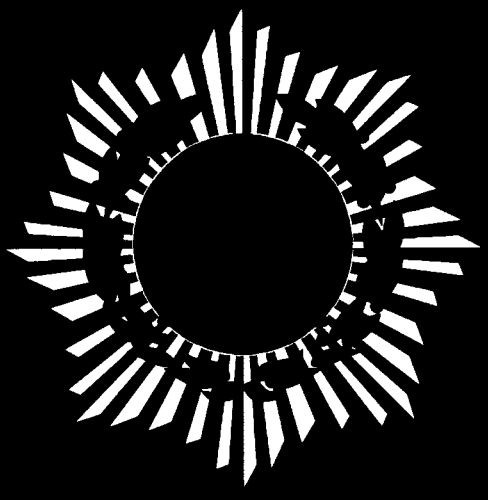
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ
МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА



3(26), 2011
НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

ЗМІСТ

ЗБРОЯ, ЗАСОБИ ІНДИВІДУАЛЬНОГО ЗАХИСТУ ТА АКТИВНОЇ ОБОРОНИ

ЗАХИСТ ІНФОРМАЦІЇ

СИСТЕМИ ТА МЕТОДИ ОБРОБКИ ІНФОРМАЦІЇ

УДК 35.075.5+355.405.1+355.40 (477)

Бурячок В.Л.., кандидат технічних наук,
старший науковий співробітник

КІБЕРНЕТИЧНА БЕЗПЕКА – ГОЛОВНИЙ ФАКТОР СТАЛОГО РОЗВИТКУ СУЧАСНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Досліджено стан кібернетичної безпеки в сучасному світі високих технологій. Вивчено і проаналізовано досвід, накопичений провідними країнами Європи та США щодо забезпечення ними власної кібербезпеки. Запропоновані науково обґрунтований понятійний апарат у цій предметній області, а також комплекс заходів щодо захисту кіберпростору України від різних проявів кібернетичних злочинів і загроз.

Ключові слова: *інформаційне суспільство, інформаційно-комунікаційна технологія, інформаційно-телекомунікаційна система, кібератака, кібербезпека, кіберзагроза, кіберзлочин, кіберпростір.*

В статье исследовано состояние кибернетической безопасности в современном мире высоких технологий. Изучен и проанализирован опыт, накопленный ведущими странами Европы и США по обеспечению ими собственной кибербезопасности. Предложены научно обоснованный понятийный аппарат в этой предметной области, а также комплекс мероприятий по защите киберпространства Украины от разных проявлений кибернетических преступлений и угроз.

Ключевые слова: *информационное общество, информационно-коммуникационная технология, информационно-телекоммуникационная система, кибератака, кибербезопасность, киберугроза, киберпреступление, киберпространство.*

The state of cybernetic safety in the modern world of high technologies is investigated. The experience of cybersafety protection which has been accumulated up by the leading countries of Europe and the USA is studied and analyzed. Scientifically substantiated conceptual apparatus in this object domain, as well as a complex of actions for the protection of the cyberspace of Ukraine from different cybernetic crimes and threats are offered.

Keywords: *information society, information-communication technology, information-telecommunication system, cyberattack, cybersafety, cyberthreat, cybercrime, cyberspace.*

Науково-технічна революція наприкінці XX – початку XXI сторіччя викликала у світі глибокі системні перетворення. Як наслідок, вони дали можливість, завдяки синтезу перспективних інформаційно-комунікаційних технологій (далі ІКТ) і бурхливому розвитку інформаційно-телекомунікаційних (ІТ) систем (далі ІТС), сформуватися та розвинутися принципово новим глобальним субстанціям – інформаційному суспільству, а також інформаційному і кібернетичному просторам (далі кіберпростір), які мають нині практично необмежений потенціал і відіграють суттєву роль в економічному й

соціальному розвитку будь-якої країни світу.

Факт створення інформаційного суспільства офіційно був визнаним представниками держав "Великої вісімки" (G8) в ході Окінавської зустрічі у червні 2000 року [1]. Пізніше, а саме в ході Женевського саміту (10–12 грудня 2003 року), відповідною Декларацією, як згодом й у Законі України "Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" № 537-V, затвердженому Верховною Радою України 9 січня 2007 року [2], була визначена його суто гуманітарна сутність, тобто відкритість для усіх бажаючих з орієнтацією перш за все на інтереси людини, і фактично констатовано, що ІКТ та ІТС:

стали важливою складовою суспільного розвитку й розвитку світової економіки та значною мірою змінили механізми функціонування багатьох суспільних інститутів та інститутів державної влади;

увійшли до числа факторів, які найбільш суттєво впливають на формування сучасного високоорганізованого інформаційного середовища й надають можливість на якісно новому рівні інформаційного обслуговування в інформаційному й кіберпросторі вести повсякденну оперативну роботу, здійснювати системний аналіз стану і перспектив діяльності інформаційно-аналітичних підрозділів тощо.

