УДК [005.311.6:004.415.24]:005.52

МЕТОДОЛОГІЧНІ ПРОБЛЕМИ ЗБОРУ ТА АНАЛІЗУ ВИТОКІВ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

© 2014 **ЖАБИНЕЦЬ О. Й.**

УДК [005.311.6:004.415.24]:005.52

Жабинець О. Й. Методологічні проблеми збору та аналізу витоків конфіденційної інформації

У статті досліджено методологічні проблеми збору та аналізу витоків конфіденційної інформації в Україні та світі. Зокрема, проаналізовано особливості методології збору та аналізу інформації про витоки різних аналітичних структур світової ІТ-індустрії, графічно доведено наявність певного розриву між даними цих структур щодо кількості витоків, подано динаміку витоків конфіденційної інформації в різних галузях економіки у світі, а також у США та Росії із коротким аналізом ситуації у сфері захисту інформації та станом інформаційної безпеки в цих країнах. Автор робить висновок, що на сьогоднішній день відсутній єдиний підхід щодо збору та аналізу причин ы видів витоків конфіденційної інформації, внаслідок чого неможливо порівняти результати досліджень різних аналітичних компаній ІТ-індустрії та зробити висновки про їх достовірність. Як правило, кожна з компаній при зборі та аналізі витоків конфіденційних даних використовує власну методологію, здійснює відбір витоків за власною системою та намагається розв'язати лише ті проблеми, які виникли внаслідок використання програмного забезпечення власного виробництва. Непорівнюваність отриманих результатів через відсутність спільних показників і методології збору та аналізу витоків ускладнює процес прийняття ефективних рішень у системі захисту інформації та інформаційної безпеки.

Ключові слова: *витоки конфіденційної інформації, методологічні проблеми, аналітичні структури, світова ІТ-індустрія, фінансові втрати від витоків.*

Рис.: *7.* ***Табл.:*** *1.* ***Бібл.:*** *12.*

Жабинець Ольга Йосифівна *– кандидат економічних наук, доцент, доцент, кафедра фінансів, Львівський державний університет внутрішніх справ (вул. Городоцька, 26, Львів, 79066, Україна)*

E-mail: *olza@ukr.net*

УДК [005.311.6:004.415.24]:005.52

Жабинец О. И. Методологические проблемы сбора и анализа утечек конфиденциальной информации

В статье исследованы методологические проблемы сбора и анализа утечек конфиденциальной информации в Украине и мире. В частности, проанализированы особенности методологии сбора и анализа информации об утечках различных аналитических структур мировой ИТ-индустрии, графически доказано наличие определенного разрыва между данными этих структур по количеству утечек, представлена динамика утечек конфиденциальной информации в различных отраслях экономики в мире, а также в США и России с кратким анализом ситуации в сфере защиты информации и состоянием информационной безопасности в этих странах. Автор делает вывод, что на сегодняшний день отсутствует единый подход к сбору и анализу причин и видов утечек конфиденциальной информации, в результате чего невозможно сравнить результаты исследований различных аналитических компаний ИТ-индустрии и сделать выводы об их достоверности. Как правило, каждая из компаний при сборе и анализе утечек конфиденциальных данных использует собственную методологию, осуществляет отбор утечек по собственной системе и пытается решить только те проблемы, которые возникли в результате использования программного обеспечения собственного производства. Несопоставимость полученных результатов из-за отсутствия общих показателей и методологии сбора и анализа утечек усложняет процесс принятия эффективных решений в системе защиты информации и информационной безопасности.

Ключевые слова: *утечки конфиденциальной информации, методологические проблемы, аналитические структуры, мировая ИТ-индустрия, финансовые потери от утечек.*

Рис.: *7.* ***Табл.:*** *1.* ***Библ.:*** *12.*

Жабинец Ольга Иосифовна *– кандидат экономических наук, доцент, доцент, кафедра финансов, Львовский государственный университет внутренних дел (ул. Городоцкая, 26, Львов, 79066, Украина)*

E-mail: *olza@ukr.net*

UDC [005.311.6:004.415.24]:005.52

Zhabynets Olga Yo. Methodological Problems of Collection and Analysis of Confidential Information Leakage

