УДК 343.96+343.326+343.341

ЗАПОБІГАННЯ КОМП'ЮТЕРНОМУ ТЕРОРИЗМУ ЯК ОДИН ІЗ НАПРЯМІВ ПРОТИДІЇ ТЕРОРИЗМУ В УКРАЇНІ

Дмитро Мельник
Служба безпеки України

Анотація: **Статтю присвячено актуальним аспектам запобігання компютерному тероризму як одному із важливих напрямів протидії тероризму в Україні.**
Summary: **The article is devoted to the problems of prevention and counteraction to the cyberterrorism in Ukraine.**
Ключові слова: **Тероризм, компютерний тероризм, запобігання, протидія.**

I Вступ

Поширення у світі новітніх інформаційних технологій змінило роль і значення державних кордонів у контексті забезпечення національної безпеки. Світовий інформаційний простір за останні десятиліття став ареною геополітичного протиборства між провідними державами світу за досягнення стратегічної переваги у вирішенні міжнародних та регіональних проблем.

Сучасні процеси глобалізації та тенденції розвитку суспільства призвели до зростання транснаціонального тероризму, появи на озброєнні терористів новітніх інформаційних технологій та виникнення принципово нового виду тероризму – комп'ютерного, безпосередньо пов'язаного з рівнем науково-технічного прогресу. Інформаційні технології, які були створені з метою розширення можливостей отримання-передачі даних та комунікацій, стали джерелом нової загрози.

Реальна можливість застосування інформаційних технологій терористами створює передумови до масштабних технологічних аварій, блокування роботи транспортної системи, дезорганізації державного управління, фінансової системи, роботи наукових та медичних центрів. Сумний досвід більшості розвинених країн світу свідчить про те, що збитки від терористичних кібератак можуть значно перевищувати збитки від терористичних актів, учинених у традиційний спосіб.

З приєднанням України до глобального інформаційного простору проблема комп'ютерного тероризму набула для нашої держави особливої актуальності. Високий рівень інформатизації вітчизняного суспільства обумовлює потребу створення сучасної та надійної системи забезпечення інформаційної безпеки. Вагоме місце у цій системі повинні займати заходи запобігання комп'ютерному тероризму як протиправному явищу загалом, так і його окремим проявам.

II Результати досліджень

Науковими дослідженнями актуальних аспектів протидії тероризму загалом та комп'ютерному тероризму зокрема, а також діяльності спецслужб та правоохоронних органів у цій сфері займалися такі вчені як В. Ф. Антипенко, С. Б. Гавриш, В. О. Голубєв, М. Г. Гуцало, С. М. Баліна, К. І. Беляков, В. М. Бутузов, В. Ібрагімов, О. О. Климчук, В. Н. Кубальський, М. В. Кулешов, В. В. Мараховський, М. М. Оліфіренко, А. Л. Осипенко, В. І. Полевий, О. Г. Семенюк, О. М. Солодка, І. В. Ткачов, Т. Тропініна, В. В. Шорошев, В. С. Цимбалюк, В. Б. Хлевицький та ін. Однак більшість їх публікацій стосуються переважно проблеми комп'ютерного тероризму та загроз, які він породжує.

Разом з цим, лише деякі дослідники (В. М. Бутузов, В. О. Голубєв, М. В. Кулешов, В. С. Овчинський, С. В. Печериця, В. Б. Хлевицький) торкалися у своїх роботах такого важливого напряму протидії комп'ютерному тероризму, як запобігання. З необхідною повнотою у розробках вітчизняних дослідників запобігання цьому протиправному явищу поки що не було досліджено.

Тому ***завданням*** статті є висвітлення запобігання комп'ютерному тероризму як одного з напрямів протидії тероризму в Україні та надання пропозицій з його удосконалення.

