ISSN 2078-6115. Вісник Львівського університету. Серія економічна. 2014. Випуск 51. С. 173 - 179
Visnyk of the Lviv University. Series Economics. 2014. Issue 51. P. 173 - 179

УДК 004.056.5:343.9.024]:316.77

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВУ

Н.Міщук

Львівський національний університет імені Івана Франка
79008 м.Львів, проспект Свободи, 18
E-mail: mishchuk_n@ukr.net

Досліджено поняття кіберзлочинності та кіберзлочинів як динамічної групи злочинів, проаналізовано існуючі методи класифікації комп'ютерних злочинів, охарактеризовано особливості злочинів, скоєних в глобальних комп'ютерних мережах. Запропоновано заходи щодо профілактики та запобіганню кіберзлочинності на вітчизняному інформаційному просторі.

Ключові слова: кіберзлочинність, кіберзлочини, інформаційні технології, комп'ютерні мережі, захист інформаційних ресурсів.

В сучасних умовах більшості бізнес процесів переносяться у віртуальний простір. Цей процес є невід'ємною складовою розвитку інформаційного суспільства та основою формування інформаційної економіки.

На думку більшості фахівців інформаційна економіка – це економічні відносини в яких акцент зосереджується на провідній ролі електронно-інформаційних технічних засобів зв'язку в розвитку всіх основних сфер економіки. Сама ж інформація ототожнюється з товарною продукцією і досліджується здебільшого за допомогою статистичних методів.

Саме тому, в епоху невпинного розвитку інформаційних технологій, комп'ютерних мереж і Інтернету, кіберзлочинність стала реальністю суспільного життя.

Поняття «кіберзлочинність» вперше з'явилось в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних.

Поняття кіберзлочинності як сукупності злочинів поширюється на всі види злочинів, скоєних в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати (бути) предметом (метою) злочинних посягань, середовищем, в якій відбуваються правопорушення і засобом або знаряддям злочину. Таким чином, кіберзлочинність може бути визначена як сукупність злочинів, скоєних в кіберпросторі за допомогою комп'ютерних систем чи комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [4].

На нашу думку, кіберзлочинність включає поняття комп'ютерної злочинності, де предметом злочину виступає власне комп'ютер, а також інформаційну безпеку, яку

вважатимемо об'єктом злочину та інші злочинні посягання з використанням інформаційно-комунікаційних систем.

Кіберзлочини є найдинамічнішою групою суспільно небезпечних посягань. Надзвичайно швидко зростає кількість комп'ютерних злочинів, а також збільшуються і масштаби комп'ютерних зловживань. Про зростання суспільної небезпечності цих злочинів свідчить повсякденна практика служб безпеки підприємницьких структур. За оцінкою фахівців США, збиток від комп'ютерних злочинів збільшується на 35% у рік і становить близько 3,5 мільярдів доларів. Однією з причин є сума грошей, яка одержана внаслідок злочину: тоді як збиток від середнього комп'ютерного злочину становить 560 тисяч доларів, при пограбуванні банку − всього лише 19 тисяч доларів [5].

Основною причиною наявності втрат від злочинів, пов'язаних з інформаційно-комунікативними системами, є недостатня обізнаність користувачів у питаннях безпеки інформації.

Тільки наявність у кінцевого користувача певних знань про заходи безпеки може забезпечити припинення інцидентів та помилок, ефективне вживання заходів захисту, запобігти злочину або своєчасно знайти злочинця. У цьому контексті можна визначити п'ять рівнів захисту комп'ютерних та інформаційних ресурсів (рис.1).

Запобігання	функціонування системи в напрямі повного виключення несанкціонованого доступу − лише авторизований персонал отримує за спеціальною процедурою доступ до інформації та технологій
Виявлення	забезпечення раннього викриття передумов, ознак виникнення і формування намірів («голого умислу») до зловживань, приготування і скоєння злочинів і навіть у випадку якщо обійшли механізми захисту
Припинення	забезпечення локалізації або повної нейтралізації зусиль зловмисника щодо завдання шкоди чи збитку інформації, інформаційній базі, системі управління і механізму обробки інформаційних ресурсів
Обмеження	зменшення розміру втрат, якщо злочин все-таки відбувся, попри заходи щодо його запобігання, виявлення і припинення
Відновлення	забезпечення ефективного відновлення інформації за наявними документованими і перевіреними планами з відновлення, з одночасним відновленням ушкоджених або знищених елементів інфраструктури технічних систем і механізмів та програмних засобів

Рис. 1. Рівні захисту комп'ютерних та інформаційних ресурсів

Кіберзлочини поділяють на види залежно від об'єкта, від предмета посягання, залежно від способів скоєння тощо.