The article studies methodological problems of collection and analysis of confidential information leakages in Ukraine and in the world. In particular, the article analyses specific features of the methodology of collection and analysis of information about leakages of various analytical structures of the world IT industry, graphically proves availability of a certain gap between data of these structures by the number of leakages, and also presents dynamics of confidential information leakages in various branches of economy in the world, and also USA and Russia, with a brief analysis of the situation in the sphere of protection of information and state of information security in these countries. The author holds that, as of today, there is no common approach to collection and analysis of reasons and types of confidential information leakages, in the result of which it is impossible to compare results of studies of different analytical companies of the IT industry and make a conclusion about their authenticity. As a rule, any company uses, when collecting and analysing confidential data leakages, own methodology, selects leakages on its own discretion and tries to solve only those problems, which arose as a result of the use of in-house software. Incomparability of the obtained results due to absence of general indicators and methodology of collection and analysis of leakages complicates the process of making efficient decisions in the system of protection of information and information security.

Key words: *confidential information leakage, methodological problems, analytical structures, world IT industry, financial losses from leakages.*

Pic.: *7.* ***Tabl.:*** *1.* ***Bibl.:*** *12.*

Zhabynets Olga Yo.*– Candidate of Sciences (Economics), Associate Professor, Associate Professor, Department of Finance, Lviv State University of Internal Affairs (vul. Gorodotska, 26, Lviv, 79066, Ukraine)*

E-mail: *olza@ukr.net*

Глобальне інформаційне суспільство, яке стрімко розвивається під впливом науково-технічного прогресу та ІТ-технологій, забезпечує високу мобільність у передачі різних видів інформації, у т. ч. конфіденційної, її обробки та використання. Водночас зростає й кількість випадків несанкціонованого доступу до інформаційних ресурсів, внаслідок чого відбувається незаконне копіювання та викрадення різного виду конфіденційної інформації. Функціонування інформаційної індустрії сьогодні не можна уявити без структур, діяльність яких направлена не тільки на створення ІТ-технологій, але й систем їх безпеки, а також систематизації та аналізу даних щодо витоків кон-

фіденційної інформації, їх узагальнення та обробки. Вирішення існуючих методологічних проблем збору та аналізу витоків конфіденційної інформації є необхідним для забезпечення достовірності та порівнюваності отриманих результатів, а також постійного вдосконалення уже існуючих в системі інформаційної безпеки інноваційних технологій.

Інформаційну безпеку та проблеми захисту інформації розглядали у своїх працях такі вітчизняні та іноземні дослідники, як Брассар Ж., Войналович О., Городецький А., Калюжний Р., Кормич Б., Мотлях О., Нисневич Ю., Рівест Р., Уітті Р., Олійник О., Цимбалюк В. та ін. Незважаючи на значну кількість публікацій з даної проблематики, дослідження методологічних проблем збору та аналізу витоків конфіденційної інформації поки залишається поза увагою більшості науковців, що обумовило вибір тематики даної наукової статті.

Метою статті є дослідження методологічних проблем збору та аналізу витоків конфіденційної інформації в Україні та світі.

У створенні системи захисту інформації та забезпеченні інформаційної безпеки як на рівні держави, так і міжнародному рівні важливе значення має методологія збору та аналізу витоків конфіденційних даних.

Розглянувши аналітичні звіти різних компаній світової ІТ-індустрії, ми можемо стверджувати, що ці компанії користуються відмінними методологіями під час збору та аналізу інформації про витоки, внаслідок чого дуже важко зробити порівняльний аналіз та обґрунтовані висновки. Загальну характеристику аналітичних структур світової ІТ-індустрії, які найбільш повно та систематично публікують інформацію про витоки, використовуючи власну методологію збору та аналізу цієї інформації, а також деякі особливості їх роботи подано в *табл. 1*.

Варто зазначити, що на сайті центру Zecurion Analytics вказується, що потенційний збиток інцидентів розраховується за внутрішньою методикою Zecurion Analytics, що враховує тип і обсяг скомпрометованих даних, галузеву специфіку, особливості національного законодавства, а також реакцію на інцидент з боку регулюючих органів, ЗМІ та громадськості. Експертна оцінка збитку може відрізнятися від реального значення збитку як у бік збільшення, так і убік зменшення суми. Так, Zecurion Analytics за 2012 р. зафіксував 825 витоків інформації у світі, з них в Росії – 36, у США – 569. У відповідності до даних Privacy Rights Clearinghouse, у 2012 р. лише в США було оприлюднена інформація про 683 випадки. InfoWatch за 2012 р. дає такі дані: світ – 934, США – 576, Росія – 75.

