс субъектісінің алдына қойған жетістігі немесе қылмыс жасаудың нәтижесі. Бұл да тұлғаның психикалық жағдайын білдіреді.

Тәжірибеде компьютерлік қылмыстармен байланысты жиі кездесетін мақсат түрлері бар. Олар компьютерлік қылмыстардың ерекшелігіне байланысты типтік мақсаттар. Көп кездесетін типтік мақсаттарға жалған шоттар мен жалған төлем карталарын жасау, артық жұмыс сағаттарын жазып алу, жеңіл жолмен пайда табу, төлем құжаттарын және басқа да құжаттарды фальсификациялау, ақша-қаражат мөлшерін ұрлау, жасалған төлемдерді қайта жасау, жалған шоттарға ақша-қаражат мөлшерлерін аудару, қылмыстық пайданы заңдастыру, жалған төлеммен сатып алу, заңсыз валюталық операциялар жүргізу, заңсыз несие алу, қозғалмайтын мүлікті манипуляциялау, заңсыз жеңілдіктер мен қызметтерді алу, конфиденциалды ақпаратты сату, материалдық тауарлар мен құндылықтарды талан-таражға салу және т.б. жатады.

Аталған типтік мақсаттардан басқа жалпы кездесетін мақсаттар бар. Мысалы: кек алу, өштесу, бұзақылық мақсатта қылмыс жасау, өз біліктілігін көрсету, мақтану, ызалану, басқа қылмыстың іздерін жасыру, атақты болу және т.б. көптеген мақсатта қылмыс жасау.

Осылардың 52% ақша-қаражат мөлшерін ұрлаумен байланысты, 16% компьютерлік техника құралдарын бұзу мен жоюға байланысты, 12% алғашқы мәліметтерді ауыстырумен, 10% ақпарат пен бағдарламаларды талан-таражға салумен, 10% қызмет түрін заңсыз пайдаланумен және басқа да мақсаттармен байланысты.

Бірақ мақсаттан және кінәдан басқа қылмыстың субъективтік жағын құрайтын тағы бір белгі – ол қылмыс субъектісінің ниеті.

Ниет дегеніміз – тұлға қылмысты жасау үшін басты және үнемі түрткі болатын, қылмыстың барысында бірге жүретін және оның тоқтауына кедергі болатын, тұлғаның ішкі сезімі мен қажеттілімен шартталатын психикалық құбылыс.

Қылмыстың ниетін білмей қылмыстың шынайы себебін анықтау, қылмысты дұрыс саралау, дұрыс шараларды қолдану және қылмыспен күресу мүмкін емес.

Компьютерлік қылмыстарды жасаудың ең жиі тараған бес ниетін атап өтуге болады:

– пайдакүнемдік оймен (66%);
– саяси мақсаттар (17% мысалы: шпионаж);
– зерттеу қызығушылығы (7% негізінен жас студенттер және программистер);
– бұзақылық ниетпен (5% хакерлер);
– кек және өш алу (5%);
– тағы басқалар [94, 11 б.].

Соған қарамастан мақсат та, ниет те қылмыстың субъективтік жағының факультативті белгілері болып табылады. Компьютерлік қылмыстарды саралау кезінде олар басты рөл атқармайды, бірақ көмекші қызметін атқарады.

Сонымен компьютерлік қылмыстарға қылмыстық-құқықтық сипаттама беру кезінде біз компьютерлік қылмыстардың ұлттық заңнамадағы қазіргі жағдайын сарапқа алып, нақты ақпараттық қылмыстық әрекеттер тізімін келтіріп әрқайсысына жеке және жалпы топтық сипаттама жасадық, әр тармақ пен тармақшаларды жеке ашып көрсеттік, компьютерлік қылмыстардың объектілерін зерттеп, ерекшеліктерін көрсетіп, қылмыс объектісімен қатар жүретін қылмыстың пәні мен затын айқындадық. Компьютерлік қылмыстардың пәні мен заты ақпарат немесе мәлімет болып табылғандықтан, нақты заңмен қорғалатын мәліметтер мен ақпараттардың топтастырылуын келтірдік, ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын, ұялы байланыс абонентінің идентификациялық картасының мағыналық қолданысын ашып, оқырманға түсінікті тұрғыдан анықтап оңды және теріс жақтарын көрсеттік. Ақпараттық қылмыстардың теориялық және тәжірибелік тұрғыдан ерекшеліктерін ескере отырып объективтік жақтың барлық аспектілерін талқыладық, ақпараттық қылмыстық әрекеттердің, сондай-ақ әрекетсіздіктердің жекежеке нысандарын белгілеп, соттық және тергеу саралауларына

әсерін тигізетін немесе тигізбейтін белгілерін көрсетіп алғашқы болып ғылыми анықтамалар тізімін келтірдік. Компьютерлік бағдарлама ұғымын басқа бағдарлама түсініктерінен ерекшелігін айқындап, вирустық зиянды бағдарламалардың компьютерлік бағдарламалардан және компьютерлік вирустардан ерекшеленетінін анықтадық, вирустардың тарихы мен шығу ерекшелігін зерделедік, алғашқы аталған ұғымның айналымға жіберуін немесе пайдалануын және сол кездегі мен қазіргі таңдағы топтастырылуын жасадық. Компьютерлік қылмыстарды жасаудың субъектісін, субъективтік жағын, ниеті мен мақсатын да қарастырып өттік.

2.2. Ақпараттық құқық бұзушылықтардың криминологиялық сипаттамасы

Компьютерлік қылмыстарды жасау үшін себептер мен алғышарттар қылмыстылықтың криминологиялық сипатамасын көрсететін басты белгілер.

Аталған саладағы қылмыстармен сәтті күресу үшін теориялық тұрғыдан да, әсіресе тәжірибелік тұрғыдан да олардың жасалу себептері мен шарттарын, қоғамда өсу тенденциясын зерттеу аса маңызды.

Барлығымызға белгілі, қоғамдағы, табиғаттағы, адамзат санасындағы барлық үдерістер мен құбылыстар, оқиғалар мен жағдайлар басқа үдерістер мен құбылыстардың байланысты салдарынан туындайды.

Алайда себептерді анықтау басқа да көптеген факторларға байланысты, соның ішінде себепті байланыстың болуымен. Себеп санаты шарт санатымен тығыз байланысты, екеуі де бір ортада, бір жағдайда пайда болып ары қарай дамиды.

Қылмыстылықты жою қылмысты жасауға себеп болған шарттарды жоюдан басталады. Толыққанды профилактика кезінде көптеген қылмыстардың алды алынуы мүмкін. Сол себепті ҚР Қылмыстық-процестік кодексінде қылмыстық іс бойынша дәлелдеуге жататын жағдайларды анықтайтын, басқаларында қылмысты жасауға септігін тигізген жағдайлар аталған. Осы жағдайларды анықтау қылмыстың алдын алу үшін қажетті шарттарды қолдануға мүмкіндік береді.

Ғылымда қылмыстылықтың жалпы себептері көрсетіледі, ол себептер нақты бір әлеуметтік немесе экономикалық жағдайларда қылмыстарды тудырады. Осы жалпы себептер нақты жеке қылмыстардың себептерін тудырады.

Сол сияқты компьютерлік қылмыстардың себеп-салдары қылмыстылықтың жалпы себептерімен тығыз байланысты. Мазмұны жағынан бұл себептерді келесідей топтастыруға болады: әлеуметтік-психологиялық себептер, құқықтық себептер, саяси себептер, ұйымдастырушылық-басқарушылық себептер, экономикалық-қаржылық себептер, жеке себептер және т.б.

Қылмыстылықтың жағдайы мен дәрежесіне бірінші кезекте тоқсаныншы жылдары болған экономикалық кризис үлкен әсер етті. Инфляция жоғарылап, қоғам кедейленіп күштілер әлсіздерге қарсы қылмыс жасап өз жағдайларын көтерді не көтермек болды. Қазақстан да осы факторлардың әсерлерінен тыс қалған жоқ. Өндіріс төмендеді, жұмыссыздық өрбіді, қалған жұмысшылардың жалақысы тұрмыстық минимумның көрсеткішінен әлдеқайда төмен болды. Халықтың онсыз да әл-ауқаты төмен қоғам мүшелері бұрынғыдан да нашарлап кетті. Зейнеткерлер, инвалидтер, жастар және ауру адамдар әлеуметтік қоғамның ең әлсіз және керексіз өкілдері болып қалды.

Бірақ әлеуметтік дағдарыстар мен қылмыстылықтың өсуінде басты рөлді жаһандану атқарды. Қазіргі таңда Қазақстандағы болып жатқан экономикалық реформалар қоғамды теңсіз етіп бөлшектеп жатыр, адамдар түрлі әлеуметтік салада қарама-қайшылыққа душар болып жатыр, соның салдарынан криминалдық сипаттағы салдар туындап жатыр. Көптеген жас азаматтар мектепті бітіріп қоғамда өз орнын таба алмай жүр. Кейбіреулері жас маман болуы үшін ары қарай оқуын жалғастыратын мүмкіндік ала алмай жүр, бос жастар қалай уақытын өткізетінін білмейді, міне осының барлығы қылмыстылықтың қазіргі жағдайына үлкен әсер етеді.

Анық көрінген қоғамның әлеуметтік топтарға және таптарға бөлінуі қоғамды ыдыратып жіберді, нәтижесінде әлеумет ішінде әділсіздік пен тұрақсыздық өрбіп, кейбір субъектілер басқа қоғам мүшелерін шектеп, құқықтары мен бостандықтарын жерге таптады. Халықтың жалпы менталитеті мен әлеуметтік жағдайы ізгіліктен бас тартты. Аталған кері әсерлер қылмыстылықтың

қайнар көздері, бір тұлға өзінің толыққанды жетілмегендігін басқа тұлғаның құқықтары мен бостандықтарына және мүдделеріне нұқсан келтіру арқылы жасыруға тырысады. Виртуалды әлем осы жағымсыз әсерлерді жүзеге асыруда ең ыңғайлы құрал. Елдің кез келген тұрғыны компьютердің және Интернеттің арқасында жеңіл және жазалану қаупінсіз қылмыстық әрекетті жүзеге асырады.

Жоғарыда аталған жағдайлардың барлығы еліміздегі қылмыстылықтың басты әлеуметтік және экономикалық себептері болып табылады. Олар қылмыстылық жағдайға басқа да факторлармен байланысты қоғамдағы қарама-қайшылықтар арқылы әсер ете береді.

Қылмыстылықтың тағы да әлеуметтік-психологиялық себептері де болады. Жеке тұлғаның өмірдегі орнын табу үшін үнемі жүретін өмірлік күресі, өз-өзіне сенімсіздік, болашақтан қорқуы, өзінің әлсіздігі, шектеулі мүмкіндігі, басқаларға деген қызғаныштық сезімі, отбасылық ішкі даулар, жұмысындағы стресстік жағдай адамның психологиялық бұзылуына, алкогольдік ішімдік пен есірткі заттарды қабылдауына түрткі болып, кері әсердің нәтижесінде қылмыс немесе басқа да олқылық жасауға әкеліп соқтырады.

Мұндай референттік топтар өзінің өмір сүру кезінде өзіне тиесілі құқықтық және әдептілік жүріс-тұрыс нормаларын орнықтырып алады, олар қоғамдағы басқа тұлғаларға қалыптасқан тиесілі қылық ретінде әсер етіп, теріс, жағымсыз іс-әрекеттердің себебі ретінде қоғамдағы моральдық ахуалды бұзады [95, 16 б.].

Қылмыстылықтың саяси себептеріне еліміздегі барлық саладағы коррупцияның көрініс табуын, ұйымдасқан топтардың саясаттанып кеткенін, ішкі саяси қақтығыстардың экономикалық-қаржылық мүдделермен араласып заңсыздықтың айқын көрінуін жатқызамыз. Осының бәрі мемлекетпен жасалатын құқықтық реформаларға және жалпы қылмыстық-құқықтық саясатқа зор әсерін тигізеді.

Қылмыстылыққа мемлекеттік нормативтік актілер мен заңнамалардың жетілмегендігі де әсер етеді. Міне жиырма жылдан астам Қазақстан құқықтық жүйесін абыройлы жағдайға жеткізу үшін жетілдіру жұмыстарын жүргізіп келеді. Соның бірі-не бірнеше рет өзгертулер мен толықтырулар енгізілген қылмыс-

тық заңнама жағдайы жатады. Біздің үмітіміз бойынша, компьютерлік қылмыстылық себеп-салдары қоғамдағы өзгерістермен байланысты құқық ғылымы мен заңшығару құзырлы органдары жағынан қараусыз қалмайды. Себебі компьютеризация адамзат туындыларының ең жоғары жетістіктерінің бірі және уақыт өте келе ол бірінші қатарға шығып келеді. Өз орнында компьютерлік технологияларды пайдалану қылмыстылықтың бірден бір себебі. Ерте немесе кеш компьютерлік саладағы қылмыстар құқықтық реформалардың басты объектісі болмақ.

Компьютерлік қылмыстардың өсуіне себептер көп, себептер экономикалық, әлеуметтік, саяси және т.б. болуы мүмкін, алайда қылмыстың өсуіне бір себеп ол қылмыстылықпен күрес жүргізудің жеткілікті болмауы. Кез келген соғыста немесе қақтығыста жеңіске жету үшін тек жақсы шабуыл емес, жақсы тойтарыс беру, жақсы қорғана білу керек. Шабуылдан дұрыс қорғанбасаң, артынан соң жау жағынан келесі шабуылды күтуге болады. Сол сияқты қоғамдағы көрініс тауып жатқан компьютерлік қылмыстылыққа тойтарыс бермесе, ол қылмыстылық өзімен бірге басқа да қылмыс түрлерін алып келеді. Біз білетіндей, тәжірибеде қылмыскер сәттілікпен қылмыс жасап, ол қылмыс ашылмаса, кейін ол тағы қылмыс жасайды және тоқтамайды. Компьютерлік қылмыстардың да бір ерекшелігі олар шексіз тоқтамай істеліп жатыр. Себебі кейбір компьютерлік қылмыстылық әрекеттер заңмен шектелмеген, олар тиісті заң нормаларымен реттелмегенше, яғни компьютерлік қылмыстық іс-әрекеттер қылмыстық заңнамаға инкриминализацияланбағанша шексіз жүзеге асырыла береді.

Ғалымдар компьютерлік қылмыстылықтың пайда болуының себептері мен шарттарын түрлі етіп көрсетеді. Мысалы, В.Б. Вехов деген автордың айтуынша оның себептері мынадай:

1) Автоматтандырылған желілердің жұмыс станцияларының басқару құралдарына доступты және мәліметтерді алмастыру операцияларына қадағалауды жүзеге асыру мүмкіндігінің болмауы.

2) Қоғамдық компьютер құралдарының бақылаусыз қалуы.

3) Бағдарламалық қамтамасыз етудің төменгі дәрежеде болуы. Көп жағдайда қылмыскерлер дұрыс парольдерді табу үшін сан рет қате нұсқаларын пайдаланып көреді. Осындай деректер байқалып жатқанда уақытылы бір әсердің жетіспеуі.

4) Ақпараттық қауіпсіздік жүйелердің төменгі дәрежеде болуы.

5) Ақпараттық қауіпсіздікке жауапты болатын тұлғалардың болмауы немесе жеткілікті мөлшерде қамтамасыз етілмеуі.

6) Ақпараттық компьютерлік құралдарға, олардың желілері мен жүйелеріне рұқсаты бар тұлғалардың санаттары болмауы.

7) Қызметкерлермен ақпаратқа қатысты, жеке мәліметтерге қатысты, қызметтік және коммерциялық құпияға қатысты арнайы келісімнің болмауы [96, 114 б.].

Компьютерлік қылмыстылықтың тағы бір себебі ретінде компьютерлік қылмысты жасаған тұлғаның индивид ретіндегі нақты шарттармен қалыптасқан ерекшеліктерін жатқызуға болады. Ол ерекшеліктерді біз келесідей бөліп қарастырдық:

– жеке сипаттамалар, жеке тұлғаға қатысты психологиялық талаптар, жақсы және жеңіл өмірге деген, меркантильдік қасиеттермен сипатталатын компьютерлік қылмыстылыққа итермелейтін арамтамақтық бағыттар;
– басқа да жеке тұлғалық қасиеттер: шешім қабылдауда тұрақтылық, өзін-өзі көрсетуге талпыныс, кейде керісінше, еріктілік қасиетінің болмауы немесе жетіспеуі, қақтығыстарға жол берушілік, жасырындық қасиеттер, тәуекел сүюшілік және басқалары.

Кез келген индивидтің тұлғалық қасиеттерінің қалыптасуына, соның ішінде компьютерлік қылмыстарды жасаған тұлғалардың да, әсер ететін факторларға жатқызуға болады:

– теріс әсерлі тұрмыстық-отбасылық қатынастар (шектеулі отбасылар, балалардың тәрбиесіз өсуі, немесе керісінше балаға тым асыра көңіл аудару, балалармен қатыгез сөйлесу не айналысу, жеңіл жолмен, алдаумен, өтірік айтумен алдыға қойған жетістіктерге жетуді өз тәжірибесі арқылы көрсету және т.б.). Себебі жеке тұлғаның мінез-құлқы бала кезінен қалыптасады, ол бәрімізге белгілі;
– еңбек шарттары (жұмыс тәртібінің төмен болуы немесе жеткілікті мөлшерде қадағалау жүргізілмеуі, кей жағдайда жұмыспен қамтылу толық болмауы немесе мүлдем болмауы). Индивидумге оның референттік тобының, жұмыс ұйымының, қоршаған ортасының әсері;
– білім беру ордасындағы, мәдениеттік дәрежеде, интеллек-

тік дамуы, айналаны қабылдау қарама-қайшылықтары, жеке қызығушылық пен тұтынудың болмауы немесе шектелуі проблемалары;

– өмір сүру қалпы, достарының әсері және т.б.

Осы жоғарыда айтылғанның барлығы компьютерлік қылмыстылықтың пайда болуы және өсуін қысқаша түрде сипаттайтын мәселелер болып табылады.

Компьютерлік қылмыскердің және қылмыскерлердің жеке тұлғалық қасиеттері және ерекшеліктері. Қылмыскердің тұлғасы жөнінде мәліметтер қазіргі таңда екі арнайы ақпараттық топтардың негізінде жүргізіледі.

Бірінші топқа қылмысты жасаған белгісіз тұлғаның қалдырған іздері бойынша жасалатын және қылмыскерді іздестіру және ұстау үшін басқа қайнар көздерден алынатын сипаттамалық мәліметтер.

Екінші топқа ұсталған белгілі қылмыскерлердің жеке тұлғасын, психологиясын зерттеу арқылы алынатын ақпараттар.

Осылай бөлу қылмыскерлерді қандай да формада топтастыруға мүмкіндік береді.

Алайда, компьютерлік қылмыскерлерді немесе қысқаша айтсақ, киберқылмыскерлерді топтастырмас бұрын оларға жалпы және жан-жақты сипаттама беріп көрелік. Олардың бастамасын тарихи тұрғыдан бастап көрейік.

Ең алғаш шынайы программистер болды. Олар өздерін олай деп те, хакер деп те атамайтын, олардың нақты атауы болған емес. Шынайы программистер өткен ғасырдың 80-жылдарында пайда бола бастады. Сол жылдары Эккерт пен Мочли ENIAC-ты шығарып олардың арасында орнықты программист-энтузиастар шыға бастады. Олар компьютермен өздерінің қызығушылығы үшін ғана жұмыс жасады. Нағыз програмист болып инженерлер мен физиктер саналды. Олар қазіргі кездегі хакерлердің негізін салушы болған жай ғана кеңселерде жұмыс жасайтын, жұқа көзілдірік тағатын, есептеуіш машиналарында қазіргі кезде ескі тілдер болып саналатын ассемблер және ФОРТРАН тілдерінде бағдарламалар жазған жай ғана клерктер еді.

Хакерлер мәдениетінің бастамасын қазіргі кезге әйгілі (MIT) Массачусетс технологиялық институтының ең алғаш 1961 жылы алған компьютерімен байланыстыруға болады. Мүмкін «хакер» термині осы MIT компьютерлік мәдениеті шегінде

ойлап табылған шығар. 1969 жылы осы жерде ARPAnet желісінің пайда болуы институттың әсерін бұрынғыдан да көтерді. Осы кезден бастап 15 жылға дейін бұл машиналар хакерлердің әйгілі құралдары болып келді және бұрын бөлек-бөлек топталып жүрген хакерлерді электрондық супермагистральда біріктірді. Бұл институттарда компьютерлік ғылыммен айналысатын факультеттер ашыла бастады. Массачусетс технологиялық институты Жасанды интеллект лабораториясын дамытты. Уақыт өте келе жасанды интелектпен Стенфорд университеті, ал кейін Кернеги Меллон университеті айналыса бастады.

Уақыт өте келе MIT ITS технологиясын шығарып PDP-10, ARPAnet-тен бас тартады. ITS қолдану жағынан жеңіл, ыңғайлы және үзіліссіз жұмыс жасады. ITS-тің жобалары LISP жасанды тілінде орындалды.

Содан кейін Си тілінде жазылған ОС Unix пайда болды, кейін Xerox PARC, PDP-10, Unix, PDP-11, VAX және т.б. Осы технологиялардың барлығы сол кездегі атақты хакерлердің туындысы. Оларды атап кетсек: Деннис Ричи, Томпсон, Ричард М. Столлман (RMS) (Леви өзінің «хакерлер» атты еңбегінде Столлманды қайталанбас хакерлердің бірі деп атап өтеді), Беркли, Линус Торвальдс, Вилиям және Линн Джолицтер, Кевин Ли Поулсен, Джастин Т. Питерсон, Рональд Марк Остин, Кевин Митник және басқалары [97].

Қылмыскерлердің түрлі категорияларының типтік модельдерін анықтау, олардың ерекшеліктерін білу қылмыскерді сипаттауға және анықтауға, кейде ұстауға дұрыс әрекеттер жасауға, сезікті тұлғалар шеңберін кішірейтуге мүмкіндік береді.

Компьютерлік қылмыскерлерді келесі категорияларға бөліп көрсетуге болады:

- компьютерлік ақпаратқа заңсыз кіруді жүзеге асыратын тұлғалар;
- компьютерлік ақпаратқа заңсыз кіруді жүзеге асыратын алдын ала келісіп істеген немесе ұйымдасқан топқа кіретін тұлғалар;
- компьютерлік ақпаратқа заңсыз кіруді өзінің қызметтік бабын пайдалана жүзеге асыратын тұлғалар;
- компьютерге рұқсаты бар, бірақ ақпаратқа кіруді заңсыз жүзеге асыратын және ақпараттық құралдарды эксплуатациялау ережесін бұзатын тұлғалар;

– зиянды программаларды жасайтын, қолданатын және тарататын тұлғалар.

Шетелдік тәжірибе көрсеткендей көптеген зерттеушілер қоғамда компьютерлік қылмыстылықтың пайда болу фактісін «хакерлер» деп аталатын электрондық есептеуіш жүйелерді пайдаланушылармен тікелей байланыстырады. Хакер ағылшынның «hack» – бөлу, шабу, жұлу деген сөзінен шыққан. Хакерлер, нақтырақ айтсақ кракерлер (оның себебін төменде айтып кетеміз) мәліметтер мен олардың жиынтығын, КТҚ-на заңсыз кіру не заңсыз рұқсат алу амалдарын алуды іздеумен айналысатын және оларды теріс мақсатта заңсыз пайдалану арқылы әрекет ететін тұлғалар [98].

