УДК 004.413.4

О.А. Замула[1], В.І. Черниш[1], К.І. Іванов[1], О.І. Аніщенко[2]

[1] *Харківський національний університет радіоелектроніки, Харків*
[2] *Центральне казенне конструкторське бюро «Протон», Харків*

НЕОБХІДНІСТЬ МОДЕЛІ СТРУКТУРУВАННЯ ПРИ ОЦІНЮВАННІ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянуто метод виконання аналітичних робіт з структурування оцінки ризиків ІБ. Запропоновано 7 складових етапів наведеного методу.

Ключові слова: *інформаційна безпека, інформаційний ризик, оцінка ризиків*

Вступ та мета роботи

Загальне впровадження інформаційних технологій (ІТ) в структури сучасних організацій стало об'єктивною реальністю. На усіх управлінських рівнях є необхідність та можливість розширити комунікаційні та інформаційні можливості за рахунок впровадження сучасних ІТ. В результаті інформаційні структури організацій розгортаються: локальні мережі організацій підключаються до мереж Internet; мережі об'єднуються в офісні багаторівневі структури та розгортаються до рівня розподілених корпоративних мереж. Впровадження ІТ призводить до можливості порушення режимів інформаційної безпеки (ІБ) [1, 2].

Інформаційна безпека (ІБ) в даний час стає необхідною умовою успішного розвитку господарюючого суб'єкта (ГС). Ризик компрометації інформації впливає на матеріальні і нематеріальні активи організації і, в кінцевому рахунку, на результати її виробничо-економічної діяльності. У зв'язку з великим числом інформаційних ризиків (ІР), широким різноманіттям значень збитку при їх реалізації та обмеженістю бюджету на ІБ ГС виникає необхідність раціонального фінансування витрат на захист інформації [3].

Цілями роботи є визначення методу структурованої оцінки ризиків стану ІБ в ІС на підприємствах і в організаціях. Запропонований метод є необхідним для підвищення достовірності оцінки захищеності інформації та скорочення витрат зі створення системи захисту.

Викладення основного матеріалу

Під час проведення аналізу ризику виявляються найбільш критичні с точки зору ІБ ресурси, по кожному ресурсу визначаються характерні загрози безпеки та оцінюється вразливість системи захисту ресурсу. На основних етапах визначаються ймовірносні характеристики виникнення та реалізації загроз ІБ.

Метою процесу оцінювання ризиків є визначення характеристик ризиків в інформаційній системі та її ресурсах. На основі цього визначаються необхідні засоби управління ІБ [4, 5].

В статті надається опис методу виконання аналітичних робіт з структурування оцінки ризиків ІБ.

Метод включає в себе 7 етапів, які наведені на рис. 1.

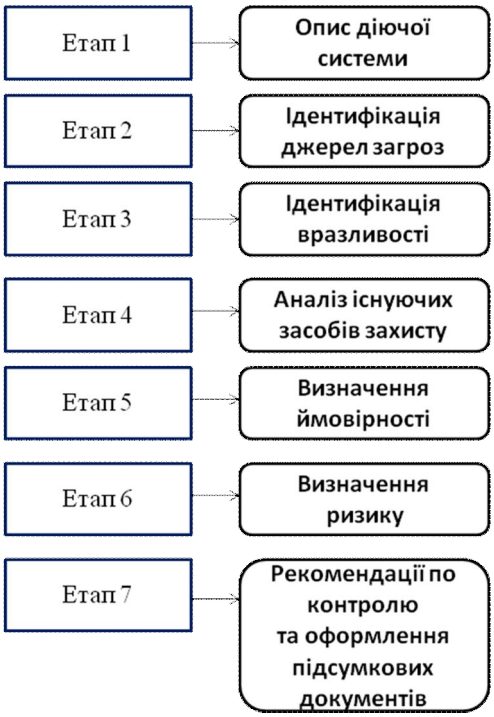

Рис. 1. Структурування оцінки ризиків ІБ

Етап 1: Опис діючої системи

На етапі опису системи проводиться збирання звітностей для опису системи та визначення границь системи на різних ієрархічних рівнях з метою виявлення вразливостей та оцінки достатньої прийнятих мір захисту.