Ponemon Institute взагалі щодо кількості витоків використовує середньозважені величини та надає лише середню кількість скомпрометованих записів за один витік інформації.

Таблиця 1

Порівняльна характеристика аналітичних структур світової ІТ-індустрії *

Назва компанії	Загальна характеристика компанії	Особливості роботи
Ponemon Institute	Американська компанія, яка проводить незалежні дослідження по конфіденційності, захисту даних і політиці інформаційної безпеки	1) інформацію збирає за допомогою інтерв'юєрів у відібраних фірмах за власною методикою; 2) до аналізу не включає ті інциденти, коли під час одного витоку інформації скомпрометовано більше, ніж 100 000 записів; 3) складає аналітику разом із розробником комп'ютерних програм Symantec Corporation
InfoWatch	Російська компанія, що випускає засоби захисту інформації на основі DLP-системи, заснована компанією Лабораторія Касперського	1) використовує дані з відкритих джерел та з бази даних, яка поповнюється спеціалістами компанії; 2) до звіту не включає випадки витоку інформації, які відбулися унаслідок зовнішніх комп'ютерних атак; 3) не проводить експертні оцінки втрат, а користується даними про їх розміри із відкритих джерел
Zecurion Analytics	Аналітичний підрозділ компанії Zecurion – найбільшого російського розробника систем захисту інформації від внутрішніх загроз	1) інформацію збирає із відкритих джерел та з результатів роботи компанії Zecurion з клієнтами; 2) в базу інцидентів не потрапляють атаки, реалізовані виключно зовнішніми зловмисниками без будь-якого сприяння з боку інсайдерів; 3) у статистиці не відображені інциденти, для яких потенційний збиток складає менше $5 тис.
Privacy Rights Clearinghouse	Американська неприбуткова компанія, що залучає, навчає та розширює можливості окремих осіб задля захисту приватного життя	Розміщує на власному сайті усі повідомлення про витоки конфіденційної інформації, які були отримані з відкритих джерел
Trustwave	Американська компанія – світовий лідер з надання послуг безпеки	Збирає інциденти шляхом отримання повідомлення від компанії-жертви або третіх осіб (правоохоронні або регулюючі органи)
incidents.su	Російський портал новин по інцидентах інформаційної безпеки	На сайті розміщуються повідомлення про витоки конфіденційної інформації, які отримані з відкритих джерел по країнах СНД

Джерело: складено автором.

* Вибірка автора для проведення порівняльного аналізу.

У Росії з кінця 2011 р. існує аналог Privacy Rights Clearinghouse – web-портал incidents.su. Компанія займається збором інцидентів в країнах СНД. Принцип внесення інцидентів до бази той самий, що й в компанії з США – збираються всі факти з відкритих джерел. На сьогоднішній день зведений звіт по інцидентам є уривчастим. Так, в Україні у 2012 р/ компанією зафіксовано 57 витоків конфіденційної інформації.

Дані про кількість витоків конфіденційної інформації в цілому у світі, е США, Росії та Україні за даними різних аналітичних структур подано на *рис. 1 – рис. 4* відповідно.

У США хронологію витоків інформації з 2005 р. веде Privacy Rights Clearinghouse. У свою чергу консалтингові фірми, фірми з IT-індустрії намагаються також публікувати звіти, в яких аналізують дані про витоки інформації й роблять певні висновки, прогнози й т.п. Адже у відповідності до американського законодавства компанія, яка допустила виток персональних даних, найперше повинна повідомити про це всіх постраждалих, Крім того, на таку компанію можуть бути накладені штрафні санкції та суми відшкодування постраждалим особам [3].

Варто зазначити, що саме в США вперше у світі було запроваджено законодавство у сфері інформаційної безпеки, і саме там започатковано збір інформації про витоки, здійснення судових процесів, а також розрахунків втрат від витоків конфіденційних даних.

Як видно з рис. 1 – 4, існує певний розрив між даними різних аналітичних структур. Особливо відчутним цей розрив спостерігається між InfoWatch та incidents.su щодо витоків конфіденційної інформації в Україні, внаслідок чого важко робити висновки про їх достовірність.