Термін «терор» (від лат. «terror» - страх, жах) наводиться в тлумачних словниках у значенні «лякати», «залякувати» [1, с. 525]. У свою чергу під «тероризмом» розуміють будь-яке навмисне, політично мотивоване незаконне використання сили чи насильства проти осіб чи власності, як правило, із застосуванням зброї з метою залякування чи примусу уряду, цивільного населення для досягнення політичних чи соціальних цілей [2, с. 6].

У ст. 1 Закону України «Про боротьбу з тероризмом» від 20. 03. 2003 р. закріплено нормативне визначення цього явища: «тероризм – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур,

залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не повинних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей».

При цьому як один з видів тероризму у Законі визначено технологічний тероризм, який передбачає вчинення з терористичною метою злочинів із застосуванням у т. ч. комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створюють або загрожують виникненням надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру.

Поява нового різновиду технологічного тероризму – комп'ютерного тероризму, що визнаний фахівцями як один із найнебезпечніших видів комп'ютерної злочинності, обумовлена переходом до методів електронного управління технологічними процесами [3, с. 77].

Комп'ютерний тероризм поряд із комп'ютерною злочинністю визначено законодавцем у ст. 7 Закону України «Про основи національної безпеки України» від 19. 06. 2003 р. однією із загроз національній безпеці України в інформаційній сфері. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8. 07. 2009 р. №514/2009, також виокремлює прояви комп'ютерного тероризму та комп'ютерної злочинності в числі основних реальних та потенційних загроз інформаційній безпеці України.

При цьому варто погодитися з науковою позицією, відповідно до якої під комп'ютерним тероризмом варто розуміти навмисну, політично мотивовану атаку на інформацію, що обробляється комп'ютером, на комп'ютерну систему та (або) мережі, якщо вона викликає дезорганізацію роботи критично важливих елементів інфраструктури держави та створює небезпеку для життя й здоров'я людей або заподіяння інших тяжких наслідків, за умови, що такі дії були вчинені з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи здійснення (нездійснення) дій органами державної влади / місцевого самоврядування, посадовими особами цих органів, об'єднаннями громадян, юридичними особами, а також залучення уваги громадськості до визначених політичних, релігійних чи інших поглядів [5, с. 49; 6, с. 132].

Для комп'ютерного тероризму, на відміну від традиційних різновидів тероризму, характерним є використання новітніх досягнень науки і техніки у сфері телекомунікацій, комп'ютерних та інформаційних технологій. Відкритість та доступність мережі Інтернет може використовуватися терористами для дискредитації урядів і держав, розміщення сайтів терористичної спрямованості, пошкодження та руйнування інформаційних систем критично важливої інфраструктури країн шляхом внесення в них недостовірних даних або систематичного виведення цих систем з робочого стану. Серед їх цілей можуть бути політична або економічна дестабілізація в країні чи у регіоні, саботаж, крадіжка військових або цивільних інформаційних ресурсів у політичних цілях [5, с. 52]. Все це породжує страх і тривогу в суспільстві та є своєрідним доповненням до традиційних видів тероризму [4, с. 78].

На сучасному етапі дослідники виділяють дві основні форми комп'ютерного тероризму [4, с. 78-80; 8, с. 223], які потребують адекватної протидії:

1) вчинення терористичних актів організаціями, групами й окремими особами за допомогою комп'ютерів і комп'ютерних мереж (виведення з ладу автоматизованих систем (АС) управління державою, збройними силами, об'єктів промисловості, життєзабезпечення і підвищеної небезпеки, спричинення надзвичайних подій шляхом втручання в програмне забезпечення АС зазначених об'єктів, у тому числі з використанням комп'ютерних вірусів).

Так, на початку 2003 р. заявила про своє існування нова терористична організація «Арабський Електронний Джихад» (AEJT), яка обрала своїм гаслом «поставити на коліна мережу Інтернет». Метою діяльності цієї організації було оголошено знищення всіх ізраїльських, американських та інших неприйнятних для неї сайтів;

2) використання кіберпростору терористичними організаціями, групами й окремими особами для інших цілей, безпосередньо не пов'язаних зі здійсненням терактів (координація й планування терористичної діяльності; збір докладної інформації про цілі терактів; використання як засобу зв'язку зі своїми членами та однодумцями; пропаганда терористичної діяльності; збір і розподіл коштів для підтримки терористичних рухів; залучення до їх діяльності нових членів тощо).

