УДК 339.137.2

Іваницька О.В.
канд. економ. наук, доцент
Рощина Н.В.
канд. економ. наук, доцент
Южаков М. А.
Національний технічний університет України «КПІ»

ІДЕНТИФІКАЦІЯ ЗБИТКІВ ПІДПРИЄМСТВА ВІД ВТРАТИ ІНФОРМАЦІЇ

ИДЕНТИФИКАЦИЯ УБЫТКОВ ПРЕДПРИЯТИЯОТ ПОТЕРИ ИНФОРМАЦИИ

IDENTIFICATION OF ENTERPRISE LOSSES BECAUSE OF LOSING THE INFORMATION

У статті наведені результати досліджень інцидентів в сфері інформаційної безпеки за останні роки у світі. Визначено наслідки та масштаби втрати інформації, що стосуються внутрішніх та зовнішніх загроз соціально-економічній безпеці підприємства. Авторами систематизовано склад ризиків втрати інформації для підприємств та визначено відповідні категорії – репутаційні, операційні, стратегічні та юридичні ризики. Розглянуто складові витоку інформації та можливі відповідні наслідки на прикладах комерційного банку та телекомунікаційної компанії. Визначено специфіку інформаційної безпеки цих форм підприємництва. Також у дослідженні розглянуто альтернативні підходи щодо оцінювання вартості інформації. Наведено перелік показників оцінювання ефективності інформаційних систем – інформаційної насиченості, інформаційного потенціалу кадрів, якості інформаційного забезпечення. На основі цього було здійснено моделювання збитків підприємства від втрати конфіденційної інформації. Побудована модель описує залежність збитків власника інформації від коефіцієнту корисної конфіденційної інформації, що була втрачена.

Ключові слова: інформаційна безпека, витік інформації, ризики втрати інформації, вартість інформації, коефіцієнт корисної інформації

В статье приведены результаты исследований инцидентов в сфере информационной безопасности за последние годы в мире. Определены последствия и масштабы потери информации, касающиеся внутренних и внешних угроз социально-экономической безопасности предприятия. Авторами систематизирован состав рисков потери информации для предприятий и определены соответствующие категории – репутационные, операционные, стратегические и юридические риски. Рассмотрены составляющие утечки информации и возможные соответствующие последствия на примерах коммерческого банка и телекоммуникационной компании. Определена специфика информационной безопасности этих форм предпринимательства. Также в исследовании рассмотрены альтернативные подходы к оценке стоимости информации. Приведен перечень показателей оценки эффективности информационных систем – информационной насыщенности,

информационного потенциала кадров, качества информационного обеспечения. На основе этого было осуществлено моделирование убытков предприятия от потери конфиденциальной информации. Построенная модель описывает зависимость убытков владельца информации от коэффициента полезной конфиденциальной информации, которая была потеряна.

Ключевые слова: информационная безопасность, утечка информации, риски потери информации, стоимость информации, коэффициент полезной информации.

The article presents the results of the research of world incidents in information security' area during recent years . Defined consequences and scales of losing the information that concerning internal and external threats to social and economic security of the enterprise. Authors structured risks warehouse of losing the information for enterprise and identified categories– reputational, operational, strategic and legal risks. On examples of commercial bank and telecommunication company , were considered the components of information leakage and possible consequences. It was defined the specificity of information security on these forms of enterprise. Also, the research considered alternative approaches about information value. It was given the list of indicators that evaluating an effectiveness of information systems- informational saturation, informational potential of personnel, quality of informational provision. Based on this data was made a model of the enterprise losses because of losing the confidential information. The model describes the dependence losses of the information's owner on the coefficient of useful information that has been lost.

Keywords: information security, information leakage, risk of losing the information, information value, coefficient of useful information.

Вступ. Процес побудови інформаційного суспільства України вимагає активізації зусиль щодо покращення ефективності використання інформації як на мікро, так і на макрорівнях. В сучасних умовах стрімкого розвитку наукомістких технологій, все більшого значення набувають інформаційні ресурси підприємств. Саме завдяки інформації підприємства мають змогу формувати, використовувати та контролювати усі інші ресурси, що є в його розпорядженні. Водночас, жорстка конкурентна боротьба через призму розвитку інформаційних технологій, є спонукальним чинником до економічного, промислового та комерційного шпигунства. У міру того як інцидентів інформаційної безпеки стає більше, ростуть і витрати, пов'язані з необхідністю управляти ризиками і мінімізувати наслідки інцидентів.

