ҒТАМР 10.77.21

Алмазқызы Қ.

заң ғылымдарының магистрі, ІІМ Академиясы,
Қазақстан, Алматы қ., e-mail: almazkyzy123@mail.ru

КИБЕРҚЫЛМЫСТЫЛЫҚ – ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚАУІПСІЗДІГІНЕ ЖАҢА ҚЫЛМЫСТЫҚ ҚАУІП РЕТІНДЕ

Әлемдік қоғамдастықта жаһандық үдерістердің дамуына түбегейлі әсер еткен заманауи құбылыстардың бірі ақпараттық-коммуникациялық технологияларды қарқынды жетілдіру болды. Желілік компьютерлік коммуникациялардың таралуынан туындаған мәдени, әлеуметтік, экономикалық, саяси, құқықтық өзгерістер ауқымы көптеген ғалымдарға оларды адамзат өркениетінің тарихындағы жаңа кезеңнің басталуының көрінісі ретінде қарастыруға мүмкіндік береді. Жаһандық компьютерлік желіні пайдалану – мемлекетаралық қатынастарды жаһандану және ақпараттық қоғамды құрудың маңызды алғышарттарының бірі екендігі құпия емес.

Біз бұрын атап өткендей, киберқылмыс – бұл киберкеңістікке қолжетімді құралдар мен құрылғылар арқылы жүзеге асырылатын, заңмен қорғалатын әртүрлі әлеуметтік қатынастарға зиян келтіруге бағытталған, ақпараттық және телекоммуникациялық желілерді пайдалану арқылы киберкеңістікте қашықтан жасалатын қылмыс. Киберқылмыс міндетті түрде құқыққа қайшылық, қоғамдық қауіп, кінәлілік және жазалау сияқты белгілерге ие.

Киберқылмыстың белгілері мен ерекшеліктерін зерттеу көбінесе белгілі бір қиындықтарды тудырады. Біріншіден, осы заңсыз әрекеттердің тобы үшін белгіленген терминологиялық аппараттың заң ғылымы мен құқық қолдану практикасында болмауы. Қарастырылып отырған қылмыстық құқық бұзушылықтардың заты – заңмен қорғалатын және электрондық жеткізгіш құралдарында қамтылған ақпарат; ақпараттық жүйелер, соның ішінде мемлекеттік органдардың ақпараттық жүйесі, телекоммуникация желісі, мемлекеттік электрондық ақпараттық ресурстар.

Түйін сөздер: киберқылмыстылық, қылмыс, жаһандану, киберкеңістік, қылмыстық кодекс.

Almazkyzy K.

Master of Law, Academy of MIA,
Kazakhstan, Almaty, e-mail: almazkyzy123@mail.ru

Cybercrime – as a new criminal threat to the security of the Republic of Kazakhstan

One of the modern phenomena that has had a major impact on the development of global processes in the global community was the intensification of information and communication technologies. The scale of cultural, social, economic, political, and legal changes arising from the spread of networked computer communications allows many scholars to consider them as the beginning of a new era in the history of human civilization. It is no secret that the use of the global computer network is one of the most important prerequisites for globalization and the creation of an information society.

As we have already noted, cybercrime is a cybercrime crime that is aimed at cybercrime-based tools and devices that are used to break various social relationships protected by law and telecommunications networks. Cybercrime has such signs as lawlessness, social danger, guilt and punishment.

The study of the characteristics and features of cybercrime often causes certain difficulties. First, the lack of a terminological apparatus established for this group of unlawful actions in judicial practice and law enforcement practice. The subject of criminal offenses is the information provided by law and contained in the electronic media; information systems, including information systems of state bodies; telecommunication network; state electronic information resources.

Key words: cybercrime, crime, globalization, cybercrime, criminal code.

Алмазқызы Қ.
Магистр права, Академия МВД,
Казахстан, г. Алматы, e-mail: almazkyzy123@mail.ru

Киберпреступность в качестве новой преступной угрозы безопасности Республики Казахстан

Одним из современных явлений, оказавших серьезное влияние на развитие глобальных процессов в мировом сообществе, стала интенсификация информационных и коммуникационных технологий. Масштабы культурных, социальных, экономических, политических и правовых изменений, возникающих в результате распространения сетевых компьютерных коммуникаций, позволяют многим ученым рассматривать их как начало новой эры в истории человеческой цивилизации. Не секрет, что использование глобальной компьютерной сети является одной из важнейших предпосылок глобализации и создания информационного общества. Как мы уже отмечали, киберпреступность – это преступление, связанное с киберпреступностью, которое направлено на средства и устройства, основанные на киберпреступности, которые используются для нарушения различных социальных отношений, охраняемых законом и телекоммуникационными сетями. Киберпреступность имеет такие признаки, как беззаконие, общественная опасность, вина и наказание. Изучение особенностей и особенностей киберпреступности часто вызывает определенные трудности. Во-первых, отсутствие терминологического аппарата, установленного для этой группы противоправных действий в судебной практике и правоприменительной практике. Предметом уголовных преступлений является информация, предусмотренная законом и содержащаяся в электронных СМИ; информационные системы, в том числе информационные системы государственных органов; телекоммуникационная сеть; государственные электронные информационные ресурсы.

Ключевые слова: киберпреступность, преступность, глобализация, киберпреступность, уголовный кодекс.

Кіріспе

Әлемдік қоғамдастықта жаһандық үдерістердің дамуына түбегейлі әсер еткен заманауи құбылыстардың бірі ақпараттық-коммуникациялық технологияларды қарқынды жетілдіру болды. Желілік компьютерлік коммуникациялардың таралуынан туындаған мәдени, әлеуметтік, экономикалық, саяси, құқықтық өзгерістер ауқымы көптеген ғалымдарға оларды адамзат өркениетінің тарихындағы жаңа кезеңнің басталуының көрінісі ретінде қарастыруға мүмкіндік береді. Жаһандық компьютерлік желіні пайдалану – мемлекетаралық қатынастарды жаһандану және ақпараттық қоғамды құрудың маңызды алғышарттарының бірі екендігі құпия емес.

Ақпараттық қоғамның дамуы саласында әлемнің жетекші елдерінің арасында лайықты орынды алуды таңдап, біздің еліміз өзінің ақпараттық және телекоммуникациялық инфрақұрылымын белсенді түрде дамытып, ақпараттық қауіпсіздікті қамтамасыз ету үшін тиісті саясатты қалыптастырады.

