УДК 007:341.4(045)

Якубівська Ю.Є. *кандидат економічних наук, доцент кафедри фінансово-економічної безпеки та інтелектуальної власності Тернопільського національного економічного університету*

СВІТОВІ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ

Анотація. *На сучасному етапі розвитку України особливої уваги потребує система кібернетичної безпеки як ключовий елемент інформаційної, а відтак, і національної безпеки. Зважаючи на зростаючу кількість кібератак, необхідним є не лише дослідження світових тенденцій розвитку кіберзлочинності, створення ефективного нормативно-правового забезпечення, але й системи заходів для попередження та захисту від кіберзлочинності.*

Стаття присвячена дослідженню тенденцій кіберзлочинності, що є загрозою інформаційній безпеці країни. Визначено місце і роль кібербезпеки в системі національної безпеки. Основна увага зосереджена на дослідженні проявів кіберзлочинності й активності кібератак на світовому рівні, а також тих, які торкнулися українського інформаційного простору. Подано рекомендації щодо покращення системи захисту та боротьби з кіберзлочинністю.

Ключові слова: *національна безпека, інформаційна безпека, кібернетична безпека, кіберпростір, кіберзлочинність, кібератака.*

Постановка проблеми. Сучасні світові тенденції розвитку кіберзлочинності та її посилення свідчать про зростання значення боротьби з нею для подальшого розвитку суспільства, що, в свою чергу, зумовлює віднесення певних груп суспільних відносин кіберсфери до компетенції правового регулювання. Особливо актуально зазначена проблема торкається забезпечення національної безпеки та, відповідно, суспільно небезпечних діянь, які повинні набути статусу злочинів у кіберсфері та нести за собою відповідну юридичну відповідальність. На жаль, Україна на сьогоднішній день слабко задіяна у процесі боротьби з кіберзлочинністю й, відповідно, є незахищеною від атак у сфері інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Проблематика боротьби та подолання кіберзлочинності виступає об'єктом дослідження таких вчених, як: Н. Андерсон [9], В. Бурячок [2], А. Козловскі [10], Е. Старостіна [7], А. Щетилов [8] та ін. На основі опрацювання вищевказаних публікацій можна зробити висновок, що кіберсфера як сфера обміну та обробки інформації, представленої у вигляді комп'ютерних даних, відіграє значну роль у процесах розвитку кожного суспільства, а поява кіберзагроз зумовлює необхідність охоплення її відповідними регулятивними та охоронними функціями права, відповідно підвищуючи увагу як теоретиків, так і практиків до кібербезпеки як до окремої складової національної безпеки України. Однак, є ряд проблем, які, зважаючи на стрімкий розвиток кіберзлочинності та, зокрема, кібератак на Україну з боку окремих країн світу (а, насамперед, ідеться про Китай, США та Росію), потребують додаткового дослідження і визначають актуальність написання даної наукової статті.

Метою дослідження є вивчення тенденцій розвитку кіберзлочинності. Для досягнення зазначеної мети були поставлені такі завдання:

– визначити роль та місце кібернетичної безпеки в контексті національної безпеки України;

– дослідити генезу й проаналізувати прояви кібератак на світовий та український простір;

– запропонувати шляхи захисту українського простору від кібератак.

Виклад основного матеріалу. Сучасні тенденції державотворення України характеризуються поступовим формуванням системних підходів до національної безпеки, в контексті яких забезпечення інформаційної безпеки, у тому числі й кібербезпеки, посідають одне з го-

ловних місць. Згідно з Доктриною інформаційної безпеки України, інформаційна безпека визначена невід'ємною складовою національної безпеки і, в той же час, важливою її самостійною сферою, а відповідно до ст. 17 Конституції України вона детермінується як одна із головних функцій держави [5; 6]. На сьогодні активно відбуваються процеси розробки нормативно-правового забезпечення, яке визначає правове підґрунтя державної діяльності у даній сфері. Заслуговує на увагу, думка автора, що кібернетична безпека як нова на законодавчому рівні, однак важлива складова інформаційної безпеки, а відтак, і національної безпеки України.

