Н.В. Савчук, асп.

КІБЕРЗЛОЧИННІСТЬ: ЗМІСТ ТА МЕТОДИ БОРОТЬБИ

У статті розкривається зміст поняття кіберзлочинність, її схеми та способи боротьби з нею.

The term computer crime, its schemes and cybercrime – fighting ways are described in this article.

Національна економіка та інфраструктура будь-якої країни сьогодні тісно пов'язані з сучасними комп'ютерними технологіями. Щоденна робота банківської та енергетичних систем, управління польотом літаків, транспортна мережа і навіть швидка допомога знаходяться в залежності від надійної роботи автоматизованих систем. Як і будь-який прогресивний винахід Інтернет та Інтернет-послуги містять у собі ряд небезпек, а саме нову особливу форму злочинства – «кіберзлочинність».

У XXI ст., в епоху розвитку інформаційних технологій та економіки знань, практично всі підприємства використовують в своїй роботі комп'ютери, а отже знаходиться в «зоні ризику». Швидкість, з якою розповсюджуються цифрові технології, можна порівняти лише з епідемією. Виникає небезпека несанкціонованого втручання в приватне життя громадян, шахрайство, розповсюдження вірусів, злому паролів, крадіжки кредитних карток та розповсюдження протизаконної інформації (від наклепу до матеріалів порнографічного змісту). Все це свідчить про актуальність вивчення поняття кіберзлочинності та способів боротьби з нею.

Питанням кіберзлочинності займаються такі зарубіжні та українські вчені як: Волчинская Е., Баурин Ю.М., Дашян М.С., Дешамп С., Кохутов М.М., Марков А.С., Юрасов А.В. та ін.

Метою статті є вивчення змісту поняття кіберзлочинність, її схем, негативних наслідків та способів боротьби з нею.

Поняття «комп'ютерна злочинність» вперше з'явилась в американській, а потім і в іншій іноземній літературі на початку 60-х років минулого століття. «***Комп'ютерна злочинність***» *– це порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних* [5, с.387]. За останні 10-15 років сформувалось поняття «***кіберзлочинність***» *– під якою розуміють злочинність в традиційному сенсі цього слова, але яка має місце в мережі Інтернет* [6, с.165]. Кіберзлочинність – це поняття, яке охоплює, на нашу думку, комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо.

Відповідно до оцінок експертів, кіберзлочинність здатна нанести збитки які можна порівняти з обсягом крадіжки виробів мистецтва у всьому світі. За даними ООН збитки, які наносить кіберзлочинність, можна порівняти з доходами від протизаконного обороту наркотиків та зброї. Крім того, кіберзлочинність виступає стримуючим фактором розвитку конкурентоспроможності економіки країн світу, в тому числі і України, оскільки покупці, підприємства та банки з пересторогою використовують нові технології – Інтернет-

послуги. Головною «жертвою» кіберзлочинності є економіка. Економічні наслідки в кіберпросторі досить важко підрахувати, тому що звертається до правоохоронних органів лише третина постраждалих. За даними Ради Європи, шахрайство з кредитними картками обходиться в 400 млн. дол. збитків щорічно, віруси за той же час спричиняють збитків на 12 млн. дол., прибутки від незаконного використання патентів та торгових марок складають 250 млн. дол. в рік – 5% від обсягів світової торгівлі [8].

Компанія Trend Micro опублікувала рейтинг десяти найбільш суттєвих кіберзлочинів за 2008 р., це:

1) фальшиві рахунки на оплату із Інтернет-магазину (підроблені рахунки, які розсилаються електронною поштою, містять посилання на шкідливі програми);
2) фальшиві повідомлення про доставку товару (злочинці часто видають себе за популярні поштові служби та розсилають листи, які під прикриттям повідомлення містять віруси);
3) фішинг – заволодіння платіжних особистих даних користувачів шляхом обману та шахрайське їх використання, який пов'язаний з електронною комерцією;
4) крадіжка особистих даних через фальшиве анкетування (користувачі, які люблять заповнювати різного роду анкети в обмін на різні подарунки, потрапляють до групи ризику);
5) компроментування популярних веб-сайтів (кіберзлочинці атакують ті сайти, які відвідує найбільша кількість користувачів);
6) відправлення результатів пошукових запитів (користувачам розсилаються посилання веб-сайти при використанні яких комп'ютер отримає вірус, що призводить до значних збитків);
7) вірусна реклама;
8) небезпечні привітальні листівки;
9) підроблені сайти благодійних фондів;
10) шахрайство на розпродажах (відвідавши сайт користувачі, клікнувши по банерній рекламі дешевого мобільного телефону, стають жертвами програми – троянський кінь TROJ_AYFONE) [10].