«Хакер» терминіне түрлі анықтамаларды келтіруге болады, әр автор анықтаманы өзінің бұл ұғымға қатысты түсінігі негізінде болжалайды. Соларға қатысты «хакер» деген ұғымды адам естігенде компьютер саласындағы қылмыскер, бұзақы, зұлым, залал келтіруші және вирустарды шығарушы деген критерийлер ойға шалады. Шын мәнінде осы әр әрекетпен (біреуі вируспен, екіншісі қылмыспен, үшіншісі ғылыммен) айналысатын тұлғалардың өзінің жеке-жеке атауы және өзінің айналысатын қызмет түрі бар. Шынайы хакерлерді осылармен шатастырған үлкен бір қателік шығар.

Хакерлердің тарихынан біз екі аспектіге келеміз. Ол тәжірибелі программистерден және желілік сиқыршылардан тұратын үлкен бір қоғам, ортақ бір мәдениет. Олардың тарихы ең алғашқы уақыт өте келе шыққан миникомпьютерлерден бастап, ең алғашқы желі арқылы өткізілген ARPAnet тәжірибелерімен тығыз байланысты. Осы мәдениеттің мүшелері «хакер» терминінің тууына мүмкіндік берді. Хакерлер операциялық жүйені, Internet желісін ойлап тапты, оның үнемі жұмыс істеуін қамтамасыз етуді қамтамасыз етті. Unix-тің қазіргі жағдайы солардың арқасы. Хакерлер көптеген біз жұмыс жасайтын операциялық жүйелерді, программаларды, техникалық қамтамасыз етілуді адамға ыңғайлы, қолайлы етіп дамытты. Қазіргі кездегі барлық саладағы жұмыстың электронды түрде жүруі, адамдардың жеке, жұмыс уақытын үнемдеуі, электронды почта, хаттардың, тіпті көлемді құжаттардың әлемнің бір нүктесінен екінші нүктесіне дереу және сол қалыпты жетуі осының бәрі бірінші кезекте хакерлердің жетістіктері. Хакерлер World Wide Web жұмысын қамтамасыз етеді.

Хакерлердің әлемге деген көзқарасы программист-хакерлердің мәдениетімен шектеле қоймайды. Хакерлердің білімі басқа да салаларда көрініс тауып жүр, мысалы, электроника немесе музыка саласында. Қазіргі кезде олардың жетістіктерін кез келген салада (ғылым салалары, басқару жүйесі, тұрмыстық жағдайда, құқыққорғау органдарында, жалпы барлық жерде) кездестіруге болады.

Хакерлердің табиғаты шын мәнінде олардың жұмыс жасайтын ортасына қатысты емес. Кейде өздерін хакерміз деп атайтын адамдар тобы болады, олар компьютерлік және телефон жүйелерін бұзумен айналысатын жас ер балалар. Шын мәнінде олар хакер емес. «Нағыз хакерлер» ондай адамдарды «кракерлер» деп атайды және олармен ешбір ортақ мүдделері жоқ екенін білдіреді. Нағыз хакерлер «кракерлерді» қараңғы, жалқау, жауапкершілігі аз және білімі таяздау адамдар деп санайды. Қорғаныс жүйесін бұзу адамды хакер қылмайды, мысалы, автомобильді ұрлау ұрыны автомастер қатарына қоспайды. Өкінішке орай көптеген журналистер мен жазушылар кракерлер туралы жазғанда қателесіп хакер атауын пайдаланады.

Хакерлер мен кракерлердің ерекшелігін бір сөзбен түсіндіретін болсақ, хакерлер құрайды, кракерлер олардың құрғанын бұзады.

Компьютерлік қылмыстар субъектілерінің тұлға ретіндегі ерекше психологиялық және тәндік сипаттамасы бар. Компьютерлік қылмыстардың субъектісі, яғни кракер – айлакер жас адам, ол компьютер алдында шамамен 12-16 сағат, кейде тіпті одан да көп уақыт жұмыс істейді, ара-арасында өзінің физикалық қажеттігі салдарынан тамақтанады, бірақ жай адамға қарағанда мөлшері екі-үш есе аз болады. Сыртқы әлпетіне, бейнесіне көп көңіл бөлмейді, өзі туралы бөтен адамдардың пікіріне қызықпайды. Киімі, жасына қарамастан, жеңіл желпі бос киім: джинсы, қатпарланып қалған жейде, көзілдірік тағуы мүмкін, шашы таралмаған, кейде өсіп кеткен, кейде сақалы өсіп кеткен болуы мүмкін. Операциялық жүйені, ассемблер тілін және перифериялық құрылғыларды өзінің бес саусағындай біледі [99].

Хакерлікті олардың өмір сүру стилі деуге болады. Хакер негізінен өзіне және өзінің компьютерлік мүмкіндіктеріне ғана сенетін адам, оның ең жақын досы – оның «машинасы». Қарапайым адам, жинаған қаражатын жаңа компьютерлік техника құралдарына

жаратады, көбінесе қоғамдық көлік құралдарымен қатынайды. Негізінен 13-35 жастағы ер адамдар. Оларда өздерінің ерекше принциптеріне негізделген биресми хакерлік кодексі бар және соны ұстанады.

Хакерлердің этикасы мына қағидалардан тұрады:

– компьютер – ол қоғамның құралы. Ол тек байларда ғана болмауы тиіс;
– ДОС-ты бұзуға болады;
– хак – өмір сүру стилі, ал өмір ол тек қана программа;
– программалау – ол өнер;
– ақпарат барлығына тиесілі. Хакерлердің көбісі университеттен аяқ басты. Университеттің мақсаты білімді жасап, оны жасырмай көпшілікке тарату. Хакерлер бұл принципті студент болуына, болмауына қарамастан ұстанады;
– идеалды операциялық жүйе болмайды;
– бұзуға келмейтін программа мен қорғаныс жүйесі жоқ;
– программалық код көпшіліктің құндылығы. Жақсы кодпен барлығы пайдалану керек, жаман код түзетілуге тиіс. Программаларға авторлық құқықпен қорғалуға қажеті жоқ және көшіруге тыйым салынбауға тиіс;
– басқа пайдаланушыларға зиян келтіру хакерлікке жатпайды. Хакерлер басқа пайдаланушылар мен бөтен адамдарға зиян келтіруді, заңсыз әрекеттерді жасауды көздемейді.

Хакерлерді олардың түрлі мақсаттары мен қызметтеріне байланысты бірнеше топқа бөліп көрсетуге болады. Біреулері түрлі ұсақ құжатталмаған жүйелік бағдарламаларды шығарумен айналысады. Әдетте оларды жасау біреудің бағдарламаларын «жұлу» арқылы істеледі. Олардың қызметінің мақсаты барлығын (операциялық жүйенің, ойынның, вирустың, антивирустың, программалау тілінің және т.б. программасын) жасай алатын суперпрограмма ойлап табу.

Басқа топтағы хакерлердің мақсаты қандайда бір жүйеге кіріп, ол жүйенің қорғаныс бөлімін өшіру және өзіне қажетті ақпараттарды алу, операцияларды жүзеге асыру болып табылады.

Үшінші топқа кейде «ақпараттық серуендеушілер» деп аталатын пайдаланушылар жатады, мақсаты бөтен компьютерлер мен желілерге кіру.

Соңғы төртінші топқа зиянды бағдарламаларды, яғни троялық аттар мен компьютерлік вирустарды жасайтындар жатады. Бұл топтағыларды хакерлерге жатқызуға болмайды, себебі жоғарыда айтып кеткендей шынайы хакерлер пайдаланушыларға зиян келтіретін әрекеттермен айналыспайды және вирус тарату олардың кодексіне қайшы келеді.

Қазіргі таңда хакерлер аумақтар бойынша, өздерінің ортақ көзқарастары бойынша, басқа да белгілер мен жағдайлар бойынша топтар, одақтар құрып жүр, өздерінің электрондық бұқаралық ақпарат құралдарын шығарумен айналысып жүр (газеттер, журналдар, жедел хабарламалары бар электрондық тақталар, вебсайттар, электронды конференциялар, бастауыш хакерлерді үйрететін оқу құралдар, әдіснамалар, өздерінің жаргондық сөздіктері, компьютерлік бюллетеньдер, буклеттер және т.б.). Хакерлер бірбірімен тығыз байланыс ұстайды және тәжірибелерімен глобалды телекоммуникациялық арналар арқылы алмасып отырады.

Хакерлер өзінің саласын «А»-дан «Я»-ға дейін жетік білуі тиіс. Соның ішінде олар мына бағдарламаларды (программаларды) міндетті түрде білуі тиіс: Sourcer, Qaid Analyzer, Turbo Debugger және т.б. Хакерлер білуі тиіс тілдер мен құжаттар: Assembler, Паскаль, Сюшечка, Interrupt list by Ralf, Tech Help және т.б. Онша ұната бермейтін программалары: Clipper x.xx, Байсик, Lexicon x.xx, Windows.

Компьютерлік вирустарға қатысты жазған еңбегінде Н.Н. Безруков хакерлер туралы былай дейді: «...операциялық жүйені, ассемблер тілін, перифериялық құрылғының жұмысының ерекшеліктерін жетік біледі» [100, толығырақ қараңыз].

Н.Н. Безруковтің еңбегін ары қарай қарайтын болсақ былай делінген: «...Машинамен үнемі жұмыс жасау мұндай адамдардың тілі мен ойлау әдісінде із қалдырады. Жай тұрмыста кейбір программистік терминдердің қолдануы байқалады: «завис», «вычислить» т.б. Оларға басқа адамдар программа ретінде, ал қоршаған орта әлемдік гиперкомпьютерге арналған операциялық жүйе ретінде танылатын сияқты көрінеді».

Сонымен, хакер – ол компьютерлік жүйелердің қалай жұмыс істейтінін білу үшін оларды тінтитін адам. Бұл термин өзінің нақты ұғымын баспада дұрыс қолданбаудың әсерінен жоғалтқан, сол себепті оларды бұрынғы атауы бойынша «программист» деген қазір орынды. Программист ол тех-

никамен және оның функциялары негізінде жатқан принциптермен қызыға айналысатын, басқа хакерлер тапқанды табуға ұмтылатын, ізденетін адам.

Азартты ойыншыға ойын – ол өмір. Ойын ұтыстан маңыздырақ. Сол сияқты программиске дисплей алдында отыру шынайы өмір, ал басқасының бәрі күнделікті міндет.

Компьютерлік қылмыстық құқықбұзушылықтардың субъектілерін жіктеу (топтастыру). Жоғарыда компьютерлік қылмыстардың субъектісіне қатысты көптеген мәлімет айтылып кетті, оларды объектілерге байланысты, заңда көрсетілгені бойынша, криминологиялық сипаттамасы бойынша, әдебиеттер бойынша, мақсатына және қызметіне қарай топтарға бөліп көрсеттік. Енді оларды жеке жағдайларға байланысты, сонымен қоса ерекшеліктеріне байланысты топтарға бөліп көрсетуге болады.

1. Компьютерлік қылмыскерлердің бірінші тобына компьютерлік техника мен программалау саласындағы кәсіптік деңгейі айқын көрінетін өзінше фанатизм және тапқырлық элементтері байқалатын тұлғаларды жатқызуға болады. Бұл топтағы қылмыскерлердің ерекшелігі оларда айқын көрініс тапқан заңға қайшы ниетінің болмауы. Барынша барлық олармен істелген әрекеттер өздерінің зияткерлік және кәсіби мүмкіндіктерін тексеру және жоғарылату мақсатында жасалады. Олар білімге құмар, ерекше интеллектке ие. Соған қарамастан шамалы азарттық, құштарлық байқалады. Жоғары дәрежелі компьютерлік жүйелердің қауіпсіздік шаралары психологиялық тұрғыдан олардың мүмкіндіктерін сынайтын бір барьер ретінде қабылданады.

Бұл категориядағы тұлғалардың қылмыс жасау ерекшеліктерінің қатарына мыналарды жатқызуға болады:

- қылмысқа деген ойластырылған, мақсатқа не болса да жетемін деген дайындықтың болмауы;
- қылмысты жасау тәсілінің өзгешелігі;
- қылмыстың құралы ретінде тұрмыстық техникалық заттар мен құралдарды қолдану;
- қылмысты жасыру шараларын қолданбау;
- оқиға болған жерде бұзақылық әрекеттер жасау.

2. Келесі топтағы қылмыскерлерге психикалық аурудың жаңа түрімен (ақпараттық аурулар немесе компьютерлік фобиялар) ауратын адамдарды жатқызамыз.

Бұл топтағы адамдардың ауруымен қазіргі кезде шет елде медицинаның жас және жаңа саласы ақпараттық медицина айналысып жүр.

Денсаулық сақтаудың әлемдік ұйымы (Всемирная организация здравоохранения) айтқандай, персоналды компьютермен жиі жұмыс істеу адамның денсаулығы үшін жағымсыз, теріс нәтиже алып келеді және ол объективті шындық және анық болып табылады.

Компьютерлік қылмыстар аталған науқас түрімен ауыратын тұлғалармен жасалуы мүмкін. Тергеу және қылмысты ашу процесі кезінде мұндай фактілер орын тапса, компьютерлік қылмысты жасау кезіндегі қылмыскердің есі дұрыстығын анықтау үшін міндетті түрде арнайы сот психиатриялық сараптама тағайындау керек. Бұл өз кезегінде қылмыскердің іс-әрекетін саралау үшін әсерін тигізеді (қылмыс аффект жағдайында жасалды ма не психикалық аурумен ауыратын тұлғамен жасалды ма).

Бұл топтағы қылмыскерлермен жасалатын компьютерлік қылмыстар негізінен өзінің іс-әрекеттерін жартылай немесе толығымен қадағалай алмай, компьютерлік техника құралдарын қылмыстық ниетсіз физикалық жою немесе бүлдірумен байланысты деген қорытындыға келуге болады.

3. Үшінші топты кәсіби компьютерлік қылмыскерлер құрайды. Олардың мақсаты мен ниеті айқын танылған пайдакүнемдік, пайдақорлық, арамдық, зұлымдық. Олар компьютерлік қылмыстарды жасаудың көп мәрте қайталануымен, оларды міндетті түрде жасыру әрекеттерімен және осы саладағы тұрақты қылмыстық тәжірибелігімен сипатталады.

Бұл топтың қылмыскерлері әдетте жақсы ұйымдасқан, жоғары дәрежелі құрылғылармен және арнайы техникамен мобильді және техникалық қамтылған қылмыстық топтардың, одақтардың, ұйымдардың және бірлестіктердің мүшесі болып табылады. Бұл жоғары техникалық арнайы білімі бар жоғары білікті мамандар. Дәл осы топ қоғамға басты қауіпті тудырады, компьютерлік қылмыстылықтың сапалы және санды жағынан кадрлік ұясы болып табылады.

Қылмыскерлердің бұл топтарға саралануы олардың ниеті мен мақсатына тікелей байланысты. Сол себепті кез келген қылмыстың ниеті мен мақсаты анықталуы тиіс. Бұл сотпен тиісті жазаны

тағайындау үшін ғана емес, жалпы қылмыстың ашылуына маңызды болып келеді.

Компьютерлік қылмысты жасаудың алуан түрлі ниеттері болуы мүмкін, соның ішіндегі ең маңыздыларын атап кетейік:

1) пайдақорлық ниет (көбінесе үшінші топтағы қылмыскерлерде байқалады);

2) саяси мақсаттарда (мысалы, шпионаж: үшінші топтағы қылмыскерлерде байқалады);

3) зерттеушілік қызығушылық (студенттер және бірінші топтағы кәсіби программистер);

4) бұзақылық және ойын негізінде (бірінші топтағы тұлғалар, хакерлер);

5) кек алу мақсатында (бірінші және екінші топтағы қылмыскерлер).

Жиі кездесетін қылмыс мақсаттары ол: жалған шоттарды және төлем ведомостарын жасау; жұмыс уақыттарын жазып алу; төлем құжаттарын жасау; ақша-қаражат соммаларын ұрлау; ақша соммаларын жалған шоттарға лақтыру; қылмыстық кірістерді заңдастыру; жалған төлемдер арқылы заттар сатып алу; заңсыз төлем операцияларын жүргізу; заңсыз несие алу; қозғалмайтын мүлікті манипуляциялау; заңсыз қызметтер мен льготалар (жеңілдіктер) алу; конфиденциалды ақпаратты сату; материалдық құндылықтар мен тауарларды талан-таражға салу және т.с.с.

Соған қарамастан қылмыстардың жартысынан астамы ақша соммаларын ұрлаумен байланысты, содан кейін компьютерлік техника құралдарын бұзумен және жоюмен байланысты, кейін мәліметтерді ауыстыру және ақпараттар мен бағдарламаларды ұрлыққа салумен байланысты.

Осы қылмыскерлерді көбісі хакерлерге жатқызады. Шын мәнінде хакерлер олар қылмыскерлер, бірақ ең қауіпсіздері. Ал кейде олардан қылмыспен қатар пайда да тиеді. Кейбір хакерлер қорғаныс жүйесін бұзғаннан кейін, қорғаныс жүйесін жетілдіру немесе жақсарту жөнінде кеңестерін қалдырып кетеді. Хакерлер бөтен операциялық жүйеге кіру арқылы қылмыс жасайды, бірақ ешбір пайдакүнемдік мақсатқа ие болмайды. Ең қауіптілері хакерлерге жатпайтындары, олар төмендегілер.

Кракерлер – бұзушылар, операциялық жүйелерді, лицензияланған бағдарламаларды пайда табу мақсатында, желіде-

гі барлық объектілерді ақшасын үнемдеу үшін немесе тегін пайдалану үшін бұзатын тұлғалар.

Дефейсерлер – бұзақы хакерлер. Интернет сайттары мен коммерциялық серверлерге шабуыл жасайтындар. Тәжірибеде ең жиі кездесетін хакерлер түрі. Дефейсерлердің кейбір түрлері сайтты бұзудан материалдық пайданы, ақша мәселесін көздемейді, оларға ең басты істеген қылықтарының моральдық жағы мен абыройы, өзін-өзі көрсету болып табылады. Олар сайттарды дефейстеуді, өздерінің түсінігі бойынша, жаман адамдарға қарсы жасайды. Мысалы: экстремистік ұйымдардың серверлерін бұзып қою, заңсыз порно порталдарды жою және т.б.

Кейлогерлер – аңдығанды жақсы көретін тыңшылар (шпиондар). Желі арқылы адамдарды, олардың жүріс-тұрысын бақылау. Пайдаланушының енгізген парольдері жайлы мәліметтер шығаратын бағдарламаларды, сонымен қоса, коммерциялық құпияны, пайдаланушының жеке өмірі жайлы жасырын мәліметті ашуға көмектесетін троялық программаларды пайдаланушылар.

Кардерлер – несие карталарына, банктерге және ақшаға деген құштарлық басқаратын тұлғалар. Бұлардың мақсаты желі арқылы қалай да болса да өзінің материалдық жағдайын жақсарту, тікелей айтқанда, баю. Өздерінің іс-әрекеттері біреуге ұнай ма, біреуге зиян тигізеді ме, оларды көп мазаламайды.

Вирмейкерлер – вирус программаларын (бағдарламаларын) жазушылар. Олардың мақсаты вирустарды шығару арқылы пайда табу, жақсы вирусты сатуға немесе іске жіберуге болады. Кейде олардың мақсаты вирусты жасап шығарып, оны таратып бұзушылық нәтижелерін салтанаттау болып табылады.

Кодерлер – ол өте ақылды адамдар. Олардың қызмет саласы ақпаратты қорғау. Басқа хакерлер оларды ақылдың атасына теңейді. Қысқаша айтқанда кодерлер кодтарды, парольдерді не бұзумен, не жасаумен айналысады.

Компьютерлік қылмыскерлерді сипаттауда ерекше талдау және зерттеу жұмысын жасаған ресейлік ғалымдар Д.А. Вечерский және И.И. Шалькевич топтастыруды кесте түрінде көрсетеді [101, 13 б.].

Жалпы айтатын болсақ, компьютерлік қылмыскерлердің жасы шамамен 15 пен 45 арасында болады. Бірақ кейбір зерттеулер бойынша жалпы қысмыскерлердің 33% – 20 жасқа де-

йінгілер, 54% – 20 мен 40 жас аралығындағылар, 13% – 40-тан асқандар. Осыдан көретініміз компьютерлік қылмыстарды көбінесе ортажастағылар жасайды.

Келесі қарастыратынымыз компьютерлік қылмыстарды жасау әдіс-тәсілдері мен амалдары.

Компьютерлік техника құралдарын пайдалана жасалған нақты қылмыстар бойынша анализ және арнайы әдебиеттерді зерттеу негізінде компьютерлік қылмыстарды жасаудың жиырма басты тәсілдерін және қырыққа жуық түрлерін белгілеп көрсетуге болады. Бұл сандар қылмыскерлермен жаңа математикалық, информатикалық және физикалық әдістерді қолдануға байланысты, жаңа технологиялардың қарқынды дамуына байланысты шексіз өсе беруі мүмкін.

Ал жалпы компьютерлік қылмыстарды жасаудың барлық тәсілдерін 5 негізгі топқа бөліп көрсетуге болады. Соған қарамастан негізгі топтастырушы белгі болып әртүрлі мақсатпен компьютерлік техника құралдарына рұқсат алуға бағытталған осы не басқа да әрекеттерді қылмыскермен пайдалану әдісі табылады. Осы белгіге сүйене, Ю.М. Батурин келесідей жалпы топтарды бөліп көрсетеді [102]:

1) компьютерлік техника құралдарын (КТҚ) алу;

2) ақпаратты бұрып алу;

3) КТҚ-ға заңсыз рұқсат алу;

4) мәліметтермен және басқарушы командалармен манипуляция жасау;

5) кешенді әдістер.

Қылмысты жасау әдіс-тәсілдері ретінде ғылыми-тәжірибелік тұрғыдан субъектінің объективті және субъективті шартталған қылмысқа дейінгі, қылмыс кезіндегі және қылмыстан кейінгі мінез-құлық жүйесі, тергеу кезінде болған оқиға жөнінде түсінік беретін түрлі сипаттағы іздерді қалдыру, қылмыскердің жеке тұлғалық қасиеттерін беретін амалдар танылады.

Басқаша айтқанда қылмысты жасаудың әдісі қылмыстың ерекше моделін ақпараттық сипатта көрсететін қылмыскердің қылмысқа дайындалуы, оны жасауы және жасыруы бойынша арнайы іс-әрекеттерінің жиынтығы.

Қылмысты жасаудың әдісі әрқашан да қажетті факторлар санының жиынтық әрекеттерінің нәтижесі болып табылады. Және қаншалықты олар іс-әрекеттер арқылы көрініс тапса, соншалық-

ты қылмыскер қылмыс іздерін қалдырып кетеді, соншалықты тергеуші тергеу және іздестіру версияларын ұсынатын ақпаратқа ие болады.