Негізгі бөлім

Қазіргі уақытта отандық қылмыстық заңнамада «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» деп аталатын 7-тарау бекітілген. Аталған тарау келесідей баптарды қамтиды: 205-бап. Ақпаратқа, ақпараттық жүйеге немесе ақпараттық-коммуникациялық желіге құқыққа сыйымсыз қол жеткізу; 206-бап. Ақпаратты құқыққа сыйымсыз жою немесе түрлендіру; 207-бап. Ақпараттық жүйенің немесе ақпараттық-коммуникациялық желінің жұмысын бұзу; 208-бап. Ақпаратты құқыққа сыйымсыз иеленіп алу; 209-бап. Ақпаратты беруге мәжбүрлеу; 210-бап. Зиян келтіретін компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату; 211-бап. Қолжетімділігі шектелген электрондық ақпараттық ресурстарды құқыққа сыйымсыз тарату; 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 өзгерту үшін бағдарламаларды жасау, пайдалану, тарату (Sergazin, Esimova, Kozhakhmetova, Mukasheva, 2018: 26).

Біздің пікірімізше, жоғарыда аталып өткен қылмыстардың кейбір ерекшеліктерін қарастырып өту қажет.

Қарастырылып отырған қылмыстық құқық бұзушылықтардың қоғамдық қауіптілігі, ең алдымен, олар азаматтар мен ұйымдардың құқықтарын және заңды мүдделерін, ақпараттық салада қоғам мен мемлекеттің заңмен қорғалатын мүдделерін бұзады, ақпараттық ресурстардың, ақпараттық жүйелердің және байланыс инфрақұрылымының құпиялылығына, тұтастығына, қолжетімділігіне зиян келтіреді (Борчашвили, 2015).

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды саралау, ашу және тергеу Қазақстан Республикасының құқық қорғау және арнайы органдар қызметкерлері үшін әлі күнге дейін ауыр міндет болып табылады. Осындай себептерге төмендегілердің болмауын жатқызуға болады:

– тергеу және сот практикасын жалпылау;

– тиісті ғылыми-әдістемелік және сот-сараптамалық ұсыныстар;

– ІІМ оқу орындарында тергеу-криминалистикалық мамандығы қызметкерлерінің, сондай-ақ тергеушілерді, анықтаушыларды біліктілікті көтеру және қайта даярлау курстарында жедел даярлықтан өткізетін арнайы дайындық курстары

– осы қылмыстық құқық бұзушылықтарды жасау мен өзге де бірқатар факторлар нәтижесінде туындаған дәлелдемелік ақпараттың арнайы түрлерімен жұмыс жасауға құқық қорғау органдары қызметкерлері дайындығының жеткіліксіз болуы.

Бізбен зерттеліп отырған киберқылмыстылықтың кейбір ерекшеліктерін түсіну мен айқындау үшін объектісі болып бірінші кезекте ақпараттық қауіпсіздік саласындағы қоғамдық мүдде болатын кейбір қылмыс құрамдарына тоқталып өту қажет.

205-бап. Ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне құқыққа сыйымсыз қол жеткізу. Қоғамдық қауіптілігі ақпараттың құпиялылығы, ақпараттық жүйелер иелері мен ақпараттық-коммуникациялық желілер иелерінің заңды мүдделеріне нұқсан келтіру құқығын бұзады.

Бұл қылмыстық құқық бұзушылықтың объектісі – ақпараттың, ақпараттық жүйелердің және телекоммуникация желілерінің құпиялылығына азаматтар мен ұйымдардың құқықтары мен заңды мүдделері.

Мұнда ақпарат электронды есептеу құралдарында электронды есептеу техникасының элементтерінің жай-күйінің немесе белгілі бір ақпаратты, хабарларды, деректерді орындайтын ақпаратты өңдеудің, сақтаудың және берудің басқа электрондық құралдарының тізбегін білдіретін электронды түрде сақталатын ақпарат ретінде түсінілуі керек. Ақпараттар сандар, мәтіндер, суреттер, аудио-, бейне-, бағдарламалық код немесе екеуінің тіркесімі түрінде ұсынылуы мүмкін. Мәнсіз және кезкелген нәрсеге арналмаған таңбалар жиынтығы ақпаратқа қолданылмайды (Parodi, 2013: 59).

Электронды жеткізгіштер деп есептеуіш техника құралдарымен өңдеуге болатын, деректерлер форматында, ақпараттарды жазуға, сақтауға және жаңғыртуға мүмкіндік беретін кез келген материалды жеткізгіштер танылады. Деректерлер форматы сандық, бинарлы және аналогты болуы мүмкін. Электронды жеткізгіштерге үнемі сақтап отыратын құрылғыларды ғана жатқызып қоймай, мысалға алатын болсақ магниттік және оптикалық дискілер магниттік және жартылай өткізгіш карталардан басқа компьютердің немесе басқа электрондық құрылғының жедел жады сияқты жедел сақтаушы құрылғыларды жатқызу керек. Ақпарат көбінесе файл түріндегі электронды жеткізгіште сақталады (Hui, Kim, Wang, 2017: 523).

Электронды түрде ақпараттық жүйелерде сақталатын ақпарат электронды ақпараттық ресурс немесе басқаша айтқанда ақпараттық мәліметтер базасы деп аталады. Электронды ақпараттық ресурстар үшін едәуір көлем және деректердің құрылымдалғандығы, олардың белгілі бір функционалды бағыты тән.

Электронды түрде ашық ақпараттық-коммуникациялық жүйелерде қызмет ететін ақпараттық жүйелерде сақталатын ақпарат Интернет-ресурстарға жатады.

Сәйкесінше, қарастырылып отырған қылмыстық құқық бұзушылықтардың заты болып танылатын ақпараттық жүйелерге төмендегілерді жатқызамыз:

– мемлекеттік құпияға жатқызылатын мемлекеттік электронды ақпараттар ресурсын құрайтын ақпараттық жүйелер;

– құпиялы электронды ақпараттық ресурстарды, оның ішінде заңмен қорғалатын құпиялар, дербес деректерді құрайтын ақпараттық жүйелер;

– меншік иесімен қолжетімділікке шектеу қойылған өзге де ақпараттық жүйелер.

