Порфімович О. Л.,
проф.

УДК 044.738: 323.28 (70)

Віртуальний криміналітет: від хакера до терориста (портрет явища)

Досліджуються потенційні загрози мережевого тероризму. Подано аналіз хакерської спеціалізації. Описуються основні ознаки сучасної кібернетичної злочинності, способи використання інтернету кібертерористами та сфери злочинної діяльності у всесвітній павутині. Розглядається правове регулювання інтернет-відносин.
Ключові слова: кіберзлочинці, інтернет, інформація.

The potential threats of network terrorism are explored in the article. The analysis of hacker specialization is given. The basic signs of modern cybernetic criminality methods of the use of the internet by cyber terrorists and sphere of criminal activity in the world wide web are described. The legal regulation of internet relations is examined.
Keywords: cyber criminals, internet, information.

Исследуются потенциальные угрозы сетевого терроризма. Подан анализ хакерской специализации. Описываются основные признаки современной кибернетической преступности, способы использования интернета кибертеррористами и сферы преступной деятельности во всемирной паутине. Рассматривается правовая регуляция интернет-отношений.
Ключевые слова: киберпреступники, интернет, информация.

У програмному документі — Концепції національної безпеки України (Основи державної політики) визначено загрози національній безпеці та інтересам України, до яких віднесено й комп'ютерну злочинність та комп'ютерний тероризм.

Чимало сучасних дослідників означеного питання сперечаються щодо оцінки реального ризику кібертероризму, кібервійни та інших кіберзагроз. Так, Джеймс Льюїс із Центру стратегічних та міжнародних досліджень (США, Колумбія) вважає, що говорити про комп'ютерні мережі, як про велику ахіллесову п'яту, не слід. Мовляв, відповідні загрози несуть у собі ймовірну проблему для великого та середнього бізнесу, і аж ніяк неспроможні налякати тих, хто серйозно опікується державною інфраструктурою.

Для того щоб визначити ступінь небезпеки ймовірного комп'ютерного вторгнення, слід з'ясувати ступінь залежності інфраструктури від комп'ютерних мереж.

Не секрет, що будь-яке індустріально розвинене суспільство характеризується високим ступенем залежності від комп'ютерних мереж. Водночас чимала кількість американських дослідників намагається переконати у зворотному. Мовляв, загроза вторгнення є мінімальною, і кіберзлочинці здатні застосувати хіба що "зброю не масового ураження, а зброю масового роздратування" [1]. Один із аргументів такої позиції ґрунтується на тому, що кібератаки, за досвідом, дуже рідко спричиняють фізичні збитки, що потребують довготривалого ремонту. Так, Дж. Льюїс зазначає, що "в контексті макроекономіки збої в системах водопостачання, електроенергії та повітряного руху, так само інші сценарії кібертерору, видаються стандартними подіями". Стандартними, цебто такими, що не торкаються системи національної безпеки країни. На думку цього автора, для національної економіки, де десятки чи навіть сотні систем забезпечують роботу найважливіших інфраструктур, збої в системах, коли обслуговування споживачів припиняється на години та навіть дні — є "стандартним випадком на регіональному рівні". Відверто кажучи, шановному Дж. Льюїсу хочеться не повірити: невже пересічний американець, якому на кілька годин чи навіть днів відімкнули енерго- або водопостачання, сприймає цей факт як цілком нормальний та звичний? А те, що відімкнення сталося через кібервторгнення (злочинця або терориста, байдуже), теж не має значення, оскільки всі вже давно звикли до таких перебоїв: техніка, хоч і високоякісна, але не досконала [2]. За такої логіки, згадується вислів лідера українського "Братства" Дмитра Корчинського, котрий одного разу сказав, що якби Христос прийшов на Землю сьогодні, то з ним повелися б значно гірше, ніж стародавні юдеї: сьогодні його просто не помітили б. Не проводячи паралелей між Ісусом Христом та кіберзлочинцями або кібертерористами, все ж таки розумієш, що Дж. Льюїс має рацію: на тлі неякісної та нестабільної роботи систем державної інфраструктури (зокрема, в США) можна елементарно не помітити кібервторгнення! "Кібертерористи повинні атакувати безліч цілей одночасно та продовжувати атаку протягом доволі тривалого періоду, щоб посіяти жах і досягти стратегічної мети, чи навіть будь-якого іншого ефекту. Щодо більшості найважливіших інфраструктур, такий сценарій множинних нападів є нездійсненним для хакерів, терористичних груп та держав (особливо для держав, коли ризик розкриття і

розгляду вторгнення як акту воєнної агресії є більшим за ті сумнівні переваги, котрі можна одержати від кібернападів на інфраструктуру)" [1]. Хоча, думається, Дж. Льюїс прагне якось прикрасити картину, що склалася в мережевій інфраструктурі США. Адже практично хрестоматійною стала історія 1997 року (вона наводиться практично в усіх публікаціях про кіберзлочини та кібервторгнення), коли американське військове відомство провело експеримент, дозволивши незалежним хакерам змоделювати інформаційну атаку проти найважливіших систем життєзабезпечення США за допомогою комп'ютерних програм та інтернету. Начебто трьох хакерів відправили на човнах в океан, давши їм із собою лише портативні комп'ютери та забезпечивши їх каналом супутникового зв'язку. Завдання, поставлене перед хакерами в межах цього експерименту — завдати шкоди будь-якій системі життєзабезпечення країни шляхом несанкціонованого втручання в комп'ютерні мережі. Шкоду, що її зуміли заподіяти хакери (зазначимо, що шкода мала віртуальний характер і ніяк не позначилася на роботі систем) можна було порівняти хіба що з наслідками ядерного вибуху. Найуразливішою виявилася система енергопостачання США: тільки за перший день атаки (якби її було завершено) могло б загинути не менше 20000 осіб, а економічні збитки становили б кілька мільярдів доларів...

І все ж таки частина спеціалістів вважає, що цифровий Перл-Харбор неможливий, а загрози кібервторгнень переважно надумані, вони мають на меті одержання чималого фінансування на розробки відповідних заходів протидії. Інша справа — загрози звичні, традиційні, "старомодні". На превентивні заходи щодо них слід витрачати більші кошти, оскільки їх застосування може бути не віртуальним, а реальним. Кібератаки можуть мати характер хіба що явища супутнього...

