УДК 004.942

к.т.н. Єрмошин В.В., д.т.н., проф. Хорошко В.О.,
к.т.н. Капустян М.В. (ДУІКТ)

МЕТОДИКА ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Вступ

Вітчизняних методик оцінки ризиків в якості документа групи НД ТЗІ на сьогодні не існує. Існує декілька методик, розроблених міжнародними організаціями та об'єднаннями фахівців в галузі інформаційної безпеки, а також окремі напрацювання вітчизняних фахівців в галузі інформаційної безпеки.

На основі аналізу наявного матеріалу в межах виконання науково-дослідної роботи "Розробка методики оцінки ризиків системи управління інформаційною безпекою" (Шифр "РИСКИ СУИБ") було розроблено методику оцінки ризиків системи інформаційної безпеки, яку можна застосовувати на практиці в різних сферах виробництва та бізнесу.

Мета роботи

Розробка методики оцінки ризиків системи управління інформаційною безпекою.

Основна частина

В результаті виконання науково-дослідної роботи "Розробка методики оцінки ризиків системи управління інформаційною безпекою" було запропоновано наступну етапність при оцінці оцінки ризиків системи управління інформаційною безпекою.

1. Аналіз інформаційної інфраструктури.
2. Визначення множини інформаційних загроз та вразливостей.
3. Комплексна оцінка інформаційних активів.
4. Розрахунки та звіт за результатами оцінки.

1. Аналіз інформаційної інфраструктури

Аналіз інформаційної інфраструктури (ІТ-системи), обов'язковий етап будь-якої з розглянутих методик оцінки, і чим глибший цей аналіз, тим об'єктивніший буде отриманий результат оцінки.

Під час аналізу інформаційної інфраструктури необхідно визначити призначення системи; функціональні вимоги до системи; дані та інформацію, яка циркулює в системі; критичність системи та даних; чутливість системи та даних; апаратні засоби системи; програмне забезпечення яке використовується в системі; поточна топологія мережі; системні інтерфейси; інформаційні потоки в системі; персонал підтримки та використання системи; політика системи безпеки; архітектура системи безпеки; захист інформаційного сховища, який гарантує доступність, цілісність і конфіденційність даних та системи; технічні засоби контролю для системи; управління контролем системи; операційний контроль системи; фізична безпека системи; забезпечення екологічної безпеки для середовища системи (наприклад, контроль вологості, електроенергії, забруднення навколишнього середовища, температури, хімічних речовин).

При визначенні призначення системи необхідно надати найменування системи, її власника, призначення системи, її функції та територіальне розміщення. При цьому необхідно вказати в рамках чого ця система була створена, використовуючи в якості додатку технічне/технічні завдання на систему.

В якості функціональних вимог до системи, необхідно надати їх перелік. При цьому обов'язково необхідно надати посилання на відповідний розділ технічного завдання та інших документів, які ці вимоги до системи висувають.

Під час аналізу системи необхідно загально описати дані та інформацію яка циркулює в ній. При цьому необхідно вказати вимоги яких документів регламентують правила поводження з нею, гриф обмеження інформації.

Під час аналізу системи необхідно визначити апаратні засоби системи та програмне забезпечення, яке на них використовується – ресурси системи. При цьому метою повинна бути програмно-апаратна типізація ресурсів системи, що значно спростить її подальшу оцінку.

Під час аналізу необхідно визначити поточну топологію мережі, її системні інтерфейси, промалювати інформаційні потоки в системі. В загальному випадку в результаті проведеного аналізу експерт, який проводить оцінку, повинен отримати функціональну схему системи.

Під час аналізу необхідно визначити категорії персоналу підтримки та користувачів системи, їхні права та механізми щодо доступу до системи і інформації.

Під час аналізу необхідно проаналізувати Політику системи безпеки на відповідність категоріям персоналу та правам його доступу до інформації, а також провести аналіз достатності архітектури системи безпеки виконувати вимоги політики щодо доступності, цілісності і конфіденційності даних та самої системи.

Також необхідно визначити наявність технічних засобів контролю для системи, впроваджені принципи і механізми управління та операційного контролю, механізми та засоби забезпечення фізичної безпека системи, забезпечення екологічної безпеки для середовища системи (наприклад, контроль вологості, електроенергії, забруднення навколишнього середовища, температури, хімічних речовин).