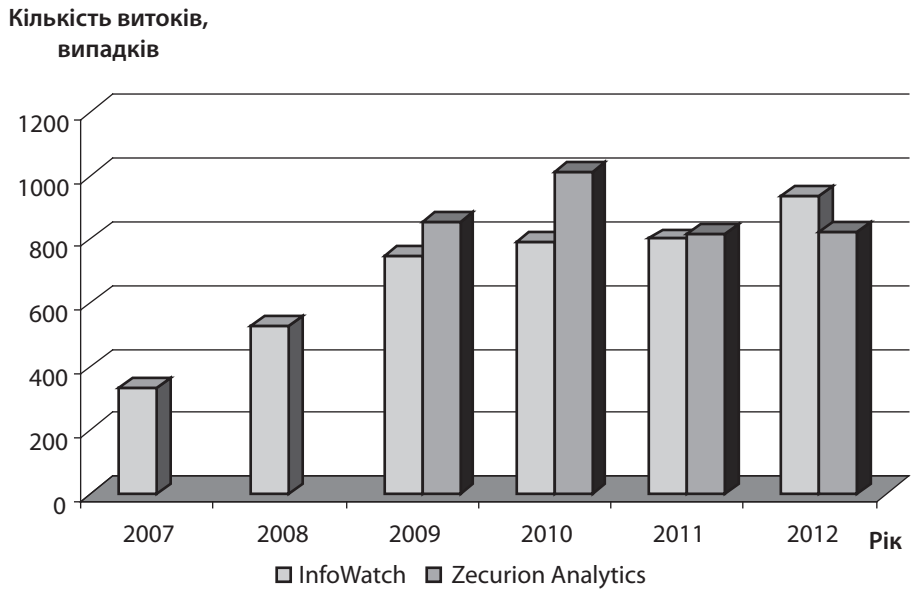

Рис. 1. Кількість витоків конфіденційної інформації у світі (випадків)

Джерело: побудовано автором за [1; 2].

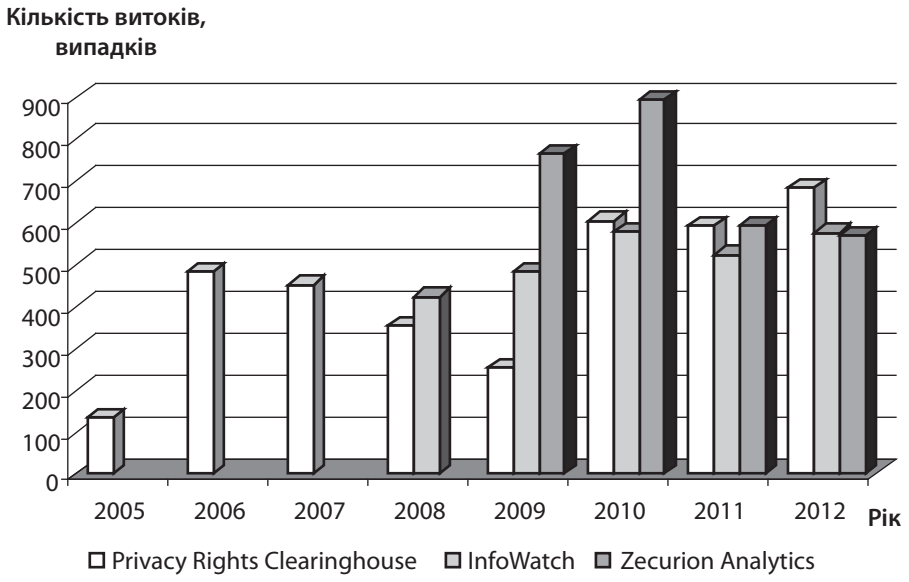

Рис. 2. Кількість витоків конфіденційної інформації у США (випадків)

Джерело: побудовано автором за [1; 2; 3].