Так, свого часу чеченські терористи використовували мережу Інтернет як канал інформаційного впливу (Веб-сторінка «Кавказ-центру» на http: www. kavkaz.org) та засобу для збирання коштів на підтримку своєї діяльності під час бойових дій у Чечні в 1994 – 1997 рр. На сучасному етапі терористичні та релігійні екстремістські організації («Хізб-Ут-Тахрір», «Брати мусульмани» та ін.) використовують мережу Інтернет для експансії в інформаційний простір України з метою розпалювання сепаратиських настроїв у «мусульманських» регіонах держави та пропаганди створення державних утворень ісламського типу.

З огляду на сучасний стан розвитку систем зв'язку та глобальних мереж телекомунікацій, що суттєво посилює та розширює можливості терористів, дослідники проблеми комп'ютерного тероризму констатують пропорційну залежність між кількістю його проявів та рівнем розвитку інформаційної інфраструктури й комп'ютеризації країни, що обирається як ціль терористичної атаки [6, с. 134].

Високий ступінь централізації органів державного управління в Україні та низький рівень кваліфікації персоналу вітчизняних інформаційних систем, на думку фахівців, суттєво підвищують вразливість й так недостатньо захищеної національної інфраструктури та можуть привести до її руйнування в разі вчинення терористичних актів через Інтернет. Фактично в сучасних умовах неочікуваного інформаційного удару по критичній інфраструктурі країни може завдати будь-який підготовлений терорист з власного помешкання, використовуючи комп'ютер, під'єднаний до мережі Інтернет [7, с. 57–58].

Звертаючи увагу суспільства та керівництва держави на зростаючі загрози, які породжує комп'ютерний тероризм, фахівці зазначають, що терористів можуть зацікавити державні установи та об'єкти критичної інфраструктури країни, де використовуються інформаційно-телекомунікаційні технології: системи управління та обчислювальні центри урядових установ, центри управління військовими мережами й медичними закладами, системи управління реакторами вітчизняних АЕС, сховищ радіоактивних матеріалів, стратегічних нафто- й газопроводів, системи водопостачання й розподілу електроенергії, космічні супутники, транспортні вузли, хімічні заводи та бактеріологічні лабораторії [7, с. 55; 8, с. 319–320]. У випадку реалізації цих загроз терористи можуть завдати значної шкоди національній безпеці України.

Одним із прикладів такого розвитку подій може бути виявлений британськими спецслужбами навесні 1999 р. факт встановлення контролю над одним із чотирьох військових супутників зв'язку Міністерства оборони Великобританії невідомою групою «хакерів». У свою чергу американськими спецслужбами було отримано достовірні дані про російських «хакерів», які зламали секретні коди ВМС США й отримали доступ до інформації про системи керування балістичними ракетами [7, с. 56]. В іншому випадку групи «хакерів» із Росії, Сербії та інших країн під час бомбардування Югославії силами НАТО у 1999 р. цілеспрямовано атакували сервери державних установ США з метою порушення їх роботи, що завдало значної економічної, військової та політичної шкоди США та їх союзникам по НАТО [8, с. 321–322].

Оцінюючи рівень загрози комп'ютерного тероризму для України також слід враховувати наступні особливості: високий потенціал і професійний рівень програмістів, послугами яких охоче користуються провідні компанії світу; здатність молоді швидко опановувати технічні новинки; зростання економіки, що стимулює зростання комп'ютеризації країни та низку інших факторів [6, с. 134].