Разом з цим неконтрольоване поширення і використання ІКТ та ІТС призвело до того, що поряд із отриманням значних переваг від виникнення інформаційного суспільства, інформаційного і кібернетичного просторів світове співтовариство набуло й усіх пов'язаних із цим проблем, внаслідок чого:

суттєво ускладнилось завдання добування даних, що необхідні органам державного і військового управління для прийняття виважених (раціональних), науково обґрунтованих та адекватних умовам обстановки рішень;

світ став надто уразливим від появи нових деструктивних впливів – викликів, фактично неприхованих кібернетичних злочинів і загроз у ІТ сфері;

все частіше інформаційний і кібернетичний простори почали використовуватися спеціальними службами та злочинними угрупованнями, включаючи терористичні організації як об'єкти інформаційно-технічного та інформаційно-психологічного впливу (протиборства) тощо.

Ці проблеми висвітлено у багатьох публікаціях зарубіжних і вітчизняних авторів. Найвідомішими серед них є роботи Возженікова А.В., Ліпкан В.А., Лєнкова С.В., Мірошниченко В.М., Хорошка В.О., Ярочкіна В.І., Н. Панаріна, Г. Почепцова, М. Кастельса, М. Лібіцкі, К.А. Мініхена, О. Шермана, Е. Тоффлера, Ф. Фукуями та інших фахівців. Висновки і твердження, що містяться в їх працях, частково заклали методологічну базу теоретичних засад розвитку інформаційного суспільства в Україні та вітчизняної політики інформаційної безпеки. Проте, тим не менше, аналіз публікацій у предметній області, що розглядається, свідчить про те, що комплексне дослідження проблеми інформаційної й, передовсім, кібернетичної безпеки, її складових та особливостей на цей час практично відсутнє. Тому, враховуючи реалії сьогодення, вона потребує додаткового й більш глибокого вивчення.

Таким чином, усе викладене вище дає можливість стверджувати, що проблеми кібернетичної безпеки за сучасних умов і для України, і для переважної більшості інших держав світу стають нині особливо актуальними. Відповідно, метою статті є дослідження стану кібернетичної безпеки (далі **кібербезпеки**) у сучасному світі, вивчення накопиченого провідними державами досвіду

щодо її забезпечення, формування зрозумілого та науковообґрунтованого понятійного апарату в цій предметній області, а також пропозицій щодо захисту кіберпростору України від різних проявів кібернетичних злочинів і загроз.

Формування та розвиток інформаційного суспільства базується, як відомо [2–5], на синтезі двох технологій – комп'ютерної і телекомунікаційної, та визначається двома простими, але дуже змістовними висловлюваннями. Перше з них, сформульоване одним із засновників корпорації *Intel* Гордоном Муром, говорячи про те, що "... кількість транзисторів у процесорах збільшуватиметься вдвічі кожних півтора роки ...", фактично пояснює:

гарантоване зростання швидкості обчислень і об'ємів інформації, що при цьому обробляється;

формування на рубежі тисячоліть так званих інформаційного і кібернетичного просторів й виникнення нових, специфічних за формою і способами взаємовідносин їх суб'єктів та об'єктів.

Друге належить Роберту Меткалфу, винахіднику найпоширенішої на сьогодні технології комп'ютерної мережі *Internet*. Ведучи мову про те, що "... цінність мережі знаходиться у квадратичній залежності від кількості вузлів, які є її складовими ...", він фактично констатує, що основу сучасного інформаційного суспільства становлять мережі різного функціонального призначення, сукупність та взаємозв'язок яких інформаційний та кіберпростори, власне, і утворюють.

У цьому випадку з урахуванням змісту основних понять, визначених зарубіжними і вітчизняними експертами, а також окремих нормативно-правових документів іноземних країн (зокрема Росії та США) під **інформаційним простором** будемо розуміти глобальне інформаційне середовище, яке у реальному масштабі часу забезпечує комплексну обробку відомостей про конфліктуючі сторони та їх оточення з метою підтримки прийняття рішень зі створення оптимального для досягнення поставлених цілей складу сил і засобів та їх ефективного застосування в різних умовах обстановки, а під **кіберпростором** – комунікаційне середовище, утворене системою зв'язків між об'єктами інформаційної інфраструктури (інформаційними ресурсами, системами і мережами усіх форм власності), що керуються автоматизованими системами управління (АСУ) й використовуються як для передавання інформації, яка в них циркулює, так й для впливу на аналогічні об'єкти протилежної сторони. Говорячи про кіберпростір як основну високорозвинену модель об'єктивної реальності й враховуючи його сучасні найбільш відмінні ознаки і характерні риси, можна стверджувати, що останнім часом саме він усе частіше використовується протиборчими сторонами для проведення певних, заздалегідь спланованих деструктивних дій на кшталт:

проникнення до ІТ систем одне одного;

блокування або виведення з ладу їх найбільш уразливих елементів;

дезорганізації оборонних АСУ протилежної сторони, систем управління її транспортом та енергетикою, економікою та фінансовою системою тощо.

