УДК 658.1+004.056+65.012

Голубев В.А.

АНАЛІЗ КІБЕРЗЛОЧИННОСТІ У СФЕРІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Анотація:

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

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

Аннотация:

В статье предлагаются результаты проведенного авторами анализа киберпреступности, которая 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 сфере, на основе которых сформированы выводы и рекомендации. В некоторых деталях показаны существующие международные юридические акты, направленные на улучшения состояния дел в сфере киберпреступности.

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

Abstract:

Some results were proposed based on conducted by authors a cybercrime analysis, which can consider 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 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.

***Keywords:** 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”. Всі ці поняття тією чи іншою мірою є аспектами економічної безпеки (ЕБ). Крім того, всі уявляють обсяги шкоди, що завдається в результаті “виникнення” подібних понять, й сьогодні вони обчислюються мільйонними і мільярдними сукупними сумами. І, природно, про всі ці аспекти знають багато керівників фірм та підприємств. Однак тільки незначна 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 [10]) і повідомляло про два вибухи і 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 повинен (читаємо як зобов’язаний) знати, як захистити себе в кіберпросторі.

Аналіз публікацій

Сьогодні відомо досить багато досліджень у даній сфері, серед яких можна виділити найбільш помітні [8, 6, 5, 4], також відстежується тенденція, що подібні статті в більшості своїй публікуються в електронному вигляді. Однак проведений аналіз публікацій дозволив підтвердити ряд головних висновків: комп’ютерна кримінальна епідемія розвивається стрімкими темпами; масштабність кіберзагроз а, тобто, оборот злочинних співтовариств у цій сфері сягає 105–114 млрд. дол на рік (за оцінками різних джерел), що підтверджують результати дослідження “Доповідь про кібернетичну злочинність 2010: ступінь впливу на суспільство”, проведеного компанією Norton, яке було оприлюднено в Гонконзі.

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

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

Основний матеріал дослідження

Наведемо деякі статистичні показники (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, для Росії, Німеччини, США та інших країн. Даний сайт-ресурс також примітний тим, що показує у реальному часі світову карту проведення атак, яка основана на свідченнях 101 датчика. При цьому загальносвітова тенденція має негативну динаміку збільшення середньої кількості кіберзлочинів.

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 даний частотний розподіл може корелювати з динамікою реалізацій кібератак і кіберзлочинів, однак, як і всяке припущення, воно вимагає додаткової перевірки, яким би не було очевидним це припущення. Також непрямим чином подібну кореляційну залежність підтверджує розподіл вагової частки проникнення Інтернет за географічними регіонами (рис. 2б).

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

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

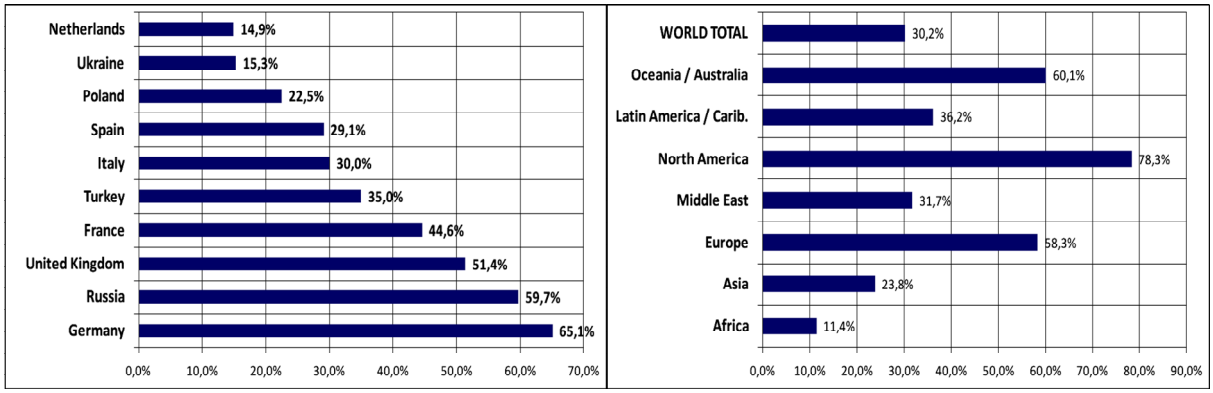
а) 9.03.2013

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 з 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, джерело Internet Word Stats – www.internetworldstats.com

Як відомо, Інтернет вже давно розділився на загальнодоступну частину, тобто "видиму" частину (це сукупність сайтів, на які ми можемо вийти за допомогою таких пошукових систем як 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 порядку 20–30 % вмісту всієї Мережі. Найсміливіші джерела зазначають іншу цифру – не більше 50%. Таким чином, можна стверджувати, що невидимий Інтернет – це основна частина ресурсів, доступних онлайн.