З огляду на викладене, можна прийти до висновку про двоїстий характер актуальності проблеми комп'ютерного тероризму для нашої держави. З одного боку, Україна не настільки заможна, щоб оперативно переобладнати сучасними системами управління свої стратегічно важливі підприємства, АЕС, що зробить їх невразливими для атак комп'ютерних терористів. З іншого боку, все більше зростає значення створеної в державі інформаційної інфраструктури як стратегічного ресурсу, що теж вимагає постійної уваги й охорони. Тому проблема протидії комп'ютерному тероризму потребує належної уваги на загальнодержавному рівні та необхідних для цього матеріально-технічних і інтелектуальних ресурсів.

Разом з тим, результати дослідження проблем протидії комп'ютерній злочинності та комп'ютерному тероризму свідчать про те, що орієнтація лише на технічні й технологічні засоби забезпечення інформаційної безпеки в умовах інформатизації не має значного успіху. Особливо це відчувається із часу приєднання до міжнародних систем телекомунікації нових країн і підвищення інтелектуального рівня користувачів комп'ютерних систем.

Так, за даними Національного відділення ФБР США з протидії комп'ютерним злочинам, від 85% до 97% нападів на корпоративні мережі не лише не блокуються, але й не виявляються. Випробування, проведені ще в 1995 р. за фінансової підтримки Міністерства оборони США, показали наступні результати: у 88% випадків проникнення спеціальних груп експертів у військові інформаційні системи було успішним і лише в 4,36% випадків атаки були виявлені, в той час як про 5% таких атак повідомили системні адміністратори. В 2001 р. інша група експертів обстежила близько 8 тис. комп'ютерів Міністерства оборони США й виявила 150 тис. уразливих місць [7, с. 57].

Тому закономірним буде висновок про те, що чим складніше стає програмне забезпечення автоматизованих систем, тим більш недосконалими стають традиційні організаційні заходи й засоби захисту інформації в цих системах. Проблемою є також те, що з розвитком сучасних електронних засобів обробки інформації розвиваються також технічні засоби перехоплення й доступу до інформації, що передається в електронних системах телекомунікації. Такі засоби можуть бути доступними для терористичних та злочинних організацій [5, с. 51].

Національна система протидії тероризму визначена у ст. 4 Закону України «Про боротьбу з тероризмом» від 20. 03. 2003 р. Організація протидії тероризму в Україні та забезпечення її необхідними силами, засобами

і ресурсами здійснюється Кабінетом Міністрів України у межах його компетенції. Інші центральні органи виконавчої влади беруть участь у протидії тероризму у межах своєї компетенції, визначеної законами та виданими на їх основі іншими нормативно-правовими актами.

Суб'єктами, які безпосередньо протидіють тероризму у межах своєї компетенції, є: СБ України, МВС України, МНС України, Міністерство оборони України, ДПС України, Держдепартамент України з питань виконання покарань, Управління державної охорони України. До участі у здійсненні заходів, пов'язаних із запобіганням, виявленням і припиненням терористичної діяльності, залучаються у разі необхідності також: СЗР України, МЗС України, Мінінфраструктури України (колишній Мінтранс України), ДМС України, ДПА України та низка інших державних органів.

СБ України визначена законодавцем головним органом у загальнодержавній системі протидії терористичній діяльності, який здійснює досудове слідство у справах про злочини, пов'язані з терористичною діяльністю. Координацію діяльності суб'єктів, які залучаються до протидії тероризму здійснює Антитерористичний центр при СБ України.

У свою чергу, МВС України здійснює протидію тероризму шляхом запобігання, виявлення та припинення злочинів (у т. ч. й компютерних), вчинених з терористичною метою, розслідування яких віднесене законодавством України до компетенції органів внутрішніх справ.

Зважаючи на визначену за СБ та МВС України у ст. 112 КПК України підслідність справ про злочини, відповідальність за які передбачена низкою норм Розділу XVI КК України, а також на їх повноваження, визначені у Законі України «Про боротьбу з тероризмом», саме вони є уповноваженими протидіяти комп'ютерному тероризму як одному із проявів комп'ютерної злочинності.

