УДК 658.1+004.056+65.012

Кавун С. В., Голубєв В. О.

АНАЛІЗ КІБЕРЗЛОЧИННОСТІ У СФЕРІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

У статті пропонуються результати проведеного авторами аналізу кіберзлочинності, який розглядається як загроза економічній безпеці для організацій. Аналіз виконано в рамках чинного законодавства України і низки міжнародних нормативних актів. Також наведено статистичні дані щодо стану в зазначеній проблемній сфері, на основі яких сформовано висновки та рекомендації. Деталізовано чинні міжнародні юридичні акти, спрямовані на поліпшення стану справ у сфері кіберзлочинності.

Ключові слова: *кіберзлочинність, загрози, економічна безпека, аналіз.*

В статье предлагаются результаты проведенного авторами анализа киберпреступности, который рассматривается как угроза экономической безопасности для организаций. Анализ выполнен в рамках действующего законодательства Украины и ряда международных нормативных актов. Также приведены статистические данные состояния в указанной проблемной области, на основе которых сформированы выводы и рекомендации. Детализированы существующие международные юридические акты, направленные на улучшение состояния дел в области киберпреступности.

Ключевые слова: *киберпреступность, угрозы, экономическая безопасность, анализ.*

Some results were proposed based on conducted by authors a cybercrime analysis, which can considering as an economic security threat for enterprises. This analysis is made in borders of current legislation of Ukraine and some international regulatory acts. In addition, a statistical condition data are shown in s specified problem area, based on which the conclusions and recommendations were formed. Some cur-rent international regulatory acts were shown in some details, which are directed to improve the state of affairs in the cybercrime.

Key words: *cybercrimes, threats, economic security, analysis.*

Постановка проблеми. У багатьох аналітичних звітах вітчизняних і зарубіжних дослідників та експертів [3; 9] досить часто зустрічаються поняття «кіберзлочинність» або «загрози». Усі ці поняття тією чи іншою мірою є аспектами економічної безпеки (ЕБ). Крім того, усі уявляють обсяги шкоди, що завдається в результаті «виникнення» подібних понять, і сьогодні вони обчислюються мільйонними і мільярдними сукупними сумами. І, природно, про всі ці аспекти знають багато керівників фірм та підприємств. Однак, тільки невелика кількість дійсно далекоглядних керівників виділяють на забезпечення ЕБ на підприємстві достатні обсяги коштів для запобігання (бо це дешевше), локалізацію та усунення (це вже дорожче) подібних випадків. Сьогодні вже всім зрозуміло, що стратегічні і навіть тактичні рішення щодо розвитку економіки і бізнесу неможливі без забезпечення інформаційної безпеки бізнесу та активної протидії кіберзлочинності.

Згадайте фатальне Твіт-повідомлення (від 23.04.2013 р.) для акаунта @AP (Агентство Associated Press), яке було запущено сирійськими хакерами (відповідальність за злом акаунта взяла на себе «Сирійська електронна армія» – угруповання, що підтримує уряд Башара Асада [8]) і повідомляло про два вибухи та поранення Барака Обами. Рух цін акцій, описаний одним із трейдерів як чистий хаос, швидко знищив $ 136 500 000 000 їх вартості протягом декількох хвилин. У результаті можна сформулювати узагальнений логічний висновок: кожен громадянин має (читаємо як зобов'язаний) знати, як захистити себе в кіберпросторі.

Аналіз публікацій. Сьогодні відомо досить багато досліджень у цій сфері, серед яких можна виділити найбільш помітні [4; 5; 6; 10], також відстежується тенденція, що подібні статті у своїй більшості публікуються в електронному вигляді. Однак проведений аналіз публікацій дозволив підтвердити ряд головних висновків: комп'ютерна

кримінальна епідемія розвивається стрімкими темпами; масштабність кіберзагроз, тобто обіг злочинних співтовариств у цій сфері, сягає 105-114 млрд дол. на рік (за оцінками з різних джерел), що підтверджують результати дослідження «Доповідь про кібернетичну злочинність 2010: ступінь впливу на суспільство», проведеного компанією Norton, які були оприлюднені в Гонконзі.

