УДК 343.346.8

Кіберпрофесіонали і кіберзлочинність

Горова Світлана Валеріївна –
науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат наук із соціальних комунікацій

У статті розглядаються основні проблеми, пов'язані із актуалізацією теми кіберзлочинності у зв'язку з активним розвитком інформаційних і телекомунікаційних технологій, масовою інформатизацією в Україні, в контексті чого з'явилось таке явище як хакерство, що використовується останнім часом у протиправній діяльності.

Ключові слова: кіберзлочинність, комп'ютерні технології, хакери, протиправні дії, інформаційне суспільство.

Постановка проблеми. Розглядаються основні напрями розвитку технологій протидії кіберзлочинності, що проникає у вітчизняну інфосферу.

Аналіз останніх досліджень і публікацій. Розробкою питань інформаційної безпеки та кіберзлочинності займаються вітчизняні та зарубіжні науковці, а саме: В. М. Бутузов, В. Д. Гавловський, В. М. Горовий, В. М. Петрик, М. М. Присяжнюк, В. С. Цимбалюк, О. М. Юрченко та інші, проте сучасний стрімкий розвиток інформаційного суспільства постійно дає новий матеріал для науково-практичних узагальнень.

Актуальність дослідження обумовлена зростанням суспільної важливості національної інформаційної безпеки в умовах глобальної інформатизації.

Метою статті є розгляд процесу кіберзлочинності в контексті розвитку хакерського руху, визначення основних загроз, пов'язаних з даним процесом.

Виклад основного матеріалу. Розвиток інформаційних і телекомунікаційних технологій, масова інформатизація в Україні забезпечили доступ до інформаційних ресурсів, до оперування цими ресурсами, до нового інфотворення, до розвитку програмного забезпечення управління інформаційними ресурсами, а, отже – і управління різними процесами суспільного життя – всім категоріям громадян, у тому числі й тим, що вбачають коло своїх інтересів за межами правового поля держави. Серед останніх найбільш помітною з початком розвитку електронних технологій в нашій країні стало хакерське, віртуальне співтовариство.

Характеризуючи розвиток цього специфічного для інформаційного суспільства співтовариства, Мануель Кастельс не лише зауважує про те, що його члени одержують задоволення від здобуття певного статусу в співтоваристві, від радості творчості, від зближення зі світом мистецтва, психологічним збудженням – "драйвом" від процесу творіння. Він говорить про розвиток характерного для цієї категорії людей "почуття вищості над усім іншим комп'ютерно безграмотним світом і тенденції спілкування з комп'ютером або з іншими представниками людства за посередництва комп'ютерів, зосереджуючись винятково на питаннях програмного забезпечення, незрозумілих для решти людства" [1, с. 47]. Дослідник звертає увагу також на те, що, на думку лідерів хакерського руху, лише тоді, "коли люди задовольнили свої базові потреби, вони можуть дозволити собі присвятити життя інтелектуальній творчості й лише потім діяти в умовах культури дарування" [1, с. 48].

Враховуючи той факт, що хакери в своїх захопленнях завжди опираються на найновіші здобутки комп'ютерної науки, техніки і технологій, і що за цими здобутками завжди не встигає і міжнародна правова база, і правотворення на рівні окремих держав, об'єктивно хакерська діяльність в основному своєму змісті знаходиться за межами законності. Щоправда, в засобах масової інформації час від часу з'являються повідомлення про використання талановитих хакерів у інтересах реалізації певних завдань інформаційних воєн, нової форми взаємовідносин інформаційного суспільства, про створення відповідних секретних підрозділів у оборонних відомствах, насамперед, основних країн – глобалізаторів. Однак, за тими ж повідомленнями, до роботи в цьому напрямі залучаються, як правило, хакери, що серйозно "засвітилися" на протиправних діях: зламах електронного захисту і грабуванні банків, у несанкціонованому входженні

в комп'ютерні системи управлінських структур, у протиправних заходах економічної розвідки та ін.

Отже, з одного боку, Інтернет дозволив ефективніше і безкарно вчиняти традиційні злочини, що існували раніше, з іншого – породив нові, донині невідомі види суспільно небезпечних посягань, сукупність і система яких виражається в такому негативному соціальному явищі як Інтернет-злочинність [2].

До речі, недавно ЗМІ інформували про пошук США "українських комп'ютерних геніїв", які спробували стягнути $15 млн з рахунків банків і держустанов, у тому числі Пентагону і податкової служби США. Кіберзлочинці проникали і зламували ці системи з березня 2012 року по червень 2013 року. За продуманою схемою хакери отримували контроль над рахунками компаній, потім переводили частину грошей на підконтрольні рахунки, а решту суми – в готівку [3].