Загалом протидію комп'ютерному тероризму можна розглядати як систему правових, оперативних, організаційних, технічних та інформаційних заходів, спрямованих на запобігання, виявлення, розкриття і припинення як терористичної діяльності, так і недопущення окремих терористичних актів в інформаційному просторі України з використанням сучасних інформаційній технологій для здійснення впливу на інформаційні ресурси країни (системи, мережі тощо). Така протидія повинна здійснюватись з урахуванням природи цього протиправного явища, його причин і умов.

Важливою складовою у цій діяльності є запобігання – пріоритетна форма впливу уповноважених суб'єктів на причини та умови вчинення таких злочинів, а також на схильних до їх вчинення осіб, у т. ч. й шляхом активного залучення необхідних джерел інформації, новітніх інформаційних технологій та спеціальних технічних засобів, широкого використання можливостей органів виконавчої влади, які відповідно до ст. 4 Закону України «Про боротьбу з тероризмом» зобов'язані брати участь у протидії тероризму в межах своєї компетенції.

Окрім того, в ст. 5 Закону з метою негласного збору інформації про діяльність міжнародних терористичних організацій та отримання упереджувальної інформації в разі загрози вчинення терористичного акту органам СБ України надане право проведення оперативно-технічних пошукових заходів у системах і каналах телекомунікацій, які можуть використовуватися терористами.

З огляду на те, що Україна є активним учасником міжнародної антитерористичної коаліції та відповідно до покладених законодавством завдань, органи СБ і МВС України зобов'язані здійснювати активний запобіжний вплив на інформаційний простір держави з метою стримування окремих екстремістськи налаштованих осіб від здійснення терористичних та інших екстремістських акцій з використанням сучасних інформаційній технологій.

Разом з тим, проведений аналіз практики протидії комп'ютерному тероризму та наявних наукових досліджень дає можливість зробити висновок про те, що на сучасному етапі ця діяльність ускладнюється низкою чинників.

По-перше, комп'ютерні терористичні атаки внаслідок їх прихованого характеру практично неможливо спрогнозувати або простежити в реальному часі. Такі атаки можуть початися в будь-який час, всередині країни або поза її межами, її ініціаторами та виконавцями можуть бути як недосвідчені молодики, які шукають гострих відчуттів, так і терористи або злочинці. Для встановлення суб'єктів, відповідальних за вчинення таких атак, будуть потрібні значні інтелектуальні та матеріальні ресурси, оскільки сучасний рівень технологій не дає можливості найближчим часом вирішити цю проблему [5, с. 50].

По-друге, комп'ютерний тероризм спроможний не лише блокувати чи нейтралізувати діяльність об'єктів терористичної атаки, побудованих на основі або з використанням інформаційно-телекомунікаційних технологій, але й викликати системну кризу у тих суспільствах, де широко розвинена інфраструктура інформаційного обміну [8, с. 323].

По-третє, в законодавстві різних країн світу чітко не визначені та не розмежовані поняття комп'ютерного тероризму та комп'ютерної злочинності. Невирішеність цього питання на законодавчому рівні ускладнює реалізацію правозастосовної функції уповноваженими органами в Україні.

По-четверте, складність та моральна застарілість норм процесуальних законів, що діють у більшості країн світу, суттєво ускладнюють збір доказів у випадках вчинення терористичних актів та інших злочинів з використанням мережі Інтернет або інших електронних засобів, а також кримінальне переслідування, пошук, затримання й видачу окремих злочинців. Тому у багатьох країнах проводиться робота, спрямована на прийняття нових та удосконалення й узгодження норм існуючих законів у цій сфері [5, с. 50].

По-п'яте, запобігання як вагома складова протидії комп'ютерному тероризму навіть за наявності спеціального нормативного акту – Закону України «Про боротьбу з тероризмом» – не може бути достатньо якісним та ефективним в умовах відсутності в Україні необхідної й достатньої нормативної бази для цього, зокрема, законів «Про запобігання злочинам (або правопорушенням)» та «Про протидію екстремістській діяльності».

