Н. Ж. Апахаев, И. Т. Мусабекова,
И. С. Амреева

КИБЕРҚЫЛМЫСТЫЛЫҚ

ОҚУ ҚҰРАЛЫ

Н.Ж. Апахаев, И.Т. Мусабекова, И.С. Амреева.

КИБЕРҚЫЛМЫСТЫЛЫҚ

Оқу құралы

Алматы 2021

ӘОЖ 343(075.8)
КБЖ 67.411я73
А 72

«Қайнар» Академиясының әдістемелік кеңесінің отырысында қаралды және мақұлданды. Хаттама № 5/76, 27 желтоқсан 2021 ж.

Сын пікір берушілер: Алмагамбетов П.А.; Тлеуов Г.Б.

А 72 Апахаев Н.Ж., Мусабекова И.Т., Амреева И.С. Киберқылмыстылық: оқу құралы (дәріс конспектілері). – Алматы, 2022. – 147 б.

ISBN 978-601-80854-1-3

Бұл жұмыс киберқылмыстылықтың теориялық аспектілері жалпы түрде ашылатын оқу құралы болып табылады.

Оқу құралы студенттерге, жоғары оқу орындарының оқытушыларына, құқық қорғау органдарының қызметкерлеріне арналған.

ӘОЖ 343(075.8)
КБЖ 67.411я73

ISBN 978-601-80854-1-3

МАЗМҰНЫ

Кіріспе

Ақпараттық-коммуникациялық технологиялар (АКТ) адамдардың бизнес жүргізу, тауарлар мен қызметтерді сатып алу, ақша жіберу және алу, қарым-қатынас жасау, ақпарат алмасу, бір-бірімен қарым-қатынас жасау, басқалармен қарым-қатынас жасау және дамыту тәсілдерін өзгертті. Бұл өзгерістер, сондай-ақ АКТ-ны үнемі ұлғайып келе жатқан қолдану мен тәуелділік, қылмыскерлер мен басқа шабуылдаушылар АКТ-ға бағытталған және/немесе қылмыс жасау үшін АКТ-ны пайдалана алатын осалдықтарды тудырады. Бұл оқу құралы киберқылмыстылыққа қатысты негізгі ұғымдарға кіріспе береді, киберқылмыстылық деген не екенін түсіндіреді, интернеттің, технологияның және киберқылмыстылықтың даму тенденцияларын, сондай-ақ киберқылмыстарды тергеу мен киберқылмыстылықтың алдын алуға қатысты техникалық, құқықтық, этикалық және операциялық мәселелерді қарастырады. Осы пән бойынша таңдалған оқу әдебиеті негізгі ұғымдарға, негізгі терминдер мен анықтамаларға шолу жасайды, сондай-ақ киберқылмыстылық, онымен байланысты проблемалар мен оның алдын алу шараларына шолу жасайды.

1 Тақырып. Киберқылмыстылыққа кіріспе.

1. Компьютерлік технологиялардың негіздері.

Компьютерлік жүйе жұмыс үстелі немесе ноутбук компьютерлерімен ұсынылуы мүмкін. Бірақ ұялы телефондар, планшеттік компьютерлер және бір-бірімен байланысатын және өзара әрекеттесетін Интернетке қосылған құрылғылар (тұрмыстық техника және смарт сағаттар сияқты) болып табылатын Интернет заттары (IoT) объектілерді, адамдарды, жануарларды және/немесе өсімдіктерді бақылауға, сондай-ақ осы құрылғыларды пайдаланушыларға белгілі бір қызмет көрсету үшін олар туралы ақпарат алмасуға мүмкіндік береді және басқа да көптеген құрылғыларды компьютерлік жүйелер ретінде қарастыруға болады. Компьютерлік жүйенің әртүрлі анықтамалары бар. Мысалы, Еуропа Кеңесінің 2001 жылғы Киберқылмыстылық туралы конвенциясының 1(a) бабында «компьютерлік жүйе» «бір немесе өзара байланысты немесе іргелес құрылғылар тобы, олардың біреуі немесе бірнешеуі бағдарламаға сәйкес әрекет етіп, мәліметтерді автоматтандырылған өңдеуді жүзеге асырады». (Конвенцияға енгізілген «компьютерлік жүйе» түсінігіне қатысты нұсқаулармен танысу үшін 2012 жылғы Киберқылмыстылық туралы конвенцияға қатысушылар Комитетінің жарияланымын қараңыз (Cybercrime Convention Committee, 2012). Сонымен бірге, 2014 жылғы Африка одағының киберқауіпсіздік және жеке деректерді қорғау туралы конвенциясының 1-бабында компьютерлік жүйе «логикалық, арифметикалық функцияларды немесе сақтау функцияларын, соның ішінде деректерді сақтау құралдарын немесе осындай құрылғылармен тікелей байланысты немесе осындай құрылғымен (құрылғылармен) бірге жұмыс істейтін электрондық, магниттік, оптикалық, электрохимиялық немесе басқа да жоғары жылдамдықтағы деректерді өңдеу құрылғысы немесе өзара байланысты немесе біріктірілген құрылғылар тобы» ретінде анықтайды. Компьютерлік жүйелер деректерді өңдеуге бейім. 2010 жылғы Ақпараттық технология қылмыстарына қарсы Араб мемлекеттері лигасының конвенциясының 2(3) бабында деректерді «сандар, әріптер, белгілер және т.б. сияқты ақпараттық технологиялар арқылы сақтауға, өңдеуге, жасауға және беруге болатын кез келген нәрсе» деп анықтайды.

Басқа терминдер деректерге сілтеме жасау үшін пайдаланылады: Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясының 1(b) тармағында «компьютерлік деректер» («компьютер жүйесінде өңдеуге жарамды формадағы фактілердің, ақпараттың немесе тұжырымдамалардың кез келген көрінісі, функцияны орындау үшін компьютерлік жүйе үшін қолайлы бағдарламаны қоса алғанда»;

2014 жылғы Африка одағының киберқауіпсіздік және жеке деректерді қорғау туралы конвенциясында «компьютерленген деректер» термині пайдаланылады, ол Еуропа Кеңесінің 2001 жылғы Киберқылмыстылық туралы конвенциясында («компьютерлік жүйеде өңдеуге жарамды пішін кез келген фактілерді, ақпаратты немесе тұжырымдамаларды ұсыну» терминімен бірдей деректер анықтамасына ие»);

және 2001 жылғы Тәуелсіз Мемлекеттер Достастығына қатысушы

мемлекеттердің компьютерлік ақпарат саласындағы қылмысқа қарсы күрестегі ынтымақтастығы туралы Келісімнің 1(b) бабында «компьютерлік ақпарат» термині қолданылады («компьютер жадында сақталған ақпарат, ЭЕМ-да немесе басқа тасымалдаушыларда компьютердің қабылдауына қол жетімді нысанда немесе байланыс арналары арқылы жіберілетін ақпарат»).

Бізге таныс компьютерлік жүйелердің көпшілігі деректерді сақтайды. Мысалы, смартфон кірістірілген камераның көмегімен суретке түсіре алады (деректерді өңдеу), сонымен қатар ол фотосуретті кейінірек қол жеткізу үшін сақтай алады (деректерді сақтау). Деректер әдетте қатты диск деп аталатын ішкі тұрақты жадта сақталады. Компьютерлік жүйеге қатысты қызметтерді ұсынатын тұлғалар қызмет жеткізушілер деп аталады. 2010 жылғы Араб мемлекеттері лигасының 5 ақпараттық технология қылмыстарға қарсы конвенциясының 2(2) бабында қызмет жеткізушісі «абоненттерге ақпараттық технологияларды пайдалана отырып байланысу үшін қажетті қызметтерді ұсынатын, немесе байланыс қызметінің немесе оның пайдаланушыларының атынан ақпаратты өңдейтін немесе сақтайтын кез келген жеке немесе заңды тұлға.

Үйдегі компьютерлер мен ұялы телефондарға арналған интернет қызметтерін Интернет-қызмет жеткізушісі ұсынады. Интернет-қызмет жеткізушісі компьютерлерге немесе телефондарға жібере алатын және компьютерлерден немесе телефондардан жіберілген деректерді қабылдай алатын компьютерлік жүйелерді пайдаланады. Екі немесе одан да көп компьютерлер бір-біріне мәліметтер жіберу арқылы алмаса алатын болса, компьютерлік желі құрылады. Электрондық поштаңызды елестетіп көріңіз. Электрондық поштаны пайдаланған кезде сіз браузерді ашып, веб-сайтқа қосылуыңыз мүмкін. Жүйеге кіргеннен кейін электрондық хаттарды жіберуге және алуға болады. Мүмкін, бұл веб-сайт сізге емес, басқа ұйымға тиесілі. Бұл ұйым электрондық пошта қызметтерін ұсынады және оны қызмет жеткізушісі деп санауға болады. Интернетке кіру қызметтері мен электрондық поштаға кіру қызметтері екі түрлі қызмет екенін ескеріңіз. Бұл бізді компьютерлік қылмыстар туралы Еуропа Кеңесінің 2001 жылғы Конвенциясының 1(d) бабында «байланыс тізбегінің ажырамас бөлігі болып табылатын компьютерлік жүйемен желі қызметінің көзін, тағайындалған орнын, бағытын, уақытын, күнін, өлшемін, ұзақтығын немесе түрін көрсететін компьютерлік жүйе арқылы ақпаратты беруге қатысты кез келген компьютерлік деректер» ретінде анықталған трафик деректеріне әкеледі. Бұрын біз компьютерлік жүйеде сақталатын немесе өңделетін деректер ретінде компьютерлік деректер туралы айттық. Трафик деректері – компьютерлік желі арқылы таралатын деректер. Енді тағы да электрондық поштаңызды елестетіп көріңіз. Сіз электрондық хатыңызды жазасыз, содан кейін сол хабарламаны алушыға «жібересіз». Электрондық хаттағы деректер адресатқа жеткенше желі арқылы жіберіледі. Трафик деректері электрондық поштаның тағайындалған жерге жетуі үшін қажетті кез келген деректер болып табылады. Телефон жақсы үлгі. Сіз досыңызға қоңырау шалғыңыз келетінін елестетіп көріңіз. Сізге де, досыңызға да телефон керек, ал екеуіңізге де телефон нөмірлері қажет. Егер

телефон шотыңызды төлесеңіз, қызмет жеткізушісі сізге телефон нөмірін және желіге кіру мүмкіндігін береді. Содан кейін қоңырау шалу үшін досыңыздың телефон нөмірін білуіңіз керек. Сіз және сіздің досыңыз қызметті алып, бір-біріңіздің нөмірлерін білгеннен кейін сөйлесе аласыз. Дәл осылай, негізінен, компьютерлік желілер туралы да айтуға болады. Веб-сайтқа кіргіңіз келгенде, домен атауын (мысалы, yahoo.com) интернет-шолғышқа (немесе веб-шолғышқа) енгізесіз (мысалы, Google, Bing). Бұл домендік атау, «компьютерлерге (немесе басқа Интернетке қосылған сандық құрылғылар) тағайындаған бірегей идентификаторлармен қосылған кезде» Интернет қызметін жеткізушісімен бір немесе бірнеше Интернет протоколының (немесе IP мекенжайларымен) байланыстырылуы (яғни, қатар қойылуы) мүмкін. (Maras, 2014, p. 385). Домендік атаулар жүйесі (DNS) домен атауларын IP мекенжайына түрлендіру арқылы Интернетке қол жеткізуді қамтамасыз етеді.

2. Технологияларды пайдалану және Интернетке қосылу саласындағы жаһандық үрдістер.

Жер бетінде Интернетке қол жеткізе алмайтын жерлер өте аз. Көптеген елдерде ірі қалалар үшін желілік инфрақұрылымды (аппараттық камту, жабдық, кабельдер және сымсыз кіру сияқты) ұсынатын кем дегенде бір Интернет-қызмет жеткізушісі бар. Тіпті жергілікті Интернет-қызмет жеткізушілері жоқ аудандардың өзінде шалғай аудандарға жаһандық спутниктік желілер Интернетке қол жеткізуді қамтамасыз ете алады. Дамушы елдерде кең жолақты технология баяу қарқынмен енгізілуде, соның нәтижесінде бұл елдердің тұрғындары Интернетке кіру үшін мобильді технологияларды пайдаланады. 7 мобильді құрылғы арқылы Интернет қызметтерінің қолжетімділігіне байланысты Интернетті пайдалану тұрақты түрде өсуде. Смартфондар арзандады және көбірек мүмкіндіктерді қамтиды, ал мобильді қызмет провайдерлері арзанырақ ұялы байланыс желілері арқылы сенімдірек Интернетке қол жеткізуді қамтамасыз етеді. Бұл көптеген елдерде Интернеттің енуінің артуына ықпал етеді. 2016 жыл бүкіл әлем бойынша Интернетті пайдаланушылардың көпшілігі Интернетке кіру үшін мобильді құрылғыларды пайдалана бастаған бірінші жыл болды (Statcounter, 2016). Интернетке ену «интернетті пайдаланатын белгілі бір елдің немесе аймақ халқының жалпы санының пайызын» білдіреді (IGI Global, n.d.). 2017 жылдың қыркүйегіндегі жағдай бойынша ғаламдық Интернетке ену деңгейі 51% құрайды. Осылайша, әлем халқының шамамен жартысы Интернетке қол жеткізуге және Интернетті пайдалану мүмкіндігіне ие (Аймақтар бойынша Интернетке ену деңгейын 1-суретте қараңыз).

Интернетке қосылу сенімділігі артып, Интернетке қосылатын адамдар саны артқан сайын, желіде қолжетімді маңызды қызметтердің саны да артып келеді. Мысалы, Оңтүстік Кореяда интернет байланысы өте жылдам және өте сенімді. Экономикалық ынтымақтастық және даму ұйымы (ЭЫДҰ) 2018 жылы Оңтүстік Кореядағы тұрмыстық интернеттің енуі 99,5% құрады деп есептейді. Интернетке көптеген адамдар қосылғандықтан, Корея үкіметі мен бизнесі көбірек онлайн қызметтерді ұсынып жатыр. Мысалы, жылдамдықты арттырғаныңыз үшін айыппұл төлеуге түбіртек алсаңыз (интернетке қосылған

жылдамдықты арттыру камерасынан автоматты түрде), айыппұлыңыз туралы ақпаратты көру үшін үкімет веб-сайтына кіре аласыз. Содан кейін банктің электронды төлем жүйесі арқылы айыппұлды бірден төлеуге болады. Бұл есеп айырысу процесі толығымен қағазсыз болуы мүмкін. Кейбір жағдайларда офлайн көрсетілетін мемлекеттік қызметтердің саны онлайн қызметтердің санынан аз болады. Қазіргі уақытта ұқсас жағдай Қытайда да дамыды, тек одан да кең ауқымда.

2018 жылдың қаңтарында жарияланған Қытайдағы интернеттің дамуы туралы 41-ші статистикалық есеп бойынша, «2017 жылдың желтоқсан айының аяғында Қытайдағы интернет пайдаланушылар саны 772 миллионға жетіп, 2016 жылдың соңындағы көрсеткіштен 40,74 миллионға артты... Интернетке ену деңгейі 55,8%-ға жетті, бұл 2016 жылдың соңындағы көрсеткіштен 2,6 пайыздық тармаққа көп ... Қытайда мобильді интернетті пайдаланушылар саны 753 миллионға жетіп, 2016 жылдың соңынан бері 57,34 миллионға өсті». Жылдам хабар алмасу, онлайн төлемдер, онлайн-сатып алу, тағамды онлайн жеткізу немесе саяхатқа онлайн тапсырыс беру сияқты онлайн қызметтерге жүздеген миллион пайдаланушылар қол жеткізе алады. WeChat (лезде хабар алмасу құралы) және Alipay (үшінші тұлғалардың пайдасына төлем жүйесі) сияқты қолданбалар дерлік әрбір смартфон үшін маңызды қолданбаларға айналды. Мобильді құрылғылар, мобильді интернет және осы қосымшалардың танымал болғаны сонша, мемлекеттік қызметтер, төлемдер, инвестициялар, қоғамдық және жеке көліктер және басқа да көптеген қызметтер олармен толықтай біріктірілген (Kessel and Mozur, n.d.). Интернетте жиі ұсынылатын маңызды қызметтермен, кейде офлайн қызметтерінің төмендеуімен қатар, технологияны теріс пайдалану және қылмыс жасау мүмкіндіктері де артып келеді.

3. Киберқылмыстылықтың түсінігі. Киберқылмыстылықтың жалпы қабылданған анықтамасы жоқ. Дегенмен, келесі анықтама Киберқылмыстылықтың барлық қолданыстағы анықтамаларына ортақ элементтерді қамтиды. Киберқылмыс – ақпараттық-коммуникациялық технологияларды (АКТ) пайдаланатын және желілерге, жүйелерге, деректерге, веб-сайттарға және/немесе технологияға бағытталған немесе қылмыс жасауға ықпал ететін заң бұзу әрекеті (ITU, 2012; Maras, 2014; Maras, 2016). Киберқылмыстың дәстүрлі қылмыстан айырмашылығы, ол «физикалық немесе географиялық шекараларды мойындамайды» және кәдімгі қылмысқа (бірақ бұл киберқылмыстың түріне және дәстүрлі қылмыстың түрімен салыстыруға байланысты болады) қарағанда аз күш-жігермен, жеңілірек және тезірек жасалуы мүмкін (Maras, 2014). Europol (2018) киберқылмыстарды кибертәуелді қылмыстарға жіктейді (яғни, «тек компьютерлерді, компьютерлік желілерді немесе ақпараттық-коммуникациялық технологиялардың басқа түрлерін пайдалану арқылы жасалуы мүмкін кез келген қылмыс» (McGuire and Dowling, 2013, p. 4; Europol, 2018, p. 15) және кибертехнологиялар арқылы жасалатын қылмыстар (яғни Интернет және цифрлық технологиялар көмегімен жасалатын дәстүрлі қылмыстар). Киберқылмыстың осы санаттарының арасындағы негізгі айырмашылық құқық

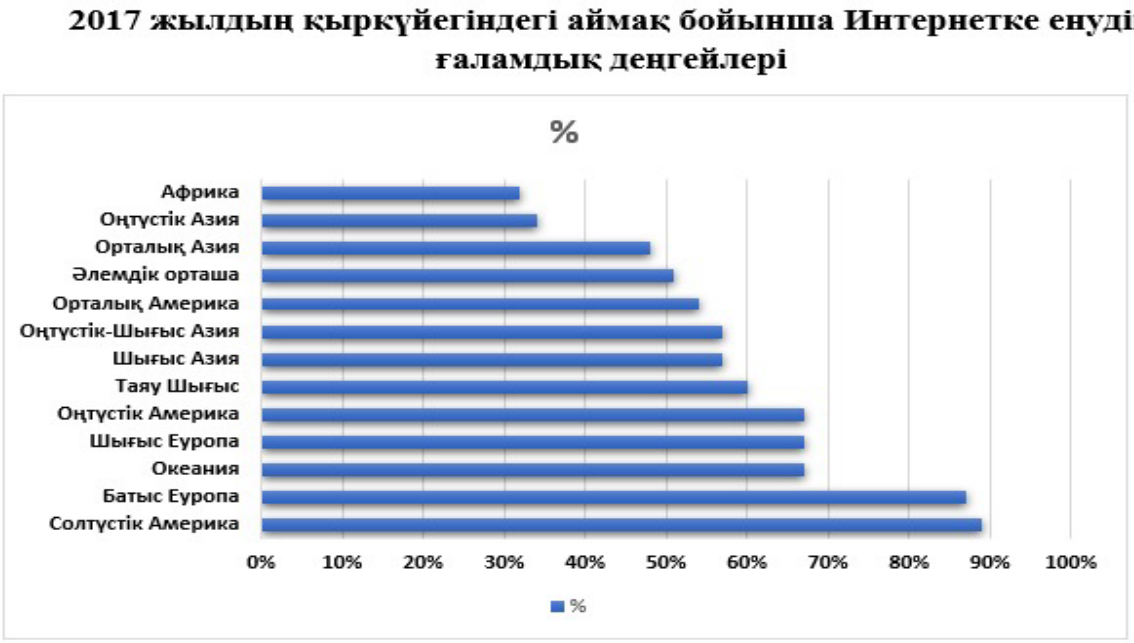
бұзушылық жасаудағы ақпараттық-коммуникациялық технологиялардың рөлі болып табылады - бұл АКТ қылмыстың мақсаты немесе қылмыскердің қылмыстың жасау жолының құрамдас бөлігі (modus operandi, яғни әрекет әдісі) (БҰҰ ЕҚБ, 2013, 16 б.). АКТ қылмыстың нысанасы болған кезде мұндай киберқылмыс компьютерлік деректердің немесе жүйелердің құпиялылығына, тұтастығына және/немесе қолжетімділігіне теріс әсер етеді (БҰҰ ЕҚБ, 2013). Құпиялылық, тұтастық және қолжетімділік «ҚТҚ Үштігі» (Rouse, 2014) деген атауын құрайды: қарапайым сөзбен айтқанда, құпия ақпарат құпия болып қалуы керек, оны иесінің рұқсатынсыз өзгертуге болмайды және деректер, қызметтер мен жүйелер әрқашан иесіне қолжетімді болуы керек. АКТ қылмыс жасау тәсілінің құрылымды бөлігі болған кезде, киберқылмысқа Интернет пен цифрлық технологиялар қандай да бір жолмен жәрдемдесетін дәстүрлі қылмыстар (алаяқтық және ұрлық сияқты) кіреді. Киберқылмысты жеке адамдар, жеке адамдар тобы, коммерциялық ұйымдар және мемлекеттер жасауы мүмкін. Бұл субъектілер ұқсас тактикалық әдістерді (мысалы, зиянды бағдарламаны пайдалану) және ұқсас мақсаттарға (мысалы, компьютерлік жүйе) шабуыл жасауы мүмкін болғанымен, киберқылмыс жасағанда олардың әртүрлі мотивтері мен ниеттері болады. Киберқылмыстылық бойынша әртүрлі зерттеулер жүргізілді (мысалы, «Deviant Behavior» және «International Journal of Cyber Criminology» журналдарында жарияланған зерттеулерді қараңыз). Бұл зерттеулер психология, әлеуметтану және криминология, сондай-ақ басқа ғылыми пәндер призмасы арқылы Киберқылмыстылықты зерттеді (сондай-ақ көпсалалы тұрғысынан Киберқылмыстылықты зерттеуге шолу үшін қараңыз: Maras, 2016). Кейбір басылымдар қылмыскерлердің әрекетін ұтымды және еркін таңдаудың нәтижесі ретінде түсіндіреді, ал басқа басылымдарда қылмыс ішкі және/немесе сыртқы күштердің нәтижесі ретінде қарастырылады (мысалы, Mclaughlin and Muncie, 2013 кітабына қосылған криминология бойынша басты және классикалық еңбектерді қараңыз). Басқа зерттеулер Киберқылмыстылықтағы «кеңістіктің» рөлін, атап айтқанда, қылмыстық құндылықтарды мәдени тасымалдаудағы онлайн кеңістіктер мен желілік қауымдастықтардың рөлін зерттеді (Maras, 2016, 6 Chapter қараңыз). Бұл Киберқылмыстылықтық зерттеулердің мақсаты Киберқылмыстылықтың салдарына, киберқылмыстылықтың сипаты мен масштабына жарық түсіруінде, «киберқылмыстылыққа қарсы реакцияларды және осы реакциялардың салдарын бағалануында және киберқылмыстармен күресу, салдарын жұмсарту және алдын алу үшін қолданылатын әдістердің тиімділігін бағалануында» (Maras, 2016, p. 13).

4. Киберқылмыстылық саласындағы тенденциялар. Аймақтық және халықаралық құқық қорғау органдары (мысалы, Еуропол және Интерпол) және аймақтық ұйымдар (мысалы, Африка одағы және Америка мемлекеттерінің ұйымы) киберқылмыстылық пен киберқауіпсіздік тенденциялары туралы ақпаратты жариялайды. Киберқылмыстық тенденцияларын жыл сайынғы есептерден және/немесе қылмысты бағалау мен виктимизацияны әртүрлі ресми өлшем құралдарынан алынған деректерден де анықтауға болады: мысалы, Оқиғаларды тіркеу Ұлттық жүйесі

(АҚШ); Жалпы әлеуметтік зерттеу (Канада); Англия мен Уэльстегі қылмысқа шолу (Англия және Уэльс). Бұл қылмысты өлшеу және виктимизацияны зерттеу құралдары жиналған және талданатын киберқылмыстық деректерінің түрлері және деректерді жинау және талдау үшін қолданылатын әдістер тұрғысынан ерекшеленеді. Қауіпсіздікті, іскерлік тәуекелдерді және/немесе бүкіл әлемге қатысы бар қауіптерді зерттейтін киберқауіпсіздік саласындағы компаниялар және басқа жеке ұйымдар орын алған киберқауіпсіздік оқиғалар, олардың түрлері, жиілігі мен салдары негізінде киберқылмыстылық және/немесе киберқауіпсіздік саласындағы тенденциялар туралы есептерін жариялайды. Мысалы, 2018 жылы компаниясы бопсалау вирусын киберқылмыс үрдісі ретінде анықтады. Киберқылмыстың бұл түрі жасалған кезде компьютерлік жүйелер зиянды кодпен (зиянды бағдарламамен) жұқтырылады және олардағы деректер киберқылмыскерге ақша төленгенге дейін иелері және/немесе заңды пайдаланушылар үшін қолжетімсіз болады. Дегенмен вирустық шабуылдар жаңа болмаса да, олардың саны, сонымен қатар, жиілігі, қарқындылығы және қамтуы өсті. Бастапқыда мұндай киберқылмысты жасайтын зиянкестер жеке тұлғаларды нысанаға алып, олардан аз мөлшерде ақша талап етті, бірақ кейін олар коммерциялық кәсіпорындарды, компаниялар мен ұйымдарды, ең соңында маңызды қызметтерді ұсынатын жеке және мемлекеттік сектордағы басқа субъектілерді нысанаға ала бастады (мысалы, ауруханалар). Мысал ретінде 2017 жылы Wanna Cry бопсалау вируспен шабуылын келтіруге болады, ол шамамен 150 елге әсер етті (Reuters, 2017), оның ішінде тек Англиядағы 80-нен астам «NHS ұйымдардың (Ұлттық денсаулық сақтау қызметі) 20 000-ға жуық қабылдауға жазулары жойылуға әкелді, 600 жалпы тәжірибелік дәрігерлер клиникалары қағаз жұмыс процесіне қайта оралуға мәжбүр болды, ал бес аурухана жедел жәрдемді басқа ауруханаларға қайта бағыттады, өйткені олар бұдан былай шұғыл көмек көрсете алмады» (Hern, 2017). 2017 жылы бопсалау вирусы Еурополдың да «Интернетте ұйымдасқан қылмыстылықтың төндіретін қауіпін бағалауында» киберқылмыстық үрдісі ретінде анықталды.

Жаңа технологиялардың (мысалы, заттар Интернеты, дрондар, роботтар, өздігінен жүретін көліктер) пайда болуымен киберқылмыстылықтың жаңа тенденциялары да пайда болады. Сонымен қатар, Еурополдың 2017 жылғы «Интернетте ұйымдасқан қылмыстылықтың төндіретін қауіпін бағалау» баяндамасында атап көрсетілгендей, құқық қорғау және қауіпсіздікті қамтамасыз ететін шаралары киберқылмыстылық пен киберқылмыскерлердің тактикасына, құралдары мен мақсаттарына әсер етеді. Демек, бұл шаралар киберқылмыстылық саласындағы болашақ тенденцияларына да әсер етеді.

1-сурет: Аймақтар бойынша Интернетке ену деңгейы.



Қайнар көзі: Statista (2018). 2017 жылдың қыркүйегіндегі жағдай бойынша әлемдегі Интернетке ену деңгейі, аймақтар бойынша бөлінген Statista.

5. Техникалық мәселелер. Киберқылмыстылықпен күресуді қиындататын бірнеше техникалық себептер бар. Бірінші себеп - атрибуция. Интернетке қосылған кез келген компьютер Интернетке қосылған кез келген басқа компьютермен байланыса алады. Біз әдетте компьютердің жалпы IP-мекенжайын сол компьютер компьютерімізге қосылған кезде көреміз. IP мекенжайы әдетте бұл компьютер қай елден және қай Интернет-қызмет жеткізушіге қосылғанын анықтауға мүмкіндік беретін жаһандық бірегей нөмір болып табылады. Мәселе мынада, шабуылдаушы өзінің IP-мекенжайын жасырудың немесе тіпті басқа IP-мекенжайынан қосылып жатыр деп ұқсатудың көптеген жолдары бар. Оның үстіне, қылмыскерлер құқық қорғау органдарының анықтауынан жалтару, Даркнетте сайттарына кіруді және оларды жасыруды қиындату үшін әртүрлі құралдарды пайдалана алады. Екінші техникалық мәселе бағдарламалық қамтамасыз етумен байланысты. Компьютерлік бағдарламалар бағдарламалық қамтамасыз ету болып табылады. Телефондағы немесе планшеттегі қолданбалар бағдарламалық қамтамасыз ету болып табылады. Веб-сайт сияқты Интернетте қосылатын қызметтер де бағдарламалық қамтамасыз ету болып табылады. Көбінесе бағдарламалық қамтамасыз етуде осалдықтар болады. Осалдық бағдарламадағы ақауға немесе шабуылдаушыларға олар жасай алмайтын нәрселерді жасауға мүмкіндік беретін қате конфигурацияға байланысты болуы мүмкін (мысалы, тұтынушы несие картасының ақпаратын жүктеп алу). Бағдарламалық жасақтама компаниялары үшін осалдықтарды табу қиын болуы мүмкін, әсіресе жиі өзгеретін ірі бағдарламалық жасақтама жобаларымен байланысты. Кейде шабуылдаушылар бағдарламалық қамтамасыз ету компаниясының алдында осалдықты табады (яғни, «нөлдік

күндік осалдық»). Билдж пен Думитрас айтуынша (Bilge and Dumitras, 2012), «Осалдық белгісіз болып қалғанша, осал бағдарламалық құралды түзету мүмкін емес, ал антивирустық бағдарламалық сигнатур негізделде сканерлеу көмегімен шабуылды анықтай алмайды». Компания мұндай осалдықты киберқылмыскерлер бағдарламалық жасақтама мен бағдарламалық жасақтаманы пайдаланушылардың құпиялылығына, тұтастығына немесе қолжетімділігіне шабуыл жасау үшін пайдаланған кезде біледі. 2017 жылы АҚШ несиелік бюросы Equifax бағдарламалық жасақтаманың осалдығына байланысты 143 миллион американдықтың «құпия жеке деректерін» жоғалтты. Бұл осалдық түзетілгенге дейін үш ай бойы пайдаланылды. Деректерді жоғалту осалдықтары тіпті ірі ұйымдар үшін де салыстырмалы түрде жиі кездеседі, себебі цифрлық жүйелерді тиісті түрде құру, күйге келтіру және қорғау қиын. Тағы бір техникалық проблема виртуалдандырылған АТ-инфрақұрылымы (мысалы, бұлт). Ұйымның инфрақұрылымы бұлтқа ауысқанда, бұл:

a) компания киберқауіпсіздік жауапкершілігінің бір бөлігін бұлттық қызмет жеткізушіге ауыстыруын (мысалы, физикалық жүйе қауіпсіздігі, деректерді өңдеу орталығының қауіпсіздігі);

b) қауіпсіздік бұзылған кезде, компания техникалық және құқықтық мәселелерге әкелуі мүмкін оқиғаларды тергеу үшін бұлттық қызмет жеткізушімен жұмыс істеу керектігін білдіреді.

6. Құқықтық мәселелер. Киберқылмыстылық – қылмыскерлері мен құрбандары Интернет байланысы бар әлемнің кез келген жерінде болуы мүмкін трансұлттық қылмыс түрі. Осылайша, киберқылмыстарды тергеушілер көбінесе трансшекаралық қол жеткізуді және деректер алмасуды талап етеді. Сұралған деректерді қызмет жеткізушілері сақтаса және құқық қорғау органдарына деректерге қол жеткізуге мүмкіндік беретін шаралар қолданылса, бұл мақсатты орындауға болады. Киберқылмыстарды тергеудегі және киберқылмыскерлерді қудалаудағы негізгі құқықтық қиындықтар мыналар болып табылады: әртүрлі елдердегі әртүрлі құқықтық жүйелер; киберқылмыстылық туралы ұлттық заңдардағы айырмашылықтар; дәлелдемелер мен қылмыстық сот ісін жүргізу ережелеріндегі айырмашылықтар (мысалы, құқық қорғау органдарының цифрлық дәлелдемелерге қолжетімділігін алу рәсімдерінде; мысалы, тінту туралы құқықтық тәртіппен немесе онсыз); аймақтық және көпжақты киберқылмыстылық туралы келісімдердің ауқымы мен географиялық қолдану мүмкіндігіндегі айырмашылықтар; және деректерді қорғау және адам құқықтарын сақтау тәсілдерінің айырмашылығы.

Этикалық мәселелер. Құқық қорғау органдары қылмыстарды (және киберқылмыстарды) тергеу кезінде, дәлелдемелерді өңдеу, талдау және түсіндіру кезінде құқықтық және этикалық стандарттарды сақтауы керек. Этикалық мәселелер тек құқық қорғау қызметін жүргізуде ғана емес, сонымен қатар жеке тұлғалардың, жеке адамдар тобының, компаниялардың, ұйымдардың және үкіметтердің ақпараттық-коммуникациялық технологияларды (АКТ) пайдалануында да туындауы мүмкін. Мысалы, АКТ

пайдаланудағы этикалық мінез-құлық басқа адамдарға, жүйелер мен деректерге зиян келтіруден аулақ болу, заң үстемдігі мен адам құқықтарын сақтауды қамтиды. Cambridge Analytica компанияның әшкереленуі барлығын әлеуметтік желі платформаларында деректерді жинауға және пайдалануға қатысты этикалық мәселелерге назар аударуға сендірді. Атап айтқанда, БАҚ мәліметтерді өңдеуші Cambridge Analytica компаниясы Facebook пайдаланушыларының жеке деректерін сатып алу үшін үшінші тарап зерттеушісі Александр Коган арқылы төлегенін анықтады, ол пайдаланушыларды хабардар ететін жеке басын куәландыратын тексеру парағы түріндегі деректерді жинау қосымшасын жасады (кіші шрифтпен) ақпарат тек ғылыми мақсатта жиналады және бұл мәлімдеме Facebook тарапынан расталмаған және жалған болып шықты. Сауалнамаға бар болғаны 305 000 адам қатысып, жеке деректерін жинауға келісім бергеніне қарамастан, олардың достарының деректері де олардың аккаунттарынан алынып, құрбандардың болжамды санын 87 миллион адамға жеткізді. Cambridge Analytica оқиғасы жеке тұлғалар туралы жиналған және (кейбір) ақпаратты беруге, олардың деректерін жинауға және пайдалануға кез келген келіскен пайдаланушылар үшін күтпеген түрде, ал ұсынбағандар үшін рұқсат етілмеген түрде пайдаланылған деректердің үлкен көлеміне жауапты тұлғалардың әдепсіз мінез-құлқын ашты. Cambridge Analytica және басқалардың қатысы бар нәрселер заңсыз деп саналмаса да, олардың әрекеттері этикалық емес еді.

Талқылауға арналған сұрақтар:

1. Киберқылмыстылық дегеніміз не?
2. Киберқылмыстылық неге ғылыми тұрғыдан зерттеледі?
3. Киберқылмыстылық тенденциялары туралы ақпаратты қайдан алуға болады? Осы қайнар көздерді бағалаңыз.
4. Киберқылмысты тергеу және киберқылмыстылықтың алдын алумен байланысты қандай құқықтық проблемалар бар?
5. Киберқылмыстарды тергеу және киберқылмыстылықтың алдын алумен байланысты қандай этикалық мәселелер бар?
6. Киберқылмыстарды тергеу және киберқылмыстылықтың алдын алумен байланысты қандай техникалық проблемалар бар?
7. Киберқылмыстарды тергеу және киберқылмыстылықтың алдын алумен байланысты қандай оперативтік проблемалар бар?

2 Тақырып. Киберқылмыстылықтың негізгі түрлері.

1. Компьютерлік деректердің немесе жүйелердің құпиялылығына, тұтастығына және қолжетімділігіне қарсы қылмыстар.

«Жаңа» киберқылмыстар (яғни кибертәуелді қылмыстар) ең алдымен жүйелерге, желілерге және деректерге бағытталған және олардың құпиялылығын бұзу мақсатында жасалған қылмыстар (яғни, жүйелер, желілер және деректер қорғалған және оларға тек рұқсаты бар пайдаланушылар ғана қол жеткізе алатын кезде), тұтастық (яғни деректер дәл және сенімді және

өзгертілмеген кезде) және қол жетімділік (яғни деректер, қызметтер және жүйелер сұраныс бойынша қол жетімді болғанда). Бұл киберқылмыстарға хакерлік шабуылдар жатады; зиянды бағдарламаларды жасау, сақтау және тарату; «қызмет көрсетуден бас тарту» шабуылдары (DoS); таратылған қызмет көрсетуден бас тарту шабуылдары (DDoS) және веб-сайттардың зақымдануы (яғни, веб-сайт мазмұнына бағытталған онлайн вандализм түрі).

Хакерлер шабуылы – жүйелерге, желілерге және деректерге рұқсатсыз кіруді (бұдан әрі – нысана) сипаттау үшін қолданылатын термин. Хакерлік шабуылдар тек мақсатқа қол жеткізу немесе кіру рұқсатының мерзімі өткеннен кейін осындай рұқсат алу және/немесе қолдау үшін жасалуы мүмкін. Қауіпсіздік шараларын айналып өтетін веб-сайтқа немесе ақпаратқа қасақана рұқсатсыз қол жеткізуді қылмыстық жауапкершілікке тартатын ұлттық және аймақтық заңдардың мысалдары Біріккен Араб Әмірліктерінің заңдары болып табылады: 2006 жылғы «Ақпараттық технологиялар қылмыстарының алдын алу туралы» №2 Федералдық заңның 1-бабы және Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясының 2-бабы (сонымен қатар Будапешт конвенциясы деп аталады; бұдан әрі Киберқылмыстылық туралы конвенция деп аталады).

Хакерлер сонымен қатар нысанаға зақым келтіру немесе басқа зиян келтіру үшін жүйелерге рұқсатсыз кіруге қол жеткізе алады. 2014 жылы британдық хакер Лаури Лав (Lauri Love) веб-сайттарды бұзып, АҚШ үкіметтік жүйелеріне рұқсатсыз қол жеткізіп, сол жүйелерден құпия ақпаратты ұрлады. Бұл киберқылмыс деректердің құпиялылығын (веб-сайтқа және жүйеге рұқсатсыз кіру және ақпаратты ұрлау арқылы) және деректер тұтастығын (веб-сайттарды бүлдіру арқылы) бұзды.

Жүйеге рұқсатсыз қол жеткізуден басқа, хакерлер деректерді желі арқылы қозғалған кезде ұстап алады. Киберқылмыстылық туралы конвенцияның 3-бабында «техникалық құралдарды қолдану арқылы қасақана жүзеге асырылуға, компьютерлік жүйеге, одан немесе оның ішінде берілетін жалпыға қолжетімді емес компьютерлік деректерді, оның ішінде осындай компьютерлік деректерді тасымалдайтын компьютерлік жүйенің электромагниттік сәулеленуін заңсыз ұстауға» тыйым салынады. Ақпаратты заңсыз ұстауға Араб мемлекеттері лигасының 2010 жылғы Ақпараттық технология қылмыстарына қарсы конвенциясының 7-бабына және 2014 жылғы Африка Одағының Киберқауіпсіздік және жеке деректерді қорғау туралы конвенциясының 29(2)(a) бабына сәйкес тыйым салынған. Заңсыз ұстап алудың мысалы ретінде делдал шабуылы (немесе «ортадағы адам» шабуылы) болып табылады, ол шабуылдаушыға жіберуші мен алушы арасындағы хабарламаларды ұстауға және/немесе жіберушінің және/немесе алушының кейпін көрсетуге және олардың атынан байланысуға мүмкіндік береді. Бұл киберқылмыс деректердің құпиялылығын (ұстау арқылы) және деректердің тұтастығын (жіберушінің және/немесе алушының атын көрсету арқылы) бұзады. Хакерлік шабуылдарды жүзеге асырумен қатар, киберқылмыскерлер компьютерлік жүйелерге кедергі келтіруі және/немесе жүйелерге, қызметтерге және деректерге қол жеткізуге жол бермеуі мүмкін.

Кедергіге деректерді, жүйелер мен қызметтерді блоктау, өзгерту, қосу, тасымалдау, өңдеу, жою немесе басқа жолмен зақымдау кіруі мүмкін. Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясы «компьютер деректерін қасақана және заңсыз зақымдау, жою, нашарлату, өзгерту немесе бұғаттау» ретінде анықталған деректерді бұрмалауға тыйым салады (4-бап). Деректерге араласуға Африка Одағының 2014 жылғы Киберқауіпсіздік және жеке деректерді қорғау туралы конвенциясының 29(2)(a) бабында және 2010 жылғы Араб мемлекеттері лигасының Ақпараттық технология қылмыстарына қарсы конвенциясының 8-бабына сәйкес тыйым салынады.

Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясында «компьютер деректерін енгізу, тасымалдау, зақымдау, жою, кемсіту, өзгерту немесе бұғаттау арқылы компьютерлік жүйенің жұмысына қасақана және заңсыз елеулі кедергі келтіру» ретінде анықталған бұрмалауға тыйым салынады (5-бап). Киберқылмыстың бұл түріне 2014 жылғы Африка одағының Киберқауіпсіздік және жеке деректерді қорғау туралы конвенциясының 29(1)(d) бабымен де тыйым салынған. Жүйені бұзудың мысалы ретінде *қызмет көрсетуден бас тарту* (немесе DoS-шабуылы) болып табылады. DoS-шабуылы заңды трафиктің сайтқа кіруіне және/немесе жүйені пайдалануға жол бермеу сұраулары бар серверлерді және/немесе делдал құрылғыларды (маршрутизаторлар сияқты) шамадан тыс жүктеу арқылы жүйелерге кедергі жасайды (Maras, 2016, p. 270). *Бөлінген қызмет көрсетуден бас тарту* (*немесе DDoS-шабуылы*) заңды пайдаланушылардың кіруіне жол бермеу үшін серверлерді және/немесе делдал құрылғыларды шамадан тыс жүктеу үшін үйлестірілген шабуылдар жасау үшін бірнеше компьютерлер мен басқа сандық технологияларды пайдалануды білдіреді (Maras, 2016, p. 270-271) DDoS-шабуылдарының бір түрінің жұмыс істеу принципін келесі мысалмен түсіндіруге болады (CloudFlare, 2018): көптеген компьютерлер бір уақытта бір компьютерге (серверге) қосылуға тырысады деп елестетіңіз. Бұл компьютердің өңдеу қуаты және желі өткізу қабілеті шектеулі. Тым көп компьютерлер оған бір уақытта қосылуға әрекеттенсе, сервер әрбір қосылымға жеткілікті жылдам жауап бере алмайды. Нәтижесінде сервер *нақты пайдаланушылардың* сұрауларына жауап бере алмайды, өйткені ол *жалған сұраулармен* тым бос емес.

DDoS-шабуылдарын жеке адам, жеке адамдар тобы немесе мемлекет жүзеге асыруы мүмкін. Мемлекеттер қоғамның жұмыс істеуі үшін маңызды болып саналатын маңызды инфрақұрылымды нысанаға алады. Мысалы, А елі өзінің қаржы секторына қарсы В елінің DDoS-шабуылдарының сериясын бастан өткерді. Осы кибершабуылдардың нәтижесінде А елінің азаматтарына интернет-банкингке кіруге тыйым салынды, ал бұл елдегі банкоматтар үзіліспен жұмыс істеп тұрды.

DDoS-шабуылдары зиянды бағдарламалық қамтумен (немесе *зиянды бағдарламамен*) зарарланған цифрлық құрылғыларды пайдаланып, осы құрылғыларды қашықтан басқаруға мүмкіндік береді және оларды кибершабуылдар жасау үшін пайдалана алады. *Бот-желі* (яғни зомби деп аталатын жұқтырылған цифрлық құрылғылар желісі) *криптоджекинг* сияқты

басқа киберқылмыстарды жасау үшін пайдаланылуы мүмкін. *Криптоджекинг* - вирус жұқтырған компьютерлердің есептеу қуатын вирус жұққан цифрлық құрылғыны басқаратын тұлға (лар) қаржылық пайда алу үшін криптовалютаны (яғни, шифрланған цифрлық валюта) шығару үшін пайдаланылатын әдіс (яғни, «бот-желінің иесі») және/немесе бот-желі иелерінің жұмыс берушілері.

Сондай-ақ киберқылмыскерлер компьютерді теріс пайдалану құралдарын, соның ішінде техникалық құрылғыларды, зиянды бағдарламалық қамтамасыз етуді (немесе зиянды бағдарламаларды), сондай-ақ құпия сөздерді, кіру кодтарын және жеке тұлғаларға заңсыз кіруге, хабарларды ұстауға немесе нысанаға басқа жолмен зиян келтіруге мүмкіндік беретін басқа деректерді шығаруы, иеленуі және/немесе таратуы мүмкін. Ақпараттық технология қылмыстарына қарсы Араб мемлекеттері лигасы конвенциясының 9-бабы («ақпараттық технологияларды теріс пайдаланумен байланысты құқықбұзушылықтар») келесілерді қылмыстық жауапкершілікке тартады:

(1): (a) 6-баппен қарастырылған (заңсыз қол жеткізу қылмысы), 7-бап бойынша (хабарламарды заңсыз ұстап алу қылмысы), 8-баппен қарастырылған (деректердің тұтастығына қарсы қылмыстар бұзу) құқық бұзушылықтарды жасау мақсатында әзірленген немесе бейімделген кез келген құралдар мен бағдарламаларды өндіру, сату, сатып алу, импорттау, тарату немесе қамтамасыз ету; (b) 6-8-баптарда қарастырылған қылмыстарды жасау үшін ақпараттық жүйеге кіруге мүмкіндік беретін жүйе құпия сөзі, рұқсат коды немесе басқа ұқсас кез келген деректерді алу... және (2) жоғарыдағы екі тармақта аталған кез келген құралдарды немесе бағдарламаларды 6-8-баптарда көрсетілген құқық бұзушылықтарды жасау үшін пайдалану мақсатында кез келген құралдар мен бағдарламарды алу.

Сол сияқты, Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясы өндіруге, сатуға, пайдалану үшін сатып алуға, импорттауға, таратуға немесе пайдалануды қамтамасыз етудің басқа нысандарына тыйым салады: ... ең алдымен 2-5-баптарында көзделген қандай да бір құқық бұзушылықтарды жасау мақсатында құрылғыларды, соның ішінде әзірленген немесе бейімделген компьютерлік бағдарламаларды ...және/немесе 2-5-баптарда көзделген қандай да бір құқық бұзушылықтардың кез келгенін жасау мақсатында компьютерлік құпия сөздерді, кіру кодтарды немесе басқа ұқсас олар арқылы компьютерлік жүйеге тұтастай немесе оның кез келген бөлігіне қол жеткізу деректерды оларды пайдалану ниетімен алуға ... сонымен қатар, 2-5-баптарда (6-бап) белгіленген қылмыстардың кез келгенін жасау мақсатында пайдалану үшін оларды иемденуге. Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясы (6-бап) мұндай заңсыз мінез құлықтарды құрылғыларды заңсыз пайдалану ретінде сипаттайды. 6(3)-бапқа сәйкес, мемлекеттер 6-бапта аталған әрекеттерге «тыйым салмау құқығын өзіне қалдырады», егер мұндай бас тарту 2-5-баптарда көзделген құқық бұзушылықтардың кез келгенін жасау мақсатында оларды пайдалану ниетімен компьютерлік жүйеге тұтастай немесе оның кез келген бөлігіне қол жеткізуге болатын «сатуға, таратуға немесе қолжетімді етудің басқа нысандарына

«компьютерлік құпия сөздерге, кодтарға басқа да осыған ұқсас деректерге қол жеткізуге» қолданылмаса. Сонымен қатар, 6(2)-бапқа сәйкес «6-бапта санамаланған заттарды «өндіру, сату, пайдалану үшін сатып алу, әкелу, иемдену, бөлу немесе қолжетімді етудің өзге де нысандары» жасау мақсатында емес осы Конвенцияның 2-5-баптарында көзделген, бірақ, мысалы, рұқсат етілген тестілеумен немесе компьютерлік жүйені қорғаумен байланысты қылмыстар» қылмыстық жауаптылыққа әкеп соқпайды. Осылайша, бұл бапта бұл құралдардың екі жақты мақсаты танылады - олар, мысалы, заңды түрде пайдаланылуы мүмкін, сондай-ақ заңсыз пайдаланылуы мүмкін.

2. Компьютерлік құралдарды пайдалануға байланысты құқық бұзушылықтар

Компьютерлік құралдарды пайдалануға байланысты құқық бұзушылықтарға «жеке немесе қаржылық пайда немесе жеке немесе қаржылық зиян үшін» кибертехнологиялар арқылы жасалған қылмыстар жатады (БҰҰ ЕҚБ 2013, 17 б.). Бұл санатқа «компьютер жүйесін (немесе цифрлық құрылғыны) пайдалану қылмыс жасау тәсілінің бір бөлігі болып табылатын» киберқылмыстарды қамтиды (БҰҰ ЕҚБ, 2013, 19 б).

БҰҰ ЕҚБ-ның «Киберқылмыстылық проблемаларын жан-жақты зерттеу» есебінің жобасы осы кең санатқа келесі киберқылмыстарды жатқызады:

Компьютерлік алаяқтық немесе жалғандық;

Жеке деректерді пайдалануға байланысты компьютерлік қылмыстар;

Спам жіберу немесе спамның таралуын бақылау;

Авторлық құқыққа немесе сауда белгілеріне қатысты компьютерлік қылмыстар;

Жеке зиян келтіру мақсатында компьютерді пайдаланумен байланысты әрекеттер;

Компьютерді балаларды азғыру және груминг мақсатында пайдаланумен байланысты әрекеттер (БҰҰ ЕҚБ 2013, 17 б.).

Компьютерлік алаяқтық немесе жалғандық.

Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясына сәйкес, алаяқтық және жалғандық *компьютерлік құралдарды пайдалану аркылы құқық бұзушылықтардың* (яғни, компьютерлік жалғандық және компьютерлік алаяқтық) ажырамас бөлігі болып саналады. Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясының 7-бабында *компьютерлік жалғандық* «компьютерлік деректерді қасақана және заңсыз енгізу, өзгерту, жою немесе бұғаттау, бұл деректердің түпнұсқалығын бұзуға әкеп соғатын, оларды қарау немесе бұл деректер тікелей оқуға және түсінікті болуына қарамастан, заңды мақсаттарда түпнұсқа ретінде пайдаланылады. Киберқылмыстылықтың бұл түріне Араб мемлекеттері лигасының ақпараттық технологиялар қылмыстарына қарсы конвенциясының 10-бабында да тыйым салынған.

Компьютерлік алаяқтық қылмыскерлер алаяқтық мақсатында желідегі заңды тұлғалардың, органдардың, мекемелердің және басқа да субъектілердің

атын жамылған кезде тұлғалану элементтерін қамтиды. Киберқылмыскерлер заңды ұйымдар мен мекемелердің адамдарының атынан оларды жеке ақпаратты ашуға және қылмыскерлерге ақшамен, тауарлармен және/немесе қызметтермен қамтамасыз етуге мәжбүрлей алады. Электрондық поштаны жіберуші заңды ұйымнан немесе мекемеден болып көрініп, пайдаланушыларды электрондық поштаның мазмұнына сенуге және ондағы нұсқауларды орындауға сендіруге тырысады. Электрондық хат жалған электрондық пошта мекенжайынан (ұйымның немесе агенттіктің шынайы электрондық поштасына ұқсайды) немесе заңды ұйымның немесе агенттіктің атына ұқсас домендік атаудан (шағын өзгерістермен) жіберіледі.

Кең таралған әдістердің бірі - басқан кезде зиянды бағдарламаны сандық құрылғыларына жүктеп алуға немесе пайдаланушының тіркелгі деректерін ұрлауға арналған зиянды веб-сайтқа қайта бағытталатын веб-сайт сілтемесі бар электрондық хаттарды жіберу (*фишинг*). «Жалған» веб-сайт ұйымның және/немесе мекеменің веб-сайтына ұқсайды және пайдаланушыдан сайтқа кіру үшін тіркелгі деректерін сұрайды. Электрондық поштада қорқынышты, дүрбелеңді және/немесе жеделдік сезімін тудыру үшін пайдаланушыны электрондық поштаға мүмкіндігінше тезірек жауап беруге (және сол электрондық поштада сұралған тапсырмаларды орындауға) итермелейтін әртүрлі ескертулер бар, мысалы, жеке ақпаратты жаңарту қажеттілігі. қаражатты немесе басқа төлемдерді алу үшін, пайдаланушының шотындағы алаяқтық әрекеттер туралы ескертулер және нысананың дереу назарын талап ететін басқа да оқиғалар.

Бұл әдіс мақсатты емес, өйткені мүмкіндігінше көп құрбандарға жету үшін электрондық хаттар көптеп жіберіледі. Мақсатты фишинг *мекенжайы фишингімен* белгілі. Мұндай алаяқтық жасалған кезде компания қызметкерлерінің ішкі істерімен және лауазымдарымен таныс шабуылдаушылар ақпаратты ашуға және/немесе шабуылдаушыларға ақша жіберуге алдау үшін қызметкерлерге электрондық хаттар жібереді. Фишингтің тағы бір әдісі – киберқылмыскерлер компанияның жоғары деңгейдегі басшыларын (соның ішінде жоғары басшылық – бас басқарушы директор, бас қаржы директоры және қауіпсіздік жөніндегі директор), заңгерлерді, есепшілерді және басшылық және жауапты лауазымдардағы басқаларды еліктіріп, қызметкерлерді оларға ақша жіберуге мәжбүрлеу үшін алдау. Бұл әдіс *уэйлинг* ретінде белгілі (whaling – ағылшынна «кит аулау» *жуық аударма*), себебі ол қылмыскерлерге құрбандардан ең үлкен пайда алуға мүмкіндік береді.

Американдық ойыншықтар Mattel компаниясы уэйлинг-алаяқтықтың құрбаны болды. Шабуылдың артында тұрған киберқылмыскерлер оқиғадан бірнеше ай бұрын компанияның компьютерлік желілері мен коммуникацияларын жасырын бақылаған. Компания жаңа бас директордың тағайындалғанын жариялағаннан кейін киберқылмыскерлер шабуыл жасау үшін жаңа бас директор Кристофер Синклердің (Christopher Sinclair) жеке басын пайдаланды. Атап айтқанда, киберқылмыскерлер Кристофер Синклердің атынан алушыдан Қытайдағы Вэньчжоу банкіне қытайлық

жеткізушінің шотына 3 миллион доллар аударуды мақұлдауды сұрайтын электрондық хат жіберді. Өтініш бас директордан түскендіктен, компания қызметкері ақшаны аударған, бірақ кейінірек бұл туралы оған хабарласқан. Бас директор ақшаны аударуға ешқандай нұсқау бермегенін айтты. Содан кейін Mattel АҚШ құқық қорғау органдарымен, АҚШ-тың Федералдық тергеу бюросымен, өз банкімен және Қытайдың құқық қорғау органдарымен байланысқа шықты (Ragan, 2016). Оқиғаның уақыты (ақша мереке қарсаңында аударылған) Қытай билігіне банктер ашылғанға дейін шоттарды уақытында бұғаттауға мүмкіндік берді, ал Mattel ақшасын қайтарып алды.

Телефон байланысын пайдаланатын фишинг *вишинг* деп аталады (алаяқтар көрсетілген нөмірге қоңырау шалуды және жеке және/немесе қаржылық ақпаратты ашуды сұрайтын дауыстық хабарлама жіберген кезде), ал мәтіндік хабарламаларды пайдаланатын фишинг - *смишинг* (немесе SMS фишинг) деп аталады.

Компьютерлік алаяқтыққа махаббат пен достық туралы жалған немесе жаңылыстыратын уәделер беруді қамтитын әртүрлі онлайн алаяқтықтары кіреді (кэтфишинг), мүлік (мұрагерлік алаяқтық арқылы), ақша мен байлық (лотерея алаяқтығы, инвестициялық алаяқтық, мұрагерлік алаяқтық және т.б. арқылы). Мұндай алаяқтықтардың түпкі мақсаты жәбірленушіні шабуылдаушыға жеке ақпаратты және/немесе қаражатты ашуға немесе басқа жолмен беруге мәжбүрлеу болып табылады (бұл *әлеуметтік инженерия әдісімен алаяқтықтың* бір түрі). Бұл әдіс, аты айтып тұрғандай, әлеуметтік инженерияны (американдық хакер Кевин Митник (Kevin Mitnick) танымал еткен термин), «адамдарды айла, алдау, ықпал ету немесе алдау арқылы - құпия ақпаратты ашуға немесе орындауға мәжбүрлеу тәжірибесіне негізделген. әлеуметтік инженерге қандай да бір жолмен пайда әкелетін әрекеттер» (Maras, 2014, p. 141).

Компьютерлік алаяқтықтың ең танымал түрі - бұл үлкенірек ақшаның орнына ақша аудару, депозит немесе басқа транзакцияны аяқтау үшін аванстық төлемді сұрайтын хаттар (*алдын ала төлем алаяқтығы*, «419 алаяқтық» деп те аталады). Шабуыл жасаушылардың айтатын оқиғасы үнемі өзгеріп отырса да (олар мемлекеттік қызметкерлерді, банк қызметкерлерін, заңгерлерді және т.б. кейіп танытады), олар дәл осындай тактиканы қолданады - үлкен соманың орнына аздаған ақша аударуды сұрайды.

Жеке деректермен байланысты компьютерлік қылмыстар және спам

Интернетте онлайн схемалардан басқа қаржылық (немесе экономикалық) алаяқтықтың кейбір түрлері де жасалады, мысалы, банктік алаяқтық, электрондық пошта арқылы алаяқтық, несиелік және дебеттік карталармен алаяқтық. Мысалы, қылмыскерлер заңсыз алған дебеттік және несиелік карта деректерді сатып, бір-біріне беріп және интернетте пайдаланады. 2018 жылы халықаралық киберқылмыстылық операциясы қылмыскерлер несиелік және дебеттік карталарды және банк ақпаратын сатқан және алмасатын ең танымал онлайн карта форумдарының бірін, Infraud-ты жауып тастады. Интернетте сатып алынатын, сатылатын және

айырбасталатын жеке, денсаулық және қаржылық ақпарат басқа қылмыстарды жасау үшін пайдаланылуы мүмкін, мысалы, кінәлі өзін басқа тұлға ретінде бұрмалаған және/немесе жеке басын заңсыз иемденетін жеке деректерді пайдалануға байланысты қылмыстар және/немесе осы сәйкестендіруді және/немесе жеке деректерді заңсыз мақсаттарда пайдаланады (UNODC, nd). Қылмыскерлер көздеген деректерге сәйкестендіру нөмірлер (АҚШ әлеуметтік сақтандыру нөмірлері сияқты), жеке басын куәландыратын құжаттар (мысалы, паспорттар, ұлттық жеке сәйкестендіру нөмірлер, жүргізуші куәліктер және туу туралы куәліктер) және интернет тіркелгі деректері (мысалы, пайдаланушы аттары мен құпия сөздер) сияқты ақпараттар (UNODC, 2011, p. 12-15). Жеке деректер бойынша құқық бұзушылық қаржылық мотивацияланған болуы немесе осындай болмауы мүмкін. Мысалы, жалған төлқұжаттарды (мысалы, паспорттар) саяхат кезінде пайдалану үшін онлайн сатып алуға болады (UN-CCPCJ, 2017, p. 4). Қылмыстың бұл түрлері, сондай-ақ экономикалық алаяқтық Интернет арқылы пайдаланушыларға сұраусыз электрондық хаттарды (спам), ақпараттық бюллетеньдерді және пайдаланушыларды адастырып, оларды алдап ашуға арналған веб-сайттарға сілтемелерді жіберу арқылы жасалады, олар пайдаланушыларды электрондық пошталар мен ақпараттық бюллетеньдерді ашуға немесе зиянды бағдарлама болуы мүмкін электрондық хаттардағы сілтемелерді басуға, ал ол сілмелер пайдаланушыларды жалған веб-сайттарға, зиянды бағдарламары бар сайттарға бағыттауға арналған.

Жеке зиян келтіру мақсатында компьютерді пайдаланумен байланысты әрекеттер

БҰҰ ЕҚБ-нің 2013 жылғы «Киберқылмыстылық проблемаларын жанжақты зерттеу» есебінің Жобасына сәйкес, «жеке зиян келтіру үшін компьютерді пайдаланумен байланысты әрекеттер» «адамды қудалау, ұмтылу, қорқыту, немесе қауіп төндіру үшін компьютерлік жүйені пайдалануды» қамтиды. Киберқылмыстың бұл түрлерінің мысалдары киберқудалау, кибералымсақтық және киберқорлау болып табылады. Бұл киберқылмыстар көпжақты және аймақтық киберқылмыстылық туралы келісімдерге қосылмаған (мысалы, Еуропа Кеңесінің Киберқылмыстылық туралы конвенциясы; Африка одағының киберқауіпсіздік және жеке деректерді қорғау туралы конвенциясы; және Араб мемлекеттері лигасының ақпараттық технологиялар саласындағы қылмыстармен күресу туралы конвенциясы).

Киберқудалау, кибералымсақтық және киберқорлау терминдері бір-бірінің орнына қолданылады. Кейбір елдерде баланың құрбан немесе құқық бұзушы ретінде әрекет етуін қамтитын кез келген әрекет киберқорлау деп аталады (мысалы, Австралия мен Жаңа Зеландияда), ал АҚШ-тың кейбір штаттарында киберқорлау термині балалар жасаған және балаларға қарсы әрекеттерге тиесілі қолданылады. Кейбір елдер «киберқорлау» терминін қолданбайды және оның орнына «кибералымсақтық» немесе «киберқудалау» терминін немесе *кибермоббинг* (Австрия мен Германияда) сияқты басқа терминдерді киберқорқорлауды белгілеу үшін пайдаланады (European Parliament, Citizens' Rights and Constitutional Affairs, 2016, pp. 24-

25), ал басқа елдер бұл терминдердің ешқайсысын қолданбайды. Мұндай елдерге, мысалы, Ямайка жатады, ол 2015 жылғы «Киберқылмыстар туралы» заңның 9(1) бабына сәйкес «зиянды және/немесе қорлайтын хабарламаларға» тыйым салады, онда адам «(a)... компьютерді пайдалану арқылы басқа адамға ұятсыз, қауіп төндіретін немесе қорқытатын кез келген деректерді (хабарлама түрінде немесе басқа жолмен) жіберсе; және (b) мұндай деректерді әдейі немесе байқаусызда жіберу арқылы осы адамға немесе кез келген басқа адамға тітіркендіргіш, қолайсыздық, алаңдаушылық немесе толқу тудырса деп бекітілген.

Киберқудалау. Ақпараттық-коммуникациялық технологияларды (АКТ) белгілі бір уақыт ішінде адамды (немесе адамдарды) құштарлық, мазалау, шабуылдау, қауіп төндіру, қорқыту және/немесе тұлғаны (тұлғаларды) сөзбен қорлау үшін қайталанатын әрекеттерді жасау үшін пайдалану.

Кибералымсақтық. АКТ-ны адамды (немесе тұлғаларды) намыстандару, тітіркендіру, шабуылдау, қорқыту, ренжіту және/немесе қорлау үшін қасақана әрекеттер үшін пайдалану.