Етап 2: Ідентифікація джерел загроз

Метою етапу ідентифікації є визначення потенційних джерел загроз для ІС, що оцінюється та складання списку актуальних джерел загроз для даної ІС.

Етап 3: Ідентифікація вразливості

Мета ідентифікації – це утворення списку вразливостей (недоліків та упущень), якими можуть скористатися потенціальні джерела загроз.

Етап 4: Аналіз існуючих засобів захисту

Мета даного етапу є аналіз засобів контролю, що вже введені компанією, або заплановані для введення для зменшення або усунення ймовірності використання вразливості системи для дії джерела загроз [5, 6].

Етап 5: Визначення ймовірності

Етап визначення ймовірності є необхідним для підрахування рівня ймовірності успішної атаки – це залежить від потенціалу загрози, що створюється активним джерелом загрози.

Побудуємо таблицю показників ваги ймовірності успішної атаки (табл. 1).

Розподіл числових значень показника рівня ймовірності описані в табл. 2.

Таблиця 1

Показники ваги ймовірності успішної атаки

Ефективність захисту Z(i,j)	Потенціал загрози U(i,j)				
	1	2	3	4	5
0 (захист відсутній)	1	2	3	4	5
1	0	1	2	3	4
2	0	0	1	2	3
3	0	0	0	1	2
4	0	0	0	0	1
5	0	0	0	0	0

Таблиця 2

Шкала значень рівня ймовірності реалізації загрози

Рівень ймовірності		Опис рівня
1	Дуже низький	Засоби захисту та методи їхнього використання гарантують захист по відношенню к даному типу загроз в межах заданої вразливості (використовуються сертифіковані профілі захисту).
2	Низький	У джерела загрози недостатньо мотивації або можливостей, або діючі засоби контролю здатні запобігти або значно завадити використанню вразливостей.
3	Середній	Джерело загрози мотивований та має можливості, але існуючі засоби контролю можуть заважати успішному використанню вразливості.
4	Високий	Джерело загрози мають високі мотивації та достатні можливості, а методи контролю для подолання прояву вразливості не гарантують захист.
5	Дуже високий	Рівень мотивації, технічні та організаційні можливості джерела загроз перевищують відповідні параметри захисту.

Етап 6: Визначення ризику

Метою даного етапу є визначення максимального рівня ризику ІБ при успішній реалізації атаки від і-го джерела по j-й вразливості.

Простий спосіб отримання оцінок ризику для кожної пари загроза/вразливість, на яких можна заснувати механізм оцінки ризиків ІБ заключається в перемноженні ймовірності реалізації загрози на збиток від реалізації загрози з наступним ранжируванням отриманих значень.

В таблиці приведені дії та процедури, що необхідно прийняти в цих випадках.

Результати виконання перемноження та наступного ранжирування отриманих значень для розглянутих вище шкал рівня ймовірності реалізації загрози та збитку від реалізації загрози висвітлюються в табл. 3 (числа – результат перемноження P(i,j) та S(i,j), а буквені індекси відображають результат ранжирування.

В шкалі для оцінювання ризиків ІБ застосовані наступні рівні (табл. 3):

- Н – низький (відповідають значенням від 1 до 3);
- С – середній (від 4 до 6);
- В – високий (від 8 до 12);
- К – критичний (від 15 до 20);
- Д – дуже високий (відповідає значенню 25).

Табл. 4 включає в себе опис рівня ризиків. За допомогою цих рівнів оцінюється ступінь ризиків, наявних у ІТ–системі (окремий елемент або процедура) у випадку, якщо проявиться окрема вразливість.