На думку російського політолога І. Морозова, проблема (а вона спільна як для США, так і для Росії) полягає в тому, що державні спецслужби та відомства цілеспрямовано нагнітають страхи навколо потенційної загрози мережевого тероризму з метою збільшення фінансування своєї діяльності [2]. Так, наводяться цифри — 50 мільярдів доларів щорічно — витрат США на створення інформаційної безпеки [3]. На думку скептиків щодо можливості успішних кібернетичних атак, гіпершвидкий розвиток мережі інтернет спровокував війни у віртуальних світах, що дало підстави футурологам виманювати чималі кошти у військових відомств на боротьбу з імовірними загрозами. Тим часом визначення ступеня ймовірності загроз перебуває у площині суб'єктивній та поза межами громадського контролю. Загроза може бути штучно гіпертрофована, через що одна країна матиме доступ до внутрішніх справ іншої. Створення "образу ворога" завжди було ефективним засобом провадження власної внутрішньої та зовнішньої політики; "холодна війна" переходить у віртуальну площину. Наслідки кібернетичного втручання однієї країни у справи іншої можуть бути різні: від впливу на економічні процеси до розгрому опозиційних рухів, здатних легко "експортуватися" на територію держави-сусіда.

Так звані "скептики" зазначають, що людина надто прилучена до процесів управління, і тому кібернетичний тероризм та кібернетичні війни сьогодні не становлять небезпеки та ризику в класичному розумінні. Наприклад, на кондитерській фабриці всі технологічні процеси виконують комп'ютери. Терорист зламав мережу та змінив рецептуру коржиків шляхом додавання в тісто стрихніну. Завтра отруйні коржики потраплять до торговельних закладів... Можливий такий сценарій? "Скептики" переконують, що така ситуація абсурдна, оскільки людський фактор на будь-якому виробництві залишається вирішальним, а тому жахливі наслідки неможливі. Але вони ж таки застерігають, що оскільки наша цивілізація дедалі більше використовує технології "безконтактного" циклу, ступінь контролю та втручання з боку людини не повинен зводитися до мінімуму.

Одним із аргументів щодо перебільшення загроз від кіберзлочинців та кібертерористів є також розвінчування професійних міфів про безкарність та анонімність інтернет-злочинців. Насправді ж будь-який провайдер може підтвердити, що для нього немає таємниць у діяльності його клієнтів, а тому він у принципі може легко знайти "точку входу" в мережу навіть так званого "зовнішнього" мережевого вандала. Так, І. Морозов стверджує, що російські провайдери чітко виконують вказівки спецслужб і "здають" їм кібернетичних злочинців та хуліганів. Хоча, зазвичай, такий бік діяльності російських провайдерів не дуже афішується... Отже, "мережа є значно підконтрольнішою та авторитарнішою, ніж про це побутує думка" [2]. У будь-якому разі, такі російські реалії.

В Україні контроль за користувачами інтернетом також існує. А от чи перебувають засоби контролю в правовій площині — щодо цього є сумніви, зокрема в Інтернет-асоціації України. Члени останньої обурені прийняттям Постанови Кабінету Міністрів № 1169 "Про затвердження порядку одержання дозволу суду на здійснення заходів, що тимчасово обмежують права людини, та використання одержаної інформації" (вересень 2007 року). Згідно з цим документом, правоохоронні органи мають змогу отримувати дозволи на приховане знімання інформації за допомогою технічних засобів, таємне проникнення в житло тощо без рішення суду. Таке рішення може одноосібно "виписувати" голова апеляційного суду, а громадянин, чию електронну пошту читають та

чиї телефони прослуховують, можуть про це ніколи й не дізнатися. О. Ольшанський, член Інтернет-асоціації України, зазначає: якщо громадянин навіть і дізнається про те, що його "сканують" у такий штиб, він усе одно не зможе звернутися по захист своїх конституційних прав, оскільки ніколи не надасть доказів таємного припису голови апеляційного суду [4]. Додамо, що в проекті нового Закону "Про інформацію", поданому Мінюстом України, пропонується вважати засобами масової інформації всі вебресурси (байдуже, домашні це чи особисті сторінки користувачів інтернету), що передбачає державний контроль за їхнім змістом.

У США, до речі, теж працюють у цьому напрямі: там узвичаєно концепцію публічно-приватного партнерства (додамо, що цю ідею не можна назвати визнаною в усьому світі — теоретики захисту прав на приватне життя дискутують про її відповідність стандартам невтручання в останнє). Отже, основні засади публічно-приватного партнерства надсилу застосовуються в США і частенько тлумачаться як альтернатива: замість правоохоронних органів інтернет контролюють провайдери. Зокрема, система непогано спрацьовує щодо виявлення фактів поширення дитячої порнографії (легше залучати до цієї справи провайдерів, ніж одержувати ордери на обшуки та отримання доступів до банків даних)...

Єдине, в чому погоджуються між собою автори "полярних" точок зору на кібернетичні загрози, це в тому, що кібервторгнення можуть успішно застосовуватися для шпіонажу. Саме цей момент створює великий ризик для систем національної безпеки: значно більший, ніж звичайні кібератаки. Такі дії матимуть латентний характер, можуть бути довготривалими в часі, ніхто не буде з показною бравадою вихвалятися своїми можливостями використання інтернету для збирання інформації про потенційні цілі. Розвідувальні служби зможуть не лише одержувати користь від інформації, що є відкритою для доступу в інтернеті, а й скористаються будь-якою можливістю таємного проникнення через комп'ютерні мережі з метою збирання інформації, не призначеної для публічного ознайомлення. "Це суттєво відрізняється від зламування, оскільки у випадку успішного проникнення до ворожої мережі, терористична група чи розвідувальна служба буде поводитися настільки скромно та тихо, наскільки можливо <...> вони створюватимуть збоїв у роботі... а спокійно збиратимуть інформацію "в тіні"" [1]. Інакше кажучи, ступінь продуктивності шпіонського ремесла підвищиться (вже підвищився) суттєво.