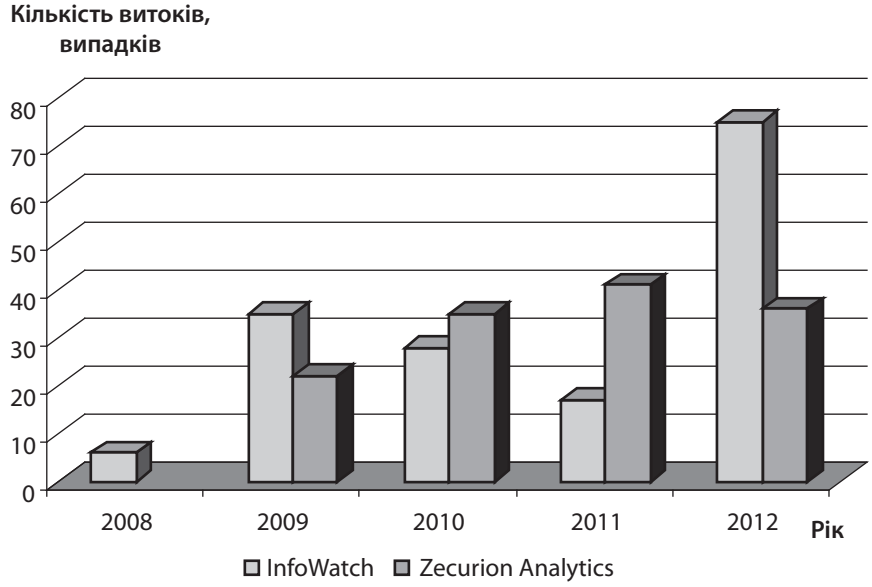

Рис. 3. Кількість витоків конфіденційної інформації в Росії (випадків)

Джерело: побудовано автором за [1;2;4;5].

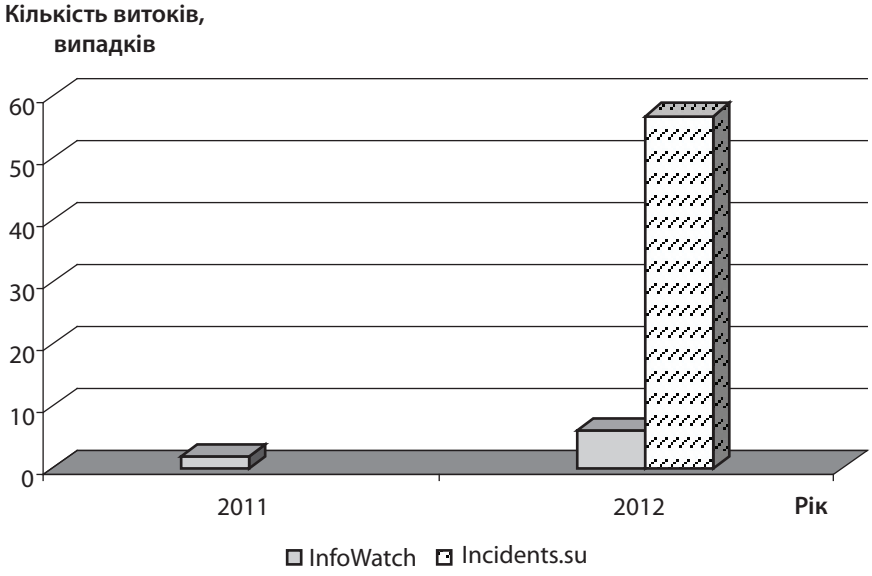

Рис. 4. Кількість витоків конфіденційної інформації в Україні (випадків)

Джерело: побудовано автором за [6; 7].

З точки зору національної безпеки забезпечення абсолютної безпеки інформації є стратегічною метою. Однак з комерційної точки зору абсолютна безпека не завжди є виправданою, якщо порівнювати витрати на її забезпечення та збитки, що можуть виникнути внаслідок втрати цієї інформації. З огляду на це, важливе значення має оцінка вартості інформації, яку необхідно захистити.

Загальна вартість збитків від витоку даних відповідно до класифікації Ponemon Institute включає такі елементи:

1) витрати на виявлення і ескалацію;
2) витрати на повідомлення;
3) витрати на відповідь постфактум;
4) прямі втрати бізнесу [8].

Наприклад, у Британії, згідно з даними аналітичної компанії Ponemon Institute, середня вартість одного витоку інформації для фірм складає приблизно 1,7 млн фунтів [9]. У нас подібні дані відсутні, та й постраждалі компанії не поспішають відкрито заявляти про свої втрати.