Қарастырылып отырған қылмыстық құқық бұзушылықтың объективті жағы ақпараттық жүйеде немесе телекоммуникация желісінде электронды жеткізгіштерде сақталған заңмен қорғалатын ақпаратқа заңсыз қолжетімділіктен

көрініс табады. Электронды бұқаралық ақпарат құралдарында заңмен қорғалатын ақпаратқа рұқсатсыз қол жеткізу осы ақпаратты тікелей алу мүмкіндігінде көрінеді және электронды бұқаралық ақпарат құралының иесі (иесі) белгілеген қорғау шараларын еңсеру арқылы жүзеге асырылуы мүмкін. Телекоммуникация желілеріне заңсыз қолжетімділік оның ақпараттық жүйелерімен және олардың құрамдас бөліктерімен тікелей өзара әрекеттесу мүмкіндігін алуда көрінеді және әдетте қорғау шараларын еңсеру арқылы жүзеге асырылады. Қолжетімділік тек қана бағдарламалық-техникалық құралдармен жүзеге асырылады.

Қорғаудан өтуге жол бермей, заңсыз кіруге рұқсаты бар адам (әкімші, жүйенің және желінің пайдаланушысы) қол жетімді болатын (сеанс) компьютер арқылы жүзеге асырылуы мүмкін. Заңсыз қолжетімділік қашықтан, соның ішінде Интернет арқылы жүзеге асырылуы мүмкін.

Қарастырылып отырған қылмыстық құқық бұзушылық материалды құрамға жатады. Ол зиянды салдардың туындау сәтінен бастап аяқталған болып табылады.

Зиянды салдар азаматтар немесе ұйымдардың құқықтары мен заңды мүдделерін, не болмаса қоғам немесе мемлекеттің заңды мүдделерін елеулі бұзудан көрінеді. Қазақстан Республикасы ҚК 3-бабының 14-тармағында елеулі зиянның ұғымы бекітілген, мұнда төмендегілерге назар аудару қажет:

– адамның және азаматтың конституциялық құқықтары мен бостандықтары, ұйымдардың құқықтары мен заңды мүдделері, қоғамның және мемлекеттің заңмен қорғалатын мүдделері;

– айтарлықтай залал келтіру (жүз айлық есептік көрсеткіштен асатын мөлшердегі зиян);

– ұйымдардың немесе мемлекеттік органдардың қалыпты жұмысының бұзылуы (ҚР ҚК, 2014).

Заңсыз қолжетімділік пен туындаған қоғамға қауіпті салдардың арасында себептік байланыс болу қажет.

Қарастырылып отырған қылмыстық құқық бұзушылық субъективтік жағынан тек қасақана нысанда (тікелей немесе жанама ниет) жасалуы мүмкін: кінәлі заңмен қорғалатын ақпаратқа, ақпараттық жүйеге немесе телекоммуникация желісіне құқыққа қайшы кіріп жатқанын сезінеді, қоғамға қауіпті салдардың туындау мүмкіндігін алдын ала біледі және олардың туындауын қалайды.

Азаматтардың немесе ұйымдардың, не болмаса қоғам немесе мемлекеттің заңмен қорғалатын мүдделеріне келтірілетін зиянды салдардың туындауына қатысты жанама ниет болуы мүмкін, яғни кінәлі тұлға саналы түрде осы салдарға жол береді немесе олардың туындауына немқұрайлы қарайды.

Осы қылмыстық құқық бұзушылықтың уәжі мен мақсаты әртүрлі болады және саралауға әсер етпейді, бірақ олар жазаны дараландыруда ескерілуі тиіс. Көбінесе бұл пайдакүнемдік уәж.

Қылмыстық құқық бұзушылықтың субъектісі 16 жасқа толған, ақыл-есі дұрыс адам.

Қазақстан Республикасы ҚК 205-бабының 2-тармағында ұлттық электрондық ақпараттық ресурстарға және ұлттық ақпараттық жүйеге қасақана құқыққа сыйымсыз қол жеткізу үшін қылмыстық жауаптылық бекітілген.

Ұлттық деп мемлекеттің экономикасы мен қауіпсіздігі үшін стратегиялық маңызы бар мемлекеттік электрондық ақпараттық ресурстардан құралған ақпараттық жүйелер танылады.

Қазақстан Республикасы ҚК 205-бабының 3-тармағында ерекше саралаушы белгі ретінде ауыр зардап қарастырылған.

Қазақстан Республикасы ҚК 3-бабының 4-тармағындағы ережелерді ескере отырып ауыр зардапқа осының ішінде келесілерді жатқызу қажет: жәбірленушінің немесе оның жақынының (жақындарының) өзін-өзі өлтіруі; ауыр және аса ауыр залал келтіру. Осы салдар құқыққа сыйымсыз қолжетімділікпен себепті байланыста болуы қажет.

Қазақстан Республикасы ҚК 205-бабына тікелей өзіміздің зерттеуіміздің аясында кішігірім талдау жасай келе, біз ақпаратқа құқыққа сыйымсыз қол жеткізуді қашықтықтан киберкеңістікті құратын Интернет арқылы компьютерлік құрылғыдан ақпараттық жүйеге немесе телекоммуникация желісіне қол жетімділікке жатқыздық.

Екіншіден, киберқылмыстылықты зерттеуді киберкеңістікте жасалатын қылмыстардың статистикалық есебінің болмауы қиынға соқтырады. Ресми статистика жоғарыда аталған қылмыстық құқық бұзушылықтар бойынша деректерге ғана ие. Киберқылмысты анықтауға біздің көзқарасымызды ескере отырып, қылмыстық құқық бұзушылықтардың айтарлықтай ауқымы Қазақстан Республикасының Қылмыстық кодексінің Ерекше бөлігінің әртүрлі тарауларында орын алған. Ақпараттық және телекоммуникациялық желілерді, киберкеңістікке қол жеткізуге арналған құрылғыларды және құралдарды пайдалану – қол сұғушылық объектілері контексінде кейбір қылмыстық

құқық бұзушылықтардың саралаушы белгісі болып табылады (Борчашвили, 2015):

1) 1-тарау. Жеке адамға қарсы қылмыстық құқық бұзушылықтар:

– 130-бабының 2-бөлігі Жала жабу, яғни көпшілік алдында немесе бұқаралық ақпарат құралдарын немесе телекоммуникациялар желілерін пайдалана отырып жалған мәліметтерді тарату;