Киберқорлау. Балалардың АКТ-ны басқа балаларды ауыртпалық акелу, намыстандару, ренжіту, құштарлық ету, қорқыту, қудалау, қатыгездікпен қарау немесе басқа жолмен балаларға арналған шабуылдау үшін пайдалануы.

Киберқылмыстың бұл түрлерінің айырмашылығы қылмыс жасаушылардың жасында (мысалы, тек балалар киберқорқыту жасайды және оның құрбаны болады), сондай-ақ киберқылмыстың қарқындылығы мен жиілігінде (киберқудалау бірнеше жылдардағы оқиғалар қатарын қамтиды). уақыт, ал кибералымсақтық бір немесе бірнеше оқиғаны қамтуы мүмкін).

Балаларды арбау немесе груминг.

Ақпараттық-коммуникациялық технологиялар балаларға қатысты груминг жасауға әрекеттесу үшін қолданылады. Балалар грумингі – бұл жәбірленушімен эмоционалды қарым-қатынасты дамыту арқылы өзара түсіністік пен сенімділікті орнату процесі (Maras, 2016, p. 244). Груминг процесі стилі, ұзақтығы және қарқындылығы тұрғысынан айтарлықтай өзгереді, бұл көбінесе қылмыскердің жеке басына және мінез-құлқына байланысты. Қылмыскер жәбірленушіні әртүрлі мәжбүрлеу және бақылау әдістерін қолдана отырып, айла-шарғы жасай алады, соның ішінде (бірақ олармен шектелмей): мақтау, сыйлықтар, оқшаулау, қорқыту және/немесе зорлық (Maras, 2016), сондай-ақ ортақ мүдделерді модельдеу немесе баланың жалғыздық сезімін имитациялау арқылы сенімге ие болу. Груминг балаларға әлеуметтік желі платформаларында, электрондық пошта, чаттар, жылдам хабар алмасу қызметтер, қолданбалар және т.б. арқылы жасалуы мүмкін. Британдық BBC телеарнасының 2017 жылы жүргізген зерттеуі әлемнің кез келген нүктесінде тікелей трансляцияға мүмкіндік беретін Periscope қолданбасын хакерлердің балалар грумингі үшін пайдаланғаны анықтады. Тікелей эфирде балалармен байланысқан шабуылдаушылар балалар туралы сексуалдық сипаттағы пікірлер айтты, ал кейбіреулері тіпті балалардан киімдерін шешуді сұрады (BBC, 2017).

3. Компьютерлік деректердің мазмұнына байланысты құқық бұзушылықтар

Атауынан көрініп тұрғандай, осы бөлімге енгізілген киберқылмыстар заңсыз мазмұнды қамтиды. Заңсыз мазмұнның көрнекі мысалы - балаларға жыныстық зорлық-зомбылық көрсететін материал. *«Балалар порнографиясының»* орнына *«балаларға жыныстық зорлық-зомбылық материалдары» т*ерминін пайдалану керек, себебі балалар порнографиясы термині қылмыстың ауырлығын азайтады. Бет арқылы қаралған материалда бала мен ересек адамның жыныстық қатынасы емес, баланың жыныстық зорлық-зомбылығы бейнеленген. Дегенмен, халықаралық, аймақтық және ұлттық заңнамада «балаларға жыныстық зорлық-зомбылық көрсететін материал» орнына «балалар порнографиясы» термині қолданылады. Киберқылмыстылық туралы Еуропа Кеңесі Конвенциясының 9-бабы балалар порнографиясына қатысты құқық бұзушылықтар үшін қылмыстық жауапкершілікті көздейді, оның ішінде балалар порнографиясы тұжырымдамасына «кәмелетке толмағанның ашық сексуалдық әрекетпен айналысатын визуалдық бейнелері, кәмелетке толмаған болып көрінетін адамның ашық сексуалдық әрекеттерге қатысуы және/немесе кәмелетке толмаған баланың ашық сексуалдық әрекетпен айналысатын шынайы бейнелері» кіреді. Балалар порнографиясының бұл тұжырымдамасы жалпыға бірдей болып табылмайды; кейбір мемлекеттер мультфильмдер мен суреттер сияқты балалар порнографиясының шындыққа жанаспайтын бейнелерін тарату үшін қылмыстық жауапкершілік бекітеді (мысалы, Бразилия, Коста-Рика, Доминикан Республикасы, Гватемала, Мексика, Никарагуа, Панама және Уругвай), ал басқа мемлекеттер тек шынайы балалармен суреттерді таратқаны үшін қылмыстық жауапкершілікті көздейді (мысалы, Аргентина, Боливия, Чили, Колумбия, Эквадор, Сальвадор, Гондурас, Парагвай, Перу және Венесуэла) (ICMEC and UNICEF, 2016).

Балаларды коммерциялық сексуалдық қанау – бұл ақшалай немесе ақшалай емес сыйақы (мысалы, баспана, тамақ) алу үшін балаларға жыныстық зорлық жасаудың белгілі бір әрекеттері мен қылмыстарын сипаттау үшін қолданылатын термин. Балаларды коммерциялық сексуалдық қанаудың мысалы ретінде балаларға жыныстық зорлық-зомбылық көрсетудің тікелей трансляциясы табылады, ол көрермендер пассивті немесе белсенді болуы мүмкін (яғни, олар жәбірленушіні бақылай және/немесе онымен әрекеттесе алады, баладан белгілі бір әрекеттерді орындауды сұрайды немесе ересектерден балаға қатысты белгілі бір әрекеттерді орындауын сұрайды) (UNODC, 2015). Балаларды коммерциялық сексуалдық пайдаланудың осы және басқа да нысандары, мысалы, *жыныстық қанау мақсатында балаларды сату*, ол «он сегіз жасқа толмаған баланы коммерциялық жыныстық қатынас мақсатында азғыруды, жұмысқа тартуды, паналауды, тасымалдауды, беруді немесе қабылдауды білдіреді».

Кейбір елдерде жалған ақпарат жариялау да қылмыс болып табылады. Танзанияда 2015 жылғы «Киберқылмыстар туралы» заңның 16 бабы «компьютер жүйесінде сурет, мәтін, таңба немесе кез келген басқа нысанда

ұсынылған ақпаратты немесе деректерді, егер бұл деректер мен ақпаратты жариялаған адам олардың жалған, қате, жаңылыстыратын немесе дәйексіз екенін біле тұра және жұртшылықты қорлау, қорқыту немесе алдау немесе өзге де жолмен адастыру мақсатында жарияланған болса, немесе кеңес беру түріндегі қылмыс жасауға қатысу мақсатындағы» ақпаратты жариялауға тыйым салады.

Сонымен қатар, Кениянының 2018 жылғы «Компьютерді теріс пайдалану және киберқылмыстар туралы» Заңы «біле тұра ... республика азаматтарының арасында дүрбелең, хаос немесе зорлық-зомбылық тудыратын немесе дүрбелеңді, бейберекеттік немесе зорлық-зомбылықты таратуға арналған не адамның беделіне нұқсан келтіруге әкеп соғуы мүмкін баспасөз және телерадио бұқаралық ақпарат құралдарында немесе компьютерлік жүйе арқылы жалған ақпаратты жариялау» үшін қылмыстық жауапкершілікке тартады.

Алайда, БҰҰ УНП-нің «Киберқылмыстылық проблемаларын жанжақты зерттеу» есебінің Жобасына сәйкес (2013), «елдер сөз бостандығына әр түрлі дәрежедегі шектеулер туралы хабарлайды, соның ішінде жала жабу, құрметтемеу, қорқыту, өшпенділік тудыру, діни сезімдерді қорлау, әдепсіз материалдар және мемлекет негіздеріне нұқсан келтіру» (БҰҰ ЕҚБ, 2013, 21б.). Бірқатар жағдайларда мемлекеттік органдардың сөз білдірудің осындай нысандарына қатысты интернет-контентті алып тастауы адам құқықтарын сақтау контексте қатысты алаңдаушылық туғызды (БҰҰ ЕҚБ, 2013, 28 б.).

2005 жылы БҰҰ Қауіпсіздік Кеңесі 1624 резолюциясын қабылдады, онда (басқа нәрселермен қатар) барлық мемлекеттер «қажет және орынды және халықаралық құқық бойынша өздерінің міндеттемелеріне сәйкес келетін шараларды қабылдауға шақырады: лаңкестік әрекетті немесе әрекеттерді жасауға шақыруға заңды түрде тыйым салу... және мұндай мінез-құлықтың алдын алу» (UNSCR 1624 (2005). Қатысушы мемлекеттер осы мақсатқа жету үшін қабылдай алатын шаралар лаңкестікке шақыруды криминализациялауды қамтиды.

Басқа халықаралық органдар да мемлекеттерді өздерінің ұлттық құқықтық жүйелерінде терроризмге шақырумен күресу үшін шаралар қабылдауға шақырады. Мысалы, Еуропа Кеңесінің 2008/919 / ЈНА 2008 жылғы 28 қарашадағы 2002/475 / ЈНА Терроризмнің жолын кесу туралы негіздемелік шешіміне және 2005 жылғы Еуропа Кеңесінің Терроризмнің алдын алу туралы конвенциясының 5-бабына түзетулер енгізу туралы 2008/919 негіздемелік шешімінің 3-бабы тиісті Қатысушы мемлекеттерді террористік актілерді жасауға итермелейтін әрекеттерді немесе мәлімдемелерді қылмыстық жауапкершілікке тартуға міндеттейді. Сонымен қатар, Еуропа Кеңесінің Терроризмнің алдын алу туралы конвенциясы мүше мемлекеттерге «террористік құқық бұзушылықтарды жасауға жария түрде шақыру» және террористерді жалдау және оқыту үшін қылмыстық жауапкершілікке тарту міндетін жүктейді (UNODC, 2012, pp. 39-40).

Қазіргі уақытта халықаралық құқықта барлық мемлекеттер үшін лаңкестікке шақыру әрекеттерін қылмыстық жауапкершілікке тарту бойынша

заңды түрде міндетті болатын әмбебап міндеттеме болмағанымен, көптеген мемлекеттер мұндай әрекеттермен күресу үшін құқықтық және қылмыстық-құқықтық тәсілдерді пайдаланады. Кейбір елдерде қолданылған тәсілдердің мысалдары АҚШ-тың лаңкестікке шақыру әрекеттерін жасаған адамдарды сәтті қудалау үшін АҚШ Заңдар жинағының 18-тарауын 373 (a) бөлімін қолдануы болып табылады, ол арандату мен сөз байласуға тыйым салады (мысалы, Америка Құрама Штаттары Эмерсон Уинфилд Беголлиге қарсы ісі United States of America v. Emerson Winfield Begolly, UNODC, 2012, pp. 39-41) және Ұлыбритания билігінің 2006 жылғы «Терроризм туралы» заңның «терроризмді насихаттауды» қылмыстық жауапкершілікке тартатын 1-бөлімін төмендегідей пайдалануы:

Адам қылмыс жасайды, егер:

(a) ол осы бөлім қолданылатын мәлімдемені жариялайды немесе басқа тұлғаны осындай мәлімдемені жариялауға итермелейді;

(b) ол осы мәлімдемені жариялаған немесе басқа тұлғаны оны жариялауға шақырған кезде:

(i) қоғам мүшелерінің түсінігін тікелей немесе жанама көтермелеу немесе терроризм актілерін немесе Конвенцияға сәйкес құқық бұзушылықтарды жасауға, дайындауға немесе шақыруға басқа итермелеу ретінде түсіндіріледі;

немесе (ii) бұл мәлімдеменің қоғам мүшелерінің тікелей немесе жанама мадақтау немесе терроризм актілерін немесе қылмыстарды жасауға, дайындауға немесе итермелеуге басқа итермелеу ретінде түсінетініне бей-жай қарамайды.

Ұлыбритания билігі 2000 жылғы «Терроризм туралы заңға» сәйкес лаңкестікке шақыру әрекеттерін қудалаудың сәтті тәжірибесіне ие. Юнис Тсулидің ісін қараңыз және осы заң бойынша өздері құрған, басқаратын және бақылайтын веб-сайттар мен чат бөлмелеріне материал жариялау арқылы шетелде терроризмге шақыру бойынша сотталғандардың ісін қараңыз (UNODC, 2012, p. 114).

Халықаралық құқықта мемлекеттердің терроризмді қоздырумен күресу шараларын қабылдау жөніндегі жалпыға бірдей заңды міндеттемесінің жоқтығына қарамастан, көптеген мемлекеттер мұндай шараларды ұлттық деңгейде қабылдады. Дегенмен, бірнеше факторлар осы проблеманы шешуде халықаралық келісілген тәсілді қабылдауда қиындықтар туғызуда, соның ішінде терроризмнің жалпы қабылданған анықтамасының жоқтығы және сөз бостандығы құқығы және ассоциация бостандығы, құпиялылық және т.б. сияқты негізгі адамның құқықтарына ұлттық конституциялық және құқықтық көзқарастардағы айырмашылықтар. Сондықтан барлық мемлекеттердің заң шығарушылары, құқық қорғау және қылмыстық сот төрелігі органдарының алдында белгілі бір саяси немесе идеологиялық көзқарастарды білдіру заңды құқыққа «шектеушілік әсер етпей» зорлық-зомбылық әрекеттерін тудыратын интернеттегі ақпараттық материалдарға бағытталған ұлттық тәсілдерді қабылдау және енгізу қиын міндет тұр (қараңыз: UNODC, 2012, pp. 39-41).

Талқылауға арналған сұрақтар:

1. Киберқылмыстардың жалпы категориялары қандай?
2. Бұл санаттарға қандай киберқылмыстар жатады?
3. Бірнеше санатқа жататын қылмыстар бар ма?
4. Олай болса, қайсысы?
5. Киберқылмыстылыққа анықтама беріңіз. Бұл киберқылмыс қалай жасалады?
6. Процесті егжей-тегжейлі сипаттаңыз.

3 Тақырып. Құқықтық база және адам құқықтары.

1. Киберқылмыстылық туралы заңнаманың рөлі. Киберқылмыстылық туралы заңнама ақпараттық-коммуникациялық технологияларды (АКТ) пайдаланушылар үшін қолайлы мінез-құлық стандарттарын анықтайды; киберқылмыстар үшін әлеуметтік және құқықтық санкцияларды белгілейді; жалпы АКТ пайдаланушыларын қорғайды және әсіресе адамдарға, деректерге, жүйелерге, қызметтерге және инфрақұрылымға келетін зиянды азайтады және/немесе алдын алады; адам құқықтарын қорғайды; интернетте (нақты әлемнен тыс) жасалған қылмыстарды тергеу және қылмыстық қудалау мүмкіндігін береді; және киберқылмыс істері бойынша мемлекетаралық ынтымақтастықты жеңілдетеді (БҰҰ ЕҚБ, 2013, 57б.). Киберқылмыстылық туралы заңнама Интернетті, компьютерлерді және олармен байланысты цифрлық технологияларды және мемлекеттік, мемлекеттік және жеке ұйымдардың әрекеттерін пайдалану кезіндегі мінез-құлық ережелері мен стандарттарын; дәлелдеу ережелері, қылмыстық процесті жүзеге асыру ережелері және киберкеңістікке қатысты қылмыстық құқықтың басқа да мәселелері; киберқылмыс жағдайында жеке тұлғаларға, ұйымдарға және инфрақұрылымға тәуекелді төмендету және/немесе залалды төмендету ережелерін қарастырады. Осылайша, киберқылмыстылық саласындағы заңнама материалдық, процессуалдық және алдын алу құқығын қамтиды.

Материалдық құқық. Құқықсыз әрекет заңда анық көрсетіліп, заңмен тыйым салынуы тиіс. *«Nullum criminaln sine lege»* (латынша «оны қамтамасыз ететін заңсыз қылмыс болмайды») моральдық қағидасына сәйкес адам осы әрекетті жасаған кезде заңмен белгіленбеген әрекет үшін жазаланбайды. акт (БҰҰ ЕҚБ, 2013, 59 б.). *Материалдық құқық* жеке тұлғаларды, ұйымдарды және мемлекеттерді қамтитын құқық субъектілерінің құқықтары мен міндеттерін анықтайды. Материалдық құқықтың қайнар көздері - жергілікті және орталық заң шығарушы органдар шығаратын нормативтік актілер мен өкімдері *(статут құқығы)*, федералдық конституциялар және федералды бірліктер конституциялары, сонымен қатар сот шешімдері (жалпы құқық жүйелерінде).

Киберқылмыс туралы материалдық заңнама киберқылмыстылықтың нақты түрлеріне тыйым салатын және бұл заңдарды орындамағаны үшін жазаларды қамтиды. Киберқылмыстарға Интернеттің өнертабысы мен

Интернет арқылы жұмыс істейтін цифрлық технологиялардың арқасында мүмкін болған «гибридті» немесе «кибержелілерді қолданып жасалатын қылмыстар», сонымен қатар «жаңа» немесе «кибертәуелді» киберкеңістікте жасалған нақты әлемдегі (интернеттен тыс) дәстүрлі құқық бұзушылықтар (мысалы, алаяқтық, жалғандық, ұйымдасқан қылмыс, ақшаны жылыстату және ұрлау) жатады (Maras 2014; Maras, 2016). Сондықтан көптеген елдерде киберқылмыстылықты арнайы қарастыратын заңдар әзірленді. Мысалы, Германия, Жапония және Қытай киберқылмыспен күресу үшін өздерінің қылмыстық кодекстерінің тиісті ережелеріне түзетулер енгізді. Сонымен қатар, кейбір елдер киберқылмыстылық пен киберқылмыскерлердің жекелеген түрлерін қамту үшін нақты әлемде (Интернеттен тыс) қылмыспен күресуге арналған қолданыстағы заңдарды қолданды. Тағы бір мысал ретінде Иракты келтіруге болад, мұнда қолданыстағы азаматтық кодекс (Ирактың 1951 ж. №40 Азаматтық кодексі) және қылмыстық кодексі (Ирактың 1969 жылғы №111 Қылмыстық кодексі) нақты әлемде Интернет пен цифрлық технологияларды қолдану арқылы жасалған қылмыстарды (мысалы, алаяқтық, шантаж, жеке деректерді ұрлау).

Кейбір елдер киберқылмыстылықпен күресудің жаңа нақты заңдарын әзірлеудің орнына өздерінің ұлттық заңдарына немесе кодекстеріне киберқылмыспен байланысты нақты ережелермен толықтырып түзетілер енгізді. Бұл тәжірибенің қызықты және елеулі салдары болды, өйткені кейбір елдер қылмыс жасау үшін ақпараттық -коммуникациялық технологияларды теріс пайдалануды бөлек қылмыстық жауапкершілікке тарту туралы шешім қабылдады. Осылайша, егер қылмыскер жалғандық немесе алаяқтық жасау үшін заңсыз қол жеткізуді пайдаланса, мұндай әрекет бір мезгілде екі қылмысты құрайды.

Құқықтық жүйелер. Әр мемлекеттің киберқылмыстылық саласындағы материалдық қылмыстық құқықты құруға әсер ететін өзінің құқықтық жүйесі бар. Бұл жүйелерге (Maras, 2020) (баспаға дайындалуда):

1) *Жалпы құқық.* Жалпы құқықтағы елдер заңдарды *сот прецеденттері* негізінде құрады (яғни, іс бойынша шешім сот пен төменгі сатылар үшін міндетті) және қалыптасқан тәжірибе негізінде. Бұл заңдар жеке заңдар мен *прецедент құқығы* түрінде болады (яғни соттардың шешімдері немесе сот прецеденттері негізінде қалыптасатын құқық).

2) *Азаматтық құқық.* Мұндай құқықтық жүйесі бар елдер мінез - құлыққа қатысты негізгі құқықтардың, міндеттемелердің, міндеттер мен күтулердің шеңберін белгілейтін кодификацияланған, шоғырландырылған және жан-жақты құқықтық нормалар мен ережелерді қабылдайды. Бұл жүйелер негізінен заңдар мен конституцияларға негізделген.

3) *Әдет-ғұрып құқығы.* Бұл құқықтық жүйелер мәдениет ішіндегі қалыптасқан және жалпы қабылданған мінез-құлық үлгілерін қамтиды, сол мәдениетті алып жүрушілер заң ретінде қабылдайды *(opioio juris - заңдылыққа сену).* Халықаралық құқықта әдет-ғұрыптық құқық мемлекеттер арасындағы қарым-қатынас пен практиканы реттейді және барлық мемлекеттер үшін міндетті болып саналады.

4) *Діни құқық.* Діни құқық жүйелері құқықтың көзі ретінде діни ілімдерге немесе діни әдебиеттерге негізделген ережелерді қолданады.

5) *Құқықтық плюрализм.* Осы түрдегі құқықтық жүйеде жоғарыда аталған екі немесе одан да көп құқықтық жүйелер қатар өмір сүруі мүмкін (яғни, жалпы, азаматтық, әдет-ғұрып немесе діни құқық).

Материалдық құқық қылмыстың *мәніне*, мысалы, тыйым салынған әрекетті (*actus reus* - «кінәлі әрекет») және субъективті жағы (*mens rea* - «қылмыстық ниет»). Әр түрлі елдерде құқық бұзушылық құрамын құрайтын әр түрлі элементтерге негізделген әр түрлі әрекеттерді криминализациялауға басымдық берілуі мүмкін. Немесе елдер бірдей әрекеттерді қылмыстық деп санай алады, бірақ заңдар «субъективті жағы» адамдарды осындай әрекетке кінәлі ететін (яғни, қылмыстық кінәсінің дәрежесі бойынша) айырмашылығы болуы мүмкін. Осыған байланысты, мысалы, компьютерлік жүйелер мен деректерге рұқсатсыз қол жеткізуді қылмыстық жауапкершілікке тартатын заңдар болжамды қылмыскердің ниетінің дәрежесіне қарай әр елде әр түрлі болады.

Қылмыстық-құқықтық кінәнің деңгейлері (нысандары).

Әр түрлі құқықтық жүйелерде әр түрлі түсіндірілетін заңсыз әрекеттің әдейі (саналы түрде немесе қасақаналықпен) немесе әдейі емес (байқаусызда немесе абайсызда жасалған) дәрежесіне байланысты қылмыстық кінәнің (немесе қылмыстық жауапкершіліктің) әр түрлі деңгейлері бар (Maras, 2020):

Саналы түрде. Адам *зиян* келтіру мақсатымен әрекет жасаған кезде біле тұра қылмыс жасайды (яғни, адамның зиян келтіру *ниеті* бар). Мысал ретінде 1990 жылы Біріккен Корольдіктің «Компьютерлік технологияларды теріс пайдалану туралы» заңын айтуға болады, ол басқалармен қатар өзгерістер және / немесе зақым келтіруге, жүйелер мен қызметтерді бұзуға, жүйелік деректер мен бағдарламаларды өзгертуге бағытталған жүйелер мен деректерге рұқсатсыз кіруді криминализациялайды.

Әдейі. Адам өзінің іс-әрекетінің зиян келтіретінін біле тұра *қасақана* қылмыс жасайды, бірақ соған қарамастан ол мұндай әрекетке барады және зиян келтіреді. АҚШ Заңдар жинағы 18 Таруының §1030(a)(1) бойынша 1986 жылғы «Компьютерлік алаяқтық және теріс пайдалану туралы» заңға сәйкес, атап айтқанда, тұлғаға айып тағылуы мүмкін, егер ол:

қажетті рұқсатсыз компьютерге әдейі кіру немесе рұқсат етілген қол жеткізу шекарасын кесіп өту және осы әрекет арқылы Америка Құрама Штаттарының үкіметі атқарушы биліктің бұйрығымен немесе актісімен ұлттық қорғаныс немесе халықаралық қатынастар себептермен рұқсатсыз жария етуден қорғауды талап ететін ақпаратты алу қарым-қатынастар немесе кез келген алу - 1954 жылғы «Атом энергиясы туралы» заңның 11(у) бабында анықталғандай кез келген жария емес ақпаратты, егер осылайша алынған ақпарат Америка Құрама Штаттарына зиян келтіру үшін пайдаланылуы мүмкін деп санауға негіз болса немесе кез келген шет мемлекеттің пайдасына, әдейі хабардар етілсе немесе хабарлау үшін тиісті шаралар қолданылса, бағытталса немесе жіберілсе немесе құқығы жоқ кез келген тұлғаға мұндай ақпаратты хабарласа, бағыттаса, жіберсе немесе хабарлау үшін тиісті шаралар

қолданса немесе бұл ақпаратты әдейі сақтаса және оны алуға құқығы бар Америка Құрама Штаттарының лауазымды тұлғасына немесе қызметкеріне бермесе.

Абайсыздықпен (немесе жеңілтектігінен). Адам өзгелерге зиян келтірудің елеулі және негізсіз тәуекелін білсе де, іс-әрекет жасаған кезде *абайсызда* қылмыс жасайды, бірақ мұндай зиян келтіру қаупіне немқұрайлы қарайды. Австралияда адамға 2001 жылғы «Киберқылмыстылық туралы» №161 заңның 477.2(1)(c) тарауының ережелері бойынша айып тағылуы мүмкін, егер «адам деректерді рұқсатсыз өзгертудің (i) кез келген компьютерде сақталған осы немесе кез келген басқа деректерге қол жеткізуі; немесе (ii) кез келген осындай деректердің дәлдігін, қауіпсіздігін немесе қолданылымдығын бұзатынын немесе бұзуы мүмкін екендігін абайсызда түсінбесе».

Абайсызда. Абайсыздық – кінәнің ең төменгі дәрежесі. Абайсызда кез келген әрекетке баратын адамдар өздерінің мінез-құлқының теріс салдарын түсінбейді. Сенегалда «Деректер туралы» заңда белгіленген формальды талаптарды сақтамай абайсыздықпен жеке деректерді өңдейтін немесе өңдеуді ұйымдастыратын кез келген адам мұндай деректерді қолданар алдында жазаға тартылады» («Киберқылмыстылық туралы» № 2008-11 Заңы, 431-17 бап).

Бұл жерде екі нәрсені атап өту маңызды. Біріншіден, заңның жергілікті қолданылуы (қылмыстық қудалау) егер қылмыстық қудалау қоғамдық мүддеге сәйкес келсе және интернеттегі алаяқтық сияқты жаппай киберқылмыстардың үлкен саны *de minimis non-curat lex* (лат. заң ұсақ-түйекке мән бермейді) принципіне сәйкес елеусіз болып саналса ғана мүмкін болады, олар жеке түрде полициялық тергеуді немесе қылмыстық қудалауды ақтау үшін олардың салдары бойынша шамалы болып саналады. Алайда, олар халықаралық масштабта елеулі кумулятивті салдарға әкелуі мүмкін, сондықтан олар халықаралық құқыққа бағынуға тиіс. Екіншіден, «белгілі бір әрекеттерді қылмыстық деп танудың сенімді негіздемесі болмаған жағдайда, шамадан тыс қылмыстылық қаупі бар. Осыған байланысты адам құқықтары саласындағы халықаралық құқығы қылмыстық құқықты сыртқы, халықаралық стандарттарға сәйкес бағалау үшін қажетті маңызды құралдардың бірі болып табылады» (БҰҰ ЕҚБ, 2013, 60 б.).

Іс жүргізу құқығы. *Іс жүргізу құқығы* материалдық құқықты қолдану кезінде орындалуы тиіс процестер мен процедуралардың шекарасын, сондай-ақ материалдық құқықты қолдану мүмкіндігін қамтамасыз ететін нормаларды анықтайды. *Іс жүргізу құқығының* маңызды бөлігі қылмыстық сот төрелігі жүйесі мен оның қызметкерлері күдіктілерге, айыпталушыларға және сотталғандарға қалай қарау керектігі туралы кешенді ережелер мен нұсқауларды қамтитын қылмыстық іс жүргізу құқығы болып табылады. Ақырында, киберқылмыстылық туралы іс жүргізу заңнамасы юрисдикция және тергеу өкілеттіктері туралы ережелерді, деректерді жинауға, хабарламаларды ұстауға, тінту мен алып қоюға, деректерді сақтап қалу және сақтау процедураларына қатысты дәлелдемелерді және қылмыстық процесті жүргізу ережелерін қамтиды. Киберқылмыстылық процедураларға, әсіресе

юрисдикцияға, тергеулерге және цифрлық дәлелдерге қатысты кейбір ерекше қиындықтар туғызады.

Юрисдикция. Құқық қорғау органдарына киберқылмыстарды тергеу құқығы берілген, ал ұлттық соттарға киберқылмыс туралы істер бойынша тиісті мемлекеттің юрисдикциясы болған жағдайда ғана шешім шығаруға өкілеттік берілген. Юрисдикция мемлекеттің заңдарды орындау және заңдарды сақтамағаны үшін жаза қолдану құқығы мен өкілеттігін білдіреді. Юрисдикция мәселесі мемлекеттік егемендікпен тығыз байланысты, яғни, мемлекеттің өз аумағында өкілеттіктерді жүзеге асыру құқығымен (БҰҰ ЕҚБ, 2013, 61 б.). Юрисдикция әдетте географиялық аумақпен немесе *locus commissi deliciti* (қылмыс жасалған орны), мемлекет өз аумағында жасалған қылмыстарға өзінің юрисдикциясын жариялаған кезде және олардың жасалуына жауаптыларды іздегенде *(аумақтық принципі).* Киберкеңістікте географиялық шекаралар мен аумақтардың жоқтығын ескере отырып, юрисдикцияны анықтау үшін орынды пайдалану мүмкін емес. Сондықтан мемлекеттер юрисдикцияны анықтау үшін әртүрлі өзге факторларды пайдаланады (Maras, 2020) (жариялануға дайындалуда). Осы факторлардың бірі қылмыскердің азаматтығы *(мемлекетке тиесілік принцип; белсенді құқықсубъектілігі принципі).* Бұл принцип мемлекеттердің өз азаматтары өз аумағынан тыс жерде болса да, олардың азаматтарын қудалау құқығын мойындайды. Аз дәрежеде (қолданылуы тұрғысынан) жәбірленушінің азаматтығы қылмысқа қатысты юрисдикцияны белгілеу үшін қолданылуы мүмкін *(мемлекетке тиесілік принцип; пассивті құқықсубъектілігі принципі).* Мемлекет сондай-ақ басқа мемлекетте жасалған құқық бұзушылық (мысалы, мемлекетке опасыздық немесе тыңшылық) осы қылмысқа қатысты юрисдикцияға ұмтылған мемлекеттің мүдделері мен қауіпсіздігіне зиян келтірген жағдайда юрисдикцияны белгілей алады *(қорғау принципі).* Ақырында, аумағында қылмыс жасалған мемлекет кінәлілерді жауапқа тарту үшін қудалауды қаламаған немесе жасай алмаған кезде, географиялық орнына қарамастан барлық адамдарға қатысты қылмыстар болып саналатын жаппай қатыгездік (мысалы, геноцид) сияқты кейбір трансұлттық қылмыстарға кез келген мемлекет юрисдикция белгілей алады *(әмбебаптық принципі).*

Тергеу әрекеттері мен өкілеттіктері. Киберқылмыстылықтың цифрлық дәлелдемелерімен жұмыс істеу тұрғысынан да, оны сот өндірісінде пайдалану жағынан да ерекше қиындықтармен байланысты. 2013 жылы БҰҰ ЕҚБ-ның «Киберқылмыстылық проблемаларын жан-жақты зерттеу» есебінің жобасында атап өтілгендей «тергеу әрекеттерінің кейбіреулері дәстүрлі өкілеттіктер негізінде жүзеге асырылуы мүмкін болса да, кеңістіктік, объектіге бағытталған көзқарасқа негізделген көптеген процессуалдық ережелерді (сандық) деректер және нақты уақыттағы деректер ағындары сақтаумен байланысты жағдайларда қолдану қиын, сондықтан тергеу жүргізу үшін арнайы өкілеттіктер қажет (БҰҰ ЕҚБ, 2013, 60 б.). Мұндай арнайы өкілеттіктер заңмен белгіленеді және тек қажетті ақпаратқа қол жеткізуді ғана емес, сонымен қатар деректердің тиісті заң тәртібіне сәйкес алынуын және заңмен рұқсат етілген және рұқсат етілген көлемде болуын қамтамасыз ететін

кепілдіктерді қамтиды. АҚШ-тың «Сақталған хабарламалар туралы» заңы (18 титул §2701-2712), 1986 жылғы «Электрондық коммуникациялар құпиялылығы туралы» заңның II титулы болып табылады, осындай кепілдіктерді қарастырады. Мысалы, 18 титулдың § 2703(a) бойынша мемлекеттік орган электрондық байланыс жүйесінің электрондық жадында жүз сексен күннен аспайтын мерзімде сақталған сымның немесе электрондық хабарламалардың мазмұнын ашуды электрондық байланыс қызметін жеткізушіден тек Федералдық қылмыстық іс жүргізу ережелерінде сипатталған процедураларға сәйкес құзыретті юрисдикция сотымен шығарылған бұйрық негізінде ғана талап ете алады. (немесе, егер штаттың соты бұйрықты осы штаттағы сот бұйрығын шығару тәртібіне сәйкес шығарған жағдайда).

Дегенмен, бұл кепілдіктер (яғни заңды диспозицияға қойылатын талап) барлық елдерде талап етілмейді. 2014 жылы Түркия Интернет-провайдерлерден бұл деректерді алу үшін заңды бұйрықсыз (мысалы, сот бұйрығы немесе тінту ордері) қолданушы деректерін сақтап қалуды және оларды билік органдарына дереу ұсынуды талап ету үшін №5651 «Интернет туралы» заңына өзгеріс енгізді. Мұндай тергеу өкілеттіктері әдеттегі дәлелдемелерді жинау шеңберінен шығады және киберқылмыстылық істері бойынша қылмыстық сот төрелігі жүйесінің басқа мүшелерімен көмек сұрауды және байланыс орнатуды қамтиды. Жағдай Танзанияда да солай, онда 2015 жылы «Киберқылмыстылық туралы» заң полицияға киберқылмысқа қатысты шамадан тыс, шектеусіз тергеу өкілеттіктерін берді. Атап айтқанда, тінту мен дәлелдемелерді алу және деректерді жария етуге мәжбүрлеу үшін полицияның рұқсаты жалғыз талап болып табылады. Тиісінше, тінту мен алу, сондай-ақ басқа да тергеу әрекеттері тиісті заңды ұйғарымсыз жүргізілуі мүмкін. Сонымен қатар, заңдар және тергеу өкілеттіктері бастапқыда киберқылмыстың бір түріне бағытталған, кейіннен киберқылмыстылықтың басқа онша ауыр емес түрлеріне таралған кезде «мандаттың таралуы (негізгіден ауытқу)» немесе «функциялардың таралуы» қаупі бар (бұл терминдер заңдарды және/немесе басқа да шараларды бастапқы қолданылу аясынан тыс салаларға тарату жағдайларын сипаттау үшін қолданылады). Соңында, киберқылмыс пен сот ісін тергеу үшін қолданылатын өкілеттіктер мен процедуралар заңның үстемдігі мен адам құқықтары стандарттарына сәйкес келуі тиіс (мысалы, 2001 жылғы Еуропалық Кеңестің киберқылмыстылық туралы конвенциясының 15 -бабын қараңыз).

Сандық дәлелдемелерді идентификациялау, жинау, айырбастау, қолдану және қолайлылығы. Киберқылмыс саласындағы іс жүргізу заңнама цифрлық дәлелдемелердің идентификациялау, жинау, сақтау, талдау және және қолайлылығы анықтау, жинау, сақтау, талдау және айырбастау аспектілерін қамтиды. Сандық дәлелдемелерге (немесе электронды дәлелдемелерге) «компьютерлік жүйелерден немесе басқа цифрлық құрылғылардан алуға болатын және құқық бұзушылықты дәлелдеу немесе жоққа шығару үшін пайдаланылатын кез келген ақпарат» жатады (Maras, 2014). Цифрлық дәлелдемелер жәбірленушінің, куәнің және күдіктінің айғақтарын растауы

немесе теріске шығаруы, факті туралы мәлімдеменің растығын растауы немесе жоққа шығаруы, құқықбұзушының ниетін, нысанасын және орналасқан жерін анықтауы, қылмыскердің мінез-құлқын (бұрынғы әрекеттері мен мінез-құлқын) және оның қылмыстық құқықтық кінәсінің дәрежесін анықтауға мүмкіндік береді (Maras 2014; Maras, 2016).

Дәлелдемелік құқық пен қылмыстық сот өндірісінің ережелері сотта цифрлық дәлелдемелердің қолайлылығын анықтау үшін қолданылатын критерийлерді қамтиды (Maras, 2014). Олар ұлттық соттарда қолайлылығын қамтамасыз ету үшін цифрлық дәлелдемелерді құжаттандыру, жинау, сақтап қалу, беру, талдау, сақтау және қорғау процедураларын сипаттайды. Сандық дәлелдемелердің сотта қолайлығы үшін олардың аутентификациясы жүзеге асырылады және тұтастығы белгіленеді. Аутентификация процедуралары сандық дәлелдемелердің қайнар көзін/авторын анықтауды (мысалы, қайнар көзі туралы идентификациялық мәлімет) және дәлелдемелердің тұтастығын тексеруді қамтиды (мысалы, оның қандай да бір жолмен өзгертілмегеніне, өңделмегеніне немесе зақымдалмағанына көз жеткізу мақсатында). Көптеген соттарда цифрлық дәлелдердің колайлылғын қамтамасыз ету үшін дәлелдемелердің егжей-тегжейлі жазбаларын, оның жай-күйін, жинау процесін, сақтау, қол жеткізу және беру мүмкіндіктерін, қол жеткізу мен беру себептерін қамтитын *дәлелдемелерді қорғау жүйесі* маңызды болып табылады (БҰҰ ЕҚБ, 2013, 60 б.; Maras, 2014). Әр түрлі елдерде дәлелдеу құқығының әр түрлі стандарттары мен қылмыстық сот өндірісінің ережелері бар. Киберқылмыстылықпен күресу дәлелдемелер мен қылмыстық сот өндірісінің ұқсас ережелерін талап етеді, өйткені қылмыстың бұл түрі шекараны білмейді және Интернет байланысы арқылы әлемнің кез келген жеріндегі цифрлық дәлелдер мен жүйелерге әсер етеді.

Алдын алу құқығы. Алдын алу құқығы құқық бұзушылықтарды реттеуге және олардын тәуекелдерін азайтуға негізделген. Киберқылмыстылық контекстісінде профилактикалық заңнаманың мақсаты не киберқылмыстардың алдын алу, не ең аз дегенде киберқылмыспен келтірілген залалды жұмсарту болып табылады (БҰҰ ЕҚБ, 2013, 61 б.). «Деректерді қорғау туралы» заңдар (мысалы 2016 жылғы ЕО Деректерді қорғау туралы жалпы ережелері және 2014 жылғы Африка одағының киберқауіпсіздік және жеке деректерді қорғау туралы Конвенциясы және киберқауіпсіздік туралы заңдар (мысалы, 2017 жылғы «Украинаның киберқауіпсіздігін қамтамасыз етудің негізгі қағидалары туралы» Украина Заңы) жеке деректердің таралуына байланысты киберқылмыстар нәтижесінде материалдық залалды азайту және/немесе азаматтардың киберқылмыстарға осалдығын азайту мақсатында қабылданды. Басқа заңдар қылмыстық сот төрелігі қызметкерлеріне мұндай әрекеттерді жеңілдету үшін қажетті құралдарды, шаралар мен рәсімдерді қосу арқылы киберқылмысты анықтауға, тергеуге және қудалауды жүзеге асыруға мүмкіндік береді (мысалы, байланыс пен деректерді сақтауға мүмкіндік беретін телекоммуникация мен электронды байланыс қызметтерін жеткізушілердің инфрақұрылымы). Америка Құрама Штаттарында 1994 ж. «Байланысты қамтамасыз етуге әрекеттесу туралы» Заң

(CALEA) (47 титулда, §1001-1010 кодификацияланған) телефондық байланыс провайдерлер мен жабдық өндірушілерінен олардың қызметтері мен өнімдері заңды рұқсаты бар билік органдарына (мысалы, тиісті сот ордері), байланыс желілеріне қол жеткізу мүмкіндігін қамтамасыз ету үшін шаралар қабылдауды міндеттейді.

2. Заңнаманы унификациялау.

Киберқылмыстылықпен күрес Интернеттен тыс жасалған құқық бұзушылықтарды қамтитын қолданыстағы заңдарды қолдану, киберқылмыспен байланысты ережелерді қамтитын заңдарға түзетулер енгізу және киберқылмыспен күресуге арнайы бағытталған заңдарды қабылдау арқылы жүзеге асырылуы мүмкін (және жүзеге асырылады). Алайда, қолданыстағы заңдар киберқылмыстылыққа қолданылмауы мүмкін, себебі олар Интернет пен цифрлық технологиялар пайда болғанға дейін және/немесе Интернет пен цифрлық технологияларды ескермей қабылданған болуы мүмкін. Сондықтан киберқылмыспен байланысты емес қылмыстармен күресуге арналған заңдар ақпараттық-коммуникациялық технологияларды (АКТ) қылмыстың субъектісі немесе құралы ретінде пайдаланатын киберқылмыскерлер мен әрекеттері қылмыс жасаудың субъектісі немесе құралы ретінде ақпараттық-коммуникациялық технологиялармен (АКТ) байланысты басқа да қылмыскерлерге шектеулі әсер етуі мүмкін. Осыған байланысты киберқылмысқа қатысты арнайы заңдарды қабылдау қажет болуы мүмкін. Киберқылмыстылық туралы заңдарды қабылдау қажет пе, «бөлек әрекеттердің сипатына және ұлттық заңнаманың ауқымы мен түсіндірілуіне байланысты» (БҰҰ ЕҚБ, 2013 ж., 52 б.).

«Құрбанды ренжіту, қорлау және/немесе басқа сипаттағы зиян келтіру» үшін (Maras, 2016, p. 255), «тиісті өзара келісімсіз жақын немесе жыныстық сипаттағы бейнелерді жасауды, таратуды және тарату қаупін төндіруді» көздейтін киберкеңістіктегі қудалаудың бір түрі болып табылатын суретты пайдаланумен байланысты жыныстық зорлық-зомбылықтың (ауызша сөйлеуде «порно кегі» деп аталады) 2013 жылғы оқиғасын қарастырсақ (Henry, Flynn and Powell, 2018, p. 566), осындай қорлауды жасаған адам Нью-Йорктің қолданыстағы заңдары бойынша қылмыстық жауапкершілікке тартылмады. Атап айтқанда, қылмыскер өзінің құрбысының жалаңаш суреттерін (оқиға болған уақыттағы) Twitter-де жариялады және бұл фотосуреттерді өзінің құрбысының әпкесі мен жұмыс берушісіне электронды пошта арқылы жіберді. Оған қарсы айып тағылды, оның ішінде ауырлататын мән-жайлармен екінші дәрежедегі алымсақтық айыбы болды. Нью-Йорк штатының Қылмыстық заңының 240.30(1)(a) бабына сәйкес, «егер адам басқа адамды қудалау, қауып төндіру немесе қорқыту мақсатында телефонмен, телеграфпен немесе электрондық пошта арқылы немесе жасырын түрде немесе қорқыныш тудыруы мүмкін кез келген басқа байланыс түрлерін қолданса, ол ауырлататын мән-жайлармен екінші дәрежедегі алымсақтық жасалуында кінәлі болып танылады». Бұл заң жәбірленуші мен қылмыскер арасындағы тікелей байланысқа қатысты болғандықтан, People v. Barber (2014) істі қараған сот сотталушының әрекеті (яғни, құрбысының әпкесі мен жұмыс берушісіне

досының жалаңаш суреттерін электронды түрде жіберу және бұл фотоларды Twitter-ге орналастыру) екінші дәрежелі алымсақтыққа жатпайды деп қаулы етті. Заңның интернет кеңістігінде шектеулі қолданылуының бұл мысалы жалғыз ғана емес. 2013 жылы БҰҰ ЕҚБ-ның «Киберқылмыстылық проблемаларын жан-жақты зерттеу» есебінің жобасында айтылғандай, «көптеген жалпы құқықтың дәстүрлі заңдар киберқылмыс пен жасау барысында электрондық дәлелдемелері бар қылмыстарды жасау үшін қолданылатын ақпарат пен ақпараттық технологиялардың ерекшеліктерін ескертпейді».

3. Халықаралық және аймақтық құқықтық құжаттар.

Киберқылмыстылықпен күресте халықаралық және аймақтық шарттар бар. Мысал ретінде 2001 жылы Еуропа Кеңесінің киберқылмыстылық туралы конвенциясын айтуға болады. Бұл конвенцияның мақсаты ұлттық заңнаманы біріздендіру, киберқылмыстарды тергеу әдістерін жетілдіру және халықаралық ынтымақтастықты кеңейту болып табылады. Ол сондай-ақ киберқылмыспен күресу үшін ұлттық деңгейде қабылданатын шаралар туралы конвенцияға қатысушы мемлекеттерге материалдық құқыққа (мысалы, қылмыстық заңнамаға киберқылмыс байланысты құқықбұзушылықтар үшін жауапкершілікті еңгізу) және қылмыстық іс жүргізу құқығына өзгерістер мен толықтыруларды қоса алғанда (мысалы, қылмыстық тергеу мен сот қудалаудың жүзеге асыру тәртібін белгілеу) қатысты нұсқаулық береді. Конвенция сонымен қатар қатысушы мемлекеттерге өзара көмек туралы нұсқаулар береді және көмек сұрайтын елмен ұқсас келісімі жоқ елдер үшін *өзара құқықтық көмек туралы шарт ретінде қызмет етеді* (яғни, екі жақтың ұлттық заңнамасында белгіленген кейбір және/немесе барлық қылмыстарды тергеу мен қудалау бойынша ынтымақтастық туралы елдер арасындағы келісім; Maras, 2016).

Киберқылмыстылыққа қарсы күрес саласында бірнеше аймақтық сипаттағы келісімдер бар.

2001 жылғы Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттер қол қойған Компьютерлік ақпарат саласындағы қылмысқа қарсы күрес жөніндегі ынтымақтастық туралы Келісім. Бұл келісім мемлекеттерді келісім ережелерін жүзеге асыру үшін ұлттық заңдарды қабылдауға және киберқылмыстылыққа қарсы ұлттық заңнаманы біріздендіруге шақырады.

2010 жылы кабылданған Араб мемлекеттері лигасы Ақпараттық технологиялар саласындағы қылмыстармен күрес туралы Конвенциясы. Бұл конвенцияның негізгі мақсаты - киберқылмыстылықтан өз меншігін, халқы мен мүдделерін қорғауға мүмкіндікті қамтамасыз ету үшін мемлекеттер арасындағы ынтымақтастықты нығайту.

2010 жылы Шанхай ынтымақтастық ұйымы қабылдаған Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы Келісім. Бұл келісімнің күші киберқылмыстылық пен киберқауіпсіздік шеңберінен шығып, келісімнің негізгі мақсаттарының бірі ретінде қатысушы мемлекеттердің ақпараттық қауіпсіздігін қамтамасыз ету шараларын, сондай-ақ ақпараттық жүйелер мен олардың мазмұнын ұлттық бақылау шараларын

қамтиды.

2014 жылғы киберқауіпсіздік және жеке деректерді қорғау туралы Африка одағының конвенциясы. Бұл конвенция басқа ережелермен қатар, киберқылмыстылықпен тиімді күресуге, ұлттық заңдарды қабылдауға және/немесе қолданыстағы ұлттық заңдарға өзгерістер енгізуге, ұлттық заңнамаларды біріздендіруге, өзара құқықтық көмек көрсету туралы шарттар жасасуға (ӨҚКШ), егер олар әлі жасалмаған болса, мемлекеттер арасында ақпарат алмасуға ықпал етуге, аймақтық, үкіметаралық және халықаралық ынтымақтастыққа әрекеттесуге және басқа мемлекеттермен, тіпті жеке сектормен ынтымақтастық үшін қолда бар құралдарды пайдалануға Африка Одағының мемлекеттеріне үндеуді қамтиды.

Сонымен қатар, аймақтық ұйымдармен және/немесе аймақтық үкіметаралық ұйымдармен киберқылмыстылықпен күресу саласындағы заңдар мен директивалар әзірленді және имплементацияланды. Мысалға:

2012 жылғы Оңтүстік Африка даму қоғамдастығының (ОАДҚ) «Компьютерлік қылмыстар мен киберқылмыстылық туралы» Үлгілік заңы. Бұл заң ОАДҚ-ға мүше мемлекеттер үшін киберқылмыстылықпен күрес саласындағы материалдық және процессуалдық құқықты әзірлеу үшін басшылық болып табылады. Бұл заң үлгілік болғандықтан, мемлекеттерге ынтымақтастық орнатуға қатысты ешқандай заңды міндеттемелер жүктемейді. ОАДҚ-нің Қылмыстық істер бойынша өзара құқықтық көмек туралы Хаттамасы мен Экстрадиция туралы Хаттамасын киберқылмыстар бойынша халықаралық тергеулерде ынтымақтастыққа және үйлестіруге ықпал ету үшін киберқылмыстылық туралы заңдары жоқ және/немесе ондай заңдарды әзірлемейтін мемлекеттер пайдалана алады.

2011 жылғы Батыс Африка мемлекеттерінің экономикалық қоғамдастығының (АМЭҚ) Киберқылмыстылық туралы директивасы. Бұл директива қатысушы мемлекеттерден киберқылмыстылықты ұлттық заңнамада криминализациялауды талап етеді және киберқылмыстылық пен киберқауіпсіздікке қатысты істерде өзара құқықтық көмекке, ынтымақтастық пен экстрадицияға ықпал етеді. Киберқылмыстарды тергеу мен киберқылмыскерлерді ұстап беруде ынтымақтастықты ықпал ету мақсатында АМЭҚ Қылмыстық істер бойынша өзара көмек туралы Конвенция мен Ұстап беру туралы Конвенциясын қабылдады.

4. Адам құқықтары саласындағы халықаралық құқық және киберқылмыстиылық туралы заңнама.

Кейбір киберқылмыстар туралы заңдардың негізгі ережелері, әсіресе билікті құрметтемеу, қорлау, мемлекет басшысының диффамациясы, ұятсыздық немесе порнографиялық материалдар сияқты интернеттегі контентке қатысты ережелер белгілі бір адам құқықтарын жүзеге асыруды тым шектеуі мүмкін. Сонымен қатар, киберқылмыстылық туралы заңдардың процессуалдық нормалары киберқылмыстарды тергеу кезінде хабарламаларды ұстау мен электронды бақылауды жүзеге асыратын құралдар мен әдістердің қолданылуын мүмкіндігін қамтамасыз етін жеке өмірге қол сұқбау құқығы сияқты адам құқықтарын жүзеге асыруда мүмкіншіліктерін

қажетсіз шектеулерге де әкелуі мүмкін (БҰҰ ЕҚБ, 2013, 136 б.). Киберқылмыспен күресу мен адам құқықтарын құрметтеу арасындағы тепе-теңдікті сақтау қажет.

Адам құқықтары саласындағы халықаралық заңнама ерекше жағдайларда заңды түрде шектелуі мүмкін белгілі бір адам құқықтарын жүзеге асыруға шектеулер енгізуге мүмкіндік береді (кейбір құқықтар шектелмеуі мүмкін). Бұл шектеулер олар орындалған кезде жарамды *заңды мақсат, қолданыстағы заңға сәйкес* және *қауіпке қажетті* және *пропорционалды,* бұл олардың қолданылуын ақтайды. Заңды мақсаттардың нақты ауқымы қолданылатын адам құқықтарына байланысты және қоғамдық қауіпсіздік, ұлттық қауіпсіздік, экономикалық қауіпсіздік, денсаулықты қорғау, адамгершілік мүдделерін және басқалардың құқықтарын қорғалуын қамтуы мүмкін. Жоғарыда аталған заңды мақсаттардың біріне жету үшін шектеулер енгізу қажеттілігінен басқа, шектеу ұлттық заңнама негізінде енгізілуі тиіс. Бұл заң азаматтарға олардың мінез-құлқын дұрыс бақылауға, осы заңды қолдану кезінде биліктің өкілеттіктерін, сондай-ақ оны орындамаудың салдарын білуі үшін қол жетімді болуы керек. Заң нақты тұжырымдалуы тиіс және мемлекеттік билік органдарына шектеулерді қолдану кезінде шектеусіз іс-әрекет еркіндігін беруге жол бермеуі тиіс. «Ұлттық қауіпсіздік», «экстремизм» немесе «терроризм» туралы нақты емес сілтемелер сияқты түсініксіз және тым кең ақтау нақты тұжырымдалған заңдарды анықтауға жарамайды. «Қажет» сөзі шектеу «мақсатқа сай», «ақылға қонымды» немесе «қажет» дегеннен артық болуы керек дегенді білдіреді. (АҚЕС, «Санди Таймстың» Ұлыбританияға қарсы ісі, 1979 жылғы 26 сәуірдегі сот қаулысы, 59-тармақ). Сонымен қатар, мемлекет көздеген заңды мақсат пен мемлекеттің осы заңды мақсатқа жету әрекеттері арасында тиісті байланыс болуы керек. Басқаша айтқанда, әрекеттер қорғалатын мүдделерге сәйкес болуы керек. Бұдан шығатыны, шектеу басқа шаралармен салыстырғанда ең аз интрузивті шара болып табылады, оның көмегімен қажетті нәтижеге қол жеткізуге болады. Мемлекеттер адам құқықтары саласындағы халықаралық заңнама шеңберінде қабылданған өз міндеттемелерін орындау кезінде белгілі бір іс-қимыл еркіндігін пайдаланады (***өз қалауы бойынша еркіндік).***

Оның үстіне, тіпті кейбір құқықтар сөз бостандығы немесе пікірін айту бостандығы құқығын жүзеге асыруға кедергі келтіруі мүмкін, мысалы, азаптаудан және басқа да қатыгез, адамгершілікке жатпайтын немесе қадір - қасиетін қорлайтын қарым-қатынастан бос болу құқығы және жеке өмірге қол сұғылмау құқығы, кемсітушіліктен бос болу құқығы және балалардың ерекше қорғалу құқығы.

Талқылауға арналған сұрақтар:

1. Қорлау жасалған әрекетке сәйкес келетін шара ма?
2. Киберқылмыстылық туралы ұлттық заңдардың болмауының салдары қандай?
3. Бүгін мұндай жағдай болуы мүмкін басқа елдер бар ма?

4 Тақырып. Сандық криминалистикаға кіріспе.

1. Сандық дәлелдемелер. Сандық криминалистика Эдмонд Локар принципіне негізделген, ол бойынша объектілер мен беттер бір-бірімен жанасқанда, бір-бірімен қиылысады, материалдар айқас түрі көшіруге ұшырайды (Maras and Miranda, 2014, pp. 2-3). Сандық криминалистика контекстінде адамдар ақпараттық-коммуникациялық технологияларды (АКТ) қолданғаннан кейін цифрлық із қалдырады. Атап айтқанда, АКТ қолданатын адам сандық іздерін қалдыра алады, яғни АКТ қолданушылары қалдырған деректер, олар туралы ақпаратты ашуы мүмкін, оның ішінде жасын, жынысын, нәсілін және этникалық тиесілілігін, азаматтығын, жыныстық бейімділігін, ойларын, қалауларын, әдетін, хоббиін, медициналық тарихы мен денсаулығындағы проблемаларын, психологиялық бұзылуларын, жұмыспен қамтулығын, кез келген қауымдастыққа тиесілілігін, қарым-қатынасын, геолокациясын, күн тәртібін және басқа белсенділіктерін қоса алғанда. Мұндай сандық іздері белсенді немесе пассивті болуы мүмкін.

Белсенді цифрлық із қолданбаларда, веб-сайттарда, хабарлар тақталарында, әлеуметтік желілерде және басқа онлайн форумдарда жарияланған жеке ақпарат, бейнелер, кескіндер және түсініктемелер сияқты пайдаланушы берген деректер арқылы жасалады.

Пассивті сандық іздер - бұл Интернет пен цифрлық технологияларды қолданатын адамдар байқаусызда қалдыратын деректер (мысалы, браузерде шолу тарихы). Белсенді және пассивті цифрлық іздерінің бөлігі болып табылатын деректер қылмыстың, соның ішінде киберқылмыстың дәлелдемесі ретінде пайдаланылуы мүмкін (яғни, цифрлық дәлелдемелер ретінде). Мұндай мәліметтер оқиғаны растау немесе жоққа шығару, жәбірленушінің, куә мен күдіктінің айғақтарын растау немесе теріске шығару, және/немесе күдіктінің қылмыс жасауға қатыстылығын немесе қатыс еместігін анықтау үшін де қолданыла алады. Деректер сандық құрылғыларда (мысалы, компьютерлер, смартфондар, планшеттер, телефондар, принтерлер, «ақылды» телевизорлар (Smart TV) және сандық жады бар кез келген басқа құрылғылар), сыртқы жад құрылғыларында (мысалы, сыртқы қатты дискілер мен USB флэш-жинақтауыштар), желілік компоненттер мен құрылғыларда (мысалы, маршрутизаторлар), серверлер және деректерді бұлтты сақтауыштарда (мұнда деректер «әртүрлі географиялық орындардағы бірнеше деректер орталықтарында» сақталғандықтан; БҰҰ ЕҚБ, 2013, 26 б.) сақталады. Алынған мәліметтер контентке қатысты деректер болуы мүмкін (мысалы, жазбаша хабарламалардағы сөздер немесе аудиофайлдардағы айтылатын сөздер; мысалы, бейнелер, электрондық хаттардың мәтіні, мәтіндік хабарлар, жедел хабарлар және әлеуметтік желі мазмұны) және контентпен байланысты емес деректер немесе метадеректер (яғни мазмұн туралы деректер; мысалы, пайдаланушылардың жеке басы мен орны және телекоммуникациялар мен электрондық хабарламаларды жіберушілер мен алушылар туралы ақпарат сияқты операциялар туралы деректер).

Онлайн режимінде алынған және/немесе сандық құрылғылардан шығарылған деректер пайдаланушылар мен оқиғалар туралы ақпараттың

үлкен көлемін қамтуы мүмкін. Мысалы, дербес компьютерлер сияқты жұмыс істейтін құрылғы пайдаланушылары туралы жеке ақпаратты сақтайтын ойын қосымшалары (мысалы, электрондық пошталардың аттаулары мен мекенжайлары), қаржылық ақпараттар (мысалы, несие картаның деректері), Интернетті қарау тарихы туралы ақпарат (мысалы, кірілген веб-сайттар туралы), бейнелер бейнежазулар және басқа деректер. Ойын қосымшаларынан алынған деректер балаларды жыныстық пайдалану және балаларға жыныстық зорлық-зомбылық материалдарын Интернетте орналастыруға байланысты істерді тергеу барысында пайдаланылды (Read et al., 2016; Conrad, Dorn, and Craiger, 2010).

Пайдаланушылар туралы деректердің айтарлықтай көлемін жинақтайтын тағы бір сандық құрылғы - Amazon Echo (Alexa дауыстық көмекшісі бар). Бұл құрылғы жинаған деректерде пайдаланушылар/иелер туралы олардың қызығушылықтары, қалауы, сұраулары, сатып алулары және белсенділігінің басқа түрлері туралы ақпарат, сондай-ақ олардың орналасқан жері туралы ақпарат болуы мүмкін (мысалы, олардың Alexa дауыстық көмекшісімен уақыт таңбаларын мен аудио жазбаларын өзара әрекеттесуін қарау арқылы үйде немесе үйінен тыс жерде екенін анықтау үшін). Amazon Echo-дан алынған деректер Америка Құрама Штаттарында кісі өлтіру тергеуінде қолданылды. Ақырында күдіктіге тағылған айып алынып тасталғанымен, бұл іс жаңа цифрлық технологияларды қолдану арқылы жиналған мәліметтер міндетті түрде дәлел ретінде сотқа ұсынылатынын айқын көрсетті. Деректер жедел іздестіру мәліметтерін табылуы және пайдаланылуы мүмкін (қосымша ақпарат алу үшін UNODC 2011 Criminal Intelligence Manual for Analysts (БҰҰ ЕҚБ, 2011 жыл, «Қылмыстық қызмет туралы оперативтік ақпарат: талдаушыларға арналған құрал» қараңыз) және/немесе сотқа цифрлық дәлел ретінде ұсынылуы мүмкін. Соңғы жағдайда цифрлық дәлелдемелер «оқиғаны анықтау» арқылы немесе осы оқиғаның ақиқаты туралы қорытынды шығару» арқылы тікелей дәлелдемелер болуы мүмкін (Maras, 2014, pp. 40-41).

Келесі гипотетикалық жағдайды қарастырайық: Twitter есептік жазба атынан нәсілшілдік мазмұнды материал (А есептік жазбасы). А есептік жазбасында нәсілшілдік материалдарды жариялауға пайдалану фактісі тікелей дәлелдеме болады. Материалдың есептік жазбаның иесімен орналастырылу фактісі жанама дәлелдеме болып табылады. Есептік жазбаның иесінің бұл материалды жариялағанын растау үшін қосымша растайтын дәлелдер қажет. Цифрлық дәлелдемелер сотта тікелей немесе жанама дәлел ретінде ұсынылмас бұрын, оның аутентификациясы жүргізілу керек (яғни, дәлелдеменің мақсатына сай екендігі көрсетілуі керек). Аутентификация тәжірибесін көрсету үшін цифрлық дәлелдердің келесі жалпы санаттарын қарастырайық: бір немесе бірнеше тұлғалармен генерацияланатын контент (мысалы, мәтін, электрондық хат немесе жедел хабарлама мен Microsoft Word сияқты мәтінді өңдеу құжаттары); мысалы Біріккен Корольдікте заттай дәлелдемелердің бірі болып табылатын қолданушының қатысуысыз компьютер немесе цифрлық құрылғымен генерацияланған контент (мысалы,

деректерді тіркеу журналдары), мысалы, , заттай дәлелдеудің бір түрі болып саналады (Regina (O) v. Coventry Magistrates Court, 2004 істі қараңыз); және пайдаланушымен де құрылғымен де генерацияланған контент (мысалы, пайдаланушы енгізетін және бағдарлама орындайтын есептеулерді қамтитын Microsoft Excel сияқты бағдарламалардағы электрондық кестелер). Пайдаланушы генерациялаған контент, егер ол сенімді және шынайы болса, жарамды дәлел ретінде қарастырылуы мүмкін (яғни, оның кез-келген адамға тиесілі екенін анықтауға болады). Егер құрылғы деректерді генерациялау кезінде дұрыс жұмыс істеп тұрғаны дәлелденсе және сол уақытта деректерді өзгертуге жол бермеуін қамтамасыз ететін механизмдердің жұмыс істегенін көрсетуге болатын болса, құрылғымен генерацияланған контент жарамды дәлел ретінде есептеледі. Контентты құрылғы мен пайдаланушы бір мезгілде генерациялаған жағдайда, олардың әрқайсысының сенімділігі мен шынайылығын анықтау қажет.

Дәстүрлі дәлелдемелермен салыстырғанда (мысалы, қағаз құжаттар, қару-жарақ, басқарылатын заттар және т.б.), аутентификациялау кезде сандық дәлелдемелер қол жетімді деректердің көлемі мен жылдамтылығынан (яғни, олардың жасау немесе басқаға жіберу кезіндегі жылдамтылығы), тұрақсыздығынан (яғни, олар қайта жазу немесе жою кезінде тез жоғалып кетуі мүмкін), осалдықтарынан (яғни оларды оңай өңдеуге, өзгертуге немесе бүлдіруге болады) бірегей қиындықтар тудырады. Кейбір елдер сандық дәлелдемелерге арнайы қатысты аутентификация талаптарын қамтитын дәлелдеу ережелерін енгізгенімен, басқа елдер дәстүрлі дәлелдер мен цифрлық дәлелдерді аутентификациялау үшін ұқсас талаптарды пайдаланады. Мысалы, Францияда құжаттарды шығарушының жеке басын және құжаттардың тұтастығын тексеру арқылы қағаз және электронды құжаттардың түпнұсқалығы расталуы тиіс. Құжаттардың тұтастығын тексеру тек олардың дұрыстығын тексеру ғана емес, сонымен бірге уақыт өте келе дәлдікті (яғни дәйектілікті) сақтау мүмкіндігін де білдіреді. Сонымен қатар, сандық емес және сандық дәлелдемелермен жұмыс істеу режимдерін біріздендіру үшін Сингапур сандық емес және сандық дәлелдемелер үшін бірдей аутентификация тәжірибесін қамтамасыз ету үшін 2012 жылғы «Дәлелдемелер туралы» Заңды (түзетулерімен) қабылдау арқылы дәлелдемелік құқық нормаларына түзетулер енгізді.

