УДК 004.621

**Скачек Л.М. (ДУІКТ)**

# МЕТОДИКА ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ ПІДПРИЄМСТВА

Пропонується методика оцінки інформаційного ризику підприємства як послідовність аналізу його структури, визначення граничного ризику його підрозділів, аналізу його інформаційної інфраструктури з подальшим накладенням її на організаційну структуру підприємства, визначення ризикової вартості автоматизованих систем, що використовуються в роботі підприємства, оцінки активів підприємства, ймовірність реалізації загроз для його автоматизованих систем, визначення ризику для окремих підрозділів підприємства.

**Мета роботи.** Метою роботи є перехід від найбільш поширеної на сьогоднішній день якісної (в порівнянні) оцінки інформаційних ризиків підприємства до кількісної оцінки, одиницею вимірювання якої є грошова одиниця.

**Основна частина**

Аналіз структури підприємства, виділення виробничих і забезпечуючих підрозділів.

Ризик розглядається як виражена в грошовому еквіваленті ймовірність реалізації загрози. Інформаційний ризик розглядається як добуток ризикової вартості автоматизованої системи, результату оцінки ресурсу і ймовірності реалізації конкретного виду загроз.

На етапі аналізу підприємства необхідно виділити його виробничі і забезпечуючі підрозділи.

Виробничі підрозділи — підрозділи, які випускають готовий продукт та є результатом діяльності підприємства направленого на отримання прибутку (доходу), забезпечуючі підрозділи — підрозділи що забезпечують роботу виробничого підрозділу.

Виділення підрозділів надалі дозволить визначити їх вартість і визначити граничне значення ризику. Розглянемо це на прикладі структури підприємства, яка була визначена в процесі аналізу ( рис.1).

У представленій структурі до виробничих підрозділів відносяться цехи основного виробництва, філії. Решта підрозділів підприємства виконує забезпечуючу функцію.

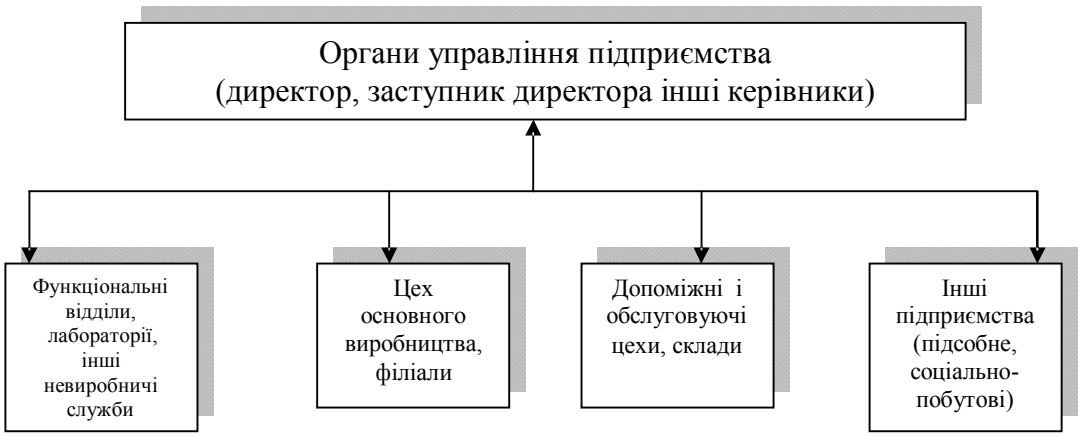


Рис. 1. Структура підприємства

Граничне значення ризику визначається як сума прибутку, що може або повинен отримати підрозділ підприємства і вартість самого підрозділу підприємства. Розмір прибутку який одержав підрозділ береться із звіту, що пройшов, діяльності підприємства або планового бюджету на поточній рік. Вартість підрозділу підприємства визначається як сума вартості його активів поточного року. В якості прикладу були прийняті наступні граничні значення ризиків в табл.1.

Таблиця 1

| | Значення граничного ризику, в грн. |
|---|---|

| Найменування підрозділу | |
|---|---|
| Органи управління підприємства | 12 000 |
| Невиробничі служби | 30 000 |
| Цех основного виробництва | 150 000 |
| Склад | 20 000 |
| Інші підприємства | 5 000 |

Аналіз інформаційної інфраструктури підприємства полягає у виділені автоматизованих систем, задіяних в процесі виробництва і його забезпечення, та накладання їх на структуру підприємства. Приклад загальної інформаційної структури представлено на рис.2

Проведений аналіз повинен бути максимально детальний, в результаті чого необхідно спуститися на рівень робочих місць (робочих станцій), скласти їх детальну характеристику, яка включає характеристику використовуваних автоматизованих систем, характеристику самих робочих станцій, типів і версій установлених на них операційних систем, детальну специфікацію встановленого програмного забезпечення.

Результати проведеного аналізу представлено нижче.

В інформаційній системі присутні такі типи інформаційних активів: файлові сервери, сервери додатків, інтернет-шлюзи, поштові сервера PostFix, поштові сервера Lotus Domino, робочі станції. На всій множині інформаційних активів використовуються наступні типи операційних систем: Windows Sever 2000, Windows Sever 2003, RHL 4,6, RHL 5, AIX5.3, Windows XP, Windows 2000 SP4. Схема проходження web-трафіка в інформаційної системи має наступний вигляд (рис. 2).