Про важливість кіберпростору свідчить поява концепцій ведення боротьби у ньому – комплексу заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на ІТС супротивника й використовувані ним ІКТ й захисту від такого впливу власних систем і технологій, а також створення у збройних силах ряду країн світу спеціальних структур, призначених для ведення такої боротьби. Такий стан справ, а також глибинні зміни стосовно більшості держав земної кулі до внутрішньої **кібербезпеки** (стану захище-

ності їх кіберпростору в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується сталий розвиток цих країн, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз їх особистим, корпоративним та/або національним інтересам) й формування, як наслідок, потужних транснаціональних злочинних груп [6, 7], що спеціалізуються на злочинах у кіберпросторі, фактично:

дають можливість вести мову про формування принципово нової геостратегічної, геоінформаційної та геополітичної ситуації, коли виникають зовсім нові загрози безпеці для об'єктів критично важливої інфраструктури цих держав, їх окремих громадян і суспільства в цілому й на безумовно вищий щабель виводять вагу досліджень, спрямованих на всебічний аналіз методів, засобів, тактики і стратегії дій у кіберпросторі, тобто ведення так званих кібернетичних воєн;

призводять до безпрецедентного розголошення персональних даних, критично важливих корпоративних ресурсів (матеріальних, фінансових, інформаційних тощо), конфіденційної інформації та інформації, що становить державну або іншу передбачену законом таємницю;

обумовлюють необхідність вироблення рекомендацій щодо коротко- та довгострокових пріоритетів трансформації безпекового сектору цих держав і у тому числі України, передовсім, за напрямом створення комплексних систем захисту власного кіберпростору, ІКТ та ІТС від внутрішніх і зовнішніх кібернетичних злочинів і загроз.

З метою уникнення багатозначності у трактуванні термінів "**кіберзлочин**" (фактично неприховані кримінальні дії, що здійснюються з використанням засобів електронно-обчислювальної техніки (далі ЕОТ), і за які передбачається юридична відповідальність) і "**кіберзагроза**" (прояв дестабілізуючого негативного впливу на певний об'єкт, що реалізується за рахунок використання технологічних можливостей кіберпростору й створює небезпеку як для нього самого, так й для свідомості людини в у цілому) інструктивні матеріали Інтерполу рекомендують поділяти їх на такі групи: власне комп'ютерні злочини (порушення авторських прав на програмне забезпечення, розкрадання даних, порушення роботи обчислювальних систем, розкрадання комп'ютерного часу тощо), злочини, "пов'язані з комп'ютерами" (головним чином, фінансове шахрайство), та мережні злочини (використання мереж для здійснення незаконних угод). Найбільший же інтерес із позицій класифікації кібернетичних злочинів і загроз нині становить схема, запропонована Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю. У ній ідеться про чотири можливі групи таких протиправних діянь, а саме:

1) злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем, що реалізуються через несанкціонований доступ в інформаційне середовище, незаконне втручання в дані та/або їх перехоплення, незаконне використання комп'ютерного й телекомунікаційного встаткування або його повне вилучення тощо;

2) злочини, пов'язані з використанням комп'ютерів які передовсім полягають у підробці документів та/або шахрайстві із застосуванням засобів ЕОТ;

3) злочини, пов'язані з розміщенням у мережах протиправної інформації, наприклад, поширенням дитячої порнографії;

4) злочини відносно авторських і суміжних прав.

Незважаючи на те, що останнім часом зазначені протиправні діяння здійснюються протиборчими сторонами