Сандық дәлелдердің түпнұсқалығын анықтаумен қатар, көптеген елдер алынған дәлелдеменің ең жақсы дәлел (яғни шынайы дәлел немесе шынайы дәлелдеменің дәл көшірмесі) екендігіне және/немесе басқа адамдардың сөздерінен (яғни соттан тыс мәлімдемелер) айғақтарға тыйым салу талаптарынан тыс жағдайларға сәйкес рұқсат етілуі мүмкін екендігіне баға береді. Мысал ретінде Танзанияны (1967 жылғы «Дәлелдемелер туралы» Заң, 2007 жылғы «Жазбаша заңдар туралы» Заң (әр түрлі түзетулермен) және 2015 жылғы «Электрондық операциялар туралы» Заң); Белиз (2011 жылғы «Электрондық дәлелдемелер туралы» Заң); Индонезия (2008 жылғы № 11 «Электрондық ақпарат және операциялар туралы және 2012 жылғы Үкіметтің № 82 Қаулысы); Малайзия (1950 жылғы «Дәлелдемелер туралы» Заң);

Үндістан (2000 жылғы «Ақпараттық технологиялар туралы» Заң); Сингапур (2012 жылғы «Дәлелдемелер туралы Заң» (түзетулермен) және басқа елдер. Сонымен қатар, сандық дәлелдемелердің түпнұсқалығын бағалау деректердің қандай-да бір жолмен өзгертілмегеніне көз жеткізу үшін сандық дәлелдемелерді жинау, алу, сақтау және талдау үшін қолданылатын процестерді, әдістер мен құралдарды зерттеуді де қамтиды.

2. Сандық криминалистика. Сандық сот сараптамасы процесі мыналарды қамтиды: сандық дәлелдемелерді іздеу, алу, сақтап қалу және сақтау; сандық дәлелдемелерді сипаттау, түсіндіру және олардың шығу тегі мен маңыздылығын анықтау; дәлелдемелерді және олардың сенімділігі, негізділігі және іске қатысы барлығын талдау; іске қатысты дәлелдемелерді ұсыну (Maras, 2014). Сандық криминалистиканың әртүрлі әдістемелері әзірленіп, қабылданды.

2001 жылы «Digital Forensic Research Workshop», «коммерциялық емес ерікті ұйым,... техникалық жұмыс топтарының қызметін қаржыландыруға, жыл сайынғы конференциялар өткізуге және ғылыми-зерттеу бағыттарын анықтауға көмектесу үшін бірқатар мәселелерді шешуге мамандандырылған», Америка Құрама Штаттарының Федералды тергеу бюросының хаттамасына негізделген, қылмыстың физикалық орнында тінту жүргізуге арналған модель жасады, оған жеті кезең кіреді: сәйкестендіру, сақтау, жинау, зерттеу, талдау және дәлелдемелерді ұсыну және шешім қабылдау.

2002 жылы сандық сот-медициналық зерттеулердің тағы бір моделі ұсынылды, ол 2001 жылғы «Digital Forensic Research Workshop» моделіне және Америка Құрама Штаттарының Федералды тергеу бюросының қылмыс орнында тінту жүргізу туралы хаттамасына негізделген.

Бұл модель («Сандық криминалистиканың дерексіз моделі») тоғыз кезеңнен тұрады:

1. Сәйкестендіру (яғни, оқиғаны белгілері бойынша тану және оның түрін анықтау);

2. Дайындау (яғни «тінту құралдарын, әдістерін, ордерлерін дайындау және рұқсаттарды алу және басшылықтың қолдауын алу процесінің мониторингі»);

3. Тәсіл стратегиясы (яғни «жәбірленушіге әсер етуді барынша азайту кезінде мінсіз дәлелдемелердің барынша көп көлемін жинау мақсатында пайдаланылатын рәсімді әзірлеу»);

4. Сақтау (яғни, «заттай және цифрлық дәлелдемелердің жай-күйін оқшаулау, қорғау және сақтау»);

5. Жинау (яғни, «қылмыстың нақты орнын тексеру хаттамасын жасау және стандартталған және бекітілген процедураларды қолдана отырып, сандық дәлелдемелерді қайталау»);

6. Зерттеу (яғни, «болжалды қылмысқа қатысты дәлелдемелерді терең жүйелі іздеу»);

7. Талдау (яғни «маңыздылығын анықтау, деректер үзінділерін қалпына келтіру және табылған дәлелдемелер негізінде қорытынды шығару»);

8. Ұсыну (яғни «қорытындылардың қысқаша мазмұны және

түсіндірмесі»);

9. Дәлелдемелерді қайтару (яғни «физикалық және сандық мүлікті заңды иесіне қайтару»).

2006 жылы АҚШ стандарттар және технологиялар Ұлттық институты инциденттерге әрекет ету жоспарларына криминалистикалық әдістердің интеграциялануы бойынша өзінің Басшылығында төрт кезеңнен тұратын сандық криминалистика моделін ұсынды: дәлелдемелер жинау кезеңі, ол қылмыс орнында дәлелдемелерді анықтауды, таңбалауды, құжаттауды және соңында дәлелдемелерді жинауды қамтиды; тиісті сандық дәлелдер алу және олардың тұтастығын сақтау үшін қолданылатын тиісті криминалистикалық құралдар мен әдістер анықталған зерттеу кезеңі; алынған дәлелдемелер олардың практикалық жарамдылығы мен іске қолданылуын анықтау үшін бағаланатын талдау кезеңі; және сандық криминалистика процесінде орындалған іс-әрекеттерді сипаттауды және нәтижелерді ұсынуды қамтитын есеп беру кезеңі.

Тергеудің тағы бір моделін 2001 жылы АҚШ Әділет департаментінің Ұлттық Әділет институты (NIJ) ұсынды және 2008 жылы қайта қаралды. Атап айтқанда, NIJ құралында қылмыстың физикалық орнындағы қоршау және қылмыс орнын бағалау (мысалы, іске қатысты ықтимал сандық дәлелдемелері бар құрылғыларды анықтау үшін), қылмыс орнын құжаттау, тиісті құрылғыларды алу, орау, тасымалдау және соңында осы құрылғылардың сақталуын қамтамасыз ету сияқты әрекеттерге назар аударылады.

Жоғарыда аталған модельдер әр қылмыс пен киберқылмысты тергеу кезінде барлық кезеңдер толық аяқталуы керек деген болжамдарға негізделген

. Алайда, іс жүзінде бұл әрдайым бола бермейді.

Деректерді жинақтайтын, сақтайтын және беретін деректердің көлемі мен сандық құрылғылардың саны геометриялық түрде өсетіндіктен, бұл белгілі бір типтегі сандық құрылғыларға қатысты қылмыстық істердің көбеюіне әкеледі, әр сандық құрылғыны мұқият тексеру іс жүзінде мүмкін емес деп танылады. Кейси, Феррaро және Нгуен атап өткендей, «аз сандық криминалистика зертханалары әлі де әр ақпарат тасымалдаушысының көшірмесін жасай алады және осы ақпарат құралдарындағы барлық деректерге терең сот сараптамасын жүргізе алады... Әрбір жеке ақпарат тасымалдаушысын талдаудың аяқталуын күту мағынасы жоқ, егер олардың кейбіреулері дәлелді құндылығы бар деректерді алуға мүмкіндік берсе» (Casey, Ferraro, and Nguyen, 2009, p.1353).

Осыған байланысты осы мәселені ескеретін сандық криминалистика процестерінің модельдері жасалды. Мысалы, сандық дәлелдерді сәйкестендіруді, талдауды және түсіндіруді қысқа мерзімде зертханаға терең зерттеу немесе сот-сараптамалық талдау үшін толық кескін жасау үшін жүйені (лерді)/тасымалдаушыларды тасымалдау қажеттілігінсіз қамтамасыз ету мақсатында сол жерде сот сараптамасын жүргізуге негізделген жергілікті деректерді киберкриминалистік сұрыптау процесінің (CFFTPM) моделі.

Осы модельге сүйене отырып, Кейси, Феррaро және Нгуен (Casey, Ferraro, and Nguyen, 2009) «сот сараптамасының үш деңгейін» ұсынды, оларды

жергілікті жерлерде немесе зертханада қолдануға болады:

1. Тексеру/сұрыптау негізінде сот-сараптамалық тексеру. Мұндай тексеру дәлелдемелердің ықтимал көздерін жылдам зерделеу және олар болуы мүмкін дәлелдемелердің маңыздылығы мен осы дәлелдемелердің өзгермелілігі негізінде одан әрі зерттеу үшін басым көздерді айқындау мақсатында жүргізіледі.

2. Алдын ала сот сараптамасы. Болжамды қылмыстың тікелей, жанама немесе басқа растайтын дәлелдерін алу үшін тергеуде қолданылуы мүмкін ақпаратты анықтау үшін тексеру/сұрыптау негізінде сот сараптамасы сатысында таңдалған көздердің сандық сот сараптамасын тездету үшін алдын-ала сот сараптамасы жүргізіледі (Casey, Ferraro, and Nguyen, 2009, pp. 1353, 1356-1359). Осы тексеру кезінде сот сараптамасы үшін артефактілерді (яғни, сандық сот сараптамасына әсер етуі мүмкін деректерді) анықтай алмау, олардың назардан тыс қалуы нәтижесінде пайда болуы мүмкін, терең сот сараптамасы жүргізілмейтінін автоматты түрде білдірмейді (бұл нақты іске және сараптама жүргізетін адамдардың саясаты мен рәсімдеріне байланысты).

3. Терең сот сараптамасы. Дәлелдемелердің барлық көздері зерттелуде. Мұндай түрдегі сараптама көбінесе «дәлелдемелерді жоюға күдік болған кезде, қосымша сұрақтар туындаған кезде және істің сотта қаралуы жақындаған кезде» жасалады (Casey, Ferraro, and Nguyen, 2009, p. 1359). Қазіргі уақытта әр модельдің және оның компоненттерінің өміршеңдігі мен өзектілігі туралы пікірталастар жалғасуда. Шындық мынада, әр ел сандық криминалистика саласындағы өзінің стандарттарын, хаттамалары мен процедураларын ұстанады. Алайда, бұл процестердегі айырмашылықтар құқық қорғау органдарының тергеулеріндегі халықаралық ынтымақтастыққа кедергі келтіреді.

3. Сандық криминалистика саласындағы стандарттар мен озық практикалық әдістер. Халықаралық стандарттау бойынша ұйымы (ХСҰ), халықаралық үкіметтік емес ұйым және Халықаралық электротехникалық комиссия (ХЭК), халықаралық коммерциялық емес ұйым әр түрлі елдерде қолданылатын тәжірибені біріздендіру үшін халықаралық стандарттарды әзірлейді және жариялайды. 2012 жылы Халықаралық стандарттау бойынша ұйымы (ХСҰ) және Халықаралық электротехникалық комиссия (ХЭК) сандық дәлелдерге қатысты халықаралық стандарттарды жариялады.

Бұл нұсқаулық сандық дәлелдермен жұмыс істеудің бастапқы процесін ғана қамтиды. Сандық дәлелдермен жұмыс істеудің келесі төрт кезеңі ұсынылады:

Сәйкестендіру. Бұл кезең тиісті дәлелдемелерді іздеуді және тануды, сондай-ақ оларды құжаттауды қамтиды. Бұл кезеңде дәлелдемелерді жинаудың басым міндеттері дәлелдердің құндылығы мен өзгергіштігі негізінде анықталады.

Жинау. Бұл кезең дәлелді құндылығы бар деректерді қамтуы мүмкін барлық сандық құрылғыларды жинауды қамтиды. Содан кейін бұл құрылғылар сандық дәлелдемелерді жинау және талдау үшін сот зертханасына немесе басқа мекемеге тасымалданады. Бұл процесс статикалық режимде

деректерді жинау деп аталады. Алайда, статикалық режимде деректерді жинау іс жүзінде мүмкін емес жағдайлар болады. Мұндай жағдайларда нақты уақыт режимінде мәліметтер жиналады. Мысалы, инфрақұрылымның маңызды объектілерінің жүйелерін (мысалы, өндірістік процестерді басқару жүйелері) қарастырайық. Бұл жүйелерді электр қуатынан ажырату мүмкін емес, өйткені олар маңызды қызметтерді ұсынады. Сондықтан, мұндай жағдайларда нақты уақыт режимінде жұмыс істейтін жүйелерден өзгермелі және өзгермейтін деректер алынған кезде нақты уақыт режимінде деректер жиналады. Алайда, нақты уақыттағы деректерді жинау өндірістік процестерді басқару жүйелерінің қалыпты жұмысына кедергі келтіруі мүмкін (мысалы, олардың жұмысын бәсеңдету).

Алу. Сандық дәлелдер деректердің тұтастығын бұзбай алынуы керек. Біріккен Корольдіктің полиция бастықтарының Ұлттық кеңесі (NPCC), бұрын Біріккен Корольдіктің полиция қызметтері басшыларының қауымдастығы ретінде белгілі, бұл талапқа үлкен мән береді және оны сандық криминалистика тәжірибесінде маңызды қағида ретінде көрсетеді (№1 қағида: «Құқық қорғау органдары, осы органдарда жұмыс істейтін адамдар немесе олардың өкілдерінің іс-әрекеттері кейіннен сотта қолданылуы мүмкін деректердің өзгеруіне әкелмеуі керек») (UK Association of Chief Police Officers, 2012, p. 6). Деректерді өзгертпестен алу көшіру процесінде деректердің өзгеруіне жол бермейтін құрылғыны (жазу блокаторы) қолдана отырып сандық құрылғы мазмұнының көшірмесін жасау арқылы жүзеге асырылады (бұрмаланбаған кескін жасау деп аталатын процесс). Көшірме түпнұсқаның дәл көшірмесі екенін анықтау үшін функцияның хэш мәні математикалық есептеулерді қолдана отырып есептеледі; мұнда хэш функциясының мәнін алу үшін криптографиялық хэш функциясы қолданылады. Егер түпнұсқа мен көшірме үшін хэш функциясының мәні бірдей болса, онда көшірменің мазмұны түпнұсқадағыдай болады. Біріккен Корольдіктің полиция бастықтарының Ұлттық кеңесі «қандай да бір адам бастапқы деректерге қол жеткізуді, яғни нақты уақыт режимінде деректерді жинауды жүзеге асыруды қажет деп санайтын белгілі бір жағдайлардың болу мүмкіндігін мойындай отырып» (осы деректерге қол жеткізетін адам) мұндай әрекеттер үшін құзыретті болуы керек және олардың іс-әрекеттерінің орындылығы мен олардың салдарын түсіндіретін дәлелдер ұсына алады» деп атап өтті (№2 қағида).

Сақтау. Цифрлық құрылғылар мен цифрлық дәлелдемелердің тұтастығы айқындалатын дәлелдемелерді қорғау жүйесін пайдалана отырып «тергеушілер іс бойынша іс жүргізудің бүкіл кезеңі ішінде қылмыс (немесе оқиға) орнын қорғауды және дәлелдемелердің сақталуын қамтамасыз ететін процесс» ретінде қамтамасыз етілуі мүмкін. Тіркеу журналына «дәлелдемелерді жинауды кім жүзеге асырғаны, олардың қайда және қалай жиналғаны, осы дәлелдемелерді қандай адамдар алғаны және оларды қашан алғаны туралы ақпарат жазылады» (Maras, 2014, p. 377). Сандық сот ісін әр кезеңде мұқият құжаттау сотта дәлелдемелердің жарамдылығын қамтамасыз ету үшін қажет. АҚШ-тың ұлттық стандарттар және технологиялар

институтында әртүрлі функциялары бар құралдар туралы ақпаратты қамтитын сандық криминалистика құралдарының мәліметтер базасы бар (мысалы, мәліметтер базасына, бұлтты қоймаларға, ұшқышсыз ұшақтарға, көлік құралдарына және т.б. криминалистикалық сараптама жүргізу құралдары).

Әр түрлі елдердің ұлттық құқық қорғау органдарының сандық сот сараптамасына арналған құралдарды қолдануға қатысты әртүрлі артықшылықтары бар. Пайдаланылған құралдар криминалистика тұрғысынан сенімді болуы керек. Бұл жағдайда деректерді (сандық) жинау және одан кейінгі талдау процесі осы құралдарды қолдана отырып, деректерді олар алғаш ашылған күйде сақтай алуы керек және техникалық немесе процедуралық қателіктерге немесе түсіндірудегі қателіктерге байланысты электрондық деректердің дәлелді құндылығын төмендетпеуі керек. Қарапайым сөзбен айтқанда, алынған мәліметтер ешқандай жолмен өзгертілмеуі керек, яғни олардың тұтастығы сақталуы керек. АҚШ ұлттық стандарттар және технологиялар институтының компьютерлік криминалистика құралдарын тестілеу бағдарламасының 17-і шеңберінде құралдардың жалпы сипаттамаларын, сынақ процедураларын, сынақ критерийлерін, сынақ жиынтықтары мен тестілеу жабдықтарын әзірлеу негізінде компьютерлік-техникалық сараптаманың бағдарламалық құралдарын тестілеу әдістемесі қабылданды.

Тестілеу әзірлеушілерге әзірленетін құралдарды жетілдіру үшін қажетті ақпаратты алуға мүмкіндік береді, пайдаланушыларға компьютерлік-техникалық сараптама құралдарын сатып алуға және пайдалануға қатысты саналы таңдау жасауға мүмкіндік береді және барлық мүдделі тараптардың құралдардың мүмкіндіктерін түсінуіне ықпал етеді.

Сандық криминалистика сандық дәлелдемелерді сәйкестендіру, алу, сақтау, талдау және ұсыну процестерін қамтиды. Сандық дәлелдемелер сотта олардың жарамдылығын қамтамасыз ету үшін расталуы керек. Сайып келгенде, сот сараптамасына арналған артефактілер және қолданылатын криминалистикалық әдістер (мысалы, статикалық немесе нақты уақыттағы режимдерінде деректерді жинау) құрылғыға, оның операциялық жүйесіне және оның қорғаныс құралдарына байланысты.

Патенттелген операциялық жүйелер (тергеушілер бейтаныс болуы мүмкін) және қорғаныс құралдары (мысалы, шифрлау) сандық сот сараптамасына кедергі келтіреді. Мысалы, пайдаланушылар туралы ақпаратқа және олардың хабарламаларына үшінші тұлғалардың қол жеткізуіне кедергі келтіретін шифрлау құқық қорғау органдарына смартфондар сияқты сандық құрылғылардағы деректерге қол жеткізуге кедергі келтіруі мүмкін.

Талқылауға арналған сұрақтар:

1. Бұл құрылғы қандай деректерді сақтайды?
2. Бұл деректер қандай түрге жатады?
3. Бұл деректер қайда орналасқан?
4. Бұл деректердің орнын қалай анықтауға болады?

5 Тақырып. Киберқылмыстарды тергеу.

1. Киберқылмыстар туралы хабарламалар.

Тергеуді бастамас бұрын, киберқылмыс фактісін анықтап, ол туралы хабарлау керек. Бұл киберқылмысты тергеудегі қарапайым алғашқы қадам болып көрінгенімен, шындық мынада – бүкіл әлемде киберқылмыстар жағдайларының едәуір бөлігі туралы хабарланбайды (БҰҰ ЕҚБ, 2013).

Қылмыстар туралы хабарлау құлықсыздығын экономист Гэри Беккер (1968) ұсынған *күтілетін пайдалылық теориясымен* түсіндіруге болады, онда адамдар кез-келген әрекетке қатысады, егер бұл әрекеттерден күтілетін пайдалылық (яғни пайда) басқа әрекеттерге қатысудың күтілетін пайдасынан асып кетсе (Maras, 2016, p. 25). Киберқылмыстылық контекстісінде киберқылмыстардың құрбандары, егер мұндай хабарламаның күтілетін пайдалылығы төмен болса, киберқылмыс туралы хабарламайды (Maras, 2016, p. 25). Алайда, адамның немесе ұйымның киберқылмыс туралы хабарлауға дайындығы киберқылмыс түріне де байланысты. Қазіргі уақытта жүргізіліп жатқан зерттеулер киберқылмыстардың хабарланбауының бірнеше себептерін, соның ішінде киберқылмыстың белгілі бір түрлерінің құрбандары (мысалы, романтикалық алаяқтық) ұят пен ұялу сезімін сезеді; киберқылмыстың жасалу фактісін жариялаумен байланысты беделді тәуекелдер (мысалы, егер киберқылмыстың құрбаны коммерциялық кәсіпорын болса немесе тұтынушылардың сенімін жоғалту қаупі болса); адамның қылмыстың құрбаны болғаны туралы хабардар болмауы; құқық қорғау органдарының көмек көрсету қабілетіне деген сенімділік немесе күтілімнің төмен деңгейі; киберқылмыс туралы хабарлау үшін тым көп уақыт пен күш жұмсау қажеттілігі; және киберқылмыс туралы кімге хабарлау керектігі туралы хабардарлықтың болмауы (БҰҰ ЕҚБ, 2013; McGuire and Dowling, 2013; Tcherni et al., 2016; Maras, 2016).

Киберқылмыстар туралы хабарламалардың төмендетілген жиілігіне ден қою шарасы ретінде үкіметтік және үкіметтік емес ұйымдар киберқылмыстар туралы ақпаратты ұсыну рәсімін оңтайландыру жолымен хабарламалар санын арттыруға бағытталған бастамаларды іске асырды, бұл әдетте жасалған киберқылмыстың түріне байланысты бірнеше мекемелердің қатысуын көздейді (мысалы, полиция, банктер және өзге де қаржы мекемелері, сондай-ақ қаржы киберқылмыстардарды тергеуінде қатысатын мемлекеттік органдар интернет желісіндегі қаржылық алаяқтық туралы хабарламаларды ала алады), және веб-сайттар немесе жедел желілер сияқты киберқылмыстар туралы ақпаратты хабарлау тетіктеріне назар аудару. Мысалы, Жаңа Зеландияда NetSafe - интернеттегі қауіпсіздікті қамтамасыз ету саласында жұмыс істейтін тәуелсіз коммерциялық емес ұйым, мемлекеттік органдармен бірлесе отырып, ел азаматтарына киберқылмыс туралы хабарлама қалдыра алатын бірыңғай және қауіпсіз орын ұсыну үшін Orb веб-сайтын әзірледі. Оңтүстік Африкада киберқылмыс туралы ресурстар мен ақпараттың Оңтүстік Африка порталы қолданушыларға киберқылмыс туралы өз порталында хабарлауға мүмкіндік береді. Сонымен қатар, 2018 жылы АҚШ-та Федералды тергеу бюросы (ФТБ) американдық «Қылмыскер сияқты ойлау» телехикаясындағы актрисаның

қатысуымен киберқылмыс туралы ақпараттық-түсіндіру кампаниясын бастады, ол қоғамды киберқылмыс туралы хабарламаларды интернет-қылмыс туралы шағымдарды қабылдау орталығына жіберу мүмкіндігі туралы хабардар етті (IC3) (FBI, Reporting CyberCrime is as easy as IC3).

Мұндай бастамалардың киберқылмыс туралы хабарлардың жиілігіне әсерін бағалау қажет. Киберқылмыскерлер туралы хабарламаларды қабылдау процедурасын жеңілдету үшін Австралияда киберқылмыстылық туралы Интернет-хабарламалар желісі (ACORN) құрылды. 2016 жылы Австралиялық криминология институты Acorn бағалау есебін жариялады, онда бұл бастама киберқылмыс туралы хабарламалардың жиілігіне және қоғамның осындай хабарламаларды қайда жіберу керектігі туралы хабардар болу деңгейіне аз ғана әсер еткенін көрсетті (Morgan et al., 2016). Мұндай бастамаларды бағалау өте маңызды, өйткені ол үкіметтерге қажетті нәтижелерге қол жеткізетін жобаларға қаражат салуға және күтілетін нәтиже бермейтін бағдарламалар мен бастамаларға өзгерістер мен толықтырулар енгізуге мүмкіндік береді.

2. Киберқылмыстар бойынша тергеуді кім жүргізеді?

Киберқылмыстарды тергеу кезінде *алғашқы жауап шараларын қабылдайтын тұлғалар* киберқылмыстың «орнында» цифрлық дәлелдердің «сақталуы» үшін жауап береді (мысалы, бұл киберқылмыстың объектісі немесе объектілері және/немесе кибержелі және/немесе кибертәуелді қылмысты жасау үшін пайдаланылған ақпараттық-коммуникациялық технологиялар құрылғылары болуы мүмкін). Мұндай алғашқы әрекет ету шараларын қабылдайтын адам құқық қорғау органдарының қызметкері, сандық криминалистика жөніндегі сарапшы, әскери полиция офицері, жеке тергеуші, ақпараттық технологиялар жөніндегі маман немесе киберқылмыстылықпен байланысты оқиғаларға жауап беру міндеті қойылған басқа адам (мысалы, жалдамалы қызметкер) болуы мүмкін. Бұл киберқылмыстарды тергеуді мемлекеттік және жеке секторлар, сондай-ақ ұлттық қауіпсіздік органдары (қандай да бір қатысу дәрежесімен) жүргізетінін көрсетеді. Алғашқы жауап шараларын кім қабылдағанына қарамастан, ақпараттық-коммуникациялық технологиялар (АКТ) құрылғыларын іздеу және алып қою рәсімдері ұлттық заңнамаға сәйкес келуі керек, ал АКТ құрылғыларынан сандық дәлелдерді алу үшін қолданылатын әдістер сотта дәлелдемелердің жарамдылығын қамтамасыз ету үшін негізделген және сенімді болуы керек.

Қылмыстық сот төрелігі органдары.

Құқық қорғау органдарының қызметкерлері, прокурорлар және судьялар сияқты қылмыстық сот төрелігі жүйесінің қызметкерлері теріс салдарлардың алдын алу, жеңілдету, киберқылмыстарды анықтау, тергеу, сондай-ақ қылмыстық қудалау және киберқылмыстылықпен байланысты істер бойынша сот шешімдерін шығару үшін жауап береді. Киберқылмыстарды тергеуге жауапты нақты органдар елге байланысты әр түрлі болады. Мысалы, Ұлыбританияда киберқылмыстарды тергеуді бірнеше органдар, соның ішінде аймақтық құқық қорғау органдары және қылмысқа қарсы Ұлттық агенттіктің құрамына кіретін киберқылмыстылықпен күрес жөніндегі Ұлттық бөлімше

жүргізеді (Global Cyber Security Capacity Centre, 2016c). Ұлыбританиядан айырмашылығы, тек бір мекеме Сьерра-Леоне сияқты елдерде киберқылмыстарды тергеумен айналысады, онда киберқылмыстылықтың алдын алу жөніндегі полиция бөлімі (Global CyberSecurity Capacity Centre, 2016d), Эквадор, онда «Ұлттық сот полициясы және тергеу дирекциясының технологиялық қылмыстарды тергеу бөлімі киберқылмыстарды тергеу үшін жауап береді» (Inter-American Development Bank, 2016, p. 72) және Исландия, Рейкьявик полициясының сандық сот-сараптама бөлімі осындай тергеулермен айналысады (Global Cyber Security Capacity Centre, 2017c).

Сонымен қатар, кейбір елдерде бірнеше мекеме бірдей киберқылмысты тергеуге қатыса алады. Осы немесе басқа мекеменің қатысуы зерттелетін киберқылмыстың түріне байланысты болады. Мысалы, Кипрде интернеттегі қаржылық алаяқтықпен байланысты қылмыстарды қылмыстық тергеу бөлімі, сондай-ақ Кипр полициясының бас дирекциясының қаржылық қылмыстарды тергеу тобы тергейді (GlobalCyber Security Capacity Centre, 2017b). Әртүрлі елдерде киберқылмыстылықпен күрес және киберқылмыстар туралы істерді тергеу үшін әртүрлі органдар жауапты болғандықтан, көптеген елдерде ресми байланыс пункттері құрылады. Мысалы, Кипрде киберқылмыстылықпен күрес басқармасы тәулік бойы жұмыс істейді (Global Cyber SecurityCapacity Centre, 2017b).

Қылмыстық сот төрелігі органдарының қызметкерлері арнайы білімге (яғни, тапсырманы орындау үшін қажетті пәндік салаға қатысты ақпаратқа), дағдыларға (яғни, пәндік саладағы кәсіби тәжірибеге) және интернеттен тыс жасалатын қылмыстарға байланысты істерді тергеу, қылмыстық қудалау және/немесе талқылау үшін қажетті білімге, дағдылар мен қабілеттерге қосымша қабілеттерге (яғни, тапсырманы орындау үшін білім мен дағдыларды қолдана білуге) ие болуы керек (барлығы бірге олар БДҚ (білім, дағдылар, қабілеттер) деп аталады. Мысалы, құқық қорғау органдарының қызметкерлері киберқылмыстарды және/немесе қандай да бір жолмен ақпараттық-коммуникациялық технологиялар құрылғыларын (мысалы, қылмыстың дәлелдерін сақтайтын смартфондар) пайдалануға байланысты басқа да қылмыстарды тергеуге және тергеу барысында АКТ-мен тиісті түрде жұмыс істеуге қабілетті болуы керек (мысалы, сандық дәлелдемелерді сотта рұқсат етілуін қамтамасыз ету үшін анықтау, алу, сақтау және талдау) (National Initiative for Cybersecurity Careers and Studies, n.d.). Құқық қорғау органдарының киберқылмыстарды тергеу мүмкіндігі елге байланысты және елдегі нақты мекемеге байланысты өзгереді. Мысалы, Қырғыз Республикасында құқық қорғау органдары арнайы білімнің, дағдылардың, қабілеттердің, дайындықтың жоқтығынан, сондай-ақ кадрлық және қаржылық ресурстардың жетіспеушілігінен киберқылмыстарды тергеу үшін шектеулі мүмкіндіктерге ие (Global Cyber Security Capacity Centre, 2017a). Мадагаскарда 2017 жылғы есеп көрсеткендей, құқық қорғау органдарының құрылымында «киберқылмыстылықпен күресудің арнайы бөлімі жоқ... киберқылмыстылық мәселелермен осы мақсат үшін арнайы тағайындалған Ұлттық полиция және жандармерия қызметкерлері айналысты» (Global Cyber Security Capacity

Centre, 2017a, p. 33). Салыстыру үшін, Францияда киберқылмыстарды тергеу үшін арнайы дайындықтары бар бірнеше бөлімшелері бар (мысалы, Les investigateurs en Cybercriminalité (киберқылмыстылық бойынша істер тергеушілері) (ICC) және N-TECH (Ұлттық жандармерия құрамына кіретін жаңа технологиялар саласындағы арнайы дайындықтары бар тергеушілер).

Қылмыстық сот төрелігі жүйесінің басқа қызметкерлері, мысалы прокурорлар мен судьялар, киберқылмыстылық және *сандық криминалистика* туралы арнайы білімге ие болуы керек (бұл «қылмыстық іс жүргізу құқығына және компьютерлерге және олармен байланысты құрылғыларға қатысты дәлелдерге мамандандырылған криминалистиканың бір саласы». Құқық қорғау органдарындағыдай, прокурорлар мен судьялардың дайындық деңгейі елдер арасында, тіпті елдер ішінде де өзгеріп отырады. Мысалы, Ұлыбританияда корольдік прокурорлық қызмет киберқылмыстардың жасалуында кінәлілерді сот қудалауына барлық мүмкіндіктерге ие, ал 2016 жылғы жағдай бойынша жергілікті прокурорлар киберқылмыстармен байланысты қылмыстық қудалауды жүзеге асыру үшін бірдей дайындық пен ресурстарға ие болмады (Global Cyber Security Capacity Centre, 2016c). 2017 жылы Сьерра-Леоне билігі прокурорлар мен судьялардың киберқылмыстылықпен байланысты істерді қудалау және қарау үшін қажетті білімі, дағдылары, қабілеттері мен ресурстары жоқ екенін хабарлады (Global Cyber Security Capacity Centre, 2016d). Осыған ұқсас жағдай Исландияда байқалады, онда прокурорлар мен судьялар ерікті негізде киберқылмыстылық мәселелері бойынша тек арнайы дайындықтан өтеді (Global Cyber Security Capacity Centre, 2017c). Сот төрелігі органдарының қызметкерлері киберқылмыстылық және сандық криминалистика туралы негізгі ақпаратпен танысу, киберқылмыстар бойынша істердегі сарапшылардың айғақтарына және сотта сандық дәлелдемелердің жарамдылығына қатысты мәселелерді зерделеу үшін дайындықтан өтуі тиіс. 2017 жылы Сенегал билігі судьялардың мұндай дайындықтан өтпейтінін хабарлады (Global CyberSecurity Capacity Centre, 2016b).

Ұлттық қылмыстық сот төрелігі органдарынан басқа, Еуропалық Одақтың құқық қорғау органдарының ынтымақтастық агенттігі (Europol) (Еуропалық Одақтағы құқық қорғау органдары арасындағы ынтымақтастықты дамыту үшін) және Eurojust (Еуропалық Одаққа мүше елдердің сот органдары арасындағы ынтымақтастықты дамыту үшін) және INTERPOL (халықаралық құқық қорғау органдары арасындағы халықаралық ынтымақтастыққа ықпал ететін Халықаралық қылмыстық полиция ұйымы) сияқты халықаралық агенттіктер, киберқылмыстарға трансшекаралық тергеп-тексерулер жүргізуге жәрдемдеседі және/немесе ықпал етеді. Мысалы, Еуропол мен Еуропалық Одаққа мүше мемлекеттер арасында Жедел деректер мен ресурстармен алмасу нәтижесінде қараңғы интернеттегі заңсыз нарықтарда 50 Euro номиналы бар жалған банкноттарды сатумен танымал қылмыскер қамауға алынды (Europol, 2018c).

Ұлттық қауіпсіздік органдары.

Ұлттық қауіпсіздік органдары киберқылмыстарды тергеуге қатысуы

мүмкін (мысалы, кейбір елдерде киберқылмыстарды тергеу әскери органдардың қатысуымен жүргізілуі мүмкін, ал басқа елдерде мұндай тергеулерді барлау органдары немесе киберқауіпсіздік ұлттық басқармалары жүргізуі мүмкін). Алайда, ұлттық қауіпсіздік органдарының киберқылмыстарды тергеуге қатысуы тергеліп жатқан киберқылмысқа, киберқылмыстың объектісіне (объектілеріне) және/немесе киберқылмыстың орындаушыларына байланысты. Мысалы, әскери органдар қарулы күштермен қандай да бір байланысы бар киберқылмыстарды, яғни әскери қызметшілерге, әскери мүлікке және/немесе әскери ақпаратқа қарсы жасалған киберқылмыстарды және/немесе әскери қызметшілер жасаған киберқылмыстарды тергеуі мүмкін. Мысал ретінде әскери полиция қызметкерлері Бірыңғай әскери әділет кодексін бұзу жағдайларын зерттейтін Америка Құрама Штаттарын келтіруге болады. Мұндай киберқылмыстарды тергеуге қосымша (немесе, кем дегенде, қандай да бір сапада киберқылмыстарды тергеуге қатысу), әскери органдар және өзге де ұлттық қауіпсіздік органдары теріс салдарларды анықтауға, жеңілдетуге, осы органдардың жүйелеріне, желілеріне және деректеріне, құпия ақпараты бар жүйелерге бағытталған киберқылмыстардың алдын алуға, сондай-ақ осындай киберқылмыстарға ден қоюдың жауап шараларын қабылдауға жауап беруі мүмкін. Бүкіл әлемдегі ұлттық қауіпсіздік органдары өздерінің киберқорғау мүмкіндіктерін дамытты және/немесе қазіргі уақытта дамытуда (яғни, киберқылмыстарды анықтауға және алдын алуға және осы киберқылмыстар жасалған жағдайда олардың салдарын жеңілдетуге арналған шаралар) және кибер шабуыл мүмкіндіктер. Бұл киберкеңістікті Ұлттық қауіпсіздік органдарының киберкеңістіктегі қызметін кеңейтуге әкелген тағы бір соғыс саласы ретінде тану (Smeets, 2018; Kallender and Hughes, 2017). Мысалы, Америка Құрама Штаттарында бесінші соғыс саласының мұндай танылуы АҚШ-тың кибернетикалық қолбасшылығының (USCYBERCOM) құрылуына әкелді. Америка Құрама Штаттарының мысалы бойынша Нидерланды, Германия, Испания, Корея Республикасы және Жапония сияқты басқа елдер де ұқсас кибернетикалық қолбасшылықтар және/немесе кибернетикалық орталықтар немесе бөлімшелер құрды.

Жеке сектор.

Жеке сектор киберқылмыстарды анықтауда, алдын-алуда, жеңілдетуде және тергеуде маңызды рөл атқарады, өйткені көп жағдайда бұл *аса маңызды инфрақұрылымға* ие жеке сектор (яғни, қоғамның жұмыс істеуі үшін қажет деп саналатын инфрақұрылым) және оны басқарады және көптеген кибершабуылдардың негізгі мақсаттарының бірі болып табылады (яғни, бұзу, зиянды бағдарламаларды тарату және «қызмет көрсетуден бас тарту» немесе DDoS-шабуылдар сияқты таратылған шабуылдар) және кибержелілерді пайдалану қылмыстары (мысалы, интернеттегі қаржылық алаяқтық, жеке деректерді пайдалануға байланысты қылмыстар, деректер мен коммерциялық құпияны ұрлау және басқалар). Біріккен Ұлттар Ұйымы Қауіпсіздік Кеңесінің 2341 (2017) резолюциясына сәйкес, оның аумағындағы «әрбір мемлекеттің өзі оның инфрақұрылымының қандай объектілері аса маңызды болып

табылатынын айқындайды». Инфрақұрылымның мұндай мәртебесін мемлекеттің өзі анықтайтындықтан, қандай инфрақұрылым объектілері маңызды болып табылатындығына қатысты елдер арасында айырмашылықтар бар. Мысалы, Австралия сегіз секторға (атап айтқанда: денсаулық сақтау; энергетика; көлік; сумен жабдықтау; байланыс, азық-түлік өндірісі және азық-түлік бөлшек саудасы; банк және қаржы; және Австралия одағының үкіметі) (Australian Government, Department of Home Affairs, n.d.) қатысты объектілерді аса маңызды инфрақұрылым ретінде айқындады, ал Америка Құрама Штаттары маңызды инфрақұрылым нысандарының 16 түрін анықтады (химиялық нысандар; сауда кәсіпорындары; байланыс объектілері; аса маңызды өнеркәсіптік нысандар; бөгеттер; қорғаныс өнеркәсібінің өндірістік базасы; төтенше жағдайлар қызметі; энергетика; қаржылық қызметтер; азық-түлік және ауыл шаруашылығы; мемлекеттік мекемелер; денсаулық сақтау және санитарлық-эпидемиологиялық қызметтер; ақпараттық технологиялар; ядролық реакторлар, материалдар мен қалдықтар; көлік жүйелері; сумен жабдықтау және сарқынды суларды жою жүйелері) (US Department of Homeland Security, n.d.).

Көптеген жағдайларда оны басқаратын және киберқылмыскерлердің негізгі мақсаттарының бірі болып табылатын жеке сектор өте маңызды инфрақұрылымға ие болғандықтан, киберқылмыстардың алдын алу немесе кем дегенде жеңілдету мақсатында киберқылмыстар мен киберқылмыскерлерді алдын-ала анықтауға, сондай-ақ жасалған киберқылмыстардың салдарын кем дегенде жұмсартуға, сонымен қатар жасалынып жатырған немесе жасалған киберқылмыстарға жауап беруге арналған қауіпсіздік шараларын қабылдауға барлық мүмкіндіктер бар. «Аса маңызды инфрақұрылым» терминін барлық елдер базалық инфрақұрылымды сипаттау үшін қолдана бермейді (Біріккен Ұлттар Ұйымы Қауіпсіздік Кеңесінің Терроризмге қарсы комитетінің Атқарушы директораты және Біріккен Ұлттар Ұйымының терроризмге қарсы Басқармасы, 2018 жыл). Мысалы, «аса маңызды инфрақұрылым» терминінің орнына Жаңа Зеландия «өмірлік маңызды байланыс» терминін энергетика, байланыс, көлік және сумен қамтамасыз етуді қамтитын өмірді қамтамасыз етудің маңызды объектілерін белгілеу үшін қолданады (New Zealand Lifelines Council, 2017). Жеке сектор қабылдаған мұндай шаралар масштабы нақты ұйымға, оның қызмет саласына немесе ұйымдық-құқықтық нысанына, оның адами, қаржылық және техникалық ресурстары мен мүмкіндіктеріне байланысты.

Жеке сектор сонымен қатар киберқылмыстарға жеке тергеу жүргізуде. Жеке сектор *ішкі қауіптерге* де (мысалы, коммерциялық кәсіпорынның немесе ұйымның қызметкерлері немесе басшылары жасаған киберқылмыстарға), сондай-ақ *сыртқы қауіптерге* де (мысалы, коммерциялық кәсіпорынмен немесе ұйыммен, мысалы, жеткізушілермен немесе тапсырыс берушілермен қандай да бір байланысы бар немесе кәсіпорынмен немесе ұйыммен ешқандай байланысы жоқ тұлғалармен жасалатын киберқылмыстарға) осал (Maras, 2014, p. 253). Киберқылмыс жасалған кезде кәсіпорындар мен ұйымдар көбінесе құқық қорғау органдарына жүгінбейді. Алайда, бұл киберқылмыстың түріне,

жеке ұйымның адами, техникалық және қаржылық ресурстарына, сондай-ақ осы ұйым үшін жасалған киберқылмыс туралы хабарлаудың салдары тұрғысынан ұйымға киберқылмыстың әсеріне байланысты (мысалы, беделге нұқсан келтіру және/немесе тұтынушылардың сенімін жоғалту).

Мемлекеттік-жекешелік әріптестік және нысаналы топтар.

Жеке сектор киберқылмыстарға тергеу жүргізу үшін адами, қаржылық және техникалық ресурстарға ие және ұлттық қауіпсіздік органдарына, құқық қорғау органдарына және киберқылмыспен байланысты істер жөніндегі басқа да мемлекеттік мекемелерге көмек көрсете алады. Осыған байланысты халықаралық деңгейде киберқылмыстарды тергеу үшін елдердің мүмкіндіктерін күшейту мақсатында мемлекеттік-жекешелік әріптестік шеңберінде көптеген жобалар әзірленді. Мысал ретінде Интерполдың киберқылмыс туралы деректер өңдеу орталығы (Cyber Fusion Centre) бар, онда құқық қорғау органдарының қызметкерлері де, киберқауіпсіздік саласындағы сарапшылар да жұмыс істейді, олар құнды жедел ақпаратты жинайды және оны тиісті мүдделі тараптармен бөліседі (INTERPOL, n.d.). Trend Micro (киберқауіпсіздік және киберқорғаныс қамтамасыз ететін бағдарламаларды жасаушы компания), Касперский Зертханасы (киберқауіпсіздік және компьютерлік вирустардан қорғау бағдарламаларын жасаушы) және киберқылмыстылықпен немесе киберқауіпсіздікпен айналысатын және/немесе Интернет қызметтері мен интернет мазмұнын жеткізушілер болып табылатын немесе интернетке байланысты басқа да қызметтерді ұсынатын басқа жеке компаниялар Интерполмен (INTERPOL, n.d.) тығыз жұмыс істейді. Солтүстік Атлантикалық Шарт Ұйымы (НАТО) сонымен бірге одақтастармен, атап айтқанда Еуропалық одақпен және жеке өнеркәсіппен, атап айтқанда, НАТО-ның өнеркәсіппен киберқорғаныс және киберсеріктестік туралы техникалық Келісімі негізінде ынтымақтасады.

Мемлекеттік-жекешелік әріптестік (МЖӘ) тетіктері де ұлттық деңгейде құрылады. Америка Құрама Штаттарында Ұлттық киберкриминалистика және кибердайындық альянсы (NCFTA) киберқылмыстардың салдарын анықтау және азайту және олармен күресу мақсатында мемлекеттік органдар, ғылыми орталықтар және жеке сектордан киберқылмыстылық бойынша мамандарды біріктіреді (NCFTA, n.d.). Жапонияда МЖӘ шеңберінде NCFTA-ға ұқсас құрылым - киберқылмыстылықпен күрес жөніндегі орталық құрылды (JC3, 2014). Еуропада 2centre жобасы (2 орталық) құқық қорғау органдары, білім беру ұйымдары және жеке бизнес арасындағы ынтымақтастық негізінде жүзеге асырылады. МЖӘ аясында бұл жобаны іске асыру Ирландия мен Францияда ұлттық орталықтар құрудан басталды, кейіннен басқа елдерде ұлттық орталықтар құрылды; 2017 жылғы жағдай бойынша мұндай орталықтар Греция, Испания, Бельгия, Эстония, Литва, Болгария және Англияда жұмыс істейді.

3. Киберқылмыстарды тергеуге кедергілер.

Киберқылмыстарды тергеу жүргізу кезінде түрлі кедергілер туындауы мүмкін. Осындай кедергілердің бірі пайдаланушыларға ақпараттық-коммуникациялық технологиялар құралдары қамтамасыз ететін анонимділік.

Анонимділік адамдарға жеке басы және/немесе іс-әрекеттері туралы ақпаратты басқа адамдарға ашпай-ақ, кез-келген қызметпен айналысуға мүмкіндік береді. Киберқылмыскерлер қолданатын анонимизацияның бірнеше әдістері бар. Осындай әдістердің бірі *прокси-серверлерді* пайдалану. Прокси-сервер - бұл клиентті (яғни, компьютерды) клиент ресурстарды сұрайтын сервермен қосу үшін қолданылатын аралық сервер (Maras, 2014, p. 294). Анонимайзерлер немесе анонимді прокси-серверлер пайдаланушылардың идентификациялық деректерін олардың IP-мекенжайларын жасыру және оларды басқа IP-ге ауыстыру арқылы жасырады. Анонимизациялау әдістері заңды және заңсыз негізде қолданылады. Анонимді болып қалуға және желіде анонимділікті сақтауға заңды негіздер бар. Мысалы, анонимділік қажетсіз немесе танымал емес ойларды білдірудің салдарынан қорықпай, ақпарат пен хабарламалардың еркін ағынына ықпал етеді. Киберқылмыскерлер анонимді желілерді трафикті шифрлау (мысалы, кіруді бұғаттау) және интернет протоколының мекен-жайын (немесе *IP-мекенжайын*) жасыру үшін, «желіге қосылған кезде интернет қызмет жеткізуші компьютерге (немесе интернетке қосылған басқа сандық құрылғыға) берген бірегей идентификаторды» (Maras, 2014, p. 385), интернеттегі белсенділігі мен орналасқан жерін жасыру үшін қолдана алады. Анонимді желілердің жақсы зерттелген мысалдары Tor, Freenet және Invisible Internet Project (I2P деп танылатын «Көрінбейтін Интернет» жобасы). Интернетте анонимді қол жетімділікті, байланыс пен ақпарат алмасуды қамтамасыз ететін пияз маршрутизаторын (немесе Tor) бастапқыда АҚШ Әскери-теңіз зерттеу зертханасы барлау деректерін қорғау үшін жасаған (Maras, 2014a; Maras, 2016). Tor көпшілікке қол жетімді болғаннан кейін, оны жеке адамдар өздерінің желідегі қызметін жеке және мемлекеттік қадағалаудан қорғау үшін қолдана бастады. Алайда, Tor және басқа да анонимді желілер киберқылмыскерлермен кибержелілер мен кибертәуелді қылмыстарды жасау үшін және/немесе осындай қылмыстарды жасау мақсатында ақпарат және/немесе құралдар алмасу үшін қолданылған (Europol, 2018). Бұл анонимді желілер «пайдаланушылардың сәйкестендіретін деректерін жасырып қана қоймайды, сонымен қатар олардың веб-сайттарын өз ресурстарында, (өздерінің) «жасырын қызметтерінің» мүмкіндіктерін … қолдана отырып, орналастырады, яғни (бұл сайттар) адамдарға тек осы анонимді желілерде қол жетімді болуы мүмкін». Осылайша, бұл анонимді желілер Даркнеттегі (немесе Қараңғы ғаламтордағы) сайттарға кіру үшін қолданылады.

Бүкіләлемдік тор: негізгі мәліметтер

Бүкіләлемдік ғаламторды көрнекі түрде көрсету үшін мұхиттағы айсберг бейнесі жиі қолданылады. Айсбергтің су бетіндегі бөлігі көрінетін Интернет (немесе көрінетін ғаламтор немесе көрінетін желі) деп аталады. Веб-сайттың бұл бөлігі көпшілікке қол жетімді және пайдалануға дайын индекстелген сайттарды қамтиды және оларды Google немесе Bing сияқты дәстүрлі іздеу жүйелерін қолдана отырып табуға болады (Maras, 2014b). Терең желі - бұл айсбергтің су бетінің деңгейінен төмен бөлігі. Ол іздеу жүйелерімен индекстелмеген және қол жетімді емес және/немесе көпшілікке оңай қол

жетімді және пайдалануға дайын емес, мысалы, парольмен қорғалған сайттар (Maras, 2016). Егер бірыңғай ресурс көрсеткіші (URL; яғни веб-сайт мекенжайы) белгілі болса және/немесе парольмен қорғалған веб-сайттар мен онлайн-форумдарға қол жеткізу үшін пайдаланушылардың есептік деректері (яғни, пайдаланушы аттары, парольдер, құпия сөз парольдері және т.б.) берілсе, осы сайттарға тікелей қол жеткізуге болады. Қараңғы веб-сайттарға кіру үшін арнайы бағдарламалық жасақтама қажет, өйткені ол сайттарға кіруді болдырмау және жасыру үшін анонимділікті арттыратын құралдарды қолданады.

Атрибуция - киберқылмыстарды тергеуді қиындататын тағы бір кедергі. Атрибуция - бұл киберқылмыс үшін кім және/немесе не жауапты екенін анықтау. Атрибуцияның мақсаты киберқылмысты белгілі бір сандық құрылғының, құрылғыны Пайдаланушының және/немесе киберқылмыстың жасалуына кінәлі басқа адамдардың есебіне жатқызу болып табылады (мысалы, егер киберқылмысты мемлекет қаржыландырса немесе бағыттаса). Анонимділікті арттыратын құралдарды пайдалану киберқылмыс жасауға жауапты құрылғыларды және/немесе адамдарды сәйкестендіруді қиындатуы мүмкін. Атрибуция процесі зиянды бағдарламалармен зарарланған зомби-компьютерлерін (немесе *бот-желілерді*) немесе *қашықтан қол жеткізу құралдарымен* басқарылатын сандық құрылғыларды (яғни, зиянды бағдарламаны таратушыға жүйелерге қол жеткізуге және оларды басқаруға мүмкіндік беретін зарарланған құрылғыда бэкдор құру үшін пайдаланылатын зиянды бағдарлама) пайдалану салдарынан күрделене түседі. Бұл құрылғыларды киберқылмыстарды жасау үшін құрылғысы зарарланған пайдаланушы білместен пайдалануға болады. Кері қадағалау (немесе *кері бағытта қадағалау*) – бұл киберқылмыстың көзін (яғни орындаушыны және/немесе сандық құрылғыны) айқындау үшін заңсыз әрекеттерді бақылау процесі. Кері бағытта қадағалау киберқылмыс жасалғаннан кейін немесе анықталған кезде жүзеге асырылады. Алдын-ала тергеу киберқылмыс туралы ақпаратты анықтауға көмектесетін журнал файлдарын (мысалы, файлдық жүйелердің белсенділігін көрсететін *оқиғалар журналдарын*) зерттеу арқылы киберқылмыс туралы ақпаратты (мысалы, оның қалай жасалғанын) анықтау мақсатында жүргізіледі. Мысалы, оқиғалар журналдары «жүйеде белсенділік пен проблемаларды бақылау, түсіну және диагностикалау үшін қолданылатын бақылау ізін алу үшін компьютерде болып жатқан оқиғаларды автоматты түрде тіркейді ...» (Maras, 2014, p. 382). Мұндай журналдардың мысалдары – «бағдарламалар мен қосымшалар тіркейтін оқиғаларды» жазатын *қосымшалар журналдары* және «жүйеге кірудің барлық әрекеттерін (дұрыс және дұрыс емес) тіркейтін *қауіпсіздік журналдары*, сонымен қатар компьютер пайдаланушысының файлдарды, бағдарламаларды немесе басқа объектілерді жасауы, ашуы немесе жоюы» (Maras, 2014, p. 207). Бұл оқиғалар журналдары киберқылмыс кезінде қолданылатын IP-мекенжайын анықтауға көмектеседі.

Кері бағытта қадағалау процесі ұзақ болуы мүмкін. Орындау үшін қажетті уақыт осы рәсімнің қылмыс орындаушылардың білімдері, дағдылары мен қабілеттеріне және олардың жеке басын және қызметін жасыру үшін

қолданған шараларына байланысты. Киберқылмыскерлер заңсыз әрекеттер жасау үшін қолданған тактикалық әдістерге байланысты қадағалау жалғыз анықталатын көзге әкелмеуі мүмкін. Мысалы, бұл киберқылмыс жасау үшін зиянды бағдарламамен залалданған зомби-компьютерлер пайдаланылған жағдайларда немесе бірнеше зиянкестер бір мезгілде «қызмет көрсетуден бас тарту» түріндегі таратылған шабуылды жүргізген кезде байқалуы мүмкін. Киберқылмыстарды тергейтін тергеушілер де техникалық проблемаларға тап болады. Мысалы, көптеген сандық құрылғыларда сандық дәлелдерді анықтау, жинау және сақтау үшін мамандандырылған құралдарды қолдануды қажет ететін патенттелген операциялық жүйелер мен бағдарламалық жасақтамалар пайдаланады. Оның үстіне, тергеушілерде сандық құрылғыларды қолдануды көздейтін киберқылмыстарды тиісті тергеу жүргізу үшін қажетті сандық криминалистика жабдықтар мен құрал-саймандары болмауы мүмкін.

Киберқылмыстарды тергеудің басқа кедергілеріне құқық қорғау органдарының мұндай тергеулерді жүргізу үшін шектеулі мүмкіндіктері кіреді. Ұлттық мамандандырылған бөлімшелері бар елдерде олар киберқылмыстар жағдайларының шектеулі санын ғана тергейді. Қылмыстарды тергеуде ақпараттық-коммуникациялық технологияларды кеңінен қолдану мұндай тәжірибені тиімсіз етеді (БҰҰ ЕҚБ, 2013). Полиция қызметінің мамандандырылмаған салаларында және техникалық емес мамандандырылған бөлімшелерде жұмыс істейтін ұлттық құқық қорғау органдарының қызметкерлерін (мысалы, есірткіге, ұйымдасқан қылмысқа, балаларға қарсы қылмыстарға қарсы күрес бойынша), киберқылмыстылық, АКТ-мен байланысты тергеу және сандық криминалистика мәселелері бойынша даярлау ұлттық әлеуетті нығайтудың бір тәсілі болып табылады (БҰҰ ЕҚБ, 2013). Сонымен қатар, құқық қорғау органдарының бұл шектеулі мүмкіндіктері киберқылмыстар бойынша істер тергеушілердің кәсіби білім өзектілігінің қысқа мерзімділігімен күрделене түседі. Өйткені, ақпараттық-коммуникациялық технологиялар үздіксіз дамып келеді. Сондықтан киберқылмыстарды тергейтін тергеушілер өмір бойы оқып, технологияның дамуын үнемі қадағалап отыруы керек, киберқылмыскерлерден артта қалмауы керек, олардың себептерін, мақсаттарын, тактикалық әдістері мен қылмыс жасау тәсілдерін білуі керек. Сонымен қатар, мемлекеттік және ұлттық қауіпсіздік қызметтері «мидың ағуы» деп аталатын проблемаға тап болады, онда киберқылмысқа Мамандандырылған жоғары білікті және тәжірибелі тергеушілер осы органдардан шығып жеке секторға ауысады, онда оларға білімі, дағдылары мен қабілеттері үшін жоғары ақшалай сыйақы ұсынылады. Бұл әлеуетті және кадрлық мәселелерді елдер мұқият қарастыруы керек, өйткені олар киберқылмыстарды тергеуге үлкен кедергі болып табылады.

4. Білімді басқару.

Білімді басқару тұжырымдамасы кадрлық және техникалық ресурстармен, сондай-ақ осы тергеулерді жүргізу үшін қажетті біліммен, дағдылармен және қабілеттермен байланысты киберқылмыстарды тергеудегі кедергілерді жою әдісі ретінде алға жылжуда. Білімді басқарудың мақсаты - процесті немесе түпкілікті нәтижені жақсарту үшін «адамдар мен ақпарат

сияқты көптеген білім ресурстарын құру, сақтау және қолдану» (Weiping and Chung, 2014, p. 8).

Білімді басқару процесі киберқылмыстарды тергеуде қолданылуы мүмкін және қазірдің өзінде қолданылды (Weiping and Chung, 2014, p. 10-11). Киберқылмыстарды тергеу контекстісінде білімді басқару процесі жалпы және арнайы сипаттағы киберқылмыстарды тергеу үшін білім қажеттіліктерін анықтауды және бағалауды қамтиды. Осындай қажеттіліктерді анықтап және бағалағаннан кейін киберқылмыстылық саласындағы тиісті органның білімі белгіленеді және бағаланады. Білімге деген қажеттілікті тергеушілердің қазіргі білім деңгейімен салыстыру кезінде білімдегі олқылықтар анықталады. Білімдегі олқылықтар анықталғаннан кейін оларды жою шаралары ұсынылады. Білімді басқарудың практикалық әдістерін осы білім кемшіліктерін толтыру үшін қолдануға болады.

Білімді басқару білімді алуға, пайдалануға, құруға, басқаруға және/немесе бөлісуге, сондай-ақ білімді басқаруға ықпал ететін процестер мен технологиялардың қатысуымен жүзеге асырылады. Құқық қорғау қызметіндегі білімді басқару процесінің ажырамас бөлігі болып табылатын біліммен алмасу басқа адамдар арасында білімді ілгерілететін сыртқы күштердің (мысалы, ағартушылық және ақпараттық кампаниялар), сондай-ақ басқа адамдарды білім алуға *итермелейтін* мысалы, сараптамалық білімді немесе белгілі бір мәселе бойынша көмек іздеу ішкі факторлардың (*тартылыс* факторлары) қатысуымен жүреді. Еуропол Dark Web Team (қараңғы желі командасы) құрды, ол білім алмасудың осы түрінің мысалы болып табылады. Атап айтқанда, Dark Web Team ақпарат алмасады, қылмыстың әртүрлі салаларында мамандардың жедел қолдауы мен қызметтерін ұсынады (оларды сұрайтындарға) және... қараңғы желіде тергеу жүргізу және ең үлкен қауіптер мен мақсаттарды анықтау құралдарын, тактикалық әдістері мен тәсілдерін әзірлейді. Бұл топ сонымен бірге бірлескен техникалық және тергеу шараларының тиімділігін арттыруды, оқыту және әлеуетті арттыру бір мезгілде қараңғы желідегі қылмысқа қарсы жан-жақты стратегия аясында алдын алу жөніндегі науқандарды өткізу бойынша бастамаларын ұйымдастыруды мақсат етеді (Europol, 2018b).

Білімді басқару процесі сонымен қатар білімге және білім көздеріне (мысалы, адамдарға) мұқтаж адамдар үшін қол жетімділікті қамтамасыз етуге бағытталған. Мысалы, АҚШ-тың Федералды тергеу бюросы киберқылмыстылықпен байланысты істерді тергеуге қолдау көрсету үшін Америка Құрама Штаттарының кез-келген жерінде 48 сағат ішінде жедел орналастырылуы мүмкін кибер-сарапшылар тобынан тұратын кибер-әрекеттер тобын (Cyber Action Team, CAT), құрды (FBI, n.d.).

Басқаруға және алмасуға болатын білімнің екі негізгі түрі бар: айқын білім және айқын емес білім. *Айқын білім* - бұл жүйеленген, құжатталған және оңай анықталатын ресми білім (мысалы, құжаттар, сот істері, заңдар және т.б.). Нақты білімді сақтау үшін құрылған *контент басқару жүйелері* киберқылмыстарды мен киберқылмыстарды тергеулер туралы білімді басқара алады, оларды веб-сайт және/немесе іздеуге болатын мәліметтер базасы

арқылы қол жетімді етеді. Мысал ретінде БҰҰ – ның Есірткі және қылмыс жөніндегі басқармасының білім басқармасы порталы (UNODC) - электрондық ресурстарды және қылмысқа қарсы күрес туралы заңдарды тарату (SHERLOC). Бұл порталда өзара құқықтық көмекке (ӨҚК) және беруге қатысты мәселелер бойынша көмек көрсету туралы елдердің өтініштерін алуға, қарауға және оларға жауап беруге уәкілетті құзыретті ұлттық органдар бойынша анықтамалық (ҚҰО бойынша анықтамалық) орналастырылған, сондай-ақ прецеденттік құқық бойынша дерекқор, заңнама туралы дерекқор және библиографиялық дерекқор (UNODC, n.d.). Сонымен қатар, БҰҰ ЕҚБ киберқылмыстылық туралы деректер репозиторийіне (Cybercrime Repository) ие, оған іс жүргізу құқығы, Заңнама және киберқылмыстарды тергеу нәтижелері бойынша жасалған қорытындылар туралы деректер базасы кіреді (UNODC, n.d.). Сондай-ақ, контентті ұлттық басқару жүйелері құрылды. Мысалы, Литвада сот органдарына сот шешімдері мен азаматтық істердің деректер базасына қол жеткізуді қамтамасыз ету үшін Литва соттарының электрондық қызметтер порталы құрылды (Global Cyber Security Capacity Centre, 2017d). Украинада Сот шешімдерінің бірыңғай мемлекеттік тізілімі елде 2006 жылдан бастап қабылданған барлық сот шешімдері мен қаулыларына қол жеткізуге мүмкіндік береді және қол жетімділіктің екі түрі бар іздеуге болатын мәліметтер базасы болып табылады: жалпы (барлығы үшін) және толық (сот органдары үшін). Ұлттық және халықаралық мәліметтер базасы мен репозиторийлер Жеке тұлғаларға осы мәліметтер базасында сақталған айқын білімді іздеуге және алуға мүмкіндік береді, осылайша осындай айқын біліммен алмасуға ықпал етеді.

