

*В. Б. Дзюндзюк,
д.держ.упр., проф.,
завідувач кафедри політології та філософії ХарРІ НАДУ;
Б. В. Дзюндзюк,
студент ХНУРЕ,
м. Харків*

ПОЯВА І РОЗВИТОК КІБЕРЗЛОЧИННОСТІ

Розглянуто поняття кіберзлочинності та її складові, сутність кіберзлочинів, історію виникнення кіберзлочинності. Визначено етапи розвитку кіберзлочинності та події, що дали початок кожному з етапів. Дано актуальну класифікацію кіберзлочинів.

Ключові слова: кіберзлочинність, кіберзлочинці, віртуальний простір, Інтернет, кібертероризм.

З появою та розвитком всесвітньої мережі Інтернет з'явився і новий вид злочинності – кіберзлочинність, який з кожним роком набирає свої оберти і несе за собою серйозні, а часом, незворотні наслідки. Особлива увага приділяється кіберзлочинності, оскільки величезний технічний потенціал і безмежні можливості Інтернет все частіше в сучасних умовах можуть бути використані в злочинних цілях. Дії кіберзлочинців стають все більш майстерними, що становить реальну проблему для суспільства. Це загострює необхідність боротьби зі злочинами такого роду, створення комп'ютерних систем і технологій з підвищеним рівнем безпеки в мережі Інтернет, а також законодавчої бази, що дозволяє карати злочинців належним чином.

Теоретико-методичні та науково-практичні основи попередження дій кіберзлочинців були закладені у дослідженнях науковців В. Голубєва, А. Долгової, К. Касперськи, М. Кастельса, Т. Кесаревої, Л. Куракова, Р. Лемоса, А. Лукацького, І. Рассолова, С. Смірнова. Хоча усі науковці достатньо ґрунтовно викладають матеріал у своїх дослідженнях, необхідно все ж таки узагальнити накопичені знання, зануритися у саму історію виникнення та розвитку кіберзлочинності для можливості аналізу дій злочинців відносно розвитку технологій.

Мета статті – розглянути та визначити поняття кіберзлочинності, її складові та сутність кіберзлочинів, що допоможе попереджати та більш ефективно боротися з ними.

Кіберзлочинність – це злочинність в так званому «віртуальному просторі». Віртуальний простір (або кіберпростір) можна визначити як модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символічному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі [2].

На відміну від традиційних видів злочинів, історія яких налічує століття, таких як вбивство або крадіжка, кіберзлочинність явище відносно молоде і нове, яке виникло з появою мережі Інтернет. Слід зазначити, що сама природа мережі Інтернет є достатньо сприятливою для вчинення злочинів. Такі її властивості, як глобальність, трансграничність, анонімність користувачів, охоплення широкої аудиторії, розподіл основних вузлів мережі і їх взаємозамінність створюють кіберзлочинцям, які використовують Інтернет, переваги на всіх етапах скоєння злочину, а також дозволяють ефективно ховатися від правоохоронних органів.

Оскільки кіберзлочинність невід'ємна від інформаційної революції, то початок її відліку слід вести з шестидесятих років минулого століття. У 1962 р. професор Джон Ліклайдер (J.c.r. Licklider), опублікував свою концепцію широко розповсюдженої комп'ютерної мережі «Galactic Network». Дана концепція припускала, що в майбутньому з'явиться глобальна мережа, підключитися до якої зможе будь-який охочий, і що дана мережа з'єднає комп'ютерні системи по всьому світу. Крім загальної ідеї Ліклайдер детально описав основоположні принципи глобальної мережі, покладені пізніше в основу Інтернет.

Першим кроком власне до появи Інтернет стало створення комунікаційної мережі комп'ютерів ARPANet (Advanced Research Project Agency network), створеної за замовленням Міністерства оборони США. Ідея

даної розробки полягала в тому, щоб створити розподілену комп'ютерну систему без одного чітко вираженого центру, який можна було б вивести з ладу у разі ядерної війни, і яка складається з взаємозамінних сегментів [5]. Таким чином, вже тоді були закладені такі принципи нинішнього Інтернет, як *розподіленість* та *глобальність*.