Як видно з представлених даних, досить значна частина інформації через відсутність класифікації і неможливість обліку, завдає невраховані втрати для підприємств. Насамперед це фінансові, кадрові, економічні, фінансові та інші види втрат.

Рис. 3 Механізми формування Інтернет-злочинності

Одним із механізмів використання “тіньового” Інтернет є Tor-механізм, сайти з його використанням мають шифровані імена з доменним ім’ям .onion. Саме Tor створив найбільшу цибулинну мережу. Це мережа, в якій немає правил, законів і країн.

Існує багато видів кримінальних правопорушень, пов’язаних з використанням комп’ютерів [1], в рамках яких має місце розкрадання грошових коштів: атаки хакерів на банки або фінансові системи; шахрайства, пов’язані з перерахунком “електронних” грошей, банківськими пластиковими картами та ін.

За інформацією НБУ України, за 2012 р. загальна кількість шахрайських операцій з платіжними картами в нашій країні зросла відразу на 47% і з 35 до 57 збільшилася кількість банків, з рахунків яких пропали кошти. Як і колись, за кількістю несанкціонованих списань з рахунків лідирували фізичні особи (щодня від населення надходить до 50 скарг, з рахунків за минулий рік пропало 11,4 млн грн). У банківській системі також з’явилися “нововведення”: на зміну скіммінгу, прийшов новий вид крадіжки грошей з банківських карт. Згідно з назвою за даною технологією “Шим” (shim – тонка прокладка), замість традиційних громіздких накладок на щілину приймача пластикових карт банкоматів (скімерів), в шиммінгу використовується дуже тонка та гнучка плата, що упроваджується через цю щілину всередину банкомату і практично непомітна.

За даними міністерства, в 2011 році було виявлено 45 таких апаратів, у 2012–2013 роках і за перший квартал 2013 року було виявлено вже 37 пристроїв.

Кількість виявлених в Україні скіммінгових пристроїв в 2012 році зросла на 62%, а в 2013 році сліди таких пристроїв вже виявляються кілька разів на тиждень, повідомив заступник начальника Управління по боротьбі з кіберзлочинністю МВС України Леонід Тимченко.

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

– як правило у фішингових сторінок у правій частині адресного рядка браузера відсутнє зображення замка, що свідчить, що обмін даними відбувається за захищеним з'єднанням, 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 й т. ін.

За даними МВС України, з січня по кінець листопада 2012 року в Україні порушили 745 кримінальних справ з кіберзлочинів, у цей період було засуджено 113 осіб.

За даними МВС Росії, кількість кіберзлочинів в Росії, зареєстрованих правоохоронними органами в 2012 році, зросла майже на третину порівняно з 2011 роком. За інформацією начальника Бюро спеціальних технічних заходів МВС РФ Олексія Мошкова, в 2012 році в Росії було зареєстровано на 28% більше високотехнологічних злочинів порівняно з 2011 роком.

Один з найпоширеніших видів мережних атак на сучасні інфраструктури є DDoS-атака (Distributed Denial of Service) [9]. Це атака на комп'ютерну систему з метою довести її до відмови, тобто створити таки 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, одну з різновидів якої представлено 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.