При цьому варто звернути увагу на те, що п. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9. 01. 2007 р. досить повно визначає загальні напрями вирішення цих проблем у контексті забезпечення інформаційної безпеки:

− підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

− вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері.

У свою чергу у п. 10 Концепції реформування Служби безпеки України, затвердженої Указом Президента України від 20. 03. 2008 р. №249/2008 передбачено необхідність здійснення заходів з організаційно-правового удосконалення системи протидії проявам комп'ютерного тероризму та комп'ютерної злочинності.

Зважаючи на викладене, на думку автора, для удосконалення системи протидії комп'ютерному тероризму доцільно вжити наступних заходів:

1) розробити коректний та узгоджений понятійний апарат у сфері забезпечення національної безпеки в інформаційній сфері та протидії загрозам їй (у т. ч. й комп'ютерному тероризму та комп'ютерній злочинності);

2) привести норми національного законодавства, у т. ч. й процесуального, у відповідність положенням Конвенції Ради Європи про кіберзлочинність 2001 року, що передбачають права та обов'язки правоохоронних органів та спецслужб щодо отримання та реалізації інформації про операторів, провайдерів та користувачів інформаційних мереж та систем;

3) узгодити між собою положення законів України «Про основи національної безпеки України» та «Про боротьбу з тероризмом», розкривши у ст. 1 останнього поняття «комп'ютерного тероризму (кібертероризму)» з огляду на загрози, які він в собі несе для національної безпеки України. Законодавче закріплення різних форм тероризму є виправданим і покликане забезпечити надійний захист об'єктів національної безпеки - особи, суспільства та держави;

4) прийняти закони «Про запобігання злочинам», «Про протидію екстремістській діяльності», «Про перехоплення телекомунікацій», а також Національну стратегію формування інформаційного суспільства;

5) доповнити Розділ XVI КК України нормою про кримінальну відповідальність за комп'ютерний тероризм, яка б дозволила розмежувати поняття комп'ютерного тероризму та комп'ютерної злочинності;

6) підвищувати ефективність діяльності органів і підрозділів СБ та МВС України, спрямованої на протидію правопорушенням у сфері комп'ютерних технологій, припинення діяльності транснаціональних терористичних та злочинних організацій, за підтримки правоохоронних органів іноземних держав;

7) активізувати діяльність уповноважених державних органів та громадських організацій із запобігання проявам комп'ютерного тероризму в державі, суспільстві та в криміногенному середовищі, в першу чергу в середовищі осіб, які вчиняють правопорушення з використанням комп'ютерних засобів та інформаційних мереж («хакерів»);

8) забезпечити накопичення, облік, узагальнення та взаємний обмін інформацією про терористичні організації, їх організаторів, учасників й окремих осіб, які діють в інформаційному просторі України або за його межами, та підозрюються в причетності до терористичної діяльності;

9) покращити взаємодію уповноважених вітчизняних правоохоронних органів і спецслужб між собою та з аналогічними компетентними органами іноземних держав та міжнародними організаціями, що здійснюють протидію тероризму в усіх його проявах (у першу чергу з Інтерполом та Європолом);

10) підвищувати ефективність використання передових форм міжнародного співробітництва в сфері протидії комп'ютерному тероризму та комп'ютерній злочинності (налагодження безперебійного інформаційного обміну з іноземними партнерами через Національний контактний пункт миттєвого обміну інформацією та реагування на кіберзлочини при СБ України, інтегрований у Цілодобову інформаційну

мережу для боротьби зі злочинами у сфері комп'ютерних технологій держав Великої вісімки (G-8) та інших країн (формату «24/7»));

11) покращити матеріально-технічне забезпечення підрозділів СБ України і МВС України, що здійснюють діяльність з протидії комп'ютерному тероризму та кіберзлочинності.

