УДК 004.056

**В.Л. Шевченко**

# КРАЩІ СВІТОВІ ПРАКТИКИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ЇХ ВПЛИВ НА ЕКОНОМІЧНУ СТАБІЛЬНІСТЬ ДЕРЖАВИ

Проаналізовані темпи зростання та основні джерела інформаційних загроз. Темпи зростання кількості інформаційних інцидентів в 2 рази перевищують темпи зростання світового внутрішнього валового продукту. Інформаційно безпечні місця на планеті вже відсутні. Визначені глобальний характер інформаційних загроз. Інформаційна безпека вже не є особистим питанням. Необхідні сумісних дії щодо забезпечення інформаційної безпеки. Безпека галузей економики залежить від частки підприємств галузі, які підтримують інформаційну безпеку на задовільному рівні. Визначені оптимальні показники видатків на інформаційну безпеку. Сьогодні найбільшу ефективність має інвестування в інформаційну безпеку малих підприємств.

***Ключові слова:*** інформаційна безпека, загрози, інціденти, видатки, ефективність інвестування.

**Постановка проблеми**

Складно заробити купу грошей. Ще складніше їх зберегти в умовах інфляції, конкуренції, криміналу. Дуже складно створити ефективну інформаційну інфраструктуру. Ще складніше зберегти її працездатність в умовах інформаційної боротьби, кіберзлочінності та кіберхуліганства. Щоб інформаційну інфраструктуру зберегти – потрібно інформаційною безпекою управляти.

**Аналіз останніх досліджень і публікацій**

Багато хто в цьому питані на перше місце ставить технології. Саме тому в управлінні інформаційною безпекою (ІБ) використовують результати всіх дисциплін ІБ: кібернетична безпека, системи технічного захисту інформації, нормативно-правове забезпечення, але насамперед технології управління, які починаються з топ-менеджменту. Це підтверджує 18-те щорічне опитування керівників більш ніж 1300 найбільших компаній світу, яке було проведеноPwC, «PricewaterhouseCoopers» (ДАВОС, ШВЕЙЦАРІЯ, 26 січня 2015 року) [1]. Кібербезпека перестала бути проблемою лише фахівців ІТ и ІБ. Інциденти в сфері ІБ впливають на діяльність вищого керівництва і на рішення ради директорів. Серед факторів, що викликають найбільшу стурбованість керівників відмічають кібер-загрози і недостатній рівень захисту даних (61%).

Кіберзагрози охоплюють сфери, які є далекими від ІТ. За даними Центру з вивчення фінансових інновацій і даним PwC**,** кіберризик вперше з 2007 року увійшов у рейтинг ризиків страхового сектору, заняв 4 місце в рейтингу основних ризиків і 1 місце в страхуванні іншому, ніж страхування життя **[2]**. Проблема полягає в тому, що інциденти ІБ зростають не лише кількісно, але й велика їх частка залишається непоміченою. На форумі Cisco 8 жовтня 2015 в Києві старший віце-президент Cisco і директор компанії з питань інформаційної безпеки Джон Стюарт повідомів, що середній час виявлення інциденту в галузі 200 днів і надзадачою є зменшення цього показника до 2 днів[3].

З матеріалів глобального дослідження з питань перспектив забезпечення ІБ на 2015 рік (TheGlobalStateofInformationSecurity®Survey 2015), який був проведенийPwC сумісно з журналами CIOiCSO слідує, щоінформаційно-безпечних місць на планеті не залишилось. Серед обєктів атак фондові біржі, банки, АСУ енергетичних компаній, супермаркети, соціальні мережі, особисті інформаційні ресурси, Інтернет речей, цифрові системи управління автомобілями тощо. Серед втрат гроши, інформація, репутація, бізнес [4, 5, 6].Новою тенденцією є вихід інформаційнх інцидентів на державний рівень. Причому не лише в частині жертв, але й в частині зловмисників. Наприклад, інциденти, які пов’язані з Едвардом Сноуденом, та також викриття компанією Symantecбагаторічної серії інцидентів, спрямованих проти урядів європейських країн з боку агентів, яких підтримують інші держави.

Не вирішена раніше частина загальної проблеми полягає в тому, що основною умовою економічного росту сьогодні є розширення впровадження інформаційних та

телекомунікаційних технологій, які, в свою чергу, потерпають від інформаційних та кібернетичних небезпек. Зростання кількості інформаційних та кібернетичних інцидентів унеможливлює економічну стабільність та економічне зростання. Життєво необхідно визначити найбільш актуальні напрями інновацій в галузі захисту інформаційних та телекомунікаційних технологій.

