УДК 338

Барташевська Ю.М.,
к.е.н., доцент,
доцент кафедри економіки та моделювання бізнес-процесів,
Університет імені Альфреда Нобеля

ОЦІНКА ЕФЕКТИВНОСТІ ВИТРАТ КОМПАНІЇ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

Анотація. У статті розглянуто проблему кіберзлочинності України та світу. Досліджено втрати, яких зазнає світова економіка внаслідок скоєння кіберзлочинів. Виявлено, що організаціями, найбільш привабливими для кіберлочинців, є банківсько-фінансові установи. Одним зі шляхів вирішення проблеми є впровадження системи інформаційної безпеки з оцінкою ефективності її роботи. Запропоновано метод оцінки ефективності впровадження системи інформаційної безпеки на основі чотирирівневої матриці «частота – втрати».

Ключові слова: кібербезпека, кіберзлочини, оцінка ефективності, методи оцінки, витрати.

Постановка проблеми. Сьогодні кіберзлочинність – загальносвітова проблема, яка не має кордонів. Жодна організація або галузь економіки не може відчувати себе повністю захищеною від небажаних наслідків кіберзлочинів. Це можуть бути фінансові збитки, вплив на імідж або репутацію організації з метою її погіршення, що в результаті може призвести навіть до втрати частки на ринку.

Оскільки багато людей та організацій використовують різні технології, включаючи Інтернет, то всі вони схильні до ризику потенційних атак шахраїв з будь-якого куточка світу, а отже, не захищені від фінансових втрат.

Згідно з оцінками експертів орієнтовні втрати світової економіки від діяльності кіберзлочинців у 2015 р. склали 445 млрд. дол. Приблизно половину цієї суми (більше 220 млрд. дол.) складають втрати США, Китаю, Японії та Німеччини [1, с. 4]. У 2016 р. за оптимістичними підрахунками цей показник перевищив 575 млрд. дол., а за песимістичними він наблизився до 650 млрд. дол. Це близько 1% світового ВВП. На 2017 р. прогнозовані втрати від кіберзлочинів можуть перевищити 1 трлн. дол., а до 2020 р. можуть зрости майже вдвічі [2]. Список країн-лідерів за втратами з 2016 р. не змінився: Німеччина, США, Китай та Японія. П'яте місце посіла Росія.

Найбільше серед підприємств та організацій постраждали від кібератак у 2015 р. фінансові організації (13,5 млн. дол.). Цей показник майже вдвічі перевищує показник в оборонній промисловості (6,61 млн. дол.), в три рази перевищує середні витрати ритейлерів (4,88 млн. дол.) та в сім разів перевищує витрати підприємств сільськогосподарської галузі (1,97 млн. дол.). Такі дані показало дослідження 100 тис. інцидентів, що сталися у 82 країнах у різних галузях. Також воно виявило, що 86% кібератак були здійснені заради грошей або шпигунства, результатами чого були фінансові втрати в чотирьох випадках з п'яти [3].

Згідно з результатами експертних досліджень [4] у 2016 р. найбільш ризиковими організаціями за кількістю кібератак також були фінансові (48% від загальної кількості досліджених організацій). Далі йдуть державний сектор (44%), втрати ритейлерів (43%) та організації сфери логістики та транспорту (42%).

У зв'язку цим питання захисту інформації, зокрема фінансових та банківських організацій, є актуальною проблемою. Одними зі шляхів такого захисту є впровадження системи інформаційної безпеки організації та оцінка ефективності її роботи.

Аналіз останніх досліджень і публікацій. Проблемами захисту інформації банківських установ, методами оцінки ефективності захисту займалась велика кількість українських та іноземних вчених, зокрема Н.О. Гребенюк [5], О.М. Степко [6], С.П. Євсєєв [7], міжнародні дослідницькі групи [1; 4]. В основі цих досліджень лежать визначення втрат банківського сектору від кібератак, методи та заходи запобігання втрат, методи оцінки безпеки банківської інформації.