Питанням забезпечення, використання, оцінювання та захисту інформаційних ресурсів присвячені багато праць науковців: Н. Г. Городька [5], Є. В. Іванченка [6], С. В. Казмирчука [6], А. Г. Корченка [6], М. Г. Монастирецького [5], Є.О. Цибульської [5], Г. І. Шалаєва [5], Л. В. Ярового [4] та інших.

Однак поряд зі збільшенням складності і надійності методів захисту інформації, удосконалюються також методи несанкціонованого доступу до

конфіденційної інформації. У результаті наноситься певний економічний збиток підприємству, який у ряді випадків може привести до нездоланних наслідків. Тому визначення вартості можливого збитку є невід'ємною складовою дослідження стану ризиків інформаційної безпеки підприємства.

Постановка завдання. Основними цілями наукової статті є визначення збитків від втрати інформації при моніторингу стану ризиків інформаційної безпеки підприємства.

Методологія. Теоретико-методологічним базисом роботи є наукові праці вітчизняних та зарубіжних вчених щодо забезпечення інформаційної безпеки. Для досягнення поставленої мети використано загальнонаукові та спеціальні методи дослідження, такі як: системний підхід, методи аналізу та синтезу, методи моделювання та узагальнення.

Результати дослідження. У світовому масштабі середній розрахунковий показник щорічних підтверджених фінансових збитків, пов'язаних з інцидентами в сфері інформаційної безпеки у 2014 р. склав 2,7 млн. дол., що на 34% більше, ніж в 2013 р. У світлі минулорічних гучних випадків витоку конфіденційної інформації не дивує висновок про те, що великі збитки зустрічаються частіше: кількість організацій, які повідомили про фінансові втрати у розмірі не менше 20 млн. дол., за 2013-2014 рр. збільшилася на 92%. Зростання числа інцидентів інформаційної безпеки є однією з причин такого збільшення фінансових збитків. Як і у випадку із загальною кількістю інцидентів, остаточну суму збитків від витоку інформації у світовому масштабі дізнатися неможливо, оскільки про багатьох кібератаках просто не повідомляється, а цінність деяких видів інформації, зокрема інтелектуальної власності, визначити нелегко. У недавньому дослідженні Центру стратегічних і міжнародних досліджень зверталася увага на труднощі при оцінці фінансових наслідків кіберзлочинності. Проте автори дослідження прийшли до висновку про те, що розмір щорічних збитків від кіберзлочинності для світової економіки становить від 375 млрд. до 575 млрд. дол. [1]. Слід мати на увазі, що ці цифри абсолютно непорівнянні з розміром збитків, внаслідок втрати конфіденційної інформації, що становить комерційну таємницю, або розкрадання інтелектуальної власності.

Наслідки втрати інформації можуть бути оцінені за допомогою фінансових і нефінансових показників. Так фінансові наслідки можуть включати в себе зниження доходів, збої в роботі бізнес-систем, штрафні санкції з боку регулюючих органів і скорочення числа клієнтів. До нефінансових

наслідків можна віднести підрив репутації компанії, піратське копіювання продуктів, витік науково-технічної інформації, наслідки для інноваційної діяльності компанії, розкрадання продуктового дизайну або дослідних зразків, незаконне копіювання бізнес-процесів та виробничих процесів, а також втрату такої особливо важливої конфіденційної інформації, як плани по здійсненню угод злиття і поглинання та стратегія розвитку компанії.

Майже половина (48%) учасників опитування в рамках підготовленого PwC Всесвітнього огляду економічних злочинів за 2014 рік, відзначили, що за минулий рік рівень усвідомлення серйозності ризику кіберзлочинності для їх організації підвищився на 39% у порівнянні з 2011 роком. Іншими словами, світові керівники вищої ланки підтверджують, що кіберзагрози перетворилися на серйозну проблему в управлінні ризиками підприємства. За результатами спільного дослідження CREAT та PwC, фінансові наслідки розкрадання комерційних таємниць становлять від 1 до 3% ВВП країни [1].

