Віра П. Братюк

СУТНІСТЬ КІБЕР-ЗЛОЧИНІВ ТА СТРАХОВИЙ ЗАХИСТ ВІД КІБЕР-РИЗИКІВ В УКРАЇНІ

У статті надано аналіз сутності, ризиків та загроз кібер-злочинності. Виявлено динаміку росту кібер-злочинів і фінансових збитків від них. Доведено доцільність страхування кібер-ризиків та досліджено напрями розвитку кібер-страхування в Україні.
Ключові слова: *кібер-злочин; кібер-ризик; фінансові збитки; кібер-страхування.*
Табл. 1. Літ. 26.

Вера П. Братюк

СУЩНОСТЬ КИБЕР-ПРЕСТУПЛЕНИЙ И СТРАХОВАЯ ЗАЩИТА ОТ КИБЕР-РИСКОВ В УКРАИНЕ

В статье представлен анализ сущности, рисков и угроз кибер-преступности. Выявлена динамика роста кибер-преступлений и финансовых убытков от них. Доказана целесообразность страхования кибер-рисков, а также исследованы направления развития кибер-страхования в Украине.
Ключевые слова: *кибер-преступление; кибер-риск; финансовые убытки; кибер-страхование.*

Vira P. Bratiuk[1]

ESSENCE OF CYBER CRIMES AND INSURANCE PROTECTION FROM CYBER RISKS IN UKRAINE

The article presents the essence of cyber crimes and the related risks and threats. The dynamics of cyber crimes rates growth is demonstrated along with the dynamics of the related financial losses. The expediency of cyber risks insurance is grounded; the directions for cyber insurance development in Ukraine are outlined.
Keywords: *cyber crime; cyber risk; financial losses; cyber insurance.*

Постановка проблеми. В останні роки в Україні у сфері економіки та суспільної практики спостерігається зростання загроз, які пов'язані з кібер-злочинністю. Схожі проблеми виявлені в зарубіжних країнах. Як реакція на зростання збитків від кібер-злочинів на ринку страхування зростають потреби на нові продукти у сфері кібер-страхування.

Аналіз останніх досліджень і публікацій. Аналіз загроз і можливості страхового захисту від кібер-злочинів проводиться в зарубіжних країнах протягом останніх 10–15 років. Питання аналізу кібер-ризиків та доцільності страхового захисту від кібер-загроз нині розглядають керівники підприємств зарубіжних країн, незалежно від галузі та сегменту ринку, в якому проводиться господарська діяльність. Аналіз останніх публікацій свідчить, що під кібер-злочинами прийнято розуміти будь-який витік даних (інформації), атаки хакерів, поширення вірусів тощо, які призводять до втручання в дію та порушення функціонування інформаційних систем та засобів комунікації. Одним з інструментів протидії кібер-ризикам є кібер-страхування. Публікації зарубіжних авторів Ю.В. Бородакія [9], С.В. Бремена [25], И.В. Бутусова [9], М.Д. Гудмана [25], А. Старовойтова [21] націлені на аналіз ризиків і страхового захисту від кібер-загроз. Публікації вітчизняних авторів В. Прохоренка [19], О.В. Сер-

[1] Mukachevo State University, Ukraine.

гієнкова [20], А. Устенка [22] розглядають переважно питання кібер-злочинності, правового та технічного захисту від кібер-загроз.

Невирішені частини проблеми. В Україні потреби страхування від кібер-злочинів сьогодні незначні. Однак страховий захист від кібер-ризиків персональних даних, інформації з грифами обмеженого доступу, порушення функціонування інформаційних систем від кібер-атак, фінансових втрат при викраденні паролів для доступу до фінансової інформації підвищує надійність роботи інформаційних та комунікативних систем вітчизняних підприємств та організацій, захищає їх від загроз фінансових збитків та втрати репутації.

Метою дослідження є аналіз сутності кібер-злочинів, систематизація кібер-ризиків та обґрунтування доцільності розвитку кібер-страхування в Україні як інструменту протидії кібер-загрозам.

Основні результати дослідження. Сучасний світ неможливо уявити без інформаційних технологій, основою яких є використання комп'ютерної техніки та засобів комунікацій. Нині комп'ютерні системи впроваджуються в найрізноманітніших галузях людської діяльності. Найважливіші функції сучасного суспільства пов'язані з роботою обчислювальних машин, інформаційними технологіями, мережами й засобами комунікації. Злочинність у кібер-просторі стала однією з головних проблем сучасного світу інформаційних технологій. Схожу думку висловили учасники Всесвітнього економічного форуму в Давосі в січні 2012 року [16].