Виділення невирішених раніше частин загальної проблеми. Однак, незважаючи на велику кількість публікацій з цієї тематики, проблема вибору методу оцінки ефективності провадження та роботи системи інформаційної безпеки не є вирішеною і потребує подальшого дослідження.

Мета статті полягає в дослідженні проблеми інформаційної безпеки банківських організацій та методів оцінки ефективності системи інформаційної безпеки банку.

Виклад основного матеріалу дослідження. З розвитком інформаційних технологій кількість способів атаки на банківські рахунки зростає в геометричній прогресії, як і кількість бажаючих ці способи випробувати. Так, керівник відділу фінансової стабільності Банку Англії Ендрю Хелдейн заявив, що найбільші п'ять банків Великобританії бояться кіберзлочинів навіть більше, ніж боргової кризи. За його словами, система захисту від хакерських атак у банківському секторі дотепер перебуває в зародковому стані: фінансисти більше опікувалися про ліквідність, ніж про безпеку. Однак останні кіберзлочини змусили керівництво установ замислитися про вкладення в захист від комп'ютерних атак [8].

В Україні рівень кіберзлочинності зростає в декілька разів щороку. Так, згідно з підрахунками управління по боротьбі з кіберзлочинністю МВС України, у 2014 р. зареєстровано 4 800 злочинів у сфері ІТ, а у 2015 р. – вже 6 025. За останні два роки кількість кіберзлочинів в Україні збільшилася більш ніж на тисячу випадків [9]. Причому за останні роки «профіль» кіберлочинів, пов'язаних із банківською інформацією, дещо змінився. Якщо до 2013–2014 рр. банківські кіберзлочини були пов'язані перш за все з різними видами махінацій з банківськими картами клієнтів-фізичних осіб, то останніми роками пройшла переорієнтація на клієнтів-юридичних осіб. Останнє передбачає втручання в системи дистанційного банківського обслуговування (наприклад, «клієнт – банк»). Також якщо в 2010–2011 рр. злочинці використовували українські банки переважно для зняття і переведення в готівку коштів, вкраде-

них з рахунків в іноземних банках, то вже з 2012 р. тенденція змінилася, отже, почалися атаки на клієнтські рахунки саме вітчизняних фінансових установ на території України [10].

В 2012 р. в Україні було зафіксовано 139 фактів несанкціонованого списання засобів з рахунків підприємств із порушенням роботи систем дистанційного банківського обслуговування. Загальна сума збитку склала більше 116 млн. грн., з яких 75% було повернуто. На початку 2013 р. було зафіксовано 14 таких фактів на загальну суму 9,4 млн. грн., з яких вдалося повернути потерпілим близько 8,3 млн. грн., або 88%. За вісім місяців 2016 р. втрати тільки від кардингу та інших видів шахрайства з платіжними картами, а також крадіжок коштів з використанням віддаленого доступу склали 7–8 млн. грн.

Банкіри та їх клієнти усе більше турбуються про інформаційно-технічну безпеку засобів на рахунках. Більше того, щоб попередити виникнення проблем, у яких клієнт зможе звинуватити фінансову установу, банки все частіше самостійно ініціюють розробку та впровадження правил IT-безпеки.

На думку авторів [5; 6; 7], щоб уникнути вторгнення зловмисників, необхідно дотримуватися таких базових правил: необхідно використовувати тільки ліцензійне програмне забезпечення; необхідно використовувати антивіруси та мережні екрани відомих виробників з регулярним автоматичним відновленням баз і перевіркою комп'ютера; не використовувати комп'ютер системи «клієнт – банк» для якихось інших цілей, окрім проведення операцій зі своїми рахунками; використовувати системи дистанційного керування комп'ютером.

Отже, розробка та впровадження системи інформаційної безпеки та оцінка її ефективності є актуальною проблемою. Сьогодні застосовуються різні методології оцінки ефективності системи інформаційної безпеки банку.

Для оцінки ефективності системи захисту інформації рекомендується використовувати такі показники ефективності, як, зокрема, показники сукупної вартості володіння (TCO), економічної ефективності бізнесу та безперервності бізнесу (BCP), коефіцієнти повернення інвестицій на ІБ (ROI).