Айқын білімнен айқын емес білімнің айырмашылығын қарасақ, *айқын емес білім* - бұл оңай анықталмайтын және тәжірибеге негізделген ноу-хау. Айқын емес біліммен бөлісу бұл білімді әлеуметтену арқылы, көбінесе құрылымданбаған түрде бөлісуді білдіреді. Жасырын білімді тәлімгерлік, оқыту және бейресми байланыс арқылы, сондай-ақ оқу бағдарламалары мен семинарлар кезінде бөлісуге болады. Кейбір жағдайларда халықаралық ұйымдар айқын емес біліммен алмасуға баса назар аударады. Мысалы, БҰҰ ЕҚБ прокурорларды, тергеушілерді және құқық қорғау органдарының қызметкерлерін сандық дәлелдемелерді жинау және киберқылмыстарды тергеу жүргізу мәселелері бойынша даярлауды ұйымдастырады. Бұдан басқа, Интерполдың Жаһандық инновациялық кешені (IGCI) киберқылмыстарға трансұлттық тергеулер жүргізуге қолдау көрсетеді (мысалы, киберқылмыстарды тергеуді жүргізу мен киберқылмыстарға қарсы күрес жөніндегі операцияларды үйлестіруді қамтамасыз етеді), құқық қорғау органдары арасында Жедел деректер алмасуға жәрдемдеседі және киберқылмыстардың тергеуі жүргізілуіндегі озық тәжірибелерімен бөліседі (INTERPOL, n.d.). БҰҰ ЕҚБ сияқты, Интерполдың Жаһандық инновациялық кешені киберқылмыстарды және киберқылмыстылық саласындағы үрдістерді тергеу мәселелері бойынша дайындық курстарын ұйымдастырады (мысалы, біліктілікті арттыру курстарын өткізеді және қараңғы желідегі тергеу дағдыларын оқыту бағдарламалары сияқты оқу бағдарламаларын әзірлейді)

(INTERPOL, n.d.). ал Еуропол, Евроәділеттілік, Интерпол және басқа агенттіктердің сарапшылары, мысалы, Қараңғы желідегі тергеу жүргізу кезінде қолданылатын құралдар, тергеу тактикалық тәсілдері мен әдістері туралы айөын емес біліммен бөліседі (Europol, 2018b). Ұлттық деңгейде айқын емес білім алмасу әлі іс жүзінде кең таралмады.

Синхронды (яғни, нақты уақыт режимінде) және асинхронды (мысалы, бейнеконференцбайланыс және файлдарды ортақ пайдалану жүйелері) өзара әрекеттесуге арналған бағдарламалық жасақтама және интерактивті жұмыс кеңістігі (мысалы, ұжымдық жұмыс қатысушылары жүктелген құжаттарды бөлісе алатын, өңдейтін және/немесе түсініктеме бере алатын Google құжаттары) сияқты ақпараттық-коммуникациялық технологиялар (АКТ) құралдары әртүрлі жерлердегі адамдарды біріктіру және айқын емес білім алмасуды жүзеге асыру үшін пайдаланылуы мүмкін. Айқын емес біліммен алмасуға әрекеттесу үшін АКТ-ны қолдану бойынша күш-жігерге қарамастан, бұл тәжірибе халықаралық және ұлттық деңгейлерде кең таралмады. Мысалы, 2017 жылы Литва «киберқылмыстылық бойынша істерді тиімді қудалауды қамтамасыз ету үшін прокурорлар мен судьялар арасында ақпарат пен озық тәжірибе алмасуға мүмкіндік беретін механизм жоқ» деп мәлімдеді (Global Cyber Security Capacity Centre, 2017d, 47 б.).

Талқылауға арналған сұрақтар:

1. Киберқылмыс туралы хабарлама қайда жіберіледі?
2. Сізге киберқылмыс туралы хабарламалар қайда жіберілуі керек екендігі туралы мәлімдеді ма? Олай болса, бұл туралы қашан және кім мәлімдеді?
3. Киберқылмыстар туралы хабарламаларды көтермелеу үшін қандай да бір ұлттық түсіндіру және/немесе ақпараттық кампаниялар өткізіледі ме? Бұл кампаниялар бағаланды ма?
4. Сіздің еліңіздегі киберқылмысты кім тергейді?
5. Әрбір жауапты және киберқылмыстарға тергеу жүргізуге тартылған ведомствоның/субъектінің рөлі қандай?
6. Бұл ведомстволар /субъектілер қандай киберқылмыстарды тергейді?
7. Киберқылмыстарды тергеу үшін Мемлекеттік-жекешелік әріптестік тетіктері бар ма? Олай болса, бұл қандай механизмдер?
8. Киберқылмыскерлерді тергеуде білімді басқарудың қандай да бір әдістері қолданылады ма? Егер иә болса, онда қандай?

6 Тақырып. Киберқылмыстарды тергеудің және сандық криминалистиканың практикалық аспектілері.

1. Құқықтық және этикалық міндеттемелер.

Киберқылмыстардың тергеушілері мен сандық криминалистика мамандары киберқылмыстарды тергеу, сандық дәлелдемелерді өңдеу, талдау және түсіндіру және нәтижелерді ұсыну кезінде құқықтық және этикалық аспектілерді ескеруі керек. Құқықтық міндеттемелер ұлттық, аймақтық және

халықаралық нормалармен белгіленсе де құқықтар этикалық міндеттемелер (барлық қолданылатын жағдайларда) ерікті түрде қолданылады және/немесе мемлекеттік органдармен және/немесе жеке кәсіби ұйымдармен белгіленеді. *Этика кодексі* болған жағдайда (яғни, шешім қабылдау процесінде дұрыс және дұрыс емес мінез-құлықты анықтайтын басқарушы принциптер), ол көбінесе киберқылмыстар бойынша істердің тергеушілері және/немесе сандық криминалистика мамандары барлық жағдайларда не *істеу керектігін* және олар ешқашан *ешқандай жағдайда жасамауы* керек екенін сипаттайды. Мысалы, халықаралық компьютерлер бойынша сот сарапшыларының қоғамы (ISFCE) этика кодексін қабылдады, оның мүшелері стандарттардың сақталуын, сонымен қатар сандық сот сараптамасының нәтижелерінің дәлдігі мен дұрыстығын қамтамасыз ету үшін ұстануы керек. Бұл Этика кодексінде қоғам мүшелері ұстануға тиісті мінез-құлық сипаттамасы (мысалы, заңды ұйғарымдарды сақтау және қолданыстағы заңдарға, стандарттарға, рәсімдерге және басқарушы принциптерге сәйкес дәлелдемелерді жан-жақты зерттеу жүргізу) және тыйым салынған мінез-құлық (мысалы, дәлелдемелерді жасыру, дәлелдемелерді талдау немесе ұсыну кезіндегі біржақтылық және олардың біліктілігі туралы жалған ақпарат беру).

2. Сандық дәлелдемелермен ұқыпты ұстау. Сандық дәлелдемелер тұрақсыз және қысқа мерзімді, сондықтан мұндай дәлелдемелерді ұқыпсыз ұстау олардың өзгеруіне әкелуі мүмкін. Дәлелдемелердің тұрақсыздығы мен сынғыштығына байланысты олармен жұмыс істеу процесінде деректердің өзгеруіне жол бермеу үшін (яғни деректерге қол жеткізу, оларды жинау, буып-түю, беру және сақтау кезінде) хаттамаларды сақтау қажет. Бұл хаттамаларда сандық дәлелдемелермен жұмыс істеу кезінде орындалуы қажет әрекеттер сипатталады. Сандық дәлелдемелермен жұмыс істеудің бастапқы процесі төрт кезеңнен тұрады: сәйкестендіру, жинау, алу және сақтау. *Тұрақсыз дәлелдемелерді* жинауға арналған хаттамалар бар. Тұрақсыз дәлелдемелерді жинау тұрақтылық деңгейінің жоғарылау тәртібімен жүргізілуі керек, яғни ең алдымен тұрақтылық деңгейі төмен дәлелдемелер жиналуы керек, ал тұрақтылық деңгейі жоғары дәлелдемелер соңғы кезекте жиналуы керек. Түсіндірмелер сұрау (RFC) 3227 (Request for Comments (RFC) 3227) деп аталатын құжатта стандартты жүйелер үшін тұрақсыз деректерді жинау тәртібінің келесі мысалы келтірілген (ең аз тұрақтыдан ең тұрақтыға дейін) (Brezinski and Killalea, 2002)

- тізілімдер, кэш;
- бағыттау кестесі, ... мекен-жай протоколы немесе ARP кэш, процестер кестесі, ядро (статистика), жад;
- уақытша файлдарға арналған жүйелер;
- диск;
- қашықтағы журнал деректері және зерттелетін жүйеге қатысы бар мониторинг деректері;
- физикалық конфигурация, желі топологиясы;
- мұрағаттық деректер тасымалдаушысы.

Сәйкестендіру. Сәйкестендіру кезеңінде цифрлық дәлелдемелерді жинау басталғанға дейін жасалған киберқылмыс туралы алдын ала ақпарат алу қажет. Бұл алдын-ала ақпарат дәстүрлі қылмыстық тергеу кезінде жиналғанға ұқсас. Тергеуші киберқылмысқа кім катысты, не болды, киберқылмыс қашан жасалды, киберқылмыс қайда жасалды, киберқылмыс қалай жасалды деген сұрақтарға жауап беруге тырысады. Бұл сұрақтарға жауаптар тергеушілерге істі тергеуді неден бастау керектігіне тұспал береді. Мысалы, «Киберқылмыс қайда жасалды?» - яғни, ол ел аумағында немесе одан тыс жерлерде жасалды ма деген сұраққа жауап. Сәйкестендіру кезеңінде киберқылмыстар бойынша істер тергеушілері көптеген дәстүрлі әдістерін қолданады, әсіресе ақпарат пен дәлелдемелер жинау кезеңінде. Мысалы, тергеліп жатқан киберқылмыс туралы ақпарат пен дәлелдемелер жинау үшін құрбандардан, куәлардан және күдіктілерден жауап алу жүргізіледі. Құқық қорғау органдары киберқылмыскерлердің жеке басын анықтау, іздеу және қылмыстық қудалау мақсатында жасырын тергеу жүргізуде. Сонымен қатар, киберқылмысты тергеуші тергеушілер жасырын бақылау жүргізеді. Мұндай бақылау «жоғары дәрежеде дәлелдемелерді жинаудың интрузивті әдісі болып табылады. Жасырын (жариялы емес) байқауды пайдалану күдіктінің жеке өмірге құқығы мен ауыр қылмыстарды тергеу қажеттілігі арасындағы мұқият тепе-теңдікті талап етеді. Жасырын бақылау туралы ережелер күдіктінің құқықтарын толық ескеруге тиіс. Адам құқықтары жөніндегі халықаралық органдар мен соттар жасырын бақылауға және оның параметрлеріне жол бермеу туралы бірқатар шешімдер қабылдады, олар орындалуы керек». Құқық қорғау органдары киберқылмыс туралы ақпарат пен оның жасалғаны туралы дәлелдемелер жинау үшін зиянды бағдарламаларды бақылау үшін де қолданады. Мысалы, АҚШ-тың құқық қорғау органдары Интернеттегі балаларды жыныстық қанауға және балаларға сексуалдық зорлық-зомбылыққа байланысты істерді тергеуде компьютерлік желілерде (NIT) – «арнайы жасалған эксплойттар немесе зиянды бағдарламаларды» - тергеу әрекеттерін жүргізу әдісін қолданады. Сандық дәлелдемелер жинауды бастамас бұрын тергеуші қажетті шынайы дәлелдемелердің түрлерін анықтауы керек. Сандық дәлелдемелерді компьютерлер, сыртқы қатты дискілер, *флэш-жинақтауыштар*, маршрутизаторлар, смартфондар, планшеттер, камералар, «ақылды» теледидарлар, интернетке шығумен тұрмыстық техника (мысалы, тоңазытқыштар мен кір жуғыш машиналар), ойын қосымшалары (және басқа да көптеген) сияқты сандық құрылғылардан, сонымен қатар жалпыға қолжетімді ресурстардан (мысалы, әлеуметтік желілер платформалары, веб-сайттар және пікірталас форумдары) және жеке ресурстардан (мысалы, интернет-провайдерлердің пайдаланушылардың белсенділігі туралы журналдары; байланыс қызметтері провайдерлерінің іскери құжаттары, пайдаланушы белсенділігі мен пайдаланушы материалдарын тіркейтін бұлтты сақтау провайдерлерінің журналдары) табуға болады. Көптеген қосымшалар, веб-сайттар және сандық құрылғылар бұлтты сақтау қызметтерін пайдаланады. Осылайша, пайдаланушылар туралы деректерді әртүрлі провайдерлер толығымен немесе фрагменттер ретінде бірнеше жерде

серверлерде сақтай алады (БҰҰ ЕҚБ, 2013). Сондықтан осы провайдерлерден деректерді алу міндеті қиын. Шынайы дәлелдемелердің түрі тергеліп жатқан киберқылмысқа байланысты. Егер тергеліп жатқан киберқылмыс - бұл жеке деректерді пайдаланатын алаяқтық болса, онда алынған сандық құрылғылар осы қылмыстың дәлелдерін іздейді (мысалы, алаяқтық транзакциялардың дәлелдемелері).

Жинау. Киберқылмысты тергеу кезінде қылмыс орны киберқылмыскерді жасау үшін пайдаланылған және/немесе киберқылмыскерлердің мақсаты болған сандық құрылғылардың физикалық орналасуымен шектелмейді. Сонымен қатар, киберқылмыстың жасалған жері сандық дәлелдемелерді қамтуы мүмкін, және бірнеше сандық құрылғыларды, жүйелер мен серверлерді қамтитын сандық құрылғылардан тұрады. Киберқылмыс жасау фактісі байқалған, киберқылмыс туралы хабарлама келіп түскен және/немесе киберқылмыс жасады деген күдік болған жағдайларда, қылмыс жасалған жерін күзету бойынша шаралар қабылданады. Алғашқы жауап шараларын атқаратын адам қылмыс жасалған жерін белгілейді, оны ластанудан қорғайды және пайдаланушыларды қылмыс жасалған жерде табылған барлық сандық құрылғылардан оқшаулау арқылы тұрақсыз дәлелдердің сақталуын (мысалы, оларды жеке бөлмеге немесе орынға ауыстыру арқылы) қамтамасыз етеді. Пайдаланушылар сандық құрылғыларды одан әрі пайдалану мүмкіндігінен айырылуы тиіс. Бұл ретте алғашқы жауап шараларын қабылдайтын адам да, тергеуші де тінту және құжаттау процесінде қандай да бір пайдаланушыдан көмек сұрауға тиіс емес. Тергеуші, егер ол алғашқы жауап шараларын қабылдаушы тұлға болмаса, қылмыс жасалған жерді тінтеді және дәлелдемелерді сәйкестендіреді. Дәлелдемелерді жинау басталғанға дейін қылмыс жасалған жері құжатталады. *Құжаттау* бүкіл тергеу процесінде (дәлелдемелерді алғанға дейін, кезінде және одан кейін) қажет болып табылады. Құжаттамада жиналған сандық құрылғылар туралы, оның ішінде құрылғының жұмыс жағдайы, қосулы, өшірулі немесе күту режимінде болғандығы туралы және оның маркасы, моделі, сериялық нөмірі, қосылыстары, кез келген айырым белгілері немесе қандай да бір зақымдануы сияқты физикалық сипаттамалары туралы толық ақпарат болуы керек. Жазбаша жазбалардан басқа, қылмыс орны мен дәлелдемелерді құжаттау үшін қылмыс жасалған жері мен дәлелдемелердің сызбалары, фотосуреттері және/немесе бейнежазбалар қажет. Тұрақсыз деректерді жинау сандық құрылғылардың жад мазмұнын және олардың ішіндегі деректерді өзгерте алады. Тергеуші немесе сарапшы-криминалист дәлелдемелерді жинайды. Рәсімдер сандық құрылғының түріне, сонымен қатар сандық дәлелдемелер орналасқан қоғамдық және жеке ресурстарға (мысалы, компьютерлер, телефондар, әлеуметтік желілер және бұлтты сақтау; мультимедиялық, бейне және мобильді құрылғыларға) байланысты өзгереді (сандық сот сараптамасының әртүрлі практикалық әдістерімен танысу үшін сандық дәлелдемелер бойынша ғылыми жұмыс тобының веб-сайты (Scientific Working Group on Digital Evidence (SWGDE) қараңыз). Құқық қорғау органдары мобильді құрылғыларда, Интернетке қол жетімді объектілерде (мысалы, сағат,

фитнес мониторлары және тұрмыстық техника), бұлтты сақтау және әлеуметтік желілер платформаларында сандық дәлелдемелермен жұмыс істеу кезінде орындалатын әрекеттерді егжей-тегжейлі сипаттайтын *стандартты операциялық процедураларды* қолданады. Стандартты жедел рәсім (СЖР) тергеушілерге көмек көрсетуге арналған, өйткені ол киберқылмысты тергеу кезінде осылайша сотта жиналған дәлелдемелердің жарамдылығын қамтамасыз ету үшін сақталуы керек әдістер мен әрекеттер тізбегін сипаттайды; сонымен қатар тергеу жүргізу үшін қажетті құралдар мен басқа ресурстарды сипаттайды. Осылайша, СЖР тергеу жүргізу кезінде сақталуы қажет рәсімдердің сипаттамасын қамтиды.

Тергеушілер тергеу барысында кездесетін ерекше шектеулерді анықтау қажет. Мысалы, киберқылмысты тергеу кезінде тергеушілер көптеген сандық құрылғылармен, операциялық жүйелермен және күрделі желілік конфигурациялармен жұмыс істеуі мүмкін, бұл арнайы білімді, дәлелдемелер жинау процедураларын өзгертуді және жүйелер мен құрылғылар арасындағы қосылыстарды (мысалы, желілік топология) анықтауға көмектесуді қажет етеді. Тергеу барысында тергеуші сонымен қатар стеганография сияқты *криминалистикаға қарсы* әдістерге тап болуы мүмкін (яғни, хабарлама мазмұны жасырылған және көрінбейтін болған кезде құпия деректерді жасыру) және *шифрлау* (яғни «парольді пайдалану арқылы немесе файлды немесе файл элементтерін жарамсыз күйге келтіру арқылы үшінші тараптың файлға кіруін физикалық блоктауы»). Сондықтан тергеуші осындай жағдайларға дайын болуы керек және осы шектеулерді жою үшін қажетті адами және техникалық ресурстарға ие болуы керек. Тергеушінің мұндай жағдайларда жасайтын әрекеттері (мысалы, тергеушінің осы құрылғыларға пароль алу және/немесе шифрық файлдарды таратып жазу қабілеті), егер олар мүлдем қабылданса, ұлттық заңдарға байланысты болады. Сандық криминалистика құралдары мұндай жағдайларда пайдалы болып, мысалы, стеганографияны анықтауға және файлдарды таратып жазуға, сонымен қатар сандық сот сараптамасының басқа да маңызды міндеттерін орындауға көмектеседі. Мұндай құралдардың мысалына AccessData, Volatile Framework, X-Ways Forensics шығарған Forensic Toolkit (FTK) сияқты компьютерлік сараптама жүргізуге арналған бағдарламалық қамтамасыз ету кіреді. Осы ресурстармен қатар, қылмыс жасалған жерін құжаттау үшін пайдаланылатын заттар, құрылғыларды бөлшектеу және қылмыс орнынан басқа дәлелдерді алып тастау үшін қажетті құралдар, сондай-ақ дәлелдемелерді белгілеу және орау үшін қажетті материалдар (мысалы, смартфондарды тасымалдау үшін Фарадейдің экрандау сөмкесі қолданылады, ол сандық құрылғымен сымсыз сигналдарды қабылдауды және беруді блоктайды, және қуат зарядтағыш құрылғысы) және басқа құралдар. Дәлелдемелерді жинау процесі тұрақсыз дәлелдемелерді сақтауды және сандық құрылғылардың қуатын өшіруді қамтиды. Табылған сандық құрылғылардың жұмыс жағдайы дәлелдемелерді жинау рәсімдерін белгілейді. Мысалы, егер компьютер қосулы күйде табылса, тұрақсыз дәлелдемелер (мысалы, уақытша файлдар, регистр, кэш, желі күйі, қосылымдар және т.б.) қуат өшіріліп, компьютер алынғанға дейін сақталады.

Егер құрылғы өшірулі болса, ол өшірулі күйде қалады және алып қойылады. Сандық құрылғыларды алып қоюға болмайтын жағдайлар бар (мысалы, жүйелердің мөлшері және/немесе күрделілігі және/немесе олардың аппараттық және бағдарламалық жасақтамасының конфигурациясы, өйткені бұл жүйелер аса маңызды қызметтерді қамтамасыз етеді). Мұндай жағдайларда тұрақсыз және тұрақты деректер *нақты уақыт режимінде деректерді жинауды* қажет ететін арнайы процедураларды қолдана отырып жиналады. Жұмыс істеп тұрған жүйелерден тұрақсыз деректерді алу үшін арнайы командаларды қолдануға болады. Мысалы, Windows операциялық жүйелері үшін *ipconfig* командасы желі туралы ақпарат алу үшін қолданылады, ал Unix операциялық жүйелері үшін *ifconfig* командасы қолданылады. Windows үшін де, Unix үшін де белсенді желілік қосылыстар туралы ақпарат алу *netstat* пәрмені қолданылады. Сондай-ақ, цифрлық құрылғылардың іске қатысы бар басқа заттарды (мысалы, парольдер немесе желілік есептік деректер, телефондар, факсимильдік аппараттар, принтерлер, маршрутизаторлар және т.б. туралы өзге де ақпаратты қамтуы мүмкін жазбалар және/немесе дәптерлер) жинауы қажет. Тергеушінің дәлелдемелерді жинау кезінде жасаған әрекеттері құжатталуы керек. Әрбір құрылғы таңбалануы (жалғағыш кәбілдермен және желілік шнурлармен бірге), буып-түйілуі және цифрлық сот сараптамасы зертханасына жіберілуі тиіс. Заттарды зертханаға тасымалдағаннан кейін олар «түгенделеді, тіркеледі және... экстремалды температурадан, ылғалдылықтан, шаңнан және басқа да ықтимал ластағыштардан қорғалған жабылатын үй-жайға сақтауға беріледі".

Алу. Дәлелдемелер алудың әртүрлі әдістері бар. Қолданылатын әдіс сандық құрылғының түріне байланысты. Мысалы, компьютердің қатты дискісінен дәлелдер алу процедурасы смартфондар сияқты мобильді құрылғылардан сандық дәлелдер алу процедурасынан өзгеше.

Деректерді нақты уақытта жинау жүзеге асырылатын жағдайлардан басқа, дәлелдемелер сот сараптамасы зертханасында алынған цифрлық құрылғылардан алынады (яғни *деректерді статикалық режимде жинау* жүзеге асырылады). Сот сараптамасы зертханасында сандық дәлелдер дәлелдердің тұтастығын сақтау үшін (деректердің өзгермеуін қамтамасыз ету), яғни *криминалистика тұрғысынан сенімді түрде* алынуы керек. Ол үшін сандық дәлелдер алу үшін қолданылатын құралдар мен әдістер деректердің өзгеруіне жол бермеуі керек немесе мүмкін болмаған кезде, кем дегенде, өзгерістерді азайту керек. Пайдаланылған құралдар мен әдістер негізделген және сенімді болуы керек. Осы құралдар мен әдістерді қолданар алдында олардың мүмкіндіктерінің шегін анықтап, ескеру қажет. АҚШ-тың Ұлттық стандарттар және технологиялар институтын әртүрлі функционалдығы бар құралдарды сипаттайтын сандық криминалистика құралдарының (digital forensics tools database) мәліметтер базасына (мысалы, бұлтты сақтау сот-сараптамалық құралдары және т. б.) ие.

Алынған сандық құрылғылар дәлелдемелердің негізгі көзі болып саналады. Сандық криминалистика бойынша сарапшы деректерді бастапқы көзден алмайды. Оның орнына осы құрылғының мазмұнының көшірмесі

жасалады және сарапшы көшірмемен жұмыс істейді. Сандық құрылғы мазмұнының көшірмесі (бұл процесс *бұрмаланбаған кескін жасау* деп аталады) сандық дәлелдердің тұтастығын сақтау үшін статикалық режимде деректерді жинау басталғанға дейін жасалады. Көшірменің түпнұсқаның дәл көшірмесі екенін анықтау үшін криптографиялық хэш функциясының мәні математикалық есептеулерді қолдану арқылы есептеледі; егер түпнұсқа мен көшірме үшін хэш функциясының мәндері сәйкес келсе, онда көшірменің мазмұны түпнұсқа мазмұнының айнадағы бейнесі (яғни көшірме) болып табылады. Көшіру процесінде деректердің өзгеруін болдырмауға арналған *жазба блокаторын* көшіру кезінде деректердің өзгеруіне жол бермеу үшін мүмкін болған барлық жағдайларда деректерді шығармас бұрын пайдалану керек. Жоғарыда сипатталған деректерді алу процесі негізінен компьютерлерге қолданылатындығын ескерген жөн. Ұялы телефондардан және оларға ұқсас құрылғылардан деректерді алған кезде, жад құрылғыдан физикалық түрде бөлінбеуі мүмкін, бұрмаланбаған бейнені жасау үшін басқа процедура қолданылады. Деректерді шығарудың екі әдісі бар: физикалық және логикалық. Физикалық шығару сандық құрылғыдағы дәлелдер сақталатын жерден, мысалы, компьютердің қатты дискісінен дәлелдер іздеуді және алуды қамтиды (Maras, 2014). Физикалық шығару *кілт сөздер бойынша іздеуді* (тергеуші ұсынған терминдер негізінде), *біртекті деректер массивін бөлу* әдісін (яғни «жоғарғы және төменгі деректемелер мен басқа идентификаторлар негізінде» іздеу) және бөлінбеген кеңістікті (яғни «жүйедегі бос болып табылатын кеңістік ешқашан қолданылмағандықтан немесе одан алынған ақпарат жойылғандықтан»; Maras, 2014, p. 36) және қатты дискінің сегменттерін бір-бірінен бөлетін бөлімдерді зерттеу арқылы жүзеге асырылуы мүмкін (Maras, 2014). Логикалық үзінді «қатты диск сияқты деректер тасымалдаушысында сақталатын файлдардың атаулары мен орналасқан жерлерін бақылау үшін қолданылатын компьютерлік операциялық жүйенің файлдық жүйесіне қатысты орналасқан жерден дәлелдер іздеуді және алуды қамтиды» (Maras, 2014, p. 36). Логикалық шығару әдісі сандық құрылғыға, файлдық жүйеге, құрылғыдағы қосымшаларға және амалдық жүйеге байланысты. Логикалық шығару белсенді және жойылған файлдардан, файлдық жүйелерден, бөлінбеген және пайдаланылмаған кеңістіктен, сондай-ақ сығылған, шифрланған және парольмен қорғалған деректерден деректерді алуды қамтиды. Дәлелдемелерді алудың барлық процесі құжатталуы керек. Бұл ретте, құжаттама дәлелдемелер алынған цифрлық құрылғылар, дәлелдемелерді алу үшін пайдаланылған аппараттық және бағдарламалық қамтамасыз ету, дәлелдемелер алынған тәсіл (яғни, олар қалай алынғандығы туралы), сондай-ақ қашан, қайда және неге алынғандығы, қандай дәлелдемелер алынғандығы және олар қандай себептермен алынғандығы туралы.

Сақтау. Дәлелдемелерді сақтаудың мақсаты - сандық дәлелдемелерді өзгерістерден қорғау. Сандық дәлелдемелердің тұтастығы сандық дәлелдемелермен жұмыс істеудің әрбір кезеңінде сақталуы тиіс (ИСО/МЭК 27037). Алғашқы жауап шараларын қабылдайтындар, тергеушілер, қылмыс

орнын зерттейтін сарапшылар және/немесе сандық криминалистика сарапшылары сәйкестендіру, жинау және алу кезеңінде сандық дәлелдемелер өзгермегенін мүмкіндігінше көрсетуі керек; мұны көрсету мүмкіндігі, әрине, сандық құрылғыға (мысалы, компьютер мен ұялы телефондарға) және олардың жағдайларына байланысты (мысалы, деректерді тез сақтау қажеттілігі). Ол үшін *дәлелдемелерді қорғау жүйесін* сақтау қажет. *Дәлелдемелерді қорғау жүйесі* - бұл «тергеушілер іс бойынша іс жүргізудің бүкіл кезеңінде қылмыс (немесе оқиға) орны мен дәлелдемелердің сақталуын қамтамасыз ететін процесс. Тіркеу журналына дәлелдемелерді жинауды кім жүзеге асырғаны, олардың қайда және қалай жиналғаны, бұл дәлелдемелерді қандай адамдар алғаны және оларды қашан алғаны туралы ақпарат енгізіледі». Дәлелдемелерді қорғау жүйесінде жүргізілетін құжаттарда дәлелдемелерді анықтаған, жинаған және алған адамдардың, сондай-ақ дәлелдемелер берілген кез келген басқа адамдардың аты-жөндері, лауазымдары және байланыс ақпараты, осы адамдарға берілген дәлелдемелер туралы егжей-тегжейлі ақпарат, беру уақыты мен күні, сондай-ақ беру мақсаты көрсетілуі керек.

Талдау және есеп беру. Сандық дәлелдемелермен жұмыс істеу кезеңінен басқа, цифрлық сот сараптамасы процесі сандық дәлелдемелерді (*талдау* кезеңін) зерделеуді және түсіндіруді және талдау нәтижелерін (*есептілік* кезеңін) ұсынуды да көздейді. *Талдау* кезеңінде құрылғыдан сандық дәлелдер алынады, деректер талданады және оқиғалар қайта құрылады. Сандық дәлелдемелерді талдау басталғанға дейін зертханадағы сандық криминалистика жөніндегі сарапшы іздеу мақсаттары туралы хабардар болып, тергеліп жатқан іс туралы анықтамалық сипаттағы кейбір мәліметтерді және тергеу барысында алынған кез-келген басқа ақпаратты алуы керек, бұл сот сарапшысына осы кезеңде көмектесе алады (мысалы, IP-мекенжайы немесе MAC-мекенжайлары). Қажетті сандық дәлелдемелердің түріне байланысты талдаудың әртүрлі түрлері қолданылады, мысалы, желіні, файлдық жүйені, қосымшаны, бейнематериалдарды, суреттерді және тасушыны талдау (яғни, сақтау құрылғысындағы деректерді талдау). Файлдар олардың шығу тегін анықтау үшін талданады, сонымен қатар бұл деректердің қашан және қайда жасалғанын, өзгертілгенін, қашан және қайдан шыққанын, қашан және қайда жүктелгенін немесе түсірілгенін және сақтау құрылғыларындағы осы файлдардың, мысалы, бұлтты сақтау сияқты қашықтағы сақтау орнына қосылуын анықтау үшін талданады. Қажетті сандық дәлелдемелердің түрі (мысалы, электрондық хаттар, мәтіндік хаттар, геолокация, мәтіндік редактор құжаттары, суреттер, бейнелер және чат журналдары) киберқылмыстың нақты түріне байланысты.

Компьютерлерде жасалатын талдаудың төрт негізгі түрі бар: уақыт шеңберін талдау; меншік пен иеленуді талдау; қосымшалар мен файлдарды талдау; және деректерді жасыру әдісін талдау. *Уақыт шеңберін талдаудың* мақсаты - оқиғаға әкелген уақыт белгілерін (күн мен уақыт) қолдана отырып, уақыт шкаласын немесе уақыт тізбегін құру немесе пайдаланушы белгілі бір әрекетті жасаған уақыт пен күнді белгілеу (US National Institute of Justice, 2004b). Мұндай талдау қылмысты оның орындаушысының есебіне жатқызу

немесе, кем дегенде, қылмысқа әкеп соққан әрекетті белгілі бір адамның есебіне жатқызу мақсатында жүргізіледі (US National Institute of Justice, 2004b); алайда уақыт шеңберін талдау нәтижелерін тексеруге байланысты белгілі бір қиындықтар бар. *Меншік пен иеленуді* талдау компьютерлік жүйеде файлдарды жасаған, оларға қол жеткізген және/немесе өзгерткен адамды анықтау үшін қолданылады (US National Institute of Justice, 2004b). Мысалы, мұндай талдау күдіктінің құрылғысында балалардың жыныстық зорлық-зомбылық көріністері бар материалдарды анықтауға көмектеседі. Бұл ақпараттың өзі балаларға жыныстық зорлық-зомбылық көріністері бар материалдардың иесі кім екенін дәлелдеу үшін жеткіліксіз. Бұл үшін қосымша дәлелдер қажет, мысалы, материалдар табылған компьютерді ерекше пайдалану фактісі. *Қосымшалар мен файлдарды талдау* компьютерлік жүйедегі қосымшалар мен файлдарды зерттеу үшін, қылмыскердің киберқылмыс жасауына қатысты алдын-ала көрінеу, ниетін және мүмкіндігін анықтау үшін жасалады (мысалы, жапсырма немесе файл атауы файлдың мазмұнын көрсетуі мүмкін; атап айтқанда, файл атауы киберқылмыскердің аты болуы мүмкін). Сондай-ақ, *деректерді жасыру әдісін талдауды* қолдануға болады. Атауынан көрініп тұрғандай, деректерді жасыру әдісін талдау жүйеде жасырын деректерді іздеуді қамтиды. Қылмыскерлер өздерінің заңсыз әрекеттері мен сәйкестендіретін ақпаратын жасыру үшін деректерді жасырудың бірнеше әдісін қолданады, мысалы, шифрлау әдісін қолдану арқылы. Талдаудың бұл түрлерінің мақсаты - *қылмысты қайта құру* (немесе оқиғаларды қайта құру). Оқиғаларды қайта құру оқиғаға кім жауапты екенін, не болғанын, қай жерде болғанын, қашан болғанын және деректерді анықтау, сәйкестендіру және байланыстыру арқылы қалай дамығанын анықтау үшін жүзеге асырылады («жалпы суретті» немесе оқиғаның мәнін ашу үшін). Оқиғаларды қайта құру процесі *уақыт талдауды* (яғни оқиғалардың уақыты мен реттілігін белгілеу), *реляциялық талдауды* (яғни, оқиғаларға қатысушыларды, олардың әрекеттерін, сондай-ақ олардың арасындағы байланыстар мен қатынастарды анықтау) және *функционалды талдауды* (яғни, оқиғалар кезінде қолданылатын жүйелер мен құрылғылардың өнімділігі мен мүмкіндіктерін бағалау) қамтуы мүмкін. Тергеушілер дәлелдемелерді анықтау және жинау кезеңдерінде оқиғаларды қайта құру бойынша алдын-ала шараларға қатысуы керек. Осы мақсаттарды орындау тергеушілерге сандық дәлелдемелердің жаңа ықтимал көздерін анықтауға көмектеседі. Сайып келгенде, талдау кезеңіндегі оқиғаларды қайта құру үшін қолда бар дәлелдемелер мен осы дәлелдемелерді талдау нәтижелері негізінде тергеп-тексерілетін іске қатысты қорытындылар шығару үшін толық емес білім пайдаланылады. Сондықтан киберқылмыс тергеушілері мен сандық криминалистика сарапшылары мұндай шектеулерді мойындап, талдау нәтижелерін *алдын-ала түсіндіруден* аулақ болу керек, мысалы, адамдар өздерінің жұмыс гипотезасын растайтын нәтижелерді іздейтін және қолдайтын және жұмыс гипотезасына қайшы келетін нәтижелерді қабылдамайтын *растау біржақтылығы* салдары болып табылатын түсіндірулер. Талдау нәтижелері есепте құжатталады. Есептер максималды

нақты және дәл болуы керек. Олар суретті материалдарды (мысалы, суреттер, кестелер, құралдардың шығыс деректер) және дәлелдемелерді қорғау жүйесінің құжаттамасы сияқты қосалқы құжаттарды, сондай-ақ деректерді зерттеу және алу үшін қолданылған әдістер мен әрекеттерді егжей-тегжейлі түсіндіруді қамтуы керек (US National Institute of Justice, 2004b). Нәтижелер талдау мақсаттарын (яғни тергеу және тергеу ісінің мақсаттары) ескере отырып түсіндірілуі тиіс. Алынған нәтижелердің шектеулілігі туралы ақпарат есепке де енгізілуі тиіс. Есептің мазмұны юрисдикцияға және тергеулер мен сандық криминалистикаға қатысты ұлттық саясатқа (егер бар болса) байланысты өзгереді. Сандық дәлелдемелердің қате түсіндірілуін немесе дұрыс емес салмақтық мәнін анықтауды болдырмау үшін есепте белгілі қателер мен нәтижелердің белгісіздігі туралы айтылуы тиіс.

3. Сандық дәлелдемелердің жарамдылығы. Сандық дәлелдердің жарамдылығын қамтамасыз ету үшін сотта белгілі бір құқықтық және техникалық талаптар орындалуы керек. Құқықтық талаптарға келетін болсақ, сот ақпараттық-коммуникациялық технологиялар құрылғыларын және олармен байланысты деректерді іздеуге және алуға заңды рұқсаттың болуы, сондай-ақ іске қатыстылығы, түпнұсқалығы, тұтастығы және сандық дәлелдемелердің сенімділігі сияқты мәселелерді қарастырады. Техникалық талаптарға сәйкестігін қарау кезінде сот сандық дәлелдемелерді алу, сақтау және талдау үшін пайдаланылған сандық криминалистика рәсімдері мен құралдарын; талдаулар жүргізілетін сандық сот сараптамасы зертханаларын; сандық криминалистика бойынша сарапшылардың есептерін; сандық криминалистика бойынша сарапшылар мен сарапшы куәгерлердің академиялық және кәсіби-техникалық біліктіліктерін сыни бағалайды (қажет болған жағдайда). 2017 жылы Антви-Боасиако (Antwi-Boasiako) және Вентер (Venter) *сандық дәлелдемелердің жарамдылығын бағалаудың бірыңғай моделі* (Harmonized model for Digital Evidence Admissibility Assessment (HM-DEAA) деп аталатын құрылымды жасады, оған дәлелдердің жарамдылығын анықтайтын негізгі техникалық және құқықтық талаптар кіреді. Атап айтқанда, HM-DEAA моделі дәлелдемелердің жарамдылығын бағалаудың үш кезеңін, соның ішінде сандық дәлелдемелердің жарамдылығын бағалау, қарау және шешім қабылдау кезеңдерін қарастырады. HM-DEAA моделі ұлттық соттарда сандық дәлелдемелердің жарамдылығын қамтамасыз ету үшін әртүрлі юрисдикцияларда кеңінен қолданылатын құқықтық және техникалық талаптарды егжей-тегжейлі көрсетуінде өзінің ролін атқарады.

Сандық дәлелдемелерді бағалау. Бұл кезеңде соттар ақпараттық-коммуникациялық технологиялар (АКТ) құрылғыларын және олармен байланысты деректерді тінтуді жүргізуге және алып қоюға тиісті заңды рұқсаттардың пайдаланылғанын анықтайды. Заңды рұқсаттарға тінту ордері, соттың үйғарымы немесе сотқа шақыру қағазы жатады. АКТ құрылғыларын және олармен байланысты деректерді алып тастау үшін қажетті заңды құжаттың түрі юрисдикцияға байланысты өзгереді және ұлттық заңмен анықталады. Бұл кезеңде сандық дәлелдемелердің маңыздылығы криминалистика тұрғысынан да бағаланады. *Криминалистика тұрғысынан*

сандық дәлелдемелердің *маңыздылығы*: қылмыскер мен нысана (мысалы, жәбірленуші, сандық құрылғы, веб-сайт және т. б.) және/немесе қылмыс орны (қылмыс немесе киберқылмыс жасалған орын) арасындағы байланысты орнатуға немесе алып тастауға; қылмыскердің, жәбірленушінің және/немесе куәгердің айғақтарын растауға немесе жоққа шығаруға; киберқылмысты орындаушының (орындаушылардың) жеке басын анықтауға; тергеу нұсқаларын ұсынуға мүмкіндік беруде; қылмыскер қолданған әрекет әдісі (қылмыс жасау әдісі (modus operandi немесе M.O.) туралы ақпарат алуды қамтамасыз етуде (яғни, қылмыскердің әдеттері, әдістері мен мінез-құлық ерекшеліктері туралы); және қылмыстың шынымен болғанын көрсетуімен белгіленеді. Сандық дәлелдемелер зиянды бағдарламаны жасаушылар мен хакерлер сияқты киберқылмыскерлердің мінез-құлқына (қолжазбаларына) тән белгілерді анықтауға көмектеседі. *Қылмыскердің қолжазбасы* - белгілі бір дереккөзге жатқызуға болатын және киберқылмыскерге белгілі бір психологиялық немесе эмоционалды қанағаттануды (мысалы, әріптестерінің мақұлдауы мен мойындауы) қамтамасыз ететін іс-әрекеттің танылатын және ажыратылатын сипаты (мысалы, нақты әдістер, құралдар және лақап ат).

Сандық дәлелдемелерді қарастыру. Бұл кезеңде сандық дәлелдемелердің тұтастығы дәлелдемелер алу үшін қолданылатын сандық сот сараптама процедуралары мен құралдарды, сандық дәлелдемелерді алған, сақтаған және талдаған сандық сот-сарапшылардың құзырлығы мен біліктілігін және сандық дәлелдемелерді зерттеген сот-зертханаларды зерттеу арқылы бағаланады. Шын мәнінде, мұндай бағалаудың мақсаты - сандық дәлелдемелерді сақтау, алу және талдау үшін ғылыми принциптердің қолданылғанын және сандық дәлелдермен жұмыс жасау және оларды зерттеу кезінде стандарттардың сақталғанын анықтау (мысалы, сандық сот-медициналық құралдар аттестацияланған ба, олар заманауи ма, олар дұрыс сақталған ба және олардың дұрыс жұмыс істеуін қамтамасыз ету үшін қолданар алдында сыналған ба).

Сандық криминалистика бойынша сарапшылар сотта өздерінің біліктілігі туралы айтып, келесі сұрақтарды түсіндіру үшін куәлік береді: сандық құрылғылар, Интернет-платформалар және АКТ-мен байланысты басқа көздер қалай жұмыс істейді; сандық сот сараптамасы процесі; басқа құралдар емес, осы сандық криминалистика құралы не үшін қолданылды; сандық дәлелдемелер қалай сақталды, алынды және талданды; талдау нәтижелерін түсіндіру және осы түсіндірулердің дәлдігі; және кез-келген деректер өзгерістері және олар не үшін орын алды.

Сандық дәлелдемелердің рұқсат етілуіне қатысты шешім қабылдау. Бұл кезеңде сандық дәлелдердің түпнұсқалығы, тұтастығы және сенімділігі алдыңғы кезеңде жүргізілген сандық сот-сараптама процедураларын бағалау нәтижелері негізінде бағаланады (яғни, *сандық дәлелдемелерді қарау* кезеңінде); мысалы, сандық дәлелдемелер алу үшін криминалистика тұрғысынан сенімді әдістер мен құралдарды қолдану, осы дәлелдердің түпнұсқалығын, тұтастығын және дұрыстығын растау үшін сарапшы куәгерлер мен сандық сот-сараптама сарапшыларының айғақтары бағаланады. Сандық дәлелдеме, егер ол істің нақты мән-жайларын белгілесе, сандық сот

сараптамасының бүкіл процесі бойында өзгеріссіз қалса, ал сараптама нәтижелері шынайы, сенімді болып табылса және сараптамалық бағалаудан өтсе, жарамды болып табылады . Нәтижелер жарамды деп танылуы үшін олар объективті түрде түсіндірілуі керек және нәтижелердегі қателіктер мен белгісіздіктер, сондай-ақ нәтижелерді түсіндірудегі шектеулер туралы ақпарат ашылуы керек.

Осылайша, бұл үш сатылы модель әртүрлі юрисдикцияларда дәлелдемелердің жарамдылығына қатысты жалпы құқықтық және техникалық талаптарды біріктіреді. Сандық сот сараптама тәжірибесін стандарттау әр түрлі елдерде сандық дәлелдемелердің жарамдылығын қамтамасыз етудің кілті болып табылады. Киберқылмыстылықтың трансұлттық сипатын ескере отырып, сандық сот сараптамасын жүргізудің тәжірибелік әдістерін біріздендіру киберқылмыстарды тергеу үшін ғана маңызды емес, сонымен қатар киберқылмыстылықпен байланысты істер бойынша халықаралық ынтымақтастықты жүзеге асыру үшін қажет.

Талқылауға арналған сұрақтар:

1. СЖР-ға не енгізілді?
2. Сандық дәлелдемелермен жұмыс істеудің қандай рәсімдері қамтылды?
3. Тергеу барысында туындауы мүмкін қандай да бір ерекше шектеулер СЖР-да қамтылды ма? Егер иә болса, онда қандай?
4. Сандық криминалистика бойынша сарапшылардың біліктілігіне қандай талаптар қойылады? Бұл біліктілік бағаланады ма? Олай болса, қалай?
5. Неліктен сандық криминалистика бойынша білікті мамандарды тарту қажет?

7 Тақырып. Киберқылмыстылықпен күресу саласындағы халықаралық ынтымақтастық.

1. Егемендік және юрисдикция. *Аумақтық егемендік* мемлекеттің өзінің географиялық аумағына қатысты құқықтары мен өкілеттіктерін толық және айрықша жүзеге асыруын білдіреді. Егемендікті қорғау киберқылмыстылықпен күрес саласындағы халықаралық және аймақтық құқықтық актілерде көрнекті орын алады. Мысал ретінде 2010 жылғы Араб мемлекеттері лигасының ақпараттық технологияр саласындағы қылмыстарымен күресу туралы конвенциясын келтіруге болады. Атап айтқанда, осы конвенцияның 4-бабында былай делінген: «Әрбір қатысушы мемлекет өз заңдарын немесе конституциялық қағидаларын басшылыққа ала отырып, осы конвенция бойынша өз міндеттемелерін мемлекеттердің егемендік теңдігі мен аумақтық тұтастығы қағидаларына және басқа мемлекеттердің ішкі істеріне араласпау қағидасына сәйкес орындауға міндеттенеді».

Аумақтық егемендік киберкеңістікке, атап айтқанда, мемлекеттердің ақпараттық-коммуникациялық технологияларының (АКТ) инфрақұрылымына

таралуы мүмкін. Үшінші тұлғалар шет мемлекеттердің АКТ-сына және/немесе АКТ орналасқан мемлекеттің хабарсыз және рұқсатынсыз және/немесе оның құқық қорғау органдарының рұқсатсыз рұқсат етілмеген қол жеткізген кезде мемлекеттің егемендігі бұзылуы мүмкін. Егер мұндай рұқсат етілмеген қол жеткізу басқа елде жасалған киберқылмысты тергеудің шеңберінде жүзеге асырылса да, бұл ел кибершабуылдың көзін анықтауға және/немесе оның жасалуын болдырмауға тырысса да, егемендік бұзылған болып саналады (*кері бұзу* немесе *хакерлерге қарсы шабуыл* ретінде белгілі тактика).

Егемендікпен байланысты юрисдикция (БҰҰ ЕҚБ, 2013, 9-ескертпе, 205б.) мемлекеттерге өз аумағындағы адамдардың міндеттері мен құқықтарын анықтау және сақтау, заңнаманы орындау және заңды бұзғаны үшін жазалау құқығы мен өкілеттігін қамтамасыз етеді. Мемлекеттер бірінші кезекте өз аумағында жасалған қылмыстарға өзінің юрисдикциясын жариялайды (аумақтық қағида). 2001 жылғы Киберқылмыстар туралы Еуропа Кеңесінің Конвенциясының 22(1) бабында былай делінген: «Әрбір Тарап осы Конвенцияда көзделген кез келген қылмысқа қатысты юрисдикцияны белгілеу үшін қажетті заңнамалық және басқа да шараларды қабылдайды, егер мұндай қылмыс … оның аумағында … жасалған болса». Дегенмен, Бреннер мен Купс (Brenner and Koops, 2004) дұрыс атап өткендей, «бір елде қылмыс жасалды ма, жоқ па, соны анықтау, алайда, қылмыс киберкеңістікті пайдаланумен байланысты болған кезде өте қиын міндет болып табылады» (10 б.).

Киберқылмыстарға қатысты юрисдикция құқық бұзушының азаматтығы (азаматтық қағидасы; белсенді тұлғалық қағида), жәбірленушінің азаматтығы (азаматтық қағидасы; пассивтік тұлғалық қағида) және киберқылмыстың мемлекет мүдделері мен қауіпсіздігіне салдары (қорғау қағидасы) сияқты басқа факторлармен анықталады, егер киберқылмыс пен юрисдикцияны жүзеге асыратын мемлекет арасында «жеткілікті немесе шынайы байланыс» болса ғана» (БҰҰ ЕҚБ, 2013, 206 б. цитата жасалынған). Мысалы, Ұлыбританияда апелляциялық сот R v. Sheppard and Anor (2010 ж.) ісінде 1986 жылғы «Қоғамдық тәртіп туралы» заңның ережелерін АҚШ серверінде орналастырылған веб-сайтта жарияланған нәсілдік арандатушы материалдарға қолдану туралы шешімді және осы материалдарды жариялағаны үшін Ұлыбританияның екі тұрғынына қатысты соттау үкімін күшінде қалдырды.

Киберқылмыстарға қатысты юрисдикция киберқылмыстылық туралы ұлттық заңнамаға сәйкес белгіленеді. Мысалы, Малайзияда 1997 жылғы «Компьютерлік қылмыстар туралы» заңы мемлекеттің киберқылмыстарға қатысты юрисдикциясын бекітті. Атап айтқанда, осы Заңның 9-бабында «осы Заңның кез келген адамға қатысты ережелері оның азаматтығына немесе бодандығына қарамастан, Малайзия аумағында да, одан тыс жерлерде де, сондай-ақ кез келген адам Малайзиядан тыс жерде осы Заңмен белгіленген қылмыс жасаған жағдайда, ол адам Малайзияның кез келген жерінде қылмыс жасағандай жауапкершілікке тартылуы мүмкін». Салыстыру үшін, Танзания киберқылмысқа қатысты өзінің юрисдикциясын келесы жағдайларда жариялайды: қылмысты құрайтын әрекет немесе әрекетсіздік Танзания

Біріккен Республикасының аумағында толық немесе ішінара жасалған кезде; ... Біріккен Танзания Республикасында тіркелген теңіз немесе әуе кемесінің бортында жасалған кезде; ... Біріккен Танзания Республикасының азаматы жасаса; ... егер әрекет немесе әрекетсіздік осы елдің заңнамасына сәйкес тең дәрежеде қылмыс болса, Біріккен Танзания Республикасынан тыс жерде тұратын Біріккен Танзания Республикасының азаматы жасаса; немесе ... азаматтығына, бодандығына немесе қылмыс болған жерге қарамастан кез келген адам жасаса... Танзания Біріккен Республикасының аумағында орналасқан компьютерлік жүйені, құрылғыны немесе деректерді пайдалана отырып қылмыс жасаса немесе ... қылмыс компьютерлік жүйеге, құрылғыға немесе деректерге не Танзания Біріккен Республикасындағы адамға қатысты жасалынса (2015 жылғы «Киберқылмыстар туралы» Заңының 30 бабы).

Бұл ретте Кения киберқылмыстарға қатысты өзінің юрисдикциясын былайша белгілейді: «Кениядан тыс жерде жасалған, егер Кенияда жасалған болса, осы Заңға сәйкес қылмыс болып табылатын әрекет немесе әрекетсіздік Кенияда жасалған болып саналады, егер - ... әрекет немесе әрекетсіздік жасаған адам... Кения азаматы болып табылса; немесе ... тұлға әдетте Кенияда тұрса; және ... әрекет немесе әрекетсіздік ... Кения азаматына қарсы жасалса;... Кениядан тыс Кения үкіметіне тиесілі мүлікке қарсы жасалса; немесе ... Кения үкіметін қандай да бір әрекеттер жасауға немесе оларды жасаудан бас тартуға мәжбүрлеу үшін жасалса; немесе ... әрекет немесе әрекетсіздік жасаған адам оны жасағаннан кейін Кения аумағында болса» (2018 жылғы «Компьютерлік технологияларды заңсыз пайдалану және киберқылмыстар туралы» Заңның 66-бабы).

Киберқылмыстылық туралы осы және басқа ұлттық заңдарға сәйкес юрисдикция негізінен қылмыскерлердің немесе құрбандардың орналасқан жері мен киберқылмыстың салдары негізінде белгіленеді.

2. Халықаралық ынтымақтастықтың ресми тетіктері.

Халықаралық ынтымақтастықтың жетістігі киберқылмыскерлер жасағаны үшін қылмыстық жауапкершілікті көздейтін киберқылмыстылықпен күрес саласындағы біріздендірілген ұлттық заңнаманың және дәлелдемелік құқық нормаларын және қылмыстық сот қылмыстық сот өндірісінің ережелерін белгілейтін киберқылмыстылық туралы ұлттық іс жүргізу заңнамасының болуына байланысты. Халықаралық ынтымақтастыққа киберқылмыстылыққа қатысты екіжақты, аймақтық және көпжақты құқықтық құжаттарды біріздендіру де ықпал етуі мүмкін. Киберқылмыстылықпен күрес туралы аймақтық және көпжақты құжаттарға қосылу және оларды ратификациялау да осы құжаттарға міндетті заңды күш беру үшін қажет.

Тиісті іс-әрекетті қылмыс деп өзара мойындаған жағдайда киберқылмыстықпен күрес саласындағы екіжақты, аймақтық және көпжақты шарттар да халықаралық ынтымақтастыққа ықпал етеді (яғни, келісім-шарттардағы тармақтар, оған сәйкес болжалды іс-әрекет ынтымақтасушы елдерде заңға қайшы деп есептелуге тиіс). Тиісті іс-әрекетті қылмыс деп өзара тану және біріздендірілген заңдар болмаған кезде киберқылмыскерлердің сот

қудалауына ұшырамауы мүмкін киберқылмыстарды жасаған адамдар үшін «қауіпсіз баспаналар» құрылады.

Мұны 2000 жылы «LOVE BUG» компьютерлік вирусын жасаушы және таратушымен болған оқиға мысалында байқауға болады, оны қылмыстық жауапкершілікке тарту мүмкін болмады, өйткені оқиға болған кезде оның әрекеттері оның тұратын елінде (Филиппинде) қылмыс болып саналмады. Алайда, халықаралық ынтымақтастық, тіпті тиісті әрекетті қылмыс ретінде өзара тануға қатысты талапты қатаң түсіндірместен де мүмкін.

Оның үстіне, «халықаралық ынтымақтастық мәселелеріне қатысты тиісті іс-әрекетті қылмыс деп өзара тану қағидасын сақтау талап етілсе, осы қағида сұрау салынатын Қатысушы мемлекеттің заңнамасы тиісті іс-әрекетті қылмыстардың сол санатына қамтитынына немесе ол оны Сұрау салушы Қатысушы мемлекет сияқты терминдердің көмегімен сипаттайтынына қарамастан, егер екі қатысушы мемлекеттің заңнамасына сәйкес сұрау салынуға қатысты тиісті іс-әрекетті қылмыс құрамын құраса сақталған деп есептеледі» (2003 жылғы Сыбайлас жемқорлыққа қарсы БҰҰ Конвенциясының 43(2) бабы).

Алайда, тиісті әрекетті қылмыс деп өзара тануға қатысты талаптан ерекше жағдайлар бар. Мысалы, 2001 жылғы Еуропа Кеңесінің компьютерлік қылмыстар туралы Конвенциясының 29(3) бабы «компьютерлік деректердің сақталуын шұғыл қамтамасыз ету қажет болған кезде» осы Конвенцияда санамаланған негізгі құқық бұзушылықтар бойынша (2-11-баптарда) «екінші Тараптың аумағында орналасқан компьютерлік жүйеде сақталатын және оларға қатысты Сұрау салушы Тарап өзара көмек шеңберінде тінту немесе осыған ұқсас қол жеткізуді қамтамасыз ететін іс-әрекеттер туралы, осы деректерді алу туралы немесе олардың сақталуын немесе жария етілуін осыған ұқсас қамтамасыз ету туралы өтініш жіберуге ниеттенгенде» тиісті әрекетті қылмыс деп өзара тануды талап етпейді. 29(4) бап мемлекеттердің, егер өзара құқықтық көмек шеңберінде екі тарап құқық бұзушылықты қылмыстық жазаланатын құқық бұзушылық ретінде саралау туралы шартты Конвенцияда санамаланған құқық бұзушылықтар үшін ұсынған жағдайларда, сақталуын қамтамасыз ету туралы өтініштен бас тарту құқығын көздейді.

Тиісті әрекетті қылмыс деп өзара тануға қатысты талапқа қосымша халықаралық ынтымақтастық үшін басқа да маңызды талап Адам құқықтары саласындағы халықаралық құқық міндеттемелерін сақтау болып табылады (БҰҰ ЕҚБ, 2013, 229 б.). Егер осы өтінішті қанағаттандыру нәтижесінде сұрау салынатын мемлекет адам құқықтары саласындағы өзінің халықаралық міндеттемелерін бұзса, халықаралық көмек көрсету туралы өтініш қабылданбауы мүмкін.

Халықаралық ынтымақтастықтың ресми тетіктеріне киберқылмыспен күрес саласындағы екіжақты, аймақтық және көпжақты шарттар кіреді. Ынтымақтастық мәселелері осы шарттарда көрнекті орын алады. Мысалы, Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің 2001 жылғы компьютерлік ақпарат саласындағы қылмыстарға қарсы күрестегі ынтымақтастығы туралы келісімде халықаралық ынтымақтастыққа арналған

бірнеше бап бар (5-7-баптар), онда осы Келісімде қамтылған ынтымақтастық нысандары (атап айтқанда: ақпарат алмасу; халықаралық құжаттарға сәйкес құқықтық көмек көрсету; компьютерлік ақпарат саласындағы қылмыстардың алдын алу, анықтау, жолын кесу және тергеу және т. б.), сонымен қатар, мүше мемлекеттер көмек сұрата алатын тәсілдер және сұрау салуларды орындауға қатысты мүше мемлекеттер үшін басшылық нұсқаулар көрсетілген. Осы Келісімнің 8-бабында көмек көрсету туралы өтініштен бас тартылуы мүмкін мән-жайлар (атап айтқанда: сұрау салуды орындау сұрау салынатын мемлекеттің ұлттық заңнамасына қайшы келген кезде) және оған сәйкес сұрау салуды орындаудан бас тартқан мемлекет бас тарту себептерін көрсете отырып, сұрау салушы мемлекетті бас тарту туралы жазбаша хабардар етуге міндетті болатын талап көрсетілген. Бұдан басқа, 2010 жылғы Араб Мемлекеттері Лигасының Ақпараттық технологиялар саласындағы қылмыстарға қарсы күрес туралы Конвенциясының 32 және 34-баптарында өзара көмек көрсету, ынтымақтастық рәсімдері және өзара көмек көрсету туралы сұрау салулар беру туралы ережелер қамтылған. Бұдан басқа, 2014 жылғы Африка одағының киберқауіпсіздік және дербес деректерді қорғау туралы Конвенциясының 28-бабына киберқылмыстықпен байланысты істер бойынша біріздендіру, өзара құқықтық көмек және ақпарат алмасу туралы ережелер кіреді. Ақпарат алмасу туралы ережеде мемлекеттерге компьютерлік инциденттерге әрекет ету топтары (CERT) немесе компьютерлік қауіпсіздік инциденттеріне әрекет ету топтары (CSIRT) сияқты киберқауіпсіздік және осалдық қатерлері туралы ақпарат алмасуға ықпал ететін мекемелер құруға шақыру берілген. 28(4) бапқа сәйкес мемлекеттерге киберқылмысқа ден қою шараларын қабылдау үшін «халықаралық, үкіметаралық, өңірлік немесе... мемлекеттік-жеке меншік әріптестіктерді» қамтуы мүмкін «халықаралық ынтымақтастықтың қолданыстағы тетіктерін пайдалану» ұйғарылды.

Киберқылмыскерлерді тергеуде және киберқылмыскерлерді қудалауда халықаралық ынтымақтастыққа ықпал ететін басқа тетіктер өзара құқықтық көмек көрсету және ұстап беру туралы шарттар болып табылады. Өзара құқықтық көмек туралы шарттар (ӨҚКШ) осы келісімдерде келтірілген тізбедегі қылмыстарға қолданылатын елдер арасындағы келісімдер болып табылады және тергеу жүргізу кезінде әрбір ел көрсететін көмек түрлерін (мысалы, дәлелдемелер жинау) айқындайды (Maras, 2016, p. 78). Қылмыстар тізіміне негізделген тәсіл өте ескірген және киберқылмыстылықтың эволюциялық сипатын ескермейді. Қылмыстың (және киберқылмыстың) өзгеріп отыратын сипатын ескере отырып, кейбір ӨКШ-да қылмыстар тізбесін көрсетудің орнына Тараптар өздерінің ішкі заңнамасы бойынша осындай деп саналатын барлық қылмыстарға қатысты тергеу мен сот қудалауында ынтымақтасуға уағдаласады (кейбір ерекшеліктерді қоспағанда).

Өзара көмек көрсету туралы сұрау салулар жазбаша нысанда жасалуға және мынадай ақпаратты: Сұрау салушы органның атауын; сұрау салудың мақсатын; сұрау салудың сипаттамасын; көмек көрсету туралы сұрау салу жататын тергеп-тексеру немесе сот талқылауын; құқық бұзушылықтың немесе құқық бұзушылықтардың және бұзылған заңдардың сипаттамасын; сұрау

салушы органға заттай және цифрлық дәлелдемелерді алу, сақталуын қамтамасыз ету және беру үшін сақталуы қажет рәсімдерге қатысты кез келген өтініштерді; деректердің сақталуын қамтамасыз ету және сұраудың орындалу мерзімін; сұрау салынатын мемлекетке сұрау салуды орындауға көмектесетін кез келген басқа ақпаратты қамту керек (мысалы, 1992 жылғы Батыс Африка мемлекеттерінің экономикалық қоғамдастығының қылмыстық мәселелер бойынша өзара көмек көрсету туралы Конвенциясының 5-бабын қараңыз (БАМЭҚ).

Өзара көмек көрсету туралы сұрау салуларды орындаудан белгілі бір жағдайларда бас тартылуы мүмкін. Мысалы, егер сұрау «егемендікке, қауіпсіздікке және қоғамдық тәртіпке зиян келтірер болса» (Қылмыстық мәселелер бойынша өзара көмек көрсету туралы БАМЭҚ Конвенциясының 4-бабын; сонымен қатар 1959 жылғы қылмыстық істер бойынша өзара құқықтық көмек туралы Еуропалық конвенцияның 2-бабын, Еуропа Кеңесінің компьютерлік қылмыстар туралы Конвенциясының 25(4) бабын және ақпараттық технологиялар және байланыс саласындағы қылмыстарды болдырмаудың және оларға қарсы күрестің арнайы ережелерін қамтитын 1430 жылғы Шаабан айының 14-күніндегі (тиісінше 2009 жылғы 5 тамыздағы) Алжирдің №09-04 Заңының 18-бабын қараңыз). Өзара құқықтық көмек көрсету туралы өтініштерде, егер, мысалы, сұрау салу «Сұрау салынатын Тарап саяси қылмыс ретінде немесе саяси қылмысқа байланысты құқық бұзушылық ретінде қарайтын құқық бұзушылыққа қатысты болса», бас тартылуы мүмкін (Компьютерлік қылмыстар туралы Конвенцияның 25(4) бабы). Егер сұрау салуды орындау немесе деректерді ашу сұрау салынатын мемлекеттің адам құқықтары саласындағы халықаралық міндеттемелерді бұзуына әкеп соғатын болса, деректер беру туралы өтініштен де бас тартылуы мүмкін. Ынтымақтастықтың басқа да ресми тетіктерін пайдалану кезінде елеулі уақыт кідірістері (яғни, «бірнеше ай туралы сөз болғанда») орын алады. Сандық дәлелдердің тұрақсыздығын ескере отырып, мұндай кідірістер өте проблемалы. Кейбір елдер өзара құқықтық көмек пен сот тапсырмаларын сұрау туралы Нұсқаулық шығарса да, тіпті сұрау үлгілерін құрса да, бұл тәжірибе жалпы қабылданған емес. Елдерге өзара көмек көрсету туралы сұрау салуларды жасауға жәрдемдесу мақсатында Біріккен Ұлттар Ұйымының Есірткі және қылмыс жөніндегі басқармасы (БҰҰ ЕҚБ) сұрау салулардың форматтарын біріздендіру жолымен осы рәсімді реттеу және сол арқылы сұрау салуларды беру және оларды орындау процестерін жеделдету үшін өзара құқықтық көмек көрсету туралы өтініштер жасау бағдарламасын әзірледі. Конвенция және 1981 жылғы Экстрадициялау туралы Америка мемлекеттерінің ұйымы (АМҰ) американааралық Конвенциясы сияқты ұстап беру туралы шарттар ұстап беруге әкеп соғатын қылмыс жазаның белгіленген ең төменгі шегіне сәйкес келген жағдайларда сұрау салушы елге адамдарды ұстап беру және/немесе ұстап беру туралы келісімдерді білдіреді.