За [9; 26], протизаконна діяльність у глобальному кібер-просторі сьогодні займає друге місце в рейтингу економічних злочинів, поступаючись лише незаконному привласненню активів. На кібер-злочини доводиться 38% економічних злочинів у сфері фінансових послуг. За оцінками експертів [8; 9] від кібер-злочинів світова економіка щорічно втрачає 114 млрд дол. США за роки існування глобальної мережі Інтернет збитки від таких злочинів сягнули 400 млрд дол. США. При цьому кібер-злочинність удосконалюється та поширюється, ігноруючи географічні та державні межі.

За даними Європейської Комісії [8; 26], сьогодні на планеті понад 9 млрд електронних пристроїв, які підключені до глобальної мережі, а до 2020 р. експерти прогнозують зростання їх кількості до 24 млрд одиниць. Напади кібер-злочинців щодня зазнають більше 1 млн. осіб в усьому світі.

Доцільно зауважити, що світова спільнота щорічно посилює боротьбу з кібер-злочинністю, зокрема, країни ЄС та США визначають цю проблему як одну з найбільш небезпечних для подальшого розвитку інформаційних технологій. Останнім часом, за даними [25], уряди країн ЄС та США ухвалили низку нормативних актів щодо захисту інформації від кібер-злочинності. Натомість, на нашу думку, українське законодавство у сфері захисту інформації та протидії кібер-злочинності вимагає значного доопрацювання.

Необхідно зазначити, що розповсюдження комп'ютерних вірусів, шахрайство з платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення роботи автоматизованих систем є не повним переліком кібер-злочинів, що мають місце в інформаційному просторі України. За даними Лабораторії Касперського [10; 15], в 2014 р. 12% усіх DDoS-атак припало на Україну, а країна увійшла до трійки лідерів щодо втру-

чання в діяльність комп'ютерних систем. Крім того, зростання обсягів безготівкових розрахунків призвело до зростання кількості потерпілих від кібершахрайства. За даними НБУ [14; 19], у 2012 р. кількість протиправних операцій за платіжними картами українських банків зросла до 12,7 тис., порівняно з 7,6 тис. у 2011 р. та 2,9 тис. у 2010 р. Обсяг неправомірно списаних коштів за цей період зріс з 6,3 млн до 23,4 млн грн. У той же час, поза межами офіційної статистики, але за оцінками експертів [13; 19], на початок 2013 р. щоденно в управлінні з боротьби з кібер-злочинністю в Києві реєстрували до 20 випадків крадіжки коштів через систему клієнт-банк. Суми крадіжок становили від 20 тис. до 4,0 млн грн. Однак про подібні факти повідомлень у ЗМІ немає [19].

Згідно з [11; 22], загрози, пов'язані з інформаційними ризиками, можуть бути більш небезпечні, ніж загрози з фізичними активами підприємств. Проблеми, пов'язані з витоком інформації та персональних даних внаслідок кібер-злочинів, як правило, викликають ланцюгову реакцію та завдають значних фінансових збитків та втрати репутації. Розвиток систем електронної комерції та нових інформаційних технологій в Україні протягом останніх 10–15 років також супроводжується зростанням кібер-злочинів, ускладненням методів, які використовують хакери.

Керівники підприємств України усвідомлюють ризик, пов'язаний з незаконним доступом до персональних даних, електронних бібліотек і джерел інформації, але не мають достатніх ресурсів для ефективного реагування на дії кібер-злочинців. При цьому експерти у сфері страхування стверджують, що ситуація в середньостроковому періоді не зміниться, а економічні збитки від діяльності хакерів зростатимуть.

В Україні діє низка Законів України та нормативних документів різних рівнів, які охоплюють проблеми правового забезпечення кібер-безпеки. Це, зокрема, Закон України «Про інформацію» [3], Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2], Закон України «Про основи національної безпеки України» [4]. Крім того, діють стратегічні та міжнародні документи, такі як: Стратегія національної безпеки України [6], Доктрина інформаційної безпеки України [5] та «Конвенція про кіберзлочинність» [1]. У той же час у вітчизняному нормативно-правовому полі сфери інформаційної безпеки спостерігається використання термінів, які не узгоджені між собою та не мають визначень.

Таким чином, на нашу думку, доцільно виділити три основні проблеми, які ускладнюють боротьбу з кібер-злочинами в Україні:

- по-перше, відсутність визначень ключових термінів та категорій у науковій та фаховій літературі;
- по-друге, неузгодженість чинних нормативно-правових документів у сфері протидії кібер-злочинності;
- по-третє, відсутність державної системи протидії кібер-злочинам, у т.ч. шляхом страхування кібер-ризиків.