Метод оцінки властивостей системи безпеки (Security Attribute Evaluation Method – SAEM) був розроблений в Carnegie Melon University і заснований на порівнянні різних архітектур систем ІБ для отримання вартісних результатів оцінки вигод від впровадження системи ІБ. Методологія SAEM полягає в тому, щоб, об'єднавши ймовірність події і ранжирувавши вплив навколишнього середовища, запропонувати різні проекти з ІБ з різноманітним впливом навколишнього середовища на відносні витрати [11].

Недоліком методу є те, що найчастіше безпека знаходиться поза межами розуміння менеджерів, які займаються оцінкою ефективності, а фахівці з інформаційної безпеки рідко мають точні дані щодо вигод, принесених технологією, тому доводиться покладатися на досвід та інтуїцію та на їх основі приймати рішення.

Метод очікуваних втрат базується на тому, що обчислюються втрати від порушень політики безпеки, з якими може зіткнутися компанія, а ці втрати порівнюються з інвестиціями у безпеці, спрямованими на запобігання порушень [11]. Метод очікуваних втрат заснований на емпіричному досвіді організацій та відомостей про вторгнення, про втрати від вірусів, про відображення сервісних нападів тощо.

Наприклад, порушення безпеки комерційних організацій призводять до таких фінансових втрат:

– під час ведення електронної комерції відбуваються втрати, пов'язані з простоєм і виходом з ладу мережевого обладнання;

– нанесення шкоди іміджу та репутації компанії;

– оплата понаднормової роботи IT-персоналу та/або оплата робіт підрядникам, які займалися відновленням корпоративної інформаційної системи;

– оплата консультацій зовнішніх фахівців, які здійснювали відновлення даних, виконували ремонт і надавали юридичну допомогу;

– оплата ремонту фізичних ушкоджень від віртуальних атак;

– судові витрати під час подачі позовної заяви про віртуальні злочини і порушення політики безпеки.

Щоб «пом'якшити» очікувані втрати, компанія повинна інвестувати кошти в безпеку, а саме мережеві екрани, системи виявлення вторгнень, щоб запобігти атаки, антивіруси для виявлення різних форм вірусів.

Якщо компанія вирішує встановити систему інформаційної безпеки, то її вартість узагальнено буде складатись з такого:

– одноразові витрати (це, як правило, вартість обладнання, а також впровадження систем захисту інформації);

– періодичні витрати (тут присутні такі параметри, як, зокрема, технічна підтримка та супровід, заробітна плата IT-персоналу, продовження ліцензій на антивіруси).

Аналіз дерева помилок (Fault Tree Analysis) – це не дуже відомий інструмент оцінки вигід [11].

Ціль застосування цього методу полягає в тому, щоб показати, у чому полягають причини порушень політики безпеки, а також які контрзаходи, що згладжують їх, можуть бути застосовані.

Дерево помилок – це графічний засіб, який дає змогу звести всю систему можливих порушень до логічних відносин і/або компонентів цієї системи. Якщо доступні дані по нормах відмови критичних компонентів системи, то дерево помилок дає змогу визначити очікувану ймовірність відмови всієї системи.

Нині цей метод ще недостатньо адаптований до галузі інформаційної безпеки і вимагає подальшого вивчення.

Для обчислення ефективності від впровадження системи інформаційної безпеки банку введемо такі критерії, як частота виникнення потенційної загрози на 1 000 банківських операцій та можливі втрати від загрози на 1 000 транзакцій.

За зведеними даними табл. 1 та табл. 2 визначено показник очікуваних втрат за чотирирівневою матрицею «частота – втрати» (рис. 1).

На перехресті рядків та стовпчиків матриці отримаємо показник ALE – показник очікуваних витрат (в гривнях), який обчислюється за такою формулою:

$$ALE = f * L,$$

де f – частота виникнення потенційної загрози (табл. 1);

L – величина можливих втрат в гривні, яка визначається на підставі ступеня тяжкості порушення (табл. 2).