Мысалы, 1994 жылғы Батыс Африка елдерінің Экономикалық бостандығынан айырумен байланысты жазамен немесе қауіпсіздік Қоғамдастығының (БАЕЭҚ) ұстап беру туралы конвенциясының 3-бабына

сәйкес жазаның шегі «кем дегенде екі жыл». Еуропалық қамауға алу санкциясы сияқты аймақтық қамауға алу санкциялары қылмыскерлерді компьютерлермен байланысты қылмыстары үшін қамауға алуға мүмкіндік береді, олар «кем дегенде үш жылға бас шарасымен жазаланады... қос қылмыстылыққа әрекетін тексерусіз (әрекетті қылмыс ретінде өзара тану)» (2(2) бап, Еуропалық Одақ Кеңесінің 2002 жылғы 13 маусымдағы «Еуропалық қамауға алу ордері туралы және мүше мемлекеттер арасында адамдарды беру рәсімдері туралы» негіздемелік шешімі - негіздемелік шешімнің қабылдануына байланысты кейбір мүше мемлекеттер жасаған мәлімдемелер).

Ұстап беру туралы шарттың болуы адамның сұрау салушы елге ұстап берілуіне кепілдік бермейді. Бұл Британдық хакер Лори Лавтың жағдайында байқалдың, ол 2003 жылы қол қойылған Ұлыбритания мен АҚШ арасындағы экстрадициялау туралы шарттың болуына қарамастан, АҚШ-қа ұстап берілмеген.

Бұдан басқа, ұстап беру туралы шарттар ұстап беру жүргізілмейтін талаптарды қамтиды. Мысалы, 1981 жылғы Экстрадициялау туралы Америка мемлекеттерінің ұйымы (АМҰ) америкааралық Конвенциясына сәйкес, қылмыс үшін жаза өмір бойына бас тарту немесе өлім жазасы болған кезде ұстап беру туралы сұрау салулар қабылданбайды (9-бап). Ұстап беруге жататын адам адамгершілікке жатпайтын немесе қадір-қасиетін қорлайтын қарым-қатынасқа немесе жазаға тартылған жағдайларда да ұстап беруден бас тартылады (мысалы, ұстап беру туралы БАЕЭҚ Конвенциясының 5-бабы және экстрадициялау туралы АМҰ америкааралық Конвенциясының 9-бабы).

Ұстап беру туралы сұрау салулар, сондай-ақ ұстап беруді негіздейтін жеткілікті дәлелдемелердің болмауы (мысалы, Ботсвананың 1990 жылғы «Ұстап беру туралы» Заңы), сұрау салу ұстап беруге әкеп соқпайтын қылмыспен байланысты болған кезде (мысалы, әскери қылмыс, ұстап беру туралы БАЕЭҚ Конвенциясының 7-бабы) немесе сұрау салынатын елдің азаматы болып табылатын адамды ұстап беру сұратылған кезде (мысалы, Алжир қылмыстық іс жүргізу кодексінің 698-бабы және Бразилия Конституциясының 5 (LI) - бабы).

Сұрау салынатын мемлекеттердің азаматтарын ұстап беруге келетін болсақ, өз азаматтарын ұстап бермеу қағидасы Конституцияда, сондай-ақ өңірлік және халықаралық шарттарда бекітілген. Осы Қағидаға қарамастан, «халықаралық қоғамдық құқық мемлекеттерге ауыр халықаралық қылмыс жасаған адамдарды қылмыстық қудалауды (aut dedere aut judicare) беру немесе жүзеге асыру туралы заңды міндеттеме береді». Кейбір қамауға алу туралы келісімдер, сонымен қатар, саяси қылмыстар сияқты белгілі бір құқық бұзушылықтарды алып тастауы мүмкін (мысалы, 2008 жылғы Кариб қауымдастығы және ортақ нарықтың (КҚОН) Қамауға алу туралы Келісімінің 3-бабын қараңыз).

3. Халықаралық ынтымақтастықтың бейресми тетіктері.

Құқық қорғау органдары арасындағы ақпарат алмасу сияқты халықаралық ынтымақтастықтың бейресми тетіктері де киберқылмыстармен күресуде қолданылады (James and Gladyshev, 2016).

Құқық қорғау органдары бейресми арналар арқылы алмасатын ақпарат түрі нақты мемлекетке байланысты өзгереді. Австралияда «билік ведомствоаралық ынтымақтастық аясында келесі көмек түрлерін ұсына алады: куәгерлердің ерікті айғақтарын алу, куәгерлердің ерікті сауалнамаларын жүргізу, бейне байланыс арқылы ерікті куәгерлердің айғақтарын алу, Австралияда тергеу жүргізетін шетелдік полиция қызметкерлерін қабылдау, жедел мәліметтермен алмасу, физикалық бақылауды жүзеге асыру, соттылық туралы ақпарат алу немесе көпшілікке қол жетімді материалдарды алу» (UNODC, «Informal cooperation channels: Australia»). Басқа елдер жеке сипаттағы кейбір деректерді бірлесіп пайдалануға келіседі. Киберқылмыспен байланысты істер бойынша қылмыстық қудалау саласында бейресми халықаралық ынтымақтастық тетігі бар: Халықаралық прокурорлар қауымдастығының электрондық қылмыстарға қарсы іс-қимыл жөніндегі жаһандық прокурорлық желісі (GPEN).

Ынтымақтастықтың бейресми тетіктері құқық қорғау органдары арасында жедел ақпарат алмасуға ықпал етеді (яғни айлар емес, күндер ішінде) (БҰҰ ЕҚБ, 2013, 239 б.). Сонымен қатар, 24/7 желілері сандық дәлелдемелер туралы шұғыл сұраулар алу және халықаралық ынтымақтастыққа жәрдемдесу мақсатында құрылады. Ынтымақтастықтың бейресми арналары негізінен құқықтық және техникалық кеңестер алу және сандық дәлелдемелер жинау туралы сұрауларға емес, киберқылмыспен байланысты істер бойынша жәрдемдесу үшін қолданылады (БҰҰ ЕҚБ, 2013, 239 б.). Мысалы, Жапонияда ресми емес арналар арқылы ақпарат беру туралы сұрау салуды Сұрау салушы ел бұл ақпаратты дәлел ретінде пайдаланғысы келмеген жағдайда ғана орындауға рұқсат етіледі (UNODC, «International cooperation: Japan»). Егер ел бұл ақпаратты дәлел ретінде пайдаланғысы келсе, өзара құқықтық көмек көрсету туралы ресми сұрау салу жіберу қажет. Осы арналар арқылы алынған цифрлық дәлелдемелер, егер дәлелдемелерді қорғау жүйесі қолдау таппаса, сұрау салушы мемлекеттің ұлттық соттарында жол берілмейтін болып танылуы мүмкін. Егер ақпаратты Америка Құрама Штаттарының, Парагвайдың, Аргентинаның (және басқа да елдердің) құқық қорғау органдары бейресми түрде берсе, сұрау салушы елдер ресми арналар арқылы әрекет етуі тиіс. Халықаралық және өңірлік ұйымдар ресми емес халықаралық ынтымақтастыққа да жәрдемдеседі. Мысалы, өзара көмек көрсету туралы шұғыл сұраулар Америка мемлекеттерінің ұйымына жіберілуі мүмкін (UNODC, «Channels for urgent requests»). Көмек көрсету туралы шұғыл сұрауларды ИНТЕРПОЛ арқылы да жіберуге болады (UNODC, «Channels for urgent requests for MLA in cybercrime cases: Liechtenstein»), әлемдегі ең ірі халықаралық полиция ұйымы, оның I-24/7 жаһандық полиция телекоммуникация желісі 190-нан астам елді қамтиды. Осы желі арқылы ұлттық құқық қорғау органдары трансұлттық қылмыстармен күресу үшін тәжірибелерімен, технологияларымен және ресурстарымен бөліседі.

Интерпол елдер арасындағы байланыс торабы ретінде әрекет етеді, оларға *хабарламалар* сияқты ақпаратты таратуға көмектеседі, тіпті бірлескен операцияларды үйлестіруге көмектеседі. Мысалы, 2012 жылы Интерпол

Испания, Аргентина, Чили және Колумбиядағы жергілікті билікке Anonymous халықаралық хакерлік тобының 25 мүшесін «Әшкерелеу» операциясы аясында қамауға алуға көмектесті (Whiteman, 2012; Interpol, «Operation Unmask»). 2017 жылы «Индонезия, Малайзия, Мьянма, Филиппин, Сингапур, Таиланд және Вьетнам құқық қорғау органдарының, сондай-ақ Қытай мен жеке сектор ұйымдарының қатысуымен Интерполдың басшылығымен жүргізілген операция «9.000-ға жуық командалық серверлерді (C2) және жүздеген бұзылған веб-сайттарды, соның ішінде мемлекеттік порталдарды анықтауға» мүмкіндік берді (INTERPOL, 2017).

Whiteman (Whiteman, 2012) мақаласында күдіктілерді Интерпол тұтқындады делінген. Бұл қате. Интерполдың қылмыскерлерді қамауға құқығы жоқ. Интерпол қылмыстық істерді тергеуге көмектесетін бірлескен тергеу тобы (Europol, n.d.) сияқты нәрсені құруға көмектесе алады, бірақ тек жергілікті тергеушілер өз елдерінің аумағында қамауға алуға құқылы. Өкінішке орай, бұқаралық ақпарат құралдары Интерполды жергілікті жерде өкілеттігі бар халықаралық полиция ретінде жиі қате көрсетеді. Интерполға елде қамауға алу құқығын берудің орнына, әр мемлекет өзінің ұлттық Орталық бюросын құрады (ҰОБ) (INTERPOL, 2018). Интерполдың Штаб-пәтері ҰОБ ақпараты мен ұсынымдарын ұсына алады, бірақ ол оларды қандай да бір іс-қимыл жасауға мәжбүрлей алмайды. Сонымен қатар, кейбір жағдайларда - бірақ әрқашан емес - жергілікті полиция қызметкерлері немесе прокурорлар ҰОБ-тың қызметкерлері болады .

4. Деректерді сақтау және сақталуын қамтамасыз ету және деректерге қол жеткізу

Халықаралық ынтымақтастық шеңберіндегі көмек сұраулары процедуралық талаптарға байланысты да қабылданбауы мүмкін. Мысалы, деректерді сақтаудың, сақталуын қамтамасыз етудің және оған қол жеткізудің практикалық әдістерін қарастырайық. Интернет және байланыс қызметтерін жеткізушілер сақтайтын деректерді ұсыну туралы өтінішті орындау қызметтерді ұсыну шарттарына, құпиялылық саясатына және қызметтер провайдерінің бизнесті жүргізу тәжірибесіне байланысты болады. Осыған байланысты қызмет провайдерлері өздері сақтайтын деректер түрімен ғана емес (мысалы, IP мекенжайларын тіркеу журналдары немесе өшірілген есептік жазбалар туралы ақпарат), сонымен қатар оларды сақтау кезеңімен (күндер, апталар, айлар немесе жылдар) ерекшеленеді. (мысалы, қосымша ақпарат алу үшін Twitter «Guidelines for Law Enforcement» («Заңдылықты қамтамасыз етудің басшылық қағидаттары») және Facebook «Data Policy» («Деректерді пайдалану саясаты») қараңыз). Деректерді сақтауға, сондай-ақ оларға қол жеткізуге қатысты саясат деректерді қорғау саласындағы ұлттық, өңірлік және халықаралық заңдарға байланысты өзгеріп отырады.

Деректердің сақталуын қамтамасыз ету туралы өтініштерді құқық қорғау органдары қызметтерді жеткізушілерге деректерді жойылғанға немесе қандай да бір түрде өзгертілгенге дейін сақтау мақсатында жібереді. Сақталған деректерге қол жеткізу рәсімі ұлттық заңнамада жазылған. Егер қызметтер жеткізушілерден әр түрлі деректер алу үшін заңды өкімдер (мысалы, сот

қаулысы немесе тінту ордері) қажеттілігі қарастырылса, оларда нақты елге байланысты түрленеді. Мысалы, Америка Құрама Штаттарында мазмұнға қатысты емес деректерді (немесе метадеректерді; мысалы, абоненттің деректері мен IP-мекенжайларын) алу үшін шақыру қағаздары мен сот шешімдері қажет, ал іздеу туралы бұйрықтар мазмұнға қатысты деректерді алу үшін қажет (АҚШ-тың 1986 жылғы «Сақталған хабарламалар туралы» Заңы; 1986 жылғы «Электрондық поштаның құпиялылығы туралы» Заңның II титулы), ал түрік құқық қорғау органдарына мазмұнға жатпайтын деректерге және мазмұнға қатысты деректерге қол жеткізу үшін заңды бұйрықтар қажет емес (№5651 «Интернет туралы» Заң). Оның үстіне, сақтаудағы және/немесе сақталған деректерге қол жеткізе алатын органдар белгілі бір елге байланысты әр түрлі болады. Мысалы, Кенияда құқық қорғау органдарының қызметкері немесе басқа уәкілетті тұлға (атап айтқанда, «ұлттық қауіпсіздік жөніндегі Министрлер Кабинетінің хатшысы тағайындайтын киберқауіпсіздік жөніндегі сарапшы») Кенияның 2018 жылғы «Компьютерлік технологияларды заңсыз пайдалану және киберқылмыстар туралы» Заңына сәйкес сақталған және/немесе сақталған деректерге қол жеткізе алады, ал Ямайкада тек құқық қорғау органдарының қызметкерлері ғана деректерге қол жеткізе алады (2015 жылғы «Киберқылмыстар туралы» Заңды қараңыз).

Сонымен қатар, ұлттық заңнамада белгіленген белгілі бір жағдайларда интернет-қызметтерді жеткізушілердің заңды бұйрықтарсыз ақпаратты өз еркімен ашуына жол беріледі. Мұндай жағдайдың мысалы ретінде ауыр дене жарақаттарының немесе өлімнің алдын алу мақсатында деректерді ұсыну туралы шұғыл сұрау салуды келтіруге болады. Егер қызмет жеткізушілер сұратылған деректерді ерікті түрде беруден бас тартса, онда белгілі бір жағдайларда және нақты жағдайға, ізделетін дәлелдемелерге, дәлелдеу ауыртпалығына және ұлттық заңнамаға байланысты бұл қызмет жеткізушілер заңда көзделген тәртіппен осы ақпаратты беруге мәжбүр етілуі мүмкін.

5. Эксаумақтық дәлелдермен байланысты мәселелер. Халықаралық ынтымақтастықтың ресми және бейресми тетіктері болса да, бұлтты сақтау орындарында және басқа қызмет жеткізушілерінде сақталатын сандық дәлелдемелерді идентификациялау және жинау кезінде қиындықтар туындайды. Бұлтты есептеу мәселесі деректердің қай жерде сақталатынын білу қиындығында. Мұндай ақпаратсыз «сандық дәлелдер алу үшін ынтымақтастық туралы сұрау жіберілетін тиісті юрисдикцияны» анықтау мүмкін емес» (БҰҰ ЕҚБ, 2013, 241 б.).

Бұлтты деректерді фрагменттерге бөліп, әртүрлі жерлерде және бірнеше елдерде сақтауға болады. Деректерді фрагментациялаудың мұндай проблемасын АҚШ-қа қарсы *United States v. Microsoft* ісі мысалмен суреттеуге болады. Бұл істі тергеу аясында АҚШ үкіметі есірткінің заңсыз айналымы туралы іс бойынша дәлелдер алу үшін 1986 жылғы АҚШ-тың «Сақталған хабарламалар туралы» Заңына (SCA) сәйкес тінту ордерін берді. Microsoft бұл сұранысты АҚШ-тағы серверлерде сақталған мазмұнға қатысты емес тиісті деректерді (мысалы, күдіктінің мекен-жай кітабын) беру арқылы қанағаттандырды, бірақ АҚШ үкіметіне мазмұнға қатысты тиісті деректерді

олардың Microsoft корпорациясының Дублиндегі (Ирландия) деректер орталығында сақталғандықтан ұсынбады (мысалы, адамның электрондық пошталарының мазмұны).

United States v. Microsoft (2018) ісіндегі дау-дамайдың мәні «Сақталған хабарламалар туралы» Заңның ережелері басқа елдегі серверлердегі деректерге қол жеткізуге мүмкіндік бере ме, жоқ па және мұндай қол жетімділік заңды түрде негізделмеген заңды эксаумақтық қолдану болып саналды ма деген сұрақ болды. Қазір бұл мәселе АҚШ-та 2018 жылы шетелде деректерді заңды пайдалану тәртібін түсіндіретін Заңның қабылдануына байланысты өзектілігін жоғалтты («Cloud» Заңы – «Бұлт»). Оны қабылдаумен Сақталған хабарламалар туралы Заңға (АҚШ заңдары жинағының 18-тарауы, §2713) мынадай түзетулер енгізілді: «электрондық байланыс қызметтерін немесе деректерді қашықтықтан өңдеу қызметтерін жеткізуші осы тараудың телеграфтық немесе электрондық хабарламалардың ішіндегісін және клиентке немесе жазылушыға қатысты кез келген жазбаны немесе өзге де ақпаратты сақтау, резервтік көшіру немесе ашу жөніндегі міндеттемелерін сақтауы тиіс», *мұндай хабарлама, жазба немесе өзге ақпарат Америка Құрама Штаттарының аумағында немесе оның аумағынан тыс жерде болуына қарамастан* (автордың курсиві).

«Cloud» Заңы эксаумақтық деректерге тікелей қол жеткізуді қамтамасыз етеді. Алайда, «егер бар болса, құқық қорғау органдары эксаумақтық деректерге тікелей қол жеткізе алатын жағдайларға қатысты жалпы стандарттар мен кепілдіктер» (БҰҰ ЕҚБ, 2013, 240 б.), 2018 жылғы жағдай бойынша әлі жоқ.

6. Ұлттық әлеует және халықаралық ынтымақтастық

Халықаралық ынтымақтастықтың тиімділігі мемлекеттердің дәлелдемелерді ұсыну туралы сұрау салуларды осы дәлелдемелердің сотта жарамдылығын қамтамасыз ететіндей түрде орындау қабілетіне байланысты. Ол үшін Ұлттық дәлелдемелік құқығына және қылмыстық сот ісін жүргізу ережелеріне сәйкес дәлелдемелер алуды қамтамасыз ете алатын киберқылмыстылық саласындағы білікті мамандардың болуы қажет. Алайда мұндай мамандар жетіспейді. Оның үстіне, бүкіл әлемдегі елдер киберқылмыстылықпен күресу үшін қажетті ұлттық әлеуеттің жетіспеушілігін сезінуде (БҰҰ ЕҚБ, 2013).

Ұлттық әлеуеттің мұндай тапшылығы кадрлық, қаржылық және техникалық ресурстардың жетіспеушілігінің нәтижесі болып табылады (БҰҰ ЕҚБ, 2013). Біріншіден, көптеген елдерде киберқылмыстарға тергеу жүргізу, сондай-ақ киберқылмыскерлерді қудалау және киберқылмыстылықпен байланысты істер бойынша халықаралық ынтымақтастық шеңберінде көмек сұрауларын қарау үшін білікті мамандардың жеткілікті саны жоқ. Екіншіден, елдерге білікті кадрларды іріктеу, жалдау және ұстап қалу үшін, сондай-ақ киберқылмыстармен айналысатын тергеушілер мен басқа да тиісті мамандар үшін тұрақты және заманауи дайындықты ұйымдастыру үшін қажетті қаржы ресурстары жетіспеуі мүмкін. Үшіншіден, елдерде цифрлық дәлелдемелерді талдау үшін қажетті материалдық база жоқ және киберқылмыстарға тергеу

жүргізу үшін цифрлық криминалистиканың қажетті жабдықтары мен құралдарын сатып алу үшін қаражат жетіспейді.

Ұлттық әлеуеттің тапшылығы проблемасын шешу үшін ұлттық, өңірлік және халықаралық ұйымдармен (мысалы, АҚШ Әділет министрлігі, Америка мемлекеттерінің ұйымы және Халықаралық электрбайланыс одағы), сондай-ақ жеке компаниялармен киберқылмыстылықпен байланысты мәселелер бойынша қаржылық, кадрлық және техникалық көмек көрсету және осындай көмекке мұқтаж елдерге олардың киберқылмыстылықпен күрес саласындағы ұлттық әлеуетін дамыту жөніндегі күш-жігеріне қолдау көрсету мақсатында әріптестік құрылды және оны құрылуы жалғасуда.

Талқылауға арналған сұрақтар:

1. Киберқылмыстылық аумақтық егемендікті қалай бұзуы мүмкін?
2. Сіздің еліңіздегі қандай заң сақталудағы және/немесе сақталған деректерге қол жеткізуді реттейді?
3. Бұл деректерге кім қол жеткізе алады? Қандай жағдайда?
4. Мазмұнға қатысты деректерге қол жеткізу үшін заңды ұйғарым қажет пе? Егер иә болса, онда қандай?
5. Метадеректерге қол жеткізу үшін заңды ұйғарым қажет пе? Егер иә болса, онда қандай?

8 Тақырып. Киберқауіпсіздік және киберқылмыстың алдын алу: стратегия, саясат және бағдарламалар.

1. Интернетті Басқару

Керрдің пікірі бойынша «Интернетке екі басым көзқарас» бар: бір жағынан, Интернет «компьютерлерін желіге қосатын соңғы пайдаланушылар арасында ақпарат беру үшін ашық платформа ретінде қызмет ететін ғаламдық мета желісі» ретінде қарастырылады; екінші жағынан, Интернет «жұмыс істеуге мүмкіндік беретін қосымшалар контекстісінде және бұл қосымшалардың соңғы пайдаланушыларға қалай әсер ететіндігі» қарастырылады (Frischmann, 2003; pp. 205-206; сонымен қатар Kerr, 2003, p. 359-360 қараңыз). Интернет туралы осы идеялардың соңғысы «киберкеңістікті виртуалды шындықтың бір түрі ретінде қабылдауға әкеледі» (немесе онлайн-әрекет жүргізілетін орта) (Frischmann, 2003, p. 206).

Интернетті және киберкеңістікті басқаруға қатысты реттеу теорияларына арналған әдебиеттерде интернет пен киберкеңістікті реттейтін адамдар, топтар, кәсіпорындар, ұйымдар мен мемлекеттік органдар, сондай-ақ киберкеңістікті және Интернетті реттеу тәсілдеріне назар аударылады. Бұл көзқарас киберкеңістік пен интернетті, мысалы, заңдармен, компьютерлік бағдарлама кодымен, жүйелік архитектурамен және интернет архитектурасымен реттелетін әдебиеттерден растау табады (яғни, өзін-өзі реттеу негізінде); және жеке тұлғалар, кәсіпорындар мен басқару үшін бірлескен жауапкершілігі бар ұйымдар (яғни, таратылған қорғау негізінде).

Интернет жаһандық мүдделерге әсер етеді және оны басқару процесі

«интернет-атаулар мен нөмірлерді тарату корпорациясы (ICANN) айналысатын интернет желісіндегі атаулар мен мекен-жайларды тағайындауға қатысты мәселелерді ғана емес; ол сонымен қатар маңызды интернет-ресурстар, Интернеттің қауіпсіздігі және қорғалуы, сондай-ақ интернетті пайдалануға байланысты дамудың аспектілері мен мәселелері сияқты мемлекеттік саясаттың басқа да маңызды мәселелерін қамтиды» (WGIG, 2005, p. 4). Сондықтан кез-келген ұйым бірыңғай халықаралық басқару органы ретінде тағайындала алмайды және тағайындалмады. Оның орнына, Интернетті басқару процесі негізінен халықаралық деңгейде бірнеше мүшелермен - үкімет, жеке сектор, ғылыми қауымдастық және азаматтық қоғаммен жүзеге асырылады және бірқатар техникалық және техникалық емес мәселелерді қамтиды. Дегенмен, елдер интернетті басқаруда қандай қатысушылар негізгі рөл атқаруы керек деген пікірде келіспеушілікке келеді. Кейбір елдер Интернетті басқаруға бірнеше қатысушы жауапты болуы керек деп санаса, басқа елдер Интернетті басқару мемлекеттің ерекше құзыретіне кіруі керек деп санайды. Егер елдер Интернетті басқаруға жауапты қатысушылардың құрамы туралы келіссе де, қылмыстық сот төрелігі жүйелеріндегі және әртүрлі елдерде қолданылатын заңдардағы айырмашылықтарға байланысты Интернетті басқарудың әмбебап қағидаларын қабылдауға басқа кедергілер бар. Интернетті басқарудың басты мақсаты барлық елдердің Интернетті бірлесіп реттеуі болса да, шындық мынада, елдер мұндай реттеуді қалай жүзеге асыру керектігі туралы пікірде келіспеушілікке келеді. Мұны әртүрлі елдердің Интернет жұмысының бостандық (яғни ақпаратқа қол жеткізу және ақпарат алмасу «негізделген шектеулерсіз» жүзеге асырылуы мүмкін), ашықтық (яғни желідегі ақпараттың кедергісіз ағымы), функционалдық үйлесімділік (яғни түрлі сандық құрылғылар мен компьютерлік жүйелердің қосылу, деректерді беру және бөлісу қабілеті), қауіпсіздік (яғни, жүйелердің, желілердің, қызметтердің және деректердің құпиялылығын, тұтастығы мен қол жетімділігін қорғау) және тұрақтылық (яғни, сәтсіздік пен жағдайдың өзгеруі кезінде жұмыс істеу) сияқты кейбір негізгі принциптеріне қалай қарайтындығы туралы мысалдан байқауға болады (2014 жылғы ЭЫДҰ-ның интернет саясатын әзірлеу жөніндегі Басшылық принциптері; 2014 жылғы Интернеттегі құқықтар мен бостандықтар Африка декларациясы; UNESCO, 2015). Ақпарат тарату және ақпарат алмасу платформасынан - ашықтық қағидатына сәйкес - Интернет әлеуметтік өзара әрекеттесу, сауда және коммерция және мемлекеттік қызметтерді ұсыну платформасына айналды. Сонымен қатар, Интернет пен АКТ-ны қауіп төндіретін адамдар мен ұйымдар және басқа да зиянкестер заңсыз және зиянды түрде қолданды және қолдануды жалғастыруда, бұл киберқылмыстың өсуіне ықпал етеді, сондықтан қауіпсіздікті камтамасыз ету шараларын күшейту қажеттілігін тудырады.

2. Киберқауіпсіздік стратегиясы: негізгі ерекшеліктері.

Киберқауіпсіздікті қамтамасыз ету стратегиясы және киберқылмыстылыққа қарсы іс-қимыл (немесе алдын алу) стратегиялары өзара алмастырылатын терминдер болып пайдаланылады. Киберқауіпсіздікті

қамтамасыз ету стратегиялары мен киберқылмыстылыққа қарсы стратегиялар бір-бірін толықтырады және бір-біріне сәйкес келеді, бірақ олардың арасында айырмашылықтар бар. Киберқылмыстылыққа қарсы стратегиялар киберқылмыстылықпен күресуге тікелей немесе жанама түрде байланысты күш-жігерді сипаттайды, мысалы, құқық қорғау органдары қабылдаған әрекет ету шаралары және үкіметтер, бизнес-топтар, ғылыми-білім беру мекемелері, ұйымдар және жұртшылық арасындағы ұлттық және халықаралық ынтымақтастықты бақылау және/немесе төмендету мақсатында жәрдемдесу. Қарапайым тілмен айтқанда, киберқылмыстылыққа қарсы стратегиялар тек қылмыстық сот төрелігі мен қылмыстың алдын алу саласындағы саясат шараларына, бағдарламаларға және тәжірибеге бағытталған. Керісінше, киберқауіпсіздікті қамтамасыз ету стратегиясында киберқауіпсіздік туралы нұсқаулар бар (олар киберқылмыстылықтың алдын-алу нұсқауларын қамтуы мүмкін) және осы мақсаттарға жету үшін қажетті міндеттерді, сондай-ақ іс-қимыл жоспарларын, шаралар мен міндеттерді анықтайды. Бұл стратегиялар жүйелерді, желілерді, қызметтер мен деректерді қорғауға арналған құқықтық, рәсімдік, техникалық және институционалдық шараларды қабылдауды көздейді.

Ұлттық киберқауіпсіздік стратегиялары ұлттық және халықаралық деңгейде киберқауіпсіздікті қамтамасыз ету және киберқылмыстылықтың алдын алу саласындағы елдердің ұмтылыстарын көрсетеді. Бұл стратегияларда стратегия негізделген қағидаттар көрсетілген, осы стратегия қорғауға арналған мүдделер сипатталған, осы мүдделерді ілгерілету және қорғау үшін қолданылатын құралдар анықталған, киберқауіптер мен ұлттық және экономикалық қауіпсіздікке қауіп төндіретін проблемалар анықталған, киберқауіпсіздік саясатының басым міндеттері және осы міндеттерді орындау үшін бөлінген ресурстар анықталған. Бұл стратегиялар «... саясатты әзірлеуге жауапты органдарды стратегиялық міндеттерді («мақсаттар») белгілеуге, осы міндеттерді орындау үшін қолда бар ресурстарды («құралдар») айқындауға және қойылған міндеттерді орындау үшін осындай ресурстарды қалай пайдалану керектігіне қатысты басшылық нұсқауларды әзірлеуге («тәсілдер») шақырады».

Киберқауіпсіздік стратегиясында стратегия неліктен маңызды және қажет (контекстісі), не нәрсеге қол жеткізу керек (мақсаттар), оның құрамы және оған не және кім әсер етеді (қолданылу аясы) (ХЭО, 2018, 30 б.). Бұл стратегиялардың негізгі компоненттері міндеттер, басым әрекеттер, күтілетін нәтижелер және бағалау тетіктері болып табылады.

Киберқауіпсіздік стратегиясының міндеттері ұлттық қауіпсіздікке қатысты міндеттерді, сондай-ақ ақпараттық-коммуникациялық технологияларға байланысты міндеттерді қамтиды. Мысалы, Швецияның киберқауіпсіздік стратегиясы «Швецияның қауіпсіздігі мақсатына негізделген: халықтың өмірі мен денсаулығын қорғау, қоғамның жұмыс істеуі және... оның демократия, заң үстемдігі және адам құқықтары мен бостандықтары сияқты негізгі құндылықтарды сақтау мүмкіндігі. ... Стратегия сонымен қатар саясаттың жалпы мақсатына негізделген ... ақпараттық

технологиялар (АТ) - Швецияны цифрлық трансформация мүмкіндіктерін жүзеге асыруда әлемдік көшбасшы ету» (Swedish Ministry of Justice, 2017, p. 1 қараңыз; Швеция Әділет министрлігі, Ұлттық киберқауіпсіздік стратегиясы, «A National Cyber Security Strategy»). Нигерияда киберқауіпсіздік стратегиясының міндеттері (Cybersecurity Strategy (2014) келесідей:

- киберқылмыстылық туралы жан-жақты заңнама және ұлттық деңгейде қабылдануы мүмкін және елдің киберкеңістігінің қауіпсіздігін қамтамасыз ету тұрғысынан аймақтық және жаһандық деңгейде өзекті болып табылатын киберқауіптерге қарсы іс-қимыл шаралары;

- аса маңызды ақпараттық инфрақұрылымды қорғау жөніндегі шараларды іске асыру, сондай-ақ киберқауіпсіздікті қамтамасыз ету тетігінің көмегімен ұлттық осалдық факторларын төмендету;

- компьютерлік инциденттерге тиімді әрекет ету саласындағы мүмкіндіктерді анықтау;

- кибершабуылдарға жедел және тиімді әрекет ету қабілетімізді нығайту үшін әлеуетті құру, қоғамды ақпараттандыру және біліктілікті арттыру мүмкіндіктерін кеңейтудің ұлттық тетіктері;

- ұлттық мүдделі тараптар мен халықаралық әріптестердің киберқауіптерге қарсы күрес жөніндегі ұжымдық күш-жігерге қатысуын қамтамасыз ету үшін сенімді тетік;

- үкіметті кибершабуылдардың барлық түрлерінен қорғау және осындай кибершабуылдарды болдырмау;

- ел үкіметінің барлық деңгейінде киберқауіпсіздікті қамтамасыз ету саласындағы бастамаларды үйлестіру;

- мемлекеттік-жеке меншік әріптестік және барлық мүдделі тараптардың өзара іс-қимылы шеңберіндегі дәйекті ынтымақтастық негізінде киберқауіптерге қарсы іс-қимыл жасау үшін Ұлттық мүмкіндіктер жасау;

- хабардарлықты арттыру, бірлескен жауапкершілік негізінде серіктестікті дамыту және сенімді мүдделі тараптардың қатысуы арқылы ұлттық киберқауіпсіздік тұжырымдамасын танымал ету;

- киберқауіпсіздікті қамтамасыз ету ісінде өңірлік және жаһандық қатысушылардың үйлестірілуіне, ынтымақтастығына және өзара іс-қимылына жәрдемдесу (3.3.2 бабы).

Басым іс-әрекеттердің мақсаты қойылған міндеттерді орындау болып табылады. Мысалы, Еуропалық Одақта киберқауіпсіздікті қамтамасыз етудің ұлттық стратегияларының көпшілігі басым әрекеттер ретінде киберқауіпсіздік саласындағы стандарттарын, нормаларын және заңдарын құруды (қажет жерде), киберқауіпсіздік мәдениетін тек мүдделі тараптар (мысалы, мемлекеттік органдар, ғылыми-білім беру мекемелері, компаниялар мен ұйымдар) арасында ғана емес, сонымен бірге жалпы халықты да, ұлттық және халықаралық ынтымақтастық пен тиісті мүдделі тараптар арасындағы өзара әрекеттестікті дамытуды анықтайды (ENISA, 2014). АҚШ-тың 2018 жылғы Ұлттық киберқауіпсіздік Стратегиясында көрсетілген басым әрекеттерге: «инновацияларды дамыту және енгізу басымдығы»; «киберкеңістіктегі нормалардың жалпыға бірдей сақталуын ынталандыру»; «объективті және

ұжымдық барлаумен көшбасшылық»; «қылмыскерлерді шетелде ұстау жүйесін жетілдіру» және басқа да көптеген әрекеттер кіреді.

Осы басым іс-қимылдардың күтілетін нәтижелері оларды жүзеге асырғаннан кейін қол жеткізілуі тиіс көрсеткіштерді қамтиды (мысалы, киберқауіпсіздік стандарттарын әзірлеу). Мысалы, АҚШ-тың 2018 жылғы Ұлттық киберқауіпсіздік Стратегиясында күтілетін нәтижелерге мыналар кіреді: киберқауіпсіздік құрылымындағы осалдықтарды сәтті жою; «Америка Құрама Штаттарының мүдделеріне қарсы бағытталған деструктивті, зиянды және диверсиялық хакерлік қызметтен болатын залалды азайту немесе «мәжбүрлеу, желілік және басқа сипаттағы шаралар арқылы киберкеңістіктегі жауапты мінез-құлыққа қайшы келетін қызметті» болдырмау және тоқтату»; және Америка Құрама Штаттарының «ұлттық қауіпсіздік мақсаттарына қол жеткізу үшін кибер мүмкіндіктерді пайдалану» қабілеті (US White House, 2018, p. 3).

3. Ұлттық киберқауіпсіздік стратегиялары: өмірлік циклдар, озық тәжірибелер және репозиторийлер.

Ұлттық киберқауіпсіздік стратегиясының өмірлік циклі бес кезеңнен тұрады (ITU, 2018, pp. 16-27):

Бірінші кезең - стратегияны әзірлеу процесінде тиісті мүдделі тараптарды және олардың рөлдерін айқындауды, сондай-ақ стратегияны әзірлеу жоспарын дайындауды көздейтін бастамашылық ету.

Екінші кезең, қолда бар тәжірибеге шолу және сыни талдау елдегі киберқауіпсіздік саласындағы жағдайды бағалауды, киберқауіпсіздік қатерлерін анықтауды және киберқауіпсіздіктің ағымдағы және болашақтағы тәуекелдерін талдауды көздейді.

Үшінші кезең - ұлттық киберқауіпсіздік стратегиясын әзірлеу. Бұл кезең стратегия жобасын дайындауды, тиісті мүдделі тараптармен кеңестерды, ескертулерді ескере отырып, стратегияны түпкілікті пысықтауды және стратегияны жариялауды көздейді.

Төртінші кезең, имплементация, іс-қимыл жоспарын әзірлеуді, стратегия міндеттеріне негізделген қандай бастамалардың іске асырылатынын айқындауды, осы бастамаларды іске асыру үшін қажетті ресурстарды айқындауды және осы іс-қимылдардың нақты іс-қимылдары мен орындалу мерзімдерін айқындауды көздейді. Бұл кезеңде бастамалардың тиімділігін (яғни уақтылығын) және нәтижелілігін (яғни оң нәтижесін) бағалау үшін қызметтің параметрлері мен түйінді көрсеткіштері әзірленеді.

Әдетте, іс-қимыл жоспарларында мақсаттарға қол жеткізу үшін іске асырылуы мүмкін шешімдер (немесе шаралар), міндеттерді орындауға жауапты мүдделі тараптар, міндеттерді орындау мерзімдерін бағалау және қалаған нәтижелерге қол жеткізу үшін пайдаланылатын параметрлер көрсетіледі. Іс-қимыл жоспарлары ұлттық деңгейде (мысалы, Ұлттық қауіпсіздік қызметі, Словакия Республикасының 2015-2020 жылдарға арналған киберқауіпсіздік тұжырымдамасын іске асыру жөніндегі іс-қимыл жоспары) және өңірлік деңгейде (мысалы, киберқауіпсіздікті қамтамасыз ету және киберқылмыстың алдын алу жөніндегі КҚОН (CARICOM) іс-қимыл

жоспары) іске асырылады.

Бесінші кезең, мониторинг және бағалау іс-қимыл жоспарының киберқауіпсіздік стратегиясының міндеттеріне сәйкестігін бағалауды, сондай-ақ стратегия мен іс-қимыл жоспарын олардың өзектілігін сақтайтындығын, елдің киберқауіпсіздікті қамтамасыз ету саласындағы қажеттіліктерін қанағаттандыратындығын және олар киберқауіпсіздіктің жаңа тәуекелдеріне қарсы тұра алатындығын анықтау үшін талдауды көздейді. Егер іс-қимыл жоспарын іске асыру нәтижесінде киберқауіпсіздік стратегиясының міндеттері орындалмаса, іс-қимыл жоспарына өзгерістер енгізіледі. Стратегияға да, егер ол бұдан былай өзекті болып табылмаса және/немесе киберқауіпсіздіктің жаңа қатерлеріне қарсы тұру үшін қолданылмайтын болса, өзгерістер енгізілуі мүмкін.

4. Киберқауіпсіздік мәселелері бойынша халықаралық ынтымақтастық.

Халықаралық Электр байланысы одағы (ХЭО), «басты Дүниежүзілік форум болып табылатын Біріккен Ұлттар Ұйымының мекемесі, оның шеңберінде тараптар АКТ саласын дамытудың болашақ бағытына әсер ететін кең ауқымды мәселелер бойынша консенсусқа қол жеткізе алады», ХЭО үшін «халықаралық ынтымақтастықтың негізі, оның мақсаты ақпараттық қоғам жағдайында сенім мен қауіпсіздікті нығайту саласында шешімдер іздеу үшін стратегияларды ұсыну болып табылатын Жаһандық киберқауіпсіздік бағдарламасын бастамашылық етті. Жаһандық киберқауіпсіздік бағдарламасында ХЭО бес стратегиялық қағидаларды айқындады: құқықтық шаралар, техникалық шаралар, ұйымдастыру шаралары, әлеуетті құру және ынтымақтастық.

Құқықтық принципі киберқауіпсіздік пен кибертәуелді қылмыстарға, сондай-ақ киберкеңістікті пайдалану арқылы жасалатын қылмыстарға қатысты ережелер мен заңдарды біріздендіруге бағытталған. Мысал ретінде киберқылмыстылықпен күрес туралы заңдарды келтіруге болады.

Техникалық принцип қолданыстағы техникалық мекемелерді, киберқауіпсіздік стандарттары мен хаттамаларын, сондай-ақ киберқауіпсіздік қатерлерімен күресу үшін қажетті шараларды қамтиды. Техникалық мекеменің мысалы – «клиенттердің нақты анықталған шеңберіне компьютерлік қауіпсіздікке қатысты оқиғалардың алдын алу үшін де, оларға жауап беру үшін де қызметтер мен қолдау көрсететін ұйым немесе топ» ретінде анықталған компьютерлік қорғаудың бұзылуына қарсы ден қою тобы (CERT).

Ұйымдастыру шараларымен байланысты принципі ұйымдық құрылымдар мен киберқауіпсіздік саласындағы саясатының шараларын және киберқауіпсіздікті қамтамасыз ету саясатын үйлестіруге жауапты мекемелерді қамтиды. Бұл принцип ұлттық киберқауіпсіздік стратегиялары мен киберқауіпсіздікті қамтамасыз етудің ұлттық тетіктерін, сондай-ақ осы стратегиялар мен тетіктердің орындалуын бақылайтын реттеуші органдарды қамтиды.

Әлеуетті құру принципі киберқауіпсіздік саласындағы хабардарлықты,

білім беруді және оқытуды қамтиды. Мысал ретінде жұртшылықты ақпараттандыру науқандары, киберқауіпсіздік саласындағы зерттеулер мен әзірлемелер, кәсіби дайындық, сондай-ақ ұлттық білім беру бағдарламалары мен оқу жоспарлары бола алады. *Ынтымақтастық* қағидаты мекеме аралық және мемлекеттік-жеке меншік әріптестіктерге, ақпарат алмасу желілеріне және ынтымақтастық туралы келісімдерге шоғырланған. Мысал ретінде мемлекеттік-жекешелік әріптестікті дамыту және елдер арасындағы ынтымақтастықты нығайту болып табылатын киберкеңістіктегі халықаралық өзара іс-қимылдың австралиялық стратегиясын (International Cyber Engagement Strategy) келтіруге болады.

5. Киберқауіпсіздік саласындағы істердің жай-күйі.

Киберқауіпсіздік жағдайы - бұл елдің, ұйымның немесе компанияның киберқауіпсіздікті қамтамасыз ету мүмкіндіктерін сипаттау үшін қолданылатын термин. Киберқауіпсіздік жағдайын бағалау үшін бірнеше құралдар қолданылады. Осындай құралдардың бірі Халықаралық Электр байланысы одағының Киберқауіпсіздіктің жаһандық индексі (КЖИ) болып табылады. ХЭО мәліметтері бойынша, КЖИ - бұл елдердің киберқауіпсіздікті қамтамасыз ету ісіне деген адалдығын бағалайтын, олардың киберқауіпсіздік жағдайын және жетілдіруді қажет ететін аспектілерді анықтайтын әлеуетті арттыру құралы. Елдердің киберқауіпсіздік саласындағы істерінің жай-күйі ХЭО Жаһандық киберқауіпсіздік бағдарламасында айқындалған бес қағидалары (құқықтық, техникалық, ұйымдастырушылық шаралар, әлеуетті құру және ынтымақтастық) негізінде бағалануы мүмкін. Атап айтқанда, елдер осы бес қағидаларды ұстанушылық деңгейіне қарай КЖИ балдарын алады. Бұл бағалаулар елдерді *жаңадан бастаған* (яғни, осы қағидаларға өздерінің ұстануын көрсететін алғашқы қадамдар жасайтын елдер), *дамушы* (яғни, осы қағидаларды ұстанатын елдер) және *жетекші елдер* (яғни, осы қағидаларға қатысты жоғары міндеттемелер қабылдаған елдер) топтарына жатқызады (ITU, 2017, p. 13). 2017 жылғы Жаһандық киберқауіпсіздік индексін зерттеу нәтижелері респонденттердің жартысында ұлттық киберқауіпсіздік стратегиясы жоқ екенін көрсетті (ITU, 2017). 2017 жылғы жаһандық киберқауіпсіздік индексін зерттеу нәтижелері сонымен қатар мемлекеттер арасында және олардың аймақтарынан тыс жерлерде киберқауіпсіздікті қамтамасыз ету бойынша қабылданған міндеттемелер бойынша айтарлықтай айырмашылықтарды анықтады. Нәтижелер сондай-ақ елдердің киберқауіпсіздікті қамтамасыз етуге қатысты міндеттемелерінің дәрежесі нақты көрсеткішке байланысты өзгеріп отыратынын көрсетті, яғни елдер бір көрсеткіш бойынша жоғары баға алды, бірақ басқа көрсеткіштер бойынша орташа және төмен бағалар алды. (нәтижелер туралы толық ақпарат алу үшін ITU, 2017 қараңыз). Алайда, күш-жігер тиімді болуы үшін киберқауіпсіздікті қамтамасыз ету саласындағы міндеттемелер барлық көрсеткіштер бойынша орындалуы керек.

Оксфорд Университетінің жанындағы Киберқауіпсіздік бойынша жаһандық әлеуетті құру орталығы (GCSCC) киберқауіпсіздік саласындағы елдердің жағдайын (яғни, киберқауіпсіздікті қамтамасыз ету мүмкіндіктерінің

жетілуін) бағалау үшін «киберқауіпсіздік саласындағы нормативтік реттеу және стратегия», «кибермәдениет пен қоғам», «киберқауіпсіздік саласындағы білім, оқыту және дағдылар», «нормативтік-құқықтық база», сондай-ақ «стандарттар, ұйымдар және технологиялар» сияқты салаларда елдердің күш-жігерін зерттеу арқылы киберқауіпсіздік әлеуетінің жетілу моделін (Cybersecurity capacity Maturity Model (CMM) жасады (Global Cyber Security Capacity Centre, 2016, pp. 10-13). Бұл бағалау елдерге олардың әлеуетінің жетілу деңгейі туралы ақпарат алуға мүмкіндік береді: *бастапқы* (яғни, киберқауіпсіздік жоқ немесе енді дами бастайды); қалыптасқан (яғни, кейбір киберқауіпсіздік бар); *белгіленген* (яғни киберқауіпсіздік бар; ресурстарды бөлу мәселесіне аз көңіл бөлінеді); *стратегиялық* (яғни киберқауіпсіздікке қатысты саналы және теңдестірілген таңдау); және *динамикалық* (яғни, киберқауіпсіздікті қамтамасыз ету шаралары шарттар мен қажеттіліктердің өзгеруіне бейімделеді) (Global Cyber Security Capacity Centre, 2016, p. 7). CMM моделі әлемнің көптеген елдерін жеке-жеке немесе аймақтық зерттеу аясында бағалау үшін қолданылды (Global Cyber Security Capacity Centre, 2018). Киберқауіпсіздік бойынша жаһандық әлеуетті құру орталығы CMM моделіне қосымша киберқауіпсіздік әлеуетін құру материалдары мен озық тәжірибелер туралы ақпаратты қамтитын және елдерге киберқауіпсіздік саласында жағдайын жақсартуға көмектесу үшін ақпарат алмасуды жеңілдететін Cybersecurity Capacity Portal порталын жасады.

Талқылауға арналған сұрақтар:

1. Бұл қағидалар ұлттық киберқауіпсіздік стратегиясына енгізілген бе? Егер иә болса, онда қандай? Егер жоқ болса, онда қандай принциптер кірмейді және неге?
2. Ұлттық киберқауіпсіздік стратегиясына кіретін басқа да принциптер бар ма? Олай болса, қайсысы және олар қандай себептермен қосылуы мүмкін?

9 Тақырып. Киберқауіпсіздік және киберқылмыстылықтың алдын алу: практикалық әдістер мен шаралар.

1. Активтер, осалдықтар және қауіптер.

Киберқауіпсіздікті қамтамасыз ету шаралары ұйымның қызметкерлері, сандық құрылғылар, компьютерлік бағдарламалық қамтамасыз ету және деректер (ITU, 2008) сияқты «маңызды немесе құнды нәрсе, оның ішінде адамдар, мүлік, ақпарат, жүйелер мен жабдықтар» (Maras, 2014b, p. 21) ретінде анықталған активтерді қорғау мақсатында жүзеге асырылады. Активтер әртүрлі зиян түрлеріне сезімтал (яғни осал). Атап айтқанда, активтерде ішкі (немесе кіріктірілген) және сыртқы (немесе енгізілген) *осалдықтар* бар. Мысалы, ақпараттық-коммуникациялық технологияларға (АКТ) қатысты ішкі осалдықтар жүйенің конструкциясында, қауіпсіздік жүйесінің конфигурацияларында, аппараттық және бағдарламалық қамтамасыз етуде және басқа компоненттерде болуы мүмкін (ENISA, 2017). Мысал - бағдарламалық жасақтама қатесі. 2018 жылы Monero криптовалюта

әмиянында бағдарламалық жасақтама қатесі табылды, ол жеке тұлғаларға осы осалдықты криптовалюта аударым сомасын заңсыз екі есе көбейту үшін пайдалануға мүмкіндік берді (Barth, 2018). Керісінше, АКТ құрылғылары сияқты активтердің өзінде сыртқы осалдықтар жоқ. Мұндай осалдықтың мысалы - АКТ пайдаланушысы. Пайдаланушы құрылғыны зиянды бағдарламалармен жұқтыруға сезімтал ететін әрекеттерді орындай алады (мысалы, белгісіз жіберушілердің электрондық хаттарында тіркемелерді ашу). Кірістірілген және енгізілген қасиеттер активтерді қауіп-қатерлерге осал етеді (яғни, жағымсыз салдарға әкелуі мүмкін барлық нәрсе үшін). Бұл қауіптер байқаусызда және қасақана *зиян* келтіруі мүмкін. Мысалы, сандық құрылғының аппараттық құралы ақаулармен жұмыс істеуі мүмкін немесе кірістірілген бағдарламалық жасақтама осалдықтарын пайдалану арқылы әдейі зақымдалуы мүмкін (ENISA, 2017).

2. Тәуекел.

Активтерді қорғау туралы шешімдер белгісіздік жағдайында қабылданады; яғни олар ықтимал қауіптер, осалдықтар және осы осалдықтарды пайдалану туралы толық ақпарат болмаған кезде қабылданады. Бастапқыда *тәуекел* материалдандырылған жағдайда қауіптің және оның әсерінің (немесе салдарының) ықтималдығы (немесе мүмкіндігі) ретінде тар анықтамаға ие болды (Dali and Lajtha, 2012). Бұл тәуекел ұғымы келесі формуламен бейнеленген:

$$\mathbf{Т_{әуекел} = Ы_{қтималдылық,} \times С_{алдары}}$$

Жоғарыда келтірілгенге ұқсас формулалар тәуекелдерді сандық бағалау үшін қолданылады.

Тәуекелдерді бағалау процесі активтердің осалдықтарын анықтауды, ішкі және сыртқы қатерлерді айқындауды және/немесе олар туралы бұқаралық ақпарат құралдарынан, мемлекеттік-жеке әріптестіктерден және/немесе мемлекеттік және жеке секторлардан басқа тұлғалардан ақпарат алуды, сондай-ақ қауіптердің салдарлары мен ықтималдықтарын айқындауды көздейді (NIST, 2018). Тәуекелдерді бағалаудың мақсаты «... қауіптерді анықтау болып табылады; ... осалдықтарды пайдалану мүмкіндігін ескере отырып, келтірілуі мүмкін залал (яғни қолайсыз әсер ету); және... залал келтірілу ықтималдығы» (NIST, 2012).

Тәуекелдерді бағалау аяқталғаннан кейін басымдылығы қолда бар ресурстар (мысалы, қаржылық) және қажеттіліктер негізінде белгіленетін тәуекелдерге ден қою шаралары (яғни *тәуекелдерді өңдеу жөніндегі шаралар*) айқындалады. Бұл кезеңде тәуекелдерді жою, азайту немесе жұмсарту шаралары жүзеге асырылады.

3. Осалдықтар туралы ақпаратты ашу

«Ақпараттық қауіпсіздік» және «киберқауіпсіздік» терминдері бір-бірінің орнына қолданылады, бірақ бұл мүлде дұрыс емес. Ақпараттық қауіпсіздік ұғымының дәйекті анықтамасының болмауына қарамастан, ISO/IEC 27002 стандартына енгізілген анықтама кеңінен қолданылады. ISO/IEC 27002 стандартында ақпараттық қауіпсіздік «ақпараттың құпиялығын, тұтастығын және қол жетімділігін сақтау» ретінде анықталады.

Ақпараттық қауіпсіздік жағдайындағыдай, киберқауіпсіздік ұғымының әмбебап анықтамасы жоқ. Халықаралық Электр байланысы одағына (ХЭО) сәйкес, «киберқауіпсіздік киберортадағы тиісті қауіп-қатерлерге қарсы бағытталған ұйымның немесе пайдаланушының ресурстарындағы қауіпсіздік қасиеттеріне қол жеткізуді және сақтауды қамтамасыз етуге ұмтылысты білдіреді». Осылайша, киберқауіпсіздік тек киберкеңістікті ғана емес, «сонымен қатар... киберкеңістікте жұмыс істейтіндерді және киберкеңістікте қол жетімді болуы мүмкін олардың кез-келген ресурстарын» қорғауды білдіреді.

ISO/IEC 27002 стандарты ақпараттық қауіпсіздікті бақылаудың 14 саласын, сондай-ақ ақпараттық қауіпсіздікті бақылау шараларын іске асыру жөніндегі нұсқаулықты және осы бақылау шараларының әрқайсысына қойылатын талаптарды қамтиды. Бұл салалар: ақпараттық қауіпсіздік саясаты; ақпараттық қауіпсіздікті ұйымдастыру; қызметкерлердің қауіпсіздігі; активтерді басқару; қол жетімділікті бақылау; криптография; физикалық қауіпсіздік және табиғи қауіптерден қорғау; өндірістік қызмет қауіпсіздігі; ақпарат алмасу қауіпсіздігі; жүйелерді сатып алу, әзірлеу және қызмет көрсету; жеткізушілермен қарым-қатынас; ақпараттық қауіпсіздік оқиғаларын басқару; бизнестің үздіксіздік менеджментінде ақпараттық қауіпсіздік аспектілері; және сәйкестік.

Ақпараттық қауіпсіздік пен киберқауіпсіздік осалдықтар туралы ақпаратты ашуға байланысты. Осалдықтарды осы саладағы зерттеушілер мен мамандар анықтаған кезде, мұндай осалдықтар туралы ақпаратты ашу толық немесе жауапты болуы мүмкін. *Толық ашу* бағдарламалық жасақтаманың немесе аппараттық құралдардың осалдығы туралы ақпаратты интернетте (мысалы, веб-сайтта) осы осалдықтар жойылғанға дейін жариялауды қамтиды. Керісінше, *жауапты ашу* аппараттық немесе бағдарламалық жасақтамаға жауапты ұйым осалдықты жойғанға дейін осалдық туралы ақпаратты ашпауды білдіреді. Жауапты ашу кезінде зерттеуші немесе маман зардап шеккен ұйыммен байланысады және ұйым анықталған осалдық үшін түзетуді шығарғанша күтеді. Түзету шыққаннан кейін зерттеуші немесе маман осалдық туралы ақпаратты ресми түрде ашып, осалдықты тапқаны үшін тану мен сыйақы ала алады. Ақпаратты ашудың осы әдісін қолданған кезде зерттеуші немесе маман оған ақпараттық қауіпсіздіктің белгілі осалдықтарының идентификаторын (CVE) беруді сұрауы мүмкін, бұл бағдарламалық жасақтаманың негізгі элементтеріндегі осалдықтарды, сондай-ақ осындай осалдықтарды анықтайтын тұлғаларды бақылау үшін қолданылатын «белгілі киберқауіпсіздік осалдықтарының жалпы сәйкестендіру элементтерінің тізімі» (CVE, n.d.). Толық және жауапты ақпаратты ашу әдістеріне қосымша, зерттеуші немесе маман осалдықты ашпау принципін таңдай алады. Ақпаратты ашудың тағы бір әдісі - *осалдықтарды үйлесімді түрде ашу*, бұл «осалдықтарды анықтаған тұлғалардан ақпарат жинау, тиісті мүдделі тараптар арасында осы ақпаратпен алмасуды үйлестіру және бағдарламалық қамтамасыз етудің осалдықтары туралы ақпаратты ашу және жұртшылықты қоса алғанда, әртүрлі мүдделі тараптарға жағымсыз салдарларды жұмсарту»

дегенді білдіреді.

4. Киберқауіпсіздік және пайдалану қолайлылығын қамтамасыз ету шаралары

Ең дұрысы, тәуекелдерге жауап беру шаралары осы шараларды қолдану ыңғайлылығын қамтамасыз ете отырып, жүйелердің, желілердің, қызметтердің және деректердің құпиялылығын, тұтастығы мен қол жетімділігін қорғауды мақсат етуі керек (NIST, 2018). Сандық құрылғыларды *қолдану ыңғайлылығы* (яғни, оларды пайдалану жеңілдігі) көбінесе осы құрылғылардың және олардың мазмұнының қауіпсіздігінен артықшылығы бар. Дегенмен, қауіпсіздік пен ыңғайлылық міндетті түрде бірін-бірі жоққа шығармайды. Киберқауіпсіздік шаралары қауіпсіздікті де, ыңғайлылықты да қамтамасыз ете алады.

Киберқауіпсіздік шараларына жүйелерге, қызметтерге және деректерге рұқсатсыз қол жеткізуді болдырмау үшін пайдаланушының жеке басын анықтауға бағытталған шаралар жатады. Бұл *аутентификация* шараларына «сіз не білесіз» (мысалы, парольдер, парольдық сөз тіркестері және PIN-кодтар), «сізде не бар» (мысалы, смарт-карталар мен токендер) және «сіз кім екенсіз» (мысалы, саусақ іздері сияқты биометриялық мәліметтер). Көп факторлы аутентификация (КПА) пайдаланушының жеке басын анықтау үшін екі немесе одан да көп аутентификация әдістерін қолдануды қамтиды.

Киберқауіпсіздік шараларының тағы бір түрі - қол жетімділікті басқару. Артықшылықтарды белгілейтін, рұқсат етілген қол жетімділікті анықтайтын және рұқсат етілмеген қол жетімділіктің алдын алатын *қол жеткізуді басқару құралдарына* кіру үшін аттар мен парольдерді қорғауға арналған аутентификация шаралары мен басқа да шаралар, қосымшалар, веб-сайттар, әлеуметтік желілер және басқа да онлайн платформалар мен сандық құрылғылар кіреді. Мысал ретінде смартфонға пароль енгізу әрекеттерінің санын шектеуге болады. Смартфондарда пайдаланушыларға сәтсіз пароль әрекетінен белгілі бір санынан кейін құрылғыдағы барлық деректерді өшіруге мүмкіндік беретін опция бар. Бұл мүмкіндік пайдаланушыларға сандық құрылғы ұрланған және/немесе пайдаланушының авторизациясынсыз қол жеткізілген жағдайда өз құрылғыларындағы деректерді қорғау мүмкіндігін қамтамасыз ету үшін жасалды.

Қол жеткізуді басқарудың басқа мысалдарына парольдің әр қате енгізілуіне күту уақытын қосу және/немесе күн ішінде рұқсат етілуі мүмкін сәтсіз пароль әрекеттерінің санын шектеу және пайдаланушылардың есептік жазбаларын біраз уақытқа бұғаттау жатады. Кіру әрекеттерін басқаратын бұл басқару құралдары пайдаланушылардың есептік жазбаларына рұқсатсыз кіру әрекеттерінен қорғауға арналған. Атап айтқанда, мұндай кідірістер «қатал күш» әдісімен шабуылдардан қорғауға қызмет етеді.

«Қатал күш» әдісімен шабуылы - сынақтар мен қателер әдісімен пайдаланушының есеп деректерін болжау үшін *скриптті* (яғни компьютерлік бағдарламаны) немесе *роботты* (яғни, пайдаланушы аты және/немесе пароль/кіру коды) пайдалану. «Қатал күш» әдісімен шабуылдар кезінде басқалармен қатар ортақ парольдер немесе кіру үшін бұзылған тіркелгі

деректер қолданылады. 2018 жылы пайдаланушыларға Mozilla Firefox браузерінде (веб-шолғыш) сақталған құпия сөздерді шифрлауға мүмкіндік беретін басты құпия сөз функциясын «қатал күш» шабуылымен оңай бұзуға болатындығы анықталды.

Құпия сөздерді жүйе жасайды немесе пайдаланушы жасайды. *Жүйе жасаған парольдер* (яғни, бағдарлама жасаған парольдер) өте қиын және пароль бұзушылардың шабуылына төтеп бере алады (бірақ бұл парольдердің ұзындығына байланысты). Жүйе жасаған парольдерге қатысты мәселе оларды есте сақтаудың қиындығында. Бұл пайдаланушыларға парольді қағазға жазуға немесе оны шолғышта, қосымшада немесе сандық құрылғыда сақтауға әкеледі. Сондықтан *пайдаланушы жасаған парольдерге* артықшылық беріледі. Алайда, пайдаланушы жасаған мұндай құпия сөздерді есте сақтау қиын болуы мүмкін. Жүйелер, қосымшалар және онлайн платформалар көбінесе пайдаланушылар ұстанатын құпия сөздерді құрудың күрделі ережелерін орнатады, парольдердің ең аз белгіленген ұзындыққа сәйкес келуін және жоғарғы және төменгі әріптердің, сандар мен таңбалардың тіркесімін қосуды талап етеді. Осылайша, жүйе жасаған парольдер сияқты, пайдаланушылар жасаған парольдердің көпшілігі есте сақтау қиын.

Сондай-ақ, пайдаланушыларға әр есептік жазба үшін әртүрлі парольдер ұсынылады. Бұл ұсыныстың мақсаты - олардың есептік жазбаларының біріне кіру үшін деректер бұзылған жағдайда пайдаланушыларға келтірілген зиянды азайту. 2017 жылы бір зерттеу компаниясы Интернетте әртүрлі әлеуметтік желілерге, ойындарға, телебағдарламалар мен фильмдерді трансляциялау сайттары және Интернет желісінің басқа сайттарына арналған 1,4 миллиард пайдаланушы аты мен парольдер файлын тапты. Егер осы тұлғалардың кез-келгені құпия сөздерді қайта қолданса, қорғаныс жүйесіндегі мұндай әрекеттер Интернеттегі басқа есептік жазбалардың (сол пайдаланушы аты мен пароль қолданылатын жерде) қауіпсіздігіне қауіп төндіреді. Әр есептік жазба үшін әр түрлі және күрделі парольдерді пайдалану жеке пайдаланушылар үшін белгілі бір қауіпсіздік деңгейін қамтамасыз ете алады, бірақ бұл олардың пайдалану ыңғайлылығына теріс әсер етеді.

5. Қылмыстылықтың ситуациялық алдын алу.

Қылмыстылықтың ситуациялық алдын-алу (ҚСА) қылмыстардың алдын-алу тәсілдеріне және оларды жасау мүмкіндіктерін азайтуға шоғырланған. ҚСА қылмыстың алдын алу бойынша БҰҰ Экономикалық және әлеуметтік Кеңесі Басшылығының маңызды бөлігі болып саналады.