Қарастырып отырған мәселе бойынша аса құнды болып қылмыскер мына жағдайлар бойынша жүзеге асырған іздер табылады: қалай қылмыскер қылмыс орнына келді, қалай кетті, түрлі кедергілерді өтті, өзінің қызметтік жағдайын пайдаланды, қылмыстық мақсатқа қалай жетті, білімі, тәжірибесі қандай, қандай физикалық күшті қолданды, іс-әрекетті жасаудың іздерін жасырды ма, жасырмады ма. Маңызды іздердің біріне қылмыскер мен қол сұғылып отырған объект арасындағы байланыс іздері жатады.

Қылмыстық-құқықтық сипаттама бойынша қылмысты жасаудың әдісі жалпы түрде көрсетілген, мысалы, ашық немесе жасырын ұрлау әдісі, ғимаратқа кіру әдісі және т.б.

Ал криминалистік тұрғыдан қылмысты жасаудың әдісі әрқашанда нақты және онда тергеу-оперативтік маңыздылыққа ие ерекшеліктері бар қырлары көп. Олардың ішінен мыналарды атап өтуге болады: бұл тәсілдің көп тарағандығы, оларды қолданудың нақты әдістері, қолдану кезіндегі техникалық және басқа да құралдар, олардың конструктивтік ерекшеліктері, қылмысты жасау мен оған дайындалу кезінде әдістерді пайдалану, және қылмыс қалай дайындалды, дайындықтар қалай өтті, қайда және қалай қажетті қылмыс құралдары мен басқа техникалық құралдарды жасады және дайындап келтірді, олардың алынған жерлері, қайнар көздері және т.с.с.

Қазіргі таңда отандық және шетелдік ғылымда компьютерлік қылмыстылықтың жасалу әдістерінің сипаттамасына қатысты, оның нақты атауларының және классификациясының қандай да анықтамалары немесе ұғымдары қалыптаса қойған жоқ.

Бұл мәселе ғылым үшін соншалықты жаңа және қазір тек теориялық даму мезетінде жүріп жатқан мәселе. Әсіресе ол біздің криминалистік ғылымға қатысты айтылған, себебі біздің ғылым бұл мәселемен тек тоқсаныншы жылдардың соңы мен екімыңыншы жылдардан кейін ғана айналыса бастады. Ал батыстық елдерде бұл мәселеге көңіл жетпісінші жылдардың соңынан бастап бөліне бастады.

Бірақ соңғы жылдарда Республикамыздың, бұрынғы ТМД елдері, әсіресе, Ресей Федерациясының заң әдебиеттерінде, ғы-

лымда және оқу жүйесінде бұл мәселе қарқынды түрде зерттеліп дамып келеді. Соның ішінде компьютерлік қылмыстардың жасалу әдіс-тәсілдерінің ерекшелігі, топталуы (классификация) және атаулары түрлі көзқарастардан байқалып жатыр.

Ақпаратқа заңсыз кіру мен заңсыз алудың біраз әдіс-тәсілдерін атап көрейік:

- жасырын тыңдайтын құрылғылар;
- арақашықтықта суретке түсіру;
- электрондық сәулелерді алу;
- мистификация (жүйелерді запрос «сұрау» ретінде жасыру);
- акустикалық сәулеленулерді бұрып алу және принтер мәтінін жаңарту;
- ақпаратты тасымалдауыштарды және өндірістік шығындарды (мусорды жинау) талан-таражға салу;
- басқа пайдаланушылардың массивтерінен мәліметтерді санау және оқу;
- қорғаныс шараларын өтіп ақпараттық тасымалдауыштарды көшіру;
- тіркелген пайдаланушы ретінде көрсету;
- программалық қапқандарды қолдану;
- аппаратураларға және байланыс линияларына заңсыз қосылу;
- қорғаныс механизмдерін істен шығару;
- және тағы да басқа амал-тәсілдер.

Отандық ғылымда статистикалық мәліметтерге сүйене жасалған анализдің болмауы шетелдік арнайы әдебиеттер мен ғылыми жұмыстарды қарауға тура келеді. Солардың негізінде 20-дан астам компьютерлік қылмыстарды жасаудың басты тәсілдерін белгілеуге және 40-тан астам олардың түрлерін атап өтуге болады. Бұл көрсеткіштер қылмыскерлермен қылмысты жасаудың түрлі комбинациясы мен алгоритмдердің логикалық модификациясын қолдануына байланысты өсіп отырады.

Осы аталғандардың негізінде, жоғарыда айтылып кеткендей, компьютерлік қылмыстарды жасаудың 5 негізгі тобын бөліп көрсетуге болады. Осы белгілер негізінде Ю.М. Батурин келесі жалпы топтарды атап кетеді:

1) компьютерлік техника құралдарын алу;
2) ақпараттарды бұрып алу;
3) компьютерлік техника құралдарына заңсыз кіру;

4) мәліметтер мен басқарушы командалармен манипуляция жасау;

5) кешенді тәсілдер [103].

Енді әрқайсысына жеке-жеке тоқталып кетейік.

Бірінші топқа, дәстүрлі тәсілмен қылмысты жасау түрі жатады. Бұл жерде қылмыскердің әрекеті бөтен мүлікті алуға бағытталады. Бөтен мүлік ретінде бұл жерде компьютерлік техника құралдары саналады.

Қылмыстық-құқықтық көзқарастан мұндай қылмыстар Қылмыстық кодекстің тиісті баптары бойынша сараланады, мысалы, ұрлық, тонау, қарақшылық, шпионаж және т.б. Бұл топтағы қылмыс құрамдарының ерекшелігі, оларда компьютерлік техника құралдары тек қылмыстық қол сұғушылықтың заты ретінде танылады, ал қылмысты жасаудың құралы ретінде басқа да құрал-жабдықтар, техникалық құрылғылар және т.б. жатады.

Бұл қатарға тағы да ақпаратты физикалық түрде тасымалдайтын заттарды, яғни магниттік ленталарды, дисктерді, дискеталарды және флэш тасымалдауыштарды, электрондық кредиттік карталарды, магниттік және магниттік оптикалық және оптикалық дисктерді, электрондық акциялар мен қызметтерді жатқызуға болады.

Бұл қылмысты жасаудың тәсілдері жеткілікті түрде криминалистік ғылыммен зерттелген, сол себепті оларды жеке-жеке қарастырудың қажеті шамалы. Нақтырақ амал-тәсілдердің басқа топтарын ғылыммен зерттелмеген бөлігін қарастырайық.

Компьютерлік қылмыстарды жасаудың екінші тобындағы тәсілдеріне қылмыскердің аудиовизуалдық және электромагниттік бұрып алу әдістерін қолдану арқылы мәліметтерді және машиналық ақпараттарды тікелей пайдалану арқылы жүзеге асыратын іс-әрекеттері жатады. Бұл әдістер көбінесе құқыққорғау органдарының жедел-іздестіру қызметімен жиі қолданылады.

Осы және кейінгі топтардағы компьютерлік қылмыстарды жасаудың әдістерінде компьютерлік техника құрал жабдықтары қылмыстық қолсұғушылықтың заты немесе пәні ретінде де, және қолсұғушылықтың қаруы немесе құралы ретінде де танылабереді.

Тікелей (белсенді) бұрып алу. Компьютердің телекоммуникациялық құрылғысына, компьютер желісі мен жүйесіне тіке-

лей қосылу немесе персоналды компьютердің тікелей сәйкес порты арқылы жүзеге асырылады. Соған байланысты бұрып алудың жылдамдатылған (форсированный) түрі, символдарды бұрып алу және хаттарды бұрып алу деген түрлері бар.

Қосылулар арнайы тұрмыстық құралдар мен құрылғылар арқылы жүзеге асырылады: телефон, сым кескіні, телефон кабелі, компьютерлік полиөткізгіш шлейфы, қысқыштар, арнайы ине тәрізді өлшегіш щуптар, радиожөндеуіш инструменттер жиыны, принтер, модем, WiFi, Bluetooth, DVD, CD дисктер, флэшкалар, «Laptop» компьютерлері, смартфондар, электронды блокноттар, USB сымдары немесе порттары, үлкен өлшемді сыртқы жадылар және т.б. жаңа жоғары технологиялар туындылары.

Электромагнитті (бәсеңді) бұрып алу. Бұрып алу құрылғысы әрдайым жүйеге қосылу арқылы жүзеге асырыла бермейді. Ақпараттар мен мәліметтер байланыс арнасында ғана емес, ешбір тікелей желісіз, кабельсіз белгілі құрылыс ішінде немесе аумақ ішінде және алыс аралық ішінде де заңсыз бұрып алу объектісі болуы мүмкін.

Сөйтіп, тікелей байланыссыз физикалық тасымалдауышқа компьютерлік техника құралдары (сонымен бірге коммуникация құралдары) функциясын жүзеге асыру кезінде туғызатын электромагниттік сәулелерді көшіруге, алуға және бекітуге болады. Себебі, сөзсіз, кез келген электрондық құрылғы электромагниттік толқындар мен сәулелер шығарады, нәтижесінде түрлі электронды қабылдау құрылғыларында қажетсіз кедергілер болып жатады, әсіресе бір құрылғыға басқа құрылғы жалғанып не қосылып жатса. Осы кедергілер арқылы біз жақын арада басқа құрылғы жұмыс істеп жатқанын немесе біздің құрылғыға заңсыз жалғанып, жасырын кіріп жатқанын байқаймыз. Бұл кедергілер жағымсыз дыбыс шығару, бейненің бұзылуы, сапаның төмендеуі, қосалқы дауыстар мен дыбыстардың пайда болуы, күнделікті кездеспейтін іс-әрекеттердің байқалуы және т.б. белгілерімен сипатталады және көрініс табады.

Электронды-сәулелі құрылғы қоршаған кеңістікке белгілі мәліметі, ақпараты бар (электронды смог) электромагнитті толқындарды таратады. Бұл құрылғы арқылы шығатын толқындар шамамен телевизиялық көрсетілімдегідей түрлі физикалық кедергілерден өтіп біраз әлсіз коэффициентпен, мысалы, үй

қабырғасы мен терезенің әйнегі арқылы өтеді. Ал көптеген эксперименттер көрсеткендей, оларды 1000 метрге дейінгі қашықтықта қабылдауға болады. Бұл сигналдар тиісті аппаратурамен қабылданғаннан кейін басқа (қылмыскердің компьютеріне) компьютерге жіберіледі. Қылмыскер компьютерінің мониторында жәбірленушінің компьютеріндегі бейне мәлімет пайда болады, ол үшін электротолқынды оның тиісті арнасының жиілігіне келтіріп қойғаны жеткілікті. Әр компьютерді оның жеке параметрлері бойынша идентификациялауға болады: жұмыс жиілігі, электромагниттік сәулелену интенсивтілігі және тағы басқа параметрлері.

Ең алғаш ақпаратты компьютер дисплейінен дистанциялық түрде арақашықтықта бұрып алу 1985 жылы Канныда ЭЕМ-ның қауіпсіздік мәселелері бойынша өткен халықаралық конгрессінде демонстрацияланған болатын. Онда голландиялық телекоммуникациялық PTT компаниясының қызметкері Вим Ван Эк конгресске қатысушыларды өзінің дайындаған құрылғысымен таң қалдырды. Ол сол ғимараттың 8-қабатында орналасқан персоналды компьютер дисплейінің экранындағы мәліметті компьютерден 100 метр қашықтықта орналасқан көшеде тұрған өзінің автомобилінде отырып құрылғысы арқылы түсіріп алады [104, 2-тарау].

Компьютерлік қылмысты аталған тәсілмен жасау кезінде қылмыскерлер жедел-іздестіру қызметінің әдістері мен амал-тәсілдерін, арнайы техникаларын, мысалы, сканерлік құрылғыны қолданады.

Аудиобұрыпалу немесе ақпаратты виброакустикалық ағым бойынша жазу. Бұл тәсіл ең қауіпті және көп тараған тәсілдердің бірі. Бұл арна бойынша қорғанысты қамтамасыз ету қиынға таяу.

Бұл ақпаратты шешу тәсілі екі түрге бөлінеді: кіру арқылы және кірмей.

Біріншісі, яғни кіру бойынша, ақпаратты өңдеу құралдарына, телефон аппаратураларына телекабельдерге, күзет өрт сигнализацияларына, коммуникациялық линияларға, тұрмыстық заттарға жасырын тыңдау құрылғысын орнату (тыңдау құралдары: «таблеткалар», «жучоктар», «клоптар» т.б.) арқылы жүзеге асырылады.

«Клопты» немесе басқа да аппаратураны объектіге орнату үш негізгі тәсілмен жасалады.

Біріншісі бойынша ғимаратқа жасырын немесе құпиялы түрде кіру керек; екіншісі бойынша радиотаратқыш және дыбыс жазғыш аппаратура ремонттау немесе ғимаратты салу кезінде орнатылады; үшіншісі бойынша жәбірленуші жақ өзі иеленеді де алған затына орнатып қояды.

Арнайы техникаға мысал ретінде мыналарды көрсетуге болады:

- дистанциондық басқарылуы мүмкін арнайы микрофондар;
- ұзақ жазатын диктофондар;
- шулы кедергілермен шығатын сөйлеу сигналдарын өңдеп шығаратын сандық бейіндік фильтрлер АФ-512, DAC-256 және DAC-1024.

Ақпаратты жазып алатын аппаратураны тауып алу өте қиын, себебі олар белгілі бір тұрмыстық немесе кеңселік заттар ретінде жасырынып тұрады. Мысалы: компьютерлік қарапайым микросхема, темекі тұтандырғыш, қалам, пульт, қарындаш, шеге, түйрегіш және басқалары.

Екіншісі, кірмей – ең қауіптісі. Оның ерекшелігі мынада. Ақпаратты шешудің акустикалық және вибрациялық датчиктері күзетулі тұрған ғимараттан тыс жерде тұрған инженерлік-техникалық құрылымдарға орнатылып бағытталған объектіден сөйлеу сигналдарын қабылдайды.

Инженерлік-техникалық құрылыстардың келесідей типтік құрылымдары болады: ғимараттың қабырғалары, тосқауылдар, жабындылар, терезелер, терезе рамалары, есіктер мен есік қабырғалары, вентиляциялық ауаөткізгіштер, суқұбырлары. Соған қарамастан ғимаратқа кірудің қажеті шамалы, оған сыртынан жақындағаны жеткілікті. Датчик не тікелей, не дистанциялы түрде орнатылады. Дистанциялы түрде ақпаратты шешу үшін терезе, есік және сол сияқтылардан түрлі ату құралдары қолданылады.

Видеобұрыпалу. Қылмысты жасаудың бұл тәсілі ақпаратты түрлі видеооптикалық техниканы қолдану арқылы алуға бағытталған қылмыскердің әрекеттеріне негізделеді. Бұл тәсілдің де өзіне тән екі түрі бар: физикалық және электрондық.

Бірінші жағдай бойынша, ақпаратты алу қылмыскермен түрлі тұрмыстық видеооптикалық әдебиеттерді қолдану арқылы жүзеге асырылады. Мысалы: бинокль, оптикалық жақындатқыштар,

түнде көретін аңшылардың құралдары, оптикалық прицел және т.с.с. Қылмыскер өзінің объектісін біраз қашықтықтан бақылайды, кейбір кездерде қажетті ақпарат физикалық тасымалдауыш құралына түсіріледі. Мұндай жағдайда қылмыстың құралы тікелей қылмыскердің қолында болды деп есептеледі.

Екінші жағдайда қылмыскермен ақпаратты алу процесі арнайы техниканы қолдану арқылы жүзеге асырылады. Бұл жерде ақпаратты беруші құрылғы бақылау объектісінде орналасады да, ал ақпаратты қабылдап алушы қылмыскердің қолында болады. Олар мынадай техника құралдарын қолдануы мүмкін: ұзақ уақыт жазатын спецвидеомагнитофондар, жасырын видео түсірім жасайтын құрылғылар, сандық электрондық видеокамералар, түнде көрсететін құрылғылар және т.б.

Мусор жинау. Бұл қылмыс жасау әдісі пайдаланушы компьютермен жұмыс жасап болғаннан кейін өзінен кейін қалдырып қойған ақпараттық процесінің техникалық шығындарын қылмыскердің заңсыз пайдалануымен сипатталады.

Ол да екі нысанда жүзеге асырылады: біріншісі – физикалық, екіншісі – электрондық.

Физикалық бойынша қоқыстарды іздеу қоқыс корзиналарын, ыдыстарын, технологиялық қоқыстарға арналған аяқтарын, олардың ішіндегісін мұқият қарауды және қалып қойған немесе тасталған ақпаратты физикалық тасымалдауыштарды жинауды қажет етеді.

Электрондық нұсқасы компьютер жадысындағы мәліметтерді қарауды, кейде оларды ары қарай зерттеуді қажет етеді.

Кейбір кездерде қылмыскер жойылған файлдардағы мәліметтерді қайта қалпына келтіретін, содан соң оларға талдау жасайтын іс-әрекеттерді жүзеге асыруы мүмкін. Бұл мақсаттарға жету үшін қылмыскер қылмыс қаруы ретінде арнайы программаларды қолданады. Солардың бірі болып PC Tools Deluxe программалық кешені табылады. Оның басты қасиетінің бірі онда pct.exe универсалды программасының болуы, ол бұрын жойылған не өшірілген программалар мен файлдарды қалпына келтіру қасиетіне ие.

Компьютерлік қылмыстарды жасау тәсілдерінің үшінші тобына қылмыскердің компьютерлік техника құралдарына заңсыз кіруге мүмкіндік алу әрекеттері жатады. Оның мынадай басты тәсілдері бар:

– қылмыскер жабық тұрған объектінің жанына орналасады да, шынайы пайдаланушыны күтеді, заңды пайдаланушы өзінің паролімен кіретін кезде қылмыскер онымен бірге сол мезетте кіріп кетеді;
– қылмыскер заңды пайдаланушының байланыс линиясына қосылып күтіп отырады, заңды пайдаланушы жұмысын аяқтай бастаған сәтінде қылмыскер инициативаны өз қолына алады. Заңды пайдаланушы активті режимнен шыққанда қылмыскер жүйеде өзінің белсенді әрекетін жүзеге асыра бастайды. Бұл тәсілдерді бір абоненттік нөмірде параллельді жалғанған екі телефонмен салыстыруға болады: «А» телефоны активті режимде болғанда «Б» телефоны көтеріледі, «А» телефоны сөйлесіп болғаннан кейін, «Б» телефоны сөзді ары қарай жалғастыра береді;
– қылмыскер өзінің объектісін жай телефон аппаратының кездейсоқ нөмірлерін теру арқылы таңдайды. Кейде қылмыскер арнайы жасалған автоматтандырылған іздеу программасын қолдануы мүмкін. Көптеген бұзуды жүзеге асыратын программалар HACK TOOLS кәсіби тілінде жазылады.

Бұзуды жүзеге асыратын программаларға парольдің авторы туралы кейбір мәліметтер келіп түседі. Түрлі эксперименттердің нәтижесі бойынша жалпы парольдердің 42 % ашылады екен. Жалпы парольдерге қатысты және олардың ашылуы бойынша келесі кестені көрсетуге болады (4-кесте).

Компьютерлік қылмыстарды жасаудың тәсілдерінің төртінші тобына қылмыскердің КТҚ-ның мәліметтері мен басқарушы командаларын манипуляциялау әдістерін пайдаланумен байланысты әрекеттері жатады.

Енді қылмыскерлермен жиі қолданылатын тәсілдерді қарастырайық:

Мәліметтерді ауыстыру – бұл тәсіл көбінесе банктік операциялардың автоматтандырылған жүйесінде мәліметтерді модификациялау үшін қолданылады. Сонда соммалар жүйесінде опреациялар жүргізілгендей болады, шын мәнінде олар жалған шотқа ауыстырылады. Мысалы: темір жолдың компьютерлік жүйесінде белгілі қылмыскер мәліметтерді ауыстырып қояды, сол себепті теміржол вагондары өзінің тиісті мекен-жайына

емес, басқа жерге жетеді, ал ол жерден қылмыскер өзіне қажетті қомақты соммадағы бағалы тауарды талан-таражға салады.

Троялық ат – бөтен біреудің бағдарламалық қамтамасыз етілуіне арнайы жасалған бағдарламалар енгізіледі. Енген троян аты қылмыскерге қажетті операцияларды жасырын түрде жүйенің ішінде жүзеге асырады.

4-кесте

Парольдердің таңдалуы мен олардың ашылуының пайыздық көрсеткіштері

Парольдердің тематикалық тобы	Адамдардың парольді таңдауының пайыздық жиілігі (%)	Парольдердің ашылуының пайыздық көрсеткіші (%)
Адамның аты, фамилиясы немесе таңдау бойынша	22,2	54,5
Адамның қызығушылықтары (хобби, спорт, музыка)	9,5	29,2
Адамның және оның жақындарының туған уақыты, жұлдыздық белгісі, олардың комбинациясы	11,8	54,5
Тұрғылықты және туған жері	4,7	55,0
Телефон нөмірлері	3,5	66,6
Компьютер клавиатурасының әріптері мен сандарының реттік тізімі, символдардың қайталануы	14,1	72,3
Құжаттардың (паспорт, жеке куәлік және т.б.) нөмірі	3,5	100,0
Қалғандары	30,7	5,7

Троялық аттың өзінің түрлері бар:

а) троян матрешкасы – ол программалық модуль фрагменттері, олар троялық атты жасауға септігін тигізеді де қажетті тапсырмаларын орындағаннан кейін өзін-өзі жойып жібереді;

б) троян құрты. Оның ерекшелігі автоматты түрде троялық атты орындауды және көбейтуді қамтамасыз ететін әрекеттер алгоритмінде. Құрт-программалар автоматты түрде өзін бір немесе бірнеше компьютер жадысында қайталап көшіре береді. Сөйтіп оның жадысын толтырып тастайды.

Троялық аттар мен құрттар туралы біз «вирустарға» қатысты айтылған алғашқы бөлімдердің бірінде тереңірек, нақтырақ талдап өткен болатынбыз.

Қылмысты жасаудың бесінші және соңғы тәсілдер тобына қылмыскермен екі не одан да көп тәсілдерді және олардың түрлі комбинациясын пайдалануы деп танылатын кешенді әдістері жатады. Бұл тәсілдер алғашқы төрт топта нақты қарастырылып кетті.

Енді компьютерлік қылмыстарды жасаудың тәжірибеде шын мәнінде жиі кездесетін тәсілдерін қарастырайық. Компьютерге, ЭЕМ-ға, ЭЕМ желісіне, жүйесіне заңсыз кіру тәсілдерінің ең негізгісі ол компьютерлік алаяқтық.

Компьютерлік алаяқтық. Шет елдердің әдеби қайнар көздерін анализдеу бір-біріне қылмыстық жазалау белгілері жағынан ұқсас іс-әрекеттерді терминологиялық ерекшелеу туралы айтуға болатынын көрсетеді. Нақты айтатын болсақ, олар: компьютерлік алаяқтық, компьютерлік махинациялар, компьютерлік манипуляциялар, ақпараттық жалғандық және бұрыс информация – осының бәрі ұқсас ұғымдар ретінде қарастырылады. Ақпараттық жалғандық және бұрыс ақпаратты осы синонимдес ұғымдар қатарына жатқызу даулы мәселе болып табылады. Құбылыстың басқа белгілеріне қатысты тоқталатын болсақ, олардың зерттеу пәнімен байланысы бар және ұқсастығы болмаса да, компьютерлік алаяқтықты жасаудың тәсілі ретінде түсініледі.