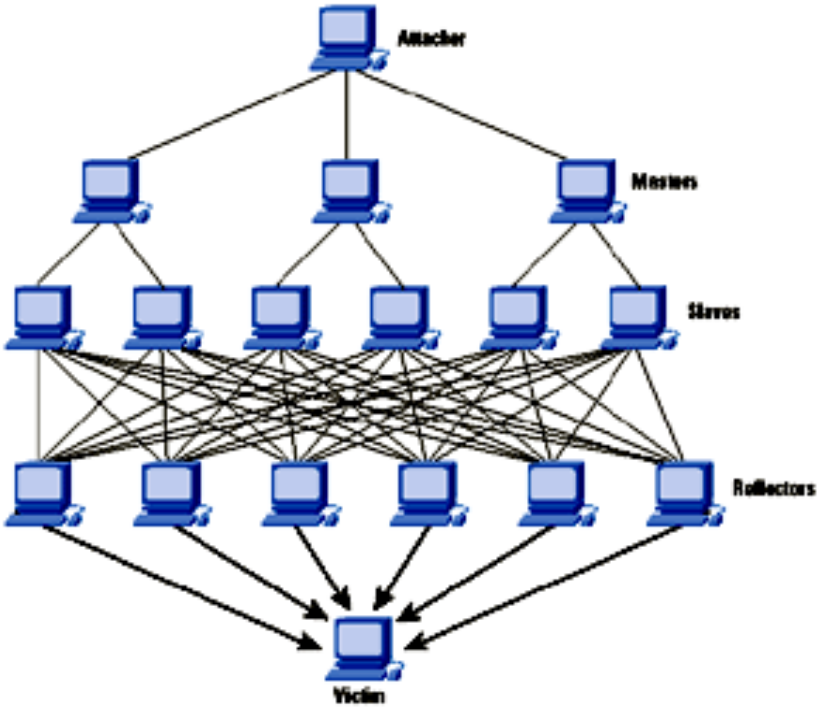


Рис. 4 Приклад реалізації розподіленої DRDoS-атаки

Робота машин зомбі може бути автономною або синхронізуватися з атакуючими. 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-атаки (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 трафіка на рівні підприємства та провайдера під час доступу до Інтернет, а також у нейтралізації бот-мереж, які здійснюють розподілені атаки.

Міжнародний аспект

На сьогоднішній день, основним документом, що регулює питання міжнародного співробітництва в боротьбі з кіберзлочинністю є "Конвенція про кіберзлочинність" [7]. Конвенція встановлює заходи, яких мають вжити країни на національному рівні щодо правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушень, пов'язаних з комп'ютерами, розповсюдженням дитячої порнографії та з 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 у разі відсутності міжнародних угод між країнами.

За даними Євросоюзу, щодня жертвами злочинів, скоєних в Мережі, стає не менш одного мільйона осіб. Сукупний збиток від них досягає 300 мільярдів євро на рік.

З кіберзлочинністю борються всі країни Євросоюзу [3], але до цього часу – 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 на засідання 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 року почав роботу Європейський центр з боротьбі 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 сприяння у підготовці кадрів співробітників правоохоронних органів різних держав.

Висновки

Для ефективної боротьби з кіберзлочинністю потрібна система заходів і реалізація відповідної державної політики у цій сфері. Одні лише нові закони не здатні протистояти зростанню ІТ-злочинності. Потрібен комплекс заходів, націлених 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. [Electronic Resource] – Mode of access: http://www.verdasys.com/mt_geer.php.

2. Kavun S.V. Enterprise Insider Detection as an Integer Programming Problem. Intelligent Decision Technologies. / S.V. Kavun, I.V. Sorbat, V.V.Kalashnikov // Smart Innovation, Systems and Technologies. – 2012. – № 16 (2). – P. 281–289.

3. Kavun. S. Management of corporate security: new approaches and future challenges [Electronic Resource] / S. Kavun, S. R. Brumnik // Cyber security challenges for critical infrastructure protection. –Ljubljana: Institute for Corporate Security Studies. – 2013. – P. 141–151. – Mode of access: 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. [Электронный ресурс] / Ю.Бочаров // International expert Center for Electoral Systems (ICES) – 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 // Экономика. Право. Менеджмент: современные проблемы и тенденции развития (Материалы II Международной научно-практической конференции, 31 августа 2012). – Режим доступа: http://www.apriori-nauka.ru/uploads/files/BURAEVA-K10.pdf.

7. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001. [Электронный ресурс] // Офіційний вісник України – 2007. – № 65. – С. 107, ст. 2535.– Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575.

8. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И.Г. Чекунов // Право и кибербезопасность. – 2012. – № 1. – С. 23–38.

9. Кавун С. В. Информационная безопасность в бизнесе. Монография / С. В. Кавун. – Харьков: ХНЭУ, 2007. – 408 с

10. ФБР расследует взлом твиттера Associated Press. [Электронный ресурс]. – Режим доступа: http://lenta.ru/news/2013/04/24/investigation.