ҚСА тұжырымдамасы нақты әлемдегі қылмыстың алдын-алуға қатысты болса да, оны киберқауіпсіздік тәжірибесі тұрғысынан киберқылмыстылықтың алдын-алу шарасы ретінде де қолдануға болады. Киберқылмыстылыққа қатысты ҚСА шаралары құқық бұзушылықтар жасау үшін мүмкіндіктерді қысқартуға және/немесе болдырмауға және киберқылмыскерлердің қылмыс жасау қабілетін бұзуға бағытталған. Киберқылмыстылықтың алдын алу техникалық шаралары қылмыстылықтың ситуациялық алдын алудың бір түрі болып табылады. Мұндай техникалық шаралардың мысалдарына зиянды бағдарламаларды анықтау бағдарламалары,

трафикті тексеру және бұғаттау арқылы рұқсатсыз кіруді болдырмайтын *брандмауэрлер* мен кибершабуылдарды, жүйелерді, желілерді, деректерді, қызметтерді және тиісті ресурстарды рұқсатсыз кіруді және рұқсатсыз пайдалануды анықтауға мүмкіндік беретін *басып кіруді анықтау жүйелері* жатады.

Корниш пен Кларк (Cornish and Clarke, 2003) қылмыстың алдын алу және азайту стратегиялары мен әдістерін ұсынды. Қылмыстың алдын алудың және/немесе азайтудың ұсынылған бес стратегиясына мыналар кіреді: қылмыс жасау үшін жұмсалған күш-жігердің (қылмыскер тарапынан) артуы; табу және ұстау қаупін арттыру; қылмыс жасағаны үшін күтілетін сыйақыны азайту; қылмыс жасауға әкелетін арандатулар санын азайту; және қылмыс жасау үшін ақтауды жою. Осы стратегиялар шеңберінде көрсетілген барлық стратегиялар мен әдістер қылмыстың барлық түрлеріне қолданыла бермейді (Clarke, 2004). Сонымен қатар, әдістер мен стратегиялар бір-біріне сәйкес келуі мүмкін, ал кейбір әдістер бірден бірнеше стратегияда қолданылуы мүмкін.

ҚСА шаралары киберқылмыстылықтың алдын алу және азайту үшін қолданылуы, бұрын қолданылуы және қазіргі уақытта қолданылуы мүмкін (Maras, 2016). Мысалы, Корниш пен Кларк ұсынған (Cornish and Clarke, 2003) ҚСА стратегиясында көрсетілген әдістердің бірі - табу және ұстау қаупін арттыру үшін «жергілікті басқарушыларды пайдалану». Киберқылмыстылыққа қатысты, белгілі бір жерде мінез-құлықты бақылайтын жергілікті басқарушылар Интернет-қызмет жеткізушілер немесе онлайн-платформалардың әкімшілері мен модераторлары болуы мүмкін. Жергілікті басқарушылар әлеуметтік желілердегі киберқылмыстылықпен күресу үшін қолданылады. Мысалы, Facebook модераторлардың санын көбейтіп, Стивен Стивенс (Steven Stephens) адамды өлтіріп, бұл кісі өлтіруді FacebookLive арқылы таратқаннан кейін зорлық-зомбылық пен қатыгездікті насихаттайтын контентті бақылауды күшейтті. Киберқылмыстылықпен күресу үшін қолданылатын ҚСА әдістерінің кейбірі адам құқығын бұзуы мүмкін (мысалы, контентті бұғаттау немесе жою кезінде).

Қылмыстылықтың жойылуы бір объектіге бағытталған қылмыс қолданыстағы қауіпсіздік шараларына байланысты басқа объектіге қатысты жасалған жағдайда орын алады. Танымал нанымға қайшы, зерттеулер, ең алдымен, қылмыстылықтың ситуациялық алдын-алу міндетті түрде қылмыстың жойылуына әкелмейтінін көрсетеді. Сутенерлардың Backpage және Craigslist Интернет-сайттардағы жеке хабарландыруларды пайдалануын зерттеу көрсеткендей, құқық қорғау органдарының осы Интернет-сайттарына байланысты күш-жігері оларды осы сайттардан шығаралмады, жыныстық қызмет жарнама үшін оларды пайдалануын жалғастырды.

ҚСА шаралары белгілі бір уақытта киберқауіпсіздік қатерлерін материалдандыру мүмкіндігіне шоғырланған. Осылайша, бұл шаралар қауіп-қатерлер жүзеге асады деген болжамға негізделген, сондықтан тиісті шаралар қабылдау қажет. ҚСА шаралары негізінен (бірақ тек қана емес) қылмыс жасауға кедергі келтіруге бағытталған болса да, шындық - бұл шаралар қабылданғаннан кейін де қылмыс жасалуы мүмкін. Осындай ықтималдықтың

болуына байланысты киберқауіпсіздік саласындағы оқиғаларды анықтауға, оларға жауап беру және олардан кейін қалпына келтіруге бағытталған шаралар іске асырылады.

Талқылауға арналған сұрақтар:

1. Тәуекелдерді бағалаудың мақсаты не?
2. ISO/IEC 27002 стандарты ақпараттық қауіпсіздікті бақылаудың қандай салаларын қамтиды?
3. Киберқауіпсіздікті қамтамасыз ету шараларын сипаттаңыз және оларды пайдаланудың ыңғайлылығы неде?

10 Тақырып. Құпиялылық және деректерді қорғау.

1. Жеке өмірге қол сұғылмаушылық: ұғымы мен маңыздылығы.

Жеке өмірге қол сұғылмаушылық - адамның негізгі құқықтарының бірі. Жеке өмірге қол сұғылмаушылық құқығы жеке тұлғалар үшін абсолютті императив болып табылады және адам құқықтары саласындағы халықаралық шарттарда бекітілген, мысалы, 1950 жылғы Адам құқықтары жөніндегі Еуропалық конвенцияның 8-бабында, 1969 жылғы Адам құқықтары туралы американдық Конвенцияның 11-бабында, 1948 жылғы Адам құқықтарының жалпыға бірдей декларациясының 12-бабында және 1966 жылғы Азаматтық және саяси құқықтар туралы халықаралық пактінің 17-бабында. Бұл құқық 1989 жылғы Бала құқықтары туралы Конвенцияның 16-бабында, 1990 жылғы Барлық еңбекші-мигранттар мен олардың отбасы мүшелерінің құқықтарын қорғау туралы Халықаралық конвенцияның 14-бабында және, 2000 жылғы Еуропалық Одақтың негізгі құқықтары Хартиясының 7-бабында және 2006 жылғы мүгедектердің құқықтары туралы Конвенцияның 22-бабында да танылады. Жеке өмірге қол сұғылмаушылықтың әртүрлі тұжырымдамалары бар, олар мыналарды қамтиды: бақылаудан босату құқығы; жалғыз қалу құқығы; өз ойларын, сенімдерін, жеке басын және мінез-құлқын құпия сақтау мүмкіндігі; жеке ақпараттың қашан, не, неге, қайда, қалай және кімге ашылатынын және оның қаншалықты ашылатынын таңдау және бақылау құқығы. Құпиялылық туралы жоғарыда аталған тұжырымдамалардың соңғысы (яғни, жеке ақпаратты таңдау және бақылау құқығы) құпиялылықты ақпаратты (немесе деректерді) қорғаумен байланыстырады.

Жеке өмірге қол сұғылмаушылық құқығы басқа адам құқықтарын жүзеге асыруға мүмкіндік береді және осы құқықтармен тығыз байланысты. Жеке өмірге қол сұқпаушылық пікір білдіру бостандығына, ой, діни сенім, жиналыстар мен бірлестіктер бостандығына құқықтарды жүзеге асыру үшін қажетті шарт болып табылады. Жеке өмірге қол сұғылмаушылық құқығы өзін-өзі анықтау құқығымен де байланысты. 1981 жылғы Африка адам құқықтары хартиясының 20(1) бабында: «барлық халықтар өмір сүруге құқылы. Олар өзін-өзі анықтаудың сөзсіз және ажырамас құқығына ие. Олар өздерінің саяси мәртебесін еркін анықтайды және экономикалық және әлеуметтік дамуында өздері таңдаған саясатты ұстанады». Өзін-өзі анықтау құқығының маңызды

аспектісі-таңдау жасау және мәжбүрлеусіз өз таңдауымен әрекет ету (*жеке автономия*). Бұл таңдау физикалық әрекеттерге ғана емес, интернеттегі әрекеттерге де қатысты. Адамның жеке өмірінің ажырамас аспектісі - бұл жеке автономия және өзін-өзі анықтау құқығы. Өзін-өзі анықтау құқығы адамдарға өзіндік өмір сүруге, таңдау еркіндігіне ие болуға, сондай-ақ өздері туралы қандай ақпаратты көруге, ашуға және бөлісуге болатындығын таңдауға және бақылауға мүмкіндік береді.

2. Құпиялылық және қауіпсіздік.

Ақпаратты ашуды бақылау және таңдау адамның жеке басын сәйкестендіру және өз қалауы бойынша әрекет ету еркіндігі құқығымен байланысты. Демек, жеке өмірге қол сұғу құқығы оның жеке басын ашпау құқығымен байланысты. *Анонимділік* пайдаланушыларға өздерін және/немесе іс-әрекеттерін басқаларға ашпай-ақ іс-әрекеттерді жасауға мүмкіндік береді (Maras, 2016). Интернеттегі анонимділіктің арқасында «жеке пайдаланушылар мен топтар интернеттегі ортада құпия кеңістікке ие болады, онда олар белгілі бір пікірлерді ұстанып, ерікті және заңсыз араласудан немесе қол сұғушылықтан қорықпай, сөз бостандығын қолдана алады». Осылайша, *құпиялылық* ақпараттық-коммуникациялық технологияларды пайдаланушыларға өздерінің жеке басын сәйкестендірусіз ойларды, пікірлерді, көзқарастар мен идеяларды білдіру үшін қорқыту, кек алу және мәжбүрлеудің немесе санкциялардың басқа түрлерінен қорықпайтын кеңістікті ұсынады. Тиісінше, «электрондық хабарламалардың қауіпсіздігін қамтамасыз етудің және құпиялылығын қорғаудың техникалық құралдары, оның ішінде ... анонимділікті қамтамасыз ету жөніндегі шаралар адам құқықтарын, атап айтқанда жеке өмірге қол сұғылмаушылыққа, өз пікірін еркін білдіруге және бейбіт жиналыстар мен ассоциация еркіндігіне құқықтарды жүзеге асыруды қамтамасыз ету үшін маңызды мәнге ие болуы мүмкін». Осыған байланысты «мемлекеттер мұндай техникалық шешімдерді пайдалануға кедергі жасамауы тиіс және оларға қатысты кез келген шектеулердің халықаралық құқық бойынша (адам құқықтары саласындағы) мемлекеттердің міндеттемелеріне сәйкес келуін қамтамасыз етуі тиіс».

Жеке басын ашпау құқығы кейбір адамдарға басқа адамдарға дөрекі, кемсітушілік, нәсілшіл, жеккөрушілік және/немесе қорлайтын сөздер айтуға батылдық береді, егер олардың жеке тұлғалары белгілі болса, олар ешқашан өздеріне жол бермейді деген пікір бар. Бұл пікір кейбір адамдарға қатысты болса да, басқа адамдар да кездеседі, олар мұндай мәлімдемелерді таратқан кезде өздерінің жеке басын ашуға батылдық береді. Олар пікірлестермен танылып, өз жақтастарын іс-әрекетке итермелеу үшін өздерінің жеке басын ашады. Мило Яннопулос, сенсациялық жаңалықтарды жариялауға мамандандырылған құқықтық басылымның бұрынғы бас редакторы (Breitbart) өзінің нәсілшіл, мизогинистік, иммигрантқа қарсы және мұсылманға қарсы сөздерімен танымал, сонымен қатар балама оң және ультра оңшыл қозғалыстардың мүшелері арасында танымал болу үшін басқа да жеккөрушілік сөздерді таратумен және/немесе сол қозғалыстардың жақтаушыларымен танымал болды және басқа адамдарды өзінің жеккөрушілік

сөздерінің нысаны болған адамдарға қатысты ұқсас әрекеттерге итермеледі.

Адамның жеке басын және оның орналасқан жерін анықтау міндеті анонимділікке және Tor сияқты құпиялылықты арттыру технологияларын қолдануға байланысты қиын болуы мүмкін. *Құпиялылықты арттыру* технологиясының тағы бір мысалы - шифрлау. *Шифрлау* пайдаланушылардың ақпараттары мен хабарламаларына үшінші тұлғалардың қол жеткізуіне кедергі келтіреді. Әлемнің көптеген елдерінің үкіметтері терроризм, ұйымдасқан қылмыстылық және балаларды жыныстық қанау сияқты ауыр қылмыстылықпен күресу үшін шифрланған хабарламалар мен ақпаратқа қол жетімділікті қамтамасыз ету қажеттілігі туралы айтты. Сондықтан кейбір елдерде шифрланған хабар алмасу қызметтері заңсыз болып саналады.

Telegram, 200 миллионнан астам адам пайдаланатын шифрланған хабарлама қосымшасы кейбір елдерде сотта бұғатталды, өйткені компания осы елдердің үкіметтеріне осы бағдарлама арқылы жіберілген пайдаланушылардың хабарламаларын бақылау үшін шифрлау кілттерін беруден бас тартты. Кейбір елдерде бэкдор құру және шифрды шешуге арналған кілттерді беру туралы міндетті талап қойылды, ал басқа елдерде билік компанияларға терроризм сияқты ауыр қылмыстармен күресу үшін бэкдор құру және шифрлау кілттерін беру туралы өтініш білдірді. Алайда, мұндай бэкдор құру және шифрды шешуге арналған кілттерді беру деректерге қол жеткізуді теріс пайдалану жағдайларына әкелуі мүмкін (мысалы, деректерді үкіметтер бастапқы рұқсат шеңберінен тыс кез-келген іс бойынша күтпеген мақсаттар үшін пайдалана алады), сондай-ақ қылмыскерлер бұл бэкдор мен кілттерді ақпаратты қарау, көшіру, жою және/немесе өзгерту мақсатында қол жеткізу үшін пайдалану жағдайларына.

3. Құпиялылықты бұзатын киберқылмыскерлер

Киберқылмыстар адамдардың жеке өміріне қол сұғылмаушылық және олардың жеке деректерінің қауіпсіздігі құқығын бұзады, мұндай киберқылмыстарға, атап айтқанда, хакерлік шабуылдар, зиянды бағдарламалар, жеке деректерді ұрлау, қаржылық алаяқтық, медициналық алаяқтық және жеке ақпаратты, хабарламаларды, бейнелер мен бейне және аудиожазбаларды осы адамдардың келісімінсіз немесе рұқсатынсыз ашуға байланысты адамдарға қатысты кейбір қылмыстар жатады.

Деректер заңды және заңсыз әрекет ететін субъектілерімен Интернет желісінде және желіден тыс тауар ретінде қарастырылады (Maras, 2016). Сондықтан деректер киберқылмыскерлердің негізгі мақсаты болып табылады. Деректер сонымен қатар көптеген киберқылмыстарды жасауда ажырамас рөл атқарады, ең алдымен олар дұрыс қорғалмағандықтан және заңсыз алу үшін қол жетімді болуы мүмкін. Деректердің жария болу жағдайлары шифрланған флеш-жинақтауыштардың және басқа да деректерді сақтау құрылғыларының (негізінен ноутбуктер мен смартфондардың) жоғалуы немесе ұрлануы, жүйелер мен деректер қауіпсіздігінің төмен деңгейі, дерекқорға рұқсатсыз кіру немесе дерекқорға санкцияланған қолжетімділіктің асып кетуі, сондай-ақ деректерді кездейсоқ ашу, жария ету немесе жариялау нәтижесінде орын алады. Төменде деректердің ағып кетуінің белгілі жағдайлары келтірілген.

Үндістан үкіметінің Ұлттық орталықтандырылған жеке деректер базасы (Aadhaar) биометриялық деректерді (мысалы, саусақ іздері мен ирис суреттері) және 1,2 миллиард Үнді азаматтарының сәйкестендіру деректерін және қаржылық, мемлекеттік, коммуналдық және басқа да қызметтерді көрсету кезінде азаматтардың жеке басын тексеру үшін пайдаланылатын деректерін сақтайды, 2018 жылы биометриялық деректерден басқа қол жеткізу аттары, он екі таңбалы сәйкестендіру нөмірлері, телефон нөмірлері, электрондық пошта және пошта индекстері сияқты жеке деректердің бұзылу проблемасына тап болды.

2017 жылы Jigsaw Holdings елдің жетекші риэлторлық компанияларының бірінде деректердің жайылып кетуі нәтижесінде Оңтүстік Африканың шамамен 30 миллион тұрғынының деректері, оның ішінде аты-жөні, жынысы, кірісі, жұмысқа орналасу тарихы, сәйкестендіру нөмірлері, телефон нөмірлері және үй мекен-жайы желіге тарады.

2013 жылы Yahoo-ның үш миллиардтан астам пайдаланушысының жеке деректері, оның ішінде аттары, электрондық пошта мекенжайлары, парольдері (оңай айналып өтуге болатын шифрлау) және туған күні бұзылды.

Deloitte, жаһандық консалтингтік фирма, 350-ге жуық клиенттің пайдаланушы аты мен пароль туралы деректеріне қорғалмаған есептік жазба арқылы қол жеткізген хакерлердің шабуылына ұшырады.

2016 жылы 49 миллионнан астам Түркия азаматтарының жеке деректері (яғни ұлттық идентификатор, аты, жынысы, ата-анасының аты, үй мекен-жайы, туған күні және туған қаласы) желіге орналастырылды және іздеу мүмкіндігі бар мәліметтер базасы арқылы қол жетімді болды.

2016 жылы Филиппинде «қара бас киімді» хакерлер сайлау комиссиясының веб-сайтына (COMELEC) рұқсатсыз кіргеннен кейін 55 миллионнан астам сайлаушылардың жеке және биометриялық деректері ашылды.

Деректердің қауіпсіздігін қамтамасыз ету ауыртпалығы көбінесе деректері ұрланған адамдарға жүктеледі. Бұл адамдарға қосымшалардың, веб-сайттардың, әлеуметтік желілердің және басқа да онлайн платформалардың қауіпсіздік параметрлерін жаңарту және басқалармен бөлісетін жеке деректерді жою және/немесе азайту арқылы өздерінің «сандық іздерін» азайту қажеттілігі туралы хабарланады (Maras, 2016). Жәбірленушінің мүдделеріне бағытталған мұндай тәсіл деректерді қорғау үшін жауапкершілікті қылмыскерлер мен қауіпсіздік жүйелері бұзылған компанияларға емес, киберқылмыскерлердің құрбандарына жүктейді. Шындық мынада, зардап шеккендер өздерінің жеке деректерін «олардың бақылауынан тыс ... үшінші тараптардың деректер базасында сақталған және осы дерекқорлардан ұрланған кезде қорғай алмайды» (Maras, 2016, p. 289). Сонымен қатар, бүгінде «сандық іздерді» азайту міндеті күрделене түсуде. Деректерді жинауды, талдауды немесе пайдалануды қаламайтын адамдар үшін іс жүзінде балама нұсқалар жоқ. Мысалы, әлеуметтік желілерді пайдаланатын адам екі мүмкін нұсқаның бірін таңдайды: әлеуметтік медиа платформасын пайдалану құқығын алу үшін талап етілетін жеке ақпараттың ең аз мөлшерін ұсыну (іс

жүзінде бұл қызметті пайдалану үшін «төлем») немесе мұндай ақпаратты беруден бас тарту және платформаны пайдаланбау. Басқа балама нұсқалар ұсынылмайды. Интернет заттарына қатысты құрылғылар оларды пайдалану мүмкіндігін алу үшін жеке ақпаратты ұсынуды талап етеді. Нарықта пайда болатын жаңа құрылғылардың, тіпті бұрын - соңды Интернетке қосылмаған, мысалы, тұрмыстық техника, зергерлік бұйымдар, киім және ойыншықтар - қазір интернетке қол жетімді екенін байқауға болады, егер олар мұндай функционалдығы жоқ құрылғыны сатып алу пайдасына таңдау жасаса, тұтынушыларға аз және аз нұсқалар қалдырады.

4. Деректерді қорғау туралы заңнама

Дербес деректерді қорғау адам құқықтары саласындағы халықаралық шарттарда көзделген жеке өмірге қол сұғылмаушылық құқығына сәйкес жүзеге асырылады. Мысалы, адам құқықтары жөніндегі Еуропалық сот телефонды, электрондық поштаны және Интернетті пайдалануға қатысты деректер (*Coplandv. United Kingdom, 2007 §§ 41-42),* және компьютерлік серверлерде сақталған деректер *(Wieser and bicos Beteiligungen GmbH V. Austria, § 45*) адам құқықтары жөніндегі Еуропалық конвенцияның 8(1) бабының қолданылу аясына жатады деп қаулы етты. Жеке деректерді сақтаудың өзі пайдаланушының жеке өмірге қол сұғу құқығын бұзу ретінде қарастырылуы мүмкін. Бұзушылықтың болу фактісі деректер алынған контекстке, оларды жинау, өңдеу және пайдалану әдісіне, сондай-ақ алуға болатын нәтижелерге байланысты. Жеке деректерді қамтитын дерекқорлар жергілікті және шетелдік мемлекеттік және жеке ұйымдардың сұрауы, іздеуі, өңдеуі, жаңартуы және қарауы үшін қол жетімді. Ақпаратты жинауды, сақтауды, пайдалануды және оны жеке және мемлекеттік ұйымдардың алмасуын басқару рәсімдері нақты елге байланысты өзгеріп отырады. Пайдаланушылардың деректерді өңдеу туралы ақпарат алуға құқығы бар; өңделген деректерге қол жеткізу құқығы; өңделген деректерді түзету құқығы; деректерді жою құқығы («ұмытып кету құқығы»; деректер субъектісі өз деректерін деректер бақылаушыларының журналдарынан жоюды талап етуге, сондай-ақ деректер субъектісінің дербес деректерін одан әрі пайдалануға және үшінші тұлғалардың беруіне жол бермеуін талап етуге құқылы); деректерді өңдеуге қарсылық білдіру құқығы; деректерді өңдеуді шектеу құқығы; деректердің тасымалдану құқығы (яғни, деректер субъектісі бақылаушыға берген жеке деректерін алуға және осы деректерді басқа бақылаушыға беруге құқылы); және автоматтандырылған шешім қабылдау процесіне қарсылық білдіру құқығы (мысалы, профильді қалыптастыру).

2013 жылғы жеке өмірге қол сұғылмаушылықты қорғау және дербес деректерді трансшекаралық беру жөніндегі Басшылықта деректерді қорғаудың және жеке өмірге қол сұғылмаушылықтың мынадай принциптері баяндалған:

Жиналған деректер көлемін шектеу принципі. Жиналған жеке деректердің көлемі белгілі бір шектерге ие болуы керек; барлық осы деректер заңды және адал түрде алынуы керек - егер мүмкін болса, онда деректер субъектісінің келісімімен.

Деректер сапасының принципі. Дербес деректер олар пайдаланылатын мақсаттарға сәйкес келуі тиіс; аталған мақсаттарға сәйкес қажетті шамада дербес деректер дәл, толық және үнемі жаңартылып отыруы тиіс.

Мақсаттарды нақтылау принципі. Дербес деректер жиналатын мақсаттар көрсетілген деректер жиналған кезден кешіктірілмей нақтылануға тиіс, ал оларды кейіннен пайдалану аталған не ұқсас (үйлесімді) мақсаттарға қол жеткізумен шектелуге тиіс, олар осы мақсаттар қайта қаралған сайын көрсетілуге тиіс.

Деректерді пайдалануды шектеу принципі. Дербес деректер жария етілмеуге, пайдалануға берілмеуге немесе 9-тармақта көрсетілгеннен өзге мақсаттарда өзгеше түрде пайдаланылмауға тиіс, бұған мынадай жағдайлар қосылмайды:

a) деректер субъектісі оған өз келісімін берсе; не

b) бұл заңмен рұқсат етілген.

Деректерді қорғау принципі. Дербес деректер деректерді жоғалтуға, санкцияланбаған қол жеткізуге, жоюға, пайдалануға, өзгертуге немесе жариялауға байланысты тәуекелдерден қорғаудың тиісті тетіктерімен қамтамасыз етілуге тиіс.

Ашықтық принципі. Жеке деректерге қатысты тәжірибе мен саясат саласында ашықтықтың жалпы саясаты болуы керек. Жеке деректердің болу фактісі мен сипатын, оларды пайдаланудың негізгі мақсаттарын, сондай-ақ деректерді басқарушының жеке басын және әдеттегі орналасқан жерін анықтауға арналған құралдар үнемі дайын болуы керек.

Жеке қатысу принципі. Әрбір деректер субъектісі (жеке тұлға) келесі құқықтарға ие болуы керек:

деректерді иеленушіден не осы деректерді иеленушіде аталған деректер субъектісіне қатысты дербес деректердің бар-жоғын растауды алу;

өзіне қатысты дербес деректерді ақылға қонымды мерзімдерде; төлемақы алынған жағдайда - шамадан тыс болып табылмайтын тариф бойынша; ақылға қонымды және ауыртпалық салынбайтын рәсім шеңберінде; және түсінуге ыңғайлы нысанда алуға;

(a) және (b) тармақтарына сәйкес берілген ақпарат беруге арналған өтінімді қанағаттандырудан бас тартқан жағдайда, бас тарту себептері туралы түсіндірмелер алуға және мұндай бас тартуға наразылық білдіруге; сондай-ақ наразылық қанағаттандырылған жағдайда мұндай деректердің жойылуын, түзетілуін немесе толықтырылуын талап етуге құқылы.

Есеп беру принципі. Деректерді басқарушы жоғарыда аталған қағидаттардың сақталуын қамтамасыз ететін шараларды қабылдау үшін жауап беруі керек.

Деректер көптеген киберқылмыстарды жасауда және киберқылмыстылыққа осалдық факторларының пайда болуында ажырамас рөл атқарады. Деректер пайдаланушыларға (жеке тұлғаларға, жеке компанияларға, ұйымдарға және үкіметтерге) сансыз мүмкіндіктер беретініне қарамастан, бұл артықшылықтарды кейбір адамдар қылмыстық мақсатта қолдана алады (және қазірдің өзінде қолдануда). Атап айтқанда, деректерді

жинау, сақтау, талдау және деректермен алмасу процестері көптеген киберқылмыстарды жасауға, сондай-ақ пайдаланушылардың ақпараттандырылған келісімінсіз және саналы таңдауынсыз, сондай-ақ қажетті құқықтық қорғау және қауіпсіздік құралдарынсыз деректердің үлкен көлемін жинауға, сақтауға, пайдалануға және таратуға мүмкіндік береді. Оның үстіне, мәліметтерді агрегаттау, талдау және беру үкіметтер мен ұйымдар дайын емес ауқымда жүреді, бұл киберқауіпсіздік тәуекелдерін тудырады. Құпиялылық, деректерді қорғау және жүйелердің, желілердің және деректердің қауіпсіздігі туралы ұғымдар өзара байланысты. Осыған байланысты киберқылмыстылықтан қорғауды қамтамасыз ету үшін пайдаланушылардың деректері мен құпиялылығын қорғауға арналған қауіпсіздік шаралары қажет.

Талқылауға арналған тапсырма:

Алдын ала белгіленген елдердің қорғау туралы заңнамасын зерттеу негізінде мыналарды анықтаңыз:

1. Деректерді қорғау туралы ұлттық заң (немесе заңдар).
2. Деректерді қорғау жөніндегі ұлттық орган.
3. Деректерді қорғау туралы ұлттық заңдардың сақталуын қамтамасыз етуге жауапты мекеме және/немесе орган.
4. Деректерді жинау және өңдеу принциптері.
5. Деректерді беруді және деректердің тарағаны туралы хабарламаны реттейтін ережелер.
6. Деректер қауіпсіздігін қамтамасыз ету жөніндегі талаптар.

11 Тақырып. Кибертехнология арқылы жасалған зияткерлік меншік саласындағы қылмыстар.

1. Зияткерлік меншік.

Дүниежүзілік зияткерлік меншік ұйымы (ДЗМҰ) *зияткерлік меншіктің* келесі анықтамасын береді: «адам ақылының жаратылысының нәтижесі. ЗМ объектілеріне өнертабыстар, әдеби және көркем шығармалар, символика, коммерциялық мақсатта қолданылатын атаулар мен кескіндер жатады». Инновацияларға, туындыларға құқықтар, идеялардың бірегей көрінісі және бизнесті жүргізудің құпия әдістері мен процестері ұлттық және Халықаралық зияткерлік меншік туралы заңнамамен қорғалады. 1967 жылғы Дүниежүзілік зияткерлік меншік ұйымын құратын (1979 жылы өзгертілген) Конвенцияның 2 (viii) бабына сәйкес, бұлар:

құқықтар: ... әдеби, көркем және ғылыми шығармалар, ... әртістердің орындаушылық қызметі, дыбыстық жазбалар, радио және теледидар бағдарламалары, ... адам қызметінің барлық салаларындағы өнертабыстар; ... ғылыми жаңалықтар; ... өнеркәсіптік үлгілер; ... тауарлық белгілер, қызмет көрсету белгілері, фирмалық атаулар және коммерциялық белгілер; ... жосықсыз бәсекелестікке қарсы қорғау, сонымен қатар өндірістік, ғылыми, әдеби және көркем салалардағы зияткерлік қызметке қатысты барлық басқа

құқықтар.

Зияткерлік меншікке қол жеткізу, оны тарату және/немесе алдын ала рұқсатсыз және/немесе осындай рұқсаттың қолданылу мерзімі аяқталғаннан кейін және зияткерлік меншік иесінің немесе иелерінің құқықтарын бұза отырып пайдалану зияткерлік меншік саласындағы қылмыс болып саналады (*зияткерлік меншікті ұрлау* деп те аталады). Зияткерлік меншік құқығы жеке меншік құқығы ретінде танылатындықтан, зияткерлік меншік қылмыстары жеке мүлікті ұрлау нысаны ретінде қарастырылады, тіпті егер ол ұрлық туралы жалпы қабылданған түсінікке сәйкес келмесе де (яғни иеліктен айыру). Мысалы, егер адам зергерлік бұйымдарды ұрлап кетсе, ол өзінің (материалдық) мүлкін жоғалтады, өйткені ол бұдан былай бұл зергерлік бұйымдарға қол жеткізе алмайды. Алайда, зияткерлік меншік жағдайында, тіпті мүлік «ұрланған» болса да (яғни, ол рұқсатсыз пайдаланылады және тұтынылады), зияткерлік меншік иесі оны меншіктен айырмайды, өйткені ол әлі де оның иелігінде. Ол жоғалтқанның бәрі бақылау, басқару және кейіннен зияткерлік меншікті пайдаланудан алуға болатын экономикалық пайда болып табылады, оны. Еңбек үшін сыйақыдан айыру (яғни зияткерлік меншікті құрғаны үшін) ұлттық экономиканың өсуі үшін аса маңызды зияткерлік меншік объектілерін құру үшін теріс ынталандыру болып табылады (ДЗМҰ, 2009). Осыған байланысты ДЗМҰ «зияткерлік меншіктің теңдестірілген және тиімді жүйесінің көмегімен барлық елдердің әлеуметтік-экономикалық және мәдени дамуы мүддесінде инновациялық және шығармашылық қызметке ықпал етеді».

Зияткерлік меншік құқықтарын қорғау мақсатында бірнеше халықаралық конвенциялар, келісімдер мен шарттар (бұдан әрі - шарттар) қолданысқа енгізілді. 1886 жылғы әдеби және көркем шығармаларды қорғау жөніндегі Берн конвенциясы мысал бола алады (1979 жылы енгізілген түзетулермен), онда мемлекеттердің зияткерлік меншікті қорғау жөніндегі міндеттемесі белгіленеді және зияткерлік меншікті қорғаудың ең төменгі стандарттары айқындалады. Берн конвенциясының сақталуын қамтамасыз ету жөніндегі алаңдаушылыққа байланысты Дүниежүзілік сауда ұйымы (ДСҰ) 1994 жылғы (1995 жылы күшіне енген) зияткерлік меншік құқықтарының сауда аспектілері жөніндегі келісімді (Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) қабылдады. TRIPS келісімі ДСҰ-ға мүше елдерден Берн конвенциясы және басқа шарттар аясында қабылданған міндеттемелерін орындауды талап етеді. Дүниежүзілік сауда ұйымы TRIPS келісімінің орындалуын бақылайды және басқалармен қатар зияткерлік меншікке қатысты саясат, заңдар, ережелер, сондай-ақ зияткерлік меншік құқықтарын қорғау жөніндегі міндеттемелердің орындалуын бақылау тетіктері үшін стандарттарды белгілейді.

2. Зияткерлік меншік түрлері.

Зияткерлік меншікке авторлық құқықтар, тауарлық белгілер, патенттер және өнеркәсіптік құпиялар кіреді.

Авторлық құқық

Авторлық құқықтар 1886 жылғы әдеби және көркем туындыларды

қорғау жөніндегі *Берн конвенциясының* 2(1) бабында мынадай түрде айқындалатын «әдеби және көркем туындыларға» құқықтарды қамтиды:

«Әдеби және көркем шығармалар» термині әдебиет, ғылым және өнер саласындағы барлық туындыларды қандай тәсілмен және қандай нысанда білдірілсе де, мынадай түрде қамтиды: кітаптар, брошюралар және басқа да жазбаша туындылар; дәрістер, үндеулер, уағыздар және басқа да осыған ұқсас туындылар; драмалық және музыкалық-драмалық туындылар; хореографиялық туындылар мен пантомималар; мәтіні бар немесе мәтіні жоқ музыкалық шығармалар; кинематографиялық туындылар, оларға теңестірілетін кинематографияға ұқсас тәсілмен жазылған туындылар; суреттер, кескіндеме, сәулет, мүсін, графика және литография туындылары; фотографиялық туындылар, оларға теңестірілген фотосуретке ұқсас тәсілмен жазылған туындылар; қолданбалы өнер туындылары; географияға, топографияға, архитектураға немесе ғылымдарға қатысты суреттер, географиялық карталар, жоспарлар, эскиздер және пластикалық туындылар.

Интернеттегі авторлық құқықты бұзу *сандық қарақшылық* деп аталады, ол авторлық құқықпен қорғалатын туындыларды орналастыруды, беруді, жүктеуді және қол жеткізуге, пайдалануға және таратуға заңда көзделген рұқсатты алмай-ақ оларды (мысалы, кітаптар, музыка және фильмдер) алмасуды қамтиды. Мысал ретінде Napster, тең-теңімен желілік файл алмасу жүйесі арқылы музыканы заңсыз таратуға мүмкіндік беретін онлайн-платформа. *Сауда белгілері* - бұл кейбір көздердің тауарларын немесе қызметтерін басқаларынан ажыратуға мүмкіндік беретін идентификаторлар (Maras, 2016). Мұндай көз кәсіпорын, жеке тұлға немесе географиялық орналасуы болуы мүмкін. Сауда белгілері, басқалармен қатар, тауарлардың, қызметтердің және брендтердің ажырамас бөлігі болып табылатын және оларды бір-бірінен ажыратуға мүмкіндік беретін логотиптер, символдар, суреттер, атаулар мен ұрандарды қамтуы мүмкін. Тауарлық белгілерді құрайтын идентификаторлар тауар белгілері иелерінің еңбегі, ақшасы, білімі мен дағдылары арқылы құндылыққа ие болады. Мұндай сатып алынған құндылық тауардың немесе қызметтің сипаттамаларына, сапасына және/немесе сенімділігіне негізделген. Сауда белгілері олардың иелерін жосықсыз бәсекелестік тәжірибесінен қорғайды, оның мақсаты тауар белгісі иесінің тауарды немесе қызметті әзірлеуге және/немесе таратуға салған инвестицияларынан пайда табуға тырысу болып табылады. Сонымен қатар, сауда белгілері тұтынушыларды тауар немесе қызмет көзін тануға көмектесу арқылы қорғайды. *Географиялық нұсқаулар* (немесе *шыққан жерінің атаулары*) зияткерлік меншіктің қорғалатын нысаны болып табылады. «Әдетте ауылшаруашылық өнімдеріне, тамақ өнімдеріне, шараптарға және күшті спирттерге, қолөнер және өнеркәсіптік өнімдерге қатысты қолданылатын географиялық белгілерді, бұл аймақта өнім жалпы қабылданған стандартты тәжірибеге сәйкес жасалған жағдайларды қоспағанда, қолдануға болмайды.

Тауар белгілерін жалған жасау (тауар немесе қызмет оның заңды иесінің тауар белгісімен таңбаланса, бірақ осы тауар немесе қызмет тауар

белгісінің заңды иесінің өзінікі болып табылмаса) жалпы әлемдік жаһандық проблема болып табылады және контрафакцияның мұндай нысаны ұйымдасқан қылмыстылықты қаржыландырады деген қауіп айтылады. Жалған сауда белгілері бар тауарларға зергерлік бұйымдар, аксессуарлар, киім, аяқ киім, электроника, ойыншықтар, тұрмыстық техника, өндірістік бөлшектер, тамақ және (алкогольді және алкогольсіз) сусындар, косметика және жеке гигиена құралдары, дәрі-дәрмектер және т.б. кіреді. Бұл контрафактілік тауарлар денсаулыққа, қауіпсіздікке, еңбекті қорғауға және қоршаған ортаға үлкен проблемалар туғызады (UNODC, 2014). Жалған сауда белгілері бар өнімдер жеке және интернет арқылы сатып алынады және сатылады (Maras, 2016). Тіпті контрафактілік өнімдердің логотиптерін, қаптамаларын және басқа да өнеркәсіптік үлгілерін интернеттен және желіден тыс сатып алуға болады.

Патент - бұл ұлттық және/немесе халықаралық деңгейде қорғауды қамтамасыз ете алатын атқарушы органда тіркелген жаңа және бірегей туындыларға, жаңашыл әзірлемелерге және өнертабыстарға құқық. Патенттер патент иесінің рұқсатынсыз (яғни, нақты көрсетілген келісімсіз немесе мақұлдаусыз) жаңалықтарды пайдалануға тыйым салуға мүмкіндік береді. Үлгілерге (немесе *өнеркәсіптік үлгілерге*) патенттер зияткерлік меншіктің қорғалатын нысаны болып табылады. Өнеркәсіптік үлгілер зияткерлік меншіктің бір түрі болып саналады, өйткені бұл үлгілер тұтынушыларға эстетикалық жағымды болу және тауарлар арасындағы тұтынушылардың таңдауына әсер ету мақсатында жасалады. Демек, өнеркәсіптік үлгілер өнімнің бәсекеге қабілеттілігі мен коммерциялық құндылығына әсер етеді.

Өнеркәсіптік құпиялар - бұл құпия болып табылатын және компанияның бәсекелестік артықшылықтарын қорғайтын бизнес-процестер мен іскери тәжірибелер туралы құнды ақпарат (Maras, 2016). Өнеркәсіптік құпиялар құпия стратегияларды, әдістерді, процестерді және формулаларды қаржылық, іскерлік, ғылыми, техникалық-экономикалық және инженерлік ақпараттың кез-келген түрлері, оның ішінде құрылғы, жоспарлар, мәліметтер жиынтығы, бағдарламалық құрылғылар, формулалар, дизайн, прототиптер, әдістер, технологиялар, процестер, рәсімдер, бағдарламалар немесе кодтар сияқты, олар қалай сақталғанына, жүйеленгеніне немесе физикалық түрде, электронды түрде, графикалық түрде, фотосуретте немесе жазбаша түрде сақталғанына қарамастан қамтуы мүмкін және бәсекелестік артықшылықты сақтауға мүмкіндік береді (АҚШ Заңдарының 18 титулы §1839(3) қараңыз).

Зияткерлік меншіктің басқа нысандарынан айырмашылығы, «өнеркәсіптік құпиялар тіркеусіз қорғалады» (яғни, «қандай да бір ресми рәсімдерсіз») және осылайша «шектеусіз уақыт аралығында қорғалады».

3. Кибертехнологиялар арқылы жасалатын авторлық құқықтар мен тауар белгілеріне қатысты құқық бұзушылықтардың себептері, негіздері және болжамды себептері.

Кибертехнология арқылы жасалған зияткерлік меншік қылмыстарының мүмкін түсіндірмелері ретінде әртүрлі криминологиялық, социологиялық, психологиялық және экономикалық теориялар ұсынылады (осы және басқа

теорияларды кибертехнология арқылы жасалған зияткерлік меншік қылмыстарына қолдану туралы ақпарат алу үшін Maras, 2016 қараңыз). Кейбір зерттеулер сандық қарақшылықпен байланысты қылмыс көрсеткіштеріне әлеуметтік-мәдени нормалар, топтық мінез-құлық және топтық динамика әсер етеді деп болжайды. Басқа зерттеулердің нәтижелері сандық қарақшылықтың басқалардан алынған мінез-құлық екенін көрсетеді.

Өзін-өзі бақылау сияқты жеке қасиеттер «адамның заңсыз әрекетке қатысу ықтималдығына, сондай-ақ мұндай заңсыз әрекеттің жиілігі мен ауқымына әсер етеді» деп саналады (Maras, 2016, p. 160). Зерттеулер көрсеткендей, өзін-өзі басқарудың төмен деңгейі (атап айтқанда, ләззат алу қажеттілігі), сондай-ақ адамдар кездесетін стресс (мысалы, авторлық құқықпен қорғалған туындылар үшін ақша төлей алмау немесе оларға қол жеткізу). Алайда, стресс, өзін-өзі бақылау және сандық қарақшылық арасындағы байланысты зерттеу нәтижелері екі түрлі. Басқа зерттеулерде стресс пен сандық қарақшылық арасындағы және өзін-өзі басқару мен сандық қарақшылық арасындағы байланыстың әлсіз немесе шамалы дәлелдері ғана табылды.

Сондай-ақ, кибертехнология арқылы жасалған зияткерлік меншік қылмыстарын орындаушылар «қоғамның жалпы қабылданған нормаларына, құндылықтары мен сенімдеріне қайшы келетін мінез-құлық үшін өкіну немесе кінәлау сезімдерін жеңу» және «өздерінің заңсыз әрекеттерін ақтау немесе негіздеу арқылы өзін жалпы қабылданған шектеулерден уақытша босату» үшін белгілі бір әдістерді (*бейтараптандыру техникасын*) қолданатыны анықталды (Maras, 2016, p. 152). Бейтараптандыру техникасының пайдаланылатын түрлері сандық қарақшылық саласында әртүрлі (*жауапкершілікті теріcтеу; құрбаннан бас тарту; зиянды теріcтеу; айыптаушыларды айыптау; және жоғары құндылықтарға жүгіну*). Тағы бір зерттеу көрсеткендей, сандық асимметрия (мысалы, интернеттегі әрекеттерді тікелей бақылаудың болмауы) адамдарды сандық девиантты мінез-құлыққа біртіндеп ауытқу және қарақшылық сияқты заңсыз әрекеттерді қолдайтын немесе стандарттайтын ақпарат/ресурстарға қол жеткізуге ықпал етуі мүмкін.

4. Қорғау мен алдын-алуда күш-жігер

Кибертехнология арқылы жасалатын зияткерлік меншік саласындағы қылмыстар проблемасының ұсынылатын шешімдері қылмыстық-құқықтық сипаттағы шараларды, зияткерлік меншік объектілеріне рұқсатсыз қол жеткізуді шектеу жөніндегі техникалық шешімдерді және ағартушылық кампанияларды қамтиды.

Қылмыстық сот төрелігі саласында қабылданатын алдын алу шаралары мыналарды қамтиды: авторлық құқықпен қорғалатын туындылар жарияланатын Интернет-сайттардың мониторингі; кибертехнология арқылы жасалған зияткерлік меншік қылмыстарының әртүрлі нысандарына қатысы бар адамдарға қатысты жасырын тергеулер (мысалы, АҚШ-тың көптеген агенттіктері қатысқан *Fastlink операциясы*, сәйкестендіру үшін бір уақытта бірнеше жасырын операциялар жүргізді және, сайып келгенде, Интернетте авторлық құқықпен қорғалған ойындар, бағдарламалық жасақтама, музыка,

фильмдер сияқты туындыларды заңсыз таратуға жауапты адамдарды қамауға алды; Department of Justice, 2004); зияткерлік меншік объектілерін әдейі тарататын сайттарды жабу (мысалы, Megaupload); кибертехнология арқылы жасалған зияткерлік меншік қылмыстарына тартылған адамдарды қудалау (мысалы, авторлық құқықпен қорғалатын туындыларды орналастыратын онлайн-платформалардың қатысушылары мен әкімшілері). Сонымен қатар, кибертехнология арқылы жасалған зияткерлік меншік қылмыстарының құрбаны болған Canada Goose және Chanel сияқты компаниялар өз тауарларының контрафактілік нұсқаларын сатқаны үшін тауарлық белгілерге құқықтардың бұзылуына байланысты интернеттегі сауда алаңдарын сотқа берді.

Қылмыстық жазалау шаралары зияткерлік меншік құқықтарын бұзудың ауыр екенін және қолданыстағы заңнамаға сәйкес жазаланатындығын көрсету әдісі ретінде де белсенді қолданылады. Кибертехнология арқылы жасалған зияткерлік меншік саласындағы қылмыстар үшін жазалар тежеу мақсатында тағайындалады. Мұндай *тежеу құралы* тиімді болуы үшін жазалау шаралары: *қатал* (яғни, жазадан келген зиян қылмыстың пайдасынан асып түсуі керек); *анықталған* (яғни, қылмыс жасаған адам осы қылмысты жасағаны үшін жазалануы керек); және *кідіріссіз* (яғни, адам қылмыс жасағаннан кейін көп ұзамай жазаланады) (Maras, 2016). Зияткерлік меншік құқықтарын бұзғаны үшін қылмыстық жазалау шаралары *нақты тежеуге* бағытталған (яғни, жаза алған адам, егер алынған жаза қылмыс жасаудан түсетін пайдадан асып кетсе, одан әрі заңсыз әрекеттерді тоқтатады) және *жалпы тежеу* (яғни, басқаларға ұқсас мінез-құлық ұқсас қатаң жазаға әкелетіні туралы сигнал жібереді). Алайда, интернеттің бүгінгі сипаты оны тежеудің практикалық іске асуын айтарлықтай шектейді, өйткені қарақшылық жағдайларының ауқымы мен жиілігі кез-келген қарсы әрекет ету мүмкіндіктерінен едәуір асып түседі.

Интернет пен басқа да цифрлық технологияларды пайдалана отырып, кез келген адам қорғалатын контентке қол жеткізе алады, оны лезде қайта басып шығарады және бүкіл әлемге қайта таратады. Кибертехнология арқылы жасалатын зияткерлік меншік саласындағы қылмыстар проблемасын шешу ретінде қылмыстық сот төрелігі саласындағы шаралар, зияткерлік меншікке рұқсатсыз қол жеткізуді шектеу жөніндегі технологиялық шешімдер және ақпараттық-ағартушылық кампаниялар ұсынылады.

Ұлттық, аймақтық және халықаралық деңгейде қабылданған нормативтік-құқықтық шараларға қарамастан, зияткерлік меншік объектілерін таратудың, сақтаудың және/немесе қол жетімділікті қамтамасыз етудің қарапайымдылығы, жеңілдігі және арзандығы осы киберқылмыстарды тергеуге, олардың алдын алуға және оларды жасауға кінәлі адамдарды қудалауға бүкіл әлемдегі тиісті органдар мен мекемелер үшін өте қиын.

Талқылауға арналған сұрақтар:

1. Зияткерлік меншік дегеніміз не?

2. Зияткерлік меншік жүйесіне қандай қызмет түрлері мен қызметтер кіреді?

3. Кибертехнологиялар арқылы жасалатын авторлық құқықтар мен тауар белгілеріне қатысты құқық бұзушылықтардың себебі, негізі және болжамды себебі неде?

12 Тақырып. Адамға қарсы киберқылмыстар.

1. Балаларды жыныстық қанау және Интернетте балаларға жыныстық зорлық-зомбылық жасау

Балаларды жыныстық қанау және ғаламторда балаларға жыныстық зорлық жасау ақпараттық-коммуникациялық технологияларды балаларға жыныстық зорлық жасау және/немесе балаларды жыныстық қанаудың құралы ретінде пайдаланумен байланыстырылады. Біріккен Ұлттар Ұйымының Азия мен Тынық мұхит аймағына арналған экономикалық және әлеуметтік комиссиясы (БҰҰ ҰҰАТ) балаларға жыныстық зорлық жасауды «бала мен одан жасы үлкен немесе хабардар баламен немесе ересек адаммен (бейтаныс адаммен, ағасымен, апкесімен, ата-анасымен немесе қамқоршысымен) арасындағы қарым-қатынас деп анықтай келе, онда бала жасы үлкен баланың немесе үлкен адамның жыныстық қажеттілігін қанағаттандыруға арналған құрал ретінде пайдаланылады. Балаға қатысты мұндай әрекеттер күш қолдану, айламен алдау, пара беру, қорқыту немесе қысым жасау арқылы жүзеге асырылады». *Балаларды жыныстық қанау* деп, қандайда бір кез-келген қажеттіліктерді қанағаттандыруға (мысалы, қамқорлық жасау, тамақ, есірткі, баспана) арналған айырбасты меңзейтін балаларға жасалған жыныстық зорлықты және/немесе балаларды пайдалана отырып басқа да жыныстық әрекеттерді айтамыз. Мұндай қылмыс жасаушы тұлғалар ақшалай немесе басқа пайда алу үшін (мысалы, жыныстық қанағаттану) «осал позицияны, билікті немесе жыныстық мақсаттарда сенімді» теріс пайдалануды немесе теріс пайдалану әрекеттерін жасайды. Шын мәнінде, балалардың жыныстық зорлық-зомбылығы мен балаларды жыныстық қанауды ажырату қиынға соғады, өйткені «олардың ортақ жақтары көп». 1989 жылғы Бала құқықтары туралы Конвенцияның 1-бабында бала деп, «егер осы балаға қолданылатын заң бойынша ол кәмелетке толмаса, әрбір 18 жасқа толғанға дейін адам» деп анықтама берілген. Жас шамасының ең төменгі шегі нақты мемлекетке байланысты өзгереді. Бұл айырмашылықтар балаларды жыныстық қанау және балаларға жыныстық зорлық-зомбылық жасау жағдайларын тергеу кезінде трансшекаралық ынтымақтастықты жүзеге асыруға кедергі келтіруі мүмкін.

Балаларды жыныстық қанаудың және Интернетте балаларға жыныстық зорлық-зомбылықтың түрлері.

Балаларды жыныстық қанау мен Интернетте балаларға жыныстық зорлық-зомбылық балаларға қатысты зорлық-зомбылықтың күрделі сипатына ие болып, ұлттық, аймақтық және халықаралық заңнамамен тыйым салынғанымен әртүрлі құқықтық құралдарда қылмыстың түрі әралуан болып келеді. Заңнамамен тыйым салынған қылмыс түрлерінің мысалы ретінде Интернеттегі грумингті, балаларды жыныстық қанау/балаларға жыныстық зорлық-зомбылық сипатындағы суреттері бар материалдарды жариялауды

және балаларға жыныстық зорлық-зомбылықтың тікелей көрсетілімдерін атауымызға болады.

Балалардың қатысуымен грумингті (балаларды азғыру немесе жыныстық мақсатта балаларға тиісу деп белгілі) ересек адамның баламен танысуы арқылы (көбінесе Интернетте, алайда Интернет желісінен тыста болуы мүмкін және оны ескерусіз қалдыруға болмайтын) балаға (ұлға/қызға) жыныстық зорлық-зомбылық жасау мақсатында іске асырылатын практика деп сипаттауға болады.
Зерттеулер мен қолда бар мағлұматтар көрсеткендей, груминг түріндегі қылмыстар көп жағдайда ер адамдармен жасалады; азырақ көлемде жыныстық мақсатта балаларға тиісуді және/немесе грумингті әйелдер жасайды.

Әдетте, груминг үдерісі құрбанды таңдаудан бастап сатылы болып келеді. Интернетте балалар түрлі әлеуметтік желілердің және коммуникациялық қосымшалардың қатысушысы болады. Қылмыскерлер олар арқылы баланың жеке басының жазбаларына қол жеткізеді. Қылмыскерлер жәбірленушіні оның «сүйкімділігі/тартымдылығы» негізінде (қылмыскердің қалауына сай анықталады), «қол жетімділіктің жеңілдігі» негізінде (мысалы, балалар қолданатын веб-сайттардағы, платформалар мен қосымшалардағы құпиялылық режимнің өшірілгені-өшірілмегеніне немесе дұрыс орнатылмауына байланысты) және/немесе «осалдықтар» негізінде (мысалы, балалар өздерінің жалғыздығы немесе түсінбеушілік сезіміне тап болғаны туралы хабарламалар орналастырады) таңдайды. Құрбанға таңдау жасалғаннан кейін оған қол жеткізу мақсатында қылмыскер онымен байланыс жасайды. Содан соң қылмыскер құрбанмен достық қарым-қатынас жасауға ниет білдіреді. Қылмыскер құрбан туралы ақпаратты барынша жинақтауға тырысады және жинақталған ақпаратты құрбанды алдау үшін, мысалы, олардың ортақ қызығушылықтары бар екендігін немесе дәл сол жағдай өзінің басында да орын алғанын алға тартып, құрбанды жақсы түсінетінін жеткізіп, оның сеніміне кіру арқылы онымен кездесуге әрекеттер жасайды. Қылмыскердің мақсаты әрі қарай достық қарым-қатынасты дамыту болып табылады. Жыныстық қанауға немесе зорлық-зомбылыққа кіріспес бұрын қылмыскер қылмысының ашылып қалу тәукелін бағалайды (мысалы, баланың ата-анасы немесе басқа тұлғалар тараптарынан оның жеке деректеріне және/немесе сандық құралдарына бақылау жасалатыны туралы құрбаннан сұрайды), өзінің және құрбан арасындағы қарым-қатынастың ерекше мәнге ие екендігін және осы қарым-қатынастардың құпия түрде сақталуын айтып, баланы оқшаулайды. Бірақ қылмыскерлер бұдан басқа да жолдарды қолдануы мүмкін.

Балалар порнографиясы деп «қандайда болмасын құралдармен баланың қатысуымен ашық түрде нақты немесе құрастырмалы жасалатын жыныстық әрекеттердің суреттерін немесе балалардың жыныстық мақсатта көрсетілген жыныстық органдарының суреттерін айтуға болады».

Балаларға жасалатын жыныстық зорлық-зомбылықтың тікелей көрсетілімі нақты уақыт режимінде қашықтықтағы тұтынушылар үшін балаларға жасалатын жыныстық зорлық-зомбылықтың бейне көрсетілімі.

Тікелей көрсетілім Интернет арқылы ұлттық шекара шегінен сыртқа бейнебелгілерді жіберу арқылы жүреді, атап өтуіміз маңызды бірқатар елдер өз елдері ішінде балаларға жасалатын жыныстық зорлық-зомбылықтың тікелей көрсетілім бейнелері оқиғалары туралы хабардар етеді.

Балаларға жасалатын жыныстық зорлық-зомбылықтың тікелей көрсетілімі Интернет-чаттарда, әлеуметтік желілерде және коммуникациялық қосымшаларда (бейнечат функциясы бар) көрсетіледі. Көрсетілім көрермендері бейтарап (көрсетілімге ақы төлейтіндер) немесе белсенді (жәбірленуші баламен, жыныстық зорлаушымен және/немесе жыныстық зорлық-зомбылықты ұйымдастырушымен сөйлесу арқылы белгілі бір әрекеттерді жасауды, мысалы, тұншықтыруды және/немесе баламен жыныстық қатынасқа түсуді, т.б. талап етушілер) болып келеді. Көрерменнің тарапынан белсенді қатысушылықты *тапсырыс арқылы балаларға жасалатын жыныстық зорлық-зомбылық* деп аталады. Тапсырыс тікелей көрсетілімге дейін де, ол жүріп жатқан кезде де болуы мүмкін. Lostprophets тобының аты-шулы танымал әншісі Иан Уоткинске балаларға жасалатын жыныстық зорлық-зомбылық қылмысына қатысты деп айып тағылған, оның ішінде ол Skype арқылы әлдебір әйелді өзінің баласына жыныстық зорлық-зомбылық жасауға итермелегені үшін қылмыскер атанып отыр. Бұл жағдай балаларға жасалатын жыныстық зорлық-зомбылықтың тікелей көрсетілімі ақылы түрде жүзеге асырылуымен қатар көңілдестеріне ляззат сыйлауы және/немесе зорлаушылар мен көрермендердің жыныстық қанағаттануы үшін және/немесе өзге де зорлық-зомбылық қатынастардың контекстісінде жүруі мүмкін (мысалы, зорлаушы тұлғаның өзі зәбір көретін зорлаушысының айтқандарын екі етпей орындауы кезінде).

2. Киберқудалау және кибералымсақтық.

Киберқудалау деп кезкелген адамды жүйелі түрде алымсақтық, мазалау, қоқан-лоққы көрсету, қауіп-қатер төндіру, қорқыту және/немесе сөзбен балағаттау мақсатында бірнеше мәрте қайталанбалы әрекеттерді жасау үшін ақпараттық-коммуникациялық технологияларды пайдалануды айтамыз (UNODC, 2015; Maras, 2016). Киберқудалау кезінде қылмыскерлер жағымсыз, анайы және/немесе балағаттау, ар-намысқа тиетін сөздерді тікелей электрондық пошта, мезеттік хабарламалар, қоңырау шалу, мәтінді хабарламалар арқылы немесе электрондық байланыстың өзге түрлерін қолдану арқылы жүзеге асыруы мүмкін. Сонымен бірге жәбірленушінің қозғалысына мониторинг, сырттан бақылау, аңду жүргізу үшін технологияларды пайдаланады (мысалы, автокөлігіне, сөмкесіне, тіпті балалар ойыншығына жасырын түрде GPS-аңду құралдарын орнату арқылы). Сондай-ақ, қылмыскерлер киберқудалауды жанама түрде жәбірленушінің сандық құралына нұқсан келтіру арқылы жүзеге асыруы мүмкін (мысалы, жәбірленушінің компьютерін зиянкес бағдарламамен бұзу және сол бағдарлама арқылы жәбірленуші әрекеттеріне құпия мониторинг жүргізу және/немесе жәбірленуші туралы қандайда бір маңызды ақпараттарды ұрлау) немесе Интернет желісінде жәбірленуші туралы жалған, оның абыройына нұқсан келтіретін немесе оны балағаттайтын ақпараттарды орналастыру,

немесе жәбірленушінің жазба деректерін пайдаланып, Интернетте (әлеуметтік желіде, чаттарда, пікір-талас форумдарында, веб-сайттарда) оның атынан жалған материалдарды жариялау.

Киберқудалауды белгілі бір уақыт аралығында қайталанатын әрекеттер жиынтығымен түсіндіруге болады. Олардың мақсаты жәбірленушіні және/немесе оның отбасын, серіктесін және достарын қорқыту болып табылады. Мұндай әрекеттерге пайдаланушының пошталық жәшігін электрондық хаттармен толтырып тастау, әлеуметтік желілердегі пайдаланушының парақшалары мен жазба деректерінде, сайттарда жиі хабарламалар орналастыру, құрбанға толастамайтын қоңырау шалулар мен мәтінді хабарламаларды жолдау, дыбысты хабарламалар қалдыру және жазылу мен достар қатарына қосу туралы сұраныстар жолдау, жәбірленуші қатысушы болып табылатын желідегі барлық топтар мен қауымдастықтарға қосылу, немесе таныстардың, әріптестердің, сыныптастардың, отбасы мүшелерінің немесе достардың жазба деректері арқылы жәбірленушінің жариялымдарына жазылу, және жәбірленушінің парақшаларын үздіксіз қарап отыру (кейбір веб-сайттар мұндай ақпаратты тіркеп, пайдаланушыға оның парақшасы қашан қаралғаны туралы хабарлап отырады). Қылмыскерлер құрбанның хабардар болуымен немесе оның хабарынсыз Интернет кеңістігінде және/немесе Интернет желісінен тыс жерде үздіксіз бақылауы, аңдуы мүмкін. Киберқудалаушылардың әрекеттері жәбірленушілерді өздерінің қауіпсіздігі мен сақтығы үшін қауіптенуге мәжбүрлейді және киберқудалаушы әрекетіне байланысты мұндай үрей құрбанның отбасының, серіктестерінің және достарының қауіпсіздігі мен амандығына да ықпал етіп, таралуы мүмкін.

Кибералымсақтық қорлау, ызаландыру, шабуылдау, қауіп-қатер төндіру, қорқыту, ренжіту және/немесе балағаттау мақсатында қасақана әрекеттерді жасау үшін АКТ-ны пайдаланумен түсіндіріледі (Maras, 2016). Киберқылмыстың жасалғаны туралы фактіні тану үшін бір оқиғаның болуы жеткілікті; алайда, мұндай киберқылмыс бірнеше оқиғалардан тұруы мүмкін. Сонымен қатар кибералымсақтыққа бір немесе бірнеше адамның ортақ күш біріктіруімен құрбанға шектелген уақыт аралығында (әдетте, аз уақыт ішінде) Интернетте азап шектіру, қорлау және/немесе ауызын жабуға мәжбүрлеу мақсатын көздейтін алымсақтықты жатқыза аламыз. Сондай-ақ, кибералымсақтыққа әлеуметтік желілерде, Интернет-сайттарда адамның әлеуметтік жағдайына, кісіаралық қарым-қатынастарына және/немесе абырой-атағына (бұл *кибер жала жабудың* бір түрі болып табылады) нұқсан келтіру мақсатында ол туралы жалған ақпаратты орналастыру немесе өсек-аяңды тарату да жатады. Мұндай жалған ақпарат веб-сайттарда, чаттарда, пікір-талас форумдарында, әлеуметтік желілерде таратылады. Қылмыскерлер кейде өздерін құрбандардың атынан аттары ұқсас жазба деректерін құрып, онда жәбірленушінің суреттерін орналастырып, жазба деректерін дос болу үшін қосылуға жәбірленушінің достарына, отбасы мүшелеріне сұраныстар жолдап, алдау арқылы осы сұраныстарды қабылдауға итермелейді (*желідегі тұлғаландырудың* бір түрі). Аталған сұраныстардың қабылдануы

қылмыскерлерге құрбандардың достары мен отбасы мүшелерінің жазба деректеріне қол жеткізу арқылы құрбандардың нақты жазба деректеріне қол жеткізулеріне мүмкіндіктер береді.

3. Киберқорлау. Киберқорлаумен айналысатын балалар басқа балаларды қорлау, төмендету, қаралау, балағаттау, жалған ақпарат пен өсек-аяң тарату, қорқыту және/немесе шеттету, араластырмау және аздыру мақсатында мәтінді хабарларды, электрондық хаттарды, веб-сайттарды, блоктарды, сауалнамаларды, әлеуметтік желілердегі хабарларды, мезеттік хабарларды, ойын сайттарын және виртуалды шындық сайттарын пайдаланады. Киберқудалау мен кибералымсақтық кезіндегідей киберқорлаудың да екі түрі болады: тікелей киберқорлау (яғни, киберқорлау жасаушы тұлға жәбірленушіге тікелей шабуылдар жасайды) және басқалардың қолымен жасалатын киберқорлау (яғни, басқа тұлғалар саналы түрде немесе бейсана күйде киберқорлауды жасауға қолғабыс етеді) (Maras, 2014). Киберқорлаумен айналысатын тұлғалар және/немесе оларға қолғабыс жасаушы басқа тұлғалар жәбірленушінің жеке басына қатысты ақпаратты, мекен-жайын, телефон номерін ашық жариялауы мүмкін (доксингтің бір түрі). Бұл ақпарат әрі қарай киберқорлау объектісінің қылмыстық қол сұғушылықтың құрбанына айналуына пайдаланылады. Құрбанның мекен-жайын көрсету шын өмірде алымсақтыққа, қорлауға, қудалауға әкелумен қатар құрбанға физикалық зиян келтіруі мүмкін. Ашық қол жетімділікте құрбанның аты-жөні, паролі және басқа да жазба мәліметтері жариялануы мүмкін. Құрбанның жазба деректерін желіде орналастыру салдарынан оның жеке басына қатысты ақпараттың, суреттерінің, бейне жазбаларының, құжаттарының ұрлануына әкеп соғады. Бұл жазба деректері қылмыскерге өзін жәбірленуші деп танытуға және әрекеттер жасауға мүмкіндік береді (мысалы, әдепсіз және балағаттау сипатындағы пікірлер қалдыру, құрбанды қорлайтын материалдар жариялау, жалаңаш суреттерін немесе ыңғайсыз билеп жатқан құрбанның бейнесін орналастыру), олар өз кезегінде басқа тұлғалар арасында теріс пікір калыптастырады (балағаттау сипатындағы пікірлер қалдыру, құрбанды мазақ ету).

