КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВУ

Олександр Буров,
головний науковий співробітник НДІ інтелектуальної власності АПрН України, начальник відділу проблем людського фактору Державного науково-технічного центру залізничного транспорту України, доктор технічних наук

Дарія Бурова,
магістр інтелектуальної власності

Анастасія Пенська,
студент-магістр факультету менеджменту та маркетингу Національного технічного університету України "Київський політехнічний інститут"

Сьогодні значну частину загального обсягу карних злочинів займає злочинність, пов'язана з використанням комп'ютерних систем та мереж. Її росту й розвитку сприяє природа даного виду злочину, що базується, перш за все, на відкритому і загальнодоступному характері мережі Internet. Так, кількість користувачів мережі Інтернет постійно зростає. В США їх 158 мільйонів, в Європі — 95, в Азії — 90, Латинській Америці — 14, в Африці — 3. У (В) Росії, за різними оцінками, кількість користувачів мережі Internet складає близько 14,6 млн. і прогнозується, що у 2008 р. цей показник сягне 40 млн. [1].

Щодо розгорнутої інфраструктури, то на сьогодні в цьому контексті Internet охоплює близько 150 країн світу. Виникненню та поширенню нових видів злочинів сприяють безкарність правопорушників, а також недостатня підготовка правоохоронних органів з питань розслідування таких злочинів.

Національна інфраструктура будь-якої держави тісно пов'язана з використанням сучасних комп'ютерних технологій. Щоденна діяльність банківських і енергетичних систем, управління рухом у повітряному просторі, транспортна мережа, швидка медична допомога знаходяться в повній залежності від надійної і безпечної роботи автоматизованих електронно-обчислюваних систем [2].

Поняття кіберзлочинності наразі є ще незвичним для правоохоронних органів, однак злочинні дії із використанням глобальної комп'ютерної мережі Internet приховують у собі величезну суспільну небезпеку. Терористичні акти в США 11 вересня 2001 року та аварія в енергетичній системі в серпні 2003 року — наочні тому приклади. Зростаючу популярність кібертероризму пояснюють ще тим, що вчинити кібертерактнабагато дешевше та простіше, ніж знайти зброю з цією самою метою.

Терористичні акти в кіберпросторі можуть здійснюватися не тільки окремими особами або терористичними групами, але й однією державою проти іншої. В цьому кібертероризм нічим не відрізняється від будь-якого іншого виду тероризму. Екстремістські угруповання, сепаратистські сили, проповідники ідей, що суперечать загальнолюдським цінностям, інтенсивно використовують сучасні технології для пропаганди своєї ідеології і ведення інформаційних воєн. Інформаційна зброя може стати ідеальним засобом для електронних терористів, що робить питання інформаційної безпеки важливим аспектом як національної, так і міжнародної безпеки.

Існують також і суб'єктивні причини комп'ютерної злочинності. Так, наприклад, спроба молодих людей реалізувати себе у створенні вірусів часто пов'язана з такими причинами, як бажання самоствердитися, "прогриміти", а також з відсутністю усвідомлених життєвих цілей.

Злочинність у сфері використання комп'ютерних технологій ("кіберзлочинність") — це явище міжнародного значення, рівень якого безпосередньо залежить від рівня розвитку й впровадження сучасних комп'ютерних технологій, мереж їх загального користування й доступу до них. Таким чином, стрімкий розвиток інформатизації в Україні несе в собі потенційну можливість використання комп'ютерних технологій з корисною метою, що певною мірою ставить під загрозу національну безпеку держави.