Починаючи з кінця 2013 року, конфлікти, що виникали, передусім, між державами, установами та організаціями, чи окремими особами перейшли у кіберпростір. Уряди провідних країн світу використовують різного роду кібератаки з метою пошкодження чи навіть ліквідації конфіденційної інформації або стратегічних ресурсів конкурентів та супротивників. Розглянемо найбільш типові загрози та об'єкти, що підлягають під кібератаку:

1. Мобільне рекламне програмне забезпечення (так зване «mobile advertising software» або «madware»). Така загроза може не лише перешкодити самому процесові використання пристрою, але також і вказати зацікавленим особам, хакерам ідентифікаційні дані вашого мобільного пристрою, місцезнаходження та контактні дані особи тощо. Спеціальна програма типу «madware», що непомітно потрапляє на пристрій користувача, паралельно встановлює додаткові програми, про які користувач до цього не здогадувався, а це, в свою чергу, створює нові ярлики, призводить до закидання користувача різними спливаючими вікнами, або ж навіть змінює налаштування браузера і водночас збирає його особисті дані, хоча сам користувач про це може й не здогадуватись. Тільки за 2013 рік кількість програм, що містять найбільш агресивні типи «madware», зросла на 210 %. На сьогодні загрозливі програми надсилають платні SMS-повідомлення, а перераховані кошти дістаються хакерам та зловмисникам.

2. Комп'ютерне програмне забезпечення, заражене вірусом, а також кібернапад. У той час, коли поширеність так званих «псевдо-антивірусів» нівелюється, в кіберпросторі з'являються потужніші загрози, як скажімо, загрози типу «ransomware» (в пер. з англ. – викуп), шантажуючі програми, які вимагають внесення відповідної суми оплати. Однак дана схема характеризується певними незручностями для хакерів, як приміром, неможливістю зручно та безпечно отримати бажані кошти. Наступним методом, що широко використовувався вже на початку 2014 року, став кібернапад з метою нанесення емоційної шкоди, так званий метод залякування – «кібербуллінг» (даний метод широко застосовується і по сьогодні щодо українських користувачів мережі Інтернет у політичному контексті).

3. Соціальні мережі. Фінансування соціальних мереж формує нову серію загроз. Адже користувачі Інтернету з кожним днем усе з більшою довірою ставляться до різного роду соціальних мереж (наприклад, Vkontakte, Odnoklassniki, Mail.Ru Agent, Skype, Viber, Instagram, Facebook, Twitter тощо), включаючи обмін своїми особистими даними й купівлю спеціальної мережевої чи ігрової валюти і так званих віртуальних подарунків іншим користувачам. Із зростанням рівня монетизації соціальні мережі надають своїм активним користувачам можливість надсилати один одному також справжні подарунки у вигляді матеріальних цінностей, а не лише нематеріального об'єкта, в соціальних мережах відбувається зростання грошового обігу, що дає хакерам нові можливості для формування загроз та здійснення атак.

4. Платіжні операції в системі он-лайн та інтернет-банкінг (скажімо, Privat24 в Україні, Pekao24 у Польщі, Vtb24 в Росії), що може стати потенційним об'єктом крадіжки особистих даних і призводить до обману користувачів та провокує останніх повідомити такі дані неофіційним соцмережам. Прикладом можуть бути фальшиві сповіщення про отримані подарунки, а також електронні листи з вимогами від певного користувача вказати особисту інформацію чи навіть домашню адресу. З першого погляду, надання такого роду нефінансової інформації може видаватись нешкідливою дією, однак хакери обмінюються та торгують нею, поєднуючи такі дані з уже наявними у них, що на перспективу дозволяє їм отримати доступ до конфіденційної інформації.