За дослідженням компанії Symantec кіберзлочинність переросла в високоефективний ринок збуту товарів, на якому присутні крадені товари та шахрайство. Загальний обсяг цього ринку у 2008 р. склав 276 млн. дол. Перше місце в рейтингу продаж займають крадені кредитні картки, їх частка складає 31% від загальної кількості пропозицій на ринку. Вартість крадених номерів кредитних карток коливається від 0,1 до 25 дол. за кожен номер. Середній залишок на картці, яка виставлена на продаж, складає 4000 дол. Зазвичай, номери карток продаються цілими лотами, а оптовим покупцям надаються знижки [10].

Нині виділяють такі види кіберзлочинності: шахрайство з пластиковими картками; несправжні Інтернет-аукціони; шахрайство з банківськими кредитами; пошук та використання «проривів» (похибок) в програмах; розсилка листів (спам); азартні ігри в онлайн середовищі; викуп та реєстрація доменних імен (кіберсквоттинг); крадіжка послуг (фоунфрейкинг, «staff fraud»); створення вірусів; крадіжка інформації та особистих даних; викладення у електронних ЗМІ неправдивих новин та ін. Так, зараження 30 млн. комп'ютерів фальшивими антивірусними програмами приносять кіберзлочинцям

прибутків в 10 млн. євро щорічно, а крадіжка особистих даних у 9 млн. громадян США обходиться у 1,2 млрд. дол. щорічно [10].

Окрім створення фіктивних електронних магазинів, інвестиційних банків, туристичних агентств, які збирають інформацію про кредитні картки та отримують гроші за неіснуючі товари та послуги, злочинці використовують ряд схем кіберзлочинності. Серед них найбільш розповсюджені такі:

1. *Схеми шахрайства з кредитними картками.* Найпростіший вид – ***Інтернет-кардинг*** – крадіжка коштів з пластикових карток в Інтернеті. Варіанти шахрайства трансакцій:

- покупець – введення номеру чужої картки; створення картки-двійника; отримання та використання товарів або послуг у формі інформації (книжки, компакт диски та інше) та відмова від їх оплати;
- продавець – збільшення суми платежу; запам'ятовування отриманого номеру картки та використання його для своїх покупок; відмова від угоди;
- банк – підробка трансакцій;
- зловмисники, які не беруть безпосередньої участі в угоді – несанкціонований збір інформації про користувача; генерація (зазвичай програмна) існуючого номеру пластикової картки; перехоплення даних платника при передачі, а також «злом» комп'ютерних систем продавця або банку, використання цих даних для маніпуляції з рахунками тощо.

Найбільш розповсюдженим видом злочинів, із-за недосконалості існуючих платіжних систем, є шахрайство з пластиковими картками.

2. Несправжні Інтернет-аукціони. Схема створення ажіотажу споживачів. Використовується при покупців товарів на Інтернет-аукціонах. Суть схеми: чим більше покупців збирається навколо виставленого лота, тим психологічно безпечно почувають себе інші учасники, які приєднуються до торгів. Щоб створити активний попит на товар, до участі в торгах «залучаються» покупці, які беруть участь в торгах до того моменту, поки реальний покупець не об'явить досить високу ціна за предмет торгу. Для виявлення таких шахраїв існують спеціальні комп'ютерні програми-роботи.

Схема покупки за найменшою ціною. Потенційний покупець пропонує найбільш низьку ставку, а його партнер – настільки високу, що інших бажаючих прийняти участь в аукціоні не знаходиться. В наступні хвилини або секунди Інтернет-аукціону, той хто запропонував високу ціну відмовляється від подальшої участі. Так, як ніхто за цей час не встигає зробити свою пропозицію то товар продається за низькою ціною.