Під час аналізу необхідно вести оцінку процесів та ступень їх формалізації. У випадку коли процес, який підлягає аналізу, відсутній, виставляється оцінка 1, у випадку коли процес, який підлягає аналізу, присутній, але не формалізований, виставляється оцінка 0,5, коли процес, який підлягає аналізу, присутній та формалізований, виставляється оцінка 0,15.

Після цього необхідно надати загальну оцінку системи, яка розраховується за формулою:

$$M_З = \frac{\sum ПР}{N_{ПР}},$$

де: $M_З$ - загальна оцінка системи;

$\sum ПР$ – сума отриманих оцінок;

$N_{ПР}$ - загальна кількість процесів.

Крім цього необхідно оцінити критичність і чутливість ресурсів системи (її елементів) та даних.

Оцінка проводиться для кожного визначеного класу/типу ресурсу системи.

Схематично процес оцінки проілюстрований на рисунку 2.1.

Процес визначення рівня доступності, цілісності та конфіденційності ідентифікованих ресурсів системи, а також процес визначення їхньої важливості супроводжується визначенням їхніх вагових коефіцієнтів.

В якості шкали оцінювання до використання пропонується:

- при визначенні рівня доступності необхідно використовувати шкалу, в якості одиниці вимірювання якої використовується час, який дорівнює найменшому проміжку, протягом якого система може бути недоступною. При цьому загальна кількість поділок шкали повинна дорівнювати частці найбільшого проміжку часу, який система може буди недоступною та найменшого проміжку часу, який система може буди недоступною. Максимальне значення шкали, яке дорівнюється значенню найбільшого проміжку часу, який система може буди недоступною, приймається за 1;
- при визначенні рівня цілісності необхідно використовувати наступну шкалу: порушення цілісності припиняє працездатність системи; порушення цілісності блокує працездатність системи; порушення цілісності уповільнює працездатність системи; порушення цілісності не впливає на працездатність системи. При цьому максимальне значення шкали приймається за 1;

• при визначенні рівня важливості ресурсу необхідно використовувати наступну шкалу: втрата ресурсу припиняє працездатність системи, втрата ресурсу блокує працездатність системи; втрата ресурсу уповільнює працездатність системи, втрата ресурсу не впливає на працездатність системи. При цьому максимальне значення шкали приймається за 1.

Чим більший ваговий коефіцієнт, тим більшим є негативний вплив на ресурс системи. Сумарна оцінка ресурсу системи для будь-якого з випадків не повинна перевищувати 1.

Оцінка проводиться для певного ідентифікованого на попередніх етапах ресурсу системи.