Характерна для сучасного рівня розвитку інформаційного суспільства в цілому і рівня правового забезпечення діяльності в сфері застосування електронних інформаційних технологій в Україні ситуація, в цілому ж, не сприяє використанню хакерського руху в інтересах суспільного розвитку. Тобто, наше суспільство, як і в більшості країн світу, не знаходить поки що способу використання творчого потенціалу найбільш освічених своїх членів, таких, що найкраще знаються на електронних інформаційних технологіях, що є локомотивом розвитку інформаційного суспільства.

У той же час, даним потенціалом усе більш успішно користується професійна злочинність. Вона уміло використовує прагнення хакерів до економічної незалежності, заражає їх вірусом наживи, втягує до світу злочинності. Як правило, хакерські послуги використовуються у найбільш комп'ютеризованих сферах суспільної діяльності. Такі сфери охоплюють, насамперед, економіку, а в економіці – сферу банківських послуг, куди, насамперед, прийшли високі інформаційні технології з-за кордону у відповідності з реалізацією інтересів міжнародного співробітництва.

Нові можливості, що з'явилися в результаті розвитку інформаційних технологій, стали широко використовуватись представниками кримінального світу. А це, в свою чергу, призвело і до появи нових видів злочинів, пов'язаних, зокрема, з незаконним втручанням у роботу систем і комп'ютерних мереж, розкраданням і несанкціонованою зміною даних та ін. Відповідно, кіберзлочинність перетворилась на чинник, який став здійснювати вагомий тиск на суспільні відносини. Дослідники зазначають, що сьогодні вже кіберзлочинність стала багатоголовою гідрою, зважаючи на такі її характеристики як транснаціональність, латентність, динамічність темпів зростання та трансформацій, анонімність, масштабність наслідків тощо. В умовах глибокого латентного проникнення кіберзлочинності у суспільне та державне життя, її подолання стає наріжним каменем на шляху розбудови інформаційного суспільства і входження України у світовий інформаційний простір [5].

Експерти все частіше говорять про тривожну тенденцію: за останні роки кіберзлочинність стала більш організованою і почала набувати ознак бізнесу. Дії хакерів орієнтовані на отримання довгострокового доходу.

При всьому цьому, слід звернути увагу ще й на таку нині існуючу тенденцію: якщо раніше українські програмісти-хакери писали віруси для злому і розкрадання даних у багатих західних країнах, то тепер, у зв'язку з посиленням більш результативної боротьби американської та європейської влади з комп'ютерними злочинами, їхня увага переключилася й на Україну. Наша країна з її низьким рівнем обізнаності про загрози використання комп'ютерів і низьким рівнем інформаційної безпеки стає для них справжнім клондайком. Розкрадання коштів у системах Інтернет-банкінгу, даних кредитних карт, інсайдерські витоки інформації, DDoSатаки на сайти та шахрайство в мережах – явища вже звичні.

Як повідомляв раніше заступник начальника управління по боротьбі з кіберзлочинністю МВС України Леонід Тимченко, "за минулий рік за фактами використання скімингового обладнання та підроблених платіжних карток до відповідальності було притягнуто 164 особи. Не всі з них громадяни України – серед затриманих було 19 іноземних громадян, зокрема 6 громадян Молдови, 3 громадянина Румунії, 5 громадян Болгарії і 5 – Китаю" [5].

Як інформували ЗМІ, понад сто клієнтів столичного банку ледве не втратили своїх грошей. Виготовити дублікати їхніх карток планували троє громадян Румунії. Іноземці встановлювали на банкомати приховані відеокамери й чіпи: копіювали магнітні стрічки, записували пін-коди. Правоохоронцям знадобилося два тижні, щоб вистежити зловмисників [6].

Сьогодні рівень кіберзлочинності в Україні неухильно й системно зростає. Підтвердженням зростання таких злочинів у нашій державі є статистичні дані. За даними Управління боротьби з кіберзлочинністю МВС України, найбільш поширеними видами кіберзлочинів є: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів) і несанкціоновані дії з інформацією, яка ними обробляється. За 10 місяців 2012 року зафіксовано 44 таких втручання. За даними Державної служби фінансового моніторингу України, в 2012 році було зареєстровано 179 спроб несанкціонованого доступу до рахунків клієнтів банків на загальну суму понад 150 млн грн, при цьому сума коштів, у подальшому знятих злочинним шляхом, лише готівкою становить 9,5 млн грн [7].

За даними Української міжбанківської асоціації членів платіжних систем ЕМА, лише за дев'ять місяців 2013 року трапилося вже 257 випадків несанкціонованого доступу до рахунків клієнтів банків на суму 108 млн грн [8].