Спочатку ARPANet складалась з чотирьох комп'ютерів, які розташовувалися в великих дослідницьких центрах. Мережа планувалася для передачі інформації і електронного листування, тому ніякі серйозні елементи, що обмежують доступ, в її структурі не присутні, оскільки появу комп'ютерних злочинців тоді ще не передбачали. Цю якість успадкує надалі і мережа Інтернет, що призведе до такої її якості, як «анархізм» [4]. Саме непродуманість питань безпеки і юридичного контролю при розробці технічних принципів мережі, породить ті проблеми, з якими світова спільнота зіткнеться в майбутньому, стане однією з головних причин широкого розповсюдження кіберзлочинності. Нижче хотілося б привести декілька фактів, що характеризують розвиток кіберзлочинності.

У 1970-х роках з'являються перші комп'ютерні злочинці, яких почали називати «хакерами». Важко точно сказати, хто саме був першим хакером, але в більшості літературних джерел для хакерів і про хакерів як перший професійний кіберзлочинець згадується Джон Дрейпер (John Draper), який також породив першу спеціалізацію хакерів, – фрікери (phreaker), скорочене від телефонний хакер (phone hacker). В рядах фрікерів у той час були навіть такі знамениті особи, як Стів Возняк (Steve Wozniak) та Стів Джобс (Steve Jobs), які в майбутньому заснували «Apple Computers». Вони налагодили виробництво пристроїв для злому телефонних мереж в домашніх умовах. І саме цей час можна вважати *початком розвитку кіберзлочинності*.

У 1983 р. в США в штаті Мілуокі відбувся перший арешт Інтернет-злочинця, про якого стало відомо громадськості. Приводом для цього послужив перший зареєстрований Інтернет-злом, здійснений шістьма підлітками, які називали себе «група 414» (414 – міжміський телефонний код Мілуокі).

Протягом дев'яти днів ними було зламано 60 комп'ютерів, серед яких були комп'ютери Лос-Аламоської державної лабораторії. Після арешту один з членів групи дав свідчення і інші її учасники отримали умовний термін покарання [8].

Взагалі, у восьмидесятих роках починає спостерігатися істотне збільшенні числа комп'ютерних атак. Так, якщо в 1988 р. було всього шість звернень користувачів Інтернет з приводу комп'ютерних атак в центр Інтернет-безпеки CERT, що відкрився в 1988 р., то в 1989 р. – 132, а в 1990 р. – вже 252. Кіберзлочинність перестає бути рідкістю, з'являються великі групи хакерів, і Інтернет починає використовуватися для ширшого круга злочинів. Це стає початком *другого етапу* в розвитку кіберзлочинності, що характеризується появою нових спеціалізацій Інтернет-злочинців.

У 1984 р. Фред Коен (Fred Cohen) опублікував відомості про розробку перших шкідливих комп'ютерних програм, які саморазмножуються, і застосував до них термін «комп'ютерний вірус». При цьому він написав програму, що демонструвала можливість зараження одного комп'ютера іншим.

У 1986 р. в США прийнятий перший комп'ютерний закон «The Computer Fraud and Abuse Act» [10], який забороняв неавторизований доступ до будь-якої комп'ютерної системи і отримання секретної військової інформації. Також цей закон захищав три види несекретної інформації: інформацію, що належить фінансовим установам (наприклад, інформація про кредитні картки і рахунки); дані, що належать урядовим установам; інформацію, що належить міжнародним або міжштатовим організаціям. Крім того закон містив статті, що забороняють пошкодження даних (наприклад, розповсюдження вірусів). І в цьому ж році арештований член групи «Legion of Doom» Лойд Бланкеншип (Loyd Blankenship), відомий під ніком «The Mentor», що написав під час відбування покарання у в'язниці знаменитий «Маніфест хакера», – «The Hacker Manifesto» [11]. Ідеї, висловлені в цьому маніфесті, до сьогодні вважаються основою хакерської ідеології і культури та широко розповсюджуються в мережі Інтернет. Очевидно, не випадково *кількісний*

стрибок кіберзлочинів співпав із зростанням популярності в комп'ютерному світі ідей хакерів, що свідчить про взаємозв'язок цих явищ.