– 131-бабының 2-бөлігі Қорлау, яғни көпшілік алдында немесе бұқаралық ақпарат құралдарын немесе телекоммуникациялар желілерін пайдалана отырып адамның абыройы мен қадір-қасиетін әдепсіз түрде кемсіту;

2) 3-тарау. Адамның және азаматтың конституциялық және өзге де құқықтары мен бостандықтарына қарсы қылмыстық құқық бұзушылықтар:

– 147-бабының 2,3,5-бөліктері Жеке өмірге қолсұғылмаушылықты және Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасын бұзу;

– 148-бабының 2-бөлігі Хат жазысу, телефонмен сөйлесу, пошта, телеграф хабарлары немесе өзге де хабарлар құпиясын заңсыз бұзу;

3) 4-тарау. Бейбітшілік пен адамзат қауіпсіздігіне қарсы қылмыстар:

– 161-бабының 2-бөлігі. Басқыншылық соғысты тұтандыруға насихат жүргізу немесе жария түрде шақыру;

– 174-бап. Әлеуметтік, ұлттық, рулық, нәсілдік, тектік-топтық немесе діни алауыздықты қоздыру.

4) 5-тарау. Мемлекеттің конституциялық құрылысының негіздеріне және қауіпсіздігіне қарсы қылмыстық құқық бұзушылықтар:

– 179-бабының 2-бөлігі. Билікті басып алуды немесе ұстап тұруды насихаттау немесе оған жария түрде шақыру, сол сияқты билікті басып алу немесе ұстап тұру не Қазақстан Республикасының конституциялық құрылысын күштеп өзгерту;

– 180-бабының 2-бөлігі. Сепаратистік әрекет.

5) 6-тарау. Меншікке қарсы қылмыстық құқық бұзушылықтар:

– 188-бабының 2-бөлігінің 4-тармағы. Ұрлық;

– 195-бабының 3-бөлігінің 3-тармағы. Алдау немесе сенімді теріс пайдалану жолымен мүліктік залал келтіру және өзге де қылмыстық құқық бұзушылықтар құрамы.

6) 10-тарау. Қоғамдық қауіпсіздікке және қоғамдық тәртіпке қарсы қылмыстық құқық бұзушылықтар:

– 256-баптың 2-бөлігі. Терроризмді насихаттау немесе терроризм актісін жасауға жария түрде шақыру;

– 274-баптың 2-бөлігінің 3-тармағы. Көрінеу жалған ақпарат тарату.

7) 16-тарау. Басқару тәртібіне қарсы қылмыстық құқық бұзушылықтар:

– 373-баптың 2-бөлігі. Қазақстан Республикасының Тұңғыш Президентін – Елбасын көпшілік алдында қорлау және оның абыройы мен қадір-қасиетіне өзгедей қолсұғушылық, Қазақстан Республикасы Тұңғыш Президентінің – Елбасының бейнесін бұлдіру, Қазақстан Республикасы Тұңғыш Президентінің – Елбасының заңды қызметіне кедергі жасау;

– 375-баптың 2-бөлігі. Қазақстан Республикасы Президентінің абыройы мен қадір-қасиетіне қол сұғу және оның қызметіне кедергі жасау;

– 376-баптың 2-бөлігі. Қазақстан Республикасы Парламенті депутатының абыройы мен қадір-қасиетіне қол сұғу және оның қызметіне кедергі жасау;

– 378-баптың 2-бөлігі. Билік өкілін қорлау;

– 402-баптың 2-бөлігі. Сот заңсыз деп таныған ереуілге қатысуды жалғастыруға арандататын әрекеттер.

Жоғары технологияларды дамыту және оларды қолдану аясын кеңейту арқылы қылмыстық киберқылмыстық құқық бұзушылықтың тізімі үнемі кеңейіп отыруы мүмкін және әрдайым қылмыстық заңнама киберкеңістіктегі жаңа қауіптерге уақтылы жауап бермейтінін ескеру қажет.

Әдетте, киберқылмыстар олардың мақсаттарымен, ықпал ету нысандарымен, қылмыстық әрекеттер жасау тәсілдері мен құралдарымен ерекшеленеді. Бөлінетін негіздерге сәйкес:

1. Киберқылмыстар көбінесе экономикалық мақсаттар үшін жасалады. Бұл мысалы ақша қаражатын немесе құпия ақпаратты жымқыру түрінде жеке және заңды тұлғаларға мүліктік залал келтіру, заңмен қорғалатын ақпаратты иемдену түрінде болуы мүмкін және т.б. Басқа мақсаттарға саяси – билік қатынастар жүйесін бұзу, билікке деген сенімі мен саяси режимді бұзатын ірі мемлекеттік және саяси институттарға зиян келтіру. Киберқылмыстың келесі мақсаттары идеологиялық болып табылады: ғаламторды пайдаланушыларды рангқа, мысалы, радикалды террористік және ұлтшыл топтарға енгізу мақсатында идеялар мен идеологияларды тарату. Киберқылмыстың әлеуметтік және психологиялық мақсаттарын анықтауға

болады, мысалы, азаматтарға моральдық, психологиялық зиян келтіру, шаруашылық субъектілерінің беделін түсіру және т.б. Сонымен қатар, киберқылмыстар телекоммуникация желілерінің тұтастығын, ақпараттық-коммуникациялық инфрақұрылымды және т.б. бұзу мақсатында жасалады. Біздің көзқарасымыз бойынша киберкеңістіктің дамуын есепке ала отырып киберқылмыстардың мақсатты спектрі ұлғаяды.

Кейбір ғалымдардың пікірі бойынша, ақпарат тарату арқылы адам өлтіру немесе денсаулыққа зиян келтірген жағдайлар да бар. Бұл жағдайда ауыр науқасқа, мысалы жақын туысқаны немесе басқа адамның өлімі жайлы жалған ақпарат беру туралы ғана емес, сондай-ақ адамдардың жаппай гипнозы немесе белгілі бір адамға алыстан ықпал ету туралы да әңгіме қозғалып отыр. Ақпаратты тарату өз-өзіне қол жұмсаудың тәсілдерінің бірі болуы мүмкін. Бұған қоса, соңғы жылдары осы мақсатта ақпараттық-коммуникациялық технологиялар да жиі қолданылып келеді. Қазіргі уақытта Интернетте адамдардың ерік-жігерін басу, оларды гипнозға алу немесе зомбалау үшін көптеген ұсыныстар бар. Ақпараттық және коммуникациялық технологияларды пайдалана отырып, тек ақпараттық ғана емес, сонымен қатар адам денсаулығына зиян келтіру немесе өлтіру мақсатында адамға, оның мүлкіне, жою немесе диверсия жасау мақсатында физикалық әсер ету мүмкін (ҚР ҚК, 2014: 128-131).