Найбільш поширена класифікація кіберзлочинів ґрунтується на структурі Конвенції Ради Європи про кіберзлочинність. Ця класифікація на даний час є «еталоном», оскільки наявні міжнародні та регіональні документи, а також наукова практика. Згідно неї комп'ютерні злочини поділяють на п'ять груп [4]:

– злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему;

– злочини, пов'язані з використанням комп'ютера, як засобу скоєння злочинів – а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення);

– злочини, пов'язані з контентом (змістом даних, розміщених в комп'ютерних мережах);

– злочини, пов'язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав;

– злочинів зафіксовані в окремому протоколі – це акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

У Конвенції Ради Європи не виділяються в окремі групи деякі діяння, які широко обговорюються, але до цих пір є спірними з точки зору техніки їх криміналізації і необхідності гармонізації законодавства на міжнародному рівні. Одне з них – це так званий «кібертероризм» і використання кіберпростору в терористичних цілях (наприклад, втягнення у вчинення злочинів терористичного характеру або інше сприяння їх вчиненню). Відсутність узгодженого визначення тероризму на міжнародному рівні в даний час ускладнює дебати про кібертероризм як про явище, криміналізація якого необхідна як універсальна для всього міжнародного співтовариства, що, втім, не заважає державам і міжнародним організаціям вживати зусилля з боротьби з використанням мережі Інтернет терористичними організаціями – наприклад, на рівні Європейського Союзу існує проект Clean IT, метою якого є боротьба з цим явищем.

Ще одна категорія злочинів, не включена окремо в Конвенцію Ради Європи (і отримала поширення після прийняття Конвенції) – identity theft, крадіжка, передача і використання персональних даних з метою вчинення злочинів. Одні країни виділяють ці злочини в окрему категорію, інші вважають, що дані діяння підпадають під кілька статей кримінального законодавства. Оскільки дані злочини набули широкого поширення відносно недавно, в даний час ведуться дебати про виділення цього злочину в окрему групу і необхідності гармонізації законодавства у цій сфері на міжнародному рівні.

Аналіз кіберзлочинності або його різновиду – комп'ютерної злочинності – в межах однієї країни чи групи країн, безумовно, цінний, але навряд чи здатний дати уявлення про справжні масштаби і про розмах цього явища.

Для більшості злочинів, скоєних в глобальних комп'ютерних мережах, характерні наступні особливості [4]:

– підвищена скритність вчинення злочину, що забезпечується специфікою мережевого інформаційного простору (розвинені механізми анонімності, складність інфраструктури тощо);

– транскордонний характер мережевих злочинів, при якому злочинець, об'єкт злочинного посягання, потерпілий можуть перебувати на територіях різних держав;

– особлива підготовленість злочинців, інтелектуальний характер злочинної діяльності; нестандартність, складність, різноманіття і часте оновлення способів скоєння злочинів і застосовуваних спеціальних засобів;

– можливість вчинення злочину в автоматизованому режимі в декількох місцях одночасно, можливість об'єднувати відносно слабкі ресурси багатьох окремих комп'ютерів в потужне знаряддя вчинення злочину;

– багатоепізодним характер злочинних дій при множинності потерпілих;

– необізнаність потерпілих про те, що вони піддалися злочинному впливу;

– дистанційний характер злочинних дій в умовах відсутності фізичного контакту злочинця і потерпілого;

– неможливість запобігання та припинення злочинів даного виду традиційними засобами.

Інтернет-злочинність проникає в персональні комп'ютери, банківські рахунки й фінансові операції. Інтернет-злочинцям усе краще вдається здійснювати шахрайства з кредитними картками чи крадіжки ідентифікаційних даних. Вони визначають логіни й паролі користувачів для інтернет-банкінгу, зламують смартфони або профілі у соціальних мережах.

Щодня не менше мільйона людей стають жертвами інтернет-злочинців. За рік діяльність останніх завдає збитків у 300 мільярдів євро. На чорному ринку торгують даними кредитних карток. Інтернет-торгівля також усе ще є небезпечною для користувача. А велика кількість інтернет-злочинців залишається непокараною.

