

від 17 вересня 2014 р. №847-п]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/847-2014-%D1%80>.

4. Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009: [Electronic Resource]. – Mode of access: URL://www.cobx.org/content/default.asp?PageID=58&DocID=27195.

УДК 368:330.131.7:004

Є.С. Сєдов,
студент IV курсу ФЕФ,
спеціальність «Фінанси і кредит»,
ДВНЗ «Київський національний економічний університет
імені Вадима Гетьмана»,
науковий керівник: А.Л. Баранов,
к.е.н., доцент, доцент кафедри страхування,
ДВНЗ «Київський національний економічний університет
імені Вадима Гетьмана»

ДЕЯКІ АСПЕКТИ СТРАХУВАННЯ КІБЕР-РИЗИКІВ

Останніми роками в Україні і світі спостерігається зростаючий інтерес до кібер-ризиків, адже їх реалізація може призвести до мільярдних збитків і втрати репутації.

Багато компаній починають розглядати кібер-безпеку як невід’ємний елемент їх роботи і, як наслідок, вони шукають методи, які забезпечать безперервність фінансових операцій у разі кібер-атак. Одним із таких методів є страхування [1].

Кібер-ризики дуже тісно пов’язані з поняттям «кібер-злочинність». Число підтверджених інцидентів в сфері інформаційної безпеки по всьому світу в 2015 р. за даними PricewaterhouseCoopers (США) зросло на 48 % і склало 42,8 млн., тобто кожен день в середньому повідомлялося про 117 339 спроб несанкціонованого доступу [2].

Компанія McAfee (США) повідомляє, що загальні збитки від кіберзлочинності для бізнес-структур в світовому масштабі за 2015 р. оцінюються на рівні \$ 400 млрд., а втрати від крадіжки персональних даних в \$ 160 млрд. [6]. У світовій статистиці злочинів кіберзлочинність по частоті виникнення поступається лише незаконному привласненню активів [3]. Перш за все, страждають банки, інвестиційні компанії, страхові компанії, учасники ринку цінних паперів, електронні платіжні системи [5].

Україна є однією з найбільш зручних країн для кібер-злочинців, що пояснюється відсутністю суворих покарань, непрофесійними розслідуваннями, простою і безпечною процедурою легалізації вкрадених грошей і інформації. За даними Управління боротьби з кіберзлочинністю, в 2014 р. сума заявленого матеріального збитку в Україні склала близько 19 млн. грн., а за I півріччя 2015 року – близько 10 млн. грн. При цьому, якщо в 2014 р. було виявлено 2 025 кримінальних правопорушень, то в I півріччі 2015 р. – вже 1 727 [4].

Страхування кібер-ризиків спрямоване на подолання наслідків втручання кібер-злочинців (відновлення функцій, інформації, комунікацій) та пов'язане з покриттям всіх необхідних для цього витрат, а також на відшкодування збитків, які є результатом простою комп'ютерних систем [1].

Для кібер-страхування характерні такі особливості:

Брак досвіду страховиків і відповідних стандартів. Кібер-страхування – це новий вид страхування, і страховики ще не мають чіткої стандартизованої процедури.

Еволюціонування інформаційних систем. Комп'ютерні системи швидко еволюціонують, з'являються нові технології, які можуть змінити природу кібер-ризиків.

Інформаційна асиметрія. Страховик не завжди має доступ до тієї ж самої інформації, що і страхувальник. Найчастіше ця інформація є засекреченою.

Еволюція кібер-атак. Техніки і прийоми, які використовують кібер-злочинці, постійно змінюються, і ці зміни є непередбачуваними.

Взаємозалежність безпеки. Рівень захисту однієї системи часто залежить від захисту інших: вірус може проникнути в систему через канал, створений з компанією-партнером.

Нестача статистичних даних. Відсутність статистичних даних про інциденти не дає змоги страховикам визначити надійність їхніх полісів, так як ця інформація часто є конфіденційною і не підлягає розголошенню.

Складність оцінити збитки. Це пов'язано з природою інформаційних активів (вартість ноу-хау чи вартість репутації).

Проблеми з визначенням покриття. Важко визначити, від чого саме страхувальник хоче застрахуватися, а страховик у свою чергу не може точно визначити, чи готовий він це покрити.

Винятки та обмеження. Поліси зі страхування кібер-ризиків містять безліч винятків та обмежень щодо покриття (наприклад, 200 млн. дол. для великих компаній, таких як Google)

Відповідальність. Коли була здійснена кібер-атака, необхідно встановити рівень відповідальності за збитки і визначити, хто несе відповідальність за шкоду. В кібер-світі все не так однозначно. У деяких випадках це можуть бути власники систем, в інших – розробники програмного забезпечення тощо.

Час для пред'явлення претензій. Багато атак відбуваються непоміченими. Порушення у роботі системи можуть бути виявлені вже після нападу. Крім того, деякі атаки є надзвичайно тривалими (наприклад, напади можуть зайняти кілька місяців). Питання про те, яким чином страховики повинні відшкодувати витрати, залишається відкритим [6].

На сучасному етапі у світовій практиці визначено кілька ризиків, які частково або повністю можуть покриватися страховим захистом:

- ризик присвоєння та використання конфіденційної інформації співробітниками компанії;
- ризик отримання хакером інформації про номери кредитних карток або рахунків клієнтів компанії;

- ризик розкрадання грошових коштів з рахунків у банку або цінних паперів з рахунку в депозитарії;
- ризик втрати або розголошення інформації через помилку співробітника;
- перерва в роботі підприємства, його комп'ютерної мережі, його сайту;
- збитки, пов'язані з розміщенням на сайті страхувальника неправдивих відомостей або інформації, що може зашкодити діловій репутації;
- ризик втрати матеріального носія, що містить конфіденційну інформацію [5].

Отже, нині злочинність у світовому кібер-просторі стала однією з головних проблем сучасного світу інформаційних технологій. Страхування може допомогти захиститися від ризиків такого роду. Але це новий напрямок, який тільки починає розвиватися і для якого характерні свої особливості і проблеми. В той же час його перспективність однозначна.

Список використаної літератури

1. Братюк В. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні / В. Братюк // Актуальні проблеми економіки. – 2015. – № 9. – С. 421-427.
2. Основные результаты Глобального исследования по вопросам обеспечения информационной безопасности. Перспективы на 2015 год [Електронний ресурс] // PwC. – Режим доступу: <http://www.pwc.ru/riskassurance/publications/assets/managing-cyber risks.pdf>.
3. Страхування від кібер-атак: тепер і на європейському ринку [Електронний ресурс] // Deutsche Welle, 15.07.2013. – Режим доступу: <http://www.dw.com/uk/страхування-від-кібер-атак-тепер-і-на-європейському-ринку/a-16950877>.
4. Украина и киберпреступность: кто кого? [Електронний ресурс] // Медіа-група From.Ua. – Режим доступу: <http://from-ua.com/articles/336424-ukraina-i-kiberprestupnost-ko-kogo.html>.
5. Цена информационной безопасности и страховая защита от кибер-рисков [Електронний ресурс]. – Режим доступу: <http://strahovkunado.ru/insur/strakhovanie-kiber-riskov.html>.
6. Marotta A. A Survey on Cyber-Insurance / Marotta A., Martinelli F., Nanni S., Yautsiukhin A. – Bologna, Italy: Unipol Gruppo Finanziario S.p.A., 2015. – 52 p.