Сонымен, Қазақстан Республикасының қылмыстық заңнамасына сәйкес алаяқтық болып бөтен мүлікті немесе оған құқықты сенімге қиянат жасау немесе алдау арқылы иеленіп алу танылады. Кең мағынада алаяқтыққа басқа да игіліктерді осындай жол арқылы иелену жатады [105, 179 б.].

Осы ұғым оның лексикографиялық талқылауымен сәйкес келеді: «Алаяқтық – ол алдау, қасақаналық мақсатпен жасалатын әділетсіз жағымсыз іс-әрекеттер» [106, 321 б.]. Синонимдік сөздік алаяқтықтың ұқсастығын шектейді.

Мұндай қарым-қатынас манипуляция және махинация сөздерінің мағынасын салыстырғанда да байқалады. Лексикографиялық манипуляция басқа мағынада махинация, алаяқтық іс ретінде талқыланады. Ал махинация – интрига, адалсыздық іс, қулық болады.

Германия Федеративтік республикасының заңнамасында манипуляция жеке категория ретінде емес, алаяқтықты жасаудың бір тәсілі ретінде қарастырылған [107, 263 (а)-тарауын қараңыз]. Сөйтіп немістің ғалымы С. Фрейдің пікірінше, манипуляция мәліметтер мен программаларды өзгертуге бағытталған, сонымен қоса, әдетте, пайдакүнемдік мақсатты көздеген, тыйым салынған әрекеттер жиынтығы. Сонымен бірге, ол ГФР Қылмыстық кодексінің осы тарауындағы «Техникалық аппараттарды теріс пайдалану» қылмыс құрамының орнына жаңа «Компьютерлік алдау» құрамын енгізуді негізді деп тауып ұсыныс жасап көреді [108, 141-152 б.].

Осыдан көріп отырғанымыздай, «компьютерлік алдау» алаяқтықтың топтас бір бөлігі болғаны. Ендеше айтылуы бойынша ұқсас сөздер болып келетін «компьютерлік алаяқтық», «компьютерлік махинация», «компьютерлік манипуляция» ұғымдары түсінігі жағынан әртүрлі болып келгені. Бірақ біздің субъективтік пікірімізше, бұл ұғымдардың барлығы бірігіп «компьютерлік алаяқтық» деп аталғаны дұрыс, ал махинация, манипуляция алаяқтықты іске асырудың әдістері және тәсілдері ретінде қолданылғаны жөн.

Осыларға негізделе «компьютерлік алаяқтық» ұғымына былай анықтама беруге болады: «компьютерлік алаяқтық» дегеніміз – бөтен электрондық, ақпараттық мүлікті, басқа да құндылықтар мен игіліктерді ақпараттық мәліметтерге, олардың өңделу процесінің нәтижесіне заңсыз әсер ету арқылы, алдын ала программаларды теріс жасау арқылы, жазу арқылы мәліметтерді бұзу, модификациялау, қабылданбайтын жалған мәліметтерді енгізу арқылы, ақпараттық құралдарды пайдаланушыларды алдау арқылы оларды немесе оларға құқықтарды заңсыз иелену.

Енді осылардың негізінде компьютерлік алаяқтықтың элементтерін талдап өтуге болады.

Компьютерлік алаяқтықты жасаудың мақсаты өзіне немесе басқа тұлғаға заңсыз мүліктік пайда келтіру.

Компьютерлік алаяқтықты жасаудың тәсілдері:

1) компьютерге әдейі бұзылған мәліметтерді енгізу;

2) программаға күтпеген өзгерістерді кіргізу;

3) мәліметтерді заңға қайшы пайдалану;

4) мәліметтерді өңдеу процесіне заңсыз әсер ету;

5) компьютерге мәліметтерді толығымен енгізбеу;

6) мәліметтерді ауыстыру;

7) заңсыз операцияларды толықтыру немесе шынайы кіріс мәліметтерін алу.

Бұл тәсілдер көбінесе аралас түрде де жүзеге асырылып жатады. Бұл тәсілдермен келесідей заңға қайшы әрекеттер іске асырылады. Бағаны өрескел төмендетіп беру, төлем соммаларын тым көтеріп жіберу, жалған төлемдер жасау, жалған қызмет түрлері мен тауарларға шот жасау, клиент төлемдерінен, жеке шоттарынан олардың қатысуынсыз не рұқсатынсыз қаражат мөлшерлерін шешіп алу немесе бір шоттан екінші шотқа аудару.

Компьютерлік алаяқтық қылмыскерлерінің тұлғасына сипаттама. Бұл тұлғалардың әдетте өздерінің функционалдық міндеттеріне байланысты компьютерлік техникаға тікелей қатысы бар және арнайы техникалық дайындығы жоғары. Өздерінің қызметтік міндеттері шегінде компьютерге кіруге заңды рұқсаты бар бұл тұлғалар өздерінің құқықтарын теріс мақсатта пайдаланады. Мысалы: «Times» газетінің мәліметтері бойынша 1200 қоғамдық және коммерциялық ұйымдардың жұмысын тексеру кезінде жасырын құқықбұзушылықтар кезінде 118 жағдай сол ұйымның қызметкерлеріне қатысты болған және олардың көбісінде компьютерге қатысты тікелей рұқсаты бар қызмет орны болды. Алаяқтық көбінесе шартты түрде аталатын «хакерлермен» жасалып жатады. Хакерлердің әрекет ету спектрі өте ауқымды – күшті ұлттық компьютерлік орталықтардан бастап бүкіл қаржылық арналарды басқарып отырған халықаралық жүйелерге дейін. Хакерлер туралы толық және жан-жақты жоғарыда айтылып кеткен болатын.

«Компьютерлік алаяқтық» автоматтандырылған ірі банк жүйелері мен үлкен коорпорацияларға, мемлекеттік қызмет түрлеріне қатысты ғана емес, кез келген электрондық есептеуіш техникалары бар ұйымдарда да жиі кездесіп жатады.

Компьютерлік программаға белгісіз өзгертулерді енгізу «троялық ат» атты әдіспен жасалуы мүмкін. Оның қызме-

ті қорғаныс модуліне техникалық шарттарды айналып өтіп арнайы программаны қолдану болып табылады. Мысалы: ақша құралдарын немесе акцияларды аудару ережелеріне араласу, содан кейін барлық іздерді жойып жіберу. Бұл тәсіл көбіне компьютерде екі пайдаланушы арасындағы жағдайларда – партнерлер арасында болатын операциялар жүзеге асырылғанда болады (мысалы, сатушы және сатыпалушы, мердігер мен жұмысты атқарушы) [109, 131 б.].

Алаяқтық көбінесе мәліметтерді ауыстыру арқылы жасалады. Мамандардың айтуынша бұл тәсіл ең қарапайым тәсілдердің бірі, ол тәсілді жай бастауыш программистер де қолдана алады.

«Компьютерлік алаяқтықты» жүзеге асырудың шарттары. Компьютерлік қауіпсіздіктің ең әлсіз жері ол өңдеу жүйесіне мәліметтерді енгізудің сапалығы мен ерекшелігін қадағалау жүйесі болып табылады. Бұл кемшіліктер жақсы ұйымдасқан ұйым ішінде де кездеседі, егер жұмыс уақыты ішінде терезелер (окнолар) пайда болса, яғни оператор жалғыз өзі барлық электрондық жүйеге жауап берсе. Бұл жерде басты рөлді кадрлық жұмыс бойынша ЭЕМ оператор қызметкеріне талапкерді алдын ала тексеру жұмысы атқарады. Бірақ кейде қажетті профильдар жетіспеген жағдайларда сенімсіз маманды жұмысқа алу қаупі туады.

Көп ұйымдар ескі не сапасы төмен, яғни компьютерлерді қорғау жүйесінің арзан түрлерін қолданады, сол арқылы ұйым үшін маңызы жоқ қаржы көлемін үнемдеп, кейін үлкен қомақты қаржы соммасын жоғалтуға әкеліп соқтырады.

Бақылау-өткізу жүйесінің әлсіз болуы ұйымның машиналық залына бөтен тұлғалардың кіруіне себеп болады.

Сонымен жоғарыда айтылған осы компьютерлік қылмыстарды жасаудың тәсілдері осылармен шектелмейді. Көптеген тәсілдерді сипаттап анықтап беру өте қиын, себебі олар кейде тек программалық тілде ғана сипатталуы мүмкін, ал кейде олар тек негізгі тәсілдің орындалуына көмекші, дайындық немесе қажетті әрекет ретінде ғана пайдалануы мүмкін.

Компьютерлік қылмыстарды жасаудың тәсілдерімен қатар криминологиялық сипаттамаға компьютерлік қылмыстарды жасаудың ниеті мен мақсаты кіреді.

Кез келген нақты қылмыстарды тергеу кезінде ниет пен мақсат анықталуы тиіс. Ол сотпен жазаны тағайындау кезінде әділ ше-

шім қабылдау үшін және қылмысты толық ашу үшін маңызды болып табылады.

Компьютерлік қылмыстарды жасаудың ең жиі тараған бес ниетін атаған болатынбыз, олар:

– пайдакүнемдік оймен (66%);
– саяси мақсаттар (17% мысалы: шпионаж);
– зерттеу қызығушылығы (7% негізінен жас студенттер және программистер);
– бұзақылық ниетпен (5% хакерлер);
– кек және өш алу (5%) [110, 11 б.].

Компьютерлік қылмыстардың толық көлемде ниеттерін А.К. Расулевтің еңбегінен көруге болады.

Көп кездесетін типтік мақсаттарға жалған шоттар мен жалған төлем карталарын жасау, артық жұмыс сағаттарын жазып алу, төлем құжаттарын фальсификациялау, ақша-қаражат мөлшерін ұрлау, жасалған төлемдерді қайта жасау, жалған шоттарға ақша-қаражат мөлшерлерін аудару, қылмыстық пайданы заңдастыру, жалған төлеммен сатып алу, заңсыз валюталық операциялар жүргізу, заңсыз несие алу, қозғалмайтын мүлікті манипуляциялау, заңсыз жеңілдіктер мен қызметтерді алу, конфиденциалды ақпаратты сату, материалдық тауарлар мен құндылықтарды талан-таражға салу және т.б. жатады. Осылардың 52% ақша-қаражат мөлшерін ұрлаумен байланысты, 16% компьютерлік техника құралдарын бұзу мен жоюға байланысты, 12% алғашқы мәліметтерді ауыстырумен, 10% ақпарат пен программаларды талан-таражға салумен, 10% қызмет түрін заңсыз пайдаланумен байланысты.

Компьютерлік қылмыстарға криминологиялық сипаттама жасаудың міндетті белгілерінің бірі, әрине, қылмыстылықтың профилактикасы, яғни компьютерлік қылмыстылықтың кездесіп жатқан түрлері мен мүмкін болар қоғамға қауіпті әрекеттерді алдын ала ескерту және тамырынан болдырмау.

Қылмыстардың алдын алу әдісі криминология ғылымының маңызды және басты бөлімдерінің бірі болып табылады және қылмыстың жеке түрлерімен күрес жүргізу әдісінің ортақ ұғымына кіреді. Қылмыстың жеке түрлерімен күресуге қазіргі кезде ешбір даусыз компьютерлік қылмыстарды да кіргізуге болады.

Кейбір мамандардың айтуынша, профилактикалық жұмыстардың нәтижелері, егер олар дұрыс ұйымдастырылса және дұ-

рыс бағытталса, қылмыстылықтың дәрежесіне, өсу динамикасы мен құрылымына оңды әсер етеді, яғни ақырғы қылмыстылықтың көрсеткіштерін төмендетеді және қоғамда үлкен маңыздылықпен криминологиялық мәнге ие болады. Оның себебі ескерту шаралары қылмыстылықтың қайнар көздеріне қарсы жасалады. Сол себепті, біз білетіндей, қылмысты ескерту криминологиялық сипаттаманың, жалпы криминология ғылымының басты және міндетті құрамдас бөлігі болып табылады.

Көптеген шетелдік мамандардың байқауынша, компьютерлік қылмыстардың алдын алған оларды тергеп ашқаннан гөрі әлдеқайда жеңіл және мүмкін.

Соған қарамастан құқыққорғау органдарының, әсіресе тергеу аппараттарының қызметкерлері, ғылыми институттар компьютерлік қылмыстардың алдын алуы бойынша ауыр және күрделі шараларды жүзеге асыру үшін төмен кәсіби дәрежелі дайындық үстінде ғана. Бұл дегеніміз қазіргі кезде осы қарастырып отырған санаттағы қылмыстарды ескерту тактикасы мен саясаты, ұйымдастыруы бойынша құрамы жағынан қандай да нақты немесе толық әдістемелік жұмыстардың болмауымен түсіндіріледі. Бұл жерде компьютерлік қылмыстардың жаңалығы мен ерекшелігін, нақтырақ айтатын болсақ, оларды анықтау, шешу және тергеу әрекеттерінің тым қиындылығын ескерген жөн.

Периодтық түрде басылымға шығып отырған отандық және шетел арнайы әдебиеттері мен шығармалары негізіндегі компьютерлік қылмыстылықпен күресу теориясы мен тәжірибесі мәселелері бойынша мәліметтерді талдау бойынша компьютерлік қылмыстардың алдын алу мен күресу шараларын 3 негізгі топқа бөліп көрсетуге болады:

1) Құқықтық;

2) Ұйымдастырушылық-техникалық;

3) Криминологиялық.

Нақтырақ тоқталып кетейік. Компьютерлік қылмыстардың алдын алуға қатысты құқықтық шараларға, бірінші кезекте, жоғарыда айтылып кеткен құқықбұзушылықтар үшін қылмыстық жауаптылықты тудыратын заңнаманың нормалары жатады.

Шетел заңнамасының осы бағыттағы даму тарихы көрсеткендей, ең алғашқы мұндай қадам 1978 жылғы Америка құрама штаттарының Флорида және Аризона штаттарының заң

жинақтарымен жасалды. Қабылданған заң «Computer crime act of 1978» деп аталды және ең бірінші болып компьютерлік қылмыстар үшін қылмыстық жауаптылықты қарастырды. Кейін АҚШ-тың басқа штаттарында да осыған ұқсас арнайы заңдар қабылданды [111, 3-тарау].

Бұл құқықтық актілер компьютерлік қылмыстарды ескертуге байланысты шараларды жүзеге асыру мақсатында заңнамаларды жетілдіруге фундамент болды.

Ал біздің отандық заңшығару қызметіміз бұл бағытта өте жай қадамдармен жылжып келеді. Мұндай заң бірінші кезекте құқықтық қорғау объектісі болып табылатын ақпараттық технологиялардың негізгі компоненттерінің анықтамасын, яғни заңи ұғымын беруі тиіс, содан кейін бұл объектілердің меншік иелерінің құқықтары мен міндеттерін белгілейді, ақпараттық технология құралдарының құқықтық режимін анықтайды, нақты ақпарат түріне субъектілердің кіру категорияларын анықтайды, мәліметтер мен ақпараттардың құпиялық дәрежесін белгілейді.

Қазақстан Республикасында электрондық ақпараттық қатынастарға қатысты оңды қадамдардың біріне Қазақстан Республикасының Президентінің 2006 жылғы 10 қазанындағы Жарлығымен мақұлданған «Қазақстан Республикасының ақпараттық қауіпсіздік Концепциясын» шығару болып табылады. Соған қарамастан киберқылмыстарға қатысты басты қадам болып шынында ҚР Қылмыстық кодексіне кіргізілген 227-бап табылады, одан кейін 2002 жылы Қазақстан Республикасы Президентінің Жарлығымен бекітілген ТМД елдері бойынша Келісімнің 3-бабы, осы келісімнің негізінде кезеңдер бойынша қылмыстық заңнамаға осы сала бойынша тиісті өзгерістер мен толықтырулар қабылдау. Сонымен қатар осы уақытқа дейін қабылданған бірқатар нормативтік актілердің тізімі ақпараттық қарымқатынастар саласын қандай да бір дәрежеде (мүмкін жеткілікті, мүмкін жеткіліксіз) реттеп келеді.

Бірақ қылмысты ескертуге қатысты тек құқықтық нормаларды қолдану қажетті нәтижеге алып келмейтіні жалпыға белгілі.

Онда келесі қадам болып КТҚ-ны заңға қайшы әрекеттерден қорғайтын ұйымдастырушылық-техникалық шараларды қолдану табылады.

Компьютерлік қылмыстарды ескертудің ұйымдастырушылық-техникалық шараларын мамандармен қолдану әдістері бойынша өз кезегінде үш топқа бөлеміз:

1) ұйымдастырушылық;

2) техникалық;

3) кешендік.

КТҚ-ны қорғаудың ұйымдастырушылық шаралары өзіне мына шаралар жиынтығын кіргізеді: персоналды жинау, тексеру және инструктаж жүргізу бойынша шаралар; ақпараттық объектілерді істен шыққаннан кейін қалпына келтіруді ұйымдастыру; КТҚ программалық-техникалық қамтамасыз етуді ұйымдастыру; нақты КТҚ бойынша қауіпсіздікті қамтамасыз ету бойынша тұлғаларға тәртіптік жауаптылықты жүктеу; компьютерлік жүйелердің жұмыс жасауы кезіндегі құпиялық режимді жүзеге асыру; объектілердің физикалық қорғалуын қамтамасыз ету; материалдық-техникалық қамтамасыз ету және т.б.

Ұйымдастырушылық шаралар ақпаратты қорғау құралдарының ең маңыздысы және әсерлісі. Соның негізінде басқа қауіпсіздік жүйелері құралады.

Кез келген ұйымда қауіпсіздікті қамтамасыз ету үшін келесі ұйымдастырушылық шараларды жүзеге асыру керек:

1) компьютерлік техника құралдарына рұқсаты бар барлық адамдардың белгілі бір рұқсат категориясы болу керек;

2) ақпараттық ресурстар үшін жауапты тұлғаларға әкімшілік жауаптылық белгілеу;

3) ақпаратты оның маңыздылығы бойынша топтастыру;

4) КТҚ-ны ұйымдық негізде физикалық қорғау.

Ұйымдық-техникалық шаралардан басқа компьютерлік қылмыстармен күресуде маңызды рөл техникалық сипаттағы шаралар атқарады. Техникалық әдістерге компьютерлік желіге не жүйеге заңсыз кіруді анықтау үшін қолданылатын арнайы құрылғыларды пайдаланудың барлық тәсілдері жатады.

Шартты түрде оларды қорғалатын объектінің ерекшелігі және сипаты бойынша 3 негізгі топқа бөлуге болады: аппаратты, бағдарламалы (программалы) және кешенді.

Аппаратты әдістер компьютерлік техниканың байланыс құралдары мен аппараттық құралдарын сыртқы физикалық әсерлерден қорғау және құпия мәліметтерді электромагниттік сәулелендіру арқылы шешу арналарына тосқауыл жасау үшін арналған.

Қорғаудың бағдарламалық әдістері ақпаратты үш бағыт бойынша тікелей қорғау үшін арналған: а) аппаратуралық; б) бағдарламалық қамтамасыз ету; в) мәліметтер және басқару командалары бойынша.

Әдетте қауіпсіздікті қамтамасыз ету мақсатында ақпаратты жасырын түрде жіберу үшін шифрлаудың түрлі әдістері қолданады, яғни мәлімет шифрлы түрде байланыс арнасына шығады да өзінің бағытына жеткенде қалпына келтіріледі. Тәжірибе көрсеткендей бұл тәсіл бөтен субъектілерден мәліметті жасыру жағдайында әсерлігімен сенім артып келеді.

Заңсыз кіру шараларымен күресуде нәтижелі әдістердің біріне тіркеу тәсілі жатады. Ол үшін шетелде жиі пайдаланылатын мониторинг деп аталатын арнайы мақсаттағы жаңа операциялық жүйені дамыту. Оның ерекшелігі компьютерге төніп тұрған қауіпті автоматты түрде бақылау. Мониторинг операциялық жүйенің өзімен жүзеге асырылады және оның міндеттеріне кіру-шығу процестерін қадағалау, машиналық ақпаратты өңдеу және жою жатады. Оперативтік жүйе мен бағдарламалық құралдарға заңсыз кірудің уақытын белгілеп отырады. Сонымен қатар бұл бағдарлама компьютерлік қауіпсіздікті қамтамасыз ету қызметіне жедел түрде компьютерлік жүйе қауіпсіздігіне қол сұғылды деген хабарлама және хабарламамен бірге ол туралы қажетті мәліметтерді жібереді.

Кейінгі кезде шетелде құпия мәліметтерге қол сұғылған жағдайда өзін-өзі жойып жіберетін программалар қолдануда, ұқсастығы жағынан ол «логикалық бомбаға» ұқсайды.

Ақпараттық ресурстарды қорғау мәселелерін қозғаған кезде компьютерлік вирустардан қорғану мәселесін де ұмытпаған жөн. Бұл жерде қорғаныс түріне жататын арнайы антивирустық программаларды (бағдарламаларды) белсенді түрде қолданған дұрыс. Жаңартылып отыратын антивирус бағдарламалары вирустарды ақпараттық ресурстардан уақытылы табады, таниды және емдейді.

Алайда антивирустық программаларды қолданумен қатар КТҚға вирустардың неғұрлым аз қаупі төну үшін оларға қатысты кешенді ұйымдастырушылық-техникалық шараларды қолданған жөн.

1. Компьютерлік техника құралдарын пайдаланатын мекеменің, ұйымның барлық қызметкерлерін вирустық шабуыл

жасалғаны немесе жасалу қаупі бар, ішкі желі арқылы тарағаны жайлы хабардар ету.

2. Қызметкерлерге мекеменің, ұйымның компьютерлік құралдарымен жұмыс жасау үстінде сырттан әкелінген бағдарламаларды, файлдарды жұмыс орнына әкелуге тыйым салу.

3. Қызметкерлерге ЭЕМ-ның жадысында және электронды тасымалдауыштарда компьютерлік ойындарды пайдалануға, сақтауға рұқсат бермеу.

4. Түрлі дәрежедегі және саладағы басқа оқу, қызмет мекемелерінің компьютерлері мен машиналық тасымалдауыштарын қызметкерлермен пайдалануын бақылау және ескерту.

5. Сыртқы компьютерлік желі арқылы келген барлық файлдар тестілеуден өтуі тиіс.

6. Ұйымның тікелей жұмысында пайдаланып жүрген бағдарламалық құралдардың көшірмелерінің мұрағатын жасау.

7. Компьютерлік жүйеде сақталынған бағдарламаларды үнемі тексеріп отыру; мүмкіндігінше құнды мәліметтерді заңсыз манипуляциядан сақтап қалу үшін файлдар мен бумаларға «тек оқу» (только чтение) қорғаныс түрін қолдану.

8. Периодтық түрде файлдарды олардың түпнұсқасымен салыстыру арқылы тексеру.

9. Электрондық пошта қажеттілігі үшін арнайы жеке компьютерді пайдалану және арнайы есеп жүргізу.

10. Аса маңызды компьютер құралдарына (мысалы, серверлерге, ұйымның орталық компьютер жүйесіне, басшылықтың компьютерлеріне, компьютер орталықтарына, мәліметтер базасына) ақпараттарды қорғау жүйесін орналастыру; оларға арнайы кешенді антивирус программаларын қосып қою.

