***М. Қ. Найманбаева**, магистрант*
*Ғылыми жетекші — **А. Қ. Қамбаров**, қылмыстық құқықтық пәндер кафедрасының аға оқытушысы, заң ғылымдарының магистрі*
(Қазақ инновациялық-гуманитарлық заң университеті, Семей қ.)

КИБЕРТЕРРОРИЗМ ҚЫЛМЫСТАРЫНЫҢ ТҮСІНІГІ ЖӘНЕ ОНЫҢ АЛДЫН АЛУДЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ

Қазіргі жағдайда қауіпсіздіктің негізгі қатерлеріне келесілерді жатқызуға болады: массалық талқандау қаруын тарату, трансұлттық ұйымдастырылған қылмыс, есірткі саудасы, халықаралық терроризм. Бүгінде терроризм XXI мыңжылдықта адамзатпен кірген өзінің аумағы, болжамдау мүмкіндігі, қоғамдық-саясаттық және адамгершілік зардаптары бойынша ең қауіптісіне айналды. Қазіргі заманғы терроризмнің сипатты шегі террористтік топтардың өсуші масштабта жоғары тиімділік қылмыстық бизнеске қосылуы болып табылады: есірткімен, қарумен, контрафакттік тауарлармен, порнографиямен сауда жасау, күштеп алушылық және төлем алу мақсатымен адамдарды ұрлау. Көбінесе ұлттық, діндік, этникалық қақтығыстар, сепаратистік және босатушы қозғалыстармен байланысқан террористтік қызметтердің көпшілігі көбейіп келеді[i].

11 қыркүйектегі қайғылы оқиға халықаралық терроризмге әлемдік бірлестіктің қатынасын орнатуда шекаралық белгі болып табылды. Бұл мәселенің мәртебесі ғалами түрде біржақты соның ішінде Бірлескен Ұлттар Ұйымының, Европадағы қауіпсіздік пен қарым-қатынас Ұйымының құжаттарында мойындалды.

«Қылмыстың және терроризмнің глобализациялануына қарсы әлемдік қоғамдастық» Мәскеу Халықаралық конференциясының (Мәскеу, 2004 ж.) қатысушылары терроризмнің негізгі детерминанты көпжақты, тең дәрежеде саясаттық және әлеуметтік, идеологиялық, діндік және этникалық табиғатына ие екеніне бірнеше рет көңіл аударған. Дегенмен терроризмнің негізгі базасы үлкен әлеуметті әділетсіздікпен көрсетілген әлеуметті-экономикалық себептері болып табылады[ii].

Лунеевтің пікірі бойынша террорды ұйымдастырушылар кең әлеуметті базасыз маңызды террористтік қызметті дамытуы мүмкін емес. Сондықтан қазіргі заманғы терроризм аталған терминнің кең түсінігінде (әсіресе халықаралық) — бұл діндердің, ұлттардың, цивилизациялардың қақтығысуы емес, дамыған елдердің үлкен байлығы мен әлеуметті бай аймақтардың ауыр кедейшілік арасындағы антагонизмі болып табылады. Бірақ мұнда да кедейшілік қозғалтушы күш болып табылмайды, тікелей және жанама қысымның көмегімен және бір топтың басқа топтан ба сым түсуі, бір елдердің басқа елдерден, бір халықтың басқа халыққа зорлық-зомбылық көрсету арқылы ұстап отыратын әлемдегі үлкен әлеуметтік әділетсіздік болып табылады.

Террористтік ұйымдардың ақпараттық технологияларды және Интернет ғаламдық желісін қолдануы XXI ғасырдағы ең жаңа және ең қауіпті қатер болып келеді. АҚШ Әділет министрлігімен дайындалған 2000 жылдағы орындалған бюджет пен 2002 жылға жоспарлары туралы баяндамада айтылғандай, ақпарат заманындағы үдерісті технологиялық жетістіктер қылмыстықпен күресуді қиындатып отыр және ғалами қылмысты қызметке жаңа мүмкіндіктер туғызып отыр. Біздің маңызды инфрақұрылымымызбен

өзара қарым-қатынастың өсуінен қылмыскерлер, террористтер және шетел барлау қызметтері кибернетикалық құралдар мен қарулардың күшін қолдануды зерттегендіктен компьютерлік және ақпараттық жүйелерге жаңа осалдықтар жасап шығарды. Кибер-қылмыскерлердің құқық қорғаушы органдарға XXI ғасырда шақыру тастағаны зиянкестердің ақпараттық жүйелерге әсерін жоққа шығару жолымен киберкеңістікті қауіпсіздендіру тапсырмасын қойып отыр.

Жоғары технологиялық терроризмнің қауіпті көрсетілімі компьютерлік терроризм немесе кибертерроризм болып табылады. Терроризмнің бұл пішіні Интернетке қосылған маңызды инфрақұрылымдарды (көлік, атомдық электростанциялар, сумен қамтамасыз ету және энергетика) басқарудың компьютерлік жүйесінің жоғары осалдығына байланысты сарапшыларды айрықша қам жегізеді.

Интернет террористтерге ерекше мүмкіндіктер береді. Ол түрлі қажетті мағлұматтарды жеңіл алудың (артық назар туғызбай) қайнары болып табылады: қару және қажетті техникалық құралдармен ықтимал жабдықтаушының ұсыныстарынан бомбаларды әзірлеу туралы нұсқауларға дейін. Оның көмегімен жалданушыларды тартуға және насихат жүргізуге болады, банктерді бұзу арқылы қайырымдылық жинау арқылы қажетті қаржылық құралдарды ауыстыруға немесе оларды алуға болады, ақыры Ғаламдық Желінің көмегімен азаматтық немесе әскери инфрақұрылымның түрлі объектілерінің дұрыс жұмыс жасауына тез және аз шығынмен зардап шектіруге болады. Мұның бәрі тиісті ақпарат ағынына мемлекеттің араласуынан қорғаудың жоғары деңгейі ғана, яғни негізгі сипаттаманы сақтау және террористтік қызмет жағдайлары — оның құпиялылығы болып табылады.