5. Електронні гаманці «eWallet», що поступово перетворюються у специфічний об'єкт, який хакери пробують використовувати у своїх цілях. «eWallet» можуть бути вразливими, що

потенційно веде до крадіжки особистої інформації. А в міру широкого впровадження зручних технологій мобільних платежів, саме мобільні телефони стануть представляти для хакерів ще більшу цінність. Даний процес схожий на загрозу «Firesheep», що працює спеціально для перехоплення чужих Wi-Fi сесій, а тому можна вже в найближчий час очікувати створення й появи на ринку спеціальних хакерських програм, які будуть перехоплювати особисту платіжну інформацію користувачів та застосовувати її з користю для зловмисників.

6. Так звані «хмарні» носії інформації типу «Cloud» (наприклад, e-Dysk, iCloud, Google Drive тощо). Включення до конкретної корпоративної мережі незахищених пристроїв, які накопичують інформацію, а після цього вона осідає вже на інших «хмарних» носіях, а це в свою чергу різко підвищує ризик витоку інформації або потенційного захоплення особистих незахищених даних. У результаті, встановлення користувачами нових програм призводить до зараження всієї системи [4].

Швидка комп'ютеризація всього світу, яка відбувається з початку 90-х років минулого сторіччя, із поширенням Інтернету призвела до того, що дедалі більше й більше інформації про людей, підприємства та державні структури було передано у віртуальний світ, у тому числі дані, що стосуються національної інфраструктури. Даний факт впливає на безпеку держави, а також, водночас, створює нові ділові можливості для заподіяння шкоди конкурентові. Україна, приміром, не є винятком, оскільки бачить можливості й ризики, які пов'язані із зростанням ролі кіберпростору в контексті формування засад національної безпеки.

Кібершпигуни не обмежуються атаками у віртуальному світі, але й виконують розширені операції кібершпигунства для доступу до стратегічних напрямів, привабливих з точки зору економічних і політичних інтересів. Прикладом кібератаки на Україну є виявлення програми-шпигуна «Snake» у мережі, який був схожий на прототип «Stuxnetu», що використовувався в іранській ядерній програмі. Дана програма дає змогу повною мірою вести контроль над програмним забезпеченням. У вересні 2013 року в Україні побільшало кібератак на засоби масової інформації (ЗМІ) – 4 кібератаки, тоді як протягом усього літа було зафіксовано лише 2 DDoS-атаки на сайти ЗМІ. Наступні дані подає щомісячний моніторинг Інституту масової інформації (ІМІ) «Барометр свободи слова»: три літніх місяці поспіль 2014 року ІМІ фіксує збільшення кількості випадків кіберзлочинів проти журналістів та ЗМІ (у липні – 4, в червні – 4, у травні – 6, в квітні – 1, у березні – 18, в лютому – 5, у січні – 13) [1].

Прикладом посягання на конфіденційну інформацію на міжнародному рівні стало викрадення хакерами у жовтні 2014 року конфіденційних даних щодо української адміністрації та американських науково-дослідних університетів зі структури НАТО. Одним із об'єктів, що становив інтерес для хакерів, була також польська енергетична компанія. Під час кібератак хакери використовують уразливість у системі Windows. Йдеться про феномен так званого розриву «Нульового дня» («zero-day») – системи, що провокує розрив у всіх версіях операційних систем, підписаних ОС Windows, починаючи з Windows Vista й закінчуючи Windows 8.1. Операційна система, яка була позбавлена помилки «zero-day» є Windows XP. Використовуючи ці знання, хакерам вдалося отримати доступ до даних щодо стратегічно важливих інститутів у структурах НАТО. Виявляється, що об'єктами кібершпигунства також стали нормативні документи з питань адміністрації України, бази даних американських університетів і багатьох інших установ, відповідальних за координацію питань, пов'язаних з національною безпекою в країні.