І все ж таки, зважаючи на популярні думки — одних дослідників, переконаних, що не можна заподіяти суттєвої шкоди комп'ютерним системам на рівні інфраструктур, інших, які вважають, що електронний Перл-Харбор — справа вже недалекого майбутнього, — беручи до уваги обидві точки зору, хочеться мати відповідь на запитання: наскільки вразливі для кібервторгнень комп'ютерні мережі? Переконують, що в індустріально розвинених країнах мережі доволі стійкі до кібератак. А в Україні? В Україні заспокоює те, що мережі не вельми розгалужені та розповсюджені. Можемо сподіватися, що маємо часову "фору", протягом якої індустріально розвинені країни вдосконалять технології захисту власних мереж від кібератак, а потім, у міру розвитку мереж вітчизняних, ми зможемо перейняти в "просунутих" сусідів їхні ноу-хау. Сподіватися можемо...

Політизація хакерів — новітнє явище серед користувачів інтернету

За узвичаєною класифікацією, хакери поділяються на піратів, броузерів (англ. *brouser* — той, що проглядає) та крекерів. Пірати — непрофесіонали, найменш технічно досвідчені, їхня діяльність обмежується хіба що здатністю проникати до систем (їх налічується близько 90 %). Броузери — люди, які мають значно ширші технічні знання та можливості, вони отримують недозволений доступ до файлів інших людей, до чужих систем, але суттєвої шкоди не завдають (близько 9 %). 1 % хакерів припадає на керкерів — це, по суті, кіберзлочинці, котрі мають великі технічні можливості, знання та навички. Саме вони шкодять найбільше: від копіювання файлів до цілковитого нищення програм та систем. Український дослідник О. Чернавський більш детально аналізує хакерську спеціалізацію [1] Він говорить про хакерів-дослідників, хакерів-зламників, хакерів-вандалів, крекерів, піратів, кібертерористів, вірмейкерів (тих, хто працює над створенням комп'ютерних вірусів), кардерів (махінації з кредитними картками та банкоматами), фрікерів (спеціалізуються на незаконному підключенні до телефонних мереж). Вітчизняний дослідник В. Голубєв наводить статистичні співвідношення різних мотивів при вчиненні комп'ютерних злочинів. Так, експертна комісія Інтерполу зазначила, що корисливі мотиви присутні в 66 % випадків, політичні — в 17 %, дослідницький інтерес превалював у 7 % випадків, хуліганство — 5 %, помста — 4 % [6].

Незаперечним є те, що кіберактивісти сьогодні намагаються перенести до кіберпростору реальні рухи громадянської непокори. На думку Д. Деннінг, інтернет сьогодні вважається впливовим важелем для зміни курсів внутрішньої та зовнішньої політики будь-якої держави і передбачає в цьому аспекті три види діяльності: 1) соціальна активність; 2) хактивізм (від англ. *hack* і *activism*); 3) кібертероризм [7].

Перший вид діяльності — соціальна (політична) активність — не передбачає якоїсь підривної діяльності, а полягає в різних формах висловлення

своїх поглядів. Форми можуть бути різними: створення сайтів, розсилання поштових повідомлень, написання електронних публікацій, обговорення проблем, створення певних коаліцій на форумах та в чатах організація діяльності останніх.

Друга категорія соціально та політично активних користувачів мережі інтернет використовує переважно незаконні методи діяльності. Їхні дії змінюються в межах делікт-злочин, але порушення нормальної роботи певних ділянок мережі, спричинені цими діями, не завдають суттєвих збитків. Приклади — страйки в інтернеті, цілеспрямовані бомбардування чиєїсь електронної пошти, вебхакерство, комп'ютерні злами, віруси та "черв'яки". *Хактивізм* — це поєднання соціальної (політичної) активності та хакерства. Останні використовують спеціалізоване програмне забезпечення. Переважна більшість соціально активних хакерів прагне якомога більшого інформування про свої дії, тому широко використовує медіаскладову.

Страйки в інтернеті полягають у відвідуванні хакерами певного сайту та створенні такого трафіку, за якого інші користувачі не можуть цей сайт відвідати. Під час передвиборних кампаній різних років українські політики відчували на собі дії хакеристів: їхні персональні сайти не працювали і по кілька діб, і протягом тижня. Одним із найвідоміших фактів страйку була атака 2007 року на сайт колишнього народного депутата політолога Дмитра Видріна. Результатом стали заголовки в інтернеті на кшталт "Видріна вбито!" — таким чином політик використав неприємний факт кількаденного страйку та зробив собі на цьому PR. До речі, дуже нетривіальний хід, коли медіаскладова стала значно ефективнішим засобом не для хакеристів, а для їхньої жертви.

Бомбардування електронної пошти, яке ще називається "роїнням" (від англ. — *swarming*). Одна справа, два-три листи на сайт політика, що передбачає зворотний зв'язок. Інша справа — тисяча або кілька тисяч листів, надісланих одночасно за допомогою спеціальних програм: поштова скринька переповнюється, інші відвідувачі сайту не можуть із її власником зв'язатися, відсутність транспарентності в діях політика та його політичної сили дратує, викликає невдоволення, в цьому починають вбачати політичний підтекст. Як наслідок — певні збитки для політичного рейтингу. Якщо такі дії хакеристів помічають не відразу або ж вони системні, фактор часу — за тиждень чи за кілька днів перед виборами — може стати фатальним [3].

Під час війни у колишній Югославії сторони з обох боків конфлікту бомбордували електронну пошту урядових сайтів США. У відповідь патріотично налаштований хакер із Каліфорнії вирішив заблокувати сайт уряду Югославії, надіславши на функцію зворотного зв'язку понад 500 000 повідомлень. Сайт "упав", а інтернет-провайдер каліфорнійця порвав зі своїм користувачем договірні стосунки через порушення антиспамової політики кампанії.

Приклади соціальної та політичної активності хакеристів з інших країн вражають. А політичну складову українських знавців роботи інтернету в нас ставлять під сумнів: на нашу думку, більшість так званих хакеристів в Україні використовують свої спеціальні знання з метою збагатитися і працюють на замовлення представників політичних чи бізнесових кіл.