Однак, крім кібератак, існує ще безліч джерел витоку інформації. Варто зазначити, що кількість загроз та потік інформації, що стосується внутрішніх та зовнішніх загроз соціально-економічній безпеці підприємства, постійно зростає й підвищує рівень невизначеності. Моніторинг змін та загроз зовнішнього середовища, а після й внутрішнього дасть можливість попередити настання негативних ситуацій. Тож постійні зміни в зовнішньому середовищі зумовлюють появу нових загроз соціально-економічній безпеці підприємства.

Для побудови систем менеджменту інформаційної безпеки, комплексних систем захисту інформації та інших систем безпеки необхідно проводити аналіз і оцінювання відповідних ризиків. На рис. 1 систематизовано склад ризиків втрати інформації для підприємств.

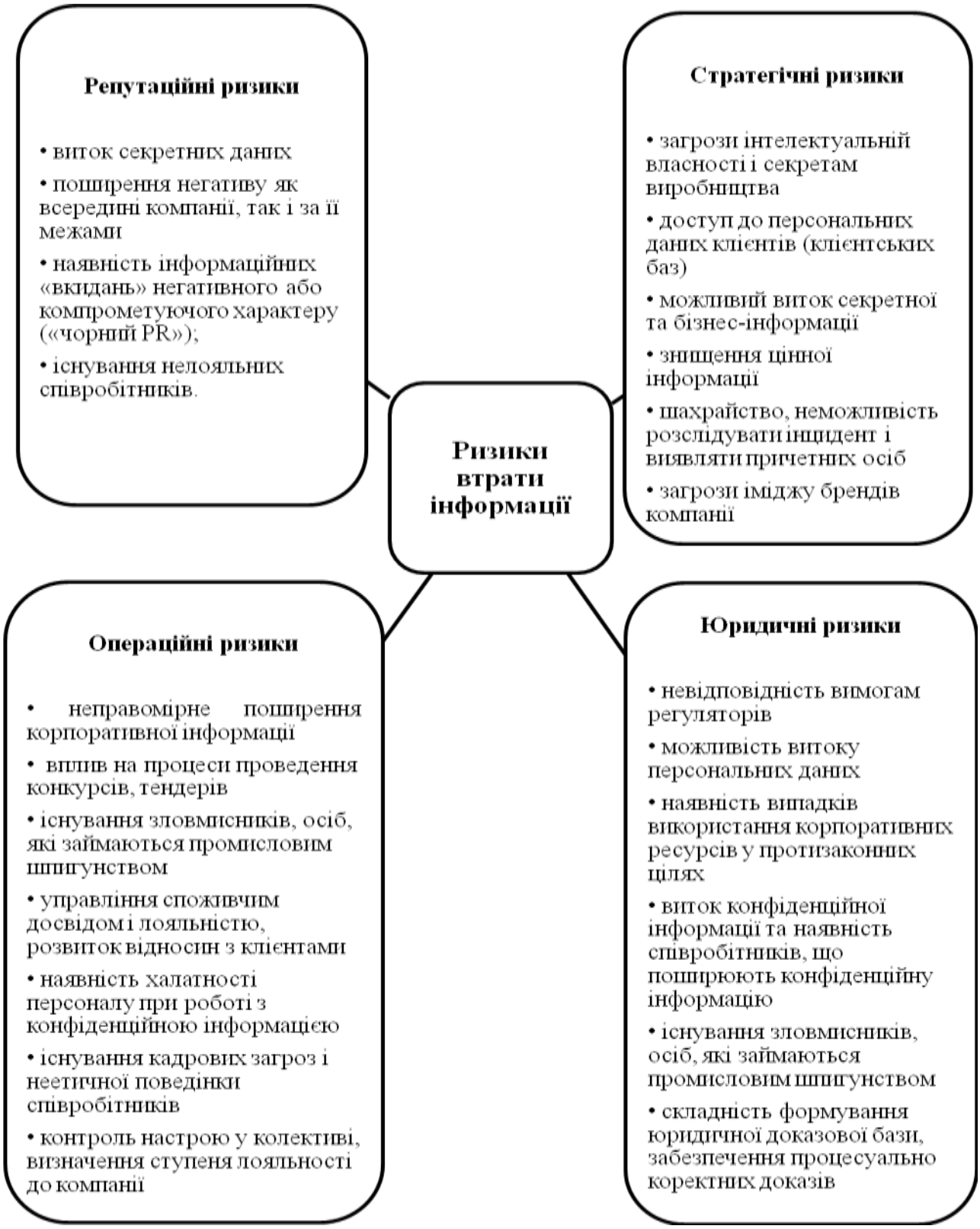

Рис. 1 Ризики втрати інформації для підприємств

Джерело: систематизовано авторами на основі [3]