Для визначення витрат на захист від потенційних загроз зіставимо значення ALE та витрат на захист, а результат занесемо до відповідної чотирирівневої матриці ефективності витрати коштів на захист інформації (рис. 2).

Градація ефективності відповідно до співвідношення очікуваних втрат та витрат на захист зведена до табл. 3.

Отже, за результатами рис. 2 можна сказати, що чим менше очікувані втрати і вищі витрати на їх попередження, тим нижче результативність вкладання коштів у інформаційну безпеку.

Таблиця 1

Частота виникнення потенційної загрози на 1 тис. транзакцій

Діапазон	Градація частоти	Опис
0–1	Низький	Загроза виникає не частіше разу на рік.
2–10	Середній	Загроза виникає не частіше/або раз на півроку.
11–100	Високий	Загроза виникає не частіше/або раз на місяць.
101–1 000	Критичний	Загроза виникає не частіше/або раз на день.

Таблиця 2

Можливі втрати від виникнення потенційної загрози на 1 млн. грн. обігу

Діапазон	Градація втрат	Опис
0–100	Низький	Загроза не веде до фінансових втрат.
101–1 000	Середній	Загроза принесе деякі матеріальні та моральні втрати.
1 001–100 000	Високий	Втрата репутації, конфіденційної інформації. Втрати на відновлення інформації.
10 001–1 млн.	Критичний	Втрата системи.

Таблиця 3

Ефективність захисту інформації

Діапазон	Градація ефективності	Опис
0–10	Низька	Очікувані втрати є низькими. Велике вкладання коштів неефективне.
11–100	Середня	Очікувані втрати майже дорівнюють витраченим коштам на захист.
101–1 000	Висока	Вкладання коштів в захист виправдане.
> 1 001	Максимальна	Вкладання коштів в захист виправдане. Ризик втрати інформації високий.

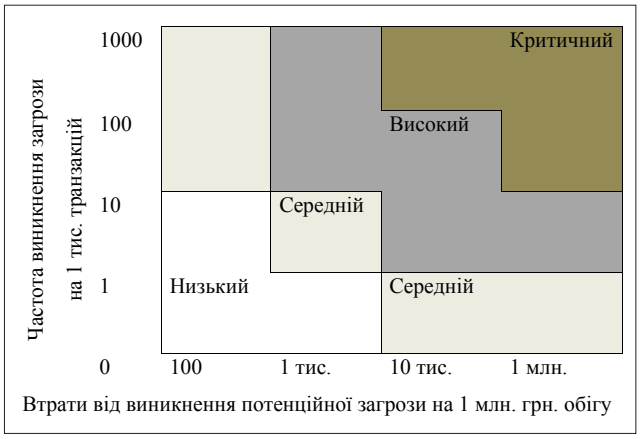

Рис. 1. Матриця «частота – втрати»

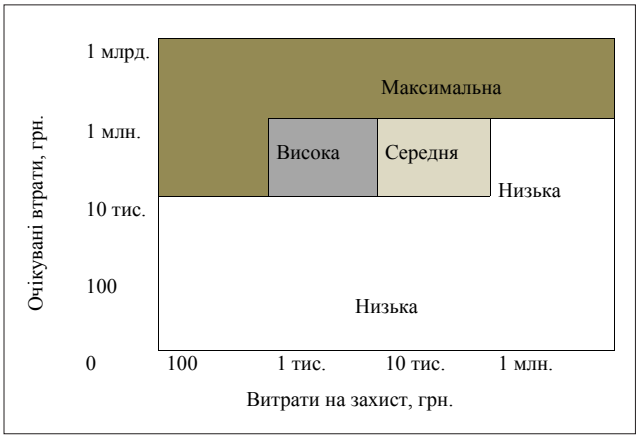

Рис. 2. Матриця «фінансові витрати – витрати на захист»

Пріоритетом для вкладання коштів є варіанти, котрі попереджають витрати, а саме області від 10 тис. до 1 млн. очікуваних втрат. В області максимальної ефективності виправданими будуть будь-які витрати, адже ризик втратити інформацію є дуже високим. І навпаки, зона високих втрат і низьких очікуваних втрат говорить про неефективність системи захисту та заходів з інформаційної безпеки.