Комп'ютерні віруси та "черв'яки" використовуються хактивістами, зазвичай, для розповсюдження месиджів, що містять протестні заклики та пошкоджують програмне забезпечення або ж можуть завдати комп'ютеру фізичної шкоди (перепрограмувати його на самознищення). З історії, перший протест, пов'язаний з використанням "черв'яка", стався 1989 року: раптом учені Адміністрації національної аеронавтики та космонавтики США побачили картинку з надписом: "Черв'яки проти ядерних убивць! Ви говорите про мир для всіх, а самі готуєтеся до війни". Таким чином протестувальники вимагали зупинити запуск на Юпітер космічного човника з обладнанням, що мало живитися від радіоактивного плутонія. Так ніхто й не довідався, що то за автор "черв'яка" з посланням... Але може здатися, що хакеристи — це просто бешкетники, які мають спеціальні знання, така собі секта втаємничених, мета якої налагодити дієвий громадський контроль на рівні користувачів інтернету. На жаль, дії хакеристів межують із діями, що мають ознаки кібернетичного тероризму. Так, 1999 року ізраїльський підліток Нір Зигдон оголосив, що знищив іракський урядовий сайт. Невдовзі хлопець став мало не національним героєм. Підліток дав інтерв'ю: "... сайт містив брехню про США, Велику Британію та Ізраїль, а також безліч жахливих заяв про євреїв... Я подумав, що коли Ізраїль боїться вбити Саддама Хусейна, то я зможу, принаймні, знищити його сайт!". Хитромудрий хактивіст послав на іракський сайт комп'ютерний вірус у додатку до електронної пошти. Не було гарантії, що службовці, які опікуються сайтом, відкриють лист та подивляться заражене вкладення. Тоді Нір Зигдон вдався до хитрощів: він написав у листі, що є палестинським прихильником Саддама і створив вірус, здатний знищити ізраїльські сайти. Довірливі іракці відкрили додаток, і вірус знищив їхній сайт протягом години. Максимум, що хакерист отримав у відповідь — це побажання "піти до дідька", відправлене йому іракськими потерпілими...

Вірусова та "черв'якова" активність в Україні доволі висока. Проте колективів, що цілеспрямовано продукують віруси та розповсюджують їх, переслідуючи якусь мету, не зареєстровано. Зараження комп'ютерів і систем відбувається на рівні про-

вайдерів, котрі нехтують безпекою своїх користувачів, або ж на рівні пересічних інтернет-користувачів, котрі взагалі не користуються антивірусними програмами або ж не слідкують за їхнім регулярним поновленням. Хакери успішно сканують інтернет і вишукують заражені комп'ютери, з хибними конфігураціями і належним чином не захищені. Такі машини можуть стати частиною "мережі ботів" (бот — це почасти автономна комп'ютерна програма, що контролюється віддаленим користувачем та здатна заражати комп'ютери). Часто виявляється, що хакер-одинак контролює тисячі заражених комп'ютерів, у різних куточках планети. Він може давати команди комп'ютерам із своєї "мережі ботів" та через зашифрований комунікаційний канал відслідковувати всі дії власників заражених комп'ютерів — сканувати їхню інформацію, переписувати файли, передавати копії їхніх даних або ж давати їм команду, одночасно здійснивши атаку на будь-який комп'ютер-мішень або мережу (так сталося із сайтом Д. Видріна). Власники про це навіть не здогадаються...

Кібертероризм — це терористичні дії в кіберпросторі та політично активне хакерство, що вчинені з метою завдати серйозних збитків життєдіяльності людини та економіці країни. Це можуть бути незаконні входження в систему управління польотами, щоб спричинити зіткнення літаків або влаштувати їм інші аварії тощо. Вважається, що термін "кібер-тероризм" зародився 1980 року завдяки науковцю з Інституту безпеки та розвідки (США, Каліфорнія).

Як зазначає Д. Деннінг, ступінь збитків від діяльності кожної із зазначених категорій наростає від першого до третього (від соціальної активності до кібертероризму), але при цьому збільшення ступеня збитків не означає підвищення рівня політичної ефективності, тому що, наприклад, електронний заклик до мільйонів користувачів із демонстрацією такого ж мільйона підписів може вплинути на політичні процеси сильніше, ніж напад, що перебив нормальну роботу якоїсь служби забезпечення життєдіяльності.

У терміна "кібертероризм" немає універсального визначення. Серед теоретиків та практиків триває з цього приводу дискусія. Найвдалішими нам видається визначення, запропоноване Клайєм Вільсоном (США) [8]. Кібертероризм — це використання комп'ютерів як зброї політично мотивованими міжнародними або національними групами чи таємними агентами, котрі завдають або загрожують завдати шкоди чи посіяти паніку, з метою вплинути на населення або уряд для зміни політики. Додамо, що метою кібертерористів можуть бути політична та економічна дестабілізація, саботаж, привласнення військових та цивільних активів з політичною метою, злам комп'ютерних мереж, кібервійна тощо.

Способи використання інтернету кібертерористами:

Оприлюднення своєї діяльності, пропаганда, психологічна війна. Інформація може подаватись як історична довідка, як відомості з біографії лідерів, маніфестів, інших програмних документів тощо. Для ведення психологічної війни вдаються до таких засобів, як дезінформація, погрози, публікація на веб-сайтах зображень, що наводять жах. До цього ж виду діяльності можна віднести медіа-тероризм.	***Пропаганда. Оприлюднення. Політичні акції. Інформаційно-психологічний вплив (війна). Шахрайство та маніпулювання даними. Дезінформація. Робота з чутками. Медіа-тероризм.***
Збирання грошей для фінансування діяльності. Відповідні заклики можуть напряму міститися на сайтах, а потім надходити у вигляді спамів на електронну пошту відвідувачів. Деякі терористичні групи фінансують свою діяльність і за допомогою шахрайських інтернет-схем (наприклад, так звані "нігерійські листи").	***Фінансування. Збирання коштів. Контроль.***
Поліпшення власної організаційної структури, мережі; децентралізація, багатоканальність. В ідеалі, терористична група не повинна мати одного лідера, котрий легко стане мішенню: всередині групи немає жорсткої ієрархії. З метою реалізації завдань група використовує новітні інформаційні та телекомунікаційні технології. Відмовившись від фізичного місця для зустрічей, новітні терористичні групи створюють свої товариства на чатах і сайтах.	***Планування діяльності. Координація діяльності. Безпечні комунікації. Анонімні й таємні комунікації. Формування субординаційних зв'язків. Організація терористичних мереж. Управління і контроль.***
Онлайн рекрутинг. Якщо рекрут не впевнений у своєму бажанні вступити до групи, або група не впевнена в ньому, рекрута відправляють у чат, де з ним можуть спілкуватися (сканувати, тестувати) інші члени товариства. Потім його можуть відправити на інший чат для детальнішої перевірки і, нарешті, дозволити фізичний контакт із членом групи.	***Вербування. Мобілізація.***
Інтернет – це безмежна цифровою бібліотекою, тому його легко використовувати для збирання інформації. В посібнику Аль-Каїди, знайденому в Афганістані, йдеться про те, що, «використовуючи відкриті ресурси, можна зібрати мінімум вісімдесят відсотків інформації про ворога». Спеціалісти вважають (Г.Вейнманн, США), що простий спосіб пошуку за ключовими словами в газетах і журналах (контент-аналіз) може дозволити	***Пошук інформації.*** ***Збирання інформації.*** ***Примітка.*** Управління охорони довкілля США видалило зі свого сайту тисячі планів ризик-менеджменту, які стосуються небезпечних хімічних заводів. Мінтранс США зняло інформацію, що містить мапи трубопроводів. Центр з контролю та попередження захворювань зітер Доповідь про хімічний тероризм. Уся перелічена інформація була потенційно корисною для терористів.