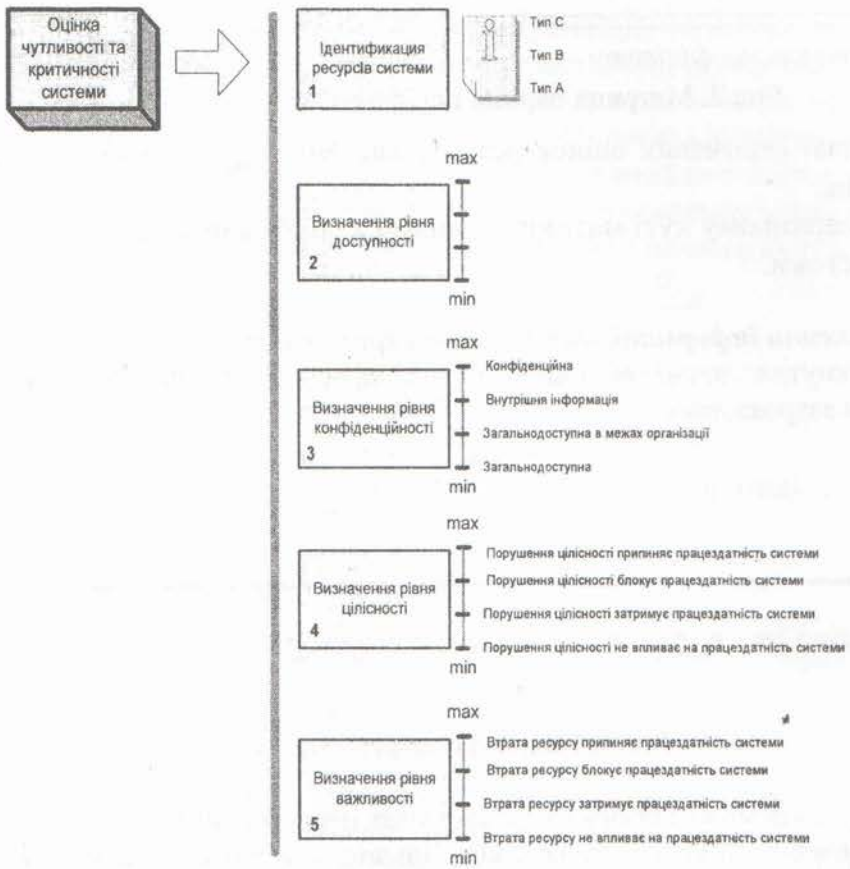

Рис. 1. Процес оцінки ресурсів

Результатом процесу оцінки чутливості та критичності ресурсу системи є числове значення яке розраховується як сума коефіцієнтів отриманих на кожному з етапів оцінки:

$$M_{\text{ч\&к}_N} = \frac{M_Д + M_К + M_Ц + M_В}{4}$$

де $M_{\text{ч\&к}_N}$- оцінки чутливості та критичності ресурсу системи;

$M_Д$ - оцінка рівня доступності для цього ресурсу;

$M_К$ - оцінка рівня конфіденційності для цього ресурсу;

$M_Ц$ - оцінка рівня цілісності для цього ресурсу;

$M_В$ - оцінка рівня важливості для цього ресурсу.

За результатами оцінки необхідно виділити найбільш чутливі та критичні ресурси системи.

У порівнянні з ресурсом типу N

	Ресурс типу A	Ресурс типу B	…	Ресурс типу N
Ресурс типу A				
Ресурс типу B				
…				
Ресурс типу N				

В порядку зменшення значення коефіцієнту

Рис 2. Матриця парних порівнянь

Для цього на підставі отриманих оцінок ресурсу системи $M_{ч\&к\,N}$ необхідно скласти матрицю парних порівнянь.

Таким чином в лівому верхньому куті матриці опиняться найбільш вразливі та критичні та ресурси системи.

2. Визначення множини інформаційних загроз та вразливостей.

На підставі розглянутих вище методик можна сформувати наступну множину напрямків інформаційних загроз:

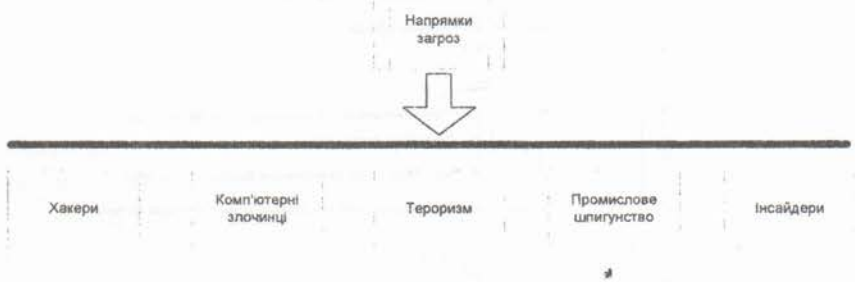

Рис.3. Напрямки загроз

На підставі цих напрямків можна сформувати множину інформаційних загроз.

Виходячи з представленої структури, переважна більшість загроз є наслідком помилок обслуговуючого персоналу та користувачів.

Оцінка можливості реалізації загрози обумовленої помилками обслуговуючого персоналу та користувачів проводиться за допомогою анкетування та подальшого аналізу отриманих результатів. При наявності організаційно-технічних стримуючих факторів, ризик реалізації загрози становить 0,5. При наявності механізмів контролю стримуючих факторів, ризик реалізації загрози становить 0,25. У випадку коли на підставі інформації отриманої від механізмів контролю були прийняті попереджувальні або коректуючи дії, ризик реалізації загрози становить 0,15.

