УДК 343.7

КИБЕР ҚАУІПСІЗДІКТІ ҚҰҚЫҚТЫҚ ҚАМТАМАСЫЗ ЕТУДІҢ ТЕОРИЯЛЫҚ ЖӘНЕ ҚҰҚЫҚТЫҚ АСПЕКТІЛЕРІ

Сапарбекова Бибінұр Ернарқызы
saparbekova.b.e@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Заң факультетінің 2 курс студенті,
Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – з.ғ.к., доцент Муратханова М.Б.

Біздің өміріміз ғаламтор мен ақпараттық-компьютерлік технологиялармен өте тығыз байланысты. Бүгінгі таңда дербес компьютерді қолданбайтын сала жоқ. Атап айтқанда, жұмыс істеу, жүйелік, электронды поштамен хат алмасу, банк істерін жүргізу, интернеттен керек мағлұматтарды алу, зат сатып алу.

Ақ болмай қара болмайды дегендей, өкінішке орай ақпараттық технологиялар тұрмысқа кеңінен енген сайын ақпараттық қауіп-қатер де өршіп барады.

ҚР Қылмыстық кодексінің «Ақпараттандыру мен байланыс саласындағы қылмыстық құқықбұзушылықтар» деп аталатын 7-тарауы киберқылмыстарға арналған. Онда осы саладағы құқықтық қатынастарды реттейтін және қылмыстық жауаптылықты көздейтін 9 бап бар. Атап айтқанда, 209-бапта былай деп жазылған: «Күш қолдану не мүлікті жою немесе бүлдіру қатерін төндіріп, сол сияқты, жәбірленушіні немесе оның жақындарын масқаралайтын мәліметтерді не жариялануы жәбірленушінің немесе оның жақындарының мүдделеріне елеулі зиян келтіруі мүмкін өзге де мәліметтерді тарату қатерін төндіріп, электрондық жеткізгіште сақталатын, ақпараттық жүйеде қамтылатын немесе телекоммуникациялар желісімен берілетін, заңмен қорғалатын ақпаратты беруге мәжбүрлеу - белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналасу құқығынан екі жылға дейінгі мерзімге айыра отырып немесе онсыз, екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады» [6].

Өйткені, қазіргі заманғы киберқылмыстар мәселесі егжей- тегжейлі қарастырылуда, себебі, қылмыс саны көбеюде және олар қарапайым ұсақ бұзушылықтардан бастап жаһандық аппаттарға дейін алуан түрлі болып келеді. Негізінен алғанда, БҰҰ анықтамасы бойынша киберқылмыс - компьютерлік жүйе немесе желілік жүйе немесе желіде, желі арқылы жасалуы мүмкін қандай да бір әрекет немесе әрекетсіздікті айтамыз. Осылайша, киберқылмыс электрондық ортада жасалған кез келген қылмысқа жатқызылуы мүмкін.

Киберкеңістіктегі қылмыс - компьютерлердің, компьютерлік бағдарламалардың, компьютерлік желілердің жұмысына, компьютерлік деректерді рұқсатсыз өзгертуге, сондай-ақ компьютерлермен, компьютерлік желілермен және бағдарламалармен жасалатын басқа да заңсыз әлеуметтік қауіпті актілерге заңсыз араласуы [7].

Өкінішке қарай, Қазақстанға қылмыскерлердің қызығушылығы өсті, бұл киберқауіпсіздік мамандарының аудит деректері бойынша орташа есеппен 2016 жылдың екінші жартысында өнеркәсіптік кәсіпорынның әрбір үшінші компьютері ай сайын кибер-шабуылға ұшыраған. Барлығы осы кезеңде кәсіпорындардың технологиялық желісімен байланысты кейбір компьютерлердің 54% зиянды бағдарламамен соқтығысқан. Мұндай деректер «Өнеркәсіптік автоматтандыру жүйелеріне қауіп төндіретін жерлер» зерттеуінде келтірілген. 2016 жылдың екінші жартысы» ICS CERT «Касперский зертханасының» өнеркәсіптік және сыни нысандардағы компьютерлік инциденттерге жауап беру орталығында көрсетілген мәліметтер бойынша Қазақстан Республикасындағы 2016 жылғы өнеркәсіптік компьютерлерге шабуылдардың статистикасы, яғни сандық мәліметтері керсетілген. «Кибертерроризм» сияқты құбылыстың беталысы қоғамға үлкен қауіп төндіріп отыр.