**Мета статті**

Виявлення найбільш важливих інформаційних ти кібернетичних небезпек, оцінювання їх масштабів та визначення пріоритетів фінансування інформаційной безпеки.

**Виклад основного матеріалу**

Кількість інцидентів зростає в середньому на 66% щорічно, що як мінімум, вдвічі вище темпів росту мобільного ринку і росту світового ВВП (рис.1). При цьому не менше 71% реалізованого несанкціонованого доступу в систему залишається невиявленими [5, 6].

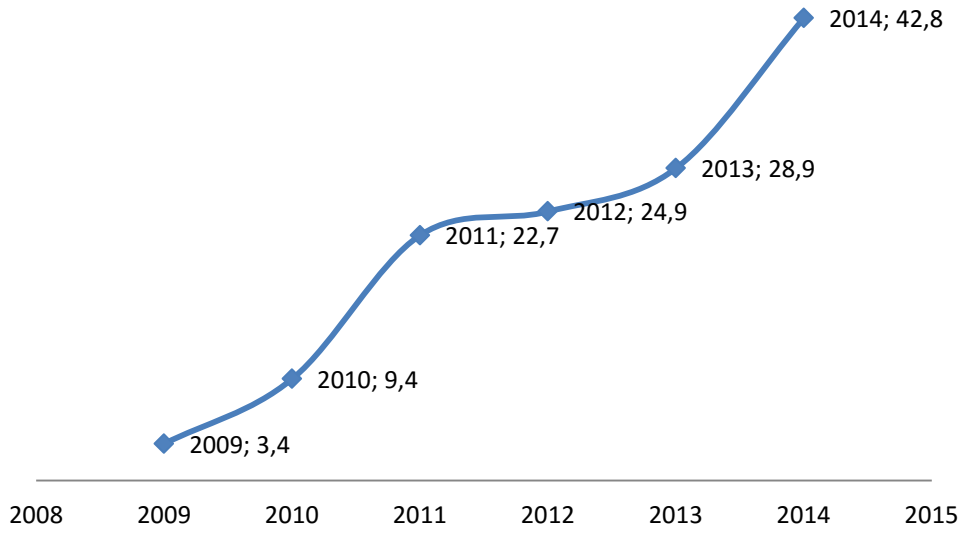


Рис.1. Темпи зростання кількості інцидентів ІБ

В сфері охорони здоровя і медичного страхування відмічається **60%**щорічний рост зареєстрованих інцидентіві збільшення фінансових втрат на **282%** [7].Тільки в США, за інформацією Бюро судової статистики, в 2012 році фінансовізбитки внаслідок викрадання та незаконного використання особистих даних, які включаютьвідомості про платіжні картки, банківськи рахункиі особисте життя, склали загалом **24,7 млрд дол.США** [5, 6].Особливо великі збитки (в розмірі не менше 20 млн долларів США) щорічно зростають майже вдвічі (наприклад, в 2013 році на 92%). Уільям Боні, керівник службикорпоративноїІБ компанії T-Mobile US пояснює це тим, що втрати все більше пов'язані не лише з відновленням внутрішньої технічної інфраструктури, але й з зовнішніми наслідками (падіння доходів, іміджу, руйнування комерційних зв'язків, виток інформації).

Згідно даних PwC, щорічні збитки від кіберзлочинності для світової економіки складають від 375 млрд до 575 млрд доларів США. Збитки від втрати інформації, що складає комерційну таємницю - від 749 мільярдів до 2,2 трильйонів доларів США щорічно, що відповідає від 1 до 3% ВВП країни.

Найбільший приріст кількості інцидентів, найбільші збитки і, відповідно, найбільші бюджети на ІБ спостерігаються в середних і великих компаніях (табл.) [5, 6]. Більш успішні показники малих компаній свідчать не про меншу кількість інцидентів, а про менший ступінь їх виявлення.