Історично термін "комп'ютерна злочинність" вперше з'явився в американській пресі на початку 60-х років, коли були виявлені перші випадки злочинів, здійснених з використанням ЕОМ. Основні ознаки комп'ютерних злочинів були сформульовані на Конференції Американської асоціації адвокатів у Далласі в 1979 році:

- використання або спроба використання комп'ютера, обчислювальної системи або мережі комп'ютерів з метою одержання грошей, власності або послуг, під прикриттям фальшивих приводів або неправдивих обіцянок, або видаючи себе за іншу особу;
- навмисна несанкціонована дія, що має на меті зміну, ушкодження, нищення або викрадення комп'ютера, обчислювальної системи, мережі комп'ютерів або, що розміщуються в них систем математичного забезпечення, програм або інформації;
- навмисне несанкціоноване порушення зв'язку між комп'ютерами, обчислювальними системами або мережами комп'ютерів [2].

Деякі групи вчених вважають, що комп'ютерних злочинів як окремої групи злочинів в юридичному значенні не існує. Однак, вони відзначають той факт, що багато традиційних видів злочинів модифікувалися через залучення в них обчислювальної техніки, і тому говорять лише про комп'ютерні аспекти злочинів, не виділяючи їх в окрему групу. Широке розповсюдження так званого "класичного хакерства", що посягає лише на загальні відносини у сфері комп'ютерної інформації або інформаційної безпеки, часто без отримання матеріальних благ, спростувало це судження, що й спонукало законодавців ряду країн, у т.ч. Росії й Азербайджану (Глава 28 КК Російської Федерації і Глава 20 КК Республіки Азербайд-

жан "Злочини в сфері комп'ютерної інформації"), Білорусі (Глава 31 КК Республіки Білорусь "Злочини проти інформаційної безпеки"), України (Розділ XVI КК Республіки України "Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж"), Сполучених Штатів Америки (ряд статей Глав 47, 63, 119 Вісімнадцятого Зводу законів США), інших, вносити відповідні зміни в національне законодавство [3].

Комп'ютерні злочини можна класифікувати наступним чином:

а) за об'єктом зазіхання: економічні комп'ютерні злочини; комп'ютерні злочини проти особистих прав і недоторканності приватної сфери; комп'ютерні злочини проти суспільних і державних інтересів;

б) за характером використання комп'ютерів або комп'ютерних систем: діяння, де комп'ютери є предметами злочинів (викрадення інформації, несанкціонований доступ, знищення або ушкодження файлів і обладнання і т.п.); дії, де комп'ютери використовуються як знаряддя злочину (електронні розкрадання й т.п.); злочини, де комп'ютери відіграють роль інтелектуальних засобів (наприклад, розміщення в Інтернеті порносайтів) [4].

Для інформаційних актів характерні наступні інструменти їх здійснення:

- різні види атак, що дозволяють проникнути в мережу, що атакується, або перехопити управління мережею;
- комп'ютерні віруси, у тому числі — мережеві (хробаки), що модифікують і знищують інформацію або блокують роботу обчислювальних систем;
- логічні бомби — набори команд, які впроваджуються в програму й спрацьовують за певних умов (наприклад, після закінчення певного проміжку часу);
- "троянські коні", що дозволяють виконувати певні дії без відома хазяїна зараженої системи;
- засобу пригнічення інформаційного обміну в мережах.

До теперішнього часу перелік комп'ютерних правопорушень значно розширився і включає в себе наступні види злочинів:

- незаконне використання комп'ютера з метою аналізу або моделювання злочинних дій для їх здійснення в комп'ютерних системах;
- несанкціоноване проникнення в інформаційно-обчислювальну мережу або масиви інформації з корисливою метою;
- розкрадання системного і прикладного програмного забезпечення;
- несанкціоноване копіювання, зміна або знищення інформації;
- шантаж, інформаційна блокада та інші методи комп'ютерного тиску;
- комп'ютерний шпіонаж і передання комп'ютерної інформації особам, які не мають права доступу до неї;
- фальсифікація комп'ютерної інформації;
- розроблення і розповсюдження комп'ютерних вірусів в інформаційно-обчислювальних системах і мережах;
- несанкціонований перегляд або розкрадання інформації з банків даних і баз знань;
- недбалість при розробленні, створенні інформаційно-обчис-

лювальних мереж і програмного забезпечення, що призводить до небажаних наслідків і втрати ресурсів;
- механічні, електричні, електромагнітні та інші види впливу на інформаційно-обчислювальні системи та лінії телекомунікацій, що викликають їх пошкодження [6].