11. Белгіленген қауіпсіздікті қамтамасыз ету ережелерінің орындалуын үнемі қадағалау және бұл ережелерді бұзғандарға, қасақана әдейі және бірнеше мәрте бұзғандарға тәртіптік, материалдық әсер ету шараларын қолдану.

Компьютерлік қылмыстардың алдын алу шараларына сонымен қатар ақпараттарды және мәліметтерді қорғау да жатады. Ақпаратты немесе мәліметті қорғау қорғаныстағы ақпараттың ауытқуына, ақпаратқа заңсыз әсер ету және оған заңсыз кіруге жол бермеу бойынша іс-әрекет жиынтығы дегенді білдіреді. Ақпаратты қорғаудың белгілі түрлері бар, оларға ақпаратты не-

месе мәліметті компьютерлік желілерде қорғау, соның ішінде шифрлеу; мәліметтерді физикалық түрде қорғау, соның ішінде кабельдік жүйе, электрқамтамасыз ету жүйесі, сенімді құрал-жабдықтарды таңдау, ақпаратты мұрағаттық және көшіру жүйелері; қорғаудың бағдарламалық және аппараттық-бағдарламалық әдістері, соның ішінде бағдарламалық қамтамасыз етуді таңдау, компьютерлік вирустардан қорғану, ақпаратқа заңсыз кіруден қорғану.

Жалпы компьютерлік қылмыстармен күресу бірінші кезекте, әрине, мемлекетіміздің, онымен тікелей байланысты ғылымымыздың, содан кейін әр жеке адам санасының қолында. Біз соған қатысты өзіміздің үлесімізді қосу үшін қылмыстылықпен күресудің құқықтық, соның ішінде криминологиялық және ұйымдастырушылық әдіс іс-әрекеттерін көрсеттік.

Ал жалпы алғанда аталған тарауда біз ақпараттық қылмыстардың криминологиялық сипаттамасын жан-жақты қарастырып көрдік. Сипаттама барысында бірнеше көкейтесті мәселелерді анықтап, тиісті негіздер келтіріп теориялық, тәжірибелік және құқыққолдану шығармашылығы жағынан ұсыныстар жасадық.

3. КОМПЬЮТЕРЛІК ҚЫЛМЫСТАРМЕН КҮРЕСУДЕГІ ХАЛЫҚАРАЛЫҚ САЯСАТ ЖӘНЕ ТӘЖІРИБЕ

3.1. Қазақстанның киберқылмыстылықпен күресудегі шет елдермен қарым-қатынасы, байланысы және даму тарихы

Қазіргі таңда халықаралық компьютерлік қылмыстар фактісі кең тарауда. Әсіресе көп кездесетін компьютерлік алаяқтық қылмыспен табылған ақшаны заңдастыру үшін компьютерлік техниканы пайдалану, хакерлердің (компьютерге, компьютерлік желіге заңсыз кіретін тұлға) халықаралық ақпараттық жүйелерге кіруі және ақпаратты ұрлауы. Осы проблемалардан көріп отырғанымыздай, халықаралық қылмыстарды тергеу және ашу кезінде көмек болатын халықаралық процедуралар қажеттілігі және Интерпол шегінде жұмыс істейтін органды ұйымдастыру ұсынысы туындайды.

Компьютерлік қылмыстардың көпшілігі жер шарын басып алған глобалды компьютер, Интернет желілерінде жасалатынын ескерсек, соңғы онжылдықтар ішінде әртүрлі елдер арасында заңшығару және құқыққолдану тәжірибесінде осы жаңа қылмыс түріне қатысты халықаралық қатынастар белсенді дамып келеді. 1996 жылы Парижде Экономикалық қатынас пен дамуды ұйымдастыру жұмысымен айналысатын сарапшылар тобы компьютерлік қылмысқа анықтама берген еді. Олар былай деді: «Компьютерлік қылмыс дегеніміз – автоматтандырылған мәліметтерді өңдеуге не беруге қатысты кез келген заңсыз, әдепсіз немесе тыйым салынған жүріс-тұрыс әрекеті».

Осыдан көріп отырғанымыздай, әлемдегі ақпараттық жағдай мен салыстырмалы түрде еліміздегі осы мәселеге деген қарым-қатынас аталған тарау негізінде зерттеу мен талдауды жүргізуге талап қойып отыр. Сол себепті халықаралық тәжірибеге көшпес бұрын еліміздегі ақпараттық қылмыстар мәселесін, соның ішінде

оның құқықтық тарихын және халықаралық қатынас жағдайын және дамуын қарастырып өткен жөн.

Компьютерлік қылмыстар еліміздің тарихында қылмыстық-құқықтық ұғым ретінде ең алғаш Қазақ ССР Қылмыстық кодексінде нақты қылмыстар тобын баянды еткен ұғым болып пайда болады. Ол кезде компьютерлік қылмыстар ҚазССР Қылмыстық кодексінің 6-шы «Шаруашылық қылмыстар» тарауында компьютерлік ақпаратқа заңсыз кіру, ЭЕМ үшін зиянды бағдарламаларды жасау, пайдалану және тарату 165-4-бабында көрініс тапқан болатын. Бұл тоқсаныншы жылдары енгізілген өзгерістер мен толықтырулар нәтижесі болатын. Сол жылдары Қазақстан ТМД елдерінің мүшесі бола отырып тәуелсіз елдердің Модельдік Қылмыстық кодексін қабылдайды. Модельді Қылмыстық кодекс ТМД қатысушы-елдердің Парламентаралық Ассамблеясымен жасалған болатын және тек ұсыныс ретінде сипатталатын.

Модельді Қылмыстық кодекс «Ақпараттық қауіпсіздікке қарсы қылмыстар» атты 30-тарауында компьютерлік қауіпсіздікке қол сұғатын келесі қылмыстық құрамдарды құрайтын:

1) 286-бап. Компьютерлік ақпаратқа заңсыз кіру;

2) 287-бап. Компьютерлік ақпаратты өзгерту (модификациялау);

3) 288-бап. Компьютерлік саботаж.

4) 289-бап. Компьютерлік ақпаратты заңға қарсы жолмен алу;

5) 290-бап. Компьютерлік жүйеге немесе желіге заңсыз кіруге рұқсат немесе мүмкіндік алу үшін арнайы құралдарды жасау және тарату;

6) 291-бап. Зиянды бағдарламаларды жасау, пайдалану және тарату;

7) 292-бап. Компьютерлік жүйелерді немесе желілерді эксплуатациялау ережелерін бұзу [112].

Аталғандардан басқа Модельді қылмыстық кодексте компьютерлік ақпарат пен компьютерлік техниканы пайдалану арқылы жасалатын, яғни қылмыстарды жасау тәсілі ретінде қарастырылатын қылмыстық құрамдар көрініс тапқан. Оларға, мысалы, компьютерлік техниканы пайдалану арқылы мүлікті талан-таражға салу немесе сол сияқты алдау, сенімге қиянат жасау арқылы, компьютерлік ақпаратты өзгерту арқылы мүліктік зиян келтіру және т.б.

Кейін 1997 жылы 16 шілдеде қабылданған ҚР Қылмыстық кодексінде компьютерлік ақпараттың қауіпсіздігіне қол сұғатын қылмыстар үшін қылмыстық жауаптылық нормалары 7-ші «Экономикалық қызмет саласындағы қылмыстар» тарауында ҚазССР Қылмыстық кодексінде болған күйіндегі нормалар шегінде тіркеледі. Өзгеріске аталған нормалардың санкциялары ғана ұшырайды. Оның себебі ҚР Қылмыстық кодексіне енгізілген жаңа жаза түрлеріне байланысты.

Соған қарамастан айта кететін жәйт, қазақстандық заңшығарушылар компьютерлік қылмыстармен күресуде үлкен және қажетті қадам жасайды. Себебі ол кезде компьютерлік ақпараттық қылмыстармен күресуде процессуалдық та, соттық та тәжірибе болмады десек асыра айтушылық болмайды. Компьютерлік қылмыстылық фактісі тіркелгенімен, тергеушілер ол қылмыстармен, қылмыстарды ашу жолымен бейтаныс болды. Көп жағдайда тергеу әрекеттері тоқтап тұратын, онсыз да жетіспейтін мамандардың біліміне жүгінуге тап болатын, кейде қылмыскерлердің өздерімен де кеңес жүргізу сәттері болатын. Ал компьютерлік құқық бұзушылар өздеріне үлкен пиар жасап алатын. Сөйтіп жоғары ақылы ақпараттық қауіпсіздікті қамтамасыз ететін жерлерге жұмысқа орналасатын. Бұл тәуелсіз Қазақстан өз егемендігін алғаш алған сәттерде болған мәселелер десек болады. Қазір жағдай өзгеше болып отыр. Ол туралы сәл кейінірек.

Тәуелсіз Қазақстанда осы қолданыстағы заңнаманы қабылдағанға дейін ақпараттық қылмыстарға тектес бірде бір қылмыс тіркелмеген болатын, тіпті ақпараттандыру және компьютеризациялау ағымдары нормативтік актілермен реттелмей өз бетімен жүзеге асып жатты. Құқықтық ғылым қоғамды компьютеризациялаудың қандай да кері ықпалы болады деп ойлап та көрмеген. Сол 1997 жылдың өзінде Қазақстанның заң шығарушы органдары аталған нормаларды қабылдау кезеңінің өзінде-ақ бұл нормалар белсенділердің қатарына жатпайтынына күмән болған жоқ, нормалардың бастапқы рөлі тек профилактикалық болды және оларды қабылдаудың басты себебі және негізі болып сол кездегі шет елдердің қарқынды жүріп жатқан тәжірибесі табылды.

Көріп отырғанымыздай мұндай құбылыс құқықшығарушылық тәжірибеде көп кездесе бермейді, себебі көбінесе қоғамда

қылмыс ауқымдылыққа ие болады, содан кейін барып қылмысқа қарсы тиісті құқықтық шаралар қолданылады.

Сол жөнінде өз жұмысында Б.Х. Толеубекова дұрыс келтіреді: «Қазақстанның Қылмыстық кодексіндегі компьютерлерді пайдалану арқылы жасалатын қылмыстарды институализациялау әлеуметтік-экономикалық және саяси-құқықтық қажеттілік болды. Осының теориялық-құқықтық негізі алдын ала ғылыми болжау мен көру шегінде тәжірибені озып кету сипатында болды. Осы мақсаттағы біздің тапсырмамыз Батыс Еуропа, АҚШ және Ұлыбритания сияқты елдердің компьютерлік қылмыстармен күресудегі мол тәжірибесінің арқасында салыстырмалы жеңіл болды» [113, 110 б.].

Қазақстан жаңа мыңжылдыққа аяқ басар кезде кішігірім ақпараттық қауіпсіздік саясатын жүргізе бастайды. Оған 1998 жылы 26 маусымда қабылданған Қазақстан Республикасының №233-1 «ҚР Ұлттық қауіпсіздігі туралы» Заңы дәлел. Осы заңнамада алғаш Қазақстан аумағында «ақпараттық қауіпсіздік» ұғымы берілген болатын. Ол былай делінген: ақпараттық қауіпсіздік – мемлекеттік ақпараттық қорлардың қорғану жағдайын, сонымен қатар ақпараттық саладағы жеке тұлғалар мен қоғам мүдделерінің және құқықтарының ақпараттық қауіпсіздік жағдайын білідіреді [114, 16 б.].

Ақпараттық саладағы анықтамалар мен ұғымдардан басқа бұл заңнама ақпараттық блокадаға жол бермеу туралы талаптар қояды, яғни басқа мемлекеттер жағынан Қазақстан Республикасының ақпараттық кеңістігінің үзіліссіз жұмыс жасауына қарсы бағытталған іс-әрекеттерге тыйым салады.

Қазақстан Республикасының бірыңғай ақпараттық кеңістігі жөніндегі концепция және оны жүзеге асыру шаралары 1998 жылы 29 шілдеде Қазақстан Республикасы Үкіметінің № 715 Қаулысымен мақұлданған болатын. Бұл қаулыда ақпараттық кеңістіктің типтік ерекшелігі ретінде келесідей мәселелер ескеріліп өткен: Біріншіден, мемлекеттік ақпараттық қайнар көздерге қадағалау жасау, яғни басқаша айтқанда ақпараттық барлау жұмыстары. Ақпараттық кеңістік өзімізге белгілі болғандай барлау жүргізу арнайы қызметтердің басты функциясы болып табылады. Қазіргі кезде ақпараттық барлау жүргізу ақпараттық және басқару жүйелеріне заңсыз кіру жолдары арқылы және заңды жолмен, яғни шетелдік ұйымдардың Қазақстанның ақпараттық инфрақұ-

рылымына қажетті шарттарды жасау себебі арқылы жүзеге асырылады.

Екіншіден, ақпараттық ресурстарды жою, бұзу мақсатында ақпараттық қарым-қатынас жасау. Ақпараттық технологиялардың жаңа замандық даму дәрежесі негізінде мұндай қарым-қатынастар жай бейбітшілік уақытында да жүзеге асырыла береді. Бұл қатынастар мемлекеттің құнды деген ақпараттарына зиян келтіруі мүмкін немесе сол ақпараттарды өзгерту арқылы мемлекеттің басқару дәрежесіндегі ақпараттармен байланысты қажетті дұрыс шешім қабылдауына кері әсер етуі мүмкін.

Қазақстан Республикасының «Ақпараттандыру туралы» Заңы компьютерлік ақпараттың қауіпсіздігіне қол сұғатын қылмыстарды анықтау, жою, алдын алу және тергеу кезінде пайдаланылатын анықтамаларды бекітті. Мысалы, ақпараттандыру, ақпараттық ресурстар, құжатты ақпарат және т.с.с.

Ақпараттық заңнама деп аталатын жүйенің қалыптасуы мемлекет өз дамуында бірінші қатарға ақпаратты өндіруді, өңдеуді, сақтауды және қорғауды қояды дегенді білдіреді. Аталған нормативтік құқықтық актіде көрсетілген қағидалар мен міндеттерді жүзеге асыру бірыңғай ақпараттық кеңістіктің негізін құрайтын мемлекеттік ақпараттық ресурстардың бірнеше қадамдық қорғау шегін қамтамасыз етуге мүмкіндік береді және оның тиімді қызмет етуіне әсерін тигізеді.

2002 жылдың 25 маусымында ҚР Президентінің жарлығымен ТМД қатысушы мемлекеттер арасында компьютерлік ақпарат саласындағы қылмыстармен күресудегі қарым-қатынас туралы Келісім бекітілді (Халықаралық Келісім 2001 жылдың 1 маусым күні Минск қаласында өткізілді).

Келісім ТМД елдерінің құқыққорғау органдары арасындағы компьютерлік қылмыстармен күрес жүргізу шараларының құқықтық негіздерін анықтайды.

Аталған келісімнің 3-бабының 1-тармағын қарастырсақ, онда келісімнің жақтары өздерінің Ұлттық заңнамаларына сәйкес қылмыстық жазалануға тиіс болып табылады, егер іс-әрекеттер қасақаналық ниетпен келесі жағдайларда жасалған болса:

а) заңмен қорғалатын компьютерлік ақпаратқа заңсыз кіруді жүзеге асырған жағдайда, егер бұл әрекет ақпаратты жоюға, бөгеуге, өзгертуге немесе көшіруге не болмаса, ЭЕМ-нің жұмысын, ЭЕМ жүйесі мен оның желілерін бұзуға әкеліп соқса;

б) зиянды бағдарламаларды жасау, пайдалану немесе тарату жағдайларында;

в) ЭЕМ-ге, ЭЕМ жүйесіне және олардың желілеріне кіру құқы бар тұлғалардың ЭЕМ-ді, ЭЕМ жүйесін және олардың желілерін эксплуатациялау ережелерін бұзуы, егер нәтижесінде заңмен қорғалатын ақпарат жойылса, өзгерсе, бөгелсе немесе елеулі зиян және ауыр салдар келтірілсе;

г) ЭЕМ және мәліметтер базалары үшін авторлық құқықтық объектілері болып табылатын бағдарламаларды заңсыз пайдалану, сонымен бірге авторлықты өзіне иеленіп алу жағдайларында, егер бұл әрекеттер елеулі зиян келтірсе [115, 8 б.].

Сөйтіп, бұл Келісім жақтары, яғни келісімді қабылдаған мемлекеттер өздерінің Ұлттық қылмыстық заңнамаларына аталған баптың нормаларын енгізуі тиіс. Бірақ осы Келісімді қарастырған таңда Қазақстанның Ұлттық заңнамасында кейбір қоғамға қауіпті әрекеттер криминализацияланған болатын. Қазақстан Республикасы Қылмыстық кодексінің 227-бабының 1-тармағы «Заңмен қорғалатын компьютерлік ақпаратқа заңсыз кіру», 227-баптың 3-тармағы «Зиянды бағдарламаларды жасау, пайдалану және тарату», ҚР Қылмыстық кодексінің 184-бабы «Зияткерлік меншік құқықтарын бұзу» мазмұны жағынан аталған талаптарға толығымен жауап беретін.

Халықаралық міндеттерді орындай отырып ҚР Парламенті 2002 жылдың 21 желтоқсанында «Кейбір заңнамаларға толықтырулар мен өзгерістер енгізу туралы» №363-II Заңын қабылдады. Соған сәйкес Ұлттық қылмыстық заңнамада болмаған халықаралық келісімдегі «ЭЕМ, ЭЕМ жүйесі және олардың желілерінің эксплуатациялау ережелерін бұзу» әрекеті криминализацияланды [116].

Ал 2007 жылы 8 қаңтарда тағы бір өзгеріс болды. 227-1-бап келесі мазмұнда болды:

«Атауы: Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын (IMEI-код), абоненттік сәйкестендіру құрылғысын (SIM-карта) құқыққа сыйымсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгерту үшін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату

1. Жасап шығарушының немесе заңды иесінің келісімінсіз ұялы байланыстың абоненттік құрылғысының сәйкестендіру ко-

дын құқыққа сыйымсыз өзгерту, ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын құқыққа сыйымсыз жасау,

– екі жүзден бес жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға, не екі айдан бес айға дейінгі еңбек ақы немесе басқа да табыс түрінде әлде 120 сағаттан 180 сағатқа дейін қоғамдық жұмыстарға тарту арқылы, немесе бір жылға дейін түзеу жұмыстарына, не дәл сол мерзімге бас бостандығынан айыруға жазаланады.

2. Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын өзгертуге немесе ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын жасауға мүмкіндік беретін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату,

– бес жүзден сегіз жүз АЕК-ке дейінгі мөлшерде немесе бес айдан сегіз айға дейінгі еңбек ақы немесе басқа да табыс түрінде айыппұл салуға, әлде бір жылдан екі жылға дейінгі мерзімге түзеу жұмыстарына, не 3 жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.

3. Нақ сол әрекеттер:

а) адамдар тобының алдын ала сөз байласуы бойынша не ұйымдасқан топпен жасалса;

б) бірнеше рет жасалса;

в) бұрын компьютерлік ақпаратқа заңсыз кіргені үшін, ЭЕМ үшін зиянды бағдарламаларды жасағаны, пайдаланғаны, таратқаны үшін сотталған тұлғамен жасалса,

– екі жылдан бес жылға дейінгі мерзімге мүлкі тәркіленіп немесе онсыз бас бостандығынан айыруға жазаланады» [117].

2009 жылы 10 желтоқсанда тағы бір келесі өзгерістер қабылданды. Ол өзгерістерге сәйкес ҚР Қылмыстық кодекстің 227-1-бабының 3-тармағының в) тармақшасы отандық қылмыстық заңнаманы жетілдіру мақсатында алынып тасталды [118].

Ал 2011 жылғы 18 қаңтардағы қабылданған Заңға сәйкес Қылмыстық кодекстегі 227-1-бабының тек санкциясы өзгеріске ұшырады, сол жылы және 2012 жылда тағы да жазаларға қатысты кішігірім өзгерістер болды. Аталған өзгерістер мен толықтырулар негізінде 227-1-бабы келесі редакцияда әзірше өзгеріссіз құқықтық функциясын жүзеге асыруда:

«227-1-бап: Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын, абоненттік сәйкестендіру құрылғысын құқыққа сыйымсыз өзгерту, сондай-ақ абоненттік құрылғының сәй-

кестендіру кодын өзгерту үшін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату.

1. Жасап шығарушының немесе заңды иесінің келісімінсіз ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын құқыққа сыйымсыз өзгерту, ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын құқыққа сыйымсыз жасау,

– екі жүзден бес жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға, не жүз жиырма сағаттан жүз сексен сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға, не бір жылға дейінгі мерзімге түзеу жұмыстарына жазаланады.

2. Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын өзгертуге немесе ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын жасауға мүмкіндік беретін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату,

– бес жүзден сегіз жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға, не бір жылдан екі жылға дейінгі мерзімге түзеу жұмыстарына, не екі жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.

3. Нақ сол әрекеттер:

а) адамдар тобының алдын ала сөз байласуы бойынша не ұйымдасқан топпен;

б) бірнеше рет жасалса;

в) ҚР 2009.10.12. №227-IV Заңымен алып тасталды,

– бір мыңнан екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға, не мүлкі тәркіленіп немесе онсыз, үш жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады» [119].

Осының барлығын көрсетіп отырғанымыз ақпараттық қылмыстар саласындағы құқық әлемінің қылмыс әлемінің өзгеруімен қатар қандай қарқында жетілгендігі немесе тым артта қалғандығы, оны әркім өзінше бағалауы тиіс.

Алайда 2014 жылы Жаңа Қылмыстық кодекстің қабылдануымен бұл мәселеге қатысты жақсы өзгеріс орын тапты. Ақпараттық құқық бұзушылықтарға жеке тарау бөлініп шықты.

Өткен ғасырдың 90-жылдары Қазақстанда болған компьютеризация қоғамда жаңа құқықбұзушылықтарға алып келеді. Ол құқық бұзушылық көздері тікелей компьютерлік құралдармен байланысты болды. Компьютерлік ақпараттың қауіпсіздігіне

қол сұғатын қоғамға қауіпті әрекеттердің жеке түрлерін криминализациялау қажеттілігі туындады.

Қылмыстық кодекске компьютерлік ақпаратқа заңсыз кіру, зиянды бағдарламаларды жасау, пайдалану және тарату, ұялы байланыстың абоненттік құрылғыларының IMEI-кодтарын заңсыз өзгерту немесе ұялы байланыс абонентінің SIM-картасын өзгерту, сонымен қатар осы мақсаттарда арнайы компьютерлік бағдарламаларды жасау, пайдалану және тарату нормаларын енгізу аталған әрекеттерді өз қылмыстық-құқықтық қорғау объектілері бар қылмыстың жеке түрлері ретінде тану дегенді білдіреді.

Компьютерлік қылмыстардың тарихы отандық қабылдау шегінде осындай болып отыр. Әзірше зерттеу жұмысының маңызды бөлімінің бірі халықаралық байланыс, қарым-қатынас және ынтымақтастық мәселелеріне бет алсақ.

Қазіргі кезде халықаралық компьютерлік қылмыстар фактісі кең тарауда. Әсіресе көп кездесетін компьютерлік алаяқтық, қылмыспен табылған ақшаны заңдастыру үшін компьютерлік техниканы пайдалану, хакерлердің (компьютерлік желіге заңсыз кіретін тұлға) халықаралық ақпараттық жүйелерге кіруі және ақпаратты ұрлауы. Осы мәселеден көріп отырғандай, халықаралық қылмыстарды тергеу кезінде көмек болатын халықаралық процедуралар қажеттілігі және Интерпол шегінде жұмыс істейтін органды ұйымдастыру қажеттігі туындауы негізді.