За результатами оцінки кожної із загроз визначається загальний рівень загрози обумовленої помилками обслуговуючого персоналу та користувачів для ресурсу системи за наступною формулою:

$$M_{У_{пN}} = \frac{\sum У_{пN}}{N_{У_{пN}}},$$

де: $M_{У_{пN}}$ - загальна оцінка рівня загрози обумовленої помилкою обслуговуючого персоналу та користувачів, для ресурсу системи;

$\sum У_{п_N}$– сума отриманих оцінок загроз обумовлених помилками обслуговуючого персоналу та користувачів, для ресурсу системи;

$N_{У_{п_N}}$ - загальна кількість загроз обумовлених помилкою обслуговуючого персоналу та користувачів, для ресурсу системи.

Оцінка інших типів загроз проводиться за наступним принципом:

- для кожного типу загроз складається оціночна шкала, в якій в порядку зростання важливості заходу протидії вказується набір всіх можливих заходів. Максимальне значення шкали при цьому приймається за 1. Одиниця поділу при цьому розраховується за формулою $P = \frac{1}{N_з}$, де $N_з$ - загальна кількість заходів протидії для певного виду загрози. Зазначена шкала не є статичною і потребує постійної актуалізації, виходячи з виявлених вразливостей. Наявність вразливостей обумовлена характеристикою ресурсу (його програмної та апаратної складової). В якості джерела інформації щодо вразливостей необхідно використовувати інформацію яка знаходиться в мережі Internet, наприклад http://www.us-cert.gov/;
- шляхом анкетування визначаються організаційно-технічні заходи, які впроваджені в системі з метою протидії негативним факторам обумовленим існуючою загрозою;
- розраховується результуюче значення рівня певного виду загрози за формулою

$$M_{ЗАГ_N} = \frac{\sum U_{P_N}}{N_{вз_N}}$$

де: $M_{ЗАГ_N}$ - оцінка рівня певної загрози для ресурсу системи;

$\sum U_{P_N}$ – сума значень, які відповідають впровадженим заходам протидії для ресурсу системи;

$N_{вз_N}$ - загальна кількість впроваджених заходів протидії для певного виду загрози відносно ресурсу системи.

3. Розрахунок ймовірності ризику

Виходячи з представленої вище інформації всі отримані оцінки можна розглядати як умовні ймовірності.

З них лише $M_З$ стосується загальної оцінки системи. Всі інші оцінки ($M_{У_{п_N}}, M_{ЗАГ_N}, M_{У_{з_N}}$) стосуються певного ресурсу системи.

Оцінку рівня ризику (ймовірності його реалізації) найбільш доцільно проводити для кожного з виділених видів/типів ресурсів системи. Це обумовлено тим, що загальна інформація щодо ризику системи не інформативна, а виконання коректуючих чи попереджувальних дій за нею ускладнена загальною складністю системи та механізмів контролю ефективності впроваджених дій. Однак при оцінці певного ресурсу системи необхідно враховувати і її загальний стан. Найбільш доцільним при такій оцінці є розрахунок середнього за всіма визначеними вище показниками. Таким чином рівень (ймовірність) ризику певного ресурсу буде мати наступний вигляд:

$$M_{P_N} = \frac{M_З + M_{чвк_N} + M_{У_{п_N}} + M_{ЗАГ_N}}{4}$$

де: M_{P_N} - ймовірність ризик певного ресурсу;

$M_З$ - загальна оцінка системи;

$M_{чвк_N}$ - оцінки чутливості та критичності ресурсу системи;

$M_{У_{п_N}}$- загальна оцінка загрози обумовленою помилкою обслуговуючого персоналу та користувачів, для ресурсу системи;

$M_{ЗАГ_N}$ - оцінка певної загрози для ресурсу системи.

Отримана оцінка має кількісне значення, одиницею виміру якої є ймовірність реалізації ризику для певного ресурсу. При необхідності грошового вираження ризику необхідно

провести додаткову його комплексну оцінку.

4. Комплексна оцінка інформаційних активів.

Подальша оцінка проводиться за напрямком визначення грошового вираження ризику.