2. Әсер ету объектілері. Киберқылмыскерлердің әрекеттері қарапайым азаматтарға, ұйымдарға және қаржы құрылымдарына, мемлекеттік институттарға, олардың жеке ақпаратына, еркіндігіне, жеке киберқауіпсіздікке және т.б. бағытталған болуы мүмкін. Бұл тұрғыда ықпал ету объектілері киберқылмысты жасау салдарынан зиян келтіретін қоғамдық қатынастардың кең ауқымы екенін атап өткен жөн (Broadhurst, 2010: 2).

3. Ықпал ету әдістері мен құралдары. Жоғары технологияларды дамыту және оларды пайдалану аймағын кеңейту арқылы киберқылмыспен қылмыстық әрекеттерді жасаудың жолдары мен құралдары дамып, жетілдірілуде. Киберқылмыскерлер жұмыс істейтін барлық қолданыстағы жолдар мен құралдарды жүйелендіру мүмкін емес. Мысалы, кешегі «шығарып алу» әдісі қысқа мерзім ішінде ескіріп келеді, киберқылмыскерлер киберқылмыс жасау үшін түрлендірілген технологиялық құралдарды пайдаланады. Киберқылмыс жасаудың осы әдістерінің, мысалы, екі түрі бар: әлеуметтік инженерия және вирустық бағдарламалар. Бірінші типтің айрықша ерекшелігі – бұл жеке ақпаратты алу үшін адамға телефон немесе компьютерлік шабуыл жасау. Адам психологиясының ерекшеліктеріне сүйене келе алаяқтар басқа адам болып көрініп, осылайша адамды жаңылыстырады. Әлеуметтік инжинирия адамның психологиясының ерекшеліктерін білу, алдауды пайдалану, сенімдерін асыра пайдалану негізінде жеке мәліметтерді «шығарып алу» тәсілдерін сипаттау үшін ақпараттық қауіпсіздік саласындағы мамандардың тар шеңберімен пайдаланылады. Бұл жеке мәліметтерді алудың психологиялық әдісі киберкеңістікке қол жеткізу арқылы жәбірленушімен байланыссыз қосылуды қамтамасыз етеді және киберқылмыскерлерге үлкен еркіндік береді. Алаяқтық және әлеуметтік инженерия қылмыскерлерге ақша талап етуге ерік береді. Мысалға, фишинг (phishing) әдісі кең таралған. Онда заңды веб-сайт немесе қосымша түрінде кейін ақша алу мақсатында, пайдаланушының құпия мәліметтері алдап алынады. Соңғы жылдары зиянды бағдарламаларды (ransomware) пайдаланып, қорқытып алу күрт өсті. Ақпарат бұғатталады немесе шифрланады. Оған кіруге рұқсат алу үшін, зиянкестер ақша талап етеді және өкінішке орай, оларды алады. Алаяқтардың мақсаты – ақша операцияларын жасайтын кез келген қосымшалар, сондай-ақ мобильді құрылғыларда сақталатын жеке ақпарат (Чекунов, 2013).

Бірқатар ғалымдардың айтуы бойынша, компьютерлік ақпарат саласындағы алаяқтықта меншік ерікті түрде тасымалданбайды, олар тікелей компьютердің мәліметтерін енгізу, алып тастау, бұғаттау және т.б жолдармен жүзеге асырылады. Демек, киберкеңістіктегі алаяқтық тек алдау немесе сенімсіздік арқылы жасалуы мүмкін. Киберкеңістікте сенімді асыра пайдалану кінәлі адамның жәбірленушімен форумдар, бейне және дыбыстық қоңыраулар арқылы жеке қарым-қатынастарға түсу, танымал емес заттарды сату туралы хабарландыру жариялау арқылы және басқа да көптеген тәсілдермен жүзеге асырылуы мүмкін. Осындай тәсілдер алаяқтың көптеген түрлерін туындатты (Сачков: 138-140).

Кибер алаяқтықтың әр түрлі түрлері бар. Мысалы, С.С. Медведев интернеттегі қарапайым алаяқтықтың келесі түрлерін анықтайды:

– құмар ойындар саласындағы алаяқтық;

– онлайн аукциондар саласындағы алаяқтық;

– электрондық ақша және электрондық төлем жүйелерін пайдаланумен жасалған алаяқтық;

– тауарлар мен қызметтерді ұсынудағы алаяқтық;

– танысу саласындағы алаяқтық;

– «Нигериялық алаяқтық» (Простосердов, 2016: 100-145).

Киберкеңістіктегі қауіп-қатерлер технологияның дамуымен өзгереді, сондықтан қылмыстық ықпал етудің әдістері мен құралдары жетілдірілуде. Сарапшылармен мысалы, 2008 жылы ең қауіпті он қауіптің ішінде: бот желілері; үкіметтік емес веб-сайттарға, жеке меншік кәсіпорындарға және түпкілікті тұтынушыларға арналған «нысаналы» шабуылдар; банктер, жекеменшік кәсіпорындар және түпкілікті тұтынушылар зардап шеккен қаржылық алаяқтық; жеке куәлікпен жасалатын алаяқтық; спам және дербес деректерлерді ұрлау; экономикалық және мемлекеттік органдардағы тыңшылық; Web-негізіндегі шабуылдар; әлеуметтік желілер; ішкі желілік ресурстардың дұрыс емес немесе зиянды қолданылуы; вирустар мен құрттар сияқты қауіптердің болғандығы ескеріледі (Медведев, 2008).

2013 жылы McAfee мамандарының болжамына сәйкес, мобильді Интернетке қолжетімділікті (ұялы телефондарға зиянды бағдарламалармен вирусқа қарсы бағдарламалар, вирусқа қарсы бағдарламалық жасақтаманы жаңартатын вирустар, вирустарды жұқтырған sms-хабарламалар) қолданумен байланысты қауіптер бірінші кезекте келеді.

