Захист інформації та кібернетична безпека

УДК 004.023 DOI: 10.30748/soi.2017.149.29

І.С. Добринін, Н.О. Мальцева

Харківський національний університет радіоелектроніки, Харків

ВДОСКОНАЛЕННЯ МЕТОДИКИ ФАКТОРНОГО АНАЛІЗУ ІНФОРМАЦІЙНИХ РИЗИКІВ

Питання розрахунку величини ризику компрометації інформації є актуальним через постійне зростання ціни інформації. Для ефективного керування бюджетом компанії, для побудови ефективної системи менеджменту інформаційної безпеки (СМІБ), необхідно мати чітку уяву про можливі ризики та збитки від них. Запропонована методика оцінки ризиків базується на методиці факторного аналізу інформаційних ризиків з імплементацією до міжнародного стандарту ISO/IEC 27001:2013 та дозволяє отримувати кількісну оцінку інформаційних ризиків.

Ключові слова: *інформаційна безпека, оцінка ризиків, загроза, вразливість, актив, кількісний аналіз.*

Вступ

Постановка проблеми у загальному вигляді. З кожним роком інформація стає дедалі важливішим активом підприємств різноманітного характеру діяльності. Це змушує керівників організацій частіше замислюватися над захистом критично важливої інформації свого підприємства, розголошення якої може призвести до значних збитків. Забезпечити належний захист можна, керуючись найбільш актуальними стандартами сьогодення. Так, міжнародною організацією International Organization for Standardization (ISO) розроблено ряд міжнародних стандартів, спрямованих на формування вимог забезпечення інформаційної безпеки. Найбільш вагому роль у цьому відіграє лінійка стандартів ISO/IEC 27000, зокрема ISO/IEC 27001:2013 [1]. Окрім цього, в Україні з липня 2012 року впроваджений Державний стандарт – ДСТУ 27001:2010, який надає підхід до створення, побудови, впровадження, експлуатації, моніторингу та вдосконалення СМІБ.

Аналіз стандартів у сфері інформаційної безпеки свідчить про те, що створення ефективної СМІБ неможливе без ідентифікації та оцінки ризиків. Проте, в стандартах чітко не вказано, яким шляхом необхідно виконувати вказані процедури. Тобто, як Державний, так і міжнародні стандарти лінійки 27000 не дають конкретної відповіді на те, яку саме методику слід використовувати. Як правило, ця задача покладається на керівників підприємств, або осіб, відповідальних за впровадження та підтримку СМІБ.

Таким чином, задача щодо вибору (розробки) методики оцінки інформаційних ризиків, при її простоті та наочності, достовірності отриманих за допомогою неї результатів є вкрай важливою не тільки науковою, але й практичною задачею.

Аналіз досліджень і публікацій. На сьогоднішній день існує широка різноманітність методик для оцінки інформаційних ризиків. Так, основні підходи до управління ризиками інформаційних технологій будуються на основі вимог Стандарту управління та аудиту інформаційних технологій Cobit v.5.0; Керівництва з управління ризиками в інформаційних технологіях NIST 800-30; сімейства стандартів ISO/IEC 27000 та ISO/IEC 31000 і т.д. Безпосередньо для оцінки ризиків, як правило, використовують наступні: метод оцінки операційно-критичних загроз, активів та вразливостей (Operationally critical threats, assets and vulnerability evaluation – OCTAVE); методологія оцінки ризиків Національного Інституту Стандартів і Технологій США (National Institute of Standardsand Technology – NIST); метод аналізу та контролю ризиків (CCTA Risk Analysis and Management Method – CRAMM) та ін. Останнім часом все більша увага приділяється методиці факторного аналізу інформаційних ризиків (FAIR), яка передбачає найбільш повне врахування факторів виникнення інформаційних ризиків [2]. Проведений авторами аналіз відомих методик показав, що кожна з методик має як переваги, так і певні недоліки. З точки зору менеджменту компаній, можна казати, що основними недоліками розглянутих методик є надання якісної (але не кількісної) оцінки,

яка не дає конкретного значення ризику, яким би могли оперувати керівники організацій (надаються лише наближені значення, діапазон яких є досить варійованим та зазначається у відповідних використовуваних шкалах) та врахування, як правило, недостатньої кількості факторів, що впливають на оцінку ризику.