В даний час не існує ні релевантної статистики, що відбиває реальну картину стану кіберзлочинності, ні надійних методів збору таких даних. І справа не тільки у відсутності однаковості національного кримінального законодавства країн у сфері боротьби з кіберзлочинністю і різної практики його застосування, відмінностях у формуванні кримінальної статистики та особливості правоохоронної системи. Так, незрозуміло, до якої міри достовірна статистика про економічні втрати в результаті кіберзлочинності.

Про зростання масштабів кіберзлочинності та зацікавленість світової спільноти у вирішенні питань даного напряму свідчать дослідження експертів. Зокрема, компанія PwC проводить міжнародне дослідження впливу економічних злочинів на бізнес – Всесвітній огляд економічних злочинів. У 2011 році Всесвітній огляд економічних злочинів робив акцент саме на зростаючу загрозу кіберзлочинності. На фоні таких проблем, як викрадення даних та виток інформації, комп'ютерні віруси та атаки хакерів, особлива увага у цьому огляді приділялась значущості цього виду економічної злочинності та його впливу на організації в усьому світі [1].

Проблема комп'ютерної злочинності привернула увагу криміналістів провідних зарубіжних країн з часу широкого впровадження комп'ютерної техніки, що викликало низку негативних наслідків та загострило ситуацію із захистом інформації, яка міститься у базах даних комп'ютерів і комп'ютерних систем. Статистика таких злочинів велася з 1958 р. Тоді під ними малися на увазі: випадки псування і розкрадання комп'ютерного устаткування; крадіжка інформації; шахрайство чи крадіжка грошей, здійснені із застосуванням комп'ютерів; несанкціоноване використання комп'ютерів чи крадіжка машинного часу [2].

Питання пошуку шляхів попередження та протидії злочинам з використанням інформаційно-комунікаційних систем уже тривалий час знаходиться у сфері уваги як державних органів, так й міжнародної спільноти.

Беручи до уваги, що розвиток технологій йде швидше ніж приймаються нормативно-правові акти, якими вони регулюються, а об'єми незаконно одержаних коштів кіберзлочинцями зростають, необхідно на постійній основі знаходити шляхи вирішення нових задач, пов'язаних з такими сферами, як захист даних, транскордонний доступ правоохоронних служб до даних та обмін інформацією між державними та приватними структурами.

Міжнародна спільнота, враховуючи можливі негативні наслідки цього явища, знаходиться у постійному пошуку заходів, які дозволяють мінімізувати загрози впливу кіберзлочинності на суспільство.

Сьогодні міжнародні організації визнають небезпеку кіберзлочинності і її трансграничний характер, обмеженість одностороннього підходу до вирішення цієї проблеми і необхідність міжнародної співпраці як у вжитті необхідних технічних заходів, так і у виробленні міжнародного законодавства.

Беручи до уваги значні обсяги збитків, кожна країна-член ЄС намагається якось боротися проти кіберзлочинності, проте із різними успіхами. Поле діяльності правоохоронців кожної країни обмежене національними кордонами, тоді як всесвітня мережа кордонів не знає. У зв'язку з цим постала необхідність боротьби проти інтернет-злочинців на загальноєвропейському рівні. Саме з цією метою під егідою Європейського поліцейського відомства (Європол) було створено Європейський центр боротьби із кіберзлочинністю, який розпочав свою діяльність з січня 2013 року в Гаазі (Нідерланди).

Серед пріоритетів Центру – розслідування шахрайства через онлайн-мережі, зокрема у системі електронного банкінгу та інших видах фінансової діяльності, протидія сексуальній експлуатації дітей через Інтернет, а також розслідування інших злочинів, що посягають на безпеку важливої інфраструктури та інформаційних систем ЄС.

Значну роль у подоланні проблем міжнародної співпраці у сфері боротьби з кіберзлочинністю відіграє ООН, яка приділяє достатню увагу питанням поширення злочинів, пов'язаних з використання інформаційних та комп'ютерних систем, та боротьби з таким злочинами. ООН неодноразово наголошувала на транснаціональному характері кіберзлочинів та необхідності координації у світовому масштабі заходів щодо запобігання таким злочинам та їх розслідування.

Правовою основою для протидії комп'ютерній злочинності на національному рівні є Кримінальний кодекс України. В цьому законодавчому акті окремі види комп'ютерних злочинів (кіберзлочинів) виділено в розділ VI Особливої частини – Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361, 363). Окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину, розміщені в інших розділах Особливої частини: у Розділі V зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину (ст. 163, 176, 177) та Злочини у сфері господарської діяльності (ст. 200) в Розділі VII [6].