перш за все з метою порушення або блокування роботи інформаційних систем і мереж стратегічно важливих галузей (об'єктів) інфраструктури одне одного, у тому числі, фінансового, енергетичного, промислового, транспортного та військового секторів, а також несанкціонованого отримання (крадіжки) інформації з відносно відкритих і закритих баз даних (баз знань) державних, комерційних й інших установ, її модифікації та/або знищення, – до визначення проблематики кіберзлочинів і кіберзагроз законодавство більшості країн світу підходить по-різному. Так, наприклад, згідно із законодавством США протиправними діяннями у сфері IT технологій, за які передбачається кримінальна відповідальність, вважають: несанкціонований доступ до інформації з комп'ютера, використовуваного урядовим відомством, ушкодження або порушення функціонування останнього; шпигунство, шахрайство, загрози, вимагання, шантаж та інші протиправні діяння, вчинені з використанням комп'ютера; торгівля викраденими або підробленими пристроями доступу, які можуть бути використані для одержання грошей (товарів, послуг), комп'ютерними паролями або аналогічною інформацією; навмисне ушкодження майна, устаткування, ліній і систем зв'язку; перехоплення й розголошення повідомлень, переданих телеграфом, усно або електронним способом; порушення конфіденційності електронної пошти й голосових повідомлень; навмисне одержання або видозміна повідомлень, що зберігаються в пам'яті комп'ютера, а також за створення перешкод для санкціонованого доступу до таких повідомлень. У Великобританії до протиправних діянь у сфері IT технологій належать: навмисний протизаконний доступ до комп'ютера або комп'ютерної інформації, що циркулює в ньому; розголошення персональних даних, виготовлення й поширення порнографічних матеріалів (у т.ч. з використанням комп'ютерної техніки). У ФРН такими протиправними діяннями є: неправомірний доступ до комп'ютерної інформації, її несанкціонована модифікація, підробка, утаювання або використання; руйнування, ушкодження, приведення в непридатність технічних засобів обробки інформації; порушення таємниці телекомунікаційного зв'язку; комп'ютерне шахрайство; незаконне втручання в роботу телекомунікаційних систем. У Франції протиправними діяннями у сфері IT технологій, як правило, вважають: перехоплення, розкрадання, використання або надання розголосу повідомленням, переданим засобами зв'язку; незаконний доступ до автоматизованої системи обробки даних; порушення або запобігання нормальній роботі комп'ютерної системи; знищення або модифікацію інформації в автоматизованій інформаційній системі; уведення або зберігання в пам'яті ЕОМ заборонених законом даних; порушення порядку автоматизованої обробку персональних даних; збір і обробка даних незаконним способом; зберігання певних даних упродовж терміну, що перевищував установлений законом; несанкціоноване використання даних; знищення, псування або розкрадання будь-якого документа, техніки, спорудження, устаткування, установки, апарата, технічного пристрою або системи автоматизованої обробки даних або внесення до них змін; виготовлення й поширення телекомунікаційними мережами дитячої порнографії; збір або передачу інформації, що міститься в пам'яті ЕОМ або картотеці іноземної держави; знищення, розкрадання, вилучення або копіювання даних, що носять характер секретів національної оборони, що втримуються в пам'яті ЕОМ або в картотеках, а також ознайомлення із цими даними сторонніх осіб; терористичні акти, пов'язані з

діяннями в області інформатики тощо.

Представлений перелік не є вичерпним, але він дає можливість:

– по-перше, умовно об'єднати зазначені вище типи протиправних діянь у дві укрупнені категорії – злочини (загрози), спрямовані безпосередньо на порушення нормального функціонування ІТ систем та підключених до них комп'ютерів (тип 1 – за схемою, пропонованою Конвенцією Ради Європи 2001 року), а також "традиційні" протиправні діяння (типи 2, 3 і 4 – за тією ж схемою), що або пов'язані з комп'ютером (*computer-related*), або вчинені за його допомогою (*computer-facilitated*);

– по-друге, зробити висновок про те, що зазначені та подібні їм протиправні діяння у кіберпросторі: вийшли за межі окремих країн і на цей час за темпами росту випереджають усі інші види організованої злочинності; отримали істотну фінансову підтримку і якісні комунікації; поширилися на всі види злочинів, учинених в ІТ сфері;

– по-третє, формалізувати зазначені вище типи протиправних діянь, представивши їх моделлю, яка міститиме три головні етапи – етап вивчення жертви, етап проведення атак на жертву й етап приховування слідів злочину.

Згідно з офіційними даними Інтерполу, темпи зростання таких протиправних діянь з року в рік неодмінно збільшуються. Свого апогею вони досягли нині у глобальній мережі *Internet*. Так, наприклад, якщо в Росії за офіційними даними у 1996 році було виявлено лише 15 кіберзлочинів, то у 1997 році – вже 101. Збитки від них склали приблизно 20 мільярдів карбованців. За наступні п'ять років кількість подібних злочинів у тій же Росії зросла у 33 рази. У 2002 році російськими правоохоронцями був зареєстрований 3371 злочин у сфері комп'ютерної інформації. Останніми роками ситуація ускладнилася ще більше. Як наслідок, у цей час практично щомісяця вчиняється щонайменше один серйозний злочин із використанням сучасної ЕОТ шляхом проведення різного роду кібератак. Вони здійснюються або окремими особами, або у складі об'єднаних певною метою злочинних угруповань. При цьому сучасні об'єднання кіберзлочинців починають працювати за принципами, властивими звичайним компаніям, де у кожного учасника своя роль і система заохочень. Так, наприклад [8–11]:

– у червні–жовтні 1994 року кримінальна група Володимира Л. Левіна, вчинивши понад 40 зломів центральної банківської електронної системи платежів Сіті-банку з використанням вкрадених паролів та ідентифікаційних номерів, здійснила переказ більш 10 мільйонів доларів з рахунків трьох постійних клієнтів банку на власні рахунки у банках Каліфорнії, Фінляндії, Німеччини, Нідерландів, Швейцарії та Ізраїлю;

– у грудні 2007 року, зламавши комп'ютери департаменту енергетики Національної лабораторії Оак Риджа (Теннессі, США), кіберзлочинці викрали понад 12 тисяч номерів карт соціального страхування й дат народження відвідувачів *ONRL* за період з 1999 по 2004 роки. У той же час, за наявними даними, атаці піддалися також Національна лабораторія в Лос-Аламосі та Національна лабораторія Лоуренса в Ліверморі (США);

– у вересні 2008 група хакерів із Греції, зламавши комп'ютерну систему CERN (Європейський центр ядерних досліджень), – організації, під керівництвом якої був створений Великий адронний коллайдер (ВАК), отримала доступ до серверів, що керують компактним мюонним соленоїдом (*Compact Muon Solenoid, CMS*), який відстежує дані в ході зіткнення елементарних часток у прискорювачі ВАК. З метою оприлюднення своїх дій вони, як

повідомило видання *The Telegraph*, на сайті організації розмістили текст грецькою мовою під заголовком "*GST: Greek Security Team*";

– у березні 2009 року латвійська газета "Час" з посиланням на дані розслідування, проведеного експертами в області комп'ютерних злочинів з канадської компанії *Information Warfare Monitor* і фахівцями Університету Торонто, повідомила, що міністерство закордонних справ Латвії разом з рядом держустанов інших країн світу (Ірану, Бангладешу, Індонезії, Філіппін, Брунею, Барбадосу й Бутану) піддалося атаці програми-шпигуна GhostNet, що орієнтовно була запущена в мережу з Китаю. Крім того, за інформацією видання, сліди "електронних шпигунів" були виявлені в посольствах Німеччини, Португалії, Індії, Пакистану, Південної Кореї, Індонезії, Румунії, Кіпру, Мальти, Таїланду й Тайваню.

Наведені вище та подібні до них приклади протиправних діянь переконливо доводять, що з часом *Internet* почав впливати на розвиток усієї планети і став незамінним депозитарієм загальнолюдського знання. За нинішніх умов він взагалі може бути як предметом (метою) злочинних посягань та середовищем, в якому скоюються правопорушення, наприклад, "ідеальним середовищем для діяльності терористів" [9], так і засобом чи знаряддям самого злочину. Такий стан справ передовсім пояснюється тим, що доступ до цієї глобальної мережі є надто легким, у ній надзвичайно легко забезпечити анонімність користувачів, вона ніким не управляється і не контролюється й зрештою, у ній, на додачу, "не діють закони та не існує поліції" [9].

Підтвердженням такого висновку стали результати досліджень *Institute for Security Technology Studies At Dartmouth College* (США) [11], метою яких було прогнозування ситуації в *Internet* у результаті здійснення Сполученими Штатами широкомасштабної антитерористичної кампанії після трагедії 11 вересня 2001 року. У звіті під назвою "*Cyber Attacks During The War on Terrorism: A Predictive Analysis*", опублікованому 22 вересня 2001 року, фахівцями інституту були проаналізовані політичні конфлікти, що стимулювали зростання кількості атак на ресурси *Internet*, а саме конфлікти між Індією й Пакистаном, Ізраїлем і Палестиною, NATO і Сербією, США та Китаєм тощо. Фахівці інституту, як наслідок, констатували, що фізичні атаки на елементи критично важливої інфраструктури провідних країн світу супроводжуються останнім часом обов'язковим зростанням кількості кібератак, передовсім на сервери та активне мережне устаткування, що підключене до цієї глобальної мережі. Представники інституту *System Administrator and Network Security* (США) та Центру із захисту національної інфраструктури при ФБР (США) взагалі зробили спільну заяву про те, що здійснення кібератак поступово стає потужним засобом ведення інформаційних воєн між державами, а *Internet* – потужним "інструментом кіберпланування" [12], який забезпечує сучасним терористам анонімність, можливість управляти і координувати дії при підготовці та здійсненні терактів. Тобто, за твердженням [8, 9, 13–15] та інших фахівців, тероризм останнім часом зробив якісний крок у своєму розвитку. До його нових особливостей на сьогодні відносять: відсутність національних кордонів; спрямованість терористичних дій як на цивільні, так і на військові об'єкти; спроможність ефективного використання конфліктних і кризових ситуацій задля досягнення власних інтересів.