Бұдан басқа, қауіпті үрдістер: Windows 8 және HTML5-та шабуыл жасау әдістерін жалғастыру; шабуылдар пайда табу емес, инфрақұрылымға зиян келтірмеуге бағытталған; ботнет жойылғаннан кейін де байланысын жаңартатын ботнеттер үшін зиянды бағдарламаларды қолдану, бұл инфекцияның одан әрі таралуына; қылмыстық топтар арасында кибершабуылдың аутсорсингін дамыту және киберқылмыстарды жасау үшін бағдарламалық қамтамасыз етуді және қызметтерді сатуға мүмкіндік береді. Сондай-ақ, Интернеттегі саяси белсенділік экстремистік топтармен ауыстырылатынын және киберқылмыстағы мемлекеттердің қатысуы мемлекеттік деңгейде ұйымдастырылған шабуылдарға байланысты және шабуылдардың нысанасына айналу мүмкіндігі туралы ескеру қажет.

«Касперский Зертханасының» сарапшыларының бағалауы бойынша, 2017 жылы киберкеңістік жағдайында барлық қауіптерді бағалауда төмендегілер атап өтілді:

– «2017 – бұл шифрлаушылар жылы.

– Қаржы компанияларына жасалатын шабуылдар. Даркнетте Cutlet Maker деп аталатын банкоматтарға арналған жаңа зиянды бағдарламалық жасақтаманың тегін сатылып жатқандығы мамандармен анықталды. Оны бірнеше мың долларға сатып алып, шабуылдаушылар банкоматтардың ішін босатып кете алатын болған. Ол үшін шабуылдаушыларға қажетті нұсқаулар мен іс жүзінде барлық қажетті заттар беріледі. Кейбір бұзып кіретін ұрылардың бірқатары тонау жасауға тырысқан кезінде ұсталып жатты, бірақ вирус жазушылардың өздері шынайы джекпотты сындырды. Осы саладағы тағы бір үрдіс банк құрылымында іштей шабуылдар жасау деп аталады.

– Мақсатты шабуылдар. Silence – мақсатты шабуылдардың немесе APT (advanced persistent threats) өкілі. 2017 жылы 100-ге жуық хакерлік топтың белсенді жұмыс істейтіні бақыланған. 2016 жылмен салыстырғанда олардың саны екі есеге өскен. Сонымен қатар, мысалы, Silence сияқты олардың 10-ға жуық бөлігі, коммерциялық мүдделерге ие, ал басқалардың мақсаты – кибершпионаж және мемлекеттік органдар мен мұнай-газ компанияларының деректеріне арналған құмарлық. Хакерлік топтар белгілі бір саяси және экономикалық күштердің мүддесі үшін белсенді түрде жұмыс істей бастады. 2017 жылы анықталған мақсатты шабуылдардың жаңа векторы өнімдерін ірі компаниялар пайдаланатын бағдарламалық жасақтама жеткізушілеріне шабуыл жасау болды. Киберқылмыскерлер сіз көздеген мақсатты кәсіпорындардың қорғалмаған жүйелеріне шабуылдау жасау жеңіл екендігін анықтаған. Жақсы мысал ретінде белгілі Windows CCleaner тазалау бағдарламалық жасақтамасының өндірушісіндегі Axiom топтамасының сенсациялық шабуылын атауға болады. Онда хакерлер бағдарламаның жаңартылуына зиянды кодты енгізіп, оны бүкіл әлем бойынша шамамен 2 миллион қолданушы жүктеген. Шабуылдаушыларды нақты құрбандар қызықтырды: олар 20 ірі компанияны бөліп шығарды, ал зиянды жаңартулар жүйеге енгеннен кейін, олардың желіге шабуылын жалғастырды.

– Криптовалюты және майнинг. Жыл бойынша криптовалюта әлемдік экономикаға бұрынсоңды болмаған әсерін тигізді және венчурлық инвестициялар нарығын өзгертті: 2017 жылы ICO арқылы тартылған қаражат көлемі 3,5 млрд. долларды құрады, ал инвестицияларды тартудың дәстүрлі әдісі IPO әлдеқайда аз нәтиже көрсетті – 1 млрд. Мұнымен жаңа қатерлер мен осалдықтар

байланысты екендігі болжанады. Біріншіден, ол әр түрлі шабуылдар үшін мүмкіндіктер ашады – фишингтік сайттарды құру; сайтты бұзу және битокин-әмиянды ауыстыру» (Goodman, 2010: 312).

2018 жылы «Касперский Зертханасының» мамандары келесідей болжам жасады:

– бағдарламалық жасақтама өндірушілеріне (бағдарламалық жасақтама) одан да көп шабуылдардың болуы;

– банкоматтарға шабуылдарды автоматтандыру және оларды бұзу үшін «қорапты шешімдер». Зақымданудың барлық жаңа әдістері әзірленеді, соның ішінде, жойылғандарға да бұзып кіру мүмкін болады (McAfee, 2013);

– ОС төменгі деңгейінде жаңа құрылғыларға шабуылдар. Мақсатты шабуылдардың векторы дәстүрлі дербес компьютерлерден әртүрлі жаңа құрылғыларға – смартфондарға, IoT элементтеріне ауысады. Шабуылдаушылар операциялық жүйенің төменгі деңгейінде қауіпсіздік жүйелерінің басқару аймағынан қашу үшін жұмыс істеуге тырысады – мысалы, UEFI деңгейінде, операциялық жүйе тікелей іске қосылмай тұрып жұмыс істейтін процессордың микробағдарламасы;

– Бопсалау бағдарламаларын қолдана отырып, мақсатты шабуылдарды көбейту. Киберқылмыскерлер компанияға ірі компанияларға ұмтылуды үйренді, мысалы, салық төлеуден бірнеше күн бұрын, ExPetr шифрланған файлдарды шабуылдауға уақыт табады. Олардың мақсаты компанияға қысқа мерзімде құн төлетіп алу болып табылады;

– крипто-валютамен алаяқтық және блок-чейндағы виртуалды құндылықтарға шабуылдар, жасырын майнингтердің әр түрлі түрлері пайда болғаннан басқа, криптоәмиандарға шабуылдардың жаңа түрлері, сонымен қатар блокчейндегі осалдықтар пайда болады. Бүгінгі күні криптовалюталық құндылықтар қазірдің өзінде құрылып жатыр – мысалы, бүгінде аты әйгілі болған криптокотиктер – бұл құндылықтардың ұрлануы қалаған мақсатқа айналуы мүмкін» (Итоги, 2017).