Для цього необхідно:

- проаналізувати структуру організації чи підприємства виділивши в ній виробничі підрозділи та підрозділи забезпечення;
- визначити граничне значення ризику по підрозділам;
- визначити ризикову вартість оцінюваного ресурсу системи;
- провести розрахунок вартості ризику для оцінюваного ресурсу системи.

Аналіз структури підприємства, виділення виробничих підрозділів та підрозділів забезпечення

На етапі аналізу підприємства необхідно виділити його виробничі підрозділи та підрозділи забезпечення.

Виробничі підрозділи – підрозділи, які випускають готовий продукт, що є результатом діяльності підприємства, спрямованої на одержання прибутку (доходу).

Підрозділи забезпечення – підрозділи, які забезпечують роботу виробничого підрозділу.

Стосовно виділених підрозділів в подальшому визначається їх граничне значення ризику $V_{гр}$.

Визначення граничного значення ризику по підрозділах

Граничне значення ризику в $V_{гр}$ визначається як сума прибутку, яку може або має отримати підрозділ підприємство і вартість самого підрозділу підприємства. Розмір прибутку, який приніс підрозділ, береться зі звіту за минулий рік діяльності підприємства або планового бюджету на поточний рік. Вартість підрозділів підприємства визначається як сума вартості його поточних активів.

Визначення ризикової вартості ресурсу системи

Ризикова вартість ресурсу системи визначається як добуток вираженого в частках рівня використання ресурсу в діяльності підрозділу підприємства та граничного значення ризику для нього.

$$V_{P_N} = R_в \times V_{гр}$$

де: V_{P_N} - ризикова вартість ресурсу системи;

$R_в$ - рівень використання ресурсу системи;

Розрахунок інформаційних ризиків для підрозділів підприємства

Інформаційний ризик для підрозділу підприємства розраховується як добуток ризикової вартості ресурсу системи та ймовірності ризику цього ресурсу.

$$V_N = V_{P_N} \times M_{P_N}$$

де: V_N - інформаційний ризик для підрозділу підприємства

V_{p_N} - ризикова вартість ресурсу системи;

M_{P_N} - ймовірність ризик певного ресурсу.

На підставі представленого вище методологічного підходу сформовано анкету-паспорт на систему яка заповняється експертом (виділено червоним) під час проведення оцінки ризиків системи управління інформаційною безпекою.

Анкета-паспорт на систему ***Назва системи***

Назва системи

Власник системи ***Повне найменування власника системи***

Адреса розташування системи ***Повна адреса розташування, включаючи поверх та номер приміщення***

Історія створення системи ***Етапи починаючи від технічного завдання***

	Оцінка	
Технічне завдання на систему	***Значення***	***Додаток – технічне завдання на систему***
Перелік функціональних вимог до системи	***Значення***	***Надається повний перелік функціональних вимог до системи***
Характеристика даних та інформації яка циркулює в системі	***Значення***	***Надається повна характеристика даних та інформації яка циркулює в системі***

Перелік апаратних засобів системи та програмного забезпечення яке на них використовується (ресурси системи)	Тип А	Тип Б	Тип В	…	…	…	Тип N
	Специфікація	***Специфікація***	***Специфікація***	***Специфікація***	***Специфікація***	***Специфікація***	***Специфікація***

	Оцінка	
Функціональна схема системи	***Значення***	***Додаток – функціональна схема системи***

Характеристика персоналу підтримки та користувачів	Тип a	Тип b	Тип c	…	…	…	Тип x
	Права	***Права***	***Права***	***Права***	***Права***	***Права***	***Права***

	Оцінка		
Політика інформаційної безпеки	***Значення***	***Додаток – політика інформаційної безпеки***	***Характеристика експерта***

	Оцінка	
Технічні засоби контролю системи	***Значення***	***Специфікація***
Принципи та механізми управління системою	***Значення***	***Специфікація***
Принципи та механізми операційного контролю	***Значення***	***Специфікація***
Механізми та засоби забезпечення фізичної безпеки системи	***Значення***	***Специфікація***
Забезпечення екологічної безпеки системи	***Значення***	***Специфікація***

Критичність і чутливість системи	Рівень	Тип А	Тип Б	Тип В	…	…	…	Тип N
Ресурс системи	Д	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*
	К	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*
	Ц	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*
	В	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*

	Тип А	Тип Б	Тип В	…	…	…	Тип N
Оцінка критичності та чутливості системи	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*	*Значення*

Матриця парних порівнянь ресурсів системи	***Додаток – матриця парних порівнянь***

Загальна оцінка системи	***Значення***

В подальшому, на підставі заповненої анкети-паспорту на систему проводиться оцінка ризиків інформаційної безпеки для кожного з виділених типів ресурсів системи (від А до N). За результатами оцінки заповнюється таблиця представлена нижче.