Складність у попередженні кібертероризму полягає в ряді аспектів, що характеризують його:
- латентність (скритність);
- трансконтинентальність;
- інформація, інформаційні ресурси, інформаційна техніка можуть виступати метою злочинних зазіхань, середовищем, у якому відбуваються правопорушення, а також знаряддям злочину;
- легкість знищення й зміни комп'ютерної інформації (слідів злочину) [5].

Серед трьох найпомітніших трендів у кіберзлочинності експерти назвали такі.

По-перше, зростаюча загроза національної безпеки, викликана веб-шпигунством. Зловмисники від хакерів-одинаків до добре організованих і фінансованих груп використовують мережу не тільки для фінансової, але й політичної та технологічний вигоди.

По-друге, підвищеному ризику піддаються онлайн-сервіси, користувачів яких атакують фішери, озброєні прийомами соціальної інженерії. Фішинг являє собою розсилання спаму, причому написаного так, начебто його надіслав який-небудь банк або інша серйозна організація з метою отримання важливої інформації (імена користувачів, паролі, екаунти Ids, ATM Pin'и або інформацію про кредитні картки). Зазвичай, фішингові атаки направляють отримувача на веб-сторінку, спроектовану так, що вона імітує справжній сайт організації та збирає особисту інформацію, причому найчастіше користувач навіть не підозрює, що на нього проводилась атака такого роду.

Третім трендом експерти називають появу ринку "програмних вразливостей". Під вразливістю розуміється вразливість перед порушенням політики безпеки, викликаним неправильно заданим набором правил або помилкою в програмі, що забезпечує безпеку комп'ютера. Варто відзначити, що теоретично всі комп'ютерні системи мають вразливості. Але те, наскіль-ки великий потенційний збиток від вірусної атаки, що використовує вразливість, дозволяє розрізняти уразливості, що активно використовуються й не використовувані зов-сім. Згідно з термінологією MITRE CVE, вразливість — це стан обчислювальної системи (або декількох систем), який дозволяє:
- виконувати команди від імені іншого користувача;
- одержувати доступ до інформації, закритої для даного користувача;
- показувати себе, як іншого користувача або ресурс;
- здійснювати атаку типу "відмова в обслуговуванні"[6].

В MITRE вважають, що атака, вчинена внаслідок слабкої або невірної політики безпеки, краще описується терміном "піддатливість" (exposure).

Піддатливість — це стан обчислювальної системи (або декількох систем), який не є вразливістю, але:
- дозволяє атакуючому робити збір захищеної інформації;
- дозволяє атакуючому прихову-

вати свою діяльність;
- містить можливості, які працюють коректно, але можуть бути легко використані в непорядних цілях;
- є первинною точкою входу в систему, яку особа, що атакує може використовувати для одержання доступу до інформації.

В Україні кількість зафіксованих вітчизняними правоохоронними органами злочинів, скоєних з використанням інформаційних та комп'ютерних технологій, постійно зростає.

Зокрема, зафіксовано чисельні спроби несанкціонованого втручання з території України та з-за кордону в інформаційні комп'ютерні мережі органів державної влади й управління. Спостерігається також зростання кількості тяжких економічних злочинів, наприклад, втручання у фіскальну пам'ять електронно-касових апаратів, використання спеціальних програм для ухилення від сплати податків у процесі обміну валюти тощо.

Водночас посилюється загроза використання сучасних інформацій-них технологій злочинними угрупуваннями терористичної спрямованості.