Интернеттің еркіндігі: негізгі еркіндіктер мен жеке өмірді қолдау. Бұл бағытқа жататындар: азаматтық қоғам қайраткерлерінің еркін пікір білдіру және бірлесуге қажетті сенімді, қорғалған және қауіпсіз платформалар құруына қолдау көрсету; азаматтық қоғам және үкіметтік емес ұйымдармен бірлесе отырып, олардың интернет-белсенділігін заңсыз сандық шабуылдардан қорғау бойынша жұмыстар жүргізу; у коммерциялық мәліметтерді тиімді қорғау мақсатында халықаралық ынтымақтастықты ынталандыру; интернеттегі өзара әрекеттестікке қажетті ашық үйлесімділікті қамтамасыз ету. Көріп отырғанымыздай, халықаралық қауымдастықтың негізгі ойыншыларының кибер/ақпараттық қауіпсіздікті қамтамасыз етуге қатысты мәселелердегі көзқарастары біршама ерекшеленеді. Ақпараттық қауіпсіздікті қамтамасыз етуге қатысты ресейлік көзқарас негізінен ақпараттық кеңістіктен тарайтын қатерлерге баса назар аудару әдістемесінен тұрады. Ал американдық дискурс болса өз кезегінде киберкеңістікті түйсіну барысында оны мүмкіндіктер кеңістігі ретінде және оны игеру ұлттық және әлемдік даму мен гүлденудің нақты шарттарының бірі ретінде қарастырады. 1 дискурс аясында кибер/ақпараттық қауіпсіздікті қамтамасыз етудің басым себебі ретінде субъектінің үштік бейнесі тұлға-қоғам мемлекет пен оның мүдделерін ақпараттық кеңістіктен тарайтын қауіп-қатерлерден қорғау алынып, осы мәселеге назар аударылады. Ал 2 дискурс аясында көпшілік деңгейде кибер/ақпараттық қауіпсіздікті қамтамсыз етудің себебі ретінде желілік технологиялар беретін барлық мүмкіндіктерді толығымен игеру қарастырылады. Нәтижесінде дискурстарға жасалынған талдау негізгі үш ерекшеліктің бар екендігін көрсетеді. Бірінші ерекшелік жалпы кибер/ақпараттық қауіпсіздік түсінігінің мәніне қатысты. Ақпараттық қауіпсіздікке қатысты ресейлік пікір негізінен ақпараттық жалпыламалық мазмұнына басымдық жасап, киберкеңістік бұл жүйенің бір элементі ретінде қарастыруға бағытталған. Ақпарат табиғи және жасанды ретінде қарастырылады. Киберкеңістік жасанды орта және ақпараттық техникалық өлшемі ретінде танылады. «Кибермен» қатар, ақпаратқа адам санасындағы ой-пікір және кітаптар мен құжаттардағы ақпарат та жатады. Осылайша, пікірталаста ақпараттың тек «кибер» бөлігі ғана емес, барлық жақтарын қарастыру тиіс деген логикалық қорытынды жасалынады. АҚШ тек электронды инфрақұрылымда пайда болған мәліметтерді ғана қарастыруға мүдделі. Олар да киберкеңістіктен тыс ақпараттың бар екендігін мойындайды, бірақ ол қазіргі таңда соншылақты басым бағыт емес. Екінші ерекшелік мемлекеттік құрылымдардың интернетті реттеу саласындағы және қолданушылардың желілерге салып отырған контентке мемлекеттік бақылау жүргізуге қатысты мүмкіндіктері мен өкілеттілігіне байланысты. АҚШ ақпаратты

қорғауды, яғни оған цензура салуға немесе тұрғындардың ақпараттандырылуына бақылау орнатуды мүлдем қарастырмайды. Бұл идеяның негізінде тұрғындарды зиянды ақпараттан қорғаудың барынша тиімді жолы білімділікті арттыру мен толығымен хабардар болу деп санайды. Міне, осы ерекшеліктер ресейлік тарапты санауға және Батыс тарапынан түрлі ұсыныстар жасалынуына ықпал етті. РФ ұсыныстарын батыстықтар «өте үлкен көңіл қалушылық» деп бағалады. Ал ресейлік тарапты қолдаушылар ұлттық мемлекеттердің өз сегментінде интернеттегі контентке бақылау орнатуға қарсы болушылық АҚШ жаһандық киберкеңістіктегі басым болуының шарты ретінде таниды. Үшінші ерекшелік кибер/ақпараттық қауіпсіздікті қамтамасыз ету саласындағы негізгі қатерлерді нақтылауға байланысты. 2 дискурс аясында негізінен киберқауіпсіздікке (ЕО үшін) және «кибертерроризмге (АҚШ үшін) қарсы тұруға назар аударылса, 1 дискурс бойынша қоғам немесе мемлекетті тұрақсыздандыру мақсатында екі немесе одан да көп мемлекеттердің ақпараттық соғыс жүргізуі, және де мемлекетті қарсы тараптың мүддесіне қажетті шешімдер қабылдауға итемелеу саналады. Соған қарамастан, АҚШ киберқауіпсіздік саласындағы өзінің негізгі мақсаттарының бірі ретінде киберкеңістікке жаһандық бақылау орнатуды және кибернетикалық шабуылдық операциялар жүргізу мүмкіндігін қарастырады, өйткені бұл өзінің ақпараттық жүйесін және олардағы ақпаратты қорғау деп есептелінеді (Вус, 2018).

Қорытынды

Біздің мемлекетіміздің заманауи дамуы ақпараттық, кибернетикалық қоғам қалыптастырумен қатар жүреді. Жоғары технологиялар адам қызметінің бір бөлігіне кірді және қазақ халқының қоғамдық өмірінің көптеген салаларының дамуын алдын ала белгіледі. Жоғары технологиялардың ғасыры үнемі жетілдіріліп, қоғамның кең топтарына қол жетімді болып, киберкеңістіктегі қызмет ауқымы мен мүмкіндіктер кеңейіп келеді. Осының барлығы қоғам мен мемлекеттің дамуына ғана емес, сондай-ақ қылмыстық құқық бұзушылықтың жаңа түрін – киберқылмыстылықты туындатады (Tatarinova, Shakirov, Tatarinov, 2016: 1127).