Згідно з повідомленням Нацбанку України, у 2012 році від кібернетичних злочинів постраж-

дали 40 % від загальної кількості українських банків. На початку 2013 року було виявлено 14 кіберзлочинів на загальну суму збитків близько 20 млн грн, з яких було повернуто 88 %.

За даними Нацбанку України, у 2011 році кількість протиправних операцій із платіжними картками в українських банках зросла до 7,6 тис. порівняно з 2,9 тис. у 2010 р., а обсяг неправомірного списання коштів збільшився майже в півтора рази і досяг 9,1 млн грн [9].

Начальник управління інформаційної безпеки Креді Агріколь банку Альона Кузьміна поінформувала, що з кожним роком правоохоронці виявляють на українських банкоматах усе більше скімерів, які зчитують пін-код з картки під час її введення: у 2011 році – 45, у 2012 році – 73, а у 2013 році – близько 160 [8].

Згідно з даними XVI випуску звіту Microsoft Security Intelligence Report (SIRv16), в якому проаналізовано вразливості та погрози по інформації з більше мільярда систем і популярних сервісів по всьому світу, Україна очолила антирейтинг країн, в яких налічується найбільша кількість сайтів, що містять шкідливі програми. Дослідження виявило, що кожен 16-й сайт в Україні містить шкідливе ПЗ, яким потенційно може бути заражений комп'ютер користувача. Так, на 1000 хостів припадає 59,2 заражених сайтів. Це найвищий показник у світі, для порівняння, в усій мережі Інтернет у середньому заражений приблизно кожен 54-й ресурс.

З усіх проаналізованих у звіті країн в Україні також виявлено найвищу концентрацію фішингових сайтів – кожен 70-й ресурс є шахрайським. Згідно з дослідженням, більш ніж кожен двохсотий сайт в Україні містить експлойти, які аналізують уразливості в системі й можуть ініціювати завантаження небажаних файлів на комп'ютер користувача без його відома [10].

На парламентських слуханнях на тему: "Законодавче забезпечення розвитку інформаційного суспільства в Україні", що відбулися у Верховній Раді України 18 червня поточного року, начальник управління боротьби з кіберзлочинністю МВС України С. Демедюк поінформував, що збитки від онлайн-злочинів та інших цифрових махінацій на сьогодні вже перевищили збитки від традиційних форм злочинності в Україні [11]. Слід також нагадати, що раніше повідомлялося, що Україна увійшла до трійки лідерів з DDoS-атак. За даними Лабораторії Касперського, 12 % від усіх атак припадає на Україну.

Експерти в своїх коментарях зазначають, що Україна – досить відомий центр хакерства, поряд із Росією, Бразилією, Китаєм і меншою мірою – Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування. Однак, в експертних колах існує й дещо спірна думка про те, що кіберзлочинність не є найбільшою загрозою для українців. Адже, наша країна в особливому становищі, – має один із найнижчих у Європі рівнів підключення до Інтернету.

Проте, незважаючи, а, можливо, всупереч вищенаведеному експертному твердженню, слід звернути увагу на дані німецького оператора зв'язку Deutsche Telekom, зазначені начальником управління інформаційної безпеки Креді Агріколь банку Альоною Кузьміною, яка вказала, що Україна за рівнем міжнародної кіберзлочинності дасть фору будь-якій іншій країні, адже вона перебуває на четвертому місці у світі після Росії, Тайваню та Німеччини за кількістю кібератак, що виходять з країни. "Щомісяця з українських серверів запускається понад 500 тис. шкідливих програм", – констатувала А. Кузьміна [8].

Начальник відділу боротьби зі злочинами у сфері платіжних систем Управління боротьби з кіберзлочинністю МВС України Богдан Тищенко раніше повідомляв про те, що СБУ у взаємодії з ФСБ Росії припинила діяльність групи хакерів, які через системи Інтернет-банкінгу протягом п'яти років викрали у різних країнах понад $ 250 млн. Організоване злочинне кіберугруповання налічувало близько 20 програмістів, які працювали в містах Києві, Львові, Одесі. ІТ-ведмежатники створили вірус, що проникав у комп'ютери під час скачування фотографій або перегляду відео в Інтернеті. Зловмисники отримували доступ до паролів й електронних ключів приватних осіб і компаній.

Строкаті за формою свого прояву протиправні дії, охоплювані поняттям "кіберзлочинність", у нашій країні самі по собі викликають занепокоєння, оскільки свідчать про проникнення цього виду злочинності в усі сфери суспільного життя. До цього ж слід звернути увагу також на ту обставину, що у зв'язку з подіями на Сході, концентрацією суспільної уваги правоохоронних органів на АТО, зростання кіберзлочинності в Україні в недалекому майбутньому може мати додатковий поштовх без відповідного посилення реакції з боку правоохоронних органів. Зростаюча злочинність, таким чином, є суттєвою перешкодою на шляху трансформації українського суспільства, підвищення його економічної, а також і політичної ефективності.