Таблиця

| | **Малі компанії** | **Середні компанії** | **Великі компанії** |
|---|---|---|---|
| Розмір доходів компанії, млн. долл. США | менш 100 | від 100 до 1000 | більш 1000 |
| **Кількість виявлених інцидентів** | | | |
| 2013 год | 1151 | 2581 | 9155 |
| 2014 год | 1091 | 4227 | 13138 |
| Приріст | **-5%** | **64%** | **44%** |
| **Бюджет на забезпечення ІБ, млн.дол. США** | | | |
| 2013 год | 0,92 | 2,8 | 10,3 |
| 2014 год | 0,73 | 3 | 10,8 |
| Приріст | **-21%** | **7%** | **5%** |
| **Середній розмір фінансових збитків від інцидентів ІБ, млн. дол. США** | | | |
| 2013 год | 0,65 | 1 | 3,9 |
| 2014 год | 0,41 | 1,3 | 5,9 |
| Приріст | **-37%** | **30%** | **51%** |

Це особливо небезпечно тим, що зловмисники використовують малі компаніїяк плацдарм подальшого проникнення в великі і середні. Поряд з управліннямсвоєюІБ стаєтакож необхідним утримання в заданих рамках ІБ партнерів. За 100 бальною шкалою межа задовільного стану галузі лежить на рівні 60 (рис.2). Необхідною умовою збереження безпечного стану галузі є підтримання задовільного рівня інформаційною безпеки щонайменше в 25% підприємств галузі. Якщо кількість таких підприємств стане менше 25%, то галузь почне входити в кризовий стан. А якщо менше 20%, то стане на межу повної інформаційної руйнації, наслідком якої буде неспроможність галузі самостійно повернутись до нормального стану за допомогою штатних заходів. Означені закономірності якісно подібні до закономірностей підтримання імунітету популяції [8, 9, 10].

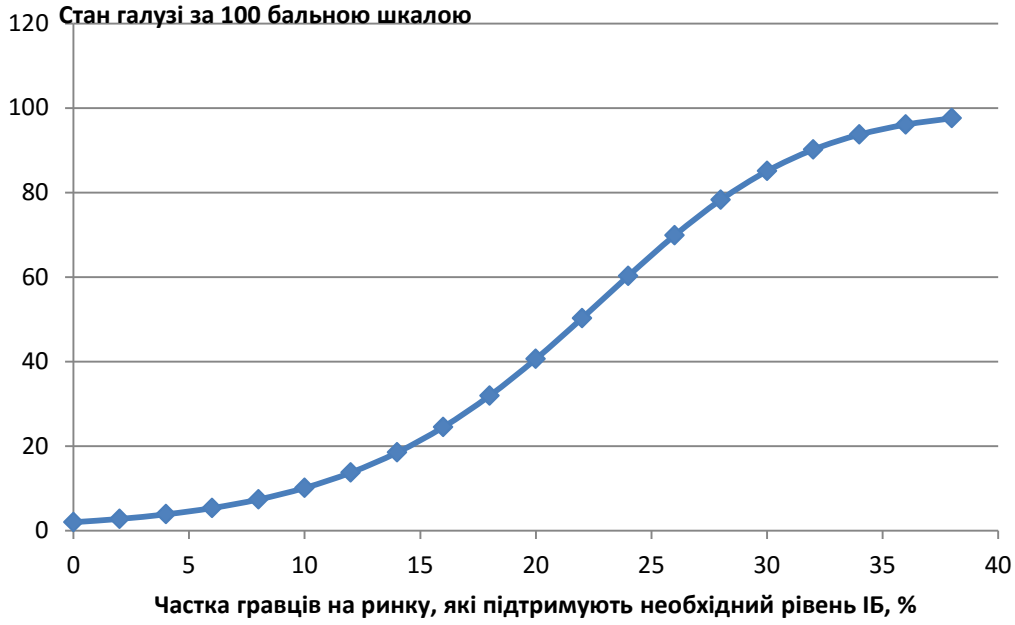


Рис.2. Залежність стану галузі від частки компаній, що підтримують ІБ на необхідному рівні.

Винуватцями інцидентів частіше всього стають свої (діючі або колишні) співробітники і партнери. Їх доля зростає[5, 6].Тому логічно, що навчання і інформування персоналу єневід'ємними елементами будь-якої програми розвитку[5, 11]. За думкою PwC в компаніях, де не проводиться навчання з питань безпеки для нових співробітників, розмір щорічних фінансових втрат в 4 рази перевищує аналогічний показник в компаніях, де таке навчання організовано.

Бюджети компаній на ІБ коливаються в діапазонівід 2,3% (Росія), 3,5% (Європа) до 3,8% (по всьому світу) від розмірівзагальних видатків на ІТ. Основними статтями видатків на ІБ є профілактика, захист, виявленняі реагування. Пріоритетними напрямками фінансування ІБ є впровадження процесівінтеграціїзасобів прогнозування, запобігання, виявленняі реагування на інциденти, а також фінансування розвитку кадрового потенціалуі функціональності процесів.