Такий стан справ, у свою чергу, призвів до появи принципово нового різновиду злочинно-терористичних дій у віртуальному просторі, який у засобах ма-

сової інформації (ЗМІ) отримав загальну назву – **кібертероризм** [16–19] та під яким західні й вітчизняні фахівці [20] розуміють нині суспільно небезпечну діяльність, що свідомо здійснюється в кіберпросторі (або з використанням його технічних можливостей) окремими особами або організованими групами з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані **кібератаки** (кібернапади) на ІТ системи з використанням високих технологій. До її основних особливих рис вони відносять:

високу ефективність кібератак;

просторово-часову невизначеність джерела кібератаки та його віддаленість від об'єкта атаки;

часову невідповідність між власне кібератакою й процесом її підготовки;

можливість організації складних кібератак одночасно на різні ІТ системи з різних напрямів тощо.

Спектр прояву кібертероризму є достатньо широким – від прийняття хибних рішень або розповсюдження паніки, до проникнення в канали і системи зв'язку та навігації тощо. Його результатом може бути, наприклад, введення хибного інформаційного ресурсу або порушення цілісності існуючого, дезорганізація роботи критично важливих елементів інформаційної та/або кібернетичної інфраструктури держави, дестабілізація суспільно-політичної обстановки в державі та регіоні, ускладнення міжнародних відносин або інші негативні наслідки, що створюють небезпеку для життя і здоров'я населення.

Виступаючи з проблем світових загроз, директор ЦРУ США Джордж Тенет зробив заяву про те, що кібертероризм, розповсюджуючись у світі, може з часом набути значно більших, ніж очікувалося, масштабів і, як наслідок, стати реальною загрозою для національної безпеки будь-якої держави. За його твердженням, уже зараз більшість терористичних угруповань на кшталт *Hizbollah, HAMAS, the Abu Nidal organization і Bin Laden's al Qa'ida ma* інших подібних до них структур для здійснення своєї протиправної діяльності використовують останні досягнення інформаційних технологій та комп'ютерного прогресу "...комп'ютерні файли, електронну пошту і шифрування (криптографію та стеганографію) ...". Підтвердженням цьому слугує той факт, що на сьогодні в *Internet* представлені абсолютно всі відомі терористичні групи порівняно з 1998 роком, коли лише половина з 30-ти організацій, зарахованих США до терористичних, мали свої сайти. Вони публікують власні матеріали, щонайменше, на 40 різних мовах і у своїй діяльності послуговуються здебільшого такими прийомами як [21]:

– завдання збитків окремим елементам кіберпростору;

– руйнування апаратних засобів, мереж електроживлення та елементної бази ІТС, а також наведення завад шляхом використання спеціальних програм, біологічних, хімічних та інших засобів;

– викрадення або знищення інформаційних, програмних і технічних ресурсів кіберпростору, що мають суспільну значимість шляхом подолання їх систем захисту, впровадження вірусів та різного роду закладок;

– вплив на програмне забезпечення та інформацію з метою їхнього спотворення або модифікації;

– розкриття та загроза опублікування або власне саме опублікування закритої інформації про функціонування інформаційної інфраструктури держави, суспільно значимі військові ІТ системи, коди шифрування та принципи роботи шифрувальних систем;

– захоплення каналів ЗМІ з метою поширення дезінформації, чуток, демонстрації сили терористичної організації та оголошення нею своїх вимог;

– знищення або активне приглушення ліній зв'язку, штучне перевантаження вузлів комутації;

– проведення інформаційних і психологічних операцій тощо.

Найбільш характерним прикладом "продуктивної роботи" кібертерористів нині вважають так званий кіберджихад, який здійснюють одне проти одного хакери Пакистану та Індії за Кашмір [11, 12, 22, 23]. Пакистанські хакери зламують *Web*-сайти індійських державних установ. У свою чергу, індійська хакерська група (*Indian Snakes*) у якості "віртуальної помсти" поширює мережний хробак "*Yaha-Q*". Головне завдання цього вірусу полягає у здійсненні *DDOs*-атак на деякі пакистанські ресурси, серед яких *Internet*-провайдери, сайт фондової біржі в Карачі (*Karachi Stock Exchange*) та урядові ресурси.