3. Шахрайство з банківськими кредитами. Схема «Повітряного змія». Найпростіша схема – відкриття в двох банках рахунків з можливістю їх кредитування. Далі гроші переводяться з одного банку в інший та назад, з поступово зростаючими сумами. Суть такої операції полягає у тому, щоб до того, як банк виявить, що доручення про переказ грошей з рахунку не забезпечено необхідною сумою, приходило б повідомлення про переказ коштів в даний банк, так щоб загальна сума коштів на рахунку покривала вимоги при першому переводі. Цей цикл повторюється велику кілька разів до тих пір, поки на рахунку не опиниться значна сума грошей, яку швидко знімають, а власник рахунків зникає. Керувати такою схемою шахрайства можливо лише за допомогою комп'ютера.

4. *Пошук та використання «розривів» (похибок) в програмах.* Метод «Люк». Даний метод базується на використанні помилок в логіці побудови програм, яка використовується на чужому комп'ютері. В найденому «розриві» програма «розривається» і туди вписується необхідна кількість команд. При необхідності «люк» відкривається, а вбудовані команди автоматично здійснюють свої задачі. Одним із способів створення розриву є – *Dos-атака*. При такій атаці, не чекаючи відповіді від сервера, йому відсилається велика кількість пакетів певного розміру. В результаті цього значна частина серверних ресурсів буде зайнята надлишком інформації, після чого сервер стає перевантаженим або аварійно відключається від Інтернету, або «зависає». Даний тип атаки досить небезпечний, оскільки після її проведення всі підмережі будуть пошкоджені. Самою відомою атакою такого типу, є атака Code Red Worm – «червоний хробак» – вірус, який привів до того, що в 2001 р. о восьмій годині вечора, «упав» сервер американського Білого дому. Інша схема цієї групи «Троянський кінь», суть якого – введення до чужого програмного забезпечення таких команд, які дозволяють здійснювати інші, не заплановані власником програмні функції, зберігаючи в той же час попередні функції програми. При цьому програма буде виконувати не тільки ті функції, які цікавлять користувача, а й працювати в інтересах кібер-злочинців. Так, наприклад використовуючи «троянського коня» QAZ хакери в 2002 році отримали доступ до секретних програмних кодів компанії Microsoft [6, с.394].

5. Піраміди та листи по ланцюжку. Зазвичай такий лист містить список прізвищ та адресу, за якою одержувачу пропонується вислати незначну суму грошей (технологія електронних грошей ідеально підходить до таких схем). Потім необхідно замінити прізвище одного з одержувачів на своє та відіслати листи далі. Ті, хто погоджуються брати участь в піраміді стають спамерами (від слова «спам» – масова неперсоніфікована розсилка листів з різного роду рекламою) і в кінцевому рахунку більшість з них втрачають гроші. Так, за даними Message Lands у 2008 р. найбільші обсяги спаму були зафіксовані в Швейцарії (79,8%), Франції (78,3%), Австрії (78,2%) та Ізраїлі (76,9%). Найбільш всього від спаму страждають працівники сфери виробництва, де рівень електронної пошти складає 80,7% [9].

Піраміда Понці. Відмінність від попередньої схеми полягає в тому, що в даному випадку рекламується начебто вигідна ділова пропозиція, яка досить часто пов'язана з торгівлею. Фактично при цьому акумулюванні засоби шахраї не інвестують, а просто використовують вклади більш пізніх інвесторів, щоб заплатити більш раннім, створюючи таким чином видимість прибутковості та залучення нових жертв.

Розквіт Інтернет-пірамід в світі відноситься до першої половини 1990-х років. Сьогодні відбувається спад – схеми «пірамід» складають всього 1% серед мережевих шахрайств [6, с.396].

