Ф. Теміртас, 3-курс
Ғылыми жетекшісі: Д. Ө. Өзбеков, заң ғылымдарының кандидаты, доцент (Е. А. Бөкетов атындағы Қарағанды мемлекеттік университеті)

КИБЕР ҚЫЛМЫСТАР

Көптеген төңкерістік технология сияқты Internet ғаламдық желісі өрлеумен қоса қиянат етушілікке үлкен мүмкіндіктер туғызады. Желідегі шабуылдар, пластикалық төлем карточкаларымен алаяқтық, банктік шоттардан қаражат ұрлау, корпоративтік тыңшылық, балалық порнографияны тарату — бұл Internet желісінде жүрген қылмыстардың тек бірнешесі ғана. Мұндай құқықбұзушылық әрекеттер әлемнің көптеген басқа еліне ғана емес, сонымен қатар біздің мемлекетке ұлттық қауіпсіздіктің жасаушысы — ақпараттық қауіпсіздікке қатер төнгізетін маңызды қоғамдық қауіп-қатерді құрайды[1].

Мемлекеттің ұлттық инфрақұрылымы бүгінде замандас компьютерлік технологияларды қолданумен тығыз байланыста. Энергетикалық және банктік жүйелердің, әуе көлігін басқарудың, көліктік жүйенің, тіпті жедел медициналық көмектің күнделікті қызметі автоматтандырылған электронды-есептеуіш жүйелердің сенімді және қауіпсіз жұмыс жасауына толығымен тәуелді[2].

Компьютерлік технологияларды қолдану аясындағы қылмыс (киберқылмыс) — қазіргі заманғы компьютерлік технологияларды енгізу және дамыту деңгейіне, оларды жалпы қолдану және оларға рұқсат беруге тікелей тәуелді деңгей болып табылатын халықаралық

маңызды құбылыс. Осымен, Қазақстан Республикасында ақпараттандырудың екпінді дамуы мемлекеттің ұлттық қауіпсіздігіне қатер төндіретін белгілі шараларды, пайдақор және басқа түрткілерді қамтитын компьютерлік технологияларды потенциалды қолдануды құрайды[3].

Киберқылмыскердің негізгі мақсаты әртүрлі процестерді басқаратын компьютерлік жүйе және онда таралатын ақпарат болып табылады. Шын өмірдегі қарапайым қылмыскерге қарағанда киберқылмыскер дәстүрлі пышақ және пистолет секілді қаруды қолданбайды. Оның арсеналы — ақпараттық қару, желіге ену, бағдарламалық қамтамасыз етуді бұзу және модификациялау, ақпаратты рұқсатсыз алу және компьютерлік жүйенің жұмысын уақытша тоқтатуға қолданылатын барлық құралдар. Киберқылмыскердің қаруына мыналарды жатқызуға болады: компьютерлік вирустар, бағдарламалық белгілер, компьютерлік жүйелерге рұқсатсыз кіруге мүмкіндік туғызатын шабуылдың әр түрі.

Қазіргі заманғы компьютерлік қылмыскерлерде тек дәстүрлі құралдар ғана емес, сонымен қатар қазіргі ақпараттық қарулар мен құралдар бар; бұл мәселе ертеден мемлекеттің шекарасынан өтіп халықаралық мәнге ие болды. Киберқылмыс мәселесі қазіргі уақытта ерекше маңызды болып отыр. Жоғары дамыған елдердегі әлеуметтік сұраулар халық арасында үрей туғызатын киберқылмыс мәселесі маңыздылардың бірі болып табылатынын көрсетеді. Бұл құбылыс қылмыскерлердің қазіргі заманғы жаңа ақпараттық технологияларды қолдануына байланысты, сонымен қатар қазіргі индустриалды қоғамның өсуші осалдығы арқылы, 5 жыл бұрынмен салыстырғанда аса маңызды қауіпті құрайды. Киберқылмыскерлермен күресуге мемлекеттердің күш-жігеріне қарамастан, әлемде олардың саны азаймай, қайта тым көбеюде[4].

Киберқылмыстармен күресудің тиімді тетіктерінің жоқтығы әрбір мемлекеттің ұлттық қауіпсіздігіне тағы да бір қатер болып анықталады. Мұндай жағдайда Қазақстан Республикасы демократиялық тәуелсіз мемлекет ретінде компьютерлік қылмысқа қарсы тұру мәселелерінен, сонымен қатар оның трансұлттық (трансшекаралық) формалары бөлігінде, шетте қалмауы тиіс. Компьютерлік қылмыстардың әдеттегі категорияларын және бүгінде қоғамның түйіскен келеңсіз оқиғаларын қарастырайық[5].