Світова статистика свідчить, що найбільша частка інформації, яка підлягає витоку,– це інформація про клієнтів або працівників. За деякими оцінками, у світі близько 90% вкрадених у 2012 р. даних були персональними [10]. Щодо України, то існує дослідження компанії SearchInform по Києву за 2012 р., у відповідності до якого персональних даних стосувалося 70% витоків інформації, друге місце займає комерційна таємниця компаній, на третьому – технічна документація компаній [7].

Варто зазначити, що в Україні (в одній з останніх серед країн СНД) лише у 2010 р. було прийнято Закон України «Про захист персональних даних». Із прийняттям цього закону різні підприємницькі структури вимушені були більш сумлінно ставитись до налагодження системи інформаційної безпеки. Однак в Україні лише 11% компаній мають спеціальні підрозділи із захисту інформації, у 10% фірм – захистом інформації займається лише один спеціаліст, у 79%

цим займаються спеціалісти ІТ-відділів або інші непрофільні спеціалісти. Крім того, серед потенційних каналів витоку найбільше контролюється корпоративна електронна пошта – у 70% компаній, а найбільш захищеними об'єктами витоків є бази даних клієнтів і співробітників [11].

Динаміку витоків конфіденційної інформації в різних галузях економіки у світі, у США та Росії демонструють *рис. 5 – рис. 7* відповідно.

У світовому масштабі (рис. 5) у 2012 році найбільше витоків конфіденційної інформації зафіксовано у роздрібній торгівлі (45%), харчовій промисловості (24%), туризмі та готельному бізнесі (9%), а також у фінансовій сфері (7%).

У США безперечним лідером за витоками конфіденційної інформації протягом 2010 – 2012 рр. є медицина (див. рис. 6), хоча ще у 2009 р. найбільше витоків було зафіксовано в системі освіти. Частка витоків конфіденційної інформації в США у 2012 р. із медичних закладів склала 32,8%, роздрібної торгівлі – 15,5%, комерційних та державних структур, а також освітніх закладів – 12,9% і сфери фінансів – 10,5%.

За даними аналітичного центру Zecurion Analytics, у Росії у 2012 р. розмір збитку від витоків конфіденційної інформації залишився приблизно на рівні 2011 р. і склав $20,083 млрд. Середній збиток від кожного інциденту дорівнює $ 24,34 млн. Як видно з рис. 7 найчастіше витік інформації відбувається із освітніх закладів (20,1%), держсектора (16,9%), підприємств роздрібної та інтернет-торгівлі (12,4%), а також медустанов (12,3%). Найбільш поширені канали витоків в Росії за даними Zecurion Analytics - це веб-сервіси (20,5 %), ноутбуки та планшети (16,5%), а також мобільні накопичувачі (11,1%). На частку Росії припадає 4,4% від світової кількості зареєстрованих внутрішніх інцидентів у сфері інформаційної безпеки [2]. Ця цифра може бути вищою, якщо враховувати інциденти із незначним по-

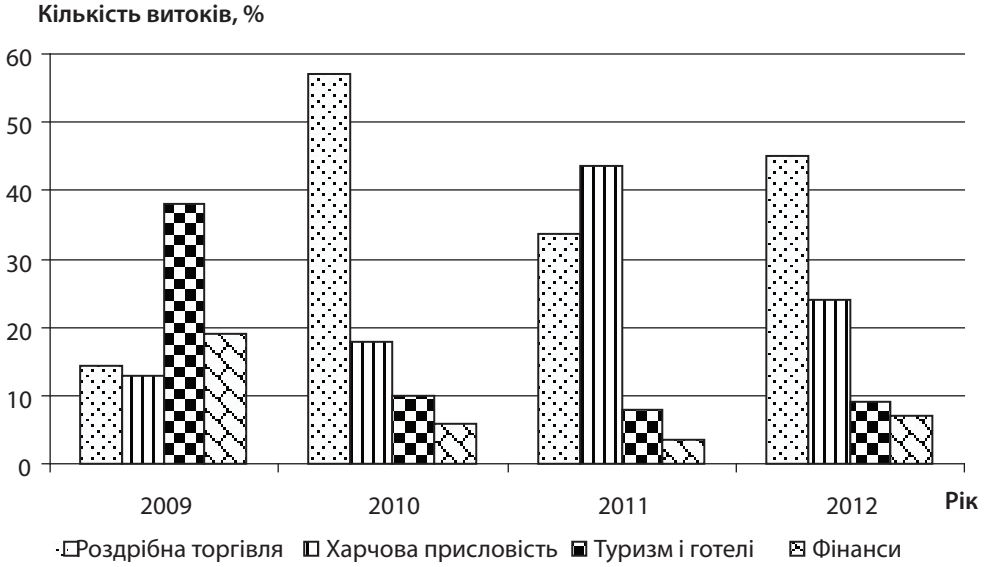

Рис. 5. Витоки конфіденційної інформації в галузях економіки у світі, %

Джерело: побудовано автором за [12].