Мета статті: розробка методики кількісної оцінки інформаційних ризиків на основі методики факторного аналізу інформаційних ризиків.

Викладення основного матеріалу

Розглянемо основні підходи методики FAIR. Зазначена методика базується на аналізі факторів, що впливають на різні складові ризику. Згідно з даною методикою, в першу чергу, ризик залежить від частоти появи інциденту і ймовірних втрат від його настання. Далі кожен з цих факторів поділяється [2]. В цілому, методика розбита на чотири етапи: ідентифікація об'єктів оцінки, оцінка частоти виникнення загроз, оцінка величини ймовірності потенційного збитку, отримання та формалізація ризику. Графічна інтерпретація оцінки ризиків за методикою FAIR наведена на рис. 1 [2].

На першому етапі (етапі ідентифікації об'єктів оцінки), оцінюються активи і загрози, які можуть бути застосовані до конкретної інформаційної системи.

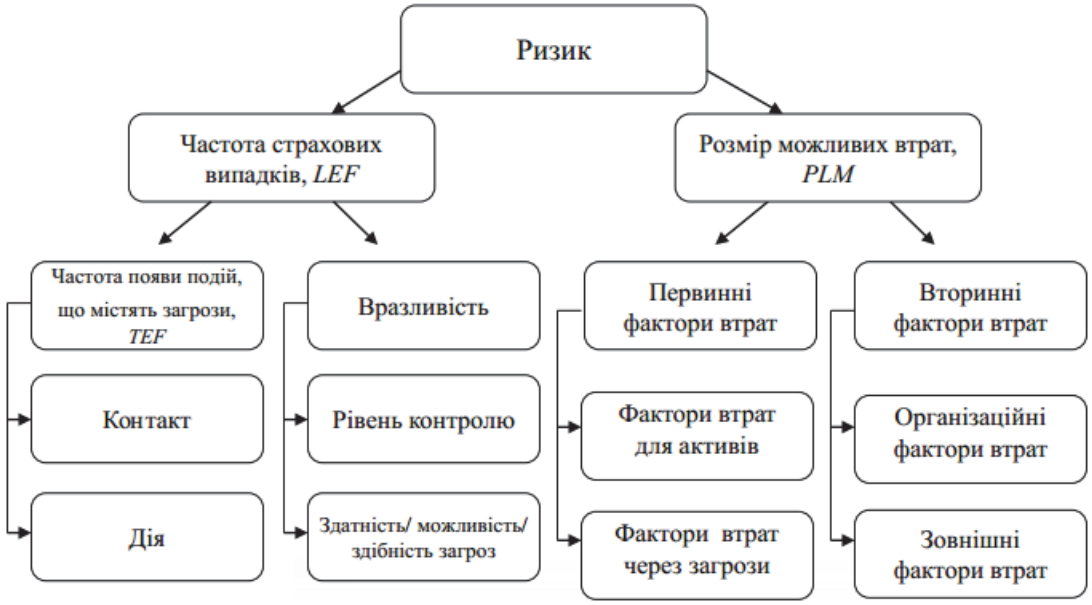

Рис. 1. Графічна інтерпретація методики FAIR

Починаючи з другого етапу (етапу оцінки частоти виникнення загроз – TEF) методика пропонує використовувати матричний підхід. При цьому, частота виникнення виражається як дуже висока, висока, середня, низька або дуже низька. Значення, які відповідають даним позначенням, визначаються компаніями самостійно [2].

Що стосується розрахунку величини втрат, то методика також пропонує використовувати шкалу переведення кількісних значень у якісні. Методика FAIR передбачає наступні етапи проведення оцінки втрат:

– оцінити найгірший варіант;

– оцінити ймовірну величину втрат.

Для оцінки найгіршого варіанту необхідно виконати наступні пункти [2]:

– визначити дію загрози, яка напевно буде результатом найгіршого випадку;

– оцінити величину кожного виду втрат, пов’язаних з дією загрози;

– підсумувати величини всіх видів втрат.

В результаті, розрахунок величини ризику зводиться до матриці, де шукана величина буде знаходитися на перетині значення частоти подій, що призводять до втрат, і максимального значення втрат обраної дії загрози.