Зауважимо, що однією з основних причин розвитку кібер-злочинності як виду кримінального бізнесу, на нашу думку, є значна прибутковість при незначних вкладеннях та виробничих затратах. Іншою причиною росту кіберзлочинності можна вважати незначні ризики при складності оперативно-

пошукових та слідчих заходів у разі скоєння кібер-злочину. Крім того, на думку [25], існує психологічний аспект кібер-злочинності: злочинці не знають об'єкти злочину (жертви) особисто, що припускає відсутність у них прояву почуття провини та стримування. У той же час, як свідчить досвід зарубіжних країн [21; 23], істотно знизити можливі збитки від дії кібер-злочинців може страхування кібер-ризиків. Таким чином, формування системи страхового захисту електронної (віртуальної) інформації як ресурсу будь-якої сучасної діяльності від інформаційних ризиків є пріоритетним завданням в Україні. У першу чергу, це необхідно для підприємств, установ та організацій, які в господарській діяльності використовують комп'ютерні, мобільні, мережеві, інформаційно-комунікаційні технології, зважаючи на тенденцію розвитку нормативно-правової бази України в напрямку посилення відповідальності за збереження конфіденційності та захист персональних даних.

Кібер-страхування в Україні сьогодні, на нашу думку, повинно стати новим видом страхування від кримінальних кібер-ризиків та загроз втручання в діяльність автоматизованих систем, оскільки країна знаходиться в процесі інформатизації, інтенсивно впроваджує нові інформаційні технології в усіх сферах суспільної практики. Адже збитки від пожежі або стихійного лиха нині можуть мати менші наслідки в порівнянні з втратами внаслідок знищення комп'ютерної мережі або бази даних, яка наповнювалася роками та є основним інформаційним ресурсом виробництва.

Аналіз досліджень у сфері кібер-злочинності [14; 24] приводить нас до висновку, що кількість протиправних посягань на інформаційні ресурси та програмно-машинні засоби їх обробки в Україні зростає, а збитки від кібер-злочиннів перевищують розмір збитків від традиційних видів злочинів. За даними огляду "Price Waterhouse Coopers" [24], кібер-злочинність стала одним із п'яти найбільш поширених економічних видів злочинів в Україні, а збитки від онлайн-злочинів і шахрайства сьогодні вже перевищили збитки від інших форм злочинності. Зауважимо, що Україні близько 18 млн громадян та юридичних осіб є постійними користувачами мережі Інтернет. З кожним роком кількість злочинів у мережі Інтернет зростає на 25–30%.

Доцільно зауважити, що за [12; 17] кібер-страхування розглядає різноманітні ризики, серед яких порушення роботи інформаційної системи в наслідок кібер-атаки, викрадення та розголошення конфіденційних або персональних даних шляхом використання незаконного доступу до комп'ютерних систем, комп'ютерного шахрайства шляхом перехвату інформації в процесі обміну тощо. На нашу думку, за аналізом [8; 9; 18] доцільно виділити характерні види кібер-ризиків і напрями кібер-страхування від кібер-злочинів (табл. 1).

Таким чином, страховик може відшкодувати витрати за діяльністю підприємства, яка спрямована на подолання наслідків втручання кібер-злочинців (відновлення функцій, інформації, комунікацій) та пов'язана з усуненням збитків, а також відшкодувати збитки, які є наслідком простою комп'ютерних систем та інформаційної технології.

Як свідчить практика електронної комерції [20; 23], вирішальні є 24 години після нападу кібер-злочинців. Тому страхові компанії за страховою подією одразу виплачують кошти на подолання наслідків.