Жаңа және жеткілікті дәрежеде зерделенбеген құбылыс болғандықтан, кибертерроризм жеке назарға алуды қажет етеді және адамзат үшін қауіпті болып табылатын осы мәселені шешуде ерекше тәсілдерді талап етеді. Бұдан басқа, террористер қатарына адам жалдау ғаламтордың коммуникациялық арналары Зерттеу нәтижелері бойынша 2016 жылы Қазақстандағы «Касперский Лабораториясы» анықтаған әрбір төртінші мақсатты шабуыл машина жасау, энергетика, химия, көлік және бас қа салалардағы кәсіпорындарға бағытталған . Сарапшылар өнеркәсіптік автоматтандыру жүйелеріндегі 75 осалдықты, яғни кемшіліктерді анықтады, олардың 58-і кәсіпорындардың қауіпсіздігі үшін аса маңызды болып табылады. Сондай-ақ, ICS CERT технологиялық желілерде шамамен 20 мың зиянды бағдарламаның модификацияларын тапты [8].

Осы орайда, тергеп-тексеру және қылмыскерлерді ұстау үдерісі қиындай түседі. Бұған мынадай мысал келтіруге болады. Алматы қаласында «Интернет-банкинг» электрондық жүйесі арқылы кәсіпкерлердің шоттарынан ақша ұрлаумен айналысқан қылмыстық топ анықталды. Тергеуде айқындалғандай, қылмыскерлер Бас прокуратураның атынан ғана емес,

сонымен қатар, Салық комитетінің, Қаржы министрлігінің, аталған министрліктегі Мемлекеттік кірістер комитетінің және әртүрлі қызметтердің де атынан хаттар жіберген. Кәсіпкерлер қауіп төндіретін бағдарламаны қосқаннан кейін оның белсенділендірілуі жүргізілген. Зақымданған компьютер мен құпия ақпаратқа қашықтан қол жеткізуге ие болу мүмкіндігі туындағаннан кейін, қылмыскерлер екінші деңгейлі банкте алдын-ала ашылған шоттарына ақша аударған.

«Кибертерроризм» сияқты құбылыстың беталысы қоғамға үлкен қауіп төндіріп отыр. Жаңа және жеткілікті дәрежеде зерделенбеген құбылыс болғандықтан, кибертерроризм жеке назарға алуды қажет етеді және адамзат үшін қауіпті болып табылатын осы мәселені шешуде ерекше тәсілдерді талап етеді. Бұдан басқа, террористер қатарына адам жалдау ғаламтордың коммуникациялық арналары арқылы жиі жүргізілетіндігі дәлелденіп, айқын факт ретінде тіркелген. Ең озық зомбылау мен сана-сезімді бағдарламалау технологиялары террористер арнайы ашқан сайттарда анық көрсетіледі.

Сондықтанда ақпараттық қауіпсіздік саласында отандық заңнаманы және мемлекетаралық ынтымақтастықты жетілдіру қажет [9].

Қазақстан Интернет желісінде экстремистік кадрларды іріктеу және насихаттаумен күресу үшін кибер қауіпсіздік тұжырымдамасын әзірлейді. Бұл туралы ҚР Қорғаныс министрлігінің және Аэроғарыштық өнеркәсіптің өкілдері хабарлады. Хабарламаға сәйкес, жүздеген радикалды қазақстандықтар Сирия мен Ирактағы боевиктер тарапында соғысуда.

Құқық қорғау органдарының мәлімдеуінше, Қазақстанда киберқылмыстардың саны жылдан-жылға артып келеді. Дегенмен, ол нақты сандық мәліметтер көрсетпеді. Қазақстанда «электрондық шекара деп аталатын байланыс желілерін орталықтандырылған басқару жүйесі бар. Қауіпсіздік сертификаты ел аумағынан шифрлау арқылы заңсыз ақпаратты шектеуге мүмкіндік береді. Өткен жылы үкімет 110 мыңнан астам экстремистік және басқа да интернет-ресурстарды блоктады немесе жойды [10]. Бүгінде халықаралық қоғамдастықта киберқауіпсіздік мәселелері ұлттық қауіпсіздік басымдықтарының бірінші тізімінде. Кибер- қауіпсіздікті күшейту мақсатында Орталық коммуникациялар қызметінде «Қазақстанның киберщит» туралы мәселе қаралуда. Жалпы алғанда, тұжырымдаманы іске асыру екі кезеңнен тұрады, олар мыналар: 2017-2018 жыл бірінші кезең, 2019-2022 жыл екінші кезең.