Виділення невирішених частин проблеми. У результаті проведеного дослідження останніх наукових публікацій можна зробити висновок, що питання дослідження кіберзлочинності та її аспектів становить інтерес для вивчення та розробки дослідників і фахівців.

Метою статті є показ поточного становища у сфері кіберзлочинності, формування низки рекомендацій щодо поліпшення стану в цій сфері з використанням міжнародної нормативної бази.

Основний матеріал дослідження. Наведемо ряд статистичних показників у цій галузі, показаних на рис. 1-4, які, на думку авторів, підтверджують актуальність і необхідність проведення досліджень у цій сфері. Як видно з рис. 1, зокрема для України, мається позитивна динаміка зменшення кількості атак-джерел, чого не можна сказати, наприклад, про Росію, Німеччину, США та ряд інших країн. Цей сайт-ресурс ще примітний тим, що показує в реальному часі світову карту проведення атак, які базуються на даних 101 джерела. При цьому загальносвітова тенденція має негативну динаміку збільшення середньої кількості кіберзлочинів.

Top 15 der Ursprungsländer von Angriffen des Vormonats

	Quelle des Angriffes	Anzahl der Angriffe
	Russian Federation	2,402,722
	Taiwan, Province of China	907,102
	Germany	780,425
	Ukraine	**566,531**
	Hungary	367,966
	United States	355,341
	Romania	350,948
	Brazil	337,977
	Italy	288,607
	Australia	255,777
	Argentina	185,720
	China	168,146
	Poland	162,235
	Israel	143,943
	Japan	133,908

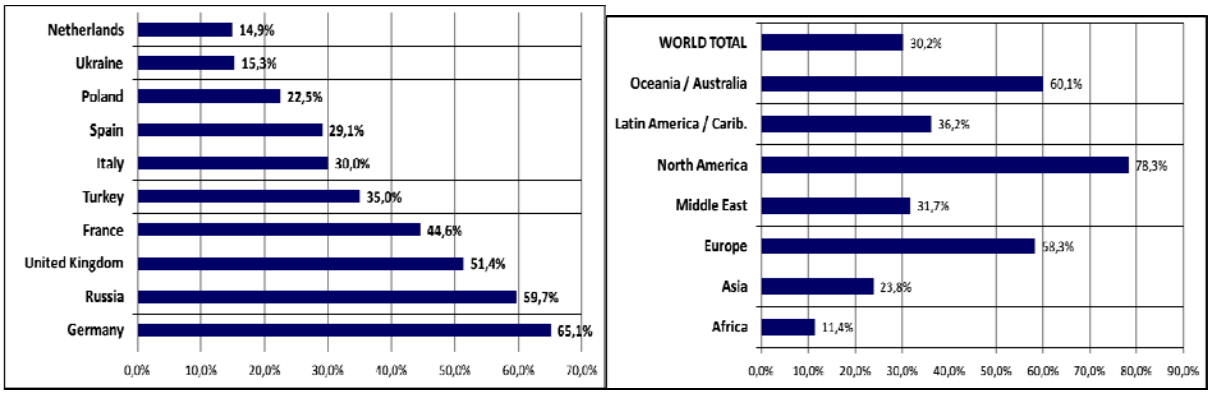
а) 9.03.2013

Top 15 der Ursprungsländer von Angriffen — Vormonat

	Quelle des Angriffes	Anzahl der Angriffe
	United States	922.045
	Russian Federation	866.048
	Taiwan	827.539
	Germany	447.668
	Israel	264.872
	United Kingdom	227.610
	Romania	197.590
	China	186.659
	Brazil	168.548
	Latvia	80.348
	Italy	74.965
	Venezuela, Bolivarian Republic of	51.766
	Japan	44.535
	Bulgaria	40.440
	Iceland	36.312