У 1994 р. світова спільнота дізналася про так звану «справу Володимира Льовіна», віднесену міжнародною кримінальною поліцією до категорії «транснаціональних мережових комп'ютерних злочинів». Міжнародна організована злочинна група у складі 12 людей, використовуючи Інтернет і мережу передачі даних «Спрінт/Теленет», подолавши захист від несанкціонованого доступу, спробувала здійснити 40 переказів грошових коштів на загальну суму 10 млн. 700 тис. 952 долари США з рахунків клієнтів названого банку, що знаходяться в 9 країнах світу, на рахунки, розташовані в США, Фінляндії, Ізраїлі, Швейцарії, Німеччині, Росії і Нідерландах [7]. Це був перший великий міжнародний фінансовий злочин з використанням Інтернет, про який стало відомо широкій громадськості, і який продемонстрував, що кіберзлочини можуть завдавати серйозного фінансового збитку.

У 1998 р. 12-річний хакер проник в комп'ютерну систему, яка контролювала водоспуск дамби Теодора Рузвельта в Арізоні. небезпека його дій полягала в тому, що у разі відкриття зливних воріт дамби вода могла затопити міста Темп (Tempe) і Месе (Mesa) із загальною чисельністю населення в 1 млн. людей [12]. Оцінка даного факту привела до появи таких термінів, як «Інтернет-тероризм», «комп'ютерний тероризм», «кібертероризм». Крім того, це показало, що найуразливішою до кібератак є сама мережа Інтернет, оскільки її ключові вузли доступні з будь-якої точки світу.

Поява кібертероризму і гучні справи про злочинну діяльність міжнародних угруповань, свідчать про те, що в цей час кіберзлочинність придбала таку властивість, як транснаціональність. Це стало початком третього етапу в розвитку кіберзлочинності. Тривожним фактором в цей час стало і те, що з розвитком Інтернет серйозні наслідки могли наступати не тільки у разі умисних кібератак, але і з вини неуважних фахівців. Так, в 1997 р. помилка співробітника «Network solutions» привела до того, що сайти, чії назви

закінчувалися на «.net» і «.com» стали недоступними. Тобто збій в роботі всієї Глобальної мережі відбувся із-за неувважності всього однієї людини.

У цей же час *кібератаки стають також способом досягнення політичних цілей*. Характерним прикладом цього є Інтернет-страйк, при якому учасники такої акції одночасно заходять на сайт, підключаються до сервісу, посилають електронні повідомлення, пишуть у форумах для того, щоб обмежити або взагалі припинити доступ на сайт іншим користувачам. Відбувається перевантаження Інтернет-сайту або сервісу зовнішніми запитами, що приводить до збоїв в роботі або повної зупинки.

Першу подібну акцію здійснила група, що називає себе «Strano Network», що протестувала проти політики французького уряду в питаннях ядерних програм і в соціальній сфері. 21.12.1995 р. ця група протягом години атакувала різні сайти урядових агентств. При цьому учасники групи з різних куточків світу були проінструктовані таким чином: їм було необхідно за допомогою браузера одночасно зайти на урядові сайти, унаслідок чого деякі сайти дійсно були виведені з ладу на якийсь час [3].

Надалі транснаціональність проблеми кіберзлочинності виявляється все ширше. Так, конфлікт в Косово вважається першою Інтернет-війною, в якій різні групи комп'ютерних активістів використовували мережу Інтернет для засудження військових дій як Югославії, так і НАТО, навмисно порушуючи при цьому роботу урядових комп'ютерів і отримуючи контроль над сайтами з подальшою зміною вмісту, «дефейсу» (deface). Паралельно в Інтернет розповсюджувалися історії про небезпеки і жахи війни, наводилися різні факти і думки політиків і громадських діячів, здійснюючи таким чином пропагандистські дії на широку аудиторію у всьому світі [1]. Все це характеризує *третій етап* розвитку кіберзлочинності.