Бүгінгі таңда әлем бойынша жоғары ақпараттық технологиялар саласында кездесетін құқық бұзушылық әрекеттерін криминализациялау мәселелерінің үш бағыты бар.

Бірінші топқа компьютерлік жүйелерге, олардың қорғаныстағы ақпараттарына заңсыз кіру әрекеттері, вирустармен жұқтыру шаралары, компьютерлік ақпарат пен мәліметтерді заңға қайшы пайдалану жатады. Мұндай бағыт Норвегияға, Сингапурге, Словакияға, Филиппиндерге, Оңтүстік Корей елдеріне тиесілі.

Екінші бағытқа компьютерлік қылмыс ретінде тек мүлікке және ақпаратты электронды өңдеуге зиян келтірумен байланысты әрекеттерді тануды жатқызамыз. Ол Австрия, Дания, Швеция, Швейцария және Жапон елдеріне тән. Мысалы, Австрия мен Дания елдерінде тұлға қылмыстық заңнама негізінде жауапқа ақпараттық-есептеу жүйесінің қызметіне қол сұққан жағдайда ғана тартылады.

Ал соңғы, яғни үшінші бағыт жоғары ақпараттық қамту мен жоғары компьютеризация дәрежесі орнаған құқықтық елдер тарапын білдіреді. Бұл елдерде криминализациялауға тек мүліктік зиянмен байланысты құқықбұзушылықтар ғана емес, жеке тұлғаның құқықтары мен мүдделеріне қарсы, ұлттық қауіпсіздікке қауіп төндіру әрекеттері, үлкен және кішігірім ұйымдарға қарсы қауіпті әрекеттер жатады. Мысалы, Ұлыбритания қылмыстық құқығы нормалары мазмұнынан біз қылмыстық санкция электронды есептеуіш құрылғылар арқылы немесе олардың желілері арқылы зиян келтірген немесе ақпаратты басқа өз мақсаттарында пайдаланған құқықбұзушыларға қатысты қолданылатынын көреміз. Ал Германияда компьютерлік қылмыстар санатына жоғары технологиялар саласында жасалған барлық заңға қайшы қылықтарды жатқызады және саралау кезінде компьютер қылмыстық әрекеттің объектісі немесе құралы болғанына ерекше қарамайды.

Мұндай тектес қылмыстарды көбінесе арнайы фирмалардың, банктердің және басқа да ұйымдардың өз қызметкерлері жасайды, нәтижесінде жасырын түрде ұйымның экономикасына қомақты қаржылық шығын келтіріледі. Мысалы, компьютерлік қылмыстардың шартты Отаны болып табылатын Америка Құрама Штаттарында бір жылдың ішінде келтірілетін компьютерлік саладағы қаржылық шығындардың сексен пайызға жуығы сол зиян шеккен ұйымдарда істейтін қызметкерлермен байланысты.

Қазақстанда да өзіндік тенденция бар. Мысалы, 2000 жылы Лондонда қазақстандық азаматтар О. Зезов пен И. Яримак заңсыз жолмен компьютерге кірген үшін, «Bloomberg LP» компаниясының сауда бөліміне қаржылық зиян келтіру мақсатында қиянаттық жасағаны үшін құқыққорғау органдарымен ұсталған болатын. Шантаж (масқаралық) сомасы 200 мың доллар көлемінде болған. Олар ақша сомасын алу кезінде әуежайда ұсталғанды. Бұл Қазақстанның азаматтары осы компанияда мәліметтер базасын жасау бөлімінде жұмыс жасап жүріп, заңсыз ойларын жүзеге асыру мақсатында өздеріне қажетті мәліметтерді сол компанияның қабырғасында жинастырған.

Қорыта келгенде жалпы айтатынымыз компьютерлік қылмыстардың көпшілігі жер шарын басып алған глобалды компьютер, Интернет желілерінде жасалатынын ескерсек, соңғы онжылдықтар ішінде әртүрлі елдер арасында заңшығару және құқық-

қолдану тәжірибесінде осы жаңа қылмыстылық түріне қатысты халықаралық қатынастар белсенді дамып келе жатыр. 1996 жылы Парижде Экономикалық қатынас пен дамуды ұйымдастыру жұмысымен айналысатын сарапшылар тобы компьютерлік қылмысқа анықтама берген еді. Олар былай деді: «компьютерлік қылмыс дегеніміз – автоматтандырылған мәліметтерді өңдеуге не беруге қатысты кез келген заңсыз, әдепсіз немесе тыйым салынған жүріс-тұрыс әрекеті».

Қазақстанның киберқылмыстылықпен күресудегі шет елдермен қарым-қатынасын және өздігінше даму тарихын қарастыра отырып, құқықтық тұрғыдан шет елдермен байланысын пост скриптум ретінде шолып өтелік. Осы талдау ақырында келесі тақырыпты жалғастырушы кезеңі ретінде рөл атқарады.

Қазіргі заман халықаралық қатынастар жүйесінің трансформациясымен және қозғалмалы глобальды ағымдармен сипатталады. Интеграция және мемлекеттердің экономикалық және саяси жағдайы шарттарында ақпараттық факторлар үлкен рөл атқаратын жан-жақты басқару механизмдері жақсартылады. Ақпараттық саланың дамуы қоғам мен мемлекеттің дамуына әсер ететін басты факторлердің біріне айналып келеді. Ақпараттық қоғамның даму дәрежесіне байланысты мемлекет экономикасы мен қорғаныс мүмкіндіктері, мемлекеттің институттарының функционалдық қызметі жұмыс істейді.

Қазіргі заманауи мемлекеттің өзін-өзі басқару қабілеттілігінің қажетті талабы болып ақпараттық қоғам азаматтарының тұтыну көрсеткішінің сәйкес келуі табылады. Сонымен бірге, технологиялық эволюция өзінің пайдасымен бірге, мемлекеттерге ақпараттық қауіпсіздік қаупі мен жаңа мәселелерді тудырады. Бұл кері қайтпалы үдеріс.

Қазіргі таңда жаһанды бәсекелестік жағдайында ақпараттық қысым мемлекетаралық қатынастарда туындайтын қақтығыстарды шешу үшін пайдалы құралға айналды. Барған сайын экстремистік және террористік ұйымдар өздерінің идеологияларын тарату, үгіттеу және жариялау үшін, радикалды идеяларын тарату үшін, өз қатарына адам санын қосу, оларды үйрету үшін, олармен байланыс жүргізу және қаржыландыру үшін глобальды ақпараттық-коммуникациялық желілерді пайдаланып келеді. Мемлекеттердің ақпараттық жүйелері террористік әрекеттердің

әдіс-тәсілдері болып келетін компьютерлік шабуылдардың қаупіне шалдығуы мүмкін.

Қылмыстық мақсатта ұйымдасқан ұлтаралық қылмыстық топтар қазіргі ақпараттық-коммуникациялық технологияларды пайдалануда белсенділік танытып келеді. Киберқылмыстылықтың динамикасы ауқымды қарқынмен өсіп өзгеріп келеді. Сонымен қатар, ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалған қылмыстардың тіркелген саны өскенімен, ресми статистика компьютерлік қылмыстардың таралуы жөнінде шынайы объективті жағдайды көрсете алмайды, себебі нағыз жасалған қылмыстардың тек жарым бөлігі ғана белгілі болатынын сан алуан айтқан болатынбыз. Киберқылмыстардың ерекшелігі болып олардың жоғары латенттілігі табылады, яғни қылмыс жасаудың жаңа әдістерінің пайда болуы оларды дәлелдеудің керекті құқықтық, ұйымдастырушылық және техникалық құралдырының тапшылығы себебімен қиыншылықтар туғызады. Сондықтан киберқылмыстармен күресу тиісті мемлекеттік жедел әсер ету қызметтері, арнайы қызметтерінің және құқыққорғау органдарының біріккен іс-әрекеттеріне деген қажеттілікпен шартталады. Сол себепті «киберқылмыстармен күресуге бағытталған трансұлттық органдар мен ұйымдар қызметіне жұмысқа тартуға болатын өкілдер мен ұлттық кадрларды, өз кезегінде, дайындауды қажет ететін, киберқылмыстармен күресті қадағалайтын және жүзеге асыратын жаңа органдар мен ұйымдар жасау туралы үлкен сұрақ» [120, 28-33 б.] Ресей мен Қазақстанның ғана емес басқа да мемлекеттердің көкейтесті мәселесі болып отыр. Қазақстанда киберқылмыстарды анықтау, алдын алу және тергеу бойынша жұмыстарды және жоғары технологияларды пайдалану арқылы жасалатын қылмыстарды жүргізуді 2003 жылы Ішкі істер министрлігі құрамында құрылған «К» басқармасы жүзеге асырады. Киберқылмыстармен жүйелі түрде күрес жүргізу үшін ақпараттық технологиялар саласындағы қылмыстармен күресу бойынша Ұлттық байланыс пункті құрылған болатын. Ол ТМД елдері және таяу шет елдерімен мәліметтер мен ақпараттарды алмастыруды жүзеге асырады.

Ақпараттық қауіпсіздік саласындағы жоғары білікті кадрлік қамтамасыз ету киберқылмыстармен күрес жүргізудің нәтижесіне әсер ететін негізгі факторлардың бірі болып табылады және де ақпараттық қауіпсіздік пен компьютерлік қылмыстармен күресу-

ді қамтамасыз ету саласында жұмыс атқаратын мамандардың біліктілігін көтеру, білім берудің үдерісі мен амалдарын жетілдіру қажеттілігі орын алып отыр.

Киберқылмыстылыққа қарсы іс-әрекеттердің тиімділігіне мемлекеттегі ақпараттық саланы құқықтық қамтамасыз етудің жетілмегенділігі әсер етеді, сол себепті, біздің ойымызша, келесі мәселелерге аса көңіл бөлген дұрыс болар:

– түрлі санаттағы ақпараттарды, ақпараттық ресурстарды, өнімдерді, қызметтерді тұтыну, алу, іздеу кезінде туындайтын ақпараттық құқықтық қатынастарды реттейтін құқықтық механизмдер;
– ақпараттарды, ақпараттық ресурстарды, ақпараттық өнімдерді және ақпараттық қызметтерді өндіру, беру және тарату процестерін реттейтін құқықтық механизмдер;
– ақпараттық жүйелерді, олардың желілерін, қамтамасыз ету құралдарын, телекоммуникациялық инфрақұрылымын жасау және қолдану кезінде пайда болатын ақпараттық құқықтық қатынастарды реттейтін құқықтық механизмдер.

Жоғары жауапкершілік ҚР ҚК-нің 205-213 баптарының ауырлататын тармақтары бойынша «егер іс-әрекет адамдар тобымен алдын ала келісу арқылы жасалса немесе ұйымдасқан топпен не өз қызмет бабын пайдалану арқылы тұлғамен жасалса және ауыр салдар туындаса» қарастырылды.

Өзбекстанның қылмыстық заңнамасында Қылмыстық заңның «Информатизация ережелерін бұзу» қылмыс құрамы (174-бап) меншікке қарсы қылмыстарға кіргізіліп Өзбекстан Қылмыстық кодексінің «Бөтен мүлікті талан-таражға салу» тарауына жатқызылған.

ТМД елдерінің және Кеңестен кейінгі кейбір елдердің қылмыстық заңнамаларында киберқылмыстардың топтық объектілері әртүрлі анықталған. Ресейдің Қылмыстық кодексінде (28-тарау, 272-274-баптар), Әзірбайжанның (30-тарау, 271-273-баптар), Қырғызстанның (28-тарау, 289-291-баптар), Түркменстанның (33-тарау, 333-335-баптар), Арменияның (IX бөлім, 24-тарау, 251-257-баптар) және Эстонияның («Компьютерлік ақпарат саласындағы қылмыстар» тарауы, 268-274-баптар) жеке тарауларында немесе бөлімдерінде компьютерлік ақпарат саласындағы қылмыстар үшін қылмыстық жауапкершілік туралы нормалар біріктірілген (компьютерлік ақпараттың қауіпсіздігі –

Арменияның Қылмыстық кодексі). Беларусь (XII бөлім, 31-тарау, 349-355-баптар) және Тәжікстан (XII бөлім, 298-304-баптар) қылмыстық заңнамасы киберқылмыстардың топтық объектісі ретінде ақпараттық қауіпсіздікті қоғамға қауіпті іс-әрекеттерді «Ақпараттық қауіпсіздікке қарсы қылмыстар» атты бір тарауға біріктіріп көрсеткен.

Киберқылмыстардың топтық объектілерін анықтауға байланысты Грузия (35-тарау «Компьютерлік қылмыстар», 284-286-баптар) мен Молдованың («Информатика саласындағы қылмыстар» тарауы, 259-261-баптар) Қылмыстық кодекстерінде қиыншылықтар туындайды.

Украинаның Қылмыстық кодексі бойынша ЭЕМ-ді (компьютерлерді), жүйелерді және компьютерлік желілерді пайдалану саласында қатынастар топтық объект болып және қоғамға қауіптілігі XVI тарауда «Компьютерлерді, ЭВМ-ді пайдалану саласындағы қылмыстар» (361-363-, 361-1-, 361-2-, 361-3-баптар) қарастырылған.

Мемлекеттердің киберқылмыстар үшін жауапкершілік саласындағы ұлттық қылмыстық заңнамаларды талдау көрсеткендей санқилылықпен сипатталады. Жоғарыда аталған мемлекеттердің киберқылмыстармен күресу бойынша ұлттық заңнаманың дамуы және өзгеруі киберқылмыстардың пайда болуы мен тенденцияларымен шартталған және тек нақты талдау жасау кезінде ғана кейбір заңдылықтар анықталады.

Ақпараттық технологиялардың дамуы және олардың адам тіршілігінің көптеген аясына енуі жаңа қылмыстық құқықбұзушылықтардың нысандарының пайда болуына алып келеді, сонымен бірге олармен күресудің тиімді шараларын өндіруге, жаңа іс-әрекеттерді криминализациялауға, жаңа нормалар мен қолданыстағы заңнамаға өзгеріс енгізуге қажеттілік тудырады.

Сөзсіз, егер бір елде заңсыз іс-әрекет криминализацияланған болып, екіншісінде қылмыстық жауапкершілік қарастырылмаған болса, киберқылмыстармен күресуде тиімді халықаралық қарым-қатынас жүргізу мүмкін емес. Мемлекеттердің ұлттық қылмыстық заңнамаларында бірқалыптылықтың болмауы шекарасы жоқ құбылыс болып табылатын киберқылмыстармен тиімді күресудің әдістеріне кері әсерін тигізеді.

Жаһанды ақпараттық желілер ақпараттық кеңістіктің шекараларын түбегейлі жойып тастады, сондықтан киберқыл-

мыскерлер мемлекеттердің виртуалды шекараларын жеңіл өтіп жатады және мемлекеттің юрисдикциясына қарамастан компьютер мен Интернетті пайдалану арқылы жердің кез келген нүктесінен қылмыстық әрекет жасайды. Шынында, осы ерекшелік киберқылмыскерлерді тергеуден сақтап қалады, сол арқылы олар жауапкершіліктен тыс болады. Сол себепті киберқылмыстардан өз азаматтарын қорғау үшін күш-жігерін жұмсайтын мемлекеттер уақыттарын бос өткізеді. Басқа жағынан өз мемлекетінің заңдарын сақтап жүрген азамат басқа мемлекетте жауапқа тартылуы мүмкін. Осындай жағдай ақпараттық технологиялар саласындағы қылмыстық-құқықтық қатынастарды реттеу саласындағы ұлттық заңнамаларды унификациялауды және киберқылмыстармен күресудің халықаралық стратегиясын жасауды негізге алады.

Сонымен қатар компьютерлік қылмыстармен күрес жүргізу бойынша кез келген тұрғыдан алдыңғы қатарлы мемлекет болатын Америка құрама штаттарының аталған қылмыстарды тергеу бойынша халықаралық байланысы жоғары дәрежеде. АҚШ-та компьютерлік қылмыстармен күресуді «Киберқылмыстылықпен күресу Агентігінен» басқа шамамен онға жуық басқа органдар, ведомстволар немесе жеке ұйымдар жүзеге асырады. Олар: Ұлттық қауіпсіздік агенттігі, Орталық қауіпсіздік қызметі, Орталық тергеу агенттігі, Тергеудің федералды бюросы, Жоғары технологиялық қылмыстарды тергеу ассоциациясы, Интерпол, Құрама штаттар құпия қызметі, Ғаламтор қылмыстары бойынша ұлттық полиция одағы, Ақпараттық қауіпсіздік жедел іздестіру орталығы, Құрама штаттарының қорғаныс министрлігі және басқалары. Осылардың барлығы өзімен одақтас елдер мен басқа да елдердің органдары мен қызмет түрлерімен үнемі байланыста жұмыс атқарады.

3.2. Компьютерлік қылмыстылықпен күресудегі тәжірибелі мемлекеттердің қылмыстық-құқықтық саясаты мен әдіснамасы

Халықаралық қатынастарды жалғастыра отырып компьютерлік қатынастармен күресу саласындағы шетелдік және халықаралық заңнамаларды қарастырып зерттедік.

Осы саладағы қылмыстылықпен күрес жүргізу аясында әрине барлық шет елдердің тәжірибелері мен құқық базасын баурап алу мүмкін емес, сондықтан зерттеу жұмысының негізінде бізге қызықты деген және қажетті деген елдердің оптималды тәжірибелік көріністерінің заңдылық сипаттарын талдауға салып көрелік.

Германия Федеративтік Республикасының ақпараттық қылмыстармен күресу саласындағы қылмыстық заңнамасы. Қазіргі кезде Германияда қолданыста сол 1871 жылы қабылданған Жалпы және Ерекше бөлімдерден тұратын, тараулардан, бөліктерден және параграфтардан тұратын Қылмыстық кодекс. Ерекше бөлімі 30 жеке тараудан құралған қылмыстың жеке түрлері үшін жауаптылықты бекіткен арнайы қылмыстық-құқықтық нормалармен, заңнамалармен толықтырылған [121, 352 б.].

Германияда заңшығару және заң ғылымы бойынша қылмыс құрамы деген ұғым болмайды, оның орнына «іс-әрекеттер құрамы» деген термин пайдаланады. Сол себепті талдау жүргізу кезінде компьютерлік қылмыстарды неміс көзқарасы жағынан компьютер саласындағы заңға қайшы іс-әрекеттер құрамы деп немесе жай ғана киберқылмыстар (cybercrimes) деген орынды болады.

Германия Қылмыстық кодексінде Қазақстанның Қылмыстық кодексі секілді компьютерлік ақпаратқа қол сұғатын қылмыстарды жасағаны үшін қылмыстық жауаптылықты қарастыратын жеке тарау жоқ. Дұрысы Қазақстанның Қылмыстық кодексі Германияның Қылмыстық кодексі сияқты деген жөн болар, бірақ сөз нақты Германия қылмыстық заңнамасы туралы болғандықтан, осы елдің кодексін негізге алып салыстырып жатырмыз.

Компьютерлік қылмыстарға қатысты арнайы тараудың болмауы Герман заңшығарушыларының бұл мәселеге толыққанды көңіл бөлмегендігі деп түсінген дұрыс емес, себебі киберқылмыстылық бұл елде басты және өзекті мәселелердің бірі және осы мәселелермен күресу бойынша Германия алдыңғы қатарлардың бірі болып отыр.

Германия Федеративтік Республикасында Қылмыстық кодекс бойынша келесідей заңға қайшы іс-әрекеттер құрамдары бар.

Біріншісі, 263а-параграфы – компьютерлік алаяқтық. Аталған параграф заңнаманың 22-і «Алаяқтық және сенімге қиянат жасау» бөлімінде бекітілген. Компьютерлік алаяқтық болып, Германия қылмыстық заңнамасы бойынша, басқа тұлғаның мүлкіне

зиян келтіру жолымен жасалатын, мәліметтерді өңдеу нәтижесіне бағдарламаларды дұрыс емес жасау арқылы, дұрыс емес және толық емес мәліметтерді пайдалану арқылы, мәліметтерді заңсыз пайдалану арқылы немесе мәліметтерді өңдеу нәтижесіне басқа да заңсыз әрекеттер арқылы әсер етумен қабаттасқан пайдакүнемдік іс-әрекеттер танылады [122, 149 б.].

Бұл жағдайда қылмыстық қол сұғушылықтың объектісі ретінде меншік қатынастары танылады, ал компьютер қылмыс жасаудың құралы болып табылады. Өйткені қылмыс жасаудың объективтік жағының жүзеге асыру нысандары пайдакүнемдік мақсаттарға жетудің жолдары болып тұр. Соның ішінде қылмыстық жауаптылық компьютерлік ақпараттың сипаты мен түріне қарамай туындай береді.

Аталған қылмыс құрамын талдай отырып, компьютерлік алаяқтық Германия Қылмыстық кодексінің 263-і параграфындағы әдеттегі алаяқтыққа өте ұқсас екенін байқаймыз. Бір ғана ерекшелік бар, ол бойынша қарапайым алаяқтық қылмысы дұрыс емес фактілерді жеткізу жолымен, фактілерді жасыру не өзгерту арқылы және жәбірленушіні немесе басқа адамдарды шатысуға, алдануға душар ету немесе соған келтіру арқылы жасалады. Қылмыстық іс-әрекеттің қоғамға қауіптілік сипаты мен дәрежесінің көрсеткіші болып табылатын санкцияларды салыстыра отырып алаяқтықтың екі түрі де қауіптілік дәрежесі бойынша бір-біріне жақын. Қорыта айтатын болсақ, Германия қылмыстық заңдылығы бір-бірінен тек жасалу әдісі бойынша ғана ерекшеленетін екі алаяқтықты, яғни қарапайым алаяқтықты және компьютерлік алаяқтықты қарастырған.

Германия Қылмыстық кодексінің «Мүлікті бүлдіру» 27-тарауында компьютерлік ақпаратқа қол сұғатын қылмыстар үшін жауаптылықты қарастырған екі іс-әрекет құрамы бар. 303а-параграфы мәліметтерді өзгерту. Аталған қылмыстық-құқықтық норма бойынша жауаптылыққа мәліметтерді заңсыз жойған, бұзған, жарамсыз күйге келтірген немесе өзгерткен тұлға тартылады [123, 167 б.].

Біріншіден, мағынасы жағынан, аталған қылмыстың пәні ретінде тек компьютерлік ақпарат табылмайды, сонымен қатар компьютерлердің ақпараттық тасымалдауыштарында бекітілген немесе сақталған ақпараттар және мәліметтер де болады. Екіншіден, құқықтық қорғау режимі бойынша ақпарат бұл жағдайда

мүлікке теңестіріледі. Оның дәлелі ретінде мүлікке зиян келтіргені үшін жауаптылық қарастырылған норма мен мәліметтерді бұзғаны үшін жауаптылық бар нормаларды және олардың санкцияларын талдау атқарады. Объективтік жағы мәліметтерді заңсыз жою, өзгерту, бұзу әрекеттерінен байқалады.