	В Україні ніхто не проводить моніторингу сайтів органів державної влади та управління щодо їхнього наповнення інформацією, що може прислужитися злочинцям на будь-який штиб. 1990 року в Україні теж було скасовано інститут цензорів у друкованих та електронних медіа.
В інтернеті вільно розміщені посібники на тему: "як зробити" (бомби, отрути тощо) пристрої, що можуть призвести до ураження великої кількості людей. ("Практикум саботажу", "Енциклопедія джихаду" - ці книги пропонують детальні інструкції про те, як створити підпільну організацію та здійснити терористичні атаки; ""Керівництво терориста", "Як робити бомби: книга друга").	***Розподіл інформації. Поширення інформації.***

За ініціативою Росії, 1998 року ООН ухвалила Резолюцію 53\70, що стосується кіберзлочинності, кібертероризму та кібервійни. Ця резолюція – перший крок до обміну досвідом між державами-членами світового співтовариства: держави-члени мають інформувати Генерального секретаря про свої погляди та оцінки щодо: 1) проблем інформаційної безпеки, 2) визначення основних понять, пов'язаних з інформаційною безпекою, 3) розвитком міжнародних принципів, що поліпшують глобальний інформаційний простір і телекомунікації та допомагають боротися з інформаційним тероризмом, зі злочинністю. Починання це, безперечно, позитивне. Одна біда: авторитет та "вага" ООН у світових міжнародних відносинах невпинно знижується. Пророкують або повну модернізацію цієї мега-міжнародної організації, або ж її самоліквідацію, як свого часу це відбулося з Лігою Націй.

Які ж основні ознаки сучасного кібернетичного тероризму та кібернетичної злочинності?

Перша ознака – територіальна. Побутує думка, що терористичні групи процвітають у тому середовищі, де молодь має обмежені умови для розвитку в межах суспільства. Інакше кажучи, йдеться про суспільства нерівних, обмежених можливостей, притаманні державам із низьким розвитком демократичних інститутів. "Легкість комунікацій у сучасному світі робить місцеперебування дійових осіб не таким уже й суттєвим чинником, як раніше. Використання "дірок" у системах безпеки дає терористам та організованим злочинним угрупованням можливість працювати не з домашніх територій, а з непередбачуваних місць" [9]. Отже, більшість транснаціональних злочинних угруповань і терористичних організацій базуються в країнах із перехідною економікою та в країнах, що розвиваються. Це пояснюється слабкою каральною системою зазначених держав, недосконалим законодавством, корупцією в органах державної влади та управління, зокрема в правоохоронних органах. Вважається загальновизнаним фактом, що більшість висококваліфікованих технічних спеціалістів, котрі, ймовірно, готові прислужитися кримінальним та терористичним структурам, проживають у країнах колишнього СРСР та в Індії. Зрозуміло, що одна шоста суші, яку мав колишній Радянський Союз та, на додачу, Індія – це вельми проблемні в соціально-економічному сенсі території. Водночас доволі лояльною щодо контролю за телекомунікаційними системами є така високорозвинена країна, як Німеччина. Більша частина терористичної змови, яка мала місце 11 вересня 2001 року (коли було зруйновано два хмарочоси в Нью-Йорку) готувалася якраз у Німеччині, закони якої уможливлюють якнайширшу таємну діяльність. Справа в тому, що Німеччина повсякчас намагається спростувати звинувачення з боку громадськості в тотальному контролі, що був притаманний державному апарату часів нацизму. Епоха надзвичайних повноважень поліції за Гітлера перейшла в свою цілковиту протилежність: сьогодні терористи мають змогу використовувати в цій країні телекомунікаційні системи, практично не ризикуючи, що їх викриють.

Що ж до України, то тут коїться велика кількість фінансових злочинів, вчинених за посередництва комп'ютерів та інтернету. І все ж, хоч Україну вважають джерелом цих злочинів, не можна з точністю стверджувати, що саме громадяни України їх вчиняють. Так, чимало іноземців використовують інтернет-ресурси України, а в світовому "кібертоваристві" Україна давно має імідж держави з обмеженими можливостями протидії кіберзлочинам. Додамо, що корупційні зв'язки дають змогу багатьом іноземцям тривалий час нелегально перебувати на території нашої держави.

Друга ознака – постійне вдосконалення способів скоєння злочинів (або терористичних актів) за допомогою кіберпростору.

І терористи, і транснаціональні злочинні угруповання (колумбійська мафія й та, що експортувалася з теренів колишнього СРСР) використовують новітні інформаційні технології: це і стільникові та супутникові телефони, і комп'ютери з чималими можливостями, і приватні інформаційні мережі. Великого значення в їхній діяльності набуває анонімність та шифри (методики шифрування та анонімайзери). Дедалі більшу кількість їхніх листів не можуть розшифрувати ні представники правоохоронних органів, ні розвідок. Останні технології взагалі дозволяють робити повідомлення невидимими для інших користувачів (спецслужб, наприклад) інтернету. Звісно, анонімність в інтернеті, з од-

ного боку, є найдемократичнішим способом отримання та надання інформації. З другого боку, ця особливість інтернету відкриває безліч можливостей для використання її кримінальними елементами.