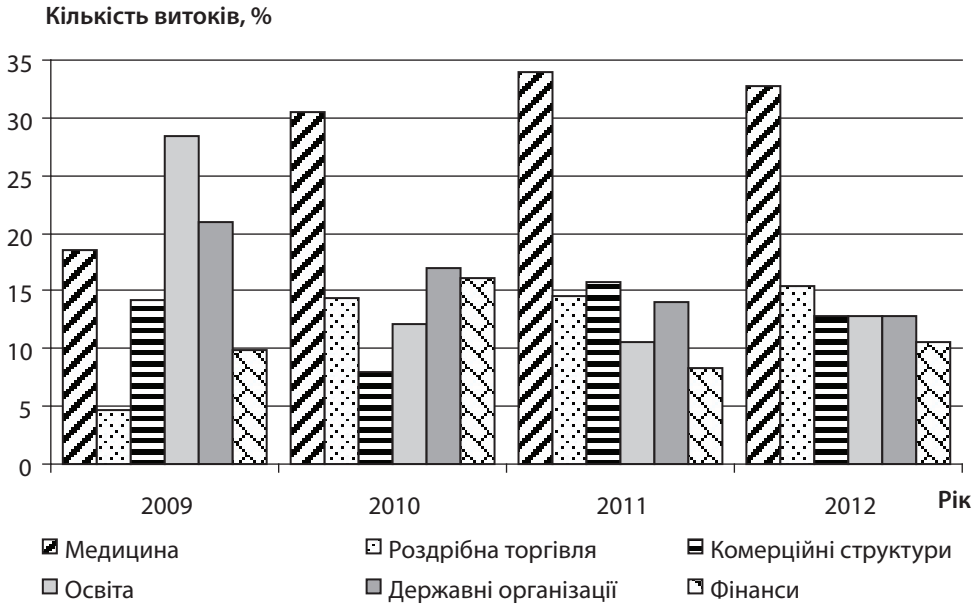

Рис. 6. Витоки конфіденційної інформації в галузях економіки у США, %

Джерело: розраховано та побудовано автором за [3].

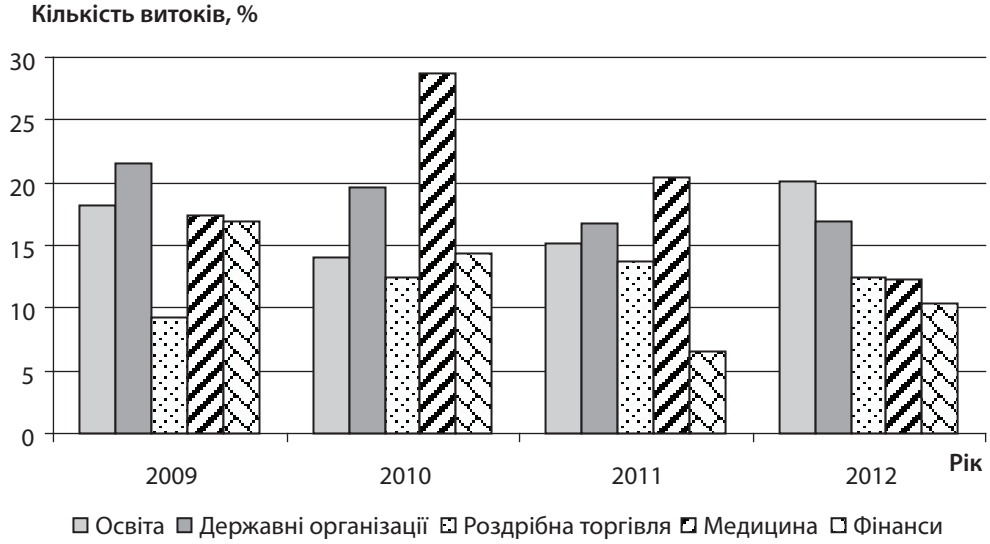

Рис. 7. Витоки конфіденційної інформації в галузях економіки у Росії, %

Джерело: побудовано автором за [2].