303-параграф «Компьютерлік іріткі (саботаж)». Қылмыстық жауаптылыққа бөтен ұйымның, ұжымның немесе органның қызметіне маңызды мәліметтердің өңделуіне зиян келтірген тұлға тартылады. Зиян келтіру бұл жағдайда мәліметтерді өңдеудің немесе ақпаратты тасымалдауыштың жұмысын бұзу, зақымдау, істен шығару, жарамсыз қалыпқа келтіру, өзгерту және жою арқылы жасалады [124, 167 б.].

Компьютерлік іріткі мәліметтерді өзгертуден объективтік және субъективтік белгілермен ерекшеленеді. Объективтік белгіге компьютерлік іріткі кезінде мәліметтерді өзгертуден басқа мәліметті өңдеу мен ақпаратты тасымалдауыш үшін құрылғы жұмысын бұзу, зақымдау, жарамсыз жағдайға келтіру, жою және өзгерту әрекеттері жатады. Аталған норма жәбірленушілердің тек белгілі бір санаттарына қатысты мүдделерін қорғауға бағытталған. Олар: ұйымдар, мекемелер мен органдар. Компьютерлік іріткі жасаған тұлға аталған объектілердің қызметкері болмауы тиіс. Ал мәліметтерді өзгерту кезінде жәбірленуші ретінде кез келген тұлға (заңды және жеке тұлғалар) таныла береді.

Сонымен, Германия мемлекетінің қылмыстық заңнамасына жасалған талдаудан анықтағанымыз, компьютерлік қылмыстарға қарсы қылмыстық-құқықтық шаралар жәбірленуші тарапына қатысты мүліктік мүдделерге зиян келтірмеу мақсатын бастапқылар қатарына қойып ұстанады.

Аталған нормалар бойынша жаза тағайындау Еуропалық Кеңес ұстанған ізгілік қағидаларына сәйкес келеді. Қоғамға қауіптілік дәрежесі бойынша компьютерлік қылмыстар үшін бас бостандығынан айырумен байланысты емес жаза түрлері басымдыққа ие. Ал компьютерлік құралдарды қолдану арқылы жасалатын қылмыстар үшін бас бостандығынан айыру жазасының мөлшері неғұрлым жоғары, себебі Германия қылмыстық заңнамасы бойынша олардың қоғамға қауіптілігі дәрежесі мен сипаты елеулі болып отыр.

Қытай Халық Республикасының (ҚХР) Қылмыстық заңнамасы. Қытайда қазіргі таңда 1979 жылы қабылданған Қылмыс-

тық кодексі қолданыста. Қытай мемлекеті мен қоғамының өмірінде және жалпы дүние жүзіндегі Қытай елімен тығыз байланысты соңғы 20 жылдан астам уақытта болған техникалық, технологиялық, ғылыми, экономикалық, әлеуметтік, саяси өзгерістер Қытайдың заңшығару билігі тарапынан Қылмыстық кодекс құрамына үлкен өзгерістер енгізу қажеттігін тудырды. Сол себепті 1997 жылдың 14 наурызында Қытай Халық Республикасының заңшығару билік тармағы Қылмыстық кодекске біршама толықтырулар мен өзгерістер енгізді.

Қытайлық мамандардың айтуынша, компьютерлік технологиялардың тез қарқынды дамуы компьютерлік қауіпсіздік пен ақпараттың құпиялығын қамтамасыз етуді қажет етеді. Ел алдында басты мақсат ақпараттық конфиденциалдылықты сақтау болып тұр. Осы мамандардың ұсыныстарына мемлекет тарапынан қолдау болмауы себебінен компьютерлік жүйе мен желілер арқылы тарайтын құпия мәліметтердің таралуы мен жариялануы қаупі жоғары болмақ [125, 161 б.].

Ақпараттық қылмыстарға қатысты Қылмыстық заңнаманың нормалары санаулы. Барлығы заңнаманың «Қоғамдық тәртіп пен басқару тәртібіне қарсы қылмыстар» атты 6-тарауында бекітілген.

285-бап. Мемлекеттік маңызды ақпараттық жүйелерге, қорғаныс құрылымдарына, ғылым мен техника салаларының алдыңғы қатарларына мемлекетпен анықталған компьютерлерге кіру тәртібі ережелерін бұзу.

286-бап. Мемлекетпен анықталған ережелерді бұза отырып компьютерлік ақпараттық жүйелердің функцияларын жою, бұзу, өзгерту, толықтыру, бөгеттеу әрекеттері нәтижесінде компьютерлік ақпараттық жүйелердің дұрыс жұмыс істеуіне тосқауыл болған ауыр және аса ауыр салдар туындаса.

Мемлекетпен анықталған ережелерді бұза отырып компьютерлік ақпараттық жүйелердің функцияларын жою, бұзу, өзгерту, толықтыру, бөгеттеу бойынша компьютерлік ақпараттық жүйелерде сақталған, өңдеуде болған немесе тасымалдау кезінде қолданбалы бағдарламалардағы мәліметтерге қатысты операциялар жүргізілген жағдайда ауыр салдар туындаса.

Қасақана түрде компьютерлік жүйелердің қызмет етуіне әсер ететін компьютерлік вирустарды немесе басқа да зиянды

бағдарламаларды жасау, тарату, нәтижесінде ауыр салдар туындаған жағдайда.

287-бап. Қаржылық алаяқтық, ұрлық, сыбайлас жемқорлық, қоғамдық құралдарды және қаражаттарды мақсатсыз пайдалану, мемлекеттік құпияларды ұрлау немесе компьютер арқылы жасалған басқа да қылмыстар, аталған Қылмыстық кодекстің тиісті ережелеріне сәйкес сараланады және жазаланады [126, 353-354 б.].

ҚХР IP-желілерді қатаң бақылау мақсатында барлық мүмкін шараларды жүргізіп жатыр, сонымен бірге қадағалау мен бақылау жүргізу шараларын ауырлату үшін үнемі түрде тиісті нормативтік актілер мен жаңа бұйрықтар беру үстінде.

ҚХР-дың Қылмыстық кодексінде орын тапқан 285-бап Қазақстан Республикасының Қылмыстық кодексінде көрсетілген 172-баппен біршама ұқсас. Басқаша айтсақ, қытайлық заңшығарушылар аталған норманы құрастыру кезінде компьютерлік ортада, қорғаныс құрылымдарында, ғылым мен техникалық салаларында айналымда жүрген мәліметтер мен ақпараттардың жасырындығын, құпиялығын қамтамасыз етуге ұмтылған. Ал компьютер құралы осы жағдайлар бойынша тек қылмысты жасаудың бір тәсілі түрінде ғана сараланып отыр.

286-баптың бірінші екі бөлімі ҚР Қылмыстық кодексіндегі «ЭЕМ-ын экплуатациялау ережелерін бұзу» қылмыс құрамына жақын. 286-баптың 1-тармағы бойынша қылмыстың пәні ретінде аппараттық жүйе ретінде компьютерлік жүйе танылады, яғни компьютерлік жүйенің дұрыс жұмыс жасауы компьютерлік ақпараттық қауіпсіздіктің қажетті шарты ретінде қарастырылған. 2-тармағының пәні болып тікелей компьютерлердегі мәліметтер табылады. Объективтік жағы бойынша қоғамға қауіпті іс-әрекеттерге ақпаратты жою, өзгерту, бөгеттеу жатады. Сонымен қатар, объективтік жақтың бір басты белгісі аталған қылмыстық іс-әрекеттерден ауыр және аса ауыр салдардың міндетті түрде туындауы.

Ал санкциясына келетін болсақ, жаза түрлері мен жаза мөлшері қазақстандық жазалау әдісінен сәл өзгеше. 286-баптағы қоғамға қауіпті іс-әрекеттерді жасағаны үшін тұлға бес жылдан жоғары мерзімге бас бостандығынан айыруға жазаланады. Яғни санкция төменгі жаза шегі көрсетілген түрі және ол 5 жылдан аз болмауы тиіс. Бірақ қытайлық қылмыстық заңнама негізінде

ең жоғары бас бостандығынан айыру жаза мөлшері 15 жылдан аспайды. Сонда ҚХР Қылмыстық кодексі бойынша 286-баптағы қылмыстық әрекетті жасаған адам 5 жылдан 15 жылға дейінгі мөлшерде бас бостандығынан айыру жаза түріне сотталуы мәлім. Қазақстан Республикасының қылмыстық және қылмыстық атқару заңдарымен салыстырғанда бұл, әрине, тым жоғары жазалау секілді көрінеді. Бірақ ҚХР заңдарының басты принциптері – ол қорқыту. Содан кейін ғана басқа ұстанымдар мен бағыттар жүзеге асады.

ҚХР ҚК 287-бабы қылмыстық кодекстің басқа қылмыстарының саралаушы белгісі болып табылатын норма. Ерекше белгісі 287-баптағы барлық қылмыстық әрекеттер компьютерлік техника құралын пайдалану арқылы жасалады немесе жүзеге асырылады.

Нидерланды (Голландия) Әмірлігінің Қылмыстық заңнамасы. Голландия Қылмыстық кодексі сонау 1886 жылдың 1-ші қыркүйегінен бастап қолданылып келеді, ол 3 томдық кітап түрінде жарияланған. 1-ші кітап – «Жалпы ережелер», 2-ші кітап – «Қылмыстар», 3-ші кітап – «Құқық бұзушылықтар немесе теріс қылықтар». Қылмыстар мен теріс қылықтар бөлімі қылмыс құрамының топтық объектілеріне байланысты тарауларға бөлінеді.

Қылмыстық кодекс байырғы болғанымен компьютерлік қылмыстарға қатысты 1993 жылы арнайы заң қабылданып, Нидерланды Әмірлігінің қылмыстық заңнамасына қосымша қылмыс құрамдары енгізілді.

Компьютерлік ақпаратқа қол сұғатын қылмыстар үшін жауаптылықты қарастыратын қоғамға қауіпті қылмыс құрамдары және осы құрамдарды сипаттайтын нормалар Голландық Қылмыстық кодекстің әртүрлі тарауларында орналасқан. Осы жағынан бұл Германия қылмыстық заңнамасына ұқсайды.

Голландиялық компьютерлік қылмыс құрамдарын жеке-жеке қарастырайық. Голландия Қылмыстық кодексінің 138а-бабы Қылмыстық кодекстің «Қоғамдық тәртіпке қарсы қылмыстар» атты 5-тарауында орналасып, жеке түрде 3 қылмыс құрамын сомдаған. 1-тармағы бойынша қылмыстық жауаптылық компьютерлік құрылғыға немесе мәліметтерді сақтау не өңдеу жүйесіне әлде осы құрылғы мен жүйенің бір бөлігіне қауіпсіздікті бұзу немесе технологиялық құралдардың арқасында кіруге рұқсат алу арқылы, арнайы жалған белгі, жалған кілттер мен парольдерді

және өкілеттіктерді пайдалану арқылы қасақана заңсыз кіргені үшін туындайды.

2-тармақ бойынша жауаптылық компьютерге заңсыз кірген үшін, егер нәтижесінде жеке мақсатта немесе басқа тұлғаға пайдалану үшін мәліметтер көшірілген жағдайда.

3-тармақ халыққа қызмет көрсететін телекоммуникациялық инфрақұрылым немесе ақпараттық телекоммуникациялық құрылғы арқылы компьютерге заңсыз кіргені үшін жауаптылықты қарастырған. Егер қылмыскер компьютерлік құралдың немесе жүйенің өңдеу мүмкіндігін өзіне пайда табу мақсатында пайдаланса және үшінші тұлғаның компьютеріне не компьютерлік жүйесіне заңсыз кіруді компьютерлік құрылғы немесе жүйе арқылы жүзеге асырса.

27-тарау «Жою немесе зиян келтіру» құрамында компьютерлік ақпарат пен қауіпсіздікке қол сұғатын екі норма бар. Голландия Қылмыстық кодексі 350а-бабының 1-тармағы былай дейді: тұлға жауапқа тартылады, егер ол компьютерлік құрал немесе жүйе арқылы берілетін, өңделетін, сақталатын ақпаратты қасақана түрде және заңсыз өзгертсе, өшірсе, жойса не жарамсыз күйге келтірсе, сонымен қатар қосымша мәліметтер енгізсе. Аталған негізгі қылмыс құрамының ауырлататын құрамы болып халыққа қызмет көрсететін компьютерлерге және телекоммуникациялық жүйелерге кіру арқылы және соларда сақталатын мәліметтерге нұқсан келтіру арқылы үлкен зардап келтірілген жағдайда жасалған болса табылады.

350а-баптың үшінші бөлімі бойынша, егер тұлға қасақана түрде және заңға қайшы мәліметтерді жойса немесе компьютерлік құрылғы мен жүйеде ақпаратты көшіру жолымен зиян келтіру үшін мәліметтерді таратса, жауапқа тартылады делінген. Осы баптың 4-тармағы жауаптылықты жеңілдететін жағдай рөлін атқарады. Тұлға қылмыстық жауаптылықтан босатылады, егер ол 350а-бабының 3-тармағындағы іс-әрекеттерден туындауы мүмкін зардаптарды болдырмау, жою, азайту, шектеу мақсатында шара қолданған болса.

Голландия Қылмыстық кодексінің 350и-бабы 1-тармағы бойынша тұлға абайсызда немесе немқұрайлық бойынша компьютерлік құрал мен жүйеде көшіру арқылы зиян келтіруге бағытталған мәліметтерді заңсыз жария етсе немесе таратса қылмыстық жауаптылыққа тартылады [127, 419-422 б.].

Аталған нормалардан басқа Голландия Қылмыстық кодексі бірқатар қылмыстық-құқықтық нормалардың құрамында (232-бап «Жалған банк карталарын жасау»; 317-бап «Қорқытып алушылық»; 362-бап «Ұрлық» және т.б.) компьютерлік құралдар мен жүйелерде жасалатын қылмыстар тізімін ауырлататын қылмыс құрамдары ретінде тіркеген.

Сонымен, Нидерланды Әмірлігінің Қылмыстық кодексі компьютерлік қылмыстарды реттейтін тек жеке нормалармен шектелмеген, басқа қылмыс түрлерінің қосымша ауырлататын құрамдарымен де әшекейленген. Мұның оңды да, солды да жақтары, дұрысы да, бұрысы да бар. Қазақстан Республикасының ұлттық қылмыстық заңнамасын жетілдіру мақсатында осы дамыған елдердің тәжірибелерін ескеру біз үшін жөнді нәрсе.

Франция Республикасының қылмыстық заңнамасы. Қазіргі кезде Францияда 1810 жылы қабылданған Наполеондық деп аталған Қылмыстық заңның орнына екі ғасыр таяулағанда келген 1992 жылғы қолданыстағы Қылмыстық кодекс іс-әрекет етеді. Заңды күшіне белгілі себептермен тек 1994 жылдың 1 наурызында енеді.

Франция Қылмыстық кодексі алты негізгі «6 кітап» деп аталатын, қылмыстық құқықтың мәселелерін реттейтін, қылмыстылық пен жазалауды (пенализацияны) анықтайтын бөлімнен тұрады. Алғашқы бірінші кітап Жалпы бөлімнің қызметін атқарады да, қылмыстық заң туралы ережелерден тұрады. Қалған бес кітап қылмыстық құқықтағы Ерекше бөлімі қызметін атқарады. Мысалы, адамға қарсы қылмыстар мен теріс қылықтар туралы, меншікке қарсы қылмыстар туралы, ұлтқа, мемлекетке және қоғамдық тыныштыққа қарсы қылмыстар туралы, басқа да қылмыстар мен олқылықтар, құқықбұзушылықтар туралы тараулар, бөлімшелер және нормалар.

Қылмыстық кодекстен басқа, Францияда қылмыстардың жеке түрлеріне қатысты жауапкершілікті қарастыратын жеке-жеке қылмыстық заң актілері бар.

Франция Қылмыстық кодексі компьютерлік ақпараттық қауіпсіздікке қол сұғатын қылмыстар үшін келесі нормаларды қарастырған: 323-1-бап. Мәліметтерді автоматты өңдеу жүйесіне толығымен не жартылай заңсыз кіру немесе онда заңсыз болу; 323-2-бап. Мәліметтерді автоматты өңдеу жүйесінің жұмысына

қарсы бағытталған іс-әрекеттер; 323-3-бап. Ақпаратты мәліметтерді автоматты өңдеу жүйесіне алдау жолымен енгізу не сол жүйеде сақталған мәліметтерді (ақпараттарды) жою немесе өзгерту.

323-4-бап. Аталған баптардағы әрекеттердің бірін немесе жиынтығы бойынша бірнеше қылмыстық әрекетті жасау үшін, алдын ала сөз байласқан топта немесе адамдар тобында әлде бірнеше адам жасаса [128, 125 б.].

Осы жоғарыда аталған қылмыс құрамдарының ішінде 323-1, 323-2, 323-3 баптары арнайы қылмыс құрамдары болатын секілді. Ал 323-4-бабы ауырлататын құрам түріне жатады, яғни бұл жерде осы қылмыстарды екі не одан да көп адамдардың жасауы орын алып отыр.

Мәліметтерді автоматты өңдеу жүйесіне толығымен немесе бір бөлігіне заңсыз кіру мәні бойынша компьютерлік ақпаратқа заңсыз кірумен тұспа-тұс келеді. Ерекшелік бұл жерде тек терминологияда болып отыр, француз заңшығарушылары өз нормаларында компьютерлік ақпарат ұғымына «мәліметтерді автоматты түрде өңдеу жүйесі» деген сөз тіркесін қолданған, ол біздің ЭЕМ (ЭВМ) сияқты электронды есептеу машинасы деген архаизмдік сөз тіркесі секілді заң нормасында қолданылып келеді. Бірақ Француз заң шығарушылары мен ғылым өкілдері осы мәселеге қатысты пікір білдіріп, терминология жөнінде жаңа ұғымдармен алмастыру ұсыныстарын жасап жатыр.

Франция Қылмыстық кодексінің 323-2-бабында қарастырылған қылмыс құрамы «компьютерлік іріткі салуды» білдіреді және Германия Қылмыстық кодексіндегі жоғарыда қарастырылған 303-параграфтың аналогы болып табылады. Ал Қазақстан Республикасының Қылмыстық заңнамасы бойынша «компьютерлік іріткі» құрамы көрсетілмеген.

Франция Республикасының Қылмыстық кодексінің 323-3-бабы компьютерлік алаяқтыққа арналған. Яғни компьютерлік алаяқтық қарапайым алаяқтықтан өзгеше норма ретінде қарастырылған және ерекшелігі қылмыстық әрекетті жасау тәсілінде болып отыр. Нақ осындай көзқарасты ГФР Қылмыстық кодексі ұстанған болатын [129, 56-58 б.].

Қазақстанда қолданыстағы заңнама бойынша компьютерлік алаяқтық мүлдем жоқ, тәжірибеде мұндай жағдайда қарапайым алаяқтық нормалары қолданылуы мүмкін, бірақ іс жүзінде көп

жүзеге асырыла бермейді. Ал ҚР Қылмыстық заңнамасын жетілдіру мақсатында жаңа редакцияда жобасын құрастыру кезінде компьютерлік алаяқтық қылмыс құрамын 190-баптың «Алаяқтықтың» ауырлататын құрамы ретінде саралау түрінде көрсеткен. Атауы 190-бап 2-тармақ 4)-тармақшасы «Ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану жолымен алаяқтық жасау», мәні мен сипаты бойынша нағыз Германия, Франция және басқа елдердегі «компьютерлік алаяқтыққа» ұқсайды.

Сонымен, осыдан көріп отырғанымыздай, әлемдегі ақпараттық жағдай мен салыстырмалы түрде еліміздегі осы мәселеге деген қарым-қатынас белгілі болып отыр. Сол себепті ойланатын кез ғана емес, шараларды жүзеге асыратын жай келді. Дамыған елдердің құқықтық тәжірибесін ескере отырып өзімізге тиесілі оңтайлы және пайдалы қолданбалы нәтижелерін алғанымыз дұрыс.

ҚОРЫТЫНДЫ

Мобильді дербес компьютерлер мен гаджеттер біздің күнделікті тұрмыста берік бекітілді. Жергілікті Интернет желілеріне қосылмаған компьютерлер мен компьютерлік жүйелерді қазіргі таңда елестету қиын, себебі кез келген заманауи құрал тікелей жаһандық желімен байланысты бағдарламалармен және қосымшалармен жұмыс істейді. Күн сайын Интернет қызметтерін пайдаланушылар саны үлкен қарқынмен артуда. Қазақстанда осы қызметтерді ұсынатын Интернет провайдерлер де аз емес. Дербес компьютерлерден басқа ұялы телефондар, смартфондар, қалта дербес компьютерлері, тіпті көлік құралдарының мультимедиялық жүйелері мен қосалқы құрылғылары сияқты байланыстың барлық мүмкін құралдарының саны да артып келеді. Жоғарыда, жаппай компьютерлендіру, ақпараттандыру және цифровизациялау процесінің жағымды жақтарынан басқа теріс ықпалы да бар екені аталып өткен болатын. Осындай салдардың бірі – ақпараттық қылмыстар.

Ақпараттық қылмыстармен күресу тиімділігіне мемлекеттегі ақпараттық саланың құқықтық қамтамасыз етілуі басты әсер етеді. Осыған байланысты әртүрлі санаттағы ақпаратты, ақпараттық ресурстарды, ақпараттық өнімдерді, ақпараттық қызметтерді қабылдау не тұтыну кезінде туындайтын ақпараттық құқықтық қатынастарды реттейтін құқықтық тетіктерді жетілдіруді; ақпаратты, ақпараттық ресурстарды, ақпараттық өнімдерді, ақпараттық қызметтерді өндіру және тарату процестерін реттейтін құқықтық мәселелерді, сонымен қатар ақпараттық жүйелерді, олардың желілерін, қамтамасыз ету құралдарын, телекоммуникациялық инфрақұрылымды құру және қолдану кезінде туындайтын ақпараттық құқықтық қатынастарды реттейтін ұйымдастырушылық-құқықтық салаларды жетілдіруді қажет етеді.

Қазақстандық қоғамда компьютерлік техниканы пайдалана отырып қылмыс жасау тек шетелдік елдерге тән құбылыс ретінде

қабылданған болатын. Алайда, аталған монографиялық еңбекте осындай тектес қылмыстар тек шет елдерде ғана емес, сонымен қатар біздің елімізде жиі кездесіп тұратыны мәлімделді. 2014 жылы қабылданған Қылмыстық заңнаманың Ерекше бөлімінде өз бетімен жеке жауаптылық қарастырып отырған 9 бап көрініс тапқан. Салыстырмалы түрде, 1997 жылғы заңнамада небәрі 2 ғана бап болатын және олар экономикалық қылмыстар құрамына кіріп кеткен еді. Осының өзі қоғамдағы заманауи өзгерістердің жылдам дамып бара жатқанын көрсетеді.

Жоғары ақпараттық технологиялар саласындағы құқық бұзушылықтарға қарсы күресті тиімді ұйымдастырудың маңызды шарты болып жасалатын заңға қайшы әрекеттердің ерекшелігін білу, тиісті қылмыстық ортада өтетін процестердің мәндік сипаттамаларын айқындау табылады.

Қазақстан аумағында тіркелген компьютерлік қылмыстар саны жыл сайын артып келеді. Сондықтан осы қылмыстарға қарсы күрес жөніндегі шаралар жүйелі түрде жүргізілуі тиіс. Қазақстан Республикасы компьютерлік қылмыстармен неғұрлым нәтижелі күресу үшін әлемнің көптеген елдерімен ынтымақтастық орнатқан болатын.