Таким чином, методика FAIR представляє собою детальний та чіткий процес оцінки ризиків, але результат, який отримується, не є достатньо зручним у використанні, оскільки діапазон значень ризику може бути достатньо великим (значення ризику може відрізнятися на порядок), в той час як організації потребують конкретних значень ризику, тобто їх кількісної характеристики.

Здійснимо перехід від якісної оцінки інформаційних ризиків (за методикою FAIR) до кількісної оцінки. При цьому, будемо враховувати вимоги міжнародного стандарту ISO/IEC 27001:2013, як найбільш актуального на сьогоднішній день у сфері інформаційної безпеки.

Цей перехід передбачає:

1. Вибір активу, у відношенні якого буде проводитися оцінка ризику.

Зазначимо, що у якості активу може бути обрано будь який актив у відношенні якого здійснюється оцінка ризику, але для прикладу, у роботі, у якості активу авторами було розглянуто файл, який містить конфіденційну інформацію (інформацію обмеженого доступу – ОД) та розташовується на комп'ютері.

2. Враховуючи те, що у відповідності зі стандартом ISO/IEC 27001:2013 порушенням інформаційної безпеки (ІБ) є порушення конфіденційності (К), цілісності (Ц) та доступності (Д) інформації, на цьому етапі визначаються:

– можливі події, що призводять до порушення К, Ц, Д. Відзначимо, що визначення цих подій повинно проводитися окремо для кожної з властивостей ІБ, тобто окремо для К, Ц, Д;

– визначається, за рахунок чого може статися ця подія;

– визначаються причини, що можуть привести до виникнення цих подій.

Результати другого етапу, з метою формування та визначення причинно-наслідкових зв'язків, доцільно розміщувати у відповідних таблицях або у вигляді діаграм Ісікави для кожної з властивостей ІБ: К, Ц, Д. Варіант табличного представлення надано у табл. 1.

Таблиця 1

Деякі події, що можуть призвести до порушення конфіденційності інформації (актив – файл, розташований на локальному хості)

Можлива подія та її ймовірність $P(A1_i)$	За рахунок чого може статися подія (гіпотеза) та її ймовірність, $P(H1_{ij})$	Причини, що призводять до виникнення гіпотез та відповідний пункт стандарту ISO/IEC 27001:2013	Умовна ймовірність виникнення події, $P(A1_i\|H1_{ij})$
Порушення конфіденційності інформації за рахунок недосконалості засобів фізичного захисту $P(A1_1)$	Подолання зловмисником периметру зони безпеки підприємства $P(H1_{11})$	Недостатня ефективність заходів, спрямованих на забезпечення фізичного захисту периметра, будівлі, вікон та дверей, (А.11.1)	Порушення конфіденційності інформації при подоланні зловмисником периметру зони безпеки підприємства $P(A1_1\|H1_{11})$
	Невиконання особами підприємства політики «чистого столу» $P(H1_{12})$	Недотримання співробітниками політик чистого робочого столу та екрана, недбале ставлення до збереження документів із обмеженим доступом, (А.11.2.9)	Порушення конфіденційності інформації при невиконанні особами підприємства політики «чистого столу» $P(A1_1\|H1_{12})$
Порушення конфіденційності інформації за рахунок недостатньо ефективного управління доступом $P(A1_2)$	Отримання зловмисником доступу до інформації з ОД через некоректно налаштовані права доступу на хості $P(H1_{21})$	Недостатньо ефективна політика розмежування доступу на локальному хості, (А.9.2, А.9.4)	Порушення конфіденційності інформації при отриманні зловмисником доступу до інформації з ОД через некоректно налаштовані права доступу на хості $P(A1_2\|H1_{21})$
	Реалізація злому пароля $P(H1_{22})$	Недостатньо ефективна система управління паролями (легко вгадуванні паролі, недостатньо часта заміна), (А.9.4.3)	Порушення конфіденційності інформації при зломі парольного захисту $P(A1_2\|H1_{22})$
	Знімання інформації з ОД зі знімних носіїв $P(H1_{23})$	Недостатня ефективність заходів, спрямованих на забезпечення безпечної роботи зі знімними носіями, (А.8.3)	Порушення конфіденційності інформації при зніманні інформації з обмеженим доступом зі знімних носіїв $P(A1_2\|H1_{23})$
	Підкуп зловмисником співробітників $P(H1_{24})$	Підкуп співробітників, (А.7)	Порушення конфіденційності інформації при підкупі співробітників організації $P(A1_2\|H1_{24})$

