УДК 343.7

КИБЕРТЕРРОРИЗМ ЖӘНЕ АҚПАРАТТЫҚ СОҒЫС

Мұқаметқазинов Аян Сымбатұлы
ayan.mukamet@gmail.com
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, «Құқықтану» мамандығының 2 – курс магистранты
Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – з.ғ.к., доцент Муратханова М.Б.

Біз компьютерлер мен телекоммуникациялық жүйелері адам мен мемлекеттің тіршілік әрекетінің барлық салаларын қамтитын ақпараттық қоғам дәуірінде өмір сүреміз. Бірақ адамзат өзіне телекоммуникация және жаһандық компьютерлік желілер қызметіне қойып, осы технологияларды теріс пайдалану үшін қандай мүмкіндіктер жасағанын болжаған жоқ. Бүгінде виртуалды кеңістіктегі қылмыскерлердің құрбандары тек адамдар ғана емес, тұтас мемлекеттер де бола алады[1]. Ұйымдасқан қылмыстық топтар менхакерлер немесе хакерлердің ұсақ топтары арасындағы байланыстарды біртіндеп жолға қою үлкен алаңдаушылық тудырады.

«Кибертерроризм» ұғымын анықтау кезінде «терроризм» жалпы ұғымымен бірдей тәсілді қолданса, онда кибертерроризм актілеріне адамдардың мүлкіне немесе өмірі мен денсаулығына қауіп төндіретін немесе инфрақұрылымдық объектілердің жұмыс істеуінің елеулі бұзылуына әкеп соғуы мүмкін және компьютерлік жүйелерге (әсіресе Интернет арқылы) жасалған шабуылдарды ғана жатқызуға болады[2].

Стратегиялық және халықаралық зерттеулер орталығы кибертерроризмді «ұлттық инфрақұрылымның сыни объектілерінің (атап айтқанда, энергетикалық, көліктік, үкіметтік) жұмыс істеуін тоқтату үшін не үкіметті немесе азаматтық халықты мәжбүрлеу немесе қорқыту үшін компьютерлік желілік құралдарды пайдалану» деп айқындайды.

Өз мақсаттарына қол жеткізу үшін террористік топтар мен жалғыз терроршылардың ақпараттық технологияларды пайдалануы. Телекоммуникация желілеріне, Ақпараттық жүйелер мен коммуникациялық инфрақұрылымға қарсы шабуылдарды ұйымдастыру және орындау үшін ақпараттық технологияларды пайдалануды не ақпарат алмасуды, сондай-ақ электр байланысы құралдарын пайдалана отырып қауіп-қатерлерді қамтуы мүмкін. Ақпараттық жүйелерді бұзу, осал желілерге вирустарды енгізу, веб-сайттардың дефейсі, Ddos-шабуылдар, электрондық байланыс құралдарымен жеткізілген террористік қауіп-қатерлер мысал бола алады.

Қибертерроризм детерминациялайтын факторлар[3]**.**

Кибертерроризм тудыратын өзара іс-қимыл жасайтын факторлар кешені ара-сында криминологияда қабылданған жіктемеге сәйкес келесі факторларды бөліп көрсетуге болады;

Құқықтық факторлар. Кибертерроризм детерминациясының құқықтық факторлары біздің ойымызша, саяси факторлармен тығыз байланысты. Халықаралық деңгейде келісімге қол жеткізбеу нәтижесінде тиісті қылмыстық – құқықтық реттеудің болмауы кибертерроризм дамуының және өсуінің маңызды факторы болып табылады. Электрондық қол сұғушылықтар өз табиғаты бойынша трансшекаралық проблема болғандықтан, осы құбылыспен күрестің құқықтық негіздері мемлекетаралық деңгейде әзірленуі тиіс. Сонымен қатар, қазіргі уақытта әлемнің түрлі елдерінің заңнамасы әзірге қарама-қайшы, ұғымдық аппараттың біркелкілігі жоқ, соның ішінде киберқылмысты анықтауда халықаралық деңгейде бекітілмеген, қылмыстық заңнамаға сәйкес қандай әрекеттер қудалануы тиіс. Сондай-ақ жоғары технологиялар саласындағы қатынастарды тиісті азаматтық – құқықтық реттеудің болмауы да әсер етеді, бұл сондай-ақ заңнамада қылмыскерлерге жауапкершіліктен кетуге мүмкіндік беретінқылықтар туғызады, ал жазасыздық, өз кезегінде қол сұғушылықтың өсуіне итермелейді[4].