III Висновки

Комп'ютерний тероризм, як різновид технологічного тероризму, є новою формою терористичної діяльності, що на сучасному етапі становить загрозу національній та міжнародній безпеці. Загальнодержавна система протидії комп'ютерному тероризму має бути достатньо універсальною й здатною запобігати терористичним загрозам в інформаційній сфері України будь-якої природи, масштабів і динаміки та адекватно реагувати на їх виникнення. Запобігання є пріоритетним напрямом протидії комп'ютерному тероризму, складовими якої мають стати: приведення вітчизняного законодавства у відповідність до сучасного рівня розвитку інформаційних технологій; організація взаємодії та координація зусиль спецслужб, правоохоронних та судових органів, забезпечення їх необхідною матеріально-технічною базою; активізація міжнародного співробітництва у цій сфері.

Література: ***1.*** *Новий тлумачний словник української мови. У трьох томах / Уклад. В. Яременко, О. Сліпушко. - Т.3 «П – Я». Вид. 2-ге виправлене. – К.: «Вид-во АКОНІТ», 2006. – 862 с.* ***2.*** *Абсаментон С. К. Сучасний тероризм та проблеми забезпечення національної безпеки Республіки Казахстан. – Павлодар, 2000. - С.6.* ***3.*** *Беляков К. І, Цимбалюк В. С. Інформаційні технології як чинник терористичного акту // Боротьба з організованою злочинністю і корупцією (теорія і практика). Науково-практичний журнал. – 2003. - № 8. - С. 89-96.* ***4.*** *Тропинина Т. Киберпреступность и кибертерроризм // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В. А., Ахтырской Н. Н. - Запорожье: Центр исследований компьютерной преступности. – 2004. - Вып.1. - С. 76-81.* ***5.*** *Голубєв В. Электронный терроризм - новое лицо терроризма // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В. А., Ахтырской Н. Н. - Запорожье: Центр исследований компьютерной преступности. – 2004. - Вып.1. - С. 49-56.* ***6.*** *Голубєв В. А. Кибертерроризм - угроза национальной безопасности и интересам Украины // Юридичний журнал. - 2004. - №1. – С. 132-134.* ***7.*** *Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября 2001 г.: оценка угроз и предложения по их нейтрализации // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В. А., Ахтырской Н. Н. - Запорожье: Центр исследований компьютерной преступности. – 2004. - Вып.1. - С. 56-75.* ***8.*** *Бутузов В. М., Тітуніна К. В. Сучасні загрози: комп'ютерний тероризм // Боротьба з організованою злочинністю і корупцією (теборія і практика). Науково-практичний журнал. – 2007. - №17. – С. 316-324.*

УДК 519.724.681

ПРО ДЕЯКІ АСПЕКТИ ВИЗНАЧЕННЯ ЦІННОСТІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Олександр Архипов

Національний технічний університет України «Київський політехнічний інститут»

Анотація: **Розглянуто особливості визначення цінності конфіденційної інформації, зокрема, з урахуванням процесів старіння та фрагментації інформаційного ресурсу на окремі блоки. Наведено структуру моделей цінності інформації.**

Annotation: **It is considered the features of determination of confidential information value, taking into account senescence and fragmentation processes of informative resource in particular. The structures of information value models are resulted.**

Ключові слова: **Цінність інформації, корисність інформації, важливість інформації, збитки, модель цінності інформації, фрагментація інформації** .

I Вступ

Сфера захисту секретної інформації набула системних ознак на рубежі 19 – 20 століть [1]. Головними чинниками її формування були інтуїція та досвід професіоналів, які опановували цю сферу. Порівняно з охороною державної таємниці галузь технічного захисту інформації (ТЗІ) системно сформувалася пізніше, у другій половині 20-го століття, а в Україні утворення системи ТЗІ фактично співпало з становленням її незалежності. Характерною ознакою формування вітчизняної системи ТЗІ була наявність вже достатньо