6. Викуп та реєстрація доменних імен. ***Кіберсквоттинг*** – вид шахрайства, який пов'язаний з викупом та реєстрацією, як правило масовою, доменних імен для їх подальшого перепродажу за значно завищеними цінами. Перепродаж доменних імен веб-сайтів характеризується великими масштабами. Постраждалими стають, як правило, власники відомих торгових марок, які дізнаються, що домен з їх торговою маркою вже зареєстровано на іншу особу або організацію. Так, наприклад, доменне ім'я business.com було продане кіберсквоттиром за 7,5 млн. долл.

7. Крадіжка послуг. До цієї групи правопорушень відносяться отримання несанкціонованого доступу до будь-якої системи, щоб безкоштовно скористатись її послугами. Прикладом даного

виду шахрайства є ***фоунфрейкинг***, тобто використання комп'ютера для проникнення в комунікаційну телефонну систему та незаконне використання послуг з надання міжнародного телефонного зв'язку. Інший приклад даного виду злочинів – *«staff fraud»* або створення нелегальних копій «двійників» мобільних телефонів. Схема «Уівінг» одна з найбільш розповсюджених злочинів цього виду, яка пов'язана з крадіжкою послуг та відбувається з використанням методу «заплутування слідів».

8. Викладення у електронних ЗМІ неправдивих новин. Схема Pump&Dump («збільшити та скинути») базується на викладенні в електронних ЗМІ, за допомогою злому сайтів новин, неправдивої інформації. Наприклад новин про наміри поглинання великою транснаціональною компанією невеликої компанії. Шахраї попередньо купують великий пакет акцій компанії, що поглинається. Ажіотажний попит, викликаний цією новиною, спричиняє зростання ціни на цінні папери цієї компанії, а шахраї продають їх на вершині попиту. Так, наприклад у 2000 р. SEC (US Securities and Exchange Commission) розкрила випадок шахрайства за схемою Pump&Dump, яке принесло комбінатору близько 300 000 дол. Шахраєм виявився 15-річний американський школяр [6, с.401].

Сьогодні кіберзлочинність має широке розповсюдження та наявність багатьох схем застосування. У зв'язку з цим виникає необхідність застосування певних заходів щодо попередження можливих негативних наслідків розповсюдження кіберзлочинності.

Способами захисту від кіберзлочинності можуть бути: отримання чіткої інформації про особу або підприємства (для перевірки репутації американських сайтів можна відвідати Інтернет-сторінку організації із захисту прав споживачів Better Business Bureau); використання електронних сертифікатів, ЕЦП, безпечних протоколів передачі даних; не надання продавцям реквізитів пластикових карт та паспортних даних; використання кредитних карток (в цьому випадку можливо здійснити чарджбек – процедуру опротестування трансакції); прийняття відповідних законодавчих актів тощо.

Боротьба з кіберзлочинністю вимагає спільних дій різних країн, активізації міжнародного співробітництва. Одним з таких кроків є підписання у листопаді 2001 р. Радою Європи, а також США, Канадою та Японією «Міжнародної конвенції про кіберзлочинність». Але оскільки кіберзлочинність частково належить до внутрішньої компетенції кожної держави окремо, то необхідним є паралельне напрацювання і національного законодавства, яке буде спрямоване на боротьбу з комп'ютерними злочинами.

Література:

1. В. Голубев. Стратегия и тактика борьбы с киберпреступностью в странах СНГ. - http://www.crime-research.ru/articles/golubev_june/
2. Голубев В.А. Интервью: Компьютерная преступность - угрозы и прогнозы. - http://www.crime-research.ru/interviews/golubev_interv06/
3. Голубев В.А. Компьютерная преступность - проблемы и решения. - http://www.crime-research.ru/articles/golubev_sept/
4. Голубев В.А. Компьютерная преступность - противодействие Интернет-мошенничеству. - http://www.crime-research.ru/articles/golubev0206/
5. Дашян М.С. Право информационных магистралей. – М, 2007. – 288 с.
6. Юрасов А.В. Основы электронной коммерции. Учебник. – М.: Горячая линия-Телком, 2008. – 480 с.
7. Dechamp C. Cybercriminalite // Defense nationale. – P., 2005. – P. 99-120.
8. www.coe.int (рада Європи)
9. http://www.itsec.ru/newstext.php?news_id=53005
10. http://www.itsec.ru/newstext.php?news_id=53003