Ще одним досить відомим прикладом є протистояння ізраїльських і палестинських хакерів [11, 12, 22, 23]. У жовтні 2000 року, після припинення мирних переговорів, вони брали участь у ряді спрямованих одна проти одної кібератак, що мали різний характер: від простої зміни змісту сторінок до скоординованого нападу з метою захоплення повноважень адміністратора системи. Так, наприклад, 6 жовтня 2000 року було уражено 40 ізраїльських сайтів і щонайменше 15 палестинських. Програмний засіб проведення розподілених атак з відмовою в обслуговуванні став головним інструментом, використовуваним ізраїльтянами. Пропалестинські хакери за можливості руйнували будь-який тип ізраїльських сайтів, змінюючи їхній зміст повідомленнями під рубрикою "За вільну Палестину" або "Вільний Кашмір". Організація "Хезболла" взагалі виробила цілу стратегію завдання збитків ізраїльському уряду, його військовим і діловим колам [24]. Першою фазою, на думку лідерів "Хезболли", повинна стати дестабілізація урядових органів Ізраїлю. Друга буде сконцентрована на краху фінансових інститутів. А в ході третьої та четвертої має відбутися знищення в комп'ютерній мережі даних про сотні угод і фінансових операцій.

Наслідки боротьби хакерів Пакистану та Індії, Ізраїлю та Палестини з усією очевидністю свідчать про безсумнівну уразливість будь-якої держави від різних проявів кібертероризму. Передовсім це пояснюється тим, що зазначений різновид кіберзагроз не має державних кордонів, а його потенційні представники здатні рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі.

Проведений аналіз стану боротьби в інформаційному й передовсім кібернетичному просторах за володіння світовим інформаційним ресурсом, зміни тенденцій у політиці провідних держав світу щодо протидії кіберзлочинам і кіберзагрозам та зміні внутрішньої інформаційної політики цих держав, зважаючи на посилення її безпекової компоненти, дає можливість зробити нині низку висновків.

1. Стрімкі темпи розвитку світової науково-технічної думки і подальшого удосконалювання ІКТ та ІТС неминуче приводять до створення в межах глобального інформаційного суспільства єдиного інформаційного і кібернетичного простору, у яких в перспективі будуть акумульовані всі засоби збору, накопичення, обробки, обміну та зберігання інформації.

2. ІКТ та ІТС перетворюються на один із найбільш важливих факторів управління сучасним світом, основним інструментом, який впливає на усталену систему міжнародних відносин. При цьому ІКТ останнім часом, окрім усього іншого, розглядаються й як засіб можливого нападу на окремі елементи національних інфраструктур.

3. Найбільш розповсюдженими формами протиправних діянь у кібернетичному просторі нині визнано так звані кіберзлочини та кіберзагрози, що здійснюються внутрішніми поодинокими інсайдерами або зовнішніми організованими злочинними співтовариствами (кіберугрупованнями хакерів, крекерів, фрікерів та/або розвідувальних організацій), які мають за мету порушення штатного режиму функціонування ІТ систем один одного і реалізуються ними за рахунок використання комп'ютерної й іншої спеціальної техніки та програмного забезпечення шляхом проведення кібернетичних атак і терактів. При цьому сучасний тероризм, як стверджують західні та вітчизняні фахівці, еволюціонує останнім часом у напрямку, який можна назвати "мережною війною" (*netwar*), і який від інших форм кіберзлочинності відрізняє наявність політичних мотивів і мети.

4. Такий стан справ викликає зростаюче занепокоєння як у розвинених державах світу, так, зокрема, і в Україні, і спонукає їх до створення власних загальнодержавних систем боротьби з кіберзлочинами та кібертероризмом. Ці зусилля, на нашу думку, мають спрямовуватися за такими головними напрямами:

уніфікації і гармонізації національного законодавства та міжнародних актів, сутність яких повинна бути спрямована на попередження та запобігання комп'ютерній злочинності та комп'ютерному тероризму;

розробки єдиного понятійного апарату;

проведення наукових розробок в області створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;

удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки;

створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом із ефективною системою координації їх взаємодії;

удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;

модернізації існуючих та розробки нових захищених ІКТ та ІТС, що, у свою чергу, мають передбачати: розробку політики безпеки зі здійснення контролю мережевого доступу; здійснення, на підставі існуючих рішень, заходів із забезпечення безпеки, аналізу можливих ризиків та уразливостей; створення відповідної інфраструктури; проектування систем захисту та визначення вимог, що висуваються до використовуваних засобів і механізмів захисту; виділення ресурсів, ранжирування обраних контрзаходів за ступенем важливості, реалізацію та тестування найбільш пріоритетних; розробку та супроводження системи виявлення атак, що є основним засобом боротьби з мережними атаками та реагування на них тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 р. // Дипломатический весник. – 2000. – № 8. – С. 51–56.

2. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9.01.2007 № 537-V.

3. Киберполитика : Глоссарий [Електронний ресурс]. – Режим доступу : http :// www.cuberpolitics.ru/content/view/77/29/.