Однією з причин вразливості інформаційної безпеки України від зазначеної загрози є технологічне відставання. За відсутності конкурентоспроможних інформаційних технологій надається перевага технічним засобам обробки інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують захист інформації [8, с. 13]. Крім того, при проведенні тендерів на придбання інформаційної продукції мають місце випадки надання переваги іноземним виробникам за умов наявності вітчизняних.

Серед проблемних питань боротьби із злочинами в сфері комп'ютерних та Internet технологій в Україні можна також виділити наступні:

1) недосконалість законодавства і пов'язані з цим питання кваліфікації й актуальності боротьби з комп'ютерною злочинністю;
2) труднощі організації і проведення комп'ютерних експертиз;
3) труднощі проведення заходів оперативно-технічного документування злочинних дій осіб;
4) відсутність практики й механізмів розкриття "транснаціональних" комп'ютерних злочинів з територіально-розподіленими й нестабільними в часі слідами, а також проведення надалі слідчих дій відносно осіб, які повинні дати свідчення в якості потерпілого, підозрюваного, свідка [9].

За умов глобалізації ринків, в тому числі інформації та інновацій, виникає потреба в регулюванні загальних правил і норм. Причому це питання з площини захисту інформації як такої переходить все більше у площину захисту інформаційного змісту виробу постачальника продукту або послуг [10]. Відповідно значущість захисту прав інтелектуальної власності за нових умов глобалізації інформаційного суспільства зростатиме, потребуючи не тільки національних заходів, але й постійних консультацій на міжнародному рівні.

Такій позиції відповідає і діяльність України. Згідно до Плану заходів Уряду України з реалізації завдань щодо розвитку інформаційного суспільства в Україні на 2007—2015 рр. передбачено розроблення проекту "Інформаційного кодексу України", який повинен

забезпечити створення єдиного правового поля в інформаційній сфері, в тому числі для захисту прав інтелектуальної власності.

Висновки та рекомендації:

1. Кіберзлочинність не є суто технічною проблемою. Вона охоплює всі сфери діяльності людини в інформаційному суспільстві, включаючи інтелектуальну власність.

2. Необхідна скоординована діяльність усіх країн, направлена на протидію й боротьбу з таким небезпечним в умовах світової інформатизації злочинним явищем, як кібертероризм.

3. Протидія цій новій і небезпечній формі тероризму не може бути результативною без серйозної реформи правоохоронних органів і спеціальних служб, без правової та методичної допомоги з боку фахівців у сфері інтелектуальної власності. ●

Список використаних джерел:

1. *Интернет: Россия станет №2 в Европе — http://www.cnews.ru/news/top/index.shtml?2008/02/11/287595*
2. *Голубев В. А. Интервью: Компьютерная преступность — угрозы и прогнозы. — http://www.crime-research.ru/interviews/golubev_interv06/*
3. *Батурин Ю. М. Проблемы компьютерного права. — М.: Юрид. лит., 1991.*
4. *Виталий Козлов "Computer crime"? Что стоит за названием? — http://www.crime-research.ru/library/CCrime.html*
5. *Голубев В. А., Сайтарлы Т. А. "Проблемы борьбы с кибертерроризмом в современных условиях" — http://www.crime-research.org/library/e-terrorism.htm*
6. *Вертузаєв М. С., Попов А. Ф. "Запобігання комп'ютерним злочинам та їх розслідування" // Право України. — 1998. — № 1. — С. 101—103.*
7. *Программные уязвимости. — http://hacker.bestresurs.com/hacker1.html*
8. *Згуровський М. З. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Науково-технологічний збірник. — К., 1998.*
9. *Артем Корягин "Преступность в сфере компьютерных и интернет-технологий: актуальность и проблемы борьбы с ней" — http://www.crime-research.ru/library/Koragin.html*
10. *Європа та глобальне інформаційне суспільство. Рекомендації Європейській Раді ЄС. Брюссель, 26 травня 1994 р.*