УДК343.9

КИБЕРҚЫЛМЫС ЖӘНЕ ОНЫҢ ТҮРЛЕРІ

Болат Айым Мұхийқызы
Aiym-97@mail.ru
Л.Н.Гумилев атындағы Еуразия ұлттық университетінің 4 – ші курс студенті
Ғылыми жетекші: Смағамбет Б.Ж., ә.ғ.к., доцент, әлеуметтану кафедрасының профессоры

Киберқылмыс - интернетті және цифрлық технологияларды өз мүдделеріне қол жеткізу үшін заңсыз пайдаланудан туындаған, кез-келген қылмыс сияқты, бір адамның немесе адамдар тобының әрекеті. Киберқылмыскерлер банк шоттарында санкцияланбаған операциялар жасау, ақшаны ұрлау, алаяқтық жасау, қорқыту немесе ботнеттердің кең желісінде вирус жұқтырған компьютерді пайдалану үшін жоғары мамандандырылған білім мен дағдылардың толық арсеналын пайдаланады.

«Компьютерлік қылмыс» ұғымы ең алғаш өткен ғасырдың 60-ыншы жылдары алдымен американдық, одан соң өзге де әлемдік басылымдарда пайда болды. 1983 жылы Париж қаласында OECD (Халықаралық экономикалық ынтымақтастық және даму ұйымы) сарапшылары бас қосып, компьютерлік қылмысқа криминологиялық анықтама берді. Этикалық-тәртіптік қағидаттарға қайшы келетін іс-әрекеттер, сондай-ақ автоматтандырылған мәліметтерге қол сұғушылық сол кезден бастап қылмыстық санатқа жатқызылатын болып шешілді.

1990-шы жылдардың басында тараған әлемдік «Киберкеңістік» термині жеке адамдар мен топтардың өзара әрекеттесуі ақпараттық-коммуникациялық технологиялар арқылы қосылған электронды желілер арқылы жүзеге асырылатын онлайн-әлемді сипаттау үшін практикалық қолданысқа енді. Мануэль Кастельс осыған байланысты «коммуникациялық гибридті» табиғи кеңістікті және киберкеңістікті қосатын орын деп атайды.

30 жыл бойы киберкеңістіктің айналасында белсенді пікірталастар болғанына қарамастан, бұл тұжырымдаманың әлі де түсінікті анықтамасы жоқ және көптеген социологиялық анықтамалықтарда бұл термин кездеспейді.

Киберкеңістік ұлттық-мемлекеттік шекаралармен бөлінбейді. Киберкеңістік байланыс үшін шексіз мүмкіндіктерді ұсынады. Көптеген әлеуметтік теоретиктер үшін киберкеңістік ішкі қарым-қатынас тұрғысынан – әлеуметтенудің жаңа нысандарын, сондай-ақ нақты географиялық, табиғи кеңістік жағынан қызықтырады.

Қарқынды ғылыми-техникалық прогрестің арқасында ақпараттық және телекоммуникациялық технологиялар қарапайым адамдардың өміріне тамыр жайып кетті, олардың көпшілігі өздерін байланысу құралғыларсыз, электронды төлем жүйелерінсіз және т.б. елестете алмайды. Осы прогреске байланысты киберқылмыс та өсе бастады. Киберқылмыс - Қазақстанда өзекті мәселелердің бірі.

2004 жылдың сәуір айында Алматы қаласының ішкі істер департаментінде киберқылмыспен күресуге арналған жаңа жедел бөлімше ашылды. Ол «К» деп аталды. Ол IT-технология саласындағы ең озық мамандардан тұрды, олар хакерлердің ізін, басқа бөлімдерден келген әріптестердің көмегінсіз біле алатын.