Әзірге террористтер Интернетті негізінен жаңа қару секілді емес, қайта ақпарат алмасу немесе өз ойларын насихаттау құралы ретінде қолданады. Күн сайын қандай да бір үкіметтік мекемеге немесе банктерге компьютерлік шабуылдар туралы хаттамалар келіп түседі. Мұндай шабуылдарды терроризм деп атауға болмайды, себебі олар адамзатты құрбандыққа немесе адам өміріне қауіп әкелмейді. Бірақ кибертерроризм масқаралық құрал болып танылды. Яғни, қалғаны тек уақыт мәселесі болып отыр, біз диверсиялардың жарылғыш құралдар көмегімен емес, ал ірі ақпараттық жүйелердің Интернет әлемдік ком-пьютерлік жүйесі арқылы істен шығару сияқты терроризмнің жаңа түрінің туындауының куәгерлері боламыз. Оның құрбандары болып ең алдымен мемлекеттік ұйымдар мен ірі коммерциялық құрылымдар болады[iii].

Бірреттік спутникалық телефондар мен анықталмайтын ұялы карточкалардан басқа, мысалы швейцарлық «Аль-Кайеда» ұстап алу мүкіндігі жоқ хаттамалармен алмасу үшін Hotmail және Yahoo секілді әйгілі порталдардың электрондық поштасын қолданады. Террористтер өз атын және ұйымын тапсырған пайдаланушының «қалпысының» мұрағатын қолданады. Топ мүшелері осылай электронды хаттамалармен алмаспай-ақ шын өмірде тіл табыса алады. Олар арнайы қызметтер білмейтін электрондық поштаны, ашық достарын және тумаларын қолданады. Әрдайым әртүрлі Интернет-кафелер олардың мінсіз базасы болып табылады[iv].

Компьютерлік қауіпсіздік бойынша форумда ұлттық қауіпсіздік бойынша АҚШ президентінің көмекшісі Кондолиза Райс «кибернетикалық кеңістіктің біздің

экономиканың бөлігі болды. Энергетика, көлік және байланыс, банктік секторды қоса ел шаруашылығының әрбір саласы компьютерлік желілерді қолданады, және олардың жұмысына тәуелді болып табылады». «Бұл желілердің жұмысын бұзу арқылы елдің зәресін кетіруге болады» — деді Райс. Президенттің көмекшісі компьютерлік қауіпсіздікті қамтамасыз ету және компьютерлік терроризмді тоқтатуда мемлекет пен жеке сектор арасындағы қарым-қатынасты атап өтті. Өзінің соңғы сұхба тында терроризм сұрақтары бойынша сарапшы, Террорды зерттеудің университетаралық орталығының директоры Йона Александер «Аль-Кайеда» секілді топтардың бүгін-ертең Батысқа қарсы диверсиялар үшін көптеп талқандау қаруын немесе өз идеологиясын насихаттауды қолданатыны туралы сақтық танытты. Александер мырза исламисттер жасырын тармақты желі құрған Еуропа жақын арада «Аль-Кайеда» үшін негізгі алаң болады деп болжап отыр[v].

«Бүкіл әлем бойынша террордың эскалациясын күтуге болады, — деп ескертеді Александер. Дәстүрлі жоспардағы жаңа теракттар да болады — атысу, террорист құрбандарының жарылысы. Сонымен қатар кибертерроризм дағдыланады — қылмыскерлер клавишті бір рет басу арқылы мысалға, барлық ауданның энергожабдықтаушы немесе әуежай жұмысын бұза алады». Кибертерроризмнің мүмкіндігі өзімен барлық маңызды шақырулар қатарын көрсетеді. Біріншіден, ішкі мінездеріне сай компьютерлік шабуылдарды болжамдау немесе шын өмірде ізіне түсу мүмкін емес. Сондықтан шабуыл кезкелген уақытта елде немесе шетелде басталуы мүмкін, және оның артынан өткір сезімге тәуелді жастар, соғыс құмар елдер, қылмыскерлер, тыңшылар мен террористтер тұруы мүмкін; оған жауапкершілікті кім тартатынын дұрыс анықтауда жоғары деңгей таныту үшін айтарлықтай қор керек. Технология бұл мәселені жақын болашақта шеше алмайды. Екіншіден, барлық әлемдегі заңдардың күрделілігінен Интернетті немесе басқа электронды құралдарды қолдану жағдайларында дәлелдерді жинау, сонымен қатар заң бойынша кейбір тұлғаларды қуғындау, іздеу, табу және табыстау қиын болып табылады. Аталған мәселелер барды мәнін ұғынуды және кибертерроризммен күресудің жаңа халықаралық-құқықтық тетіктерін құрауды қажет етеді.

---

[i] Қазақстан Республикасының 2010 жылдан 2020 жылға дейінгі кезеңге арналған құқықтық саясат тұжырымдамасы // Казахстанская правда. 2009. 27 тамыз.

[ii] Батурин Ю. М., Жодзинский А. М. Компьютерная преступность и компьютерная безопасность. — М., 1991.

[iii] Криминология: Учебн. для юрид. вузов / Под ред. В. Н. Бурлакова, В. Г. Сальникова, С. В. Степашина. — СПб., 1999.

[iv] Рудаков К. Э. Ответственность провайдеров по договорам доступа к сети Интернет. — М., 2006.

[v] Ревяко Т. И. Компьютерные террористы. — Минск, 1997.