Кибертерроризмді жоққа шығаратын құқықтық факторларға сондай-ақ жоғары технологиялар саласындағы қылмыстарды ашу процесін реттеу, дәлелдемелерді жинау, киберқылмыс жасаған тұлғаларды соттық қудалау туралы нормалардың жеткіліксіздігі жатады.

Идеологиялық және адамгершілік – психологиялық факторлар. Кибертерроризм детерминациясының адамгершілік – психологиялық факторларына ғалымдар "тұтыну психологиясы"деп аталатын пайда болуын жатқызады. Бір жағынан бұл қазіргі жастар ұрпағының арасында бүгінгі күн ғана өмір сүретін және қажеттіліктерді кез келген құралдармен қанағаттандыру мүмкін деп санайтын жоғары сұраныстары бар индивидуалистердің белгілі бір бөлігін қалыптастыру. Бұл жастар табысқа тез жетуге бағытталған, тәуекелге, іскерлік жетімділікке бейімділігі бар. Бұл ретте киберқылмыстың төмен анықталуы мен ашылуы осындай әрекеттердің жазасыздығы туралы мифтің пайда болуына алып келеді, бұл осындай қылмыстарды өмірге қауіп төндірмей жасау мүмкіндігімен жиынтығында кибертерроризм жасауға барлық жаңа және жаңа тұлғаларды тартудың қосымша алғышарттарын жасайды.

Ақпараттық соғыс идеология мен билік жүйесін қамтитын құндылықтардың өзара іздейтін, антагонистік жүйелері әр түрлі билік жүйелері бар, жеке билік жүйелері бар адам қауымдастықтары арасында жүргізіледі. Мұндай қауымдастықтар мойындалған және танылмаған мемлекеттер, мемлекеттер одақтары, аза-маттық соғыс тараптары, экстремистік, соның ішінде билікті күштеп басып алуға ұмтылатын террористік ұйымдар, сепаратистік, азаттық қозғалыстар болып табылады.

Стратегиялық деңгейде ақпараттық соғыс құндылықтарды, бірінші кезекте антагонистік, қарсы тұратын тараптарды бұзу мақсатында, оның

ішінде өз мүддесіне оларды пайдалану мүмкіндігін қамтамасыз ету үшін, қарсыластың қарсы тұру әлеуетін бұзу, оның ресурстарын бағындыру үшін жүргізіледі[5].

Ақпараттық соғысқа билік құрған құрылымдар да, жеке қауымдастықтар да, топтар мен тұлғалар да қатыса алады .

Ақпараттық соғыс үздіксіз және қарулы күрес кезінде ғана емес, бейбіт уақытта да өткізіледі

Ақпараттық соғыс ақпараттық қарама-қайшылықтың ең қатал түрі. Ақпараттық соғысты жүргізудің тәсілдері мен құралдарына жалпыға танылған заңдық, моральдық нормалар мен шектеулер жоқ, олар тек тиімділік тұрғысынан ғана шектелген.

Кибертерроризм қаупі әртүрлі мемлекеттерді онымен күресте ынтымақтасуға мәжбүр етеді. Осымен халықаралық органдар мен ұйымдар айналысады: БҰҰ, Еуропа Кеңесі, халықаралық сарапшылар ұйымы, ЭЫДҰ, Интерпол. Барлық осы ұйымдар түрлі көпжақты бейресми әріптестермен бірге халықаралық күш-жігерді үйлестіруде, жоғары технологиялар саласындағы қылмыстарға қарсы күресте халықаралық ынтымақтастықты құруда маңызды рөл атқарады.

Пайдаланылған әдебиеттер тізімі:

1. См.: Номоконов В.А. Глобализация информационных процессов и преступность //2002. - С. 98;
2. Фундаментальное значение в исследовании феномена терроризма и его новой формы - кибертерроризма имеют работы Г. Веймана, С.Вилсона, М. Конви, Ф. Коэна, М. Поллитта, П.С. Пробста;
3. Осипенко А.Л. Борьба с преступностью в компьютерных сетях: Международный опыт. М., 2004;
4. Жмыхов А. А. Компьютерная преступность за рубежом и ее предупреждение: дис. канд. юрид. наук: 12.00.08.-М., 2003.- 178;
5. См.: Вартанова Е.Л. Современная медиаструктура. // СМИ в постсоветской России. - М., 2002; Гельман А. Русский способ (Терроризм и масс-медиа в третьем тысячелетии). - М., 2003;