На перший погляд може здатися, що хакери та кібертерористи діють автономно. Насправді ж між ними прослідковується тісний зв'язок. Особливо, якщо взяти до уваги народження такого явища, як хактивізм. Оперативна інформація, зібрана правоохоронними відомствами багатьох країн, містить у собі відомості про те, що на хакерському "чорному ринку" продаються дані про дірки в програмному забезпеченні тих чи тих користувачів інтернету. Складаються поступово і тарифи на такі послуги: так, список з 5000 адрес заражених комп'ютерів (із "мережі ботів") коштує близько 500 доларів. Хто купує таку інформацію? Компанії-спамери, уряди деяких держав та, зазвичай, організовані злочинні угруповання.

"Темний бік" інтернету

Деякі дослідники "розрізняють" два поняття: організована злочинність та кібернетична злочинність. Зокрема американець Ф. Вільямс вважає, що ці поняття ніколи не стануть синонімами. "Організована злочинність продовжуватиме свою діяльність у реальному світі, а не в кіберпросторі, а більшість кіберзлочинів буде скоєно індивідумами, а не злочинними організаціями" [10]. Ф. Вільямс передрікає хіба що збільшення ступеня кореляції між цими явищами. Ми дозволимо собі не погодитися з таким підходом. Скоєння системних злочинів потребує серйозної технічної, матеріальної та організаційної підготовки, залучення спеціалістів із різних галузей. На нашу думку, кіберпростір вже став полігоном якраз для організованих злочинних угруповань, їхні дії давно набули транснаціонального характеру. Звісно, одинаки-кіберзлочинці, вільні від будь-яких злочинних зв'язків поза своїм персональним комп'ютером, трапляються та будуть траплятися. Однак викриття їх полегшено через відсутність продуманої системи відхідних маневрів, а збитки від їхніх дій не мають тотального характеру. Ефективність функціонування в кіберпросторі організованого злочинного угруповання значно підвищує ефективність її діяльності.

Конвенція Ради Європи з боротьби проти кіберзлочинності (2001 рік) поділяє цей вид злочинності на чотири категорії: 1) злам комп'ютерних систем, 2) шахрайство, 3) заборонений контент (расистські сайти, дитяча порнографія), 4) порушення авторських прав [11].

Отже, сьогодні основними сферами злочинної діяльності в кіберпросторі є крадіжки та шахрайства, дитяча порнографія, проведення допоміжних операцій із торгівлі людьми та органами, наркоторгівля. За деякими оцінками, світова торгівля наркотиками перевищує масштаби світової торгівлі нафтою та досягає рівня 400 млрд доларів на рік. Так, транснаціональні наркоторгівці широко використовують можливості шифрування, паролів, стискання файлів, стенографії, віддаленого зберігання документів на серверах, анонімної пошти, спілкування на відкритих форумах за допомогою тихтаки шифрів, комп'ютерного вторгнення та петляння через треті системи, кодованого зв'язку з мобільних і супутникових телефонів, комп'ютерних анонімайзерів, про які йшлося вище. Інтернет використовують для ефективної логістики — відслідковуються транспортування, відвантаження товару, швидко змінюються маршрути перевезення, якщо виникає небезпека розкриття поліцією незаконних операцій різних країн (зокрема, завдяки опанування новітніми комп'ютерними технологіями колумбійські наркоторгівці почали більш успішно постачати наркотики до США, втрати від перехоплення наркотрафіку поліцією складають лише 30—40 %).

Торгівці живим товаром виготовляють за допомогою комп'ютерних технологій підробні документи, що посвідчують особи тих, хто потребує незаконного перетину кордонів (ці документи часом бувають такі якісні, що відрізнити їх від справжніх годі навіть співробітникам правоохоронних органів).

Крадії та шахраї теж суттєво підвищили ефективність своєї діяльності (йдеться про розповсюдження електронного банкінгу та електронної торгівлі). Так, на острові Сицилія, де панує розгалужена мережа мафіозних кланів, група з двадцяти злочинців налагодила контакт із так званим інсайдером — співробітником Банку Сицилії. Завдяки співпраці було створено цифровий клон одного з інтернет-компонентів банку. Планувалося викрасти близько 400 мл доларів, асигнованих Євросоюзом на регіональні проекти розвитку Сицилії. Операція мала бути успішною. Викрити злодіїв пощастило випадково, — просто один із членів угруповання доброхіть сповістив поліцію про підготовку "крадіжки століття". Ще один приклад. 2000 року невідомі запустили модифікований вірус "Love Bug" з метою отримати доступ до паролів Об'єднаного Швейцарського банку та двох банків США. Поліція обох країн викрила злочинця — ним виявився студент із Філіппін. Законів, за якими студента слід було притягнути до відповідальності, на Філіппінах немає. Для того щоб злочинці були покарані, в більшості випадків має застосовуватися подвійна криміналізація, згідно з якою вчинена дія трактуватиметься як злочин в обох державах...

Шахрайство через знайомства в інтернеті

Щороку розкривають транснаціональні злочинні групи, що виманюють чималі кошти з охочих познайомитися та одружитись за кордоном. Цей вид злочину найчастіше практикується у країнах ко-

лишнього СРСР. "Наречені" тривалий час листуються з женихами зі США, Канади, Нової Зеландії, Австралії. Схема шахрайства розрахована на довірливих іноземців. Незабаром у ході листування в женихів просять кошти на оформлення віз, паспортів та квитків. Суми коливаються від 300 до 2500 доларів. Насправді, замість дівчат із женихами ведуть листування кілька молодих хлопців із непоганим знанням психології. Після одержання певної суми від іноземця листування припиняється, профайл "нареченої" зникає з сайту.