2006 жылы осындай қылмыстармен жүйелі күресу үшін ақпараттық технологиялар саласындағы қылмыспен күресудің Ұлттық байланыс пункті құрылды, ақпараттық технологияларға байланысты қылмыстар үшін қылмыстық жауапкершілікті арттыру туралы Қазақстан Республикасының заңнамасына қажетті өзгерістер енгізілді. Сондай-ақ, банктік мекемелердің өкілдерімен кездесулер өткізілді, онда электронды алаяқтық фактілерін анықтау үшін келісімдер мен ынтымақтастық туралы келісімдерге қол жеткізілді. Жоғарыда айтылғандай, ақпараттық технология саласындағы қылмыстар - көбінесе халықаралық, яғни қылмыскерлер бір мемлекетте жұмыс істейді, ал олардың құрбандары басқа мемлекетте.

Жалпы алғанда, Қазақстан Республикасының Қылмыстық кодексінің 227-бабына сәйкес компьютерлік ақпаратқа рұқсатсыз қол жеткізу, компьютерлік зиянды бағдарламаларды жасау, пайдалану және тарату туралы тіркелген қылмыстар санының статистика бойынша қарқынды өсіп отыр. Халықаралық электробайланыс одағының (ITU) есебіне сәйкес, Қазақстан Ғаламдық киберқауіпсіздік индексінде 40-шы орынды иеленді.

2019 жылы Қазақстан өз позициясын былтырғы рейтингке (82-орын) қарағанда, 42 деңгейге жақсартты. Нәтижесінде, биылғы жылы біздің мемлекет кибершабуылдарға қарсы тұруға дайындық деңгейі жоғары елдер тізіміне енді [2].

Қазақстанның ақпараттық қауіпсіздік қауымдастығы төрағасы Виктор Покусов қазақстандықтардың жиі ұшырайтын киберқылмыс түрлерін атап көрсетті. «Боттардан шабуылдар, яғни шабуыл жасайтын автоматтандырылған жүйе жетекші болып келеді, зиянды бағдарламалық жасақтамаға шабуыл жасау екінші орында тұр, шабуылдардың бұл екі түріне барлығы 60% тиесілі» [3].

Қазақстанда байқалған киберқылмыс ішінде қоғамдық қауіпсіздікті бұзатын қылмыстар, яғни террорлық мақсат үшін киберкеңістікті пайдалануды кездестіреміз (мысалы, қылмыс жасауға шақыру). Яғни ақпараттық процестердің жаһандануы лаңкестік-кибер-терроризмнің жаңа түрінің пайда болуына түрткі болды. Сонымен қатар, фишинг - әртүрлі жеке мәліметтерді (парольдерді, логиндерді, банктік карталардың нөмірлерін және шоттарын) анықтауға тырысатын онлайн-алаяқтық әдісі. Мәселен, сізді әртүрлі шағымдар бойынша жеке ақпаратты шығаруға болатын банк сияқты нақты көрініске ұқсас жалған сайттарда фишинг сілтемесіне кіруге шақырады.

Әлеуметтік желінің профилін, мысалы, спамның жіберілуі, жеке деректерді пайдаланып, бопсалауды, ақшаны жасыруды жатқызуға болады. Бұл құбылыс - цифрлық жеке тұлғаны ұрлау деп аталады.

Келесі жиі кездесетін түрі – спам. Спам жарнамаларды немесе зиянды бағдарламаларды таратуға арналған жарнамалар, жалған хабарларды қамтиды. Пайдаланушыға жеткізілген қауіп-қатер, тарату құны өте төмен екеніне байланысты және жаңа электрондық пошта мекенжайларын оңай тауып, хабарламаларды заңсыз жіберу жолдары үшін спам авторларының иелігінде көптеген құралдар бар.

Киберқылмыстың көп тараған түрі –хакерлік. Хакер - өте білікті IT-маман, компьютерлік жүйелерді жақсы түсінетін адам. (Бастапқыда, хакерлерді бағдарламалық жасақтаманың қателіктерін тез және кәсіби емес түрде түзететін бағдарламашылар деп атаған). Дегенмен, көптеген адамдар хакердің жеке ақпараттық желілерге, банк деректеріне және т.б. кіретін, құпия ақпаратқа, сондай-ақ вирустарды тарататын компьютер хакерлері деп есептейді.