Спеціалісти Національного інституту стратегічних досліджень при Президентові України у своїй аналітичній доповіді на тему «Кібербезпека: світові тенденції та виклики для України» виділяють три основні, тісно пов'язані проблеми, що ускладнюють боротьбу проти злочинів у кіберсфері:

1) відсутність сформованих визначень ключових понять і термінів: «кібербезпека», «кіберпростір», «кібератака», «кіберзахист», «кібервійна», «кібертероризм», що потенційно можуть ефективно застосовуватись у практиці правоохоронної діяльності;

2) нереформованість чинного нормативно-правового поля у сфері кібербезпеки;

3) відсутність Єдиної загальнодержавної системи протидії кіберзлочинності з необхідним

нормативним забезпеченням [3].

Українським службам безпеки необхідно постійно моніторити діяльність та специфіку кіберзлочинів у віртуальному середовищі. Події 2013-2014 рр. на світовому рівні вказали на необхідність підсилення інформаційної безпеки.

Висновки. Отже, розглянувши стан кібербезпеки на території України, проаналізувавши тенденції розвитку кіберзлочинності на світовому рівні, дослідивши досвід окремих країн світу в даному напрямі, можемо зробити наступні висновки:

1. Україна повинна продовжувати активні дії в контексті розбудови власної системи кібербезпеки. Для реалізації даного завдання необхідно пришвидшити підготовку і подальше прийняття Закону про кібернетичну безпеку, який рекомендовано внести як терміновий для розгляду Верховною Радою України.

2. Сформувати національну стратегію з кібербезпеки, що міститиме тактичні та стратегічні пріоритети й завдання у даній сфері для державних органів.

3. Посилити охорону і захист інтелектуальної власності на внутрішньому та зовнішньому ринках.

4. Внести зміни до навчального навантаження студентів за спеціальностями, що готують фахівців-професіоналів у сфері економічної безпеки, а саме: запровадити навчання з дисциплін, які пов'язані з кібербезпекою, промисловим шпигунством, безпекою ІТ-сектору.

5. Широкомасштабна інформатизація держави зумовлює необхідність розгляду даної проблеми на найвищому державному рівні. Позитивним є акцент на її обговоренні у ході засідань Ради національної безпеки та оборони України в 2014 році. Україна, зважаючи на події 2013-2014 рр., повинна посідати більш активну позицію з питань кібербезпеки на міжнародній арені, оскільки потребує здійснення системи комплексних навчань з протидії важким злочинам саме у кіберсфері. Окрім навчань на рівні держави, доречною була б участь України, приміром, у загальноєвропейських навчаннях з питань кібербезпеки.

Питання безпеки кіберпростору, боротьби з кіберзлочинністю є актуальним як на міжнародному рівні, так і на рівні окремої країни, а тому потребує подальшого розгляду.

Список використаної літератури

1. Барометр свободи слова за серпень 2014 р.: [Електронний ресурс] / Інститут масової інформації, 2014. – Режим доступу: http://imi.org.ua/barametr/45643-barometr-svobodi-slova-za-serpen-2014-roku.html

2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки : [Монографія] / В.Л. Бурячок. – К. : НАУ, 2013. – 432 с.

3. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь: [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf

4. Конфлікти між державами та організаціями у 2013 році перейдуть у кіберпростір : [Електронний ресурс]. – Режим доступу:

http://dt.ua/TECHNOLOGIES/konflikti_mizh_derzhavami_ta_organizatsiyami_u_2013_rotsi_pereydut_u_kiberprostir.html

5. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=254%EA%2F96-%E2%F0

6. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009

7. Старостина Е. Терроризм и кибертерроризм – новая угроза международной безопасности: [Электронный ресурс]. – Режим доступа: http://www.crime–research.ru/articles /starostina

8. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом: [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/library/chetilov.htm

9. Anderson N. Massive DDoS attacks target Estonia; Russia accused : [Електронний ре-

cypc] / Nate Anderson // Ars Technica. Retrieved, 2007. – Режим доступу: http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/

10. Kozłowski A. Cyberwojownicy Kremla : [Електронний ресурс] / Andrzej Kozłowski // Stowarzyszenia Europejskie Centrum Analiz, 2014. – Режим доступу: http://geopolityka.org/analizy/2836-andrzej-kozlowski-cyberwojownicy-kremla