Розглянемо складові витоку інформації та можливі відповідні наслідки для комерційного банку (табл. 1)

Таблиця 1

Виток та наслідки втрати інформації комерційного банку

Виток інформації	**Ризик**	**Збитки**
Внутрішні регламенти банку	− небезпека пограбування та шахрайства	− фінансові втрати
Персональні дані клієнтів	− втрата клієнтів з причини розголошення персональних даних − позови до суду з боку клієнтів за законом «Про захист персональних даних» − перевірки з боку регулюючих органів	− втрата клієнта − фінансові втрати
Інформація про обслуговування VIP-клієнтів	− втрата цільових клієнтів	− погіршення репутації − фінансові втрати
Плани виведення нового продукту на ринок	− конкурент випускає новий продукт швидше	− втрата частки ринку
Фінансова інформація	− зниження інвестиційної привабливості − пильна увага аудиторів	− штрафні санкції − фінансові втрати
Відомості по агентам, партнерам і умовам співпраці	− конкурент пропонує більш вигідні умови співпраці	− втрата кращих бізнес-партнерів

Джерело: узагальнено авторами на основі [2]

На відміну від багатьох інших секторів економіки, банківська індустрія більшою мірою зобов'язана відповідати вимогам законів та регулюючих стандартів. Недотримання вимог регуляторів може нести для фінансових установ величезні ризики аж до відкликання банківських, брокерських та дилерських ліцензій. Крім державних законів, актуальними стандартами банківської індустрії є Basel III, Payment Card Industry Data Security Standard (PCI DSS), ISO 27001 та інші. Відповідність стандартам досягається шляхом контролю інформаційних потоків, які містять конфіденційну інформацію, забезпечення високого рівня захисту персональних даних, гарантії захисту платіжних систем, зокрема еквайринг, а також іншої секретної документації, що стосується платіжних систем в процесингових центрах фінансових установ.

Деякі підприємства, зокрема, телекомунікаційні, наряду із вищезазначеними ризиками, можуть отримати ще й погіршення якості послуг, внаслідок витоку цінної інформації (табл. 2).

Таблиця 2

Виток та наслідки втрати інформації телекомунікаційної компанії

Виток інформації	**Ризик**	**Збитки**
Персональні дані клієнтів	– клієнти переходять до конкурента – позови до суду з боку клієнтів за законом «Про захист персональних даних» – перевірки з боку регулюючих органів	– зменшення прибутку – посилення конкуренції
Плани запуску нових тарифів та послуг	– конкуренти пропонують клієнтам вигідніші умови – конкуренти запускають нові програми раніше вас	– фінансові втрати – втрата клієнта
Відомості про ємності мереж і стан інфраструктури	– загроза стабільності роботи мереж – зниження якості послуг	– фінансові втрати – погіршення репутації
Дані про стратегічні угоди (партнерства, поглинання, злиття)	– скасування угоди – втрачений прибуток, великі збитки, збиток для репутації компанії та її керівників	– фінансові втрати – погіршення репутації
Дані маркетингових досліджень і унікальних методик аналізу	– втрата конкурентної переваги	– фінансові втрати
Відомості про перебої в роботі білінгу та інших платформ	– вразливості в інформаційних системах – шахрайство та злом систем	– фінансові втрати – штрафні санкції

Джерело: узагальнено авторами на основі [2]

Оператори зв'язку об'єднують під своїм початком велику кількість співробітників, що працюють на різних рівнях, але всі вони щодня оперують значними обсягами персональних даних та інформацією, що становить комерційну таємницю. Тому питання інформаційної безпеки у галузі телекомунікації мають бути одними з пріоритетних.