4. *Голубев В.* Проблемы противодействия киберпреступности и кибертерроризму в Украине / В.А. Голубев [Електронний ресурс]. – Режим доступу : http ://www.crime-research.ru/articles/Golubev1104

5. *Шеломенцев В.П.* Організована кіберзлочинність : до визначення поняття. / В.П. Шеломенцев [Електронний ресурс]. – Режим доступу : http : // www.nbuv.gov.ua/portal/Soc_Gum/bozk/2009_21/ 21text/g39.pdf.

6. GAO-10-606. CYBERSPASE United States Faces Challenges in Addressing Global

Cybersecurity and Governance, Washington, July 2010 [Електронний ресурс]. – Режим доступу : http ://web.ebscohost.com/

7. GAO-10-628. Key Private and Public Cyber Expectations Need to Be Consistently Addressed United States Government Accountability Office, Washington, July 2010 [Електронний ресурс]. – Режим доступу : http : // web.ebscohost.com

8. Спецслужбы США делятся опытом в сфере ИТ-безопасности. – К. : Видавничий Дім ІТС, 2009. – С. 13.

9. *Гриняев С.Н.* Информационная война : история, день сегодняшний и перспектива / С.Н. Гриняев [Електронний ресурс]. – Режим доступу : http : // www.agentura.ru/equipment/psih/info/war/.

10. *Касперский Е.* Киберпреступность как бизнес / Е. Касперский. [Електронний ресурс]. – Режим доступу : http ://www.crime-research.ru/analytics/cybercrimes20101/2.

11. Актуальные вопросы выявления сетевых атак [Електронний ресурс]. – Режим доступу : http : // kiev-security.org.ua/box/12/141.shtml.

12. Мир вступил в эпоху сетевых войн и конфликтов [Електронний ресурс]. – Режим доступу : http : // www.rodon.org/polit-100408112419.

13. Руководство по кибербезопасности для развивающихся стран [Електронний ресурс]. – Режим доступу : http ://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-r.pdf.

14. *Ільяшов О.А.* До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу / О.А. Ільяшов, В.Л. Бурячок // Наука і оборона. – 2010. – № 4. – С. 35–40.

15. *Ільяшов О.А.* Захист інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу – одна з найважливіших проблем сучасності / О.А. Ільяшов, В.Л. Бурячок // Збірник матеріалів наук.-практ. конф. "Актуальні проблеми управління інформаційною безпекою держави" Національної Академії СБ України, 22.03.2011. – С. 334– 339.

16. *Старостина Е.* Кибертерроризм – подход к проблеме / Е. Старостина [Електронний ресурс]. – Режим доступу : http ://www.crime-research.ru.

17. *Мазуров В.А.* Кибертерроризм: понятие, проблемы противодействия / В.А. Мазуров [Електронний ресурс]. – Режим доступу : http : // www.tusur.ru/filearchive/reports-magazine/2010-1/41-45.pdf.

18. A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism. By: Matusitz, Jonathan; Breen, Gerald-Mark. Journal of Human Behavior in the Social Environment, Feb2011, Vol. 21 Issue 2, p109-129, 21 p. [Електронний ресурс]. – Режим доступу : http : // search.ebscohost.com/login.aspx?direct=true&db=aph&AN.

19. *Бурячок В.Л.* Кібер-злочинність і кібертероризм – загрози національній безпеці та інтересам України / В.Л. Бурячок, О.В. Шарий // Вісник воєнної розвідки / ВДА ГУР МО України. – Вип. 21. – К. : ВДА ГУР МО України, 2010. – С. 24–29.

20. *Харченко В.П.* Кибертерроризм на авиационном транспорте / В.П. Харченко, Ю.Б. Чеботаренко, А.Г. Корченко, Е.В. Пацира, С.А. Гнатюк [Електронний ресурс]. – Режим доступу : http ://www.nbuv.gov.ua/portal/natural/pitu/2009_4/ content/archive/4-28.131-139.pdf.

21. *Вехов В.Б.* Компьютерные преступления: способы совершения, методики расследования / В.Б. Вехов. – М. : Право и закон, 1998. – С. 29–37.

22. Деякі питання розкриття та розслідування злочинів у сфері комп'ютерної інформації [Електронний ресурс]. – Режим доступу : http : // kiev-security.org.ua/box/12/66.shtml.

23. Глава АТЦ: самые опасные виды терроризма – ядерный и кибертерроризм. [Електронний ресурс]. – Режим доступу : http :// www.securitylab.ru/news/274644.php.

24. Кибератака реальной войны [Електронний ресурс]. – Режим доступу : http ://www.history.vn.ua/book/100tayn/.

Отримано 27.09.2011