б) 16.09.2013

Рис. 1. Динаміка зміни країн за кількістю вихідних із країни кібератак за даними провідного німецького оператора зв'язку Deutsche Telekom, який візуалізував карту країн-джерел кібератак (http://sicherheitstacho.eu/?lang=de)



а) б)

Рис. 2. Кількість інтернет-користувачів в Європі (а) (від загальної популяції): загальний індикатор та вагова частка проникнення інтернет за географічними регіонами; (б): загальний індикатор (Internet Word Stats – www.internetworldstats.com)

Дані, що представлені на рис. 2а, показують частку населення, яка має доступ до інтернету і, отже, є потенційними «жертвами» кібератак і кіберзлочинів. Також можна припустити, що такий частотний розподіл може корелювати з динамікою реалізацій кібератак і кіберзлочинів, однак, як і будь-яке припущення, воно вимагає додаткової перевірки, яким би не було очевидним це припущення. Також непрямим чином подібну кореляційну залежність підтверджує розподіл вагової частки проникнення в інтернет за географічними регіонами (рис. 2б).

Разом із тим, багато державних структур (податкові, антимонопольні, правоохоронні органи тощо) при виконанні ними своїх функцій отримують від різних організацій або фізичних осіб значну кількість інформації, що формує різні механізми інтернет-злочинності (рис. 3).

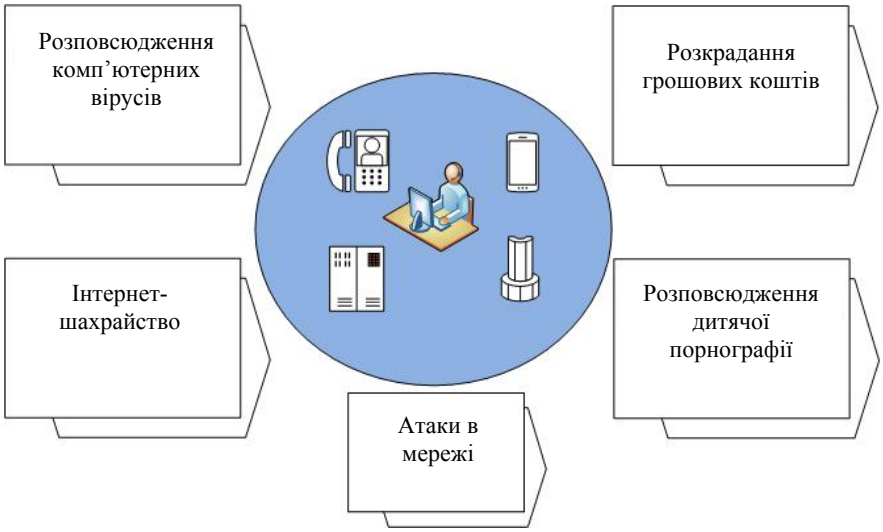


Рис. 3. Механізми формування інтернет-злочинності

.

Як відомо, інтернет уже давно розділився на загальнодоступну частину, тобто «видиму» частину (це сукупність сайтів, на які ми можемо вийти за допомогою пошукових систем, наприклад Яндекс або Google) та «невидиму мережу» (або «глибоку павутину» – «Deep Web»), потрапити в яку можна, лише знаючи конкретні адреси і через спеціальний браузер. На думку різних авторів, до видимого інтернету належить близько 20-30 % умісту всієї мережі. Найсміливіші джерела вказують іншу цифру – не більше 50 %. Таким чином, можна стверджувати, що невидимий інтернет – це основна частина ресурсів, доступних онлайн. Як видно з представлених даних, досить велика частина інформації з причини відсутності класифікації і неможливості обліку приносить невраховані втрати для підприємств. У першу чергу, це фінансові, кадрові, економічні та інші види втрат.