Необхідно відзначити, що в даний час практично будь-який військовий або політичний конфлікт супроводжується організованим протиборством в мережі Інтернет. Наприклад, в 2005 р. пройшла хвиля кібератак, приводом для якої послужив шкільний підручник історії, що вийшов в Японії та який

спотворює події в Китаї в 1930 – 1940-х рр. XX ст., зокрема в ньому вмовчується про військові злочини японських військ під час інтервенції. У списку сайтів, що підлягають атакам опинилися японські Міністерства і відомства, сайти найбільших японських корпорацій і сайти, присвячені Другій світовій війні. При цьому китайські хакери продемонстрували високий рівень організованості, про що свідчить синхронність і масовість їх атак. Знаючи про наявність державного контролю над Інтернет в Китаї, можна припустити, що дана атака була санкціонована державою. Використання кібератак в політичних цілях можна вважати початком *четвертого етапу* в розвитку кіберзлочинності.

Далі за прикладом Китаю пішли російські хакери, які зробили декілька масштабних DDos-атак (distributed denial-of-service attack). Так, у кінці квітня – на початку травня 2007 р. протягом декількох днів атакувалися урядові сайти Естонії. Відповідальність за це узяв на себе молодіжний рух «Наші». А в серпні 2009 р. американське видання Aviation Week звинуватило російських хакерів в нападі на сервер трубопроводу «Баку – Тбілісі – Джейхан». Причому, як заявило видання, атаки проводилися з тих же адрес, що і при атаках на естонські сайти.

Таким чином, на теперішній момент можна виділити 4 етапи в розвитку кіберзлочинності:

1 етап. Поява кіберзлочинності і субкультури хакерів.

2 етап. Розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинності і національних груп хакерів.

3 етап. Придбання кіберзлочинністю транснаціонального характеру, поява кібертероризму і міжнародних угруповань хакерів у всіх сферах кіберзлочинності.

4 етап. Використання Інтернет в політичних цілях, виникнення таких явищ, як Інтернет-страйк і Інтернет-війна, цілеспрямоване використання кібератак проти урядів окремих держав.

Аналізуючи суть кіберзлочинності, можна виділити наступні її характерні властивості:

– інтелектуальний характер кіберзлочинності, – здійснення кіберзлочину вимагає певного набору знань, крім того інтелектуальність серед кіберзлочинців пропагується субкультурою хакерів, що дає їм стимул для розумового саморозвитку;

– кіберзлочини, на відміну від інших інтелектуальних злочинів, доступні людям невисоких соціальних і вікових можливостей – для здійснення кіберзлочинів не треба займати високе соціальне положення, досить мати доступ в Інтернет і комп'ютер;

– анонімність і неперсоніфікованість кіберзлочинів – механізми ідентифікації глобальної мережі дозволяють особі здійснювати операції анонімно або видавати себе за іншу особу, змінювати біографічні дані або соціальний статус;

– віддаленість кіберзлочинів, – злочинця і жертву можуть розділяти тисячі кілометрів, оскільки немає відмінностей в скоєнні злочину проти комп'ютерних систем, розташованих на сусідній вулиці або в іншій країні, якщо злочин вчинюється за допомогою Інтернет;

– висока латентність кіберзлочинності, однією з основних причин якої є те, що збиток від кіберзлочину часто здається жертві незначним в порівнянні з процедурою розслідування, яка здатна забрати час, але не гарантує притягання до відповідальності винного і компенсації збитку [9].

– транснаціональність кіберзлочинності, – на думку деяких авторів, близько 62% комп'ютерних злочинів вчинюється у складі організованих груп, що знаходяться, зокрема, на території декількох країн [6; 13];

– швидке зростання кіберзлочинності, що пов'язане зі все більшим розповсюдженням Інтернет в різних сферах і здешевленням Інтернет-послуг.

Зрозуміло, що кіберзлочинність не стоїть на місці, з'являються та будуть з'являтися нові види злочинів, здійснених за допомогою кіберпростору. Проте, на сьогоднішній день серед найбільш характерними видами кіберзлочинів, що представляють загрозу для національної безпеки, можна виділити наступні:

1. Злочини проти конституційних прав і свобод людини і громадянина, такі як порушення недоторканності приватного життя, порушення таємниці листування, телефонних переговорів, поштових, телеграфних і інших повідомлень, порушення авторських і суміжних прав.