Таблиця 3

Шкала ранжирування оцінки ризиків

Збиток від реалізації загрози S(i,j)	Рівень ймовірності реалізації загрози P(i,j)				
	1 (Н)	2 (Н)	3 (С)	4 (С)	5 (В)
1	1 (Н)	2 (Н)	3 (Н)	4 (С)	5 (С)
2	2 (Н)	4 (Н)	6 (С)	8 (В)	10 (В)
3	3 (Н)	6 (С)	9 (В)	12 (В)	15 (К)
4	4 (С)	8 (В)	12 (В)	16 (К)	20 (К)
5	5 (С)	10 (В)	15 (К)	20 (К)	25 (Д)

Таблиця 4

Шкала ризику

Рівень ризику	Опис ризиків та необхідні дії
Низький (Н)	Якщо зведення розцінюються як ризик, необхідно визначити, чи існує необхідність в коректуючих діях або є можливість прийняти ризик.
Середній (С)	Якщо зведення розцінюються як середній ризик, необхідно розробити та застосувати план коректуючих дій на протязі прийнятного періоду часу.
Високий (В)	Якщо отримані зведення розцінюються як високий ризик, то виникає необхідність в коректуючих діях. Система може продовжувати роботу, але коректований план дій необхідно застосувати як можна швидше.
Критичний (К)	Система знаходиться в критичному положенні. Рівень ризику має критичне значення для основних бізнес-процесів. Необхідно миттєво прийняти міри по зменшенню ризику.
Дуже високий (Д)	Рівень ризику має дуже високий рівень, який є недопустимим для організації. Необхідно зупинити використання ІТ-системи та прийняти радикальні міри по зменшенню ризику.

В механізмі нечіткого виводу такий спосіб отримання ризику може бути представлений за допомогою наступних правил.

Вхідні дані:

- P(i,j) – ймовірність успішної реалізації атаки від (і-го) джерела загроз по (j-ій) вразливості (шкала загроз має п'ять рівнів).
- S(i,j) – величина збитку від успішної атаки від (і-го) джерела загроз по (j-й) вразливості.

Вихідні дані:

- R(i,j) – величина ризику від атаки від (і-го) джерела загроз по (j-й) вразливості.

Правила вивода:

Якщо $\mu[P(i,j)] * \mu[S(i,j)] =< 3$ ТО $R(i,j) = Н$;

Якщо $3 < \mu[P(i,j)] * \mu[S(i,j)] =< 6$ ТО $R(i,j) = С$;

Якщо $8 < \mu[P(i,j)] * \mu[S(i,j)] =< 12$ ТО $R(i,j) = В$;

Якщо $15 < \mu[P(i,j)] * \mu[S(i,j)] =< 20$ ТО $R(i,j) = К$;

Якщо $\mu[P(i,j)] * \mu[S(i,j)] = 25$ ТО $R(i,j) = Д$.

В ці правила достатньо просто можна ввести умови та інші підставні, котрі необхідно врахувати при визначені величини ризику.

Етап 7. Рекомендації по контролю та оформлення підсумкових документів

Даний етап забезпечує засоби контролю, що можуть понизити або усунути ідентифіковані ризики, та які є доцільними для даної компанії. Метою методів контролю є зниження рівня ризиків для ІТ-системи та її даних до прийнятного рівня. Після завершення оцінки ризиків слід представити документацію у вигляді офіціального звіту або коротких інструкцій [7].

У табл. 5 ми наведено загальну методологію структурування оцінки ризиків ІБ.

Висновки

У запропонованій моделі структурування визначається операції, щодо отримання якісних і кількісних оцінок величин ризику з максимальними можливостями обліку апріорних даних і результатів попередніх досліджень характеристик і властивостей ІБ. Отримані оцінки ризику можуть бути використані при розробці концепції забезпечення ІБ на етапі формування ІС і для підтримки рівня ризику на прийнятному рівні на етапі експлуатації ІС.

Список літератури

1. Черныш В.И. Методы оценивания информационных рисков компании / В.И.Черныш // Материалы XV Международного юбилейного молодёжного форума «Радиоэлектроника и молодежь в XXI веке»: сб. тез., 18–20 апреля 2011 р., т.5. – Х.: ХНУРЭ. 2011. – С. 195.