Зазвичай, при витоку конфіденційної інформації, втрачається лише її частка. Набувач аналізує цю частку та намагається відтворити інформацію в

повному обсязі. Розглянемо конфіденційну інформацію I як сукупність її часток:

$$I = \sum_{j=0}^{N} i_j \ , \tag{1}$$

де I – конфіденційна інформація;

i_j – j-та частка конфіденційної інформації;

N – кількість таких часток.

Вартістю збитків при втраті певної частки будемо вважати функцію $L(i_j)$:

$$\mathrm{L(i_j)} = \mathrm{P(i_j)} * \mathrm{k(i_j)}, \tag{2}$$

де $P(i_j)$ – вартість частки;

$k(i_j)$ – коефіцієнт корисності частки для набувача.

Для визначення вартості інформації використовують декілька підходів, зокрема традиційний підхід, оцінювання вартості грошового потоку, інвестиційний підхід, тобто визначення сукупної вартості володіння, зіставлення витрат та очікуваних вигід тощо [5].

Одночасно науковці [4, 6] пропонують оцінювати інформаційні системи шляхом показників, що дозволяють оцінити існуючий рівень ефективності виробництва і використання інформаційних ресурсів та виявити потенційні можливості його підвищення:

- показники інформаційної насиченості (інформаційна і техніко-інформаційна озброєність праці, ступінь використання комп'ютерної техніки за потужністю і за часом, відновлення парку ЕОМ, рівень організації інформаційних операцій);
- показники інформаційного потенціалу кадрів (структура витрат часу інженерно-технічних працівників на інформаційні процеси, обумовлена рівнем автоматизації робочих місць і рівнем кваліфікації користувачів);
- показники якості інформаційного забезпечення (корисність, вірогідність, повнота, доступність).

Узагальнено вартість інформації визначається її цінністю. Цінність інформації приймаємо як рівень максимальної користі, що можна отримати від залучення оцінюваної інформації до виконання певного завдання (виконання роботи, розв'язання задачі та проблемної ситуацій, оптимізація виробничого процесу тощо) за умови найліпшого способу використання цієї інформації. Формалізовано цінність інформації $P(I)$ можна визначити так:

$$P(I) = \Delta S(I) - d(I), \tag{3}$$

де S – показник, що є характеристикою ступеню успішності виконання поставленого завдання;

$d(I)$ – витрати на розробку та експлуатацію інформації Iу певному виді діяльності;

ΔS – зростання показника S за рахунок використання інформації I:

$$\Delta S(I) = S(I) - S_0 \ , \tag{4}$$

де S_0 – значення показника за відсутністю інформації I;

S(I) – значення показника S, що зріс завдяки використанню інформації I.

Аналогічно $P(i_j)$ відображає цінність частки інформації i_j так, що сума цінностей всіх часток складає цінність інформації взагалі:

$$P(I) = \sum_{j=0}^{N} \mathrm{P}(\mathrm{i_j}), \tag{5}$$

Цінність частки для набувача i_j залежить від можливості відтворити конфіденційну інформацію I. Чим більша частка, тим більша можливість відтворення I, а отже і $k(i_j)$ буде зростати зі збільшенням i_j. Причому, якщо $k(i_j) = 1$, то $i_j = I$. Межі $k(i_j)$ визначаються як $0 < k(i_j) \leq 1$.

Залежність коефіцієнту корисності інформації $k(i_j)$ від цінності частки $P(i_j)$, зображено на рис. 2.