Імітаційне моделювання показує, що сумарна залежність втрат від інформаційних інцидентів та видатків на забезпечення ІБ, має зону оптимуму в діапазоні видатків на ІБ від 1,8 до 4,4% від загальної суми видатків на інформаційні технології компанії (рис.3). Для врахування несподіваних впливів непередбачених обставин слід працювати в верньої частині означеного діапазону, що й відповідає кращім світовим практикам.

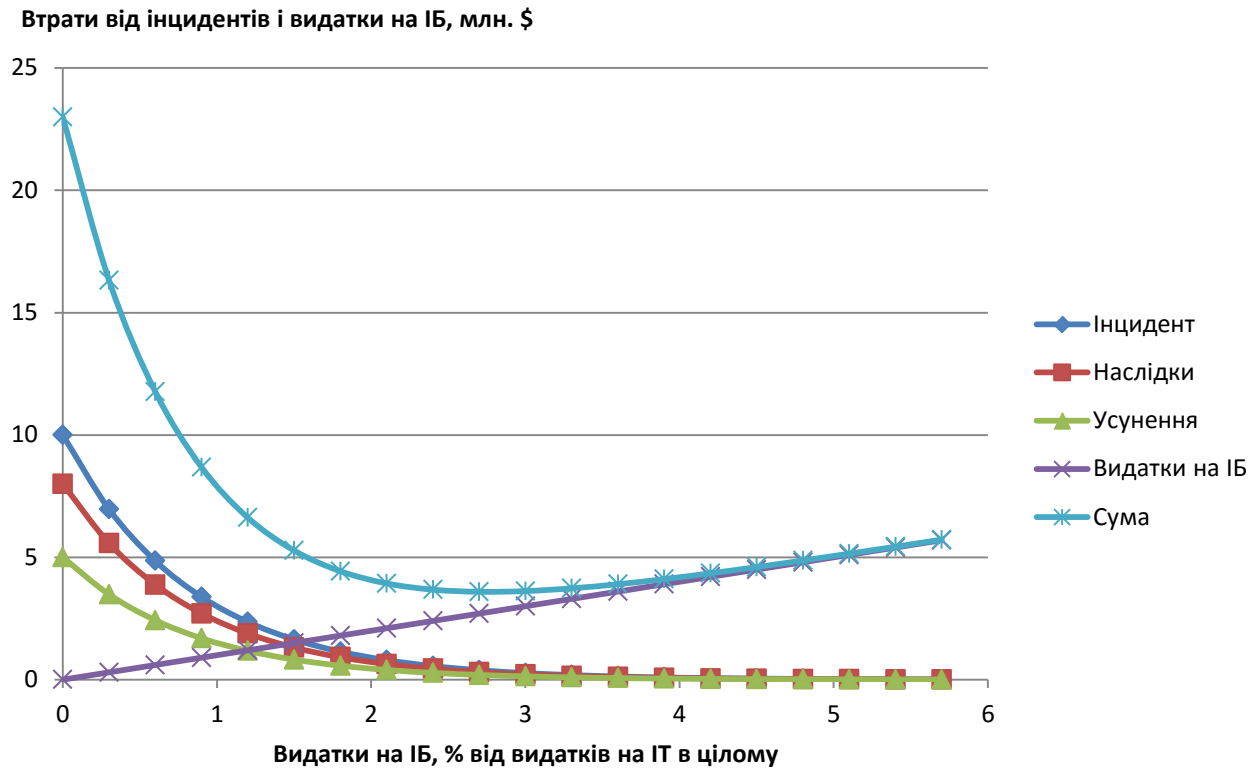


Рис.3. Втрати від інцидентів та видатки на інформаційну безпеку

З врахуванням існуючої глибини опрацьованості питання ІБ та величин ймовірних втрат в компаніях різного рівня можна визначити ефективність інвестицій в ІБ для компаній різного масштабу (рис.4). Найбільша ефективність спостерігається в малих компаніях. Причина в тому, що саме ці компанії на цей час практично не приділяють уваги питанням ІБ, оскільки вважають себе малоцікавою ціллю для зловмисників. З врахуванням помилковості останньої тези ефективність інвестицій стає ще більш високою.