Поширення дитячої порнографії

Дитяча порнографія "молодшає" з кожним роком. Сьогодні в інтернеті дедалі частіше можна знайти сцени сексуального насильства над дітьми віком 3–5 років. "Крім фізичних та моральних збитків, що їх завдають самим дітям, перегляд таких зображень може спровокувати в людей з несформованою та порушеною психікою асоціальну поведінку, що штовхає до злочинів" [12]. Вважається, що інтернетом розповсюджується до 75 % всієї дитячої порнопродукції. Так, відомий випадок появи в Мережі відеоролика, в якому двоє збоченців вступають у статевий зв'язок із малолітньою дівчинкою, в процесі якого завдають їй колоторізаних поранень, відтинають вуха, вибивають очі. На цей кліп звернули увагу співробітники ФБР США, експерти якого встановили, що події в кліпі реальні, а не імітовані. Американці отримували доступ до ролика за 400 доларів зі спеціалізованого російського сайту. За результатами розслідування до смертної кари було засуджено тих, що виготовили ролик (громадяни однієї з країн Південно-Східної Азії), а споживачів цієї продукції з різних країн теж було засуджено до тривалих термінів ув'язнення (від 10 до 120 років, залежно від суворості законодавства). Співучасника з Росії притягнути до відповідальності не вдалося через недосконаліть кримінального закону РФ, який не передбачає самого поняття "дитяча порнографія".

Азартні ігри онлайн. Реклама послуг сексуального характеру в інтернеті. Віртуальні казино. Злочини проти інтелектуальної власності.

Так звана "піратська" діяльність – реалізація через Інтернет нелегальних копій програмних продуктів, а також зазіхання на об'єкти виняткових прав: патенти, торговельні марки, зловмисна реєстрація доменних імен, схожих із відомими брендами.

Викрадання онлайн інформації, що являє собою державну таємницю – це загроза державній безпеці.

Розповсюдження інформації расистського характеру, а також такої, що може розпалювати міждержавну та міжнаціональну ворожнечу створює велику соціальну загрозу, котра переходить у площину політичну.

Незаконне вторгнення в приватне життя, листування, переговори, нелегальне копіювання інформації, а також її знищення. Незаконне одержання інформації комерційного характеру може призвести до великих збитків її законного власника. Крім того, не зрідка трапляються випадки розміщення в Мережі інформації у вигляді образ та наклепів, що ганьблять честь, гідність та ділову репутацію різних осіб. Негативний соціальний ефект має інформація, що не є рекомендованою для перегляду певним верствам населення – наприклад, інформація еротичного або порнографічного характеру. Правопорушення в інтернеті можуть торкатися й інтересів третіх осіб, які не є користувачами Мережі та навіть не знають про її існування.

Сьогодні можна стверджувати, що оформленого характеру набула криміналізація мережі інтернет за такими суб'єктами: 1) держави (уряди, силові структури, спецслужби тощо); 2) терористичні групи; 3) громадські організації, партії, громадські та релігійні рухи; 4) корпорації; 5) кримінальні угруповання; 6) приватні особи.

Правове регулювання інтернет-відносин

Спеціалісти називають п'ять основних напрямів правового регулювання: 1) захист особистих даних та приватного життя в Мережі; 2) регулювання електронної комерції та інших угод і забезпечення їхньої безпеки; 3) захист інтелектуальної власності; 4) боротьба проти протиправного змісту інформації та протиправної поведінки; 5) правове регулювання електронних повідомлень. Разом з тим, слід зазначити, що правового регулювання відносин в інтернеті дотримуються далеко не всі країни, насправді існують суттєві відмінності в правовому регулюванні та правозастосовній практиці. Як таке поняття "кіберзлочини" ("комп'ютерна злочинність"), зокрема в Україні, є незвичним, уніфікованого його тлумачення поки що не вироблено. Оскільки Кримінальний кодекс України не передбачає застосування аналогій, а діяння може бути визнане злочином тільки після включення його до кримінального закону, відсутність у цій галузі правового регулювання призводить до того, що саме поняття "кіберзлочинність" переходить до сфери явища соціального.

Висновки

Безперечно, криміналітет отримав користь від глобалізаційних процесів у світі. Особи, що перебувають поза законом, мають такий статус лише за наявності законів. Як відомо, все, що законом прямо не заборонено, вважається дозволеним. Законотворчість більшості країн не встигає за бурхливим розвитком відносин у кібернетичному просторі. Злочинці, вочевидь, отримують вигоди від дедалі більше відкритих кордонів, більшої мобільності та більш безпечних комунікацій. Розвитком комунікацій і прогресу скористалися не лише законні корис-

тувачі інтернету, а й ті, хто намагається завдати шкоди — як особистої, так і політичного характеру. Інтернет надав безліч можливостей для легального бізнесу, збільшивши швидкість та легкість виконання угод. Витрати при цьому мінімізувалися, якість стала суттєво вищою. У цей же час кримінальний світ знайшов для себе переваги паралельного існування з легальним технократизованим бізнесом.

Інтернет має транскордонний характер, тому уможливлює одержання максимальних прибутків за умов мінімального ризику. Відсутність державних кордонів робить кіберпростір привабливим для злочинних угруповань: через відмінності в юрисдикціях різних держав, недосконалість законодавства — злочини розслідуються повільно, деякі розслідування втрачають сенс уже на перших етапах. Кіберзлочини мігрують у бік тих територій, де практично немає відповідних законів або немає можливості ефективно застосовувати ці закони. На жаль, Україна належить до таких держав. Тому світове співробітництво в означеному контексті має першочергово перейти в площину уніфікації національних законів. На сьогоднішній день превалює підхід, за якого міжнародне співробітництво обмежене тим, що діяння криміналізоване суто в національній юрисдикції, і лише в поодиноких випадках діє правило подвійної криміналізації, за якого вчинене визнається злочином в обох державах.