Одним із механізмів використання «тіньового» інтернету є Tor-механізм, сайти з його використанням мають шифровані імена з доменним ім'ям onion. Саме Tor створив найбільшу цибулинну мережу, у якій немає правил, законів і країн.

Існує багато видів кримінальних правопорушень, пов'язаних із використанням комп'ютерів [1], у рамках яких має місце розкрадання грошових коштів: атаки хакерів на банки або фінансові системи; шахрайства, пов'язані з переказом «електронних» грошей; шахрайства з банківськими пластиковими картами та ін.

За інформацією НБУ України, за 2012 р. загальна кількість шахрайських операцій із платіжними картами в нашій країні виросла відразу на 47 % і з 35 до 57 збільшилася кількість банків, із рахунків яких зникали кошти. Як і колись, за кількістю несанкціонованих списань із рахунків лідирували фізичні особи (щодня від населення надходить до 50 скарг, із рахунків за минулий рік зникло 11,4 млн грн). У банківській системі також з'явилися «нововведення»: на зміну скіммінгу прийшов новий вид крадіжки грошей із банківських карт. Відповідно до назви цієї технології «Шим» (shim – тонка прокладка) замість традиційних громіздких накладок на щілину приймача пластикових карт банкоматів (скіммерів) у шиммінгу використовується дуже тонка та гнучка плата, що впроваджується через цю щілину всередину банкомату і практично непомітна. За даними міністерства, у 2011 р. було виявлено 45 таких апаратів, а за перший квартал 2013 р. було виявлено вже 37 пристроїв. Кількість виявлених в Україні скіммінгових пристроїв у 2012 р. зросла на 62 %, а в 2013 р. сліди таких пристроїв вже виявляються кілька разів на тиждень, за повідомленням заступника начальника Управління у справах боротьби з кіберзлочинністю МВС України Леоніда Тимченка.

Фішинг – ще один механізм реалізації кіберзлочинів, заснований на використанні майстерно підроблених веб-сторінок. Зовнішній вигляд таких сторінок зазвичай ідентичний справжній, однак є ряд відмінних ознак:

– як правило, у фішингових сторінах у правій частині адресного рядка браузера відсутнє зображення замка, що свідчить, що обмін даними відбувається по захищеному з'єднанню, адреса в адресному рядку починається не з https://, а з http://;

– як правило, на «фішинговій» сторінці повідомлення шахраї просять ввести отриманий від банку разовий пароль, номер мобільного телефону тощо.

За даними МВС України, із січня до кінця листопада 2012 р. в Україні порушили 745 кримінальних справ із кіберзлочинів, у цей період було засуджено 113 осіб. За даними МВС Росії, кількість кіберзлочинів у Росії, зареєстрованих правоохоронними органами в 2012 р., зросла майже на третину, порівняно з 2011 р. За інформацією начальника Бюро спеціальних технічних заходів МВС РФ Олексія Мошкова, у 2012 р. у Росії було зареєстровано на 28 % більше високотехнологічних злочинів, порівняно з 2011 р.

Один із найпоширеніших видів мережевих атак на сучасні інфраструктури – DDoS-атаки (Distributed Denial of Service) [8]. Це атака на комп'ютерну систему з метою довести її до відмови, тобто створити такі умови, при яких легітимні користувачі системи не можуть отримати доступ до надаваних системою ресурсів (серверів або сервісів), або цей доступ ускладнений. Відмова «ворожої» системи може бути як самоціллю (наприклад, зробити недоступним популярний сайт), так і одним із кроків до оволодіння системою [2]. Якщо атака виконується одночасно з великої кількості комп'ютерів, то говорять про DDoS-атаку, одна з різновидів якої представлена на рис. 4. У деяких випадках до DDoS-атаки призводить легітимна дія, наприклад розміщення на популярному інтернет-ресурсі посилання на сайт, розміщений на не дуже продуктивному сервері.