Инсайдерлер (Insiders) — ішкі ақпаратқа рұқсаты бар адамдар. Олар өз жұмыс берушілеріне қарсы жиі наразылық туғызушылар. Инсайдер (қызметкер немесе жұмыстан босатылған компания қызметкері) әлеуметті қылмыскер болып табылады. Компанияның компьютерлік жүйесінің жұқалығымен таныс, ол компанияның меншігі болып табылатын ақпаратты заңсыз алу мақсатында немесе автоматтандырылған электронды-есептеуіш машиналардың, олардың жүйесі мен компьютерлік желілеріне заңсыз араласу мақсатында жүйеге шексіз рұқсаты бар болып табылады[6].

Сонымен қатар хакерлер (Hackers) де үлкен қауіп туғызады. Кейде олар желілерді өткір сезім үшін немесе хакерлік ортада беделді жаулап алу үшін бұзады. Бірақ кейде бұл қаржылық мақсатта немесе басқа да жамандықтарға байланысты жасалады. Қағида ретінде хакерлер — бірегей мүмкіндіктері бар ақпараттық техниканың жақсы білгіштері, сондықтан оларға қашықтықтағы компьютерлік желілермен манипуляциялау айтарлықтай мәселе болып табылмайды: олар рұқсатсыз мәтіндерді және пайдаланушылардың компьютерінің сайттарына World Wide Web-тен хаттамаларды көшіреді[7].

Компьютерлік қиянат жасау мүлдем әртүрлі: бұл Интернет арқылы тауарлар мен қызметтерді жалған ұсыну, хакерлік шабуылдарды, электронды төлем карточкалары және электронды төлем жүйелерінің клиенттерінің шоттарымен аферaларды ұйымдастыру бойынша қызметтер. Өткен жылы мұндай 450-ден астам қылмыстың көзі жойылды. Статистиканың көрсетуінше, 43 пайызы оқиғада компьютерлік қиянаткерлердің құрбандары (алдын ала төлем арқылы, қандайда бір тауарды өте төмен бағамен сату ұсыныстарына пайдаланушы қызығушылық білдіргенде) онлайн аукциондардың қатысушылары болып табылады. Интернеттің қауіпсіздігі дара абыржытулықты танытады. Желіде қауіпсіздік мәселесіне аса назар аударудың қажеттілігі шын өмірдің виртуалды өмірмен баяғыда теңескенінен туындайды. Компьютер туғызатын келеңсіз жағдайлар, шын өмірдегі жағдайлар секілді: вирустар, ұрлық және тонау, дөрекілік және қуғындау, күштеп алушылық және қатер, этикалық емес және жабысқақ жарнама, терроризм мен экстремизм. Хакерлермен ұрланған ақша баяғыдан миллиардтармен есептеледі және де кейбір вирустарға көптеген ай мерзімінде қарсы тұру шаралары табылмайды[8].

Статистиканың көрсетуі бойынша:

-хакерлермен шабуылданатын компьютерлердің 86 пайызы үйдегі;

- Спам әлемдегі электрондық поштаның бақыланатын трафигінің 54 пайызы, ал Ресейде 82 пайызы трафикті құрайды;

-2006 ылдың маусымына фишингтік хаттамалардың саны (желілік қиянаткерлікпен байланысты) 81 пайызы құрады;

-зиянды вирустардың зарарсыздандыру түрлерінің 18 пайызы жаңа;

-4,2 млн сайттар — порнографиялық;

- блоггерлердің 55 пайызы өздерінің Интернет-күнделіктерін шын өмірдегі келеңсіз оқиғалардан қауіптеніп, жалған атпен жазады.

Компьютерлік қылмысқа қарсы тұру мәселесі — бұл кешендік мәселе. Бүгін заңдар технологиялар дамуының қазіргі заманғы деңгейіне сәйкес талаптарға сай болуы қажет. Осы мақсатпен телекоммуникациялық желілерде ақпаратты таратуды реттейтін заңнаманы жетілдіру бойынша мақсатты бағытталған жұмыс өткізілуі тиіс. Құқық қорғаушы органдардың, арнайы қызметтердің, соттық жүйенің күштерінің өзара әрекеттесуін және шоғырландыруды, оларды қажетті материалды-техникалық базамен қамтамасыз ету алдыңғы қатарлы бағыттардың бірі болып табылады.

[1] КурушинВ. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. — М, 1998, — С. 48.

[2] Лашин С. И. Преступность в области информационных технологий // Технологии и средства связи. — 1997. — № 1. — С. 107.

[3] Батурин Ю. М. Право и политика в компьютерном круге. — М, 1987.

[4] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества.

[5] Батурин Ю. М. Указ. раб.

[6] Лашин С. И. Указ. раб.

[7] Резолюция AGN/64ftRES/19 по вопросу: Компьютерно-ориентированная преступность // Принята Генеральной ассамблеей Интерпола (4-10 октября 1995 г.) // www.un.org.ru

[8] Айков Д, Сейгер К., ФонсторхУ. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Пер. с англ. — М., 2006.