Бірінші кезеңде:

- ақпараттық қауіпсіздікті қамтамасыз ету саласында белгіленген талаптарға сәйкестігі туралы егжей-тегжейлі атқару практикасы әзірленеді;
- білім беру бағдарламалары мен кәсіби стандарттарға аудит жүргізіледі, ақпараттық қауіпсіздік саласындағы білікті мамандардың саны мен сапасы арттыру, осы салада жұмыс істеп тұрған қызметкерлердің біліктілігі жаңарту;
- отандық әзірлемелерді құру кезінде өнеркәсіп пен ғылым арасындағы өзара іс-қимыл мен ынтымақтастықтың тиімді схемасын құру.

Екінші кезеңде:

- Қазақстанның ақпараттық технологияларының ұлттық ақпараттық - коммуникациялық инфрақұрылымын ақпараттық қауіпсіздік жүйелерімен қамтамасыз етуге Қазақстандық IT компаниялардың қатысуы;

- Мемлекеттік органдардың және квази мемлекеттік сектордың телекоммуникациялық жабдықтарын сатып алуға, тапсырыстары бар отандық кәсіпорындардың электроника өнеркәсібіне жүктелуі [11].

Қазақстан Республикасының Қорғаныс министрлігі және Аэроғарыш саласы үш ай ішінде Қазақстан Республикасының Үкіметі үшін 2017-2022 жылдарға дейін «Киберқауіпсіздік» тұжырымдамасын (Қазақстанкиберщиті) іске асыру жөніндегі іс-шаралар жоспарын әзірлейді және ұсынады [12].

Біздің пікірімізше, киберқылмыстың алдын алу үшін қазірден бастап мектептерде жеке деректерді қорғау туралы бағдармалар әдістемесін енгізу қажет және IT-жүйесін мамандығы бойынша гранттарды арттырып, ал университеттерде оқу бағдармалары қазіргі технологиялық заманға сай болуы керек.

Американдық тәжірибеге сүйенсек, оларда киберқауіпсіздікке байланысты арнайы қыз-меттер бар, соның ішінде, Oasis жүйесін дайындаған ЦРУ және ФБР-дің қол жеткізген жетістіктері көп.

Бұл жүйе қылмыскерлердің ақпарат алмасуға кедергі жасап ғана қоймай, сондай-ақ күдіктілердің компьютерлерін бұзу үшін де мүмкіндік береді. Бұл Киберщит атты бағдарлама осындай жетістіктерге жетеді деген сенімдеміз.

Пайдаланылған әдебиеттер тізімі:

1. Қазақстан Республикасының Президенті Н. Назарбаевтың «Төртінші өнеркәсіптік революция жағдайындағы дамудың жаңа мүмкіндіктері» атты 10 қаңтар 2018 жылы Жолдауы// http://ksu.kz

2. Киберқауіпсіздік тұжырымдамасын бекіту туралы ҚР Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысы

3. С.С., Нұрпейісов Д. Тәуелсіз Қазақстан - егеменді мемлекет. - Алматы, 2004. -57 б.

4. Ю.М. Право и политика в компьютерном круге.- М.: Наука, 1987.- 112 с.

5. Петренко С.А., Симонов. С. В. Управление информационными рисками. Экономически оправданная безопасность – М.: Компания АйТи, ДМК Пресс, 2004. – 384 с.

6. Қазақстан Республикасының Қылмыстық Кодексі 2014 жылғы 3 шілдедегі № 226- V ҚРЗ қабылданған. (11.07.2017 жылғы өзгертулер мен толықтыруларды қоса алғанда)

7. Концепция информационной безопасности Республики Казахстан. Одобрена Указом Президента Республики Казахстан от 10 октября 2006 г. № 199// Информационная система «Параграф».

8. Ваганов ПЛ. Правовая защита киберпространства в США // Правоведение. - 2006. - №4. - С. 73-88.

9. Правовое обеспечение информационной безопасности: Учебник / Под общ. научной ред. В.А.Минаева, А.П. Фисуна, СВ. Крыля, СВ. Дворянина, М.М.Никитина, Н.СХохлова. - М.: Маросейка. 2008. С.

10. Бердібаев Р. Қазақстан Республикасында ақпараттық қауіпсізднсті қамтамасыз етудің саяси механизмдер. - Алматы. - 2010. - 212 б.

11. Сарсенбаев А. Стратегия формирования информационной политики Республики Казахстан в переходный период: дис. д-ра полит, наук. - Алматы, 2000. - 225 с.

12. Қазақстан Республикасының Қорғаныс министрлігі және Аэроғарыш саласы үш ай ішінде Қазақстан Республикасының Үкіметі үшін 2017-2022 жылдарға дейін «Киберқауіпсіздік» тұжырымдамасы.