2. *Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки ін формації. – Х.: ХУ ПС, 2011. – Вип. 2(92). – С. 53-56.*

Таблиця 5

Загальна схема методології структурованої оцінки ризиків

Вихідні дані	Дії з оцінки ризику	Результати
1. Комп'ютерне обладнання та програмне забезпечення. 2. Системні інтерфейси. 3. Дані та інформація. 4. Люди.	Етап 1: Опис діючої системи	1. Межі системи. 2. Функції системи. 3. Критичність системи і даних. 4. Чутливість системи і даних.
1. Історія атак на систему.	Етап 2: Ідентифікація джерел загроз	1. Формулювання загроз.
1. Звіти за попередніми оцінками ризиків. 2. Повідомлення про різні аудити. 3. Вимоги до безпеки. 4. Результати тестування безпеки.	Етап 3: Ідентифікація вразливості	Перелік потенційних точок уразливості.
1. Поточний стан контролю. 2. Плановані заходи з контролю.	Етап 4: Аналіз існуючих засобів захисту	1. Перелік поточних і планованих заходів з проведення контролю.
1. Мотивація джерел загроз. 2. Можливості загроз. 3. Природа вразливості. 4. Поточний стан контролю.	Етап 5: Визначення ймовірності	1. Рейтинги можливості здійснення загроз.
1. Вірогідність загрози для експлуатації. 2. Розміри впливу. 3. Адекватність плануються або поточних заходів з контролю.	Етап 6: Визначення ризику	1. Ризики та рівні допустимих ризиків.
	Етап 7: Рекомендації по контролю та оформлення підсумкових документів	1. Рекомендовані заходи з контролю. 2. Звіт з оцінки ризиків.

3. Замула А.А. Оценивание рисков информационной безопасности в современных информационных системах / А.А. Замула, В.И. Черныш, К.И. Иванов // XIV Международная научно-практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», тезисы докладов. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2011. – С. 31.

4. Замула А.А. Математические методы оценивания информационных рисков компании / А.А. Замула, В.И. Черныш, Ю.В. Землянко // Прикладна радіоелектроніка: наук. – 2011. – Т. 9. № 1. – С. 123-127.

5. Сидоров А.О. Разработка методики структурированной оценки риска / А.О. Сидоров, Ю.А. Торшенко, А.А. Павлютенков, Л.Г. Осовецкий // Научно-технический вестник СПбГУ ИТМО. – № 55. Системы: управление, моделирование, безопасность. – С.-Пб, 2008.– С. 108-110.

6. Шубин Ю.М. Метод формирования профиля защиты автоматизированной банковской системы / Ю.М. Шубин, А.О. Сидоров // Научно-технический вестник СПбГУ ИТМО. – № 55. Системы: управление, моделирование, безопасность. – С.-Пб, 2008.– С. 113-116.

7. Петренко С.А. Экономически оправдання безопасность / С.А. Петренко, С.В. Симонов // IT Manager. – М., 2004. – № 15. – С. 35-41.

Надійшла до редколегії 4.10.2011

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Полтавський національний технічний університет, Харків.

НЕОБХОДИМОСТЬ МОДЕЛИ СТРУКТУРИРОВАНИЯ ПРИ ОЦЕНКЕ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.И. Замула, В.И. Черныш, К.И. Иванов, А.И. Анищенко

Рассмотрен метод выполнения аналитических работ по структурированию оценки рисков ИБ. Предложено 7 составляющих этапов приведенного метода.

***Ключевые слова**: информационная безопасность, информационный риск, оценка рисков.*

NEED OF MODELS FOR STRUCTURING RISK ASSESSMENT INFORMATION SECURITY

A.I. Zamula, V.I. Chernysh, K.I. Ivanov, A.I. Anishenko

The method of analytical work in structuring risk of IS. A seven components described method steps.

***Keywords:** information security, information risk, risk assessment.*