Слід зазначити, що при формуванні відповідних таблиць варто враховувати як елементи методики FAIR (див. рис. 1), так і вимоги стандарту ISO/IEC 27001:2013 [1], тобто:

– можлива подія та її ймовірність = контакт;

– умовна ймовірність виникнення події = дія;

– причини, що призводять до виникнення гіпотез та відповідний пункт стандарту ISO/IEC 27001:2013 = рівень контролю;

– за рахунок чого може статися подія (гіпотеза) та її ймовірність = можливості загрози.

Поруч із причинами, що призводять до виникнення гіпотез, доцільно мати посилання на відповідні пункти стандарту ISO/IEC 27001:2013 [1]. Це ті елементи і механізми, які повинні бути впроваджені в організації для ефективного забезпечення безпеки інформації.

1. Наступний етап передбачає визначення ймовірностей реалізації гіпотез та умовних ймовірностей виникнення подій (стовбці 2 та 4 табл. 1 відповідно). Зазначені ймовірності отримуються на підставі апріорі відомих статистичних даних аналітичних компаній, які є фаховими у цій області та відповідних рішень експертів компанії. Таким чином, дані, наведені в таблицях, дозволяють розраховувати ймовірність реалізації загроз через конкретні вразливості.

2. Розглянемо події, які можуть призвести до порушення конфіденційності, цілісності або доступності інформації. Очевидно, що вони є незалежними, тобто поява однієї з цих подій не впливає на появу іншої. У представленій таблиці це події, зазначені в стовпці «Можлива подія та її ймовірність». Реалізація будь-якої із зазначених подій (факторів) призводить до втрати конфіденційності, цілісності або доступності інформації з імовірністю P. Виходячи з теореми, що ймовірність появи хоча б однієї з подій, незалежних в сукупності, дорівнює різниці між одиницею і добутком ймовірностей протилежних подій [3], отримаємо вираз:

$$P = 1 - \prod_{i=1}^{n} (1 - P(A_i)),$$

де n – кількість подій, що можуть призвести до порушення конфіденційності, цілісності чи доступності;

i – поточний номер події;

$P(A_i)$ – ймовірність реалізації події.

Доцільно врахувати той факт, що реалізація подій A_i, в свою чергу, також залежить від ряду факторів (або гіпотез). Позначимо їхні ймовірності реалізації через $P(H_{ij})$. Вони також є незалежними один від одного в межах однієї події.

Позначимо через $P(A_i|H_{ij})$ умовну ймовірність появи події A_i за умови j-ї гіпотези. Тоді, базуючись на формулі повної ймовірності та формулі додавання ймовірностей [3], отримаємо вираз:

$$P(A_i) = \sum_{i=1}^{n} \sum_{j=1}^{m} P(H_{ij}) \cdot P(A_i \mid H_{ij}),$$

де i – поточний номер події;

j – поточний номер гіпотези;

n – кількість відповідних подій;

m – кількість гіпотез.

Таким чином, застосування вище приведених формул надасть значення ймовірностей реалізацій порушення конфіденційності, цілісності та доступності окремо.

3. Очікуване значення величини втрат може бути розраховано за формулою:

$$R = \sum_{i=1}^{n} P_i \cdot E_i,$$

де Pi – ймовірність порушення КЦД;

Ei – розмір збитків від настання цих подій.

В рамках дослідження авторами було проведено порівняльний аналіз стандартної методики оцінки ризиків FAIR та розробленого підходу з використанням статистичних даних, наданих провідними компаніями з оцінки загроз інформаційної безпеки.

В ролі активу розглядався файл з конфіденційною інформацією. Діями, що можуть нашкодити компанії, розглядалися дії зловмисника, що спрямовані на порушення конфіденційності, цілісності та доступності інформації, що зберігається в цьому файлі. Згідно з методикою FAIR, ризик – це добуток ймовірної частоти страхових випадків та ймовірної величини можливих втрат.