Хакерлер – екі топқа бөлінеді, бірі – бағдарламаны алдын ала әзірлеу барысында оның ішіне тез арада құжатсыз өзгертулер енгізіп жіберетін компьютер мамандары. Екіншілері – құпия ақпараттарды шаршамай-талмай тек қана аңдып, ұрымтал сәтті күтіп отыратын алаяқтар.

Сондай-ақ, телекоммуникациялық қылмыс. Бұқаралық ақпарат құралдары мен коммуникациялар арқылы жасалған қылмыстар. Олардың ішіндегі ең танымалы - зардап шегушінің құрал-жабдықтарын шамадан тыс жүктеу және оның әдеттегідей қолданылуына жол бермеу (DDOS-шабуыл).

Клиенттерге электрондық пошта арқылы жіберілген хабарларды шифрлаудың соңғы технологиясын қолданып, есірткінің заңсыз айналымын жүргізеді. Осы хабарламаларда саудагер курьерді пайдалана отырып, көбіне жасырын түрде ақша үшін тауарларды айырбастауға арналған орын мен әдісті белгілейді.

Осылайша, киберқылмыс - компьютерлік жүйелер мен компьютерлік желілер арқылы орындалатын қылмыстардың жиынтығы.

Киберқылмысқа барудың қарапайым мақсаттары:

- ақшаны, бағалы қағаздарды, несие, материалдық құндылықтарды, тауарларды, қызметтерді, артықшылықтарды, жеңілдіктерді, квоталарды, жылжымайтын мүлікті, отын, шикізат пен энергетикалық ресурстарды заңсыз алу;

- салықтарды, алымдарды, айыппұлдарды төлеуден жалтару;

- қылмыстық кірістерді заңдастыру;

- жалған құжаттарды, мөртабандарды және т.б. жеке пайда табу мақсатында қолма-қол ақшаны жалғандау немесе жасау;

- жалған немесе саяси мақсаттар үшін құпия ақпаратты алу;

- бопсалау, бәсекелестікті жою немесе саяси мақсаттар үшін мекеменің, кәсіпорынның немесе жүйенің жұмысын бұзу;

- басқа қылмысты жасыру ниеті;

Киберқылмыс көбінесе экономикалық мақсаттарда орындалады. Бұл, мысалы, қолма-қол ақша мен құпия ақпаратты ұрлау түріндегі экономикалық залал болуы мүмкін. Басқа мақсаттарға саяси - негізгі мемлекеттік және саяси институттарға зиян келтіріп, билік қарым-қатынастар жүйесін және үкіметке деген сенімін төмендетеді. Мақсаттардың үшінші түрі - идеологиялық: идеяларды және идеологияларды интернет пайдаланушыларды, мысалы, радикалды террористік және ұлтшыл топтар қатарына қосу мақсатында тарату. Ақырында, социопсихологиялық мақсаттарды азаматтарға адамгершілік және психологиялық зиян келтіретін төртінші мақсат түрі ретінде қарастырамыз.

Жаңа ақпараттық технологиялар тек қана заңның бұзушыларымен қылмыс жасау құралы ғана болу тиіс емес, сондай-ақ әртүрлі қауіп-қатерлерге, соның ішінде барлық қылмыспен күресу көріністеріне тиімді шабуыл құралы болу керек, сондықтан да компьютерлік қылмыспен қарсы күреске жоғары білікті мамандарды тарту керек.

Пайдаланған әдебиеттер тізімі:

1. https://primeminister.kz/ru/page/view/gosudarstvennaya_programma_digital_kazahstan
2. https://informburo.kz/novosti/kazahstan-podnyalsya-na-42-pozicii-v-reytinge-kiberbezopasnosti.html
3. https://informburo.kz/novosti/specialisty-nazvali-lidiruyushchie-vidy-kiberprestupnosti-v-kazahstane.html
4. Сериева М. М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. — 2017. — №1. — С. 104-106.
5. Карпова Д. Н. (2014). Киберпреступность: глобальная проблема и ее решение. М.: МГМИО(У), 47 с.