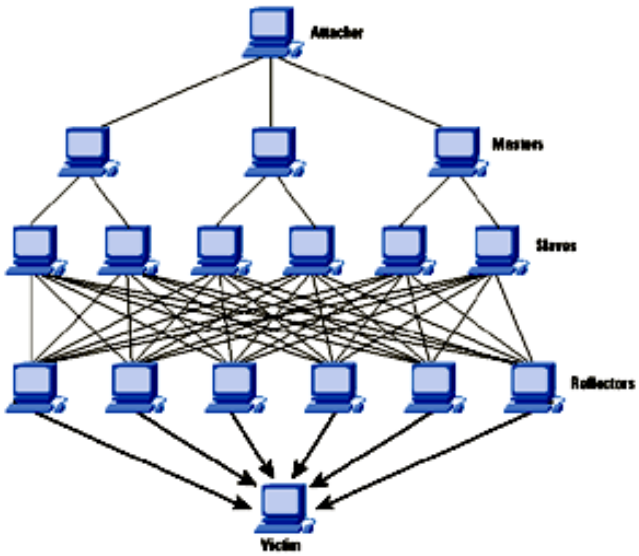


Рис. 4. Приклад реалізації розподіленої DRDoS-атаки

Робота машин зомбі може бути автономною або синхронізуватися атакуючим. Для того, щоб приховати свою IP-адресу, атакуючий фальсифікує адресу відправника, тобто крім описаного вище різновиду DDoS-атаки існує різновид DRDoS (Distributed Reflector DoS).

Фінансові та комерційні втрати через DDoS (упущений дохід, відтік клієнтів, зниження продуктивності праці і погіршення репутації) набагато перевищують прямі та операційні збитки організацій.

Захист від DDoS-атак полягає у відсіканні паразитного трафіку на рівні підприємства та провайдера під час доступу до інтернет, а також у нейтралізації мереж ботнетів, які здійснюють розподілені атаки.

Міжнародний аспект. Нині основним документом, що регулює питання міжнародного співробітництва в боротьбі з кіберзлочинністю, є «Конвенція про кіберзлочинність», [7]. Конвенція встановлює заходи, яких повинні вжити країни на національному рівні щодо правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушень, пов'язаних із комп'ютерами; правопорушень, пов'язаних із розповсюдженням дитячої порнографії, та правопорушень, пов'язаних із порушенням авторських і суміжних прав [4].

Окремий розділ Конвенції присвячено міжнародному співробітництву з питань екстрадиції у зв'язку з кримінальними правопорушеннями, передбаченими Конвенцією, добровільного надання інформації щодо проведення розслідування кримінальних злочинів, визначених Конвенцією, а також процедур, пов'язаних із запитами про

взаємну допомогу в разі відсутності міжнародних угод між країнами.

За даними Євросоюзу, щодня жертвами злочинів, скоєних в мережі, стає не менш одного мільйона чоловік. Сукупний збиток від них досягає 300 млрд євро за рік.

Із кіберзлочинністю ведуть боротьбу всі країни Євросоюзу [3], але досі – окремо один від одного і з вельми змінним успіхом. Багато національних правоохоронних органів швидко досягають меж своїх можливостей, адже місце злочину в мережі інтернет кордонів не має.

11 квітня 2013 р. на засіданні Ради Міжпарламентської Асамблеї СНД у своєму зверненні глава ПАРЄ Жан-Клод Міньйон (Jean-Claude Mignon) запропонував розвивати співпрацю з юридичних питань, а також у боротьбі з кіберзлочинністю.

Для колективної протидії загрозам кіберзлочинності 11 січня 2013 р. почав роботу Європейський центр із боротьби з кіберзлочинністю. Він є структурним підрозділом Європолу (Europol) зі штаб-квартирою в Гаазі. Серед пріоритетів Центру, розслідування інтернет-шахрайства, зокрема в системі електронного банкінгу та протидія інтернет-педофілії.