***Yakubivska Yu.E.**, PhD in Economics,*
Associate Professor of Financial-Economic Security and Intellectual Property,
Ternopil National Economic University

GLOBAL TRENDS IN CYBERCRIME

***Abstract.** At the present stage of economic development Ukraine requires special attention for cyber security system as a key element of information security, and thus national security. According to the growing number of cyberattacks in the world, it is necessary not only research of global cybercrime trends, creation of the effective legal support, but also measures to prevent and protect against cybercrime.*

The article investigates cybercrime trends that threaten state information security. The cybercrime place and role in national cyber security are determined. The main focus is concentrated on the study of cybercrime manifestations and cyberattacks activity on a global level, as well as those which have occurred in Ukrainian information space. Recommendations of protection system improvement and fighting process against cybercrime are given.

***Keywords:** national security, information security, cyber security, cyberspace, cybercrime, cyberattacks.*

References

1. Freedom speech barometer for August 2014 : [Electronic resource] / Institute of Mass Information, 2014. – Access: http: //imi.org.ua/barametr/45643-barometr-svobodi-slova-za-serpen-2014-roku.html

2. Buryachok V.L Principles of formation of cyber security state system: [Monography] / V.L. Buryachok. – K: NAU, 2013. – 432 p.

3. Cybersecurity: global trends and challenges for Ukraine. Analytical report: [Electronic resource]. – Access: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf

4. Conflicts between states and organizations in 2013 move into cyberspace: [Electronic resource]. – Access: http://dt.ua/TECHNOLOGIES/konflikti_mizh_derzhavami_ta_organizatsiyami_u_2013_rotsi_pereydut_u_kiberprostir.html

5. The Constitution of Ukraine, Law of Ukraine of 28.06.1996 № 254k/96-BP [Electronic resource]. – Access: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=254%EA%2F96-%E2%F0

6. Doctrine of information security of Ukraine, President of Ukraine Decree of July 8, 2009 № 514 / 2009 [Electronic resource]. – Access: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009

7. Starostina A. Terrorism and cyberterrorism – a new threats for international security: [Electronic resource]. – Access: http://www.crime-research.ru/articles/A.Starostina

8. Schetylov A. Some problems of struggle with cybercrime and cyberterrorism: [Electronic resource]. – Access: http://www.crime-research.ru/library/chetilov.htm

9. Anderson N. Massive DDoS attacks target Estonia; Russia accused : [Electronic resource] / Nate Anderson // Ars Technica. Retrieved, 2007. – Access: http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/

10. Kozlowski A. Cybersoldiers of Kreml: [Electronic resource] / Andrzej Kozlowski // Association of the European Centre for Analysis, 2014. – Access: http://geopolityka.org/analizy/2836-andrzej-kozlowski-cyberwojownicy-kremla

***Якубивская Ю.Е.**, кандидат экономических наук, доцент кафедры финансово-экономической безопасности и интеллектуальной собственности Тернопольского национального экономического университета*

МИРОВЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ

***Аннотация.** На современном этапе развития Украины особого внимания требует система кибернетической безопасности как ключевой элемент информационной, в том числе и национальной безопасности. Учитывая растущее число кибератак, необходимо не только провести исследование мировых тенденций развития киберпреступности, создать эффективное нормативно-правовое обеспечение, но также и систему мер по предупреждению и защите от киберпреступности.*

Статья посвящена исследованию тенденций киберпреступности, что является угрозой информационной безопасности страны. Определено место и роль кибербезопасности в системе национальной безопасности. Основное внимание сосредоточено на исследовании проявлений киберпреступности и активности кибератак на мировом уровне, а также тех, которые коснулись украинского информационного пространства. Даны рекомендации по улучшению системы защиты и борьбы с киберпреступностью.

***Ключевые слова:** национальная безопасность, информационная безопасность, кибернетическая безопасность, киберпространство, киберпреступность, кибератака.*