Як було зазначено вище, ризик за активом являє собою суму добутків величин ймовірностей порушення конфіденційності, цілісності та доступності інформації на величину ймовірного збитку від настання даних подій. Як приклад, було розраховано величину ризику, якого може зазнати компанія в разі порушення конфіденційності інформації.

Величина ризику, отримана за допомогою запропонованого методу, потрапила до діапазону вірогідної величини втрат, що визначається за стандартним підходом. Але, на відміну від якісної оцінки методики FAIR, отримана величина ризику є кількісною, що дозволяє більш ефективно прогнозувати витрати на інформаційну безпеку.

Слід відзначити, що при розрахунках за розробленою методикою потрібно відповідально підійти до процесу ідентифікації загроз та причин їх виникнення (див. табл. 1), та враховувати статистичні дані компанії та аналітичних агентств. За необхідністю, скористатися послугами експертів.

Висновки

Запропонований підхід до оцінки інформаційних ризиків базується на концепції методики FAIR з урахуванням вимог міжнародного стандарту ISO/IEC 27001:2013, як найбільш актуального на сьогоднішній день в сфері інформаційної безпеки та дозволяє кількісно уточнити оцінку ризиків, що може бути отримана за допомогою якісної методики FAIR. Розробка методики проводилася з використанням математичного апарату теорії ймовірностей, а саме Байєсовських мереж.

Результати роботи доцільно використовувати для кількісної оцінки інформаційних ризиків в різноманітних компаніях та організаціях, які створюють або експлуатують СМІБ.

Подальшим розвитком роботи мають бути дослідження, спрямовані на підвищення рівня експертної інформації, що використовується на етапі визначення ймовірностей реалізації гіпотез та умовних ймовірностей виникнення подій.

Список літератури

1. Міжнародний стандарт ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.

2. Методика факторного аналізу інформаційних ризиків An Introduction to Factor Analysis of Information Risk (FAIR) [Електронний ресурс]. – Режим доступу: http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf.

3. Корн Г.А. Справочник по математике для научных работников и инженеров / Г.А. Корн, Т.М. Корн. – М.: «Наука», 1974. – 832 с.

4. Мальцева Н.А. Выбор математического метода для обоснования варианта построения системы менеджмента информационной безопасности в соответствии с требованиями стандарта ISO/IEC 27001:2013 [Текст] / Н.А. Мальцева – Материалы 18-го международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». – Х.: ХНУРЭ, 2014, - с. 128-129

5. Астахов А.М. Искусство управления информационными рисками / А.М. Астахов. – М.: ДМК Пресс, 2010. – 314 с.

6. Сучасні підходи до оцінки ризиків інформаційних технологій. [Електронний ресурс]. – Режим доступу: http://www.auditagency.com.ua.

7. Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

Надійшла до редколегії 18.01.2017

Рецензент: д-р техн. наук проф. Є.В. Дуравкін, Харківський національний університет радіоелектроніки, Харків.

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ФАКТОРНОГО АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ

И.С. Добрынин, Н.А.Мальцева

Вопрос расчета величины риска компрометации информации является актуальным из-за постоянного роста цены информации. Для эффективного управления бюджетом компании, для построения системы менеджмента информационной безопасности (СМИБ) необходимо иметь четкое представление про возможные риски и убытки от них. Предложенная методика оценки рисков базируется на методике факторного анализа информационных рисков с имплементацией к международному стандарту ISO/IEC 27001:2013.

Ключевые слова: *информационная безопасность, оценка рисков, актив, количественный анализ.*

IMPROVEMENT OF THE METHOD OF FACTOR ANALYSIS INFORMATION RISK

I. Dobrynin, N. Maltseva

The question of calculating the value of the compromising information risk is relevant because of the constant growth of prices of information. In order to efficiently operate the company's budget for the construction of an information security management system (ISMS), you must have a clear idea about the possible risks and losses from them. The proposed risk assessment method is based on the method of factor analysis of information risks, and with the implementation of international standard ISO/IEC 27001:2013.

Keywords: *information security, risk assessment, asset, quantitative analysis.*