Ресурс ***Назва ресурсу згідно прийнятої типізації***			
№ з/п	Загроза	Стримуючі фактори	Рівень оцінки
Помилки обслуговуючого персоналу та користувачів			
1.	Відсутність підготовленого персоналу	*Опис*	*Значення*
2.	Несвоєчасне призначення посадових осіб, відповідальних за процес	*Опис*	*Значення*
3.	Тимчасова відсутність посадової особи відповідальної за процес	*Опис*	*Значення*
4.	Відсутність контролю з боку керівництва	*Опис*	*Значення*
5.	Невиконання/не якісне виконання посадових обов'язків, вимог, правил і т.і.	*Опис*	*Значення*
6.	Необізнаність персоналу з покладеними на них обов'язками	*Опис*	*Значення*
7.	Не знання вимог чинних регуляторних нормативно-правових актів, положень, інструкцій і т.і.	*Опис*	*Значення*
8.	Комп'ютерна, технічна неграмотність	*Опис*	*Значення*
9.	Незнання технічної, експлуатаційної документації, опису програм і т.і.	*Опис*	*Значення*
10.	Невміння працювати з програмними і технічними засобами	*Опис*	*Значення*
11.	Відсутність політики безпеки, плану захисту, однозначних інструкцій і правил	*Опис*	*Значення*
12.	Необізнаність з положеннями політики безпеки, плану захисту, інструкцій і правил	*Опис*	*Значення*
13.	Відсутність або недостатність документації на систему	*Опис*	*Значення*
14.	Необізнаність з документацією на систему	*Опис*	*Значення*
15.	Неправильна організація роботи декількох користувачів на одному робочому місці	*Опис*	*Значення*
16.	Втрата засобів розмежування доступу	*Опис*	*Значення*
17.	Втрата матеріальних носіїв, що містять службову інформацію	*Опис*	*Значення*
18.	Помилки користувачів під час введення даних в систему	*Опис*	*Значення*
19.	Помилки конфігуруванні, використанні та підключенні засобів захисту	*Опис*	*Значення*
20.	Порушення порядку зберігання та обліку документів, носіїв інформації, даних, технічних засобів	*Опис*	*Значення*

21.	Порушення порядку доступу до приміщень	*Опис*	*Значення*
22.	Порушення порядку допуску до інформації з обмеженим доступом та матеріальних носіїв	*Опис*	*Значення*
23.	Виведення даних за невірними адресами	*Опис*	*Значення*
24.	Порушення технології друкування	*Опис*	*Значення*
25.	Порушення порядку копіювання інформації	*Опис*	*Значення*
26.	Порушення порядку передачі матеріальних носіїв	*Опис*	*Значення*
27.	Видалення файлів без фізичного стирання інформації	*Опис*	*Значення*
28.	Порушення порядку передачі технічних засобів в ремонт	*Опис*	*Значення*
29.	Порушення порядку організації технічного обслуговування та відновлювальних робіт	*Опис*	*Значення*
30.	Дії що приводять до відмови системи або окремих її елементів	*Опис*	*Значення*
31.	Виведення з ладу технічних засобів та носіїв інформації	*Опис*	*Значення*
32.	Порушення режимів функціонування системи	*Опис*	*Значення*
33.	Несанкціоноване копіювання вихідних документів	*Опис*	*Значення*
34.	Розкрадання магнітних носіїв документів, отримання не облікованих копій	*Опис*	*Значення*
35.	Включення в програми програмних закладок та вірусів	*Опис*	*Значення*
36.	Збір за допомогою спеціальних технічних засобів електромагнітних випромінювань та паразитних наведень	*Опис*	*Значення*
37.	Використання підслуховуючи пристроїв	*Опис*	*Значення*
Загальна оцінка рівня загрози обумовленої помилкою обслуговуючого персоналу та користувачів, для ресурсу системи			*Значення*

