**КИБЕРҚЫЛМЫС ЖӘНЕ КИБЕРПОЛ**

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

Халықарылық мәртебелі ұйымның алаңдауы тектен-тек емес еді. Өйткені, интернет-ресурстардың шексіз де шетсіз мүмкіндіктері ең алдымен техникалық саладағы сан-алуан қылмысқа жаппай жол ашты. Қылмыс әлемінде бет перде кимей, қолына қару ұстамай, кісі өліміне бармай-ақ банктерді тонап, мекемелер қорындағы қаражаттарды қас пен көздің арасында қолды ететін қылмыскерлер пайда болды. Қазақстан аумағындағы осы тектес алғашқы жасалынған кибер­қыл­мысты Лисаков қаласындағы «Гол+Пас» букмекерлік кеңсесі (2003 ж.) басынан өткерді. Компьютерлік желі арқылы 3 миллион 500 мың теңгені оп-оңай жымқырған К. деген азамат сот сараптамасынан соң жасаған қылмысы үшін 5 жылға сотталды. Ел аумағында осыған ұқсас өзге де қылмыстардың біртіндеп қылаң беруі республиканың Ішкі істер министрлігінің құрылымында арнаулы бағытта жұмыс істейтін кәсібилендірілген «К» атаулы басқарманың оңаша отау құруына ықпал етті. Бұған дейін Қазақстан Республикасының 1997 жылғы 16 шілдеде күшіне енген Қылмыстық кодексінде компьютерлік қылмыстың қылмыстық жауапкершілігі туралы алғаш қаралғандығын еске сала кетейік.Таяу күнде Қазақстан Парламенті Мәжілісі мен Сенатының депутаттары Қылмыстық кодекстің жаңа нұсқасын бекітті. Онда Ақпараттық технологиялардың қауіпсіздігіне қарсы қылмыстар енгізілген жаңа тарау бар.

Компьютерлік қылмыстың ең басты кәсіби ерекшелігі мен бар қиындығы – оның халықаралық байланыс желісі арқылы қашықтық талғамай, мемле­кет­аралық шекараларды «аттап» кете­тін­дігінде болып тұр. Оның үстіне компью­терлік қылмыскерлер іс-әрекетке барарда, аты-жөні мен жұмыс орнын, компания атауларын жүз құбылтып, мың түр­лен­діретін арнайы бағдарламалық жасақ­тамаларды қолданады.

Әуелде компьютерлік қылмыс десе – кәрі де, жас та «ол – хакердің ісі»деп жауап береді.Өйткені, бұл бүгінде баршаға таныс атау. Бүгінгі барлық киберқылмыстық әрекеттерді жасайтындар осылар. Хакерлер (Hacker) – 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. Дүниежүзіндегі ең бірінші компьютерлік қылмыскер – америкалық Кевин Митник 1994 жылы ФТБ тізімінде әлемдегі іздеуде жүрген он қылмыскердің «ең азулысы» атанды. Компьютерлік қылмыскер немесе «хакинг» ұғымы қоғамға дәл сол кезден бас­тап орныққан тәрізді.

Қазақстан Республикасының Ішкі істер министрлігі республикада жаса­лынған өте күрделі, ең ауыр компью­терлік қылмысты 2013 жылдың желтоқсанында ашты. Министрліктің «К» басқармасының жедел қызметкерлері заңды тұлғалардың шотына банкіге қашықтықтан қызмет жасайтын желімен «Троялық ат» деген арнайы бағдарлама арқылы ақша ұрлаған қылмысты топтың жолын кесті. «Банк-клиент» жүйесі арқылы әртүрлі банктердегі ұйым-мекемелердің шотына компьютерлік «вирус» жіберіп, ақша ұрлай бастаған қылмыскерлердің әрекеті олар ұсталған мерзімнен әлдеқайда бұрын тіркеуге алынып, қадағалана басталған. Арада көп уақыт өтпей белгілі бір ұлттық компанияның шотынан дәл осындай жолмен екінші деңгейдегі банктен 147 миллион теңге қолды болу қаупі төнді.Міне, осы тұста қылмыскерлердің қолына кісен салынды. Сараптау барысында Қазақстандағы 30 аса ірі компанияның шотынан ұрланған соманың көлемі 400 миллион теңгеден асқаны дәлелденді.