Зазначимо, що серед інших організаційних заходів в Україні на урядовому рівні створено декілька робочих груп, які розробляють проекти законодавчих актів у сфері громадських стосунків стосовно використання інформаційних технологій, які відображають питання боротьби з кіберзлочинністю і взаємодію з різними міжнародними державними та правоохоронними структурами.

Аналіз різних ініціатив у напрямку створення проектів нормативно-правових актів свідчить, що між державними структурами не має взаємодії, координації їхньої діяльності. На законодавчому рівні ініціюються суперечливі ідеї, що не є потрібним правотворчій діяльності. На сьогоднішній день у сфері інформаційного законодавства створені умови, які дозволяють злочинцям уникати відповідальності за скоєння злочинів використовуючи недосконалу правову базу в різних країнах Вказаний чинник можна розглядати як ознаку латентності кіберзлочинності.

Проблема профілактики і боротьби з кіберзлочинністю – це комплексна та дуже актуальна проблема для нашої країни. Для ефективного вирішення даної проблеми, на нашу думку, слід розробити та впроваджувати діючу стратегію кібербезпеки держави, в основі якої необхідно:

- на урядовому рівні побудувати модель запобігання кібератакам;
- вдосконалювати українське законодавство у сфері боротьби з кіберзлочинністю;
- створити механізм партнерства в інформаційному суспільстві для взаємодії та координації заходів щодо забезпечення кібербезпеки;
- розробити регулюючі механізми, що визначатимуть права, обов'язки та відповідальність учасників у сфері протидії кіберзлочинності;
- створити єдину систему обміну інформацією про випадки кіберзлочинів;
- забезпечити підготовку висококваліфікованих ІТ-фахівців для запобіганню будь-яким злочинам в інформаційному та комп'ютерному просторі;
- налагодити міжнародну взаємодію у напрямку протидії кібератакам.

Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній [3].

Отже, кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, проте на відміну від традиційних крадіжок і шахрайства, вона постійно удосконалюється і йде в ногу з технологіями, що у свою чергу ускладнює виявлення та протидію зазначеним протиправним діям. Ефективний контроль за кіберзлочинністю вимагає більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності.

---

1. Всесвітній огляд економічних злочинів. Кіберзлочини в центрі уваги [Електронний ресурс]. – Режим доступу*:* http://www.pwc.com/ua/en/services/forensic/assets/gecs_2011_report_ukraine_ukr.pdf
2. Гуцалюк М. Протидія комп'ютерній злочинності [Електронний ресурс]. – Режим доступу*:* http://pravoznavec.com.ua/period/article/983/%C3
3. Кіберзлочинність в Україні [Електронний ресурс]. – Режим доступу*:* http://www.science-community.org/uk/node/16132]
4. Кіберзлочинність: проблеми боротьби і прогнози [Електронний ресурс]. – Режим доступу: http://anticyber.com.ua/article_detail.php?id=140
5. Кузьменко А. Сутність поняття та особливості класифікації комп'ютерних злочинів і «комп'ютерної інформації» як об'єкта протиправних посягань [Електронний ресурс]. – Режим доступу*:* http://www.justinian.com.ua/article.php?id=3448
6. Орлов О. В., Онищенко Ю. М. Організаційні та нормативно-правові засади боротьби з кіберзлочинністю [Електронний ресурс]. – Режим доступу*:* http://www.dy.nayka.com.ua/?op=1&z=715

CYBERCRIME AS A THREAT TO THE INFORMATION SOCIETY

N.Mishchuk

Ivan Franko National University of Lviv,
Prospekt Svobody 18, UA – 79008, Ukraine

Concept of cybercrime as a dynamic group of crimes are investigated, existing methods for classification of computer crimes are analyzed, features of crimes, which were committed in the global computer networks, are characterized. Measures for the prevention cybercrime in the national information space are proposed.

Key words: cybercrime, cyber-crime, information technology, computer networks, protection of information resources.

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА ИНФОРМАЦИОННОГО ОБЩЕСТВА

Н.Мищук

Львовский национальный университет имени Ивана Франко
79008 г. Львов, проспект Свободы, 18

Исследовано понятия киберпреступности и киберпреступлений как динамической группы преступлений, проанализированы существующие методы классификации компьютерных преступлений, охарактеризованы особенности преступлений, совершенных в глобальных компьютерных сетях. Предложены меры по профилактике и предотвращению киберпреступности на отечественном информационном пространстве.

Ключевые слова: киберпреступность, киберпреступления, информационные технологии, компьютерные сети, защита информационных ресурсов.