Інші види загроз

1.	Несанкціонований доступ до конфіденційної інформації сторонніх осіб та користувачів	*Опис*	*Значення*
2.	Перехват за рахунок несанкціонованих підключень	*Опис*	*Значення*
3.	Зараження інформаційної системи програмними кодами	*Опис*	*Значення*
4.	Несанкціоноване створення або знищення інформації	*Опис*	*Значення*
5.	Викрадення носіїв	*Опис*	*Значення*
6.	Збої в системі	*Опис*	*Значення*
7.	Втрати інформації через некоректну роботу програмного забезпечення	*Опис*	*Значення*
8.	Перехват інформації по каналам побічних електромагнітних випромінювань, наведень та по відвідним каналам	*Опис*	*Значення*
9.	Повторне використання об'єктів	*Опис*	*Значення*
10.	Хакерські атаки через локальну мережу, корпоративну мережу та мережу Інтернет	*Опис*	*Значення*
11.	Порушення режимів функціонування системи	*Опис*	*Значення*
Загальна оцінка рівня певної загрози для ресурсу системи		*Значення*	

Ймовірність ризик певного ресурсу	*Значення*

При необхідності визначення ризику в грошовому еквіваленті додатково заповнюються наступні таблиці.

Граничне значення ризику	***Значення***

Ризикова вартість ресурсу системи	***Значення***

Інформаційний ризик для підрозділу підприємства	***Значення***

Висновки

Розроблена методика надає фахівцю, який проводить оцінку ризиків, зручний та однозначний підхід до оцінки ризиків підприємства будь-якого розміру та напрямку діяльності.

Оцінка проводиться шляхом заповнення ряду таблиць та проведення на їх підставі ряду розрахунків, які дозволяють отримати кількісну оцінку величини ризику інформаційної безпеки, при цьому цей ризик може бути виражений як ймовірність або грошовий еквівалент.

Розроблена методика повністю відповідає вимогам міжнародного стандарту ISO/IEC 27001:2005 щодо відтворюваності та порівнянності результатів оцінки.

Розроблена методика може бути рекомендована до використання для оцінки ризиків, які пов'язані з інформаційними технологіями в рамках впровадження галузевих та загальнодержавних стандартів з побудови систем управління інформаційною безпекою в першу чергу в банківський та фінансовій галузях, або будь-якому за розмірами та напрямком діяльності підприємстві, яке взяло за мету побудувати та сертифікувати на відповідність вимогам міжнародного стандарту ISO/IEC 27001:2005 систему управління інформаційною безпекою.

Список літератури

1. BS ISO/IEC 27005:2008 Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности.

2. А.М. Литовских, И.К. Шевченко. Терминологический словарь: финансы, денежное обращение и кредит.

3. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 384с.: ил. – (Информационные технологии для инженеров).

4. Єрмошин В. Методологія оцінки ризиків у відповідності до вимог міжнародного стандарту ISO/IEC 27001 // Одиннадцатая Международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах", Тезисы докладов. –К: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ" . –2008. - С.63.

5. Ермошин В.В. Методика оценки информационных рисков предприятия // Захист інформації. – 2009. – №4(45), С. 80-88.

6. Factor Analysis of Information Risk (FAIR) http://www.riskmanagementinsight.com/.

7. IS RISK ASSESSMENT MEASUREMENT http://www.isaca.org.

8. NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems http://www.nist.gov.

9. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach http://www.cert.org/octave/.

Запропоновано методику оцінки ризиків системи інформаційної безпеки, яку можна застосовувати на практиці в різних сферах виробництва та бізнесу.
Ключові слова: ризик, сертифікація, загроза, ресурси системи, інформаційна безпека.

Предложена методика оценки рисков системы управления информационной безопасностью, которую можно использовать на практике в различных сферах производства и бизнеса.
Ключевые слова: риск, сертификация, угроза, ресурсы системы, информационная безопасность.

In the paper the method for assessment of information risks of information security management system has been developed. It can be used in practice in different spheres of business.
Key words: risk, certification, threat, system resources, information security.

Надійшла 22.06.2010