Осыған байланысты киберқауіпсіздікті қамтамасыз ету саласындағы өзекті мәселелерді дәстүрлі әдістермен және құралдармен толығымен шешуге болмайды және көптеген киберқауіптерге төтеп бере алатын интеграцияланған қауіпсіздік механизмін құруда жүйелі тәсіл қажет. Біріншіден, бұл мемлекеттік органдардың, мемлекеттік емес құрылымдардың, бизнес пен қоғамның осы бағыттағы күш-жігерін үйлестіру. Екіншіден, киберқылмыс жасауға себеп болатын объективті жағдайларды және субъективті мәнжайларды, оларды жүзеге асыру тетіктерін, анықтауды, жолын кесуді, тергеуді жүргізуді және сот қарауындағы тәжірибені қамтитын киберқылмыспен күресудің барабар жүйесін дамыту.

Әдебиеттер

Sergazin E., Esimova Zh., Kozhakhmetova A., Mukasheva M. Security Strategy As A Factor In The Sustainable Development Of The Republic Of Kazakhstan. – Central Asia & The Caucasus. – 2018. – v.19 (1). – pp. 26-37

Борчашвили И.Ш. Комментарий к Уголовному кодексу Республики Казахстан. Особенная часть (том 2) / Под общ. ред. Генерального Прокурора Республики Казахстан, Государственного советника юстиции I класса Даулбаева А.К. – Алматы: Жеті Жарғы, 2015. – 1120 с.

Kai-Lung Hui, Seung Hyun Kim, Qiu-Hong Wang, Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. –Research Collection School of Information Systems. – 2017. – 41 (2). – p. 523

Parodi F., The concept of Cybercrime and Online Threats Analysis. – Int.J.Info. Sec. & Cybercrime. – 2013. – 2. – p.59

Қазақстан Республикасының Қылмыстық кодексі. Қазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ (12.07.2018 жылғы өзгерістермен және толықтырулармен). // http://adilet.zan.kz/kaz/docs

Broadhurst R., A New Global Convention on Cybercrime. – Pakistan Journal of Criminology. – 2010, v.2(4). – pp. 1-10

Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: дисс...канд. юрид. наук: 12.00.08. – Москва: Московский Университет МВД РФ, 2013. – 223 с.

Сачков И. Атаку можно совершить из любой точки мира, где есть интернет // https://www.kommersant.ru/doc

Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис..канд. юрид. наук: 12.00.08. – Москва: Российский государственный университет правосудия, 2016. – 232 с.

Медведев С.С. Мошенничество в сфере высоких технологий: дисс…..канд. юрид. наук: 12.00.08. – Краснодар: Кубанский государственный аграрный университет, 2008. – 210 с.

Goodman M., International Dimensions of Cybercrime. – Cybercrimes: A Multidisciplinary Analysis. – 2010. – Pp. 311-339

McAfee, 2013 Threats predictions // http://www.mcafee.com/us/resources

Итоги 2017 года и прогноз на 2018 год «Лаборатории Касперского» // https://www.kaspersky.ru/)

Вус М.А. Вопросы совершенствования и гармонизации законодательства государств-членов ОДКБ в сфере обеспечения информационной безопасности, 2018 http://iscs-expo.primexpo.ru

Lola F. Tatarinova, Karimzhan N. Shakirov, Danila V. Tatarinov, Criminological Analysis Of Determinants Of Cybercrime Technologies. – Iejme – Mathematics Education. – 2016, v. 11(5). – pp. 1127-1134

References

Sergazin E., Esimova Zh., Kozhakhmetova A., Mukasheva M. Security Strategy As A Factor In The Sustainable Development Of The Republic Of Kazakhstan. – Central Asia & The Caucasus. – 2018. – v.19 (1). – pp. 26-37

Borchashvili I.Sh. Commentary on the Criminal Code of the Republic of Kazakhstan. Special part (volume 2) / Under total. ed. Prosecutor General of the Republic of Kazakhstan, State Counselor of Justice Class I Daulbayev AK – Almaty: Zheti Zharky, 2015. – 1120 p.

Kai-Lung Hui, Seung Hyun Kim, Qiu-Hong Wang, Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. –Research Collection School of Information Systems. – 2017. – 41 (2). – p. 523

Parodi F., The concept of Cybercrime and Online Threats Analysis. – Int.J.Info. Sec. & Cybercrime. – 2013. – 2. – p.59

Criminal Code of the Republic of Kazakhstan. The Code of the Republic of Kazakhstan dated July 3, 2014 No. 226-V (with amendments and supplements 12.07.2018)// http://adilet.zan.kz/kaz/docs

Broadhurst R., A New Global Convention on Cybercrime. – Pakistan Journal of Criminology. – 2010, v.2(4). – pp. 1-10

Chekunov I.G. Criminological and criminal law support for the prevention of cybercrime: diss ... cand. legal Sciences: 12.00.08. – Moscow: Moscow University of the Ministry of Internal Affairs of the Russian Federation, 2013. – 223 p.

Sachkov I. Attack can be made from anywhere in the world where there is Internet // https://www.kommersant.ru/doc

Prostoserdov MA Economic crimes committed in cyberspace, and measures to counter them: dis..kand. legal Sciences: 12.00.08. – Moscow: Russian State University of Justice, 2016. – 232 p.

Medvedev S.S. High-tech fraud: diss ... ..cand. legal Sciences: 12.00.08. – Krasnodar: Kuban State Agrarian University, 2008. – 210 p.

Goodman M., International Dimensions of Cybercrime. – Cybercrimes: A Multidisciplinary Analysis. – 2010. – pp 311-339

McAfee, 2013 Threats predictions // http://www.mcafee.com/us/resources

Results of 2017 and the forecast for 2018 of Kaspersky Lab// https://www.kaspersky.ru/)

Vus M.A. Issues of improving and harmonizing the legislation of the CSTO member states in the field of ensuring information security, 2018 http://iscs-expo.primexpo.ru

Lola F. Tatarinova, Karimzhan N. Shakirov, Danila V. Tatarinov, Criminological Analysis Of Determinants Of Cybercrime Technologies. – Iejme – Mathematics Education. – 2016, v. 11(5). – pp. 1127-1134