1981 жылы туған қарағандылық А. (осындай әрекеті үшін бұрын сотталған) мен 1976 жылы туған жамбылдық Б. Алматыда отырып 3 жыл бойы «Троялық ат» атты компьютерлік «вирусты» («BackDoor.Shell.218») бухгалтерлердің электрондық пошталарына желі арқылы жіберіп келген. Зиянды бағдарлама салық органдарының атынан жалған атпен бухгалтерге электрондық хатқа мұқият тіркелген. Хатты ашқан кезде Троян аты заңсыз жұмысын жүзеге асыра бас­тайды. Содан соң ғана «Банк-клиент» желісі бойынша электронды қаржылық басқармадан тікелей қолжетімді ақпаратқа ие болған. Қылмыскерлерден қазіргі заманғы барлық сатыдағы компьютерлік шапшаң техника алынды. Алаяқтар осы техника түрлерімен Ұлыбритания мен Германиядағы, Украинадағы серверлерді Алматыдан басқарып отырған. Жедел іздестіру шаралары барысында бұдан да тыс өте көптеген электронды дәлелдеме деректер жинақталып, айқындалды. Дәл осыған ұқсас электронды қаражат ұрлаудың 16 түрі Астана мен Алматыда, Атырау мен Қостанайда, сондай-ақ Шығыс Қазақстанда кездесті, жолы кесілді. Компьютерлік «вирусты» пайдалану арқылы заңсыздыққа бару әрекеті бойынша қосымша 13 қылмыстық іс қозғалды.

Келесі бір оқиғаның болмысы бас­қа­шалау болғанымен, мәні осыған ұқсас. Петропавл қаласында ұсталған қылмыстық топ пластикалық карта үлгісін жасап, шетелдік азаматтардың шотындағы ақшаны үзбей ұрлаған. Интерполдың көмегімен көп кешікпей олардың бірінің германиялық азамат екендігі, Германияда жүріп осыған ұқсас 56 қылмыс жасағаны белгілі болды. Міне, бүгінгі таңда кең өріс алған киберқылмыскерлердің жаңаша сипатта «кардер» деп аталуы да сондықтан. Кардерлер азаматтардың төлем карта­лары­ның нөмірлерімен қоса PIN-коды мен CVV-кодын қолды етеді. Банкомат, интернет, тіпті, магазиндегі төлем операциялары арқылы азаматтардың жеке мәліметтерін «ұрлап»алады. Ол үшін скиммер аталатын өте шағын ғана қалтаға салып жүретін есептегіш құрылғы банкоматтың байқаусыз бетіне жапсырылады. Алаяқ сол арқылы магнитқуаты жететін аумақ­тағы барлық дерек-мәліметтерді жіпке тізгендей етіп, жиып алады. Кез келген банкоматқа жабысып қалатын бай­қаусыз скиммингтік құрылғылардың «өміршеңдігіне» орай, қазіргі кезде банкоматтың жаңа түрлеріне сондай құрылғыларды байқай қоятын қарсы құрылғылар қойылатын болды.

2013 жылы сәуірде Алматыда ІІМ «К» бөлінісі мен «Казкоммерцбанктің» қауіпсіздік қызметі бірлесіп жүргізген шаралар арқасында халықаралық дәрежедегі үлкен қылмыс ашылды. Скиммерлік құрылғымен жеке тұлғалардың төлем карталары арқылы белгілі мөлшерде ақша ұрлап алып жүрген Румыния мен Молдавиядан келген 3 қылмыскер қамауға алынды. Көп кешікпей дәл осындай әрекеттегі Болгария азаматы тұзаққа түсті. Дегенмен, бұларды «алаяқ­тар­дың соңғы тұяғы» деуге тым ерте әрі асығыстық болар еді.

Компьютерлік қылмыс телефондық байланыс жүйесінде де асқынып тұр. Оның бір мысалы – 2005 жылы бізге КCЕLL компаниясы әлдекімдердің “SIM-BOX”қондырғысын пайдалану арқылы GSM-траффигінің орасан мөлшерін ұрлап жатқанын хабарлады. Қазақстанның ұялы телефондары операторларына 5 миллиондай АҚШ долларына шығын келтірген телефон алаяқтары (фрикер) қанатын кеңінен жазып үлгергенше тұтқынға түсті. Олардың бұған дейін Әзербайжан мен Украинада да осындай қылмыс жасағаны айғақталып, біреуі 5, екіншісі 8 жылға сотталды.

Осы жылдың басында Алматы қала­сында ІІМ қызметкерлерінің жедел-іздестіру әрекетінің арқасында бір ЖШС директоры ұсталды. Ол әлгі айтқан «SIM-бокс» құрылғысының көмегімен «TELE-2» ұялы телефон операторынан GSM-траффигін ұдайы ұрлап келген. Оның офисін тексеру барысында әрқайсысы 20 слоттан сим-картқа жегілген 5 «SIM-бокс» қондырғысы табылды.