2. Злочини проти життя і здоров'я. Першим зафіксованим фактом вбивства, здійсненим за допомогою Інтернет, був випадок, що відбувся в лютому 1998 р. в США. Важко поранений свідок злочину був захований в закритому госпіталі на території військової бази, проте злочинці через Інтернет змінили режими роботи кардіостимулятора і апарату вентиляції легенів, що призвело до смерті свідка [5]. Крім того, загрозливі масштаби в Інтернет придбали сайти, що пропагують наркоманію, публікують технологію виготовлення наркотичних препаратів в домашніх або промислових масштабах, або які розповсюджують наркотичні засоби, психотропні речовини і їх аналоги.

3. Злочини проти честі і гідності особи. Анонімність, широка аудиторія Інтернет дають безмежні можливості в розповсюдженні інформації будь-яких видів, у тому числі і наклепницької, такої, що порочить честь і гідність особи.

4. Злочини проти власності. Одним з найпоширеніших видів злочинів сучасності в Інтернет є Інтернет-шахрайство, при цьому з кожним днем з'являються все нові його форми, види і способи.

5. Злочини у сфері комп'ютерної інформації, в першу чергу, такі як неправомірний доступ до інформації і створення, використання і розповсюдження шкідливих програм.

6. Злочини проти суспільної моральності. Так, широкого поширення в Глобальній мережі набув порнобізнес, при цьому порносайти в Інтернет доступні для будь-якої точки миру і для будь-якої категорії населення, а розповсюджувачі аморальної продукції відчують себе безкарно, оскільки діють анонімно.

7. Злочини проти безпеки держави. Із зростанням використання Інтернет в державних структурах стає можливим нелегально дістати доступ не

тільки до приватної і корпоративної інформації, але також до інформації, що є державною таємницею, і за допомогою Інтернет скоювати такі злочини, як шпигунство, державна зрада або розголошення державної таємниці.

І, звичайно ж, головне місце серед останнього виду злочинів займає кібертероризм, який набуває все більш загрозливих масштабів, маючи тенденцію зрощення із «звичайним» тероризмом.

Безконтрольність та розповсюдженість Інтернет серед усіх верств населення, відсутність захисних заходів населення з боку департаментів державних органів безпеки по боротьбі із кіберзлочинністю відносно місцевих Інтернет провайдерів, доступність інформації про методи скоєння кіберзлочинів. Перераховані вище проблеми повинні стати пріоритетними напрямками роботи відповідних державних органів в тих країнах, де кіберзлочинність має велику питому вагу у відношенні до кіберзлочинів, що вчиняються у всьому світі. Також потрібна організована робота департаментів багатьох країн через транснаціональність кіберзлочинності.

Конвенція Ради Європи з кіберзлочинності була підписана багатьма країнами Європи, а також США, Канадою, Японією, Південною Африкою в 2001 році. На даний момент вона ратифікована та вступила в силу в 39 країнах світу, зокрема в Україні (з 01.07.2006 р.). Цей документ має позитивну регулятивну силу та враховує усі права та свободи громадян, які проживають в країнах, що ратифікували його. На його базі можна приймати державні закони, які не будуть суперечити аналогічним прийнятим в країнах, що також ратифікували його. Це дозволить створити універсальну міжнародну нормативно-правову базу та спростить роботу органів безпеки.

Надшвидкий науково-технічний прогрес безпосередньо пов'язаний із тією ситуацією, в якій опинився світ кіберзлочинності. Кіберзлочинці створюють нові методи скоєння злочинів та знаходять помилки в системах безпеки швидше, ніж ті, хто їм протидіє, встигають виправити помилки та вдосконалити систему захисту.