Висновки. Таким чином, запропонований метод оцінки ефективності витрат на інформаційну безпеку на основі чотирирівневої матриці «частота – витрати» дає змогу визначити ефективність системи та заходів захисту інформації залежно від частоти настання ризикових випадків та витрат на цей захист.

Література:

1. A Guide to Cyber Risk / [L. Sethoga, F. Claret, J. Tilburn, J. Dias, H. Polke-Markmann etc.]. – Munich : Allianz Global Corporate & Specialty SE, 2015. – 32 p.
2. Грамматчиков А. Идет кибервойна народная / А. Грамматчиков, О. Вандышева [Електронний ресурс]. – Режим доступу : http://expert.ru/expert/2017/05/idet-kibervojna-narodnaya.
3. Киберпреступность переживает период роста // Депозитарум. – 2016. – № 4 (144). – С. 41–43.
4. Global Economic Crime Survey 2016 [Електронний ресурс]. – Режим доступу : https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf.
5. Гребенюк Н.О. Фінансова безпека банків: система розпізнання загроз та усунення ризиків / Н.О. Гребенюк // Вісник Харківського національного університету імені В.Н. Каразіна. – 2016. – № 91. – С. 53–64.
6. Степко О.М. Аналіз головних складових інформаційної безпеки держави / О.М. Степко // Науковий вісник Інституту міжнародних відносин НАУ. – 2011. – № 3. – Т. 1. – С. 90–100.
7. Евсеев С.П. Синергетический подход к оценке безопасности банковских систем / С.П. Евсеев // Системи обробки інформації. – 2016. – № 4 (141). – С. 90–103.
8. Британские банки боятся кибератак больше, чем кризиса [Електронний ресурс]. – Режим доступу : http://englant.ru/bez-rubriki/britanskie-banki-boyatsya-kiber-atak-bolshe-chem-krizisa#more-1119.

9. В Україні зростає кількість кіберзлочинів [Електронний ресурс]. – Режим доступу : https://www.epravda.com.ua/news/2016/03/28/587044.
10. Киберпреступность: скрытая и явная угроза [Електронний ресурс]. – Режим доступу : http://gazeta.zn.ua/macrolevel/kiberprestupnost-skrytaya-i-yavnaya-ugroza-_.html.
11. Синяк А.А. Анализ методов оценки эффективности вложений в информационную безопасность / А.А. Синяк, Н.Е. Губенко // Автоматизація технологічних об'єктів та процесів. Пошук молодих : зб. наукових праць. – Донецьк : ДонНТУ, 2012. – С. 85–88.

Барташевская Ю.Н. Оценка эффективности затрат компании на информационную безопасность

Аннотация. В статье рассмотрена проблема киберпреступности Украины и мира. Исследованы расходы мировой экономики в результате совершения киберпреступлений. Выявлено, что организациями, наиболее привлекательными для киберпреступников, являются банковско-финансовые учреждения. Одним из путей решения проблемы является внедрение системы информационной безопасности и оценки эффективности ее работы. Предложен метод оценки эффективности внедрения системы информационной безопасности на основе четырехуровневой матрицы «частота – потери».

Ключевые слова: кибербезопасность, киберпреступления, оценка эффективности, методы оценки, затраты.

Bartashevska Yu.M. Assessment of the company cost effectiveness for information security

Summary. The article deals with the problem of cybercrime of Ukraine and the world. The losses of the world economy as a result of the commission of cybercrimes were investigated. It was revealed that the organizations most attractive for cybercriminals are banking and financial institutions. One way to solve the problem is to implement an information security system and evaluate its effectiveness. A method for evaluating the effectiveness of implementing an information security system based on a four-level matrix "frequency – loss" is proposed.

Keywords: cybersecurity, cybercrime, performance evaluation, assessment methods, costs.