Бұл ғылыми зерттеу жұмысы барысында заң актілерін, заңдарды және арнайы әдебиеттерді талдай отырып, қарастырылып отырған мәселе бойынша ақпараттық құқықбұзушылықтар ұғымы жан-жақты талқыланып өткен. Соның нәтижесінде ақпараттық құқық бұзушылықтарға ғылыми тұрғыдан қорытынды дефиниция берілді. Яғни, ақпараттық (компьютерлік) құқық бұзушылықтар дегеніміз – қылмыстық заңнамамен анықталатын, машиналық ақпараттық қылмыстық қол сұғушылықтың объектісі болатын, ақпараттық заңға қайшы әрекет жасау кезінде компьютерлік сақтағыштағы немесе операциялық жадыдағы мәліметке немесе ақпаратқа қандай да заңсыз әсер ететін қоғамға қауіпті іс-әрекеттер жиынтығы. Бұл жағдайда құқық бұзушылықтардың заты мен құралы болып компьютерлік ақпарат, компьютер, компьютерлік желілер мен жүйелер, техникалық құралдар және қосалқы бөлімдер танылады.

Отандық заңнамадағы «Ақпараттандыру және байланыс саласындағы қылмыстық құқықбұзушылықтар» тарауындағы ақпараттық қылмыстар шет елдердің заңнамаларымен, атап

айтқанда Қытай Халық Республикасының, Францияның, Голландияның, Германия Федеративтік Республикасының, сондай-ақ бұрынғы Тәуелсіз Мемлекеттер Достастығы елдерінің, яғни көршілес елдердің заңнамаларымен салыстырмалы талдауға түсті.

Бұдан басқа, осы қылмыс түрлерінің объективті және субъективті белгілерін жан-жақты талдау жолымен компьютерлік қылмыстардың қылмыстық-құқықтық сипаттамасы жасалды. Сонымен қатар, ақпараттық құқық бұзушылықтардың криминологиялық сипаттамасы да қарастырылды. Қылмыскердің жеке басы зерттелді. Компьютерлік қылмыстарды жасауға ықпал ететін себептер мен жағдайлар анықталды. Компьютерлік қылмыстардың алдын алу шаралары әзірленіп ұсыныстар жасалды.

Ендігі көтеретін мәселе ақпараттық қауіпсіздік саласындағы құқық бұзушылықтар үшін жауаптылық мөлшерін көбейту және ..

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР

1 Қазақстан Республикасы Президентінің 2018 жылғы 5 қазандағы Қазақстан халқына жолдауы. – www.akorda.kz
2 Қазақстан Республикасы Президентінің 2006 жылғы 10 қазанда қабылданған «Қазақстан Республикасының ақпараттық қауіпсіздік концепциясы туралы» №199 Жарлығы.
3 ҚР 2014 жылғы Қылмыстық кодексінің 7-тарауы. – www.adilet.zan.kz
4 Гаврилов В.А. Компьютерные технологии в правотворческой деятельности: учебное пособие. – М.: Норма-Инфра, 1999.
5 Компьютерные преступления и обеспечение безопастности ЭВМ. Проблемы преступности в капиталистических странах. – М.: Винити, 1983. – №6. – С.3.
6 На скамье подсудимых – школьники-хакеры. // http://www.newsfactory.kz/index.php?do=art&id=25005.
7 Хакерские атаки. // http://www.if-safety.kz/profit.kz /Uralsk.info. – 2011.
8 Карпинский О. Защита информации, виртуальные частные сети. // Технология ВипНет (Инфотекс компаниясының мәліметтері бойынша). – 2001.
9 Францияның 1992 жылғы Қылмыстық кодексі.
10 Ресей Федерациясының 1992 жылғы «Электронды-есептеу машиналарының және мәліметтер базасының программаларын құқықтық реттеу туралы» Заңы.
11 Фигурнов В.Э. IBM PC для пользователя. – М.: ИНФРА-М-НОРМА, 1997. – С.14.
12 Компьютерные преступления и обеспечение безопастности ЭВМ. // Проблемы преступности в капиталистических странах. – М.: ВИНИТИ, 1983. – №6. – С.5.
13 Некоторые аспекты компьютерной преступности. // Проблемы преступности в капиталистических странах. – М.: ВИНИТИ, 1990. – №6. – С.12.
14 Назмышев Р.А. Методика расследования преступлений в сфере компьютерной информации: учебное пособие. – Костанай, 2007. – 156 с.
15 Элеонора Мелик. Компьютерные преступления: информационно-аналитический обзор // http://www.wse-wmeste.ru. – 1999-2013 Openstat. Все права защищены. – Т.1. – glava_1.html#_1_1.
16 www.melik.narod.com // www.crime-research.ru.
17 Россия: статистика компьютерной преступности. // http://www.google.kz. – computer crimes. / http://www.crime-research.ru/news/12.03.2004/2004-03-1202/.
18 Washington ProFile. – Cybercrimes. – 03.08.2007. – Computer crime research center.

19 Дулов А.В. Криминалистический анализ компьютерных преступлений. // Проблемы компьютерной преступности: – Минск: НИИ ПККСЭ МЮ РБ, 1992.– Вып. 2. – С.3-4.
20 Селиванов Н.А. Проблемы борьбы с компьютерной преступностью // Законность. – М., 1993. – №8. – С.37.
21 Крылов В.В. Информация как элемент криминальной деятельности. // Вестник Моск. ун-та. Сер. 11. Право. – М., 1998. – №4. – С.50-64.
22 Батурин Ю.М. «Компьютерное преступление» – что за термином? // Право и информатика. – М.: МГУ, 1990. – С.9.
23 Чуфаровский Ю.В. Криминология в вопросах и ответах: учебное пособие. – М.: ТК Велби, изд-во «Проспект», 2004. – 270 с.
24 Уголовное право России. Часть Общая / отв. ред. Л.Л. Кругликов. // 2-і басылым, өзгерістер мен толықтырулармен бірге. – М., 2005. – 1-тарау, § 1.7.
25 Франц Фон Лист. Задачи уголовной политики. Преступление как социально-патологическое явление. – М.: Инфра-М, 2008. – С.110.
26 Лопашенко Н.А. Уголовная политика. – М.: Изд. Вольтерс клубер, 2009. – 579 с.
27 Исмаилов И.А. Преступность и уголовная политика (актуальные проблемы борьбы с преступностью). – Баку, 1990. – С.124.
28 Миньковский Г.М. Политология борьбы с преступностью (вместо предисловия) к книге И.А. Исмаилова. Преступность и уголовная политика (актуальные проблемы борьбы с преступностью). – Баку, 1990. – С.7.
29 Недотко Ю.В. Тенденции российской уголовно-правовой политики постсоветского периода: автореф. – Челябинск, 2005. – С.6-7.
30 Чубинский М.П. Очерки уголовной политики (понятие, история и основные проблемы уголовной политики как составного элемента уголовного права). – СПб., 1905.
31 Босхолов С.С. Указ. соч. – 1999. – С.16.
32 Побегайло Э.Ф. Кризис современной российской уголовной политики // Уголовное право. – 2004. – №3.; Проблемы уголовной политики в сфере обеспечения безопасности жизни граждан (законотворческий аспект). // Уголовное право. – 2001. – №1; Психологические детерминанты криминальной агрессии. // Уголовное право. – 2002. – №1; Кризис современной российской уголовной политики. // Уголовное право. – 2004. – №4.
33 Дзигарь А.Л. Уголовная политика и ее отражение в теории, законодательстве и практике: дис. … докт. юрид. наук. – Рязань, 2007. – 489 с.
34 Загородников Н.И., Стручков Н.А. Направления изучения советского уголовного права. // Советское государство и право. – 1981. – №7. – С.4.
35 Гаухман Л.Д., Ляпунов Ю.И. Понятие советской уголовной политики и ее основные направления. – М., 1980. – С.4.

36 Беляев Н.А. Уголовно-правовая политика и пути ее реализации. – Л., 1986. – С.15.
37 Исмаилов И.А. Преступность и уголовная политика (актуальные проблемы организации борьбы с преступностью). – Баку, 1990. – С.100-101.
38 Панченко П.Н. Советская уголовная политика. // Общетеоретическая концепция борьбы с преступностью: ее становление и предмет. – Томск, 1988. – 90 с.
39 Босхолов С.С. Указ. соч. – 1999. – 32 с.
40 Беляева Л.И. Уголовная политика и ее реализация органами внутренних дел: учебник. – М., 2003. – С.7.
41 Дзигарь А.Л. Уголовная политика и ее отражение в теории, законодательстве и практике: дис. … докт. юрид. наук. – Рязань, 2007. – 490 с.
42 Жетібаев Н.С. Қылмыстық саясат және медицина қызметкерлерінің жауаптылығы. – Алматы: Қазақ университеті, 2011. – 155 б.
43 Глобализация человеческое измерение. – М.: РОССПЭН, 2002. – 380 с.
44 Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. // Монография. – Караганда: КВШ ГСК РК, 1995. – 320 с.
45 Лисицын С. Капли ИКТ на мозг homo sapiens. Раздел: общество. // Казахстанская правда. – Алматы, 2012. – июнь 23. – С.10.
46 Лисицын С. Капли ИКТ на мозг homo sapiens. Продолжение. Раздел: общество. // Казахстанская правда. – Алматы, 2012. – июнь, 23. – С.11.
47 Қазақстан Республикасы Президентінің 2006 жылғы 10 қазанда қабылданған «Қазақстан Республикасының ақпараттық қауіпсіздік концепциясы туралы» №199 Жарлығы.
48 Толығырақ қараңыз: Қазақстан Республикасы Президентінің 2011 жылғы 14 қарашада №174 Жарлығымен мақұлданған «Қазақстан Республикасының 2016 жылға дейінгі ақпараттық қауіпсіздік Концепциясы».
49 Криминология: учебник для вузов / под общ. ред. д.ю.н., профессора А.И. Долговой. – изд. 3-е, перер. и доп. – М.: Норма, 2007. – 736 с.
50 Батурин Ю.М., Жоджинский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 2006. – 186 с.
51 Лысов Н.Н. Содержание характеристики компьютерных преступлений // Проблема криминалистики и методики ее преподавания. – М., 2004. – 224 с.
52 1997 жылғы 16 шілдеде (167-I) қабылданған Қазақстан Республикасы Қылмыстық кодексі. // толықтырулар және өзгерістермен бірге. – Алматы: ЮРИСТ, 2012. – С.81.
53 Батурин Ю.М., Жодзинский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991. – 156 с.
54 Батурин Ю.М. Проблемы компьютерного права. – М., 1991. – С.115.
55 ҚазКСР Азаматтық кодексіне комментарий. – Алматы, 1990. – С.538.
56 Ожегов С.И. Талқылау сөздігі: «бір қалыпқа, стандартқа келтіру». – 1990. – Басылым 22. – 832 б.

57 Журнал «Советы Казахстана». – Алматы, 1992. – №18/2. – С.17.
58 Казанцев В.В. Криминалистическое исследование средств компьютерных технологий и программных продуктов. – М., 2008.
59 Қазақстан Республикасының 1995 жылғы 30 тамызда референдумда қабылданған Конституциясының 2-тарауы, 20-бабы.
60 Қазақстан Республикасының 1998 жылғы 26 маусымда қабылданған «Қазақстан Республикасының Ұлттық қауіпсіздігі туралы» №233-II Заңы.
61 Толығырақ қараңыз: Қазақстан Республикасының 2007 жылғы 11 қаңтарда қабылданған «Информатизация туралы» Заңы (2003 жылғы 8 мамырда қабылданған «Информатизация туралы» Заң күшін жойған).
62 Қазақстан Республикасының 1997 жылғы қабылданған Қылмыстық кодексінің 227-1-бабы.
63 Сеитов Т.Б. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане: учебное пособие. – Алматы: Дәнекер, 1999. – С.14.
64 Ожегов С.И. Модификация – «түрін өзгерту». – 22-басылым. – 1990. – 359 б.
65 Сеитов Т.Б. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане: учебное пособие. – Алматы: Дәнекер, 1999. – 134 б.
66 Нақтырақ қараңыз: Ресей Федерациясының Қылмыстық кодексі. Ресми мәтін. – М.: ИНФРА-М-НОРМА, 1996.
67 Қазақстан Республикасының 1999 жылғы 20 қаңтарда қабылданған ҚР Үкіметінің «ҚР-дың электрбайланыс желілеріндегі арнайы жедел-іздестіру шараларын жүргізуді қамтамасыз етуі бойынша шаралар туралы» №1937 Қаулысы.
68 Мазуров В.А. Компьютерные преступления: оқу-тәжірибелік құралы. – М.: Палеотип Логос, 2002.
69 Қазақстан Республикасының 1997 жылғы 16 шілдеде қабылданған №167-I қолданыстағы Қылмыстық кодексі.
70 Ағыбаев А.Н. ҚР Қылмыстық кодексіне түсіндірме. – Алматы: Жеті жарғы, 2010. – 807 б.
71 ҚР 3 шілде 2014 жылғы Қылмыстық кодексі. – http://adilet.zan.kz/kaz/docs/K1400000226.
72 Коммуникатор. // http://ru.wikipedia.org/wiki/communicator.
73 Крылов В.В. Информационные компьютерные преступления. – М.: Издательская группа «ИНФРА М-НОРМА», 1997. – 430 с.
74 Компьютер. // http://ru.wikipedia.org/wiki/Компьютер.
75 Қазақстан Республикасының 1999 жылғы 15 наурызда қабылданған «Мемлекеттік құпиялар туралы» №349-I Заңы. – Алматы: ЮРИСТ, 2009.
76 Қазақстан Республикасының 1994 жылғы 27 желтоқсанда қабылданған Азаматтық кодексі. // Жалпы бөлім. – Алматы: Юрист, 2011. – Б.128.

77 Қазақстан Республикасы Президентінің 1995 жылғы 31 тамызда қабылданған «Қазақстан Республикасындағы банктер және банктік қызмет туралы» № 2444 Жарлығы және Қазақстан Республикасының 2003 жылғы 6 наурызда қабылданған «Микронесиелік ұйымдар туралы» №392-II Заңы.
78 Қазақстан Республикасының 2008 жылғы 10 желтоқсанда қабылданған «Салық және бюджетке төленетін басқа да міндетті төлемдер туралы» №99-IV Кодексі (Салық кодексі).
79 Қазақстан Республикасының 1997 жылғы 16 сәуірде қабылданған «Психиатриялық көмек және көмек көрсету кезінде азаматтар құқықтарының кепілі туралы» №96-I Заңы. – «Параграф» ақпараттық жүйесі.
80 Қазақстан Республикасының 1994 жылғы 5 қазанда қабылданған «ЖҚТБ ауруының алдын алу туралы» №176-XIII Заңы.
81 Қазақстан Республикасының 1997 жылғы 5 желтоқсанда қабылданған «Адвокаттық қызмет туралы» №195-I Заңы (21.06.2012 жылғы өзгерістер мен толықтырулармен бірге).
82 IMEI // http://ru.wikipedia.org/wiki/imei.
83 Аманов Ж.К. Уголовная ответственность за преступления, посягающие на безопасность компьютерной информации. – Алматы, 2007. – 184 с.
84 Касперский Е. Компьютерные вирусы в MS-DOS. – М.: Изд-во «Эдэль», 1992. – С.172.
85 http://www.pitachok.net. – Хакинг. – 1-тарау.
86 Балапанов Е.Қ., Бөрібаев Б.Б., Дәулетқұлов А.Қ. Жаңа информациялық технологиялар: информатикадан 30 сабақ. – Алматы: Шартарап, 2001. – 440 б.
87 Компьютерные вирусы. // http://www.referat.ru/referats/view/1442.
88 Фигурнов В.Э. IBM PC для пользователей. – Уфа: ПК «Дегтярёв и сын», 1993. – С.12-22.
89 Бостанбеков Қ.А. Вирустар және оларға қарсы күрес. – Алматы, 2007. – Б.25.
90 Куринов Б.А. Научные основы квалификации преступлений. – М.: МГУ, 1976. – 320 с.
91 Орымбаев Р. Специальный субъект преступления. – Алма-Ата: Наука, 1977. – 220 с.
92 Филановский И.Г. Социально-психологическое отношение субъекта к преступлению. – Санкт-Петербург, 1970. – С.19.
93 Люцик В.В. Учение о вине по уголовному праву Республики Казахстан и зарубежных государств: дис. … докт. юрид. наук. – Алматы, 2005.
94 Расулев А.К. Компьютерные преступления: уголовно-правовые и криминологические аспекты: автореф. … канд. юрид. наук. – Ташкент, 2006. – С.11.
95 Мауленов Г.С. Криминологическая характеристика организованной преступности. – Алматы, 1997. – 232 с.

96 Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / под. ред. Акад. Б.П. Смагоринского. – М.: Право и закон, 1996. – 520 с.
97 Эрик С. Реймонд Краткая история страны хакеров. // www.pitachok.net.
98 Взлом хакинг. // http://www.pitachok.net. – 2007.
99 Безруков Н.Н. Компьютерные вирусы. – Киев, 1997.
100 Безруков Н.Н. Компьютерные вирусы. – М.: Наука, 1991.
101 Вечерский Д.А., Шалькевич И.И. Расследование компьютерных преступлений. – Минск, 2001. – 326 с.
102 Батурин Ю.М., Жодзинский А.М. Компьютерные преступления и компьютерная безопасность. – М.: Юрид. лит., 1991. – 156 с.
103 Батурин Ю.М. Компьютерные преступления и компьютерная безопасность. – М.: Юридическая литература, 1991.
104 Хакинг. // http://www.pitachok.net. – 2-тарау.
105 Заңдық энциклопедиялық сөздігі. – М., 1984. – С.179.
106 Ожегов С.И. Толковый словарь. – М., 1989. – С.321.
107 Германияның Қылмыстық кодексінің 263(а)-тарауы.
108 Қараңыз: Фрей С. Компьютерная преступность с точки зрения уголовного права собственности и имущества // Общественные науки за рубежом. сер. 4. – М., 1989. – С.141-152.
109 Паркин Г., Уихман Б. Интеллектуальные модули защиты // Защита программного обеспечения. – М., 1992. – С.131.
110 Толығырақ қараңыз: Расулев А.К. Компьютерные преступления: уголовно-правовые и криминологические аспекты: автореф. … канд. юрид. наук. – Ташкент, 2006. – С.11.
111 Элеонора Мелик. Компьютерные преступления: информационно-аналитический обзор // http://www.wse-wmeste.ru. – 1999-2013 Openstat. Все права защищены. – Т.3. – glava_3.
112 Модельный Уголовный кодекс для государств-участников Содружества независимых государств. // http://www/medialow.ru/exussrlaw /1/sng/05.htm.
113 Толеубекова Б.Х. Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники: дис. … докт. юрид. наук. – Алматы, 1998. – 172 с.
114 Қазақстан Республикасының 1998 жылғы 26 маусымда қабылданған «ҚР Ұлттық қауіпсіздігі туралы» №233-1 Заңы. // Нормативтік актілер. – Алматы: Аян Әдет, 1998. – Б.16.
115 Соглашение о сотрудничестве государств-участников Содружества независимых государств в борьбе с преступлениями в сфере компьютерной информации. Минск, 1 маусым 2001 ж. // Дипломатический курьер. – Астана, 2001. – №3. – С.8.
116 Қазақстан Республикасының 2002 жылғы 21 желтоқсанда қабылданған «ҚР Қылмыстық, Қылмыстық іс жүргізу және Қылмыстық-атқару ко-

декстеріне өзгерістер мен толықтырулар енгізу туралы» №363-II Заңы. // Казахстанская правда. – 2008.
117 Қазақстан Республикасының 2007 жылғы 8 қаңтарда қабылданған «Қылмыстық заңнаманы жетілдіру мәселелері бойынша ҚР Қылмыстық, Қылмыстық іс жүргізу кодекстеріне өзгерістер мен толықтырулар енгізу туралы» №210-III Заңы. – «Параграф» ақпараттық жүйесі.
118 Қазақстан Республикасының 2009 жылғы 10 желтоқсанда қабылданған «Қылмыстық заңнаманы жетілдіру мәселелері бойынша ҚР Қылмыстық, Қылмыстық іс жүргізу кодекстеріне өзгерістер мен толықтырулар енгізу туралы» №227-IV Заңы. – «Параграф» ақпараттық жүйесі.
119 Қазақстан Республикасының 2011 жылғы 18 қаңтарда қабылданған №393-IV, 2011 жылғы 28 қаңтарда қабылданған №402-IV, 2011 жылғы 28 желтоқсанда қабылданған №524-IV, 2012 жылғы №529-IV, №547-IV, №551-IV, №557-IV, №19-V, 24-V, 2013 жылғы №63-V «Өзгерістер мен толықтырулар енгізу туралы» Заңдары. – Алматы: ЮРИСТ, 2013. – 164 б.
120 Протасевич А.А., Зверянская П.П. Борьба с киберпреступностью как актуальная задача современной науки. // Криминологический журнал Байкальского государственного университета экономики и права. – 2011. – №3. – С.28-33.
121 Уголовное законодательство зарубежных стран (Англии, США, Франции, Германии, Японии): Сборник законодательных материалов / под ред. И.Д. Козочкина. – М.: Зерцало, 1998. – 452 с.
122 Уголовный кодекс ФРГ / пер. с нем. А.В. Серебренникова. – М.: ИКД «Зерцало-М», 2001.
123 Уголовный кодекс ФРГ / пер. с нем. А.В. Серебренникова. – М.: ИКД «Зерцало-М», 2001. – С.167.
124 Уголовный кодекс ФРГ / пер. с нем. А.В. Серебренникова. – М.: ИКД «Зерцало-М», 2001. – С.168.
125 Ахметшин Х.М., Ахметшин Н.Х., Петухов А.А. Современное уголовное законодательство КНР. – М.: ИД «Муравей», 2000. – 406 с.
126 Ахметшин Х.М., Ахметшин Н.Х., Петухов А.А. Современное уголовное законодательство КНР. – М.: ИД «Муравей», 2000. – С.353-354.
127 Голландия Қылмыстық кодексі / под ред. Б.В. Волженкина. – СПб., 2001. – 522 с.
128 Францияның жаңа Қылмыстық кодексі. – М.: Юридический колледж МГУ, 1993. – 196 с.
129 Аманов Ж.К. Уголовная ответственность за преступления, посягающие на безопасность компьютерной информации: монография. – Алматы, 2007. – 184 с. – С.56-58.

Ғылыми басылым

Қуаныш Аратұлы

АҚПАРАТТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРМЕН КҮРЕСУ АСПЕКТІЛЕРІ

Монография

Редакторы А. Шуриева
Мұқаба дизайнері А. Қалиева
Беттеген Г. Шаккозова

ИБ № 12749
Басуға 19.02.2019 жылы қол қойылды. Пішімі 60х84 $^{1}/_{32}$.
Офсетті қағаз. Сандық басылыс. Көлемі 8, 3 б.т.
Тапсырыс №2133. Таралымы 500 дана.
Әл-Фараби атындағы Қазақ ұлттық университетінің
«Қазақ университеті» баспасы.
050040, Алматы қаласы, әл-Фараби даңғылы, 71.
«Қазақ университеті» баспаханасында басылды.