Люди стають хакерами через нестачу грошей, або через бажання реалізувати свій інтелектуальний потенціал в спосіб, що не приймається суспільством. Першу проблему за хакерів можуть вирішити великі міжнародні компанії або навіть державні органи безпеки, яким потрібні справжні професіонали своєї справи. Але, звичайно, це стосується найменшої частини кіберзлочинців. Друга проблема повинна бути вирішена упереджувальними заходами, в першу чергу деромантизацією образу хакера в суспільстві.

Говорячи про суспільство з одного боку та про кіберзлочинців з іншого, не можна не сказати про підвищення комп'ютерної грамотності усіх верств населення, особливо молоді, бо саме вона стає на слизький шлях.

Список використаних джерел

1. *Андреев А.* Об информационном противоборстве в ходе вооруженного конфликта в Косово [Електрон. ресурс] / А. Андреев, С. Давыдович / «ПСИ-ФАКТОР» Центр практической психологии. – Режим доступа : <http://www.psyfactor.org/warkosovo.htm>.
2. *Голубев В. А.* «Кибертерроризм» – миф или реальность? [Електрон. ресурс] / В. А. Голубев ; Центр дослідження комп'ютерної злочинності. – Режим доступа : <http://www.crime-research.org>. – Computer Crime Research Center.
3. *Деннинг Д.* Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику [Електрон. ресурс] / Д. Деннинг ; [пер. Т. Л. Тропиной] / Владивостокский центр исследования организованной преступностью. – Режим доступа : <http://www.crime.vl.ru/index.php?p=111&more=1&c=1&tb=1&pb=1>.
4. *Касперски К.* Техника отладки программ без исходных текстов / К. Касперски. – СПб. : БХВ-Петербург, 2005. – С. 24.
5. *Кесарева Т. П.* Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет : дис. ... канд. юрид.наук : 12.00.08 / Т. П. Кесарева. – М., 2002. – С. 20, 36.
6. Криминология : учеб. для вузов / под общ. ред. д.ю.н. проф. А. И. Долговой. – 2-е изд., перераб. и доп. – М. : НОРМА, 2003. – С. 682.
7. *Кураков Л. П.* Информация как объект правовой защиты / Л. П. Кураков, С. Н. Смирнов. – М. : Гелиос, 1998. – С. 220–221.
8. *Лукацкий А.* Хакеры управляют реактором [Електрон. ресурс] / А. Лукацкий ; Центр исследования компьютерной преступности. – Режим доступа : <http://www.crime-research.org/library/Lukac0103.html>.
9. *Рассолов И. М.* Право и Интернет. Теоретические проблемы / И. М. Рассолов. – М. : НОРМА, 2003. – С. 251–254.
10. Computer Fraud and Abuse Act [Електрон. ресурс]. – Режим доступа : http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act. – Wikipedia The free encyclopedia
11. Mentor. Hacker Manifesto, Written on January 8, 1986 [Електрон. ресурс]. – Режим доступа : http://project.cyberpunk.ru/idb/hacker_manifesto.html.
12. *Lemos Robert.* Cyberterrorism: The real risk [Електрон. ресурс] / Robert Lemos ; Центр дослідження комп'ютерної злочинності. – Режим доступа : <http://www.crime-research.org/library/Robert1.htm>.

13. *Schweitzer D. Incident response: computer forensics toolkit / D. Schweitzer. – Wiley, 2003. – P. 26.*

Дзюндзюк В. Б., Дзюндзюк Б. В. Появление и развитие киберпреступности.

Рассмотрено понятие киберпреступности и ее составляющие, сущность киберпреступлений, история возникновения киберпреступности. Определены этапы развития киберпреступности и события, давшие начало каждому из этапов. Приведена актуальная классификация киберпреступлений.

Ключевые слова: киберпреступность, киберпреступники, виртуальное пространство, Интернет, кибертерроризм.

Dziundziuk V., Dziundziuk B. The Emergence and Development of Cybercrime.

The concept of cybercriminality and its constituents, essence of cybercrimes, history of origin of cybercriminality are considered. The stages of development of cybercriminality and events, which were at the beginning of each stage, are defined. Actual classification of cybercrimes is given.

Key words: cybercriminality, cybercrimes, virtual space, Internet, cyberterrorism.