Дана небезпека, однак, стосується не лише наших внутрісуспільних проблем. Курс Президента П. Порошенка на прискорене зближення з Європою й Заходом обумовлює необхідність серйозної турботи про імідж України в зовнішньому світі. І серед складових цього іміджу все більшого значення набуває боротьба з кіберзлочинністю. Турбота про вирішення цієї проблеми в нинішніх умовах має життєво важливе значення для України, оскільки вона як ніколи раніше потребує інвестицій, активізації міжнародного економічного співробітництва, що не може бути ефективним у криміналізованій країні. У зв'язку з цим, очевидно, в рамках реалізації плану реформування органів внутрішніх справ, що сьогодні визначається як один із пріоритетів у сфері суспільних реформ – серйозний заслін існуванню і розвитку кіберзлочинності, як одній із основних небезпек розвитку сучасного інфор-

маційного суспільства. Трансформація правоохоронної системи має також передбачити постійне і системне співробітництво в даній сфері на міжнародному рівні. Саме тому окрім гармонізації кримінально-правових норм потрібна гармонізація процесуальних інструментів і вироблення нових механізмів міжнародного співробітництва. Тому важливу роль у боротьбі з кіберзлочинністю відіграють міжнародні угоди у відповідній області, такі як: Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського Союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проект ESCWA) та ін.

У процесі розвитку правової бази інформаційної діяльності дуже необхідним є також передбачення використання інтелектуального потенціалу комп'ютерних працівників, що визначаються сьогодні хакерами, в інтересах розвитку суспільства. Очевидно, держава має стимулювати цей вид інтелектуальної діяльності, сприяти, в тому числі й за допомогою правових актів, введенню його в суспільно значиме русло.

Список використаних джерел

1. Кастельс Мануель Інтернет – галактика / Кастельс Мануель. – К. : Ваклер, – 2007. – 304 с.
2. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.
3. Влада США розшукує двох хакерів-киян за спробу вкрасти 15 млн дол. [Електронний ресурс] // news-on.com.ua. – Режим доступу : http://www.news-on.com.ua/holovni-temy/2527-vlada-ssha-rozshykyut-dvoh-hakeriv-kiian-za-sproby-vkrasti-15-mln.html.
4. Тихомиров О. О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки / О. О. Тихомиров // Право України. – 2011. – № 4. – С. 252–259.
5. Обережно – кібершахраї! [Електронний ресурс] // ua24news. – Режим доступу : http://www.ua24news.com/suspilstvo/2167-oberejno-kibershahrai.html.
6. В столиці затримано банду кіберзлочинців [Електронний ресурс] // НТН. – Режим доступу : http://ntn.ua/uk/products/programs/svidok/news/2012/05/23/7954.
7. Протидія кіберзлочинності у фінансово-банківській сфері / [Електронний ресурс]. – Режим доступу : http://hbs.kharkov.ua/news_arcl.html.
8. Злодії нашого часу. В Україні зростає кількість крадіжок грошей з банківських карток [Електронний ресурс] // Кореспондент.net. – Режим доступу : http://ua.korrespondent.net/business/financial/3284906-korrespondent-zlodii-nashoho-chasu-v-ukraini-zrostaie-kilkist-kradizhok-hroshei-z-bankivskykh-kartok.
9. Правове регулювання кіберзлочинності [Електронний ресурс] // Всеукраїнська правова газета "Правосуддя України". – Режим доступу : http://ukrjustice.com.ua/pravove-rehulyuvannya-kiberzlochynnosti/.
10. Україна лідирує за кількістю шкідливих сайтів. Microsoft [Електронний ресурс] // finance.ua. – Режим доступу : http://news.finance.ua/ua/~/1/0/all/2014/05/25/326228.
11. Справа державної безпеки (нотатки з парламентських слухань "Законодавче забезпечення розвитку інформаційного суспільства в Україні) [Електронний ресурс] // Зовнішні справи. – Режим доступу : http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/sprava-derzhavnoji-bezpeki-notatki-z-parlamentskikh-sl/.

В статье рассматриваются основные проблемы, связанные с актуализацией темы киберпреступности в связи с активным развитием информационных и телекоммуникационных технологий, массовой информатизацией в Украине, в контексте чего появилось такое явление как хакерство, используемое в последнее время в противоправной деятельности.

The article examines the main problems concerning the actualization of the issue of cybercrime in connection with active development of information and telecommunication technologies, mass informatization in Ukraine, in this context there was such a thing as hacking, used in illegal activities.

Стаття надійшла до редакції журналу 16 вересня 2014 року.