Таблиця 1. **Характерні види кібер-ризиків і напрями кібер-страхування***

Види кібер-ризиків	Напрями кібер-страхування ризиків
Ризик втрати інформації та порушення роботи систем при зламі пароля доступу або внаслідок DDoS-атаки	За сутністю відноситься до кібер-ризику втрати інформації та порушення роботи комп'ютерних систем. Кібер-страхування відшкодує витрати на поновлення діяльності інформаційної технології, наприклад, web-сайту.
Ризик фінансових втрат через порушення роботи комп'ютерних систем	За сутністю відповідає ризику втрати впущеної вигоди в offline-страхуванні. Напрям страхування захищає IT-підприємства від втрат з вини кібер-злочинців у разі порушення роботи комп'ютерних систем. Напрям страхування є доцільним для захисту online-магазинів, медіа-кінотеатрів, систем трекер-торентів.
Ризик фінансових втрат за регрес-позовами при викраденні, розголошенні або використанні персональної інформації	Сутність полягає в ризику втрат від регрес-позовів власників даних при викраденні, розголошенні та використанні кібер-злочинцями їх персональної інформації. Цей напрям страхування відшкодовує збитки підприємств за регрес-позовами власників персональної інформації.
Ризик фінансових втрат за здирництвом при вірусному блокуванні комп'ютерних систем	Сутність полягає в кібер-вимаганні (здирництві) через примушення до сплати (наприклад, шляхом SMS) за розблокування інформаційних систем або інформації при попередньому блокуванні вірусом програм комп'ютерів або баз даних. Кібер-страхування покриває витрати на розблокування інформаційних систем при доведенні витрат та фіксації кібер-злочину для страхувальника.
Ризик фінансових втрат на відновлення програмного забезпечення та (або) інформації вгаслідок дії кібер-злочинців	За сутністю є аналогом майнового страхування та відноситься до кібер-ризику фінансових втрат при пошкодженні програмного забезпечення та (або) інформації внаслідок дії кібер-злочинців. Кібер-страхування відшкодовує витрати на відновлення програмного забезпечення та (або) інформації.

* опрацьовано та узагальнено за [8; 9; 18].

Доцільно зауважити, що впровадження кібер-страхування в Україні, перш за все, вимагає банківська діяльність. Аналіз [7; 14] свідчить, що стрімкий постійний розвиток нових інформаційних технологій унеможливлює повний захист банківських інформаційних систем шляхом застосування технічних засобів на програмно-машинній основі. Зокрема, на думку [25], практика світових фінансових установ доводить, що забезпечення стабільності та стійкого розвитку сьогодні неможливо досягти в межах традиційних методів захисту шляхом уникнення відомих банківських ризиків та загроз від кібер-шахрайства. Утім, на нашу думку, в цьому випадку доцільним є використання спеціальних фінансових інструментів, зокрема, кібер-страхування, що дозволяє зменшити банківські ризики від кібер-шахрайства, крадіжок з банківських рахунків, викрадення паролів та персональних даних клієнтів банку тощо. При цьому значні витрати на покриття можливих фінансових збитків кібер-злочинців будуть замінені на планові доступні страхові платежі банку. Таким чином, залучення страхових інструментів захисту майнових інтересів банку та вкладників від ризиків кібер-злочинів сьогодні є об'єктивною необхідністю.

За [7; 20], з метою зменшення банківських ризиків провідні страхові компанії зарубіжних країн створили та впроваджують комплексні програми страхування банківських ризиків, що в сукупності застрахованих ризиків банківської діяльності передбачають страхування від комп'ютерних злочинів. Необхідно зауважити, що поліс страхування від кібер-злочинів створено для забезпечення захисту банку від зростаючого ризику несанкціонованого доступу до інформації автоматизованих систем, які використовуються для обслуговування клієнтів. При цьому, поліс кібер-страхування в комплексних страхових продуктах для банків та інших фінансових установ за формою є доповненням до полісу комплексного страхування від загроз кримінальних ризиків банку.

За [11; 20; 22], з метою уникнення або скорочення втрат банківських установ від дії кібер-злочинців страхові організації зарубіжних країн створили комплексні страхові продукти, наприклад, страхування від комп'ютерних злочинів – CCI (computer crime insurance) та страхування від атак хакерів – HI (hacker insurance). Сутність цих страхових продуктів полягає в покритті збитків банку в результаті несанкціонованого доступу до комп'ютерних і комунікаційних систем фінансової організації, введення неправомірних даних або команд, знищення інформації та програм вірусами. За даними [10; 20; 25], у світовій практиці ризики комп'ютерних злочинів та атак хакерів, як правило, приймаються на страхування як додаток до основного полісу комплексного банківського страхування – BBB (banker's blanket bond).

Особливістю страхових полісів "Computer Crime Insurance" та "Hacker Insurance" є те, що при настанні страхового випадку страхова компанія відшкодовує як збитки, заподіяні банку, так і шкоду, заподіяну третім особам (клієнтам банку).