Складність проблем, які характерні для кримінальних правопорушень у мережі інтернет, робить необхідним тісне співробітництво між громадськими організаціями, експертами та правоохоронними органами країн СНД у цій сфері. У цьому напрямі багатьма компаніями здійснюється співробітництво у формі обміну інформацією, проведення розслідувань комп'ютерних інцидентів та надання сприяння в підготовці кадрів співробітників правоохоронних органів різних держав.

Висновки. Для ефективної боротьби з кіберзлочинністю потрібна система заходів і реалізація відповідної державної політики в цій галузі. Одні лише нові закони не здатні протистояти зростанню ІТ-злочинності. Потрібен комплекс заходів, спрямованих не лише на розвиток правозастосовної бази, але й на підвищення рівня грамотності громадян, судових та правоохоронних органів [9].

Одне з головних завдань – це організація плідної взаємодії з правоохоронними органами у сфері боротьби з кіберзлочинністю, а також надання допомоги компаніям, що постраждали від кібератак [3].

ЛІТЕРАТУРА

1. Geer D. Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. Geer Risk Services, LLC [Электронный ресурс] / D. Geer. – Режим доступу : http://www.verdasys.com/mt_geer.php.
2. Kavun S. V. (2012). Enterprise Insider Detection as an Integer Programming Problem. Intelligent Decision Technologies. Smart Innovation, Systems and Technologies / S. V. Kavun, I. V. Sorbat, V. V. Kalashnikov. – 16 (2), pp. 281–289.
3. Kavun S. (2013). Management of corporate security: new approaches and future challenges. Editorial Denis Galeta and Miran Vrsec. Cyber security challenges for critical infrastructure protection (pp. 141–151) / S. Kavun, R. Brumnik. Ljubljana : Institute for Corporate Security Studies. Retrieved August 5, 2013, from http://www.ics-institut.com/research/books/5.
4. Алавердов О. С. Международное сотрудничество в области борьбы с интернет-преступностью / О. С. Алавердов // Общество и право. – № 3. – 2010. – С. 165–167.
5. Бочаров Ю. Киберпреступность и кибертерроризм. Новая глобальная угроза государственному строю. 24 октября 2011 г. [Электронный ресурс] / Ю. Бочаров. – Режим доступа : http://www.elections-ices.org/russian/publications/textid:12835.
6. Бураева Л. А. Глобализация информационных процессов и рост киберпреступности [Электронный ресурс] / Л. А. Бураева. – Режим доступа : http://www.apriori-nauka.ru/uploads/files/BURAEVA-K10.pdf.
7. Закон України «Конвенція про кіберзлочинність» № 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, № 5-6, ст. 71 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_575.
8. Кавун С. В. Информационная безопасность в би знесе [монографія] / С. В. Кавун ; Харьковский национальный экономический университет. – Х. : 2007. – 408 с.
9. ФБР расследует взлом твиттера Associated Press. Материалы ресурса lenta.ru [Электронный ресурс]. – Режим доступа : http://lenta.ru/news/2013/04/24/investigation.
10. Чекунов И. В. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений [Электронный ресурс] / И. В. Чекунов. – Режим доступа : http://x5443x.ru/publ/1-1-0-36.

Дата надходження статті до редколегії 18.09.2013 р.

КАВУН Сергій Віталійович – кандидат технічних наук, доцент кафедри інформаційних технологій Харківського інституту банківської справи Університету банківської справи Національного банку України, м. Харків.

Коло наукових інтересів: дослідження у сфері інформаційної та економічної безпеки, моделювання інформаційної та економічної безпеки, кібербезпека, банківська безпека.

ГОЛУБЄВ Володимир Олександрович – кандидат юридичних наук, доцент, директор департаменту протидії кіберзлочинності корпорації «Noosphere Ventures», м. Запоріжжя.

Коло наукових інтересів: криміналістичні аспекти розслідування кіберзлочинів та інтернет-шахрайства.