Сыртқы бақылаушылар киберқорлау кезінде өте маңызды роль атқарады. Олар «маған ұнайды» түймесін басу, материалдарды немесе хабарларды екінші мәрте жариялау, әрі қарай жолдау арқылы киберқорлауды жүзеге асырушы тұлғаға әдейілеп немесе байқаусызда көмектеседі. Сыртқы бақылаушылар жеке мүддесіне негізделген шешімдері топтың, ұжымның шешімдерінен басым болып келетін *әлеуметтік дилеммаға* байланысты араласпауға ниетті болады. Зерттеулер көрсеткендей, ұжым мүддесі үшін жасалған бұндай әрекетсіздік топтағы басқа адамдар осы пікірге қосылып, қолдайды ме екен, қолдамайды ме екен деген сенімсіздіктен туындайды.

Балалар арасында АКТ-ды қолдану масштабы әлем бойынша артып келеді, сандық технологиялар мен Интернет жасы кіші балаларға да қол жетімді болып отыр (UNODC, 2015). АКТ-лар балаларға ақпаратқа қол жеткізуге, ақпаратпен бөлісуге, басқа адамдармен қатынасуға кеңінен мүмкіндіктер бергенімен, екінші жағынан осындай технологиялар балалардың

қауіпсіздігіне қауіп-қатер әкеліп, оларды киберқылмыстарға, әсіресе киберқорлауға осал етеді. Киберқорлау кезінде балалар АКТ-ды басқа балаларды «ызаландыру, қорлау, қорқыту, балағаттау немесе өзге шабуылдар жасау үшін» қолданады (Maras, 2016, p. 254). Сонымен, киберқудалау мен кибералымсақтыққа қарағанда киберқорлаудың орындаушылары да, құрбандары да балалар болып келеді.

Әдетте, киберқорлау туралы заңдарды қабылдау орын алған оқыс жағдайдан кейін, яғни бала киберқорлау нәтижесінде өз-өзіне қол салғаннан кейін, оған жауап әрекеті ретінде қабылданады. Мысалы, Италияда 2017 жылғы 29 мамырдағы №71 заң құрбан киберқорлау нәтижесінде ғимараттың 3-ші қабатынан секіріп, өз-өзіне қол салғаннан кейін қабылданған (Reuters, 2017). Алайда мемлекеттер балаларды қорғауға міндетті және бұл міндет балалар құқықтарын қорғауға қатысты міндеттемелермен қатар балалар құқықтары туралы Конвенцияда бекітілген. Аталған Конвенцияның 37(а) бабында бірде бір бала «азаптау немесе басқа қатігез, адамгершілікке жатпайтын немесе ар-намысын қорлайтын әрекеттерге немесе жазаларға» ұшырамауы тиіс. Демек, киберқорлау балалар құқықтары туралы Конвенцияны өрескел бұзу болып табылады. Сонымен қатар, киберқорлау балалардың басқа да құқықтарын бұзады: кемсітушіліктен еркіндік құқығы (2 бап), өз пікірін білдіру еркіндік құқығы (13 бап), жеке өмірге қол сұғылмаушылық (16 бап) және басқалар. Бірқатар елдерде киберқорлау туралы ұлттық заңдар қабылданып, жұмыс жасауда (мысалы, 2013 жылғы «Қорлауды тоқтату шараларын ынталандыру туралы» Жапония заңы, 2017 жылғы 29 мамырдағы №71 Италия заңы), дегенмен оқушылардың амандығын қорғау бойынша шараларды қабылдауға бірінші кезекте оқу мекемелері жауапты, олар балаларды қорлаудан (оның ішінде киберқорлаудан) қорғауға және балалардың қауіпсіздігі мен амандығына қауіп-қатер туындататын оқиғаларға ден қоюға міндетті. 2010 жылғы «Білім туралы» Швеция заңы (Заң 2010: Білім туралы заң 800) және 1989 жылғы «Балалар туралы» Ұлыбритания және Солтүстік Ирландия Біріккен Корольдігінің заңы осындай міндеттердің шекарасын айқындайды. Ұлыбритания және Солтүстік Ирландия Біріккен Корольдігінде мектептердің бірінші кезекте балалардың қауіпсіздігі мен денсаулығы қауіп-қатерлерінен қорғау (киберқорлау сияқты), алдын алу және ден қою шаралары бар нақты саясаты болуы міндетті.

4. Адамға қарсы киберқылмыстарды алдын алу.

Адамға қарсы киберқылмыстармен күресу үшін жәбірленушілерге бағдарланған алдын алу стратегияларын қолдану ұсынылады. Лоренс Коэн (Lawrence Cohen) және Марк Фелсон (Mark Felson) 1979 жылы ұсынған әдеттегі қызмет теориясына сәйкес қылмыс екі элемент болған жағдайда – *ынталанған қылмыскер* мен *қолайлы нысана,* және бір элемент болмаған жағдайда – *әрекет қабілеттілігі бар қорғаушы* (қылмыскердің қылмыс жасауына кедергі келтіруге қабілетті біреудің немесе бір нәрсенің болуы) жасалады.

Әдеттегі қызмет теориясына сәйкес қылмыстың алдын алу үшін негізгі элементтердің біреуін өзгерту қажет - әрекет қабілеттілігі бар қорғаушының

болуы, ынталанған қылмыскердің немесе қолайлы нысананың болмауы. Демек, қылмыскер үшін қылмысты тартымсыз ету үшін әрекет қабілеттілігі бар қорғаушылардың болуы ұсынылады, олардың ролінде адамдар (мысалы, ата-аналар, ағалар, әпкелер, достар, серіктестер және басқалар) немесе қауіпсіздікті қамтамасыз ету бойынша шешімдер (мысалы, құпиялылық параметрлерін орнату, ата-аналық бақылау, сүзгілеу немесе тыйым салу бағдарламалық қамтамасыз ету және т.б.). Өзін-өзі қорғау шаралары әрекет қабілеттілігі бар қорғаушы ретінде бола алатынын және қылмыскерлердің құрбанға жақындауына, онымен байланыс орнатуына, оның қудалануына кедергілер жасай алатынын теория түсіндіреді.

Жәбірленушілерге бағдарланған алдын алу стратегиялары адамға (кем дегенде, бұл үшін білімі, дағдылары мен қабілеттері бар адамдар) қарсы киберқылмыстарды болдырмау үшін құрбандарға жедел әрекеттер жасауға, ең кем дегенде киберқылмыс жасауға бекінген тұлғаның жоспарын құртуға мүмкіндіктер береді. Мұндай амалдардың негізгі сыны адамға қарсы киберқылмыстардың алдын алу ауыртпалығын адамдарды қиындықтардан қорғауға міндетті мекемелердің емес, құрбанның өзіне артатындығында болып отыр (Maras, 2016; Henry, Flynn and Powell, 2018).

Зорлық-зомбылықты және қорлауды алдын алуда басым кедергі, өкінішке қарай, адамға қарсы киберқылмыстардың құрбанға кінә артатын және осы киберқылмыстармен келтірілетін залалдың «салмағын» азайтатын қалыптасқан көзқарасқа, орныққан құндылықтарға байланысты болып келеді. Мысалы, суретті пайдалана отырып жасалған жыныстық қорлау мәселесі бойынша 2017 жылы жүргізілген австралиялық зерттеудің барысында респонденттердің 70 пайызы «суреттерін ешкімге жолдамасада адамдар өздерін жалаңаш түрінде суретке түсіруге болмайтынын түсінуі қажет» деген пікірмен келіссе, 62 пайызы «егер адам жыныстық сипаттағы суретін біреуге жолдаса және ол сурет желіде жүретін болса, оған кем дегенде ішінара жауапкершілік жүктеледі» деген пікірмен келіскен (Henry, Flynn and Powell, 2018). Жалпы Генри, Флин мен Пауэллдің зерттеуінде (Henry, Flynn and Powell, 2018) әр екі ер кісінің біреуі (немесе 50 пайызы) және әр үш әйелдің біреуі (немесе 30 пайызы) не келтірілетін залалдың «салмағын» азайтатын, не құрбанға кінә артатын көзқарасты ұстанған. Құрбанға кінә артатын мұндай көзқарастар даулы болып табылады және қылмыскерлердің немесе әлеуетті қылмыскерлердің арасында басым болып қана қоймай, суретті пайдалана отырып жасалған жыныстық қорлаудың құрбаны болған тұлғалар өздерін кінәліміз деп танып, оқиға туралы хабарлай алмай, сыртқы көмекке жүгіне алмайды (Henry, Flynn and Powell, 2018). Егер қоғам мүшелері осындай көзқарасты ұстанатын болса, олар қылмыстың құрбаны болғанын ашық жария еткен тұлғаларға қосымша зиян келтіруі мүмкін.

Балалардың қатысуымен жасалатын адамға қарсы киберқылмыстар мәселесі көптеген елдерде ата-аналық бақылау мен білім бастамалары арқылы шешіліп келеді.

Балалардың Интернетке қол жетімділігіне, Интернетті пайдалануына, сондай-ақ, желіде өткізетін уақытына ата-аналар тарапынан жүргізілген

мониторинг балаларды киберқорлаудан қорғайтынын зерттеулер көрсетіп отыр. Алайда ата-аналардың басқа тұлғалардың көмегінсіз (мысалы, мектептің, мемлекеттік органдардың, балаларды қорғау қызметтерінің және туыстардың) балалардың Интернеттегі әрекеттерін бақылауға және/немесе қажетті технологиялық шешімдерді қабылдауға (мысалы, кейбір сайттарды қол жетімсіз етуге арналған сүзгілеу құралдарын орнату) мүмкіндіктері болмауы ықтимал (UNODC, 2015). Білім бастамалары балаларды және ата-аналарды Интернетті қауіпсіз пайдалануға үйретеді және оларды киберқорлау туралы хабардар етеді. Киберқорлау ренжітушілердің, құрбандардың және сыртқы бақылаушылардың қатысуымен жүзеге асатындықтан алдын алу бойынша күш-жігер әрбір қатысушыны қамтуы қажет.

Талқылауға арналған тапсырма:

Даниель Сон Вунг Ли – Табло деген атпен танымал оңтүстіккореялық музыкант, ол оңтүстіккореялық әртіс әйелге үйленген және оның көптеген сүйермендері бар. Өзінің музыкалық маңсабына дейін ол Стэнфорд университетінде бакалавр және магистр дәрежесін алған. Оңтүстік Кореяда жалған дипломдармен орын алған жанжалдардан кейін (көптеген жоғары лауазымды жеке және мемлекеттік кайраткерлердің білімдері туралы дипломдары жалған екендігі анықталған кезде) аноним азаматтар онлайн топтар құрып, Лидің дипломдарына күмән келтірген. Осы топтардың ірісі «Біздер Таблодан ақиқатты талап етеміз» (TaJinYo) Интернет-форумы болды. Осы топтың мүшелері және Интернеттің басқа пайдаланушылары Лиге анонимдік шабуылдар жасап, оны балағаттаған. Лидің дипломдары заңды екендігі туралы дәлелдемелерді (тіпті Стэнфорд университетінің дәлелдерін) місе тұтпай, жалған дәлелдемелер деп танып, оларды Лиді ақтау үшін әдейілеп ақша алып отырған адамдардың тірлігі деп айыптаған. Оны қорғауға талпынған кезкелген тұлға өтірікші атанып, өзінің беделіне нұқсан келу тәукелдерімен соқтығысты. Осы себептен Лиге ашық қолдау көрсетуге ешкім дайын болмады. Тіпті Оңтүстік Кореядағы бұқаралық ақпарат құралдары фактілер тексерілмей, желіде қарсылық білдірушілермен тағылған шағымдар туралы хабарлады. Бұл мәселенің одан сайын шиеленісуіне әкеп соқты. Оңтүстік Корея халқы оны сөзбен балағаттауға, ашықтан ашық қауіп-қатер төндіруге көшті, тіпті ұрып-соғуға дейін баратындарын айтып, көшеде жүргізбей, қуғын-сүргінге ұшыратуға дейін барған. Оған шабуыл жасаған адамдар оның отбасы мүшелерін де сырт қалдырмады, отбасы беделіне нұқсан келтіріп, олардың өмірлеріне қауіп төндірді. Тек танымал оңтүстіккореялық журналисті жанына ертіп, түсірілім тобымен Калифорнияға барып, өзінің Стэнфорд университетінде оқуы жайлы бейнематериал түсіргеннен кейін және оның *сынақ-емтихан тізімдеудің үзіндісі Стэнфорд университетінің өкілдерімен камераға расталғаннан* кейін Лиге жасалған киберқылмыстар біршама (толық емес) тоқтады.

Сұрақтар:

1. Таблоға қарсы қандай киберқылмыстар жасалды? Сіз неге солай деп есептейсіз?

2. Егер Сіз басқа елде болсаңыз жоғарыда аталған сұрақтарға Сіздің жауаптарыңыз өзгерер ме еді? Өз жауабыңызды негіздеңіз.

13 Тақырып. Ұйымдастырылған киберқылмыстылық.

Ұйымдастырылған киберқылмыстылық: бұл не?

Көптеген қылмыстар мен киберқылмыстар ұйымның белгілі бір деңгейінде жасалады, яғни бұл қылмыстар мен киберқылмыстар «жоспарланған және жеке топтардың күш-жігерін көрсететін ұтымды әрекеттерді білдіреді».

1. Киберкеңістік және қылмыстық топтарды ұйымдастыру

Көптеген ұйымдасқан қылмыстық топтар бір-бірімен сөйлесу және өз істерін жүргізу үшін Интернет технологиясын қолданады. Мұндай «істер «Интернет қылмыскерлерді дербес қылмыс жасау мақсатында біріктіру үшін пайдаланылатын ұйымдардың» эфемерлік» нысандарын құруға әкелуі мүмкін, содан кейін олар жаңа одақтар құру үшін таратылады. Сонымен қатар, ұйымдасқан қылмыстық топтар ұзақ уақыт бойы өмір сүретін және оның қанатының астында әрекет ететін қылмыскерлерді сол салада жұмыс істейтін басқа қылмыскерлерден, сондай-ақ құқық қорғау органдарынан қорғауды қамтамасыз ететін ұйымдардың «тұрақты» нысандарын құру үшін желілік технологияны қолдана алады (Varese, 2010, p.14). Спектрдің осы екі экстремалды полюстерінің арасында ұйымдардың «гибридті» формалары да бар, онда кең танылған қылмыстық мақсатты кішігірім негізгі топ «іс жүзінде» белсенді түрде таратады, бірақ кейбір хакерлік топтарда немесе қылмыс пен терроризм арасында байланыс орнатылған офлайн жағдайларда оның физикалық көрінісін жеке жалғыз қасқырлар немесе жергілікті жасушалар жүзеге асырады.

Айта кету керек, «террористер мен ұйымдасқан қылмыстық топтардың қызметі бір-біріне сәйкес келуі мүмкін», «олар әдетте әртүрлі мақсаттарға ұмтылады». Ұйымдасқан қылмыстық топтардың көпшілігі, әдетте, ортасында гибридті формасы бар эфемерлі және тұрақты ұйым формалары арасындағы спектрде болады және белгілі бір дәрежеде Интернет-технологияны өзін-өзі ұйымдастыру үшін қолданады.

Киберкеңістік және киберқылмыстарды ұйымдастыру

Ұйымдасқан қылмыстық топтардың барлығы дерлік өз қылмыстарын өзін-өзі ұйымдастыру және ұйымдастыру үшін желілік технологияны қолданса да, кейбіреулері бұл технологияларды киберқылмыс жасау үшін де қолданады. Киберқылмыскерлерді ұйымдастырудың нақты сипаты цифрлық және желілік технологиялардың деңгейіне, іс-қимыл режиміне және жоспарланған құрбандарға байланысты өзгереді, бұл олардың арасындағы айырмашылықтарды анықтауға көмектеседі.

Сандық және желілік технологияларды пайдалану немесе

қылмыстық мінез-құлықты трансформациялау деңгейі.

Дәстүрлі ұйымдасқан қылмыстық топтар, әдетте, кибершабуылдарға, яғни Интернет болмаған кезде жасалмайтын қылмыстарға қатыспайды. Алайда, қылмыстарды ұйымдастыру немесе құрбандарды табу мақсатында бір-бірімен байланыс жасау үшін желілік технологияны көбірек қолданады. Мысалы Интернет немесе даркнет арқылы есірткіні сату. Киберқылмыстың бұл түрлері кибертехнологияны қолдана отырып (әдетте байланыс технологияларын қолдана отырып) жасалған қылмыстарға жатады, өйткені интернетсіз да басқа байланыс құралдарымен немесе кибертехнология арқылы бұл құқықбұзушылық жасалар еды, немесе кибертехнологиялар арқылы жасалатын бұрыннан бар (әдетте локализацияланған) заңсыз құмар ойындар, алаяқтық және бопсалау сияқты қылмыстар түрлері сандық және желілік технологиялардың арқасында жаһандық қол жетімділікке ие болады. Егер Интернет алынып тасталса, онда құқық бұзушылықтар жаһандық ауқымын жоғалтып қайтадан локализацияланған пішінге ие болады. Олар хакерлік шабуылдар, «қызмет көрсетуден бас тарту» типтегі және бопсалау бағдарламаларды қолдану арқылы бөлінген шабуылдар, сондай-ақ жоғарыда айтылғандай, интернетті теңдеуден алып тастаған кезде жоғалып кететін спам сияқты «кибертәуелді» қылмыстардан күрт ерекшеленеді.

Киберқылмыстар *modus operandi*-ге, яғни қылмыскерлердің себептері мен профилімен байланысты құқық бұзушылық жасау әдісіне байланысты да өзгереді. «Машинаға карсы киберқылмыстардың», мысалы, хакерлердің компьютерлерді заңсыз пайдалануы сияқты қылмыстардың ұйымдасуынан алаяқтық және бопсалау сияқты «машинаны пайдалану арқылы киберқылмыстардың» ұйымдасуы мүлдем өзгеше. Қылмыстың бұл екі түрі «машинадағы киберқылмыстардан» айтарлықтай ерекшеленеді, мысалы, балаларға жыныстық зорлық-зомбылық бейнеленген материалдарды тарату, жеккөрушілікті насихаттау, террористік материалдар. Киберқылмыстылық пен оны ұйымдастыруды зерттеу кезінде ескерілетін соңғы фактор-қылмыскерлер бағытталған құрбандар тобы. Кейбір қылмыстық топтар жекелеген пайдаланушыларға әдейі мақсаттанады, мысалы, алаяқтық немесе алдау мақсатында жаңылыстыратын электрондық хаттарды жаппай жіберу арқылы. Басқа топтар ірі көлемде алаяқтық жасау, коммерциялық құпияны игеру немесе іскерлік белсенділікті бұзу мақсатында (бопсалау немесе бәсекелестің өтініші бойынша) коммерциялық немесе үкіметтік ұйымдарға әдейі бағытталған. Сонымен, әдетте мемлекеттік субъектілерді қамтитын үшінші топтар сенімсіздік немесе наразылық атмосферасын құру және/немесе зиян келтіру үшін басқа мемлекеттердің инфрақұрылым объектілерін әдейі нысанаға алады. Сондықтан, мәселе желілік технологияларды қолданатын қылмыскерлерді ұйымдастырудың тәсілі қылмыскерлердің интернеттегі қылмыстарды қалай ұйымдастыратындығынан мүлдем өзгеше емес, сонымен қатар Интернеттегі қылмыстарды ұйымдастырудың сипаты қолданылатын технологиялардың деңгейіне, қылмыскерлер жасаған нақты қылмыстық әрекеттерге, сондай-ақ жоспарланған құрбандарға байланысты.

Түрлі зерттеулер нәтижелері офлайн ортада жұмыс істейтін ұйымдасқан

қылмыстық топтар интернетте өз қызметін жүзеге асыратын ұйымдасқан қылмыстық топтарға мүлдем қарама-қайшы екенін және олардан мүшелерінің жасына, мотивтеріне, ұйымдастырылуына және жынысына қарай ерекшеленетінін көрсетеді. Бұл топтар бір-бірінен тек қатысушыларымен ғана ерекшеленбеуі мүмкін; офлайн ортадағы ұйымдасқан қылмыстық топтармен салыстырғанда олардың ұйымы орталықтандырылмаған болуы мүмкін.

2. Ұйымдасқан қылмыстылықты концептуализациялау және оның қатысушыларын анықтау.

Белгілі бір киберқылмыстар ұйымдасқан қылмыстылықтың бір түрі болып саналады ма, әлде ұйымдасқан қылмыстылыққа байланысты ма деген сұрақ «ұйымдасқан қылмыстылық» термині үшін қолданылатын анықтамаларына байланысты (БҰҰ ЕҚБ, 2013, 49-50 бб.). Біріккен Ұлттар Ұйымының Трансұлттық ұйымдасқан қылмыстылыққа қарсы конвенциясында ұйымдасқан қылмыстылықтың анықтамасы жоқ. Бұл мемлекеттер арасындағы уағдаластықтың болмауымен емес, Конвенция бойынша келіссөздерге қатысушылар жасаған саналы таңдаумен байланысты. Кез-келген анықтамада ұйымдасқан қылмыстық топтардың үнемі өзгеріп отыратын және қарқынды дамып келе жатқан әлемнің жағдайларына бейімделетін заңсыз әрекеттерінің тізімі болуы мүмкін; сондықтан кез-келген осындай анықтама тез ескірер еді. Қылмысты анықтаудың орнына, ұйымдасқан қылмыстылыққа қарсы Конвенция оны жасауға қатысатын «ұйымдасқан қылмыстық топ» субъектіні анықтайды. Атап айтқанда, Конвенцияның 2(а) бабына сәйкес «ұйымдасқан қылмыстық топ» «белгілі бір уақыт кезеңі ішінде жұмыс істейтін және бір немесе бірнеше елеулі қылмыстар немесе осы Конвенцияға сәйкес осындай деп танылған қылмыстар жасау мақсатында келісілген, тікелей немесе жанама түрде қаржылық немесе өзге де материалдық пайда алу үшін құрамында үш немесе одан да көп адам бар құрылымдық ресімделген топты» білдіреді. Мұнда құрылымдық түрде құрылған топта «оның мүшелерінің рөлдері ресми түрде анықталмайды немесе мүшеліктің үздіксіз сипаты келісілмейді». Бұл анықтама кең болып табылады және топтар арасында бір-бірімен тығыз байланысы жоқтығын, ресми түрде анықталған рөлдері мен дамыған құрылымның болмауын қамтиды.

Ұйымдасқан қылмыстылықтың жалпыға бірдей қабылданған анықтамасы болмаса да, оны «қоғамдық сұранысқа ие қызметтердің салаларында заңсыз әрекеттер арқылы пайда табу мақсатында ұтымды әрекет ететін тұрақты жұмыс істейтін қылмыстық кәсіпорын деп анықтауға болады. Ұйымдасқан қылмыстылықтың ұзақ уақыт бойы жалғасуы мемлекеттік қызметкерлерге пара беру, қорқыту және қылмыстық әрекеттерді қорғау үшін күш қолдану арқылы қолдау табады». Тиісінше, ұйымдасқан киберқылмыстылық термині киберкеңістіктегі ұйымдасқан қылмыстық әрекетті сипаттау үшін қолданылады. Ұйымдасқан қылмыстылық сияқты, киберқылмыстылық немесе ұйымдасқан киберқылмыстылық анықтамасы бойынша біріңғай пікір жоқ (БҰҰ ЕҚБ, 2013; Broadhurst et al., 2014; және Maras, 2016).

Ұйымдасқан киберқылмыстылық туралы зерттеулер ұйымдасқан қылмыстылықтың кейбір дәстүрлі сипаттамаларын киберкеңістік жағдайында түсіндіру қиын екенін көрсетеді. Мұндай сипаттаманың мысалы ретінде «аумақты бақылау» болып табылады (БҰҰ ЕҚБ, 2013, 50 б.). Варезеның (Varese) айтуынша, ұйымдасқан қылмыстық топ «белгілі бір тауарлар мен қызметтерді өндіру мен таратуды заңсыз реттеуге және бақылауға күш салады» (Varese, 2010, p. 14). Мұндай реттеу әкімшілер мен модераторлар сайт пен контентті бақылайтын және платформаларды пайдалану ережелерін орындалуын қамтитын қараңғы нарықтарда (мысалы, жойылған DarkMarket және CardersMarket нарықтарында) мүмкін. Ережелер сақталмаған жағдайда ережені бұзған тұлғалар сайт мүшелерінің қатарынан шығарылады. «Белгілі бір тауарларды немесе қызметтерді өндіру және тарату» осы сайттарда бақылануы мүмкін болғанымен, мұндай бақылау басқа онлайн форумдарға қолданылмайды (бұл желілердің құқықтары мен өкілеттіктерін шектейді). Сондықтан, дәстүрлі ұйымдасқан қылмыстан айырмашылығы, олардың «қылмыстық астыртын өндірістегі өндіріс пен белгілі бір тауарларды (немесе қызметтерді) бақылауы» шектеулі (Leukfeldt, Lavorgna, and Kleemans, 2017, p. 296).

Қараңғы нарықтарда заңсыз тауарлар мен қызметтердің құрылымы, ұйымдастырылуы, реттелуі және бақылауы оларды басқаратын және/немесе модерациялайтын адамдарға емес, интернет сайттарына байланысты. Нәтижесінде, бұл қараңғы нарықтың сайттары Интернеттен ажыратылғанда (мысалы, құқық қорғау органдарының тергеуіне немесе сайтты тәркілеуге байланысты) сол сайтпен байланысты желі көп жағдайда жұмысын тоқтатады. Дегенмен, полицияның тергеуі мен қудалау процестеріне қатыспайтын сайттың қатысушылары немесе басқа тұлғалар тоқтатылған сайтты шынайы түрде қайта шығаратын басқа сайтты жасайтын ерекше жағдайлар бар. Сыбайлас жемқорлықпен және күш қолданумен немесе күш қолдану туралы қорқытумен байланысты дәстүрлі ұйымдасқан қылмыстық желілерге тән тағы екі сипаттама (Arsovska, 2011) ұйымдасқан киберқылмыс контекстінде өз көрінісін таппайды (Leukfeldt, Lavorgna, and Kleemans, 2017). Дегенмен, бұл ұйымдасқан қылмыстық әрекет түріне байланысты. Бірінші сипаттама үшін зерттеулер саяси сыбайлас жемқорлық ұйымдасқан қылмыспен айналысу туралы шешімдерге әсер ететінін көрсетті. Бір елде интернет-алаяқтық басқа қаржылық қылмыстармен қатар мемлекет қызметінің ажырамас бөлігі ретінде танылды. Екінші белгі бойынша, зорлық-зомбылық немесе зорлық-зомбылық қаупі ұйымдасқан киберқылмыстық әрекеттің мақсаттарына жету үшін қолданылып жатқаны туралы дәлелдер аз (БҰҰ ЕҚБ, 2013; Leukfeldt, Lavorgna, and Kleemans, 2017), мысалы, кейбір жағдайларды қоспағанда, *ақша қашырлары* (яғни, «басқалардың сұрауы бойынша және сыйақы үшін ... ақшаны заңсыз түрде алатын және аударатын жеке тұлғалар»; Maras, 2016) ұйымдасқан киберқылмыстық әрекеттеріне қатысып және билікке олардың заңсыз әрекеттерге қатысқаны немесе қылмыскерлер қауіп төндіргендіктен қатысуын жалғастырып жүргені туралы хабарлайды (Leukfeldt, Lavorgna, and Kleemans, 2017, p. 294). Физикалық зорлық-зомбылыққа балама ретінде

ұйымдасқан киберқылмыскерлер кибершабуылдар жасайды немесе кибершабуылдар немесе басқа да киберқылмыстарды жасаймын деп қорқытады, оларды талаптарын орындауға мәжбүрлейді (Maras, 2016). Мысалдарға ұйымдасқан киберқылмыскерлердің *криптобопсалаушы* (пайдаланушының цифрлық құрылғысын жұқтыратын, пайдаланушы құжаттарын шифрлайтын және жәбірленуші төлемді төлемеген жағдайда файлдар мен деректерді жою қаупін төндіретін зиянды бағдарлама) және/немесе *шифрлық бопсалаушыны* пайдалануы жатады.

3. Ұйымдасқан киберқылмыстылықпен айналысуға тартылған қылмыстық топтар.

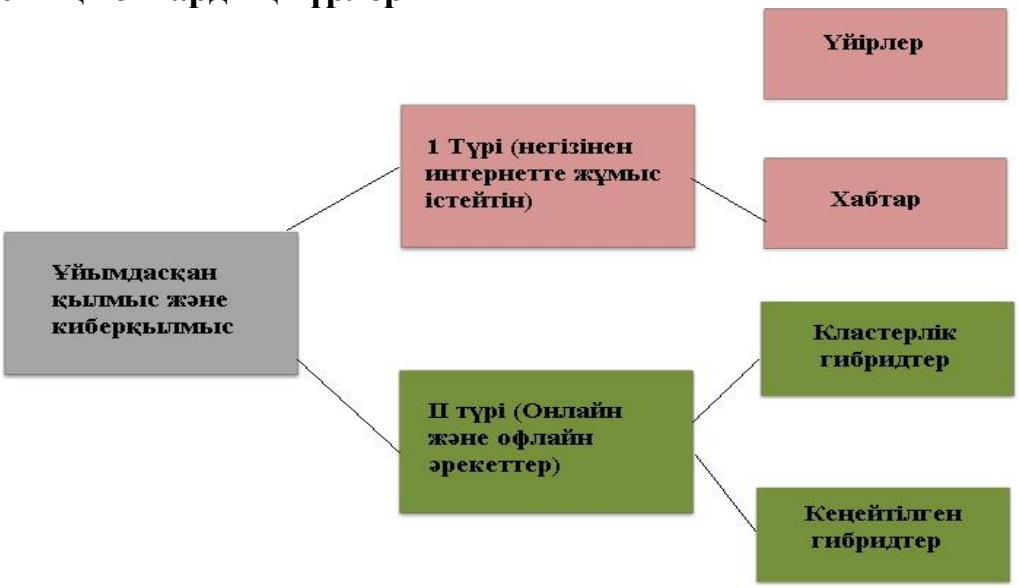
Ұйымдасқан киберқылмыстылыққа киберқылмыстылыққа тартылған ұйымдасқан қылмыстық топтардың, сондай-ақ Ұйымдасқан қылмыстылыққа қарсы конвенцияда белгіленген критерийлерге сәйкес келмейтін және әдетте ұйымдасқан қылмыстылықпен байланысты әрекеттерге тартылған киберқылмыскерлер немесе басқа топтардың әрекеттері кіруі мүмкін. Ұйымдасқан киберқылмыстың бірінші түрі үшін дәстүрлі ұйымдасқан қылмыстық топтардың киберқылмыспен айналысатыны туралы деректер бар (БҰҰ ЕҚБ, 2013). Зерттеулер сондай-ақ ұйымдасқан қылмыстық топтардың киберқылмыс жасау үшін ақпараттық-коммуникациялық технологиялар ұсынатын мүмкіндіктерді пайдаланатынын көрсетеді. Атап айтқанда, бір зерттеу ұйымдасқан қылмыстық топтар ақпараттық және коммуникациялық технологияларды жаңа қылмыстық онлайн нарықтарды (мысалы, онлайн құмар ойындар нарығын) пайдалану үшін қолданатынын көрсетті. Мысалы, 2016 жылы Каморра және Ндрангета қылмыстық топтарының мүшелері онлайн құмар ойындарын ұйымдастырғаны үшін қамауға алынды (OCCRP, 2016). Оның үстіне, ұйымдасқан қылмыстық топтар офлайн ұйымдасқан қылмыстық әрекеттерге әрекеттесуі үшін киберқылмыстарға тартылады. Мысалы, есірткі саудасымен айналысатын ұйымдасқан қылмыстық топ Бельгияның Антверпен портының контейнерлік деректерін сақтайтын ақпараттық жүйелеріне қол жеткізу үшін хакерлерді жалдаған.

Ұйымдасқан киберқылмысқа тартылған ұйымдасқан қылмыстық топтар тек киберкеңістікте әрекет ете алады немесе киберкеңістікті ішінара ғана пайдалана алады. Оның үстіне, зерттеушілер ұйымдасқан қылмыс түсінігін толық немесе ішінара Интернетте орын алатын қандай да бір тікелей немесе жанама пайда алу ниетімен әрекеттерді қоса алғанда кеңейтті. Осылайша, бұл топтар ішінара, басым немесе тек қана желілік ортада жұмыс істей алады. Желілер құрылған және/немесе тек және/немесе негізінен желіде жұмыс істейтін жағдайлар болғанымен дегенмен, ұйымдасқан киберқылмыстық желілерді құру және дамыту бойынша зерттеулер осы желілердің кеңеюінде географиялық жақындық пен офлайн байланыстардың қалыптасуы мен кеңеюінде (жалдау арқылы) үлкен рөл атқаратынын көрсетеді. (Broadhurst et al., 2014; Leukfeldt, Lavorgna, және Kleemans, 2017, pp. 292-293). Мысалы, Шығыс Еуропада ұйымдасқан киберқылмыстық желілердің танымал нүктелері мен хабтары анықталды. Сонымен қатар, Еуропол «ЕО азаматтарына бағытталған әлеуметтік инженерлік алаяқтықты Батыс

Африканың ұйымдасқан қылмыстық топтары жасайды» деп тапты (Europol, 2018, p. 13).

Осы уақытқа дейін ұйымдасқан киберқылмыстық әрекеттерді ұйымдастыру дәрежесі туралы іс жүзінде ештеңе белгілі емес. Ұйымдасқан киберқылмыстың құрылымы, киберқылмыстың осы түріне тартылған топтар және жасалған киберқылмыс түрлері бойынша эмпирикалық дәлелдеме базасы шектеулі (БҰҰ ЕҚБ, 2013, 50 б.). Дегенмен, ұйымдасқан қылмыс пен киберқылмыс арасындағы байланыстардың қолда бар дәлелдерін ескере отырып, «Интернеттегі әрекеттерге топтардың тартылу дәрежесіне (офлайн әрекеттерге қарағанда) және топ ішіндегі байланыстардың құрылымына» негізделген (BAE) типологиялар ұсынылған. Systems Detica және Лондон Метрополитен Университеті, 2012, UNODC-да келтірілген, 2013, 51-бет). Атап айтқанда, топтардың үш негізгі түрі анықталды: негізінен интернетте жұмыс істейтін және киберқылмыс жасайтын топтар (I түрі); офлайн және онлайн жұмыс істейтін және қылмыс пен киберқылмыстылыққа тартылған топтар (II түрі) (2-суретті қараңыз); және офлайн қылмыстар жасау үшін тек ақпараттық-коммуникациялық технологияларды пайдаланатын топтар (III түрі; 2-суретте көрсетілмеген).

2-сурет: Ұйымдасқан киберқылмыстылыққа тартылған қылмыстық топтардың түрлері



Қайнар көзі: BAE Detica/ LMU

Сонымен қатар, әр түрдегі топтар арасында айырмашылық жасалады. (BAE Systems Detica және London Metropolitan University, 2012; БҰҰ ЕҚБ, 2013; Broadhurst et al., 2014):

I түрлі топтар одан әрі *«үйірлер»* (яғни, негізінен желіде жұмыс істейтін аз құрылымды топтар) және *«хабтар»* (яғни, негізінен желіде жұмыс істейтін неғұрлым құрылымды топтар) болып бөлінуі мүмкін. «Үйірлер» - белгілі бір мақсатқа жету үшін құрылатын және міндеттерін орындағаннан кейін жойылатын қысқа мерзімді бірлестіктер (BAE Systems Detica and London Metropolitan University, 2012).

II типті топтар одан әрі *кластерлік гибридтерге* (яғни, белгілі бір қылмыс пен киберқылмыс, жұмыс әдістері мен тактикасы немесе орналасқан жері негізінде топтасатын шағын топтар) және *кеңейтілген гибридтерге* (яғни, офлайн және онлайн режимінде нақты анықталған, аса күрделі топтар) бөлуге болады.

III түрлі топтар *иерархиялар* (яғни, ақпараттық-коммуникациялық технологияларды пайдалана отырып, офлайн әрекеттерін жеңілдету үшін басқаларды пайдаланатын дәстүрлі ұйымдасқан қылмыстық топтар) және *агрегациялар* (яғни, офлайн әрекеттерді жылжыту үшін шектеулі, нақты себептермен АКТ-ны пайдаланатын қысқа мерзімді, нашар ұйымдастырылған топтар) болуы мүмкін.

Бұл топтардың мүшелері әртүрлі рөлдерді орындайды және өз топтары үшін әртүрлі дәрежеде маңыздылыққа ие. Олардың кейбіреулері топ және оның әрекеттері үшін маңызды, ал басқалары қосымша мүшелер немесе тіпті бір реттік тапсырмалар үшін мүшелер болып саналады. Бірінші санатқа жасалатын киберқылмысқа (немесе киберқылмыстарға) байланысты топ қызметінің табысты болуы үшін маңызды болып табылатын жетекші және кейбір негізгі мүшелер кіреді (мысалы, бағдарламашылар, жүйелерды басып алушы зиянкестер, техникалық сарапшылар, деректер өндіруші, ақша операциялар бойынша мамандар және т.б.). Екінші категорияға, мысалы, ақша қашырлары жатады. Бұл адамдар (біле тұра, білмей) қылмыскерлермен жалданады, олар үшін жұмыс істейді, үшінші тұлғалар арасында тауарларды береды және ақшаны жылыстату үшін пайдаланылады (Maras, 2016).

2018 жылы ұйымдасқан киберқылмыстылққа тартылған қылмыстық топ «*іскерлік хат алмасудың ымыраласуы*» типтегі шабуылын жасады, ол өз құрбандарына компаниялармен жұмыс істеген заңды тұлға ретінде таныстырған киберқылмыскерлерге ақша аударма жасатқан. Бұл оқиғада Құрама Штаттардағы ақша қашырлары ақша аударымдарын қамтитын жұмыс ұсынысын алды және/немесе жалған компанияларды құруға және онлайн алаяқтықтан кіріс алу үшін жалған компанияларға банк шоттарын ашуға жалданды. Ақша қашырымен бақыланып отырған банктік шоттарға ақша аударылғаннан кейін, ақша қашыры кірістің бір бөлігін (жалдаушымен және/немесе топ мүшелерімен келісім бойынша) өзіне қалдырып және қалған ақшаны Польшадағы немесе Қытайдағы банкке аударды. Ақша қашырлары және ұйымдасқан киберқылмыстық топтардың негізгі емес мүшелері топтың уақытша мүшелері болып табылады және оның қызметіне қажетінше және/немесе олар өз міндеттерін орындағанға дейін ғана қатысады.

4. Ұйымдасқан киберқылмыстылық қызмет.

Ұйымдасқан киберқылмыскерлер әртүрлі киберқылмыстарға, соның ішінде алаяқтық, хакерлік шабуылдары, зиянды бағдарламаларды жасау және тарату, DDoS шабуылдары, бопсалау және контрафактілік немесе жалған брендтік тауарларды (мысалы, киім, аксессуарлар, аяқ киім, электроника, дәрілік өнімдер, автомобиль бөлшектер және т.б.) сондай-ақ осы өнімдерге арналған жапсырмалар, қаптамалар және кез келген басқа тауар сәйкестендіру белгілерін сату сияқты зияткерлік меншік саласындағы қылмыстарына

қатысады. Сонымен қатар киберқылмыстылыққа тартылған қылмыстық топтар қылмыстар мен киберқылмыстарды жасауға көмектесетін қызметтерді көрсетумен айналысады («қызмет ретіндегі қылмыс»), бұларға деректер мен жеке басын куәландыратын құжаттарды (мысалы, қаржылық және медициналық деректер, төлқұжаттар, тіркелген сайлаушылардың жеке басын куәландыратын деректер) ұсыну; зиянды бағдарламар ұсыну (арнайы тапсырыспен немесе белгілі бағдарламалар, мысалы, пайдаланушының банктік ақпаратын және интернет-шоттарға кіру үшін қажетті басқа ақпаратты құпия түрде алуға арналған Zeus банктік троян бағдарламасы); таратылған бас тарту шабуылдарын (DDoS шабуылдары) және бот желілері қызметтерін жүргізу; пернетақтаталық шпиондарды ұсыну; фишинг/мақсатты фишинг құралдарын, хакерлік оқулықтарды, осалдықтар мен эксплойттар туралы мәліметтерді, сондай-ақ пайда алу үшін оларды қалай пайдалану керектігі туралы нұсқауларды ұсыну (Broadhurst et al., 2018; Maras, 2016). Мысалы, Shadowcrew, «шамамен 4000 мүшесі бар халықаралық ұйым... Интернеттегі ауқымды және әр түрлі қылмыстық әрекетті ілгерілетіп және жеңілдеткен, оның ішінде электрондық жеке басын куәландыратын мәліметтердің ұрлықтары, несиелік және дебеттік карталар алаяқтығы, жеке басын куәландыратын жалған құжаттарды жасау және сату (*United States v. Mantovani et al*., criminal indictment, 2014).

Ұйымдасқан қылмыстық топтар сонымен қатар Интернетте заңсыз өнімдер мен қызметтерді сатудан табыс көреді және/немесе басқа пайда көреді. Мысалы, Butterfly Bot зиянды бағдарламасының жасаушысы оны Windows және Linux компьютерлерін басқаруға қабілетті деп желіде жарнамалады (BBC News, 2013). Butterfly Bot жасаушысы сонымен қатар зиянды бағдарламаның функционалдығын өзгертетін плагиндерді сатты, сонымен қатар төлем жасай алатын тұтынушылар үшін бағдарламаның теңшелген нұсқасын жасауды ұсынды. Әртүрлі онлайн қылмыстық желілер Botfly Bot-ты пайдаланды және осы зиянды бағдарламаның масштабы бойынша ең үлкен пайдаланылуы әлем бойынша 12,7 миллион компьютерді жұқтырғаны Mariposa ботнетінің жасалуына әкелді (BBC News, 2013).

Ұйымдасқан киберқылмыскерлер сонымен қатар қылмыскерлерге серверлерді киберқылмыс жасау үшін пайдалануға мүмкіндік беретін және сол серверлерден қылмыстық мазмұнды жоймайтын «*оқ өткізбейтін хостинг»* қызметтерін ұсынады (National Cyber Security Centre, 2017, p. 8). Интернеттегі қылмыстық транзакцияларға сенімнің төмендігі және алаяқтардың болуына байланысты ұйымдасқан киберқылмыстық топтар ұсынатын шартты үшінші жаққа ақшаны сақтауға беру қызметтері жоғары сұранысқа ие. Мұндай қызметтер қылмыстық тұтынушылар заңсыз тауарлар мен қызметтер үшін төлейтін ақшаны олар төлеген тауарлар немесе қызметтерді алғанын растағаннан кейін ғана жіберуге мүмкіндік береді (National Cyber Security Centre, 2017, p. 8).

Заңсыз тауарлар мен қызметтер негізінен *криптовалюта* арқылы сатып алынады (яғни «қауіпсіздік мақсатында криптографияны пайдаланатын цифрлық валюта»; Maras, 2016, p. 337). Нарықта көптеген криптовалюталар

бар (мысалы, биткойн, Litecoin, Dogecoin, Ethereum, Monero және т.б.). Даркнет нарықтарының көпшілігі негізінен биткоинмен сауда жасайтынымен, басқа криптовалюталар (мысалы, Ethereum және Monero) да пайдаланылады және кейбір жағдайларда биткоиннен оларға артықшылық беріледі (US Department of Justice, 2017; Broadhurst et al., 2018; Europol, 2018). Кейбір даркнет сайттары «тумблер» атаулы «барлық төлемдерді жалған транзакциялардың күрделі, жартылай ерікті сериясы арқылы» жіберетін «қосқыш қосқышты» құралды пайдаланады, бұл төлемді кез келген сайттан шыққан криптовалютамен байланыстыруды іс жүзінде мүмкін емес етеді. (United States v. Ross William Ulbricht, Criminal Complaint, 2013, p. 14).

Сонымен қатар, ұйымдасқан киберқылмыскерлер *ақшаны жылыстату* қызметтерін де ұсынады, яғни, «қылмыскерлердің заңсыз қаражатын жасыру және заңдастыру» (Maras, 2016). Ұйымдасқан киберқылмыскерлердің қызметтерінен түскен кірістер де жылысталуда. Ақшаны жылыстату процесі үш кезеңді қамтиды: заңсыз кірістерді қаржы жүйесіне енгізу (*орналастыру*), заңсыз ақша қаражаттарының пайда болу көзін жасыру (*қабаттау*) және шығу көзін көрсетпей ақша қаражаттарын экономикаға қайтару. Ақшаны жылыстату *сандық валютаны* қолдану арқылы жүзеге асырылады (яғни, тек виртуалды түрде бар реттелмейтін валюта); алдын ала төленген несиелік және дебеттік карталар (тіпті биткоин карталары); сыйлық карталары; ақша қашырларының банктік шоттары; ойдан шығарылған тұлғалар мен жалған компаниялардың атына ашылған банк шоттары; PayPal шоттары; интернеттегі құмар ойын сайттары (виртуалды ойын валютасы арқылы); және заңсыз ойын сайттары. Сонымен қатар, ұйымдасқан киберқылмыскерлер ақпараттық-коммуникациялық технологияларды (АКТ) мигранттардың контрабандасы және адам саудасы, жабайы табиғат объектілері, есірткі, атыс қаруы және темекі саудасы сияқты офлайн дәстүрлі ұйымдасқан қылмыстық әрекеттерге әрекеттесу үшін пайдаланады. Мысалы, Біріккен Ұлттар Ұйымының Трансұлттық ұйымдасқан қылмыстылыққа қарсы конвенциясын толықтыратын 2000 жылғы мигранттарды құрлық, теңіз және әуе арқылы заңсыз алып өтуге қарсы Хаттаманың 3(а) бабына сәйкес мигранттардың контрабандасы «тікелей немесе жанама түрде кез келген қаржылық немесе басқа да материалдық пайда алу мақсаты, азаматы немесе оның аумағының резиденті болып табылмайтын кез келген тұлғаның кез келген Қатысушы мемлекетке заңсыз кіруін қамтамасыз ету» ретінде анықталады, бұл өз қызметтерін жарнамалау, мигранттарды тарту, олармен байланыс орнату және ақыр соңында, оларға өз қызметтерін сату үшін АКТ-ны пайдаланатын контрабандашылардың әрекеттесуымен жүзеге асырылады.

Талқылауға арналған сұрақтар:

1. Сіздің елдің азаматтары негізінен қандай криптовалютаны пайдаланады? Ол не үшін пайдаланылады?

2. Қолданылатын басқа криптовалюталар бар ма? Олай болса, оларды анықтап, талқылаңыз.

3. Ұйымдасқан киберқылмыскерлер криптовалюталарды қалай

пайдаланады?

14 Тақырып. Хактивизм, терроризм, тыңшылық, жалған ақпараттық кампаниялар және киберкеңістіктегі соғыстар.

1. Хактивизм.

Ақпараттық-коммуникациялық технологиялар әлеуметтік немесе саяси өзгерістер кампанияларда (яғни онлайн белсенділік үшін) пайдаланылады. Бұл түрдегі науқандарға онлайн петицияларға қол жинау, хэштег-кампаниялары, кампанияның веб-сайтын жасау, еріктілерді тарту, қатысушылар мен қолдаушылардан қаражат алу, оффлайн-наразылық акцияларын ұйымдастыру және жоспарлау кіреді (Maras, 2016). Дегенмен, өз идеяларына назар аудару үшін мұндай әдістерді жеткіліксіз деп санайтын және оның орнына саяси наразылық құралы ретінде веб-сайттар мен онлайн-сервистердің жұмыс істеуіне немесе қолжетімділігіне тікелей әсер ететін стратегияларға жүгінетін жеке адамдар мен адамдар топтары бар (яғни, *хактивистер*) (Maras, 2016).

Хактивизм терминінің жалпы қабылданған анықтамасы болмаса да, бұл әрекеттер жүйелерге, веб-сайттарға және/немесе деректерге рұқсатсыз немесе рұқсат етілген қол жеткізуден асатын әдейі қол жеткізу және/немесе жүйелердің жұмыс істеуіне және/немесе қол жетімділігіне әдейі кедергі жасау, әлеуметтік немесе саяси өзгерістерді алға жылжыту үшін рұқсатсыз немесе рұқсат етілген қол жеткізуден асатын веб-сайттар мен деректер болып табылады (Maras, 2016). Хактивизмнің заңды саяси наразылықтың бір түрі ретіндегі заңдылығы туралы пікірлер әртүрлі. Мысалы, таратылған қызмет көрсетуден бас тарту шабуылдарын имитациялауға арналған, бірақ веб-сайтқа бағытталған зиянды бағдарлама жұқтырған сандық құрылғыларды (яғни, бот-желілерді) пайдалануды қамтымайтын виртуалды ереуіл отырыстарды кейбір зерттеушілер саяси әрекеттің бір түрі ретінде сипаттады. наразылық. Виртуалды отырыстар (немесе блокадалар) ұжымдық әрекетті қамтиды, онда «мыңдаған белсенділер бір уақытта веб-сайтқа кіріп, басқа пайдаланушылар оған кіре алмайтын сайтта жеткілікті трафикті жасауға тырысады». Мысалы, адамдар тобы сайтқа кірген кезде бір уақытта және үздіксіз жаңару түймесін басқанда. Мұндай виртуалды ереуілдер осы веб-сайтқа қайталанатын және жиі кірумен байланысты веб-сайтқа рұқсаты бар әрекеттер ретінде сипатталады; мұндай қайталанатын және жиі қол жеткізу басқа пайдаланушылардың осы веб-сайтқа кіруіне кедергі болатын ауқымда болады. Әртүрлі әлеуметтік және саяси мақсаттары бар хакерлердің көптеген топтары бар. Хактивисттер жасайтын киберқылмыстарға веб-сайттарды бүлдіру, пайдаланушыларды басқа веб-сайтқа қайта бағыттау, «қызмет көрсетуден бас тарту» (DoS) немесе таратылған «қызмет көрсетуден бас тарту» (DDoS) шабуылдары, зиянды бағдарламаларды тарату, деректерді ұрлау және ашу, сондай-ақ саботаж кіреді (Maras, 2016). Бұл әдістердің барлығы шабуылдың нысанасы болып табылатын жүйелерге, веб-сайттарға және/немесе деректерге рұқсатсыз кіруді білдіреді. Мысалы, Угандада ел президентінің ресми резиденциясының және Уганданың Инвестициялық басқармасының веб-сайттарын хакерлер

бұрмалап, президент резиденциясының сайтында нацистік свастика мен Адольф Гитлердің суретін жариялап, ал Инвестициялық басқармасының сайтының бір бөлігін қорқынышты клоунның суретымен ауыстырған.

2. Кибертыңшылық.

Тыңшылық терминінің бірыңғай әмбебап анықтамасының болмауына қарамастан, ол барлау деректерін жинау әдісі ретінде анықталады: атап айтқанда, «адами көздерін (агенттерді) немесе техникалық құралдарды (мысалы, компьютерлік жүйелерді бұзу арқылы) қолдана отырып, әдетте көпшілікке қол жетімді емес ақпарат алу» процесі (UK MI5 Security Service, n.d.). Алайда, тіпті «барлау деректерін жинау» термині «халықаралық деңгейде танылған және қолдануға болатын анықтамаға» ие емес. Оның үстіне, «барлау деректері» терминінің осы терминді анықтауды сұрайтын сарапшылар да сияқты көптеген анықтамалары бар. Уорнердің (Warner) айтуынша, «шпиондық операциялар» терминінің аудармашылары әдетте қарсыластардың екі лагерінің біріне сілтеме жасайды: «бірінші лагерьде талдаушылар XX ғасырдағы американдық әскери терминологияны ұстанады және барлау шешім қабылдаушыларға арналған ақпарат деп санайды; бұл кез-келген ақпарат көзінен алынған кез-келген ақпарат, ол басшыға қарсыласпен қалай әрекет ету туралы шешім қабылдауға көмектеседі. Екінші лагерьде барлауды жинау тыныш жолмен соғыс ретінде анықталады». Любин шпиондық операциялардың егжей-тегжейлі анықтамасын ұсынады. Ол мұндай операциялардың барлығы мынадай төрт элементті қамтиды деп бекітеді: «1) операция мемлекеттің немесе мемлекеттердің шешімдер қабылдауы үшін маңызы бар не өзге де қатынастарда белгілі бір мемлекеттік мүдделерге қызмет ететін мәліметтерді жинауды, талдауды, тексеруді және таратуды көздейді; 2) операция мемлекеттің немесе мемлекеттердің агенттерімен не тиісті мемлекетпен немесе мемлекеттермен тығыз байланысты адамдармен бастамашылық жасайды; 3) операция шет мемлекетке немесе шет мемлекеттерге, олардың субъектілеріне, қауымдастықтарына, корпорацияларына немесе агенттеріне бағытталған және осы мемлекеттің немесе осы мемлекеттердің білместен және олардың келісімінсіз жүзеге асырылады; және 4) операция оның жүргізілуіне себепші болатын қажеттіліктерге және/немесе оның тиімділігін қамтамасыз ету үшін жинау мен талдаудың пайдаланылатын әдістеріне қатысты құпиялылық пен құпиялылықтың белгілі бір дәрежесін көздейді».

Кибертыңшылық белгілі бір экономикалық немесе жеке пайда алу үшін жеке тұлғалардың, адамдар тобының немесе компаниялардың ақпараттық-коммуникациялық технологияларды (АКТ) пайдалануын көздейді. Кибер тыңшылық Ұлттық қауіпсіздік, экономикалық бәсекеге қабілеттілік және/немесе өз елінің әскери қуатын арттыру үшін жүйелер мен деректерге рұқсатсыз қол жеткізу және оларды қызықтыратын объектілер туралы барлау жинау үшін үкіметтік құрылымдар, мемлекет қаржыландыратын немесе бақылайтын топтар немесе үкімет атынан әрекет ететін басқа да адамдар жүзеге асыра алады (Maras, 2016). Тыңшылық жаңа құбылыс болмаса да, АКТ-ның пайда болуы прецеденті болмаған жылдамдықпен, жиілікпен,

қарқындылықпен және бұрын-соңды болмаған масштабта басқа елдер жасаған және/немесе ұйымдастырған барлауды заңсыз жинау әрекеттерін жүзеге асыруға мүмкіндік берді, сондай-ақ тыңшылықты жүзеге асырумен байланысты тәуекелдерді азайту (мысалы, деректерді жинауға бағытталған елімен ұсталыну қаупі). Кибертыңшылықты интернетте кеңінен қол жетімді көптеген хакерлік құралдардың арқасында мүмкін болды. Бұл құралдарға *эксплойттар* (мысалы, *нөлдік күндік осалдық*, яғни олар анықталғаннан кейін бұрын белгісіз осалдықтар немесе жүйелерге еніп, брандмауэрлерді айналып өтуі мүмкін зиянды бағдарламалар) және *имплanттар* (мысалы, *бэкдор*, жүйелерге рұқсатсыз қол жеткізу үшін пайдаланылатын құпия портал немесе қашықтан қол жеткізу RAT құралы) кіреді. 2016 жылдан бастап Shadow Brokers деп танылатын топ хакерлік құралдарды шығарады (Newman, 2018). Осындай құралдардың бірі Windows осалдығын пайдалануға арналған (EternalBlue эксплойты); ол WannaCry бағдарламасының бөлігі болды, ол бүкіл әлем бойынша денсаулық сақтау, көлік және басқа жүйелерге зиян келтіру мақсатында шабуыл жасады.

3. Кибертерроризм.

Ақпараттық-коммуникациялық технологиялар (АКТ) терроризмге байланысты қылмыстарды жасауға ықпал ету үшін (кибертехнология арқылы жасалған терроризмнің бір түрі) немесе террористердің мақсаты болуы мүмкін (кибертәуелді терроризм нысаны). Мысалы, АКТ террористік актілерді көтермелеу, қолдау, оларды жасауға және/немесе оларға қатысу үшін әрекеттестікте пайдаланылуы мүмкін. Атап айтқанда, интернетті террористік іс-әрекеттің «үгіт-насихат» тарату (терроризмге тарту, радикалдандыру және терроризм қоздыруды қоса алғанда) терроризмді қаржыландыру; террористерді дайындау; террористік шабуылдарды жоспарлау (оның ішінде құпия байланыс арналары мен ашық көздерден алынған ақпаратты пайдалану арқылы); террористік актілерді орындау; және кибершабуылдар» сияқты мақсаттары үшін пайдалануға болады. (UNODC, 2012, p. 3). Кибертерроризм терминін кейбір зерттеушілер интернетті террористік мақсатта пайдалануға байланысты әрекеттерді сипаттау үшін қолданады.

«Киберқылмыстылық» терминінің анықтамасына қатысты бірыңғай пікір жоқ сияқты, дәл солай терроризмнің де, кибертерроризмнің де жалпы қабылданған анықтамалары жоқ. Кибертерроризм ұғымдары «кең тұжырымдамалардан... интернеттегі террористік әрекеттің кез-келген түрін қамтитын... осы ұғымды неғұрлым тар түсінуге дейін» өзгерып отырады. Кейбір зерттеушілер кибертерроризмді тар мағынада «таза кибертерроризм» деп түсіндіреді. Осындай тар анықтамада кибертерроризм саяси мақсатта қорқыныш тудыратын, шабуыл объектісі болып табылатын үкіметті немесе халықты қорқыту және/немесе оған қысым жасау, сондай-ақ зиян келтіру немесе зиян келтіру қаупін төндіру үшін жасалған кибершабуыл ретінде қарастырылады (мысалы, саботаж). Кибертерроризмнің осындай тар түсініктемесінің мысалдарына «өлімге немесе денеге зиян келтіруге, жарылыстарға, ұшақ апаттарына, судың ластануына немесе ауыр экономикалық шығындарға әкелетін шабуылдар жатады... Маңызды

инфрақұрылым объектілеріне елеулі шабуылдар олардың салдарына байланысты кибертерроризм актілері болуы мүмкін. Екінші кезектегі қызметтердің жұмысын бұзатын немесе негізінен шығындарға байланысты қиындықтар тудыратын шабуылдар кибертерроризм емес».

4. Киберсоғыс.

Бұқаралық ақпарат құралдары, саясаткерлер, ғалымдар және тәжірибелі мамандар киберқылмыспен байланысты көптеген оқиғаларды «кибернетикалық соғыстар» немесе «киберсоғыс» санатына жатқызады (Maras, 2014; Maras, 2016). Жоғарыда қарастырылған басқа терминдер сияқты, киберсоғыс туралы бірыңғай әмбебап анықтама жоқ. *Киберсоғыс* термині маңызды инфрақұрылым жүйелеріне қауіп төндіретін және бұзатын және қарулы шабуылға теңестірілуі мүмкін киберкеңістіктегі әрекеттерді сипаттау үшін қолданылады (Maras, 2016). Қарулы шабуыл - бұл жойқын салдарға әкелетін қасақана әрекет (яғни, тірі адамдардың өлімі және/немесе тірі жандардың дене жарақаты және/немесе мүліктің жойылуы) (Maras, 2016). Кибер соғысқа тек үкіметтер, мемлекеттік органдар немесе мемлекет басқаратын немесе қаржыландыратын жеке тұлғалар немесе адамдар тобы қатыса алады.

Соғыс әдістеріне қатысты қолданыстағы құқықтық нормалар мен ережелер киберсоғыстарға қолданылады. Киберсоғысты бастамас бұрын, *jus ad bellum* (яғни, күш қолдану құқығы) бекіту керек. Бұл ретте кез келген нысандағы күш қолдану себептері заңды болуға және заңнамамен рұқсат етілуге тиіс. Осындай негізделген себептердің бірі - өзін-өзі қорғау. Елдер өзін-өзі қорғау мақсатында күш қолдана алатындығы 1945 жылғы БҰҰ Жарғысының 51-бабында қарастырылған, онда былай айтылған: «Осы Жарғы, Егер қауіпсіздік кеңесі халықаралық бейбітшілік пен қауіпсіздікті қолдау үшін қажетті шараларды қабылдағанға дейін ұйым мүшесіне қарулы шабуыл жасалатын болса, жеке немесе ұжымдық өзін-өзі қорғаудың ажырамас құқығын ешбір жағдайда қозғамайды. Ұйым мүшелерінің өзін-өзі қорғауға осы құқықты жүзеге асыру кезінде қабылдаған шаралары Қауіпсіздік Кеңесіне дереу хабарлануға тиіс және осы Жарғыға сәйкес халықаралық бейбітшілік пен қауіпсіздікті қолдау немесе қалпына келтіру үшін өзі қажет деп санайтын әрекеттерді кез келген уақытта қабылдауға қатысты Қауіпсіздік кеңесінің өкілеттіктері мен жауапкершілігін ешқандай да қозғамауға тиіс.

Өзін-өзі қорғау құқығы БҰҰ Жарғысының 2 (4) - бабында көзделген басқа мемлекеттерге қарсы күш қолдануға жалпы тыйым салудан ерекшеліктердің бірі болып табылады «Біріккен Ұлттар Ұйымының барлық мүшелері өздерінің халықаралық қатынастарында кез келген мемлекеттің аумақтық қол сұғылмаушылығына немесе саяси тәуелсіздігіне қарсы, сондай-ақ Біріккен Ұлттар Ұйымының мақсаттарымен үйлеспейтін қандай да бір басқа жолмен күш қолданудан немесе оны қолдану туралы қауіп төндіруден қалыс қалады».

Кибер соғысқа қатысқан кезде *jus in bello* (яғни, соғыс ережелерін) сақтау қажет. Бұл ретте күш қолданумен тең келетін киберкеңістіктегі іс-әрекеттер: мөлшерлес болуы (жауап іс-әрекеттері үшін негіз болған қауіп

ретінде де, сондай-ақ ықтимал ілеспелі залалды ескере отырып та); белгілі бір сақтық шараларын қолдану арқылы шығындарды барынша азайтуға бағытталуы; мақсаттарды тануы (яғни, тек нақты мақсат кибершабуылдарға ұшырауы тиіс) тиіс; және аз агрессивті құралдар таусылғаннан және/немесе мүмкін емес ретінде шығарылғаннан кейін ғана соңғы шара ретінде қолданылады (Maras, 2016).

5. Ақпараттық соғыс, жалған ақпарат және сайлау алаяқтық.

Ақпараттық соғыс термині жауға белгілі бір артықшылық алу үшін ақпаратты жинау, тарату, өзгерту, бұзу, бүлдіру, зақымдау және сапасының нашарлауын сипаттау үшін қолданылады. Бұл процестің мақсаты белгілі бір нәтижеге қол жеткізу үшін қандай да бір мәселеге немесе қандай да бір оқиғаға қатысты объектінің қабылдауын өзгерту үшін осы ақпаратты пайдалану мен хабарлауда. Ақпараттық соғыста екі әдіс қолданылады: *жалған ақпарат* (яғни, жалған ақпаратты әдейі тарату) және *жалған жаңалықтар* (яғни, нақты жаңалықтар түрінде таратылатын үгіт-насихат және жалған ақпарат). Айта кету керек, аталған терминдердің соңғысы нақты анықтамаға ие емес және дұрыс пайдаланылмауы мүмкін (Пікір білдіру, сонымен қатар «фейк» жаңалықтар, жалған ақпарат және үгіт-насихат бостандығы туралы Бірлескен декларация туралы төмендегі кірістіруді қараңыз).