Висновки. Нині злочинність у світовому кібер-просторі стала однією з головних проблем сучасного світу інформаційних технологій. В 2014 р. 12% усіх DDoS-атак припало на Україну, внаслідок чого країна увійшла до трійки лідерів з втручання злочинців у діяльність комп'ютерних систем. В Україні діє низка законів та нормативних актів щодо правового забезпечення кібер-безпеки, в яких використані терміни, які не узгоджені між собою та не мають визначень. Кібер-злочинність стала одним із п'яти найпоширеніших економічних видів злочинів в Україні, а збитки від онлайн-злочинів та шахрайства нині перевищили збитки від інших форм злочинності. При кібер-страхуванні страховик відшкодовує витрати за діяльністю, яка спрямована на подолання наслідків утручання кібер-злочинців (відновлення функцій, інформації, комунікацій) та пов'язана з усуненням збитків, а також відшкодовує збитки, які є наслідком простою комп'ютерних систем та інформаційної технології. У світовій практиці ризики комп'ютерних злочинів та атак хакерів за страховими полісами "Computer Crime Insurance" та "Hacker Insurance" є додаток основного полісу комплексного банківського страхування BBB (banker's blanket bond). Особливість страхових полісів "Computer Crime Insurance" та "Hacker Insurance" полягає в тому, що при настанні страхового випадку страхова компанія відшкодовує як збитки, заподіяні банку, так і шкоду, заподіяну його клієнтам.

1. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001. Конвенцію ратифіковано із застереженнями Законом України від 07.09.2005 №2824-IV // zakon.rada.gov.ua.

2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 №80/94-ВР зі змін. та допов. від 27.03.2014 №1170-VII // zakon.rada.gov.ua.

3. Про інформацію: Закон України від 2.10.1992 №2657-XII зі змін. та допов. від 2.12.2010 №2756-VI // zakon.rada.gov.ua.

4. Про основи національної безпеки України: Закон України від 19.06.2003 №964-IV зі змін. та допов. від 12.02.2015 №186-VIII // zakon.rada.gov.ua.

5. Про введення в дію Доктрини інформаційної безпеки України: Указ Президента України від 23.04.2008 №377 (втратила чинність згідно з Указом Президента України від 6.06.2014 №504/2014) // zakon.rada.gov.ua.

6. Стратегія національної безпеки України: Указ Президента України від 12.02.2007 №105 зі змін. та допов. від 8.06.2012 №389/2012) // zakon.rada.gov.ua.

7. Банківська діяльність: Навч. посібник / З.Б. Живко, О.П. Просович, М.І. Копитко та ін.; За ред. З.Б. Живко. – К.: Алерта, 2012. – 248 с.

8. *Бозен Р., Позднякова Н.* Европа объявила войну киберпреступности // Deutsche Welle, 1.06.2012 // www.dw.com.

9. *Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В.* Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности.– 2013.– №1. – С. 2–9.

10. *Гарнаева М.А., Функ К.* Kaspersky security bulletin 2013 // Вопросы кибербезопасности.– 2014.– №3. – С. 65–68.

11. *Жукова Д.* Чего стоит ожидать от киберпреступников // Internetua, 2015 // internetua.com.

12. Киберпреступность в Украине набирает обороты // Медиа-группа Golos.Ua // ru.golos.ua.

13. Кіберзлочинність можна зупинити тільки разом // Україна: бізнес-ревю.– 11.02.2013.– №5–6.

14. Кіберзлочинність: проблеми боротьби і прогнози / НАБУ // anticyber.com.ua.

15. Лаборатория Касперского. Блокеры всех времен и народов // www.kaspersky.ru.

16. Підсумки Всесвітнього економічного форуму в Давосі в контексті удосконалення процесів глобального управління: висновки для України: Аналітична записка / Національний інститут стратегічних досліджень // www.niss.gov.ua.

17. Правове регулювання кіберзлочинності // Правосуддя України: Всеукраїнська правова газета // ukrjustice.com.ua.

18. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування: Аналітична записка / Національний інститут стратегічних досліджень // www.niss.gov.ua.

19. *Прохоренко В.* Кіберзлочинність для України стає актуальним поняттям – НБУ // Економічна правда.– 26.02.2013.

20. *Сергієнкова О.В., Мелентьєва О.В.* Проблеми та перспективи розвитку страхування банківських ризиків в Україні // конференция.com.ua.

21. *Старовойтов А.* Кибербезопасность как актуальная проблема современности // Информатизация и связь.– 2011.– №6. – С. 4–7.

22. *Устенко А.* Страна становится эпицентром киберпреступности // focus.ua.

23. *Clapper, J.R.* (2013). Worldwide Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence, March 12, 2013, p. 1–7.

24. Computer Emergency Response Team of Ukraine // cert.gov.ua.

25. *Goodman, M.D., Brenner, S.W.* (2012). The Emerging Consensus on Criminal Conduct in Cyberspace. UCLA J.L. & Tech., No 3 // www.lawtechjournal.com.

26. Usage and Population Statistics // Internet World Stats // www.internetworldstats.com.

Стаття надійшла до редакції 12.05.2015.