Қазіргі таңда Халықаралық NCP (Ұлттық байланыс бекеті) желісінің ұлттық бекеті Дүниежүзінің 78 елінде қызмет істейді. Олардың қатарында Германия, Ұлыбритания, АҚШ, Ресей, Украина, Беларусь, Бразилия, Испа­ния, Швеция секілді өзге мемлекеттер бел­сенді орын алады. Рим-Лион тобын­да­ғы «Сегіздік» деп аталатын жұмыс органы тікелей терроризм мен транс­ұлттық ұйымдасқан қылмысқа қарсы тегеурінді қызмет атқарып келеді. 2008 жылғы 9-11 желтоқсан аралығында Жапонияның Киото қаласында өткен Рим-Лион тобының кезекті мәжілісінде Қазақстан NCP Халықаралық желісіне тең құқықты мүше болып қабылданған болатын. Аталған ұйым киберқылмыс саласында болатын яки болуға дайындалып жатқан қылмыс туралы алдын ала ақпарат алмасуға, жедел іздестіру шараларына сәйкес техникалық немесе өзге сипаттағы ақпараттар алуға кең жол ашты. Қазақстан полициясы дәрежелі ұйымға мүше елдердің қатарында құқық қорғау органдарының мүдделес бөлімшелерімен тікелей байланыс орнатқан. Олармен ынтымақтастық қызметін ойдағыдай жалғастырып келеді. Эстония,Украина, Испания мен Германия, Қытай, Жапония Корея мен АҚШ елдерімен жоғарыда аталған халық­аралық желі арқылы болып жатқан әріптес­тік қызмет туралы ерекше атап өту орынды. Балалар порнографиясын насихаттайтын Қазақстандағы сайттың жұмысы мен республикадағы электронды жәшіктердің жаппай бұзылуы туралы бізге аса құнды мәлімет-деректермен қолұшын берген неміс ақпараты сондай ынтымақтастықтың жемісі. Германия­ның Криминалдық полициясы бас бас­қар­масының қызметкерлері сервер үлгі­лері­нің заттай-электрондық айғақ­тары арқылы Қазақстанда орасан зор қаражат ұрлаған хакердің қылмысын мойнына бұлтартпай қойды. Күні кеше ғана ондағы әріптес офицерден сақталынған айғақты ол деректердің барлығы ресми хатталып, Қазақстанға жіберілу алдында Германия прокуратурасына өткізілгені туралы қосымша хабарлама алдық. Бұл екі ел полициясы арасындағы қым-қуыт жұмыстағы кезекті кәсіби байланыстың шынайы бір ғана көрінісі болса керек.

Елбасының тікелей тапсырмасына сәйкес соңғы үш жылдың ішінде Қазақстанның арнайы мамандандырылған жұмыс тобы іссапарға аттанып, АҚШ пен Оңтүстік Кореяның, Қытай мен Эс­тонияның, Ресей мен Жапонияның кибер­қылмысқа қарсы күрес бөлімдерінің озық тәжірибесімен танысты. Солардың ішінде Вашингтон қаласындағы Федерал­ь­­ды тергеу бюросының (ФТБ) компью­терлік қылмысқа қарсы күрес басқар­масында болған тәжірибе алмасу­дың тигізер пайдасы ерекше зор болғанын атап өткеніміз жөн. Квантика қаласындағы (Вирджиния штаты) ФТБ-ның академиясы аумағындағы жылжымалы лабо­ра­торияның, оңтүстік корей­лердің осы сала­дағы ғылыми теңдес­сіз үлгілері, эстон­дықтардың салаға кеш келсе де алға түсіп үлгерген көрнекті тәжірибесі қазақ­тың болашақ «киберполының» дамуына сөзсіз үлкен үлес қосатынына еш дау жоқ.

Бүгінде халықтың көзі компьютерге, құлағы ақпараттық технология атауына әбден үйренді. Дегенмен, ақпараттық технологияның (ІТ) ғарыштық жылдамдықпен дамуы тұсында кибер-қылмыстың да көштен қалмай, қайта өршелене өсе түскенін ерекше байқап та келеміз. Ойлап қараңыздаршы, бір елдің бір елден шекарасы сондайлық шалғайда жатқанына қарамастан екі жақтың банк шоттарына миллиондаған ақша аудару қас пен көздің арасында жүзеге асады. Бәрі де қуатты компьютерлік байланыстың арқасы. Киберқылмыскерлердің ұйқысын бұзатын да осындай ақпараттық техно­логиядағы аса бақуат байланыстар. Сондықтан да Қазақстан полициясының «К» бөлінісінің қызметкерлері борышты міндеттерін адал атқаруға бейімделген әрі дағдыланған. Суық қарусыз жасалынатын мұндай қауіпті қылмыстың жолын кесуге қазақ полициясының білімі мен білігі жетеді. Сала бойынша ең соңғы жаңа технологиялық жабдықтар да баршылық.