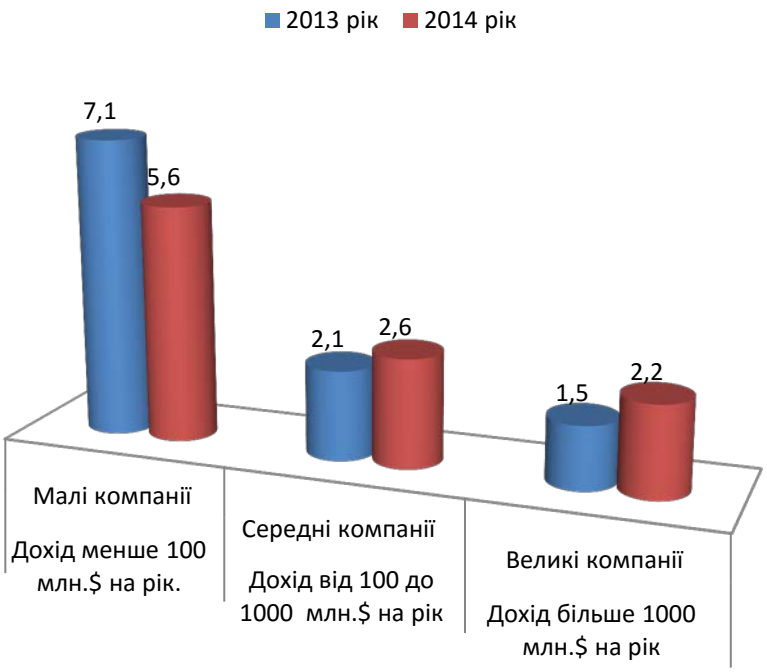


Рис.4. Сумарний дохід на 1 грн. інвестицій в інформаційну безпеку.

**Висновки**

1. Інформаційно небезпечних місць на планеті не залишилось.
2. Інформаційна безпека тепер питання не особисте, а галузеве, суспільне або державне.
3. Ефективність інвестицій в інформаційну безпеку в окремих випадках може перевищувати ефективність інвестицій в розвиток інформаційних та телекомунікаційних технологій. 1 грн. вкладена в інформаційну безпекупопереджує збитки в великих та середніх компаніях на суму від 1,5 до 2,6 грн, а в малих компаніях до 7,1 грн.

**Напрямки подальших досліджень**

Розвиток методів уточнення оптимальних рішень щодо обсягів та напрямків інвестування в інформаційну безпеку.

**Література**

1. CEOs Less Optimistic about Global Economy for 2015.DAVOS, SWITZERLAND – 26 January 2015 [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers - Режим доступу http://www.pwc.com/ua/ru/press-room/2015/18-ceo-survey.html.

2. Киберриски и процентные ставки наряду с изменениями в регулировании названы основными рисками для страховщиков. [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers.Результати опитування Banana Skins. 15.06.2015.- Режим доступу http://www.pwc.ru/ru/press-releases/2015/banana_skins_2015.html

3. Костюченко А. В Киеве прошел Форум Cisco по сетевой безопасности, технологиям для совместной работы и ЦОД. [електронний ресурс] // Сайт новин Vido.- Режим доступуhttp://vido.com.ua/article/13358/v-kiievie-proshiel-forum-cisco-po-sietievoi-biezopasnosti-tiekhnologhiiam-dlia-sovmiestnoi-raboty-i-tsod/

4. PwC представляет результаты глобального исследования по вопросам обеспечения информационной безопасности, перспективы на 2015 год. [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers - Режим доступу http://www.pwc.ru/ru/press-releases/2015/cyber-security-press-release.html

5. Управление киберрисками во взаимосвязанном мире. Основные результаты глобального исследования по вопросам обеспечения информационной безопасности. Перспективы на 2015 год. Январь 2015. [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers - Режим доступу http://www.pwc.ru/ru/riskassurance/publications/assets/ managing-cyberrisks.pdf

6. The Global State of Information Security® Survey 2016. Turnaround and transformation in cybersecurity [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers - Режим доступуhttps://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

7. Healthcare cybersecurity challenges in an interconnected world. Key finding from The Global State of Information Security. Survey 2015. [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers- Режим доступу http://www.pwc.ru/en/riskassurance/publications/ assets/healthcare.pdf

8. Britton T., Janson S., Martin-Lf A. Graphs with specified degree distribution, simple epidemics and local vaccination strategies. Adv. Appl. Prob. – 2007, 39. – 922-948.

9. van Doorn E.A. Quasi-stationary distribution and convergence to quasi-stationary of birth-death processes. Adv. Appl. Prob. – 1991, 23. – 683-700.

10. Kermack W.O., McKendrick A.G. A contribution to the mathematical theory of epidemics. Proc. Roy. Soc. Lond. A. – 1927, 115. – 700-721.

11. A guide to the project management body of knowledge: PMBOK guide. – 3rd ed. An American National Standard ANSI/PMI 99-001-2004- . – 2004. - 390 pp.

Надійшла 15.11.2015 р. Рецензент: д.т.н., проф. Толубко В.Б.