тенційним збитком, адже статистика Zecurion Analytics не враховує витоки, для яких потенційний збиток складає менше $ 5 тис. (див. табл. 1).

Незважаючи на поступове посилення нормативного пресингу та збільшення штрафних санкцій за витік конфіденційної інформації, ситуація в Росії у сфері захисту від внутрішніх загроз практично не змінюється в кращий бік. Кількість витоків не зменшується, що вказує на неефективність тих засобів захисту, які використовуються, а також на недостатність уваги до проблеми з боку топ-менеджменту компаній. Істотні фінансові та репутаційні втрати від інцидентів інформаційної безпеки в Росії відчутно впливають на бізнес навіть великих компаній.

ВИСНОВКИ

Проведене дослідження засвідчило, що на сьогоднішній день відсутній єдиний підхід щодо збору та аналізу причин і видів витоків конфіденційної інформації, внаслідок чого неможливо порівняти результати досліджень різних аналітичних компаній ІТ-індустрії та зробити висновки про їх достовірність. Як правило, кожна з компаній при зборі та аналізі витоків конфіденційних даних використовує власну методологію, здійснює відбір витоків за власною системою та намагається розв'язати лише ті проблеми, які виникли внаслідок використання програмного забезпечення власного виробництва. Непорівнюваність отриманих результатів через відсутність спільних показників і методології збору та аналізу витоків ускладнює процес прийняття ефективних рішень в системі захисту інформації та інформаційної безпеки. Однією з причин такого стану речей може бути й те, що лише в останні роки в окремих країнах світу почало формуватися законодавство, яке вимагає від організацій стандартизованих заходів щодо збереження конфіденційної інформації та посилює відповідальність за її втрату. ■

ЛІТЕРАТУРА

1. Глобальное исследование утечек корпоративной информации и конфиденциальных данных 2012 [Электронный ресурс]. – Режим доступа : http://www.infowatch.ru

2. Утечки конфиденциальной информации 2012 [Электронный ресурс]. – Режим доступа : http://www.zecurion.ru

3. Chronology of Data Breaches Security Breaches 2005 – Present [Электронный ресурс]. – Режим доступа : http://www.privacyrights.org

4. Глобальное исследование утечек 2009 [Электронный ресурс]. – Режим доступа : http://www.infowatch.ru

5. Глобальное исследование утечек конфиденциальной информации 2010 [Электронный ресурс]. – Режим доступа : http://www.infowatch.ru

6. Утечки по странам [Электронный ресурс]. – Режим доступа : http://www.infowatch.ru

7. Идов Р. Самые популярные утечки информации в Киеве за 2012 год / Р. Идов [Электронный ресурс]. – Режим доступа : http://delo.ua

8. 2013 Cost of Data Breach Study: Global Analysis [Електронний ресурс]. – Режим доступу : https://www4.symantec.com

9. Brewster T. UK Data Breach Cost Drops To £1.75 Million / T. Brewster [Електронний ресурс]. – Режим доступу : http://www.techweekeurope.co.uk

10. Trustwave 2013 Global Security Report [Електронний ресурс]. – Режим доступу : http:// www.trustwave.com

11. Zecurion Analytics: Данные в украинских компаниях будут защищаться лучше [Електронний ресурс]. – Режим доступу : http://delo.ua

12. Trustwave 2010, 2011, 2012, 2013 Global Security Report [Електронний ресурс]. – Режим доступу : http:// www.trustwave.com

REFERENCES

Brewster, T. "UK Data Breach Cost Drops To £1.75 Million" http://www.techweekeurope.co.uk

"Chronology of Data Breaches Security Breaches 2005 - Present" http://www.privacyrights.org

"2013 Cost of Data Breach Study: Global Analysis" https://www4.symantec.com

"Globalnoe issledovanie utechek 2009" [A global study of leaks in 2009]. http://www.infowatch.ru

"Globalnoe issledovanie utechek konfidentsialnoy informatsii 2010" [A global study of leaks of confidential information in 2010]. http://www.infowatch.ru

"Globalnoe issledovanie utechek korporativnoy informatsii i konfidentsialnykh dannykh 2012" [A global study of corporate