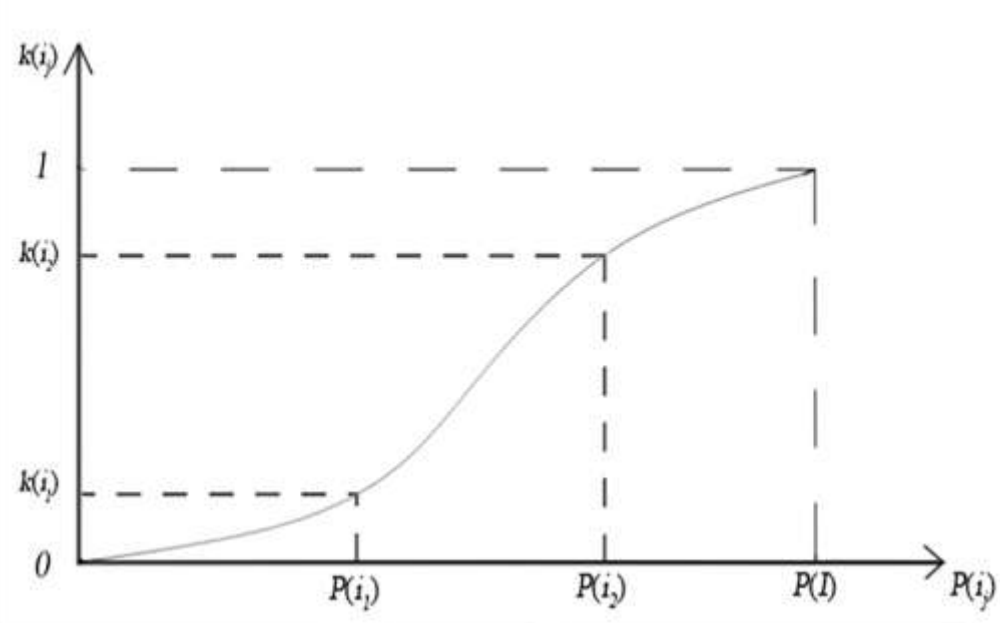

Рис. 2. Типова залежність коефіцієнта корисності інформації $k(i_j)$ від цінності її частки $P(i_j)$.

Приріст коефіцієнта корисності інформації для набувача на ділянці від 0 до $P(i_1)$ незначний, оскільки заволодівши частками до i_1 набувач не зможе

відтворити необхідні відомості про I в повному обсязі. На ділянці від $P(i_2)$ до $P(I)$ приріст корисності інформації також невеликий, оскільки починаючи з i_2 для набувача не складе труднощів відтворення відомостей про I в повному обсязі. На ділянці від $P(i_1)$ до $P(i_2)$ буде відбуватися значне зростання коефіцієнту корисності інформації порівняно з незначним зростанням її цінності.

Очевидно, що чим більше буде коефіцієнт корисної інформації що отримає набувач, тим більших потенціальних збитків може понести власник інформації.

Висновки. У статті значну увагу приділено результатам досліджень інцидентів в сфері інформаційної безпеки за останні роки у світі, які свідчать про необхідність систематизованого підходу до виявлення та оцінювання потенційних загроз та збитків внаслідок втрати інформації. Систематизовано склад ризиків втрати інформації для підприємств та визначено відповідні категорії – репутаційні, операційні, стратегічні та юридичні ризики. Наведено складові витоку інформації, ризики та можливі наслідки для комерційних банків та телекомунікаційних компаній, визначено специфіку інформаційної безпеки. Розглянуто підходи щодо оцінювання вартості інформації. На основі цього було здійснено моделювання збитків підприємства від втрати конфіденційної інформації. Побудована модель описує залежність збитків власника інформації від коефіцієнту корисної конфіденційної інформації, що була втрачена.

Наукова новизна проведеного дослідження полягає в запропонованому методологічному підході щодо визначення збитків підприємств від втрати інформації. Результати дослідження можуть бути використано для подальшого вивчення та удосконалення систем менеджменту інформаційної безпеки підприємства.

Література:

1. The Global State of Information Security Survey 2015. [Електронний ресурс]. – Режим доступу: http://www.pwc.ru/ru/riskassurance/publications/assets/managing-cyberrisks.pdf
2. Обеспечение безопасности бизнес-процессов. [Електронний ресурс]. –
3. Режим доступу: http://www.infowatch.ru/solutions/business_processes_optimization
4. Управление рисками. [Електронний ресурс]. – Режим доступу: http://www.infowatch.ru/solutions/risk_management
5. Яровий Л.В. Теоретичні підходи до оцінювання інформаційних ресурсів / Л.В. Яровий // Наукові праці НУХТ. – 2015., № 2 (21) – С. 93-99.

6. Монастирецький М.Г. Методологія дослідження та оцінки інформаційних
7. ресурсів / М.Г. Монастирецький, Г.І. Шалаєва, Н.О. Городько, Є.О. Цибуль-
8. ська // Реєстрація, зберігання і обробка даних. — 2002. — № 2. — С. 96-103.
9. Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №1 (50). – С. 96 – 101.