Сенім деңгейінің төмендеуі жалған жаңалықтардың тез таралуына және қоғамның тұтынуына ықпал етті (Morgan, 2018, p. 39). Жалған ақпарат пен жалған жаңалықтар әлеуметтік желілер платформаларында, сондай-ақ жетекші және екінші кезектегі бұқаралық ақпарат құралдары арқылы таратылады. Әлеуметтік желілер платформалары жалған ақпаратты тезірек таратуға және басқа онлайн платформаларға қарағанда кең аудиторияға қол жеткізуге мүмкіндік береді; кейбір платформаларда ол нақты уақыт режимінде таралуы мүмкін (мысалы, Twitter). Автоматты бот есептік жазбалары бұл ақпаратты жеке пайдаланушыларға қарағанда тезірек және жоғары жиілікте таратуға көмектесе отырып бұл күш-жігерді жеңілдетеді. Мысалы, ИЛИМ (Ирак пен Левант ислам мемлекеті) «The Dawn of Glad Tidings» («Жақсы жаңалықтардың таңы») қосымшасын жасады, оны оның мүшелері мен жақтастары мобильді құрылғыларға жүктей алды; бұл қосымша, басқалармен қатар, Twitter пайдаланушыларының есептік жазбаларына қол жеткізуге және олардың атынан хабарламалар жариялау үшін жасалынған болатын. Жалған ақпарат кампаниялары жақтаушылары мен боттар интернеттегі жалған ақпарат пен жалған жаңалықтардың кең таралуына ықпал етеді. Жалған ақпарат пен жалған жаңалықтардың таңдамалы, қайталанатын және жиі әсер етуі жіберілген хабардың шындыққа деген сенімін қалыптастыруға, нығайтуға және арттыруға көмектеседі. Жалған ақпарат пен жалған жаңалықтар сайлаушылардың мінез-құлқына және сайып келгенде сайлау нәтижелеріне әсер етеді деп саналады.

Сайлаудағы алаяқтық «сайлау нәтижелеріне әсер ету мақсатында сайлаушыларды таңдау еркіндігіне кедергі келтіретін немесе олардың ерік-жігерін бұрмалайтын сайлау процестері мен материалдарын айла-шарғы жасау үшін жасалған кез-келген мақсатты әрекет ретінде анықталуы мүмкін».

Сайлау алаяқтықтарының бір мысалы - дауыс беру құрылғыларына рұқсатсыз кіру және дауыс беру нәтижелерін өзгерту. Атап өту маңызды, сайлаудағы алаяқтықтың жалпы қабылданған анықтамасы жоқ, өйткені алаяқтық ұғымы контекстке байланысты: сайлау процесін алаяқтық айла-шарғы жасау ретінде қабылданған әрекет белгілі бір елге байланысты уақыт өте келе әр түрлі түсіндіріледі. Тіпті ғылыми ортада алаяқтықтың теориялық анықтамалары халықаралық және ішкі құқық, салыстырмалы және американдық саясаттану және дамыған және дамушы елдерде сайлау өткізу салаларында әлі күнге дейін біріздендірілмеген (Alvarez, Hall, and Hyde, 2008, pp. 1-2).

Кейбір елдерде сайлаушылардың мінез-құлқына және сайлау нәтижелеріне әсер етуі мүмкін жалған ақпарат таратқаны үшін, сондай-ақ сайлаудағы алаяқтықтың басқа түрлері үшін қылмыстық жауапкершілік қарастырылған заңдар бар (мысалы, Франция, Ұлыбритания және АҚШ-тың әртүрлі Штаттары). Жалған ақпарат пен жалған жаңалықтар таратқаны үшін қылмыстық жауапкершілікке тартылатын заңдар бар басқа елдер бұл заңдарды үкіметті сынайтын тілшілер мен басқа адамдарды қудалау үшін қолданады (Reuters, 2018).

Талқылауға арналған тапсырма:

Кибершабуылдарға әрекет ету шаралары. А елінде орналасқан компьютерлік компанияның қызметкерлері қаржылық қызметтер секторына «қызмет көрсетуден бас тарту» сияқты көптеген таратылған шабуылдарды жасады және Б. еліндегі дамбаны басқарудың автоматтандырылған жүйесіне қол жеткізді деп айыпталуда. Қаржылық қызметтер секторының өкілдері айтарлықтай экономикалық залал туралы хабарлады; алайда дамба өкілдері тек ақпараттың ұрлағаны туралы хабарлады. Зиянкестер бөгетті басқарудың автоматтандырылған жүйесіне (БАЖ) қол жеткізсе де, бұл жүйені өзгертуге және бөгетті қашықтан басқаруға мүмкіндік береді, бірақ БАЖ-дың бұған мүмкіндік беретін бөлігі автономды режимде болды және оқиға кезінде техникалық қызмет көрсетуден өтті. Бұл компанияның қызметкерлері А елімен қаржыландырған деп саналады.

Сұрақтар:

1. Бұл сценарийде кибер оқиғаның қандай түрі сипатталған? Неге сіз осылай ойлайсыз?
2. Бұл сценарийде А елі оқиға үшін жауапты екенін дәлелдеу үшін не қажет?
3. А елінің жауапкершілігін дәлелдеу кезінде қандай кедергілерге тап болуыңыз мүмкін?
4. Бұл кибераралысуға жауап ретінде қандай әрекеттер жасауға болады? Неге сіз осылай ойлайсыз?
5. Бұл сценарийде жалған жаңалықтарды оңай тануға бола ма? Өз жауабыңызды түсіндіріңіз.
6. Бұл сценарийде адамдар жалған жаңалықтарды тану үшін қандай әрекеттер жасай алады?

Глоссарий

Аванстық төлем алаяқтығы. Ақша аудару, депозиттеу немесе аса ірі ақша сомасына айырбастап өзге де мәміле бойынша операцияны аяқтау үшін аванстық төлем жүргізу туралы өтінішпен хаттарды пайдалануды көздейтін компьютерлік алаяқтықтың түрі.

Адам денесінің іздеу жүйесі. Бірлескен күш-жігермен мақсатты анықтайтын және Интернетте келісілген қорлауды жүзеге асыратын интернет пайдаланушыларын сипаттау үшін қолданылатын термин.

Адамға қарсы киберқылмыстар. Жеке адамдар өзара әрекеттесетін, қарым-қатынас жасайтын және/немесе нақты немесе қиялдағы қарым-қатынасы бар адамдарға қарсы жасалған киберқылмыстар.

Актив. Маңызды және/немесе құнды деп саналатын нәрсе.

Ақпараттық соғыс. Жауға белгілі бір артықшылық алу үшін ақпаратты жинау, тарату, өзгерту, бұзу, бүлдіру, зақымдау және сапасының нашарлау процесі.

Ақшаны жылыстату. Заңды және заңсыз операцияларды біріктіру арқылы заңсыз құралдарды жасыру.

Ақша қашырлары. Заңсыз тауарларды алу және тасымалдау, заңсыз қызмет көрсетуге қатысу және/немесе сыйақы үшін басқа адамдарға заңсыз ақша алу немесе аудару арқылы саналы түрде немесе бейсаналық түрде қылмыс және/немесе киберқылмыстар жасайтын адамдар.

Алғашқы жауапты адамдар. Қылмысқа бірінші болып ден коятын және қылмыс жасалған жерде дәлелдемелердің сақталуы үшін жауап беретін адамдар.

Алдын алу құқығы. Қылмыстардың алдын алу мақсатында тәуекелдерді реттеуге және азайтуға, не, кем дегенде, қылмыс жасау нәтижесінде келтірілген залалды жұмсартуға бағытталған құқықтық нормалар.

Анонимділік. Адамның жеке басын жасыруы, бұл оған өзі және/немесе іс-әрекеті туралы ақпаратты басқа адамдарға ашпай-ақ, кез-келген әрекетті жасауға мүмкіндік береді.

Анонимді прокси-серверлер. Бұл прокси-серверлер пайдаланушыларға IP-мекен-жайларын жасыру және оларды басқа IP-ге ауыстыру арқылы сәйкестендіретін деректерді жасыруға мүмкіндік береді. *Анонимизаторлар* деген атпен де белгілі.

Анонимизаторлар. Бұл прокси-серверлер пайдаланушыларға IP-мекен-жайларын жасыру және оларды басқа IP-ге ауыстыру арқылы сәйкестендіретін деректерді жасыруға мүмкіндік беретін прокси-серверлер. *Анонимді прокси-серверлер* деп те аталады.

Антикриминалистика. Киберқылмыскерлердің тергеуін шатастыру үшін қолданылатын құралдар мен әдістер сандық сот сараптамасын жүргізуді қиындатады. *Сандық антикриминалистика* деп те аталады.

Аса маңызды инфрақұрылым. Қоғамның дұрыс жұмыс істеуі үшін негіз болып саналатын өмірлік маңызды салалар.

Атрибуция. Киберқылмыс үшін кім және/немесе не жауапты екенін анықтау.

Аумақтық егемендік. Мемлекеттің өзінің географиялық аумағына қатысты өз құқықтары мен өкілеттіктерін толық және айрықша жүзеге асыруы.
Әлеуметтік дилемма. Егер шешімдер топтың немесе ұжымның қызығушылығына емес, жеке қызығушылыққа негізделсе, тіпті ұжымдық мүдделердегі іс-әрекеттердің практикалық пайдасы жеке мүддеге ұмтылудың пайдасынан жоғары болса да.
Әлеуметтік инженерия. Қаскүнем алдау арқылы өзінің мақсатын ақпаратты ашуға немесе басқа әрекет жасауға мәжбүрлейтін тактика.
Әлеуметтік инженерия арқылы алаяқтық. Жәбірленушіні қаскүнемге жеке ақпаратты және/немесе қаражатты ашуға немесе басқаша ұсынуға көндіру.
Бағдарламалар мен файлдарды талдау. Компьютерлік жүйеде қосымшалар мен файлдарды зерттеу үшін қылмыскердің киберқылмысқа қатысты алдын-ала, ниеті мен мүмкіндіктерін анықтау үшін жасалатын талдау түрі.
Балалар грумингі. Балаларды азғыру немесе жыныстық мақсаттары бар балаларға тиісу.
Балаларға жыныстық зорлық-зомбылық тапсырыс. Балаға жыныстық зорлық-зомбылық көрсетуді көрермендер баламен, жыныстық зорлаушымен және/немесе балаға жыныстық зорлық-зомбылықты ұйымдастырушымен қарым-қатынас жасау және баланың нақты физикалық әрекеттерін және/немесе жыныстық әрекеттерін және/немесе балаға қатысты әрекеттерін талап ету арқылы зорлық-зомбылыққа белсенді қатыса алады.
Балаларға жыныстық зорлық-зомбылық тікелей көрсетілімі. Алыс жерлердегі (көбінесе) көрермендерге балаларға сексуалдық зорлық-зомбылық көріністерін нақты уақыт режимінде көрсету.
Балаларға сексуалдық зорлық-зомбылық бейнеленген материалдар. Балаларға сексуалдық зорлық-зомбылықтың және/немесе балаларды қолданатын басқа жыныстық әрекеттердің бейнесі.
Басқа адамдардың сөздерінен айғақтар. Соттан тыс мәлімдемелер.
Басып кіруді анықтау жүйесі. Киберқауіпсіздікті қамтамасыз ету жүйесі кибершабуылдардың жүйелерге, желілерге, деректерге, қызметтерге және тиісті ресурстарға рұқсатсыз қол жеткізуін және рұқсатсыз пайдалануын анықтауға мүмкіндік береді.
Бейтараптандыру техникасы. Заңсыз әрекетке қатысуға байланысты жағымсыз эмоцияларды жеңу немесе азайту үшін қолданылатын әдістер.
Белсенді сандық із. Пайдаланушы ұсынған деректермен жасалады.
Бесінші сала. Киберкеңістікті соғыс жүргізудің тағы бір саласы ретінде сипаттау үшін қолданылатын термин.
Бизнестің үздіксіздігі жоспары. Орындалуы керек нұсқаулар мен киберқауіпсіздік оқиғасы туындаған жағдайда жасалатын әрекеттер туралы жоспар. Сондай-ақ, *төтенше жағдайларды реттеу жөніндегі іс-қимыл жоспары* деген атпен белгілі.
Білімді басқару. Білімге қажеттілікті анықтау және бағалау және білім ресурстарын пайдалану.
Бот-желісі. Бот-кодты жұқтырған компьютерлер желісі.

Бот желісінің «иесі». Жұқтырған сандық құрылғыларды басқаратын адам.
Бот-код. Бұл құрылғыларды қашықтан басқаруға және оларды киберқылмыстар жасау, ақпаратты ұрлау және/немесе кибершабуылдарға қатысу үшін пайдалануға мүмкіндік беретін зиянды бағдарламалық жасақтама түрі.
Бөлінбеген кеңістік. Пайдалану үшін қол жетімді кеңістік, өйткені одан алынған ақпарат немесе ешқашан пайдаланылмаған кеңістік.
Бұрмаланбаған бейнені жасау. Сандық құрылғы мазмұнының көшірмесін жасау.
Біртекті деректер массивтерін оқшаулау. Контент идентификаторлары негізінде іздеу.
Бэкдор. Жүйелерге рұқсатсыз қол жеткізу үшін пайдаланылатын құпия портал.
Вирус. Тарату үшін пайдаланушының қатысуы талап етілетін зиянды бағдарлама.
Вирус-бопсалаушы. Жүйелерді, файлдарды және/немесе пайдаланушылардың деректерін кепілге алуға және бақылауды пайдаланушыларға төлемді төлегеннен кейін ғана қайтаруға арналған зиянды бағдарлама.
Вишинг. Телефон байланысын пайдалану арқылы фишинг.
Географиялық нұсқаулар. Өнім осы аймақта жалпы қабылданған стандартты тәжірибеге сәйкес жасалған жағдайларды қоспағанда, қолдануға болмайтын өнім сапасының белгісі және оны жасау орнының беделі. *Шығу орындарының атаулары* ретінде де белгілі.
Дамыған тұрақты қауіптер. Объектіге үнемі мақсатты шабуыл жасайтын жеке тұлғалар және/немесе адамдар тобы.
Даркнет. Дүниежүзілік ғаламтордың бір бөлігі қол жетімділігі қиын веб-сайттарымен және заңсыз әрекеттер мен заңсыз тауарлар мен қызметтерді жүзеге асыратын жасырын веб-сайттарымен танымал және оларға тек мамандандырылған бағдарламалық жасақтама арқылы қол жеткізуге болады. *Қараңғы тор* деген атпен де белгілі.
Дәйексіз ақпарат. Жалған немесе дәл емес ақпарат.
Дәлелдемелерді қорғау жүйесі. Көптеген соттарда сандық дәлелдемелердің жарамдылығын қамтамасыз ету үшін маңызды болып табылатын дәлелдемелерді, олардың жай-күйін, жинау, сақтау, қол жеткізу және беру процестерін, сондай-ақ қол жеткізу мен берудің себептерін егжей-тегжейлі есепке алу.
Деректер. Сандық құрылғы жүйесінде өңделетін ақпараттың кез-келген көрінісі. *Компьютерлік деректер* немесе *компьютерлік ақпарат* деп те аталады.
Деректерді жасыру әдісін талдау. Жүйеде жасырын деректерді іздейтін талдау түрі.
Деректерді қорғау. Жеке ақпаратты қорғау және оны жинау, сақтау, талдау, пайдалану және алмасу процестерін реттеу.
Деректердің сақталуын қамтамасыз ету. Құқық қорғау органдарының

қызметтерді жеткізушілерге деректерді жойылғанға немесе қандай да бір түрде өзгертілгенге дейін сақтау мақсатында өтініш жіберуі.

Диссоциативті анонимділік. Интернеттегі адамдардың мінез-құлқының интернет пен сандық технологияларды пайдалану кезінде қамтамасыз етілетін анонимділікке байланысты нақты өмірдегі әдеттегі мінез-құлық контекстінен түсуі.

Диссоциативті қиял. Киберкеңістікті күнделікті өзара іс-қимыл ережелері, мінез-құлық кодекстері, әлеуметтік нормалар және/немесе адамға күнделікті өзара іс-қимыл ережелеріне, мінез-құлық кодекстеріне, әлеуметтік нормаларға және/немесе нақты әлемде қолданылатын заңдарға қайшы әрекет етуге тыйым салатын заңдар қолданылмайтын форум ретінде қабылдау.

Догпайлинг. Интернеттегі бір кеңістіктегі пайдаланушылар құрбандарды ұятсыз, қорлайтын және қорқытатын хабарламалармен толтырып, оларды өшіруге, сөздерін қайтарып алуға және/немесе кешірім сұрауға немесе платформадан кетуге мәжбүрлейтін тактика.

Доксинг. Интернетте зиян келтіру мақсатында жеке ақпаратты жариялау.

Домен атауы. Интернет-шолғышта (немесе веб-шолғышта) IP-мекенжайын ұсыну.

Домендік атаулар жүйесі. Домендік атауларды IP-мекенжайына түрлендіру арқылы Интернетке қол жетімділікті қамтамасыз етеді.

Егемендік. Мемлекеттің өз аумағында өкілеттіктерді жүзеге асыру құқығы.

«Екпе» теориясы. Бұл теорияда адамдарды басқа адамдар қабылдаған сенім әрекеттеріне иммунитетті ету тәсілі оларды осы әрекеттерге итермелеу және оларға осы әрекеттерге қарсы тұру үшін қажетті құралдарды беру болып табылады.

Ең жақсы дәлел. Шынайы дәлелдеме немесе шынайы дәлелдің нақты көшірмесі.

Жазу блокаторы. Көшіру процесінде деректердің өзгеруін болдырмауға арналған.

Жалған жаңалықтар. Нақты жаңалықтар түрінде таратылатын насихат және жалған ақпарат.

Жанама дәлелдемелер. Фактінің ақиқаты туралы қорытынды жасауға мүмкіндік беретін дәлелдемелер.

Желіаралық экран. Рұқсат етілмеген трафикті блоктау арқылы ақпараттың еркін ағынын шектейтін қорғаныс жүйесі.

Жеке автономия. Таңдау жасау және мәжбүрлеусіз өз таңдауымен әрекет ету мүмкіндігі.

Жеке деректерді пайдалануға байланысты қылмыстар. Қылмыскер өзін басқа адамға заңсыз түрде көрсетеді және/немесе жәбірленушінің сәйкестендіру деректерін заңсыз иемденеді және/немесе осы сәйкестендіру және / немесе жеке деректерді заңсыз мақсаттарда пайдаланады.

Жеке өмірге қол сұғылмаушылық. Жалғыз қалу құқығы; байқаудан бостандық құқығы; өз ойларын, сенімдерін, жеке басы мен мінез-құлқын құпияда сақтау қабілеті; және жеке ақпарат қашан, неге, қайда, қалай және кімге ашылатынын, қандай жеке ақпарат ашылатынын және қандай көлемде

ашылатынын таңдау және бақылау құқығы.

Жыныстық пайдалану мақсатында балаларды сату. Балаларды жалдауды, балаларды коммерциялық жыныстық қанауға әкелетін, оның себебі болып табылатын, оны қолдайтын және/немесе оған басқаша ықпал ететін әрекет.

Заттар интернеті. Нысандарды, адамдарды, жануарлар мен өсімдіктерді бақылауға, сондай-ақ олар туралы ақпаратты жинауға, талдауға, сақтауға және таратуға мүмкіндік беретін Интернетке кіретін өзара байланысты және өзара әрекеттесетін құрылғылар желісі.

Зиянды бағдарлама. Зиянды бағдарламалық қамтамасыз ету.

Зияткерлік меншік. Шығармашылық өнімдер, мысалы, шығармалар, инновациялар, туындылар, идеялардың түпнұсқа көрінісі және құпия әдістер, адамдардың заңға сәйкес құқығы бар бизнес жүргізу процестері.

Интернет-қызмет жеткізушілер. Компьютерлік жүйеге немесе басқа сандық құрылғы жүйесіне Интернет қызметін ұсынатын адамдар.

Интернет протоколының мекен-жайы. Интернетке қосылған сандық құрылғыға желіге қосылу үшін Интернет-қызмет жеткізуші тағайындайтын бірегей идентификатор. *IP-мекенжайы* ретінде де белгілі.

Интернет троллдары. Интернетте араздық пен наразылық туғызуға бағытталған дөрекі, агрессивті және қорлайтын сөздерді әдейі жариялайтын адамдар.

Интернетте балаларды жыныстық пайдалану. Ақпараттық-коммуникациялық технологияларды балаларды жыныстық пайдалану құралы ретінде пайдалану, егер балаларға сексуалдық зорлық-зомбылық және/немесе балаларды пайдаланатын басқа жыныстық қатынас әрекеттері кез-келген қажеттіліктерді қанағаттандыру үшін алмасуды қажет етсе.

Интернетті басқару. Интернетті пайдалануды және оны дамытуды реттеу үшін әртүрлі субъектілердің интернет жұмысының принциптерін, ережелерін, рәсімдерін әзірлеу және қолдану.

Интернеттегі балаларға жыныстық зорлық-зомбылық. Ақпараттық-коммуникациялық технологияларды балаларға сексуалдық зорлық-зомбылық жасау құралы ретінде пайдалану.

Интернеттің ену деңгейі. Интернетті пайдаланатын белгілі бір аймақтағы халықтың үлесі.

Кері бағытта қадағалау. Киберқылмыстың көзін анықтау үшін заңсыз әрекеттерді бақылау процесі. *Кері бақылау* ретінде де белгілі.

Кері бақылау. Киберқылмыстың көзін анықтау үшін заңсыз әрекеттерді бақылау процесі. Сондай-ақ, *кері бағытта бақылау* ретінде белгілі.

Кибер жала жабу. Ересек адам немесе бала туралы оның әлеуметтік жағдайына, тұлғааралық қатынастарына және/немесе беделіне нұқсан келтіру үшін жалған ақпаратты немесе сыбыстарды Интернетте басқа жолмен орналастыру немесе тарату.

Кибер-прокси. Мемлекетке әдейі бағытталған кибершабуылға тәуелді қылмыс жасауға тікелей немесе жанама ықпал ететін делдалдар.

Кибер соғыс. Маңызды инфрақұрылым жүйелеріне қауіп төндіретін және бұзатын және қарулы шабуылға теңестірілуі мүмкін киберкеңістіктегі

әрекеттер.

Кибералымсақтық. АКТ-ны адамды (немесе тұлғаларды) намыстандару, тітіркендіру, шабуылдау, қорқыту, ренжіту және/немесе қорлау үшін қасақана әрекеттер үшін пайдалану.

Киберқауіпсіздік. Жүйелердің, желілердің, қызметтердің және осы қатерлерге қатысты деректердің қатерлері мен осалдықтарын анықтауға; осалдықтарды пайдаланудың алдын алуға; материалдандырылған қатерлерден келтірілген зиянды жеңілдетуге; адамдарды, мүлікті және ақпараттық-коммуникациялық технологияларды қорғауға арналған стратегиялар, тетіктер мен шаралар жиынтығы.

Киберқауіпсіздік саласындағы істердің жай-күйі (әлеуеті). Елдің, ұйымның немесе компанияның киберқауіпсіздікті қамтамасыз ету мүмкіндіктерін сипаттау үшін қолданылатын термин.

Киберқудалау. Кезкелген адамды жүйелі түрде алымсақтық, мазалау, қоқан-лоққы көрсету, қауіп-қатер төндіру, қорқыту және/немесе сөзбен балағаттау мақсатында бірнеше мәрте қайталанбалы әрекеттерді жасау үшін ақпараттық-коммуникациялық технологияларды пайдалану.

Кибертәуелді қылмыс. Интернет пен сандық технологиясыз мүмкін емес киберқылмыс.

Киберкеңістік. Сандық құрылғылардың көмегімен онлайн қызмет жүзеге асырылатын Интернетке шығуы бар қол жетімді орта.

Киберқорлау. Балалардың АКТ-ны басқа балаларды ауыртпалық акелу, намыстандару, ренжіту, құштарлық ету, қорқыту, қудалау, қатыгездікпен қарау немесе басқа жолмен балаларға арналған шабуылдау үшін пайдалануы.

Кибертерроризм. Қандай да бір зиян келтіру және халықтың мақсатты тобына қорқыныш тудыру үшін аса маңызды инфрақұрылым объектілеріне қарсы жасалған кибертәуелді қылмыстар.

Кибертехнология арқылы жасалған қылмыс. Интернет және цифрлық технологиялар арқылы жасалатын киберқылмыс.

Кибертыңшылық. Мемлекеттік құрылымдардың, мемлекет қаржыландыратын немесе бақылайтын топтардың немесе Үкімет атынан әрекет ететін басқа адамдардың ақпараттық-коммуникациялық технологияларды жүйелер мен деректерге рұқсатсыз қол жеткізу және өз елінің ұлттық қауіпсіздігін, экономикалық бәсекеге қабілеттілігін және/немесе әскери қуатын арттыру үшін өз мақсаттары туралы барлау жинау үшін пайдалануы.

Коммерциялық жыныстық қанау балалар. Кез-келген ақшалай немесе ақшалай емес сыйақының орнына балаларға жыныстық зорлық-зомбылықпен байланысты кейбір әрекеттер мен қылмыстарды сипаттау үшін қолданылатын термин.

Компьютерлік қауіпсіздік саласындағы оқиғаларға ден қою тобы. Компьютерлік қауіпсіздікке қатысты оқиғалар болған жағдайда қолдау көрсететін топ. Сондай-ақ, *компьютерлік қорғаудың бұзылуына ден қою тобы* ретінде белгілі.

Компьютерлік қорғаудың бұзылуына ден қою тобы. Компьютерлік

қауіпсіздікке қатысты оқиғалар болған жағдайда қолдау көрсететін топ. Сонымен қатар *компьютерлік қауіпсіздік саласындағы оқиғаларға ден қою тобы* деген атпен белгілі.

Компьютерлік ақпарат. Сандық құрылғы жүйесінде өңделетін ақпараттың кез-келген көрінісі. *Компьютерлік деректер* немесе *деректер* деп те аталады.

Компьютерлік деректер. Сандық құрылғы жүйесінде өңделетін ақпараттың кез-келген көрінісі. Сондай-ақ *компьютерлік ақпарат* немесе *деректер* деп те белгілі.

Компьютерлік желі. Деректерді бір-біріне жіберетін екі немесе одан да көп компьютерлер.

Компьютерлік жүйе. Деректерді өңдеуді және басқа функцияларды орындайтын автономды немесе желілік құрылғы.

Контентке қатысы жоқ деректер. Мазмұны туралы деректер. Сондай-ақ *метадеректер* деп аталады.

Контентке қатысты деректер. Жазбаша хабарламалардағы сөздер немесе айтылған сөздер.

Көрінетін Интернет. Қол жетімді және көпшілікке пайдалануға дайын және дәстүрлі іздеу жүйелерін қолдана отырып табуға болатын индекстелген сайттар. Сондай-ақ, *көрінетін желі* немесе *көрінетін тор* деген атпен белгілі.

Көрінетін тор. Қол жетімді және көпшілікке пайдалануға дайын және дәстүрлі іздеу жүйелерін қолдана отырып табуға болатын индекстелген сайттар. Сондай-ақ, *көрінетін Интернет* немесе *көрінетін тор* деген атпен белгілі.

Криминалистика тұрғысынан маңыздылығы. Сот сараптамасы үшін деректердің маңыздылығы сандық дәлелдемелердің: қылмыскер мен қылмыстың нысаны және/немесе орны арасындағы байланысты орнатуға немесе жоққа шығаруға; қылмыскердің, жәбірленушінің және/немесе куәгердің айғақтарын растауға немесе жоққа шығаруға; киберқылмысты орындаушының (орындаушылардың) жеке басын анықтауға; тергеу нұсқаларын ұсынуға мүмкіндік беру; қылмыскер қолданған әрекет әдісі туралы ақпарат алуды қамтамасыз ету; және қылмыстың шынымен болғанын көрсету.

Криптовалюта. Жетілдірілген шифрлау стандартын қолдана отырып қорғалған сандық валютаның бір түрі.

Криптобопсалаушы. Пайдаланушының сандық құрылғысын жұқтыратын зиянды бағдарлама пайдаланушының құжаттарын шифрлайды және егер жәбірленуші төлем жасамаса, файлдар мен деректерді жою қаупін тудырады.

Криптоджекинг. Жұқтырған компьютерлердің есептеу қуаты жұқтырған сандық құрылғыларды басқаратын адамның (адамдардың) қаржылық пайдасын алу үшін криптовалюта өндіру үшін пайдаланылатын әдіс.

Криптомаркет. Сайт пайдаланушыларын қорғау үшін криптографияны қолданатын Веб-сайт.

Күнделікті қызмет теориясы. Қылмыс екі элемент болған кезде жасалады - *дәлелді қылмыскер* және *қолайлы мақсат*, ал бір элемент болмаған кезде - *әрекетқабілетті қорғаушы*.

Күтілетін пайдалылық теориясы. Бұл әрекеттерден күтілетін пайдалылық басқа әрекеттерге қатысудың күтілетін пайдасынан асып түсетін кезде адамдар қандай-да бір іс-әрекетке қатысады деген теория.

Кілт сөздер бойынша іздеу. Тергеуші ұсынған терминдер негізінде іздеу.

Кэтфишинг. Уақытты, ақшаны және/немесе басқа заттарды алаяқтық жолмен алып кою үшін жалған немесе жаңылыстыратын махаббат пен достық уәделерін беру.

Қалпына келтіру. Оқыс оқиға кезінде қол жетімсіз, бұзылған, бүлінген және/немесе бұзылған жүйелердің, желілердің, қызметтер мен деректердің тұрақтылығын күшейту және қалпына келтіру жөніндегі шараларды айқындау, әзірлеу және түпкілікті іске асыру.

Қараңғы тор. Дүниежүзілік ғаламтордың бір бөлігі қол жетімділігі қиын веб-сайттарымен және заңсыз әрекеттер мен заңсыз тауарлар мен қызметтерді жүзеге асыратын жасырын веб-сайттарымен танымал және оларға тек мамандандырылған бағдарламалық жасақтама арқылы қол жеткізуге болады. *Даркнет* деген атпен де белгілі.

«Қатыгез күш» әдісімен шабуыл. Пайдаланушының тіркелгі деректерін болжау үшін сценарийді немесе роботты пайдалану.

Қатты диск. Компьютердің ішкі тұрақты жады.

Қаупі. Зиян келтіруі мүмкін жағдай.

«Қызмет көрсетуден бас тарту» түріндегі шабуыл. Веб-сайтқа және/немесе жүйені пайдалануға заңды трафиктің кіруіне жол бермеу үшін серверлерді сұраулармен жүктеу арқылы жүйелерге кедергі келтіретін киберқылмыс. *DoS-шабуыл* деген атпен де белгілі.

«Қызмет көрсетуден бас тарту» түріндегі таратылған шабуыл. Заңды пайдаланушылардың кіруіне кедергі жасау үшін серверлерді шамадан тыс жүктеу мақсатында үйлестірілген шабуыл жасау үшін бірнеше компьютерлер мен басқа да сандық технологияларды пайдалану. *DDoS шабуылы* деп те аталады.

Қылмыстылықтың ситуациялық алдын алу. Қылмыстардың алдын алу және оларды жасау мүмкіндіктерін азайту үшін қолданылатын шаралар.

Қылмысты қайта құру. Қылмыс үшін *кім* жауапты екенін, *не* болғанын, *қай жерде* болғанын, *қашан* болғанын және деректерді анықтау, сәйкестендіру және байланыстыру арқылы *қалай* дамығанын анықтау үшін жүргізілетін процесс. Сондай-ақ, *оқиғаларды қайта құру* деген атпен белгілі.

Қол жетімділік. Деректер, қызметтер және жүйелер сұраныс бойынша қол жетімді болған кезде.

Қол жеткізуді басқару құралдары. Артықшылықтарды белгілейтін шаралар рұқсат етілген қол жетімділікті анықтайды және рұқсат етілмеген қол жетімділіктің алдын алады.

«Құрт». Пайдаланушының қатысуынсыз таратылатын автономды зиянды бағдарлама.

Қылмыстылықты ығыстыру. Бір объектіге бағытталған қылмыс қолданыстағы қауіпсіздік шараларына байланысты басқа объектіге қатысты жасалған кезде.

Құпиялылық. Жүйелер, желілер және деректер қорғалған және оларға тек авторизация жасаған пайдаланушылар қол жеткізе алады.
Қызметтің негізгі көрсеткіштері. Ұлттық киберқауіпсіздік стратегиясының стратегиялық міндеттерін іске асыруда прогресті бағалау үшін қолданылатын шаралар.
Логикалық үзінді. Файлдық жүйеге қатысты орналасқан жерден дәлелдерді іздеу және алу.
Мақсатты фишинг. Алушыны қосымшаны ашуға немесе сілтемені басуға мәжбүр ету үшін вирус жұққан тіркемелермен немесе сілтемелермен электрондық хаттарды жіберу.
Материалдық құқық. Мемлекет юрисдикцияны жүзеге асыратын адамдардың мінез-құлқы мен міндеттерін реттейтін құқықтық нормалар.
Меншік және меншікті талдау. Компьютерлік жүйеде файлдарды жасаған, оларға қол жеткізген және/немесе оларды өзгерткен адамды анықтау үшін қолданылатын талдау түрі.
Менялалар. Жартылай автоматты криптовалюта биржалары.
Метадеректер. Мазмұны туралы деректер. Сондай-ақ, *контентке қатысы жоқ деректер* ретінде белгілі.
Микро-жуу. Ақшаны жылыстату нысаны, оның көмегімен қылмыскерлер көптеген ұсақ транзакцияларды жүзеге асыру арқылы қомақты ақшаны жылыстатады.
Морфинг. Жәбірленушінің беті немесе басы басқа адамдардың денелеріне салу арқылы диффамация, порнография және/немесе жыныстық зорлық жасау мақсатында қолданылатын процесс.
Нөлдік күннің осалдығы. Олар анықталғаннан кейін пайдаланылатын бұрын белгісіз осалдықтар.
Ойластырылған әрекеттер негізінде деректерді қорғау. Жүйелер мен технологиялардың конструкциясына салынған құпиялылықты қамтамасыз ету жөніндегі шаралар. Сондай-ақ, *ойластырылған әрекеттерге негізделген құпиялылық* деген атпен белгілі.
Ойластырылған әрекеттер негізінде құпиялылық. Жүйелер мен технологиялардың конструкциясына салынған құпиялылықты қамтамасыз ету жөніндегі шаралар. Сондай-ақ, *ойластырылған әрекеттер негізінде деректерді қорғау* деген атпен белгілі.
Оқиғаларды анықтау. Активтерді белсенді мониторингтеу және аномалды белсенділікті анықтау арқылы қауіптерді белгілеу процесі.
Оқиғаларды қайта құру. Оқиғаға *кім* жауапты екенін, *не* болғанын, *қай жерде* болғанын, *қашан* болғанын және деректерді анықтау, сәйкестендіру және байланыстыру арқылы қалай дамығанын анықтау үшін жүргізілетін процесс. Сондай-ақ, *қылмысты қайта құру* деген атпен белгілі.
«Оққа төзімді» хостинг. Қылмыскерлерге киберқылмыстарды жасау үшін серверлерді пайдалануға, тыйым салынған контентті сақтауға және тыйым салынған контентті құқық қорғау органдарының қол жетімділігінен және/немесе Интернеттен ажыратудан қорғауға мүмкіндік беретін қызмет.
Осалдық. Зиянға ұшырау.

Осалдық туралы ақпаратты жауапты ашу. Жауапты ұйым осалдықты жойғанға дейін осалдық туралы ақпаратты ашпау тәжірибесі.
Осалдықтарды толық ашу. Осы осалдықтар жойылғанға дейін онлайн-форумдарда немесе веб-сайттарда бағдарламалық немесе аппараттық осалдықтар туралы ақпаратты жария ету.
Осалдықтарды үйлесімді түрде ашу. Тиісті мүдделі тараптарға келісілген ақпарат алмасу және осалдықтар туралы ақпаратты ашу практикасы және осындай ашудың теріс салдарын жұмсарту.
Өзара құқықтық көмек туралы шарт. Екі Тараптың ұлттық заңнамасына сәйкес осындай деп саналатын кейбір және/немесе барлық қылмыстарға қатысты тергеу мен сот қудалауындағы ынтымақтастық туралы елдер арасындағы келісім.
Өнеркәсіптік құпиялар. Құпия болып табылатын және компанияның бәсекелестік артықшылықтарын қорғайтын бизнес-процестер мен іскери тәжірибелер туралы құнды ақпарат.
Өнеркәсіптік үлгілер. Тұтынушылар үшін эстетикалық тартымды болу және тауарлар арасындағы тұтынушылардың таңдауына әсер ету мақсатында жасалған үлгілерді қамтитын зияткерлік меншік нысаны. Сондай-ақ, *үлгілерге патенттер* деген атпен белгілі.
Пайдалану ыңғайлылығы. Сандық құрылғыларды қолдануға болатын жеңілдік.
Пассивті сандық із. Интернетті және сандық технологияларды пайдаланатын адамдар алатын және байқаусызда қалдыратын мәліметтер.
Патент. Әдетте қандай да бір іс-әрекетті орындаудың жаңа тәсілін білдіретін немесе қандай да бір міндеттің жаңа техникалық шешімін ұсынатын бұйым немесе процесс болып табылатын өнертабысқа (инновацияға немесе жасампаздыққа) берілетін айрықша құқық.
Патенттік тролльдер. Бұл адамдар ештеңе жасамайды немесе ойлап таппайды; олар жай патенттерді сатып алады, басқаларға лицензия береді, содан кейін сатып алынған патенттік құқықтарын бұзатын кез-келген адамды, топты немесе ұйымды сотқа береді.
Педофил. Балаға жыныстық құмарлықты сезінетін адам.
Прокси-сервер. Клиент ресурстарды сұрайтын серверге клиентті қосу үшін пайдаланылатын аралық сервер.
Псевдонимизациялау. Жазбадағы сәйкестендіру деректері жасанды идентификаторлармен алмастырылатын процесс.
Растау біржақтылығы. Адамдар жұмыс гипотезасын растайтын нәтижелерді іздейтін және қолдайтын және жұмыс гипотезасына қайшы келетін нәтижелерді қабылдамайтын процесс.
Реляциялық талдау. Оқиғаларға қатысушыларды, олардың іс-әрекеттерін, сондай-ақ олардың арасындағы байланыстар мен қатынастарды анықтау.
Сайлаудағы алаяқтық. Сайлау нәтижелеріне әсер ету үшін заңсыз әдістерді қолдану.
Сандық антикриминалистика. Киберқылмыскерлердің тергеуін шатастыру үшін қолданылатын құралдар мен әдістер сандық сот сараптамасын жүргізуді

қиындатады. Сондай-ақ, *қылмысқа қарсы күрес* деген атпен белгілі.

Сандық дәлелдемелер. Ақпараттық-коммуникациялық технологиялар құрылғыларынан алынған деректер. *Электрондық дәлелдемелер* деп те аталады.

Сандық із. АКТ пайдаланушыларынан олар туралы ақпаратты, оның ішінде жас, жыныстық, нәсілдік және этникалық, азаматтық, жыныстық бағдар, ойлар, қалаулар, әдеттер, хобби, медициналық тарих және денсаулық мәселелері, психологиялық бұзылулар, жұмыспен қамту мәртебесі, қандай да бір қоғамдастыққа жататындығы, қарым-қатынас, геолокация, күн тәртібі және басқа да белсенділік туралы ақпаратты ашуы мүмкін деректер.

Сандық криминалистика. Құқық мәселелерін ақпараттық-коммуникациялық технологиялар мен цифрлық құрылғыларға қолданатын криминалистика саласы.

Сандық қарақшылық. Авторлық құқықпен қорғалатын туындыларды тарату құқығын алмай, үшінші тараптың веб-сайтынан фильмдерді заңсыз жүктеу.

Сандық сот сараптамасы процесі. Сандық дәлелдемелерді іздеу, алу, сақтап қалу және сақтау; сандық дәлелдемелерді сипаттау, түсіндіру және олардың шығу тегі мен маңыздылығын анықтау; дәлелдемелерді және олардың нанымдылығын, анықтығы мен іске қатыстылығын талдау; және іске қатысы бар дәлелдемелерді ұсыну болып табылады.

Секстинг. Жыныстық сипаттағы жеке ашық суреттер жіберу.

Сексторшн. Қылмыскер құрбанның фотосуреттерін немесе бейнежазбаларын, егер оның талаптары орындалмаса, ашық сексуалдық сипаттағы таратамын деп қорқытқан кезде жасалатын кибершабуылдың бір түрі.

Скрипт. Компьютерлік бағдарлама.

Смишинг. Мәтіндік хабарламаларды пайдалану арқылы фишинг. *SMS-фишинг* ретінде де белгілі.

Сот тапсырмалары. Дәлелдемелерді ұсыну туралы өтінішпен ұлттық соттардың шет мемлекеттің органдарына жазбаша сұрау салулары.

Солипсиялық интроекция. Пайдаланушылардың басқа адамдарға қатысты қабылдауы және олармен нақты байланыс болмаған кезде олардың сипаттамалары, соның ішінде нақты ақпаратқа емес, қиялға негізделген қатынастар нәтижесінде пайда болған адамдардың ойдан шығарылған бейнесі.

Спам. Сұралмаған электрондық хаттарды жіберу.

Стандартты операциялық процедуралар. Киберқылмыстарды тергеу және ақпараттық-коммуникациялық технологиялар құрылғыларындағы сандық дәлелдемелерді қарау кезінде сақталуы керек әдістер мен әрекеттер тізбегін сипаттайтын құжаттар.

Стеганография. Хабарлама мазмұны жасырылған және көрінбейтін болған кезде құпия деректерді жасыру.

Суару алаңына шабуыл. Зиянды бағдарламаларды құрбандар жиі кіретін веб-сайттарға орналастыру, олардың жүйелерін жұқтыру және оларға рұқсатсыз қол жеткізу.

Суреттерді пайдалана отырып жыныстық қорлау. Қылмыскерлер құрбандардың келісімінсіз олардың интимдік фотосуреттерін және/немесе бейнежазбаларын әдейі жасайтын, тарататын немесе таратамын деп қорқытатын сексуалдық зорлық-зомбылық түрі. Мұндай әрекет жәбірленушіге зиян келтіруі және / немесе қылмыскерге қандай да бір жолмен пайда әкелуі мүмкін (мысалы, ақшалай пайда, жыныстық қанағаттану, әлеуметтік мәртебені көтеру және т.б.).

Таза бейтараптық. Дереккөзге қарамастан, барлық деректерге бірдей қатынасты талап ететін принцип.

Тауар белгілері. Кейбір көздердің тауарларын немесе қызметтерін басқаларынан ажыратуға мүмкіндік беретін идентификаторлар.

Тауар белгілерін жалған жасау. Тауар таңбасы иесінің тауары немесе қызметі болып табылмайтын тауарды немесе қызметті таңбалау үшін тауар таңбасын әдейі рұқсатсыз пайдалану.

Тәуекелі. Қауіптің әсері және оның пайда болу ықтималдығы.

Тәуекелдерді өңдеу. Тәуекелдерге ден қою шаралары.

Тәуекелді бағалау. Қауіптің ықтималдығын, оның салдарын және активтің осы қауіпке ұшырауын бағалау.

Тежеу. Жаза арқылы заңсыз қызметке кедергі жасау.

Терең желі. Веб-сайттар іздеу жүйелерімен индекстелмейтін және қол жетімді емес және/немесе көпшілікке пайдалануға дайын емес бүкіләлемдік ғаламтордың бөлігі.

Технологиялық процестерді басқару жүйелері. Аса маңызды инфрақұрылым объектілеріндегі өндірістік процестерді басқару жүйелері.

Тиісті әрекетті қылмыс деп өзара тану. Халықаралық шарттардағы ынтымақтастық елдерінде іс-әрекеттерді заңсыз деп санауды талап ететін тармақ.

Тікелей дәлелдеме. Фактіні анықтайтын дәлелдеме.

Тіркелгі деректерін басқару. Пайдаланушылардың сәйкестендіру деректерін аутентификациялау, тиісті артықшылықтарды сәйкестендіру және осы артықшылықтар негізінде пайдаланушыларға қол жетімділікті қамтамасыз ету процесі.

Трафик туралы мәліметтер. Компьютерлік желі арқылы берілетін деректер.

Трояндық ат. Пайдаланушыны тыңшылық, ұрлық және/немесе зиян келтіру мақсатында пайдаланушы жүйесін жұқтыратын бағдарламаны жүктеуге алдау үшін заңды бағдарламалық жасақтама ретінде жасырылған зиянды бағдарлама.

Тұрақтылығы. Ақауларға төтеп беру, өзгеретін жағдайларға бейімделу және АКТ оқиғаларынан қалпына келтіру, сонымен қатар жүйелердің, желілердің, қызметтер мен деректердің құпиялығын, тұтастығы мен қол жетімділігін қорғау мүмкіндігі.

Тұтастық. Деректер дәл және сенімді және өзгертілмеген.

Уақыт шеңберін талдау. Оқиғаға әкелген уақыт (күн және уақыт) белгілерін қолдана отырып, уақыт шкаласын немесе әрекеттердің уақыт тізбегін құру немесе пайдаланушы белгілі бір әрекетті жасаған уақыт пен күнді белгілеу

мақсатында орындалатын талдау.
Уақытша талдау. Оқиғалардың уақыты мен реттілігін белгілеу.
Уэйлинг. Қылмыскерлер компанияның аға басшыларын, заңгерлерді, бухгалтерлерді және басқа да басқарушы және жауапты лауазымдарды қызметкерлерді алдау арқылы оларға ақша жіберуге мәжбүрлейтін әдіс.
Ұйымдасқан қылмыс. Тұрақты жұмыс істейтін қылмыстық кәсіпорын, үлкен қоғамдық сұраныс бар салаларда заңсыз қызмет арқылы пайда табу үшін ұтымды жұмыс істейді.
Ұйымдастырылған киберқылмыскерлер. Үш немесе одан да көп адамнан тұратын, белгілі бір уақыт кезеңі ішінде жұмыс істейтін және тікелей немесе жанама түрде қаржылық немесе өзге де материалдық пайда алу үшін Интернет желісінде толық немесе ішінара әрекет ететін Біріккен Ұлттар Ұйымының 2000 жылғы Трансұлттық ұйымдасқан қылмыстылыққа қарсы Конвенциясына сәйкес бір немесе бірнеше ауыр қылмыстар немесе осындай деп танылған қылмыстар жасау мақсатында келісілген құрылымдық ресімделген топ.
Ұйымдастырылған киберқылмыстылық. Интернетте үлкен сұранысқа ие қызметтер саласындағы заңсыз әрекеттер арқылы пайда табу үшін ұтымды жұмыс істейтін тұрақты қылмыстық кәсіпорынды сипаттау үшін қолданылатын термин.
Үлгілерге патенттер. Тұтынушылар үшін эстетикалық тартымды болу және тауарлар арасындағы тұтынушылардың таңдауына әсер ету мақсатында жасалған үлгілерді қамтитын зияткерлік меншік нысаны. Сондай-ақ, *өнеркәсіптік үлгілер* атты белгілі.
Үлкен деректер. Бірлестіктерді, заңдылықтар мен тенденцияларды анықтау үшін біріктіруге және талдауға болатын үлкен көлемдегі құрылымдалған және құрылымданбаған мәліметтер.
Фарминг. Пайдаланушыларды кіру деректерін енгізуге алдау үшін жалған, қайталанатын веб-сайт құру.
Физикалық шығару. Дәлелдер сақталатын сандық құрылғыдағы осындай жерден дәлелдемелерді іздеу және алу.
Фишинг. Веб-сайтқа сілтемесі бар электрондық хаттарды жіберу, оны басқан кезде пайдаланушылар зиянды бағдарламаны сандық құрылғыларына жүктей алады немесе пайдаланушылардың тіркелгі деректерін ұрлау үшін құрылған зиянды веб-сайтқа қайта жіберілуі мүмкін.
Функционалдық талдау. Оқиғалар кезінде қолданылатын жүйелер мен құрылғылардың өнімділігі мен мүмкіндіктерін бағалау.
Хакерлік шабуыл. Жүйелерге, желілерге және деректерге рұқсатсыз қол жеткізу.
Хэш. Құрылған мән.
Цензура. Заңмен тыйым салынған ақпаратты, көрнекі бейнелерді және жазбаша немесе ауызша хабарламаларды таратуға және үкімет, қоғамдастық немесе топ тарапынан олардың жолын кесуге тыйым салынады, өйткені олар заңсыз және/немесе зиянды, танымал емес, қалаусыз немесе саяси қате деп саналады.
Шифрлау. Шара, ол блоктар қол жеткізу үшінші тұлғалардың ақпарат пен

хабарламаларға пайдаланушылар.
Шпиондық бағдарлама. Вирус жұққан жүйелерді жасырын бақылауға, сондай-ақ шпиондық бағдарламаны жасаушыға және/немесе пайдаланушыға ақпарат жинауға және беруге арналған зиянды бағдарламалық қамтамасыз ету.
Шығу жерлерінің атаулары. Өнім осы аймақта жалпы қабылданған стандартты тәжірибеге сәйкес жасалған жағдайларды қоспағанда, қолдануға болмайтын өнім сапасының белгісі және оны жасау орнының беделі. *Географиялық бағыт* ретінде де белгілі.
Іздеу роботтары. Нақты мақсаттарға жету үшін Интернет беттерін айналып өтуге арналған қосымшалар.
Іс жүргізу құқығы. Материалдық құқық нормаларын қолдану кезінде сақталуы тиіс процестер мен рәсімдерді қамтитын құқықтық нормалар, материалдық құқық нормаларының сақталуын қамтамасыз етуге мүмкіндік беретін ережелер, сондай-ақ қылмыстық сот өндірісіндегі ережелер мен стандарттар.
Электрондық дәлелдемелер. Ақпараттық-коммуникациялық технологиялар құрылғыларынан алынған деректер. *Сандық дәлелдемелер* деп те аталады.
Этика кодексі. Шешім қабылдау процесінде дұрыс және дұрыс емес мінез-құлықты анықтайтын нұсқаулар.
Юрисдикция. Мемлекеттің заңдарды қолдану және заңдарды сақтамағаны үшін жаза тағайындау құқығы мен өкілеттігі.
Data mining. Деректер жиынтығынан ақпарат алу.
DDoS-шабуылы. Заңды пайдаланушылардың кіруіне кедергі жасау үшін серверлерді шамадан тыс жүктеу мақсатында үйлестірілген шабуыл жасау үшін бірнеше компьютерлер мен басқа да цифрлық технологияларды пайдалану. Сондай-ақ, «*қызмет көрсетуден бас тарту» түріндегі таратылған шабуыл* ретінде белгілі.
DoS-шабуылы. Веб-сайтқа және/немесе жүйені пайдалануға заңды трафиктің кіруіне жол бермеу үшін серверлерді сұраулармен жүктеу арқылы жүйелерге кедергі келтіретін киберқылмыс. Сондай-ақ, *«қызмет көрсетуден бас тарту» түріндегі шабуыл* деген атпен белгілі.
Doxware (шифрлаушы-бопсалаушы). Егер файлдар мен деректерді шифрлау үшін код бергені үшін төлем төленбесе, шабуылдаушылар құрбандарға қарсы пайдаланатын криптобопсалаудың бір түрі пайдаланушының деректерін ашамын деп қорқытады.
eDiscovery (электрондық құжаттарды іздеу). Сот процесінде дәлелдеме ретінде пайдалану үшін сандық деректерді іздеу, сәйкестендіру және сақтау процесі.
IP-мекенжайы. Интернетке қосылған сандық құрылғыға желіге қосылу үшін Интернет-провайдер тағайындайтын бірегей идентификатор. *Интернет-протоколының мекен-жайы* ретінде де белгілі.
SMS фишинг. Мәтіндік хабарламаларды пайдалану арқылы фишинг. *Смишинг* ретінде де белгілі.
Stalkerware. Компьютерде, смартфонда немесе интернетке қосылған басқа сандық құрылғыда жұмыс істей алатын тыншылық бағдарламалық

жасақтаманың бір түрі және осы құрылғылардағы пайдаланушының барлық әрекеттері туралы деректерді жинау және беру - жіберілген және алынған электрондық және мәтіндік хабарламалардан бастап түсірілген фотосуреттер мен пернелер туралы ақпаратқа дейін.

Әдебиет:

1. Масалков А.С. Особенности киберпреступлении в России. Издательство: ДМК-Пресс, 2018. - 226 б. https: //www.labirint.ru/books/626293/
2. Клаверов В.Б. Современная киберпреступность. Изд: LAP Lambert Academic Publishing, 2012. - 92 б.
3. Исмагулова А.Т. Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан: монография / А.Т. Исмагулова, А.М. Галиаскарова; Костанайский филиал ФГБОУ ВПО «Челябинский государственный университет». - Костанай: ТОО «New Line Media», 2016. - 160 б.
4. БҰҰ ЕҚБ (2013). Draft Comprehensive Study on Cybercrime.
5. Segal, Mark (2013). How to Train: A Practical Guide for Training and Working with Others.
6. Weiping Chang, Peifang Chung. Knowledge Management in Cybercrime Investigation – A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. PAISI 2014: Intelligence and Security Informatics /https://link.springer.com/book/10.1007/978-3-319-06677-6
7. Berliner, Lucy and Jon R. Conte (1990). The process of victimization: A victims' perspective. Child Abuse & Neglect, Vol. 14(1), 29-40. https://www.sciencedirect.com/science/article/abs/pii/0145213490900788
8. O'Connell, Rachel. (2003). A typology of cyber sexploitation and online grooming practices. Cyberspace Research Unit: University of Central Lancashire. http://image.guardian.co.uk/sysfiles/Society/documents/2003/07/17/Groomingreport.pdf
9. Ospina, Maria, Christa Harstall, and Liz Dennet (2010). Sexual exploitation of children and youth over the internet: A rapid review of the scientific literature. Alberta, Canada: Institute of Health Economics. https://era.library.ualberta.ca/items/d45bd9d4-2c28-4172-8f91 c529e8d96df7/view/7b0416bb-843f-4492-a872 2388ed56bec2/sexual_exploitation_of_children_and_youth_over_the_internet_a_rapid_review_of_the_scientific_literature-20(1).pdf
10. UNODC, 2011 (Всемирный доклад о наркотиках, 2011 г.). https://www.unodc.org/unodc/en/data-and-analysis/WDR-2011.html
11. UNODC, 2012 (Всемирный доклад о наркотиках, 2012 г.) https://www.unodc.org/unodc/en/data-and-analysis/WDR-2012.html
12. UNODC, 2014. https://www.unodc.org/documents/AnnualReport 2014/ Annual_Report_2014_WEB.pdf
13. UNODC, 2015./https://www.unodc.org/wdr2015/
14. Maras 2014. 4th International Conference on Mobile, Adaptable and Rapidly Assembled Structures 11-13 June 2014. Ostend, Belgium. https://www.wessex.ac.uk/conferences/2014/maras-2014
15. Maras 2016. 5th International Conference on Mobile, Adaptable and Rapidly Assembled Structures. 21-23 September 2016 Siena, Italy. https://www.wessex.ac.uk/conferences/2016/maras-2016.

16. Susan W. Brenner, Bert-Jaap Koops. Approaches to Cybercrime Jurisdiction. Journal of High Technology Law, Vol. 4, No. 1, 2004. 46 p. Posted: 25 Aug 2005. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507
17. Policing image-based sexual abuse: stakeholder perspectives. Nicola Henry, Asher Flynn, Anastasia Powell. Pages 565-581/Published online: 20 Sep 2018. https://www.researchgate.net/publication/327794543_Policing_image based_sexual_abuse_stakeholder_perspectives
18. Maras and Miranda, January 2014. Forensic Science in book: Encyclopedia of Law and Economics, pp.1-6. /https://www.researchgate.net/publication/ 304088810_Forensic_Science
19. Cognitive Bias and Blindness: A Global Survey of Forensic Science Examiners Jeff Kukuckaa, Saul M. Kassinb, Patricia A. Zapfb, Itiel E. Dror. Journal of Applied Research in Memory and Cognition. Volume 6, Issue 4, December 2017. /https://www.sciencedirect.com/science/article/ abs/pii/ S2211368117300323?via%3Dihub.
20. A survey of mutual legal assistance involving digital evidence. Joshua I.James, PavelGladyshev. Digital Investigation. Volume 18, September 2016. /https://dl.acm.org/doi/abs/10.1016/j.diin.2016.06.004
21. International Law Enforcement Access to User Data: A Survival Guide and Call for Action. Kate Westmoreland Gail Kent. Home > JOURNALS > CJLT > Vol. 13 (2015) > No.2./ https://digitalcommons.schulichlaw.dal. ca/cjlt/ vol13/iss2/5/
22. Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing. 22 Pages Posted: 25 Jul 2017. David S. Wall./https://papers.ssrn.com/sol3/papers. cfm?abstract_id=3005872
21. International Telecommunication Union, ITU,2012. Understanding cybercrime: phenomena, challenges and legal response /https://www.itu.int/en/ITU D/Statistics/Documents/publications/mis2012 /MIS2012_without_Annex_4.pdf
23. Understanding cybercrime: phenomena, challenges and legal response (pp. 11-33).2014. /https://www.itu.int/en/ITU-D/Cybersecurity/Documents /cybercrime2014.pdf
24. Statcounter, 2016. /http://www.oszone.net/29945/StatCounter_ August_2016_OS_stats
25. Bilge, L. and Dumitras, T. (2012) Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World. Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, 16-18 October 2012, 833-844. /https://doi.org/10.1145/2382196.2382284
26. Henry, Flynn and Powell, 2018 https://doi.org/10.1080/15614263.2018. 1507892
27. Broadhurst et al., 2014. /https://www.researchgate.net/publication/288262190_ Organizations_and_cyber_crime_An_analysis_of_the_nature_of_groups_engaged _in_cyber_crime
28. Broadhurst et al., 2018./https://link.springer.com/article/10.1007/s11306-018-1367-3

29. ITU 2008. https://www.itu.int/council/C2008/index.html
30. ITU 2012. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf
31. ITU 2017. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
32. ITU 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
33. Morgan et al., 2016. /https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-016-2882-7
34. UNSCR 1624 /2005. https://digitallibrary.un.org/record/556538?ln=ru 28. UN-CCPCJ, 2017. /https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/E_CN15_2017_CRP4_e_V1703636.pdf
35. OCCRP, 2016; Reuters, 2016. /https://www.reuters.com/article/europe-moneylaundering-idUKL3N20T2PD
36. Leukfeldt, Kleemans, and Stol, 2017; Leukfeldt, Lavorgna, және Kleemans, 2017, 292-293 бб. /https://journals.sagepub.com/doi/abs/10.1177/0002764217734267
37. Leukfeldt, Lavorgna and Kleemans, 2017. /https://www.cybercrimeworkingroup.com/rutger-leukfeldt
38. Hern, 2017. /https://www-theguardian-com.translate.goog/technology/2017/aug/01/data-browsing-habits-brokers?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc
39. Bilge and Dumitras, 2012. /https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=2024179
40. Henry, Flynn and Powell, 2018, 566 p. /https://www.researchgate.net/publication/327794543_Policing_image-based_sexual_abuse_stakeholder_perspectives
41. Morgan et al., 2016 /https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-016-2882-7
42. NIST, 2018. /https://www.nist.gov/publications/2018-national-institute-standards-and-technology-environmental-scan
43. NIST, 2012. /https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1
44. Hubbard and Seiersen, 2016. /https://www.amazon.com/How-Measure-Anything-Cybersecurity-Risk/dp/1536669741
45. Lehtinen, Russell, Gangemi Sr., 2006. /https://books.google.kz/books/about/Computer_ Security_Basics.html?id=DyrLV0kZEd8C&redir_esc=y
46. Cornish and Clarke, 2003. /https://popcenter.asu.edu/sites/default/files/Responses/ crime_prevention/PDFs/Cornish%26Clarke.pdf
47. Clarke, 2004. /http://www.sciepub.com/reference/203861
48. Reuters, 2017. /https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf
49. Reuters, 2018. https://www.digitalnewsreport.org/survey/2018/
50. Henry, Flynn and Powell, 2017. /https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf

51. Henry, Flynn and Powell, 2018.
/https://www.tandfonline.com/doi/abs/10.1080/15614263.2018.1507892
52. Varese, 2010 / https://www.routledge.com/Organized-Crime/Varese/p/book/9780415460743
53. United States v. Ross William Ulbricht, Criminal Complaint, 2013.
/https://caselaw.findlaw.com/us-2nd-circuit/1862572.html
54. Newman, 2018./https://global.oup.com/academic/product/networks-9780198805090?cc=us&lang=en&#
55. Morgan, 2018. /https://www.jpmorgan.com/solutions/cib/insights/health-care-conference
56. Alvarez, Hall, and Hyde, 2008 /https://www.jstor.org/stable/41403728
57. McGuire and Dowling, 2013. /https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
58. Europol, 2018./ https://www.europol.europa.eu/activities-services/main-reports/europol-in-brief-2018.
59. Read et al., 2016. /https://agupubs.onlinelibrary.wiley.com/doi/10.1002/2016WR019993
60. Conrad, Dorn, and Craiger, 2010. /https://commons.erau.edu/publication/999/
61. Casey, Ferraro, and Nguyen, 2009. /https://www.researchgate.net/publication/26819089_Investigation_Delayed_Is_Justice_Denied_Proposals_for_Expediting_Forensic_Examinations_of_Digital_Evidence.
62. Tcherni et al., 2016./https://www.researchgate.net/publication/305630752_Reasons_for_Gaps_in_Crime_Reporting_The_Case_of_White-Collar_Criminals_Investigated_by_Private_Fraud_Examiners_in_Norway
63. Smeets, 2018. /https://econpapers.repec.org/paper/zbwwtowps/ersd201803.htm
64. Kallender and Hughes, 2017. /https://www.tandfonline.com/doi/abs/10.1080/01402390.2016.1233493
65. Brenner and Koops, 2004. /https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507
66. Frischmann, 2003. /https://lawecommons.luc.edu/luclj/vol35/iss1/8/
67. Kerr, 2003, /https://www.unodc.org/e4j/data/university_uni/the_problem_of_perspective_in_internet_law.html?lng=en
68. Report of the Working Group on Internet Governance. Château de Bossey. June 2005. (WGIG, 2005). /https://www.wgig.org/docs/WGIGREPORT.pdf
69. Enisa 2014. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
70. Enisa 2017./ https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
71. NIST 2012./ https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1
72. NIST 2018. /https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
73. Leukfeldt et al., 2017. /https://www.researchgate.net/publication/320323730_The_Use_of_Online_Crime_Markets_by_Cybercriminal_Networks_A

_View_From_Within
74. Leukfeldt, Lavorgna, and Kleemans, 2017. /https://www.researchgate.net/publication/309960777_Organised_Cybercrime_or_Cybercrime_that_is_Organised_An_Assessment_of_the_Conceptualisation_of_Financial_Cybercrime_as_Organised_Crime
75. Arsovska, 2011./ https://journals.sagepub.com/doi/abs/10.1177/0094306110391764l
76. Whiteman, 2012. /https://www.tandfonline.com/doi/abs/10.1080/14780887.2015.1008913

Баспаға 04.07.2022 ж. Қол қойылды. Формат 60×84 1/16.
Офсеттік қағаз. Шартты баспа парақтары 9,25. Таралымы 500 дана. № 3880 Тапсырыс.
«LEM» баспасы ЖШС-те басылды.
050008, Алматы қ. Әуезов к-сі, 82. Тел./факс 375 51 33.