Робота у сфері модернізації законодавства потребує термінової активізації. Звісно, деякі колективи уже близько десяти років працюють над цим питанням. Так, найвідомішим документом є Проект Концепції стратегії і тактики боротьби з комп'ютерною злочинністю в Україні, розроблений Міжвідомчим науково-дослідним центром із проблем боротьби з організованою злочинністю (2001 рік). Але на жаль, дослідження науковців, які спеціалізуються на згаданій проблематиці, надто далекі від тих людей, котрі відповідають за натискання кнопок у Парламенті під час голосування щодо внесення змін та доповнень до чинних законодавчих актів. Зокрема, в українських законах мають бути прописані такі злочинні дії, як вторгнення в комп'ютерні мережі, порушення цілісності мереж, одержання незаконного доступу до мереж, комп'ютерна диверсія, неправомірне перетину комунікацій, комп'ютерний шпіонаж, кібертероризм, загроза завдати тілесні ушкодження чи скоїти вбивство через інтернет, кіберпереслідування (наприклад, через електронну пошту), дитяча порнографія (створення порнографічних матеріалів за участю неповнолітніх, поширення цих матеріалів), протиправне порушення володіння в кіберпросторі (наприклад, зазіхання на власну інтернет-сторінку або веб-сайт, портал), кіберкрадіжка (привласнення коштів, корпоративний шпіонаж, плагіат, піратство, крадіжка персональних даних тощо), кібершахрайство, кібервандалізм (злам мережі та знищення програмного забезпечення, злам веб-серверів чи веб-сторінок, організація DOS-атак, що паралізують роботу сервера та перекривають законним користувачам доступ до його ресурсів). Доки буде існувати проблема кваліфікації злочину, котра полягає в тому, що злочин скоєно у "віртуалі", а наслідки його настають "в реалі", доти чимала кількість злочинців у процесі переведення справи з віртуальної площини до площини реальної уникатимуть покарання взагалі.

"Діяльність з протидії кіберзлочинності в Україні повинна мати системний та комплексний характер. Потрібно будувати цю роботу на базі чіткої взаємодії всіх правоохоронних органів, запроваджувати ефективні методи розкриття та профілактики такого виду злочинів, а також вдосконалювати правові норми. Жодна держава не може протистояти цьому злу самотужки. Сьогодні доконче треба активізувати міжнародне співробітництво у цій сфері. <...> Боротьба з комп'ютерним тероризмом, як і з тероризмом взагалі, не може бути справою окремих держав, тому слід забезпечити взаємодію спецслужб, у тому числі й національної служби безпеки та спеціальних підрозділів з боротьби проти тероризму на національному, регіональному та міжнародному рівнях" [6]. Доки власне законодавство не буде "підтягнуте" до реперних точок того явища, характеристику якого нами було наведено вище, про гармонізацію вітчизняного законодавства з міжнародним годі й говорити.

На наш погляд, є кілька основних завдань, виконання яких потребує комплексного підходу. Перше: систематичне збирання розвідувальних даних про потенційні кібертерористичні загрози та ресурси. Друге: забезпечення захисту життєво важливих елементів вітчизняної інфраструктури (передбачає окрему статтю фінансування органів державної влади та управління). Третє: розробка технологій превенції комп'ютерних нападів (співпраця з науковими та науково-дослідними установами й організаціями). Четверте: зведення до мінімуму прогалин у вітчизняному законодавстві. П'яте: зниження рівня латентності комп'ютерних злочинів (сьогодні приблизно 80 % комп'ютерних атак не тягнуть за собою звернення до правоохоронних органів). Шосте: припинити масове використання у різних сферах не захищеного належним чином програмного забезпечення. Сьоме: створити загальнодержавну систему захисту інформації. Восьме: активізація громадської думки в дусі неприйняття аналізованого явища та активної протидії йому.

Без сумніву, кращим способом боротьби проти злочинності в галузі високих технологій є самі високі технології та стимул науково-технічного прогресу, що має слугувати справі протидії кіберзлочинності. Фінансування високих (прогресивних)

технологій у сфері боротьби з кіберзлочинністю має стати державним пріоритетом уже сьогодні.

1. *Льюїс, Дж.* Оцінка ризику кібертероризму, кібервійни та інших кіберзагроз // Центр стратегічних та міжнародних досліджень, США, Колумбія / James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. Washington, D. C. December. — 2002. — <http://www.crime. vl.ru/index. php?p=1104&more=1>.

2. *Морозов, І.* Політичний екстремізм в Інтернеті // Политическая коммуникация в постсоветской России: проблемы формирования и парадигмы развития : материалы секции "Политическая коммуникация" Третьего всерос. конг. политологов [28—29 апреля 2003 г.]. — М. ; Улан-Удэ : Изд-во ОАО "Республиканская типография", 2003. — С. 302—308. — <http://morozov.vlz.ru/library-/vstphtm>.

3. *Гриняев, С.* Концепция ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. — 2002. — № 2. — С. 11—15.

4. *Старостин, В.* Все под контролем? // Столичные новости. — 2007. — № 47—48. — 18—24 груд.

5. *Чернавський, О.* Анализ формирования компьютерного андерграунда в контексте современной киберкультуры // Компьютерная преступность и кибертерроризм. — Запорожье, 2004. — № 2. — С. 58—65.

6. *Голубєв, В.* Проблемы противодействия киберпреступности и кибертерроризму в Украине. — <http://crime-research.ru> [січ. 2005 р.].

7. *Деннінг, Д.* Активність, хактивізм та кібертероризм: Інтернет як засіб впливу на зовнішню політику, Нью-Йорк, 2001 / Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy by Dorothy E. Denning, Georgetown University. — <http://www.crime.vl.ru/ index. php?p=1114&more=1>.

8. *Clay, W.* Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. — <http:// www.fas.org/sgp/crs/terror/index.htm>.

9. *Шеллі, Л.* Організована злочинність, тероризм та кіберзлочинність / Louise I. Shelley. Organized Crime, Terrorism and Cybercrime, 2004 // Security Sector Reform : Institutions, Society and Good Governance. — <http:// www. crime.vl.ru/index.php?more=1&c=1&tb=more928>.

10. *Уільямс, Ф.* Організована злочинність та кіберзлочинність: взаємодія, тенденції, протидія / Phil Williams. Organized Crime and Cybercrime: Synergies, Trends, and Responses, University of Pittsburgh, Global Issues. — August. — 2001. — Volume 6. — Number 2. — US Department of State — USA (2001). — <http://www.crime.vl.ru/index. php?p =929& more=1&c= 1&tb=1&pb=29>.

11. *Про* боротьбу з кіберзлочинністю : Конвенція Ради Європи. — 2001.

12. *Сухаренко, А. Н.* Распространение детской порнографии через сеть Internet / А. Н. Сухаренко // Владивостокський центр дослідження організованої злочинності. — <http://www.crime.vl.ru/index.php?p=1077&more=1>.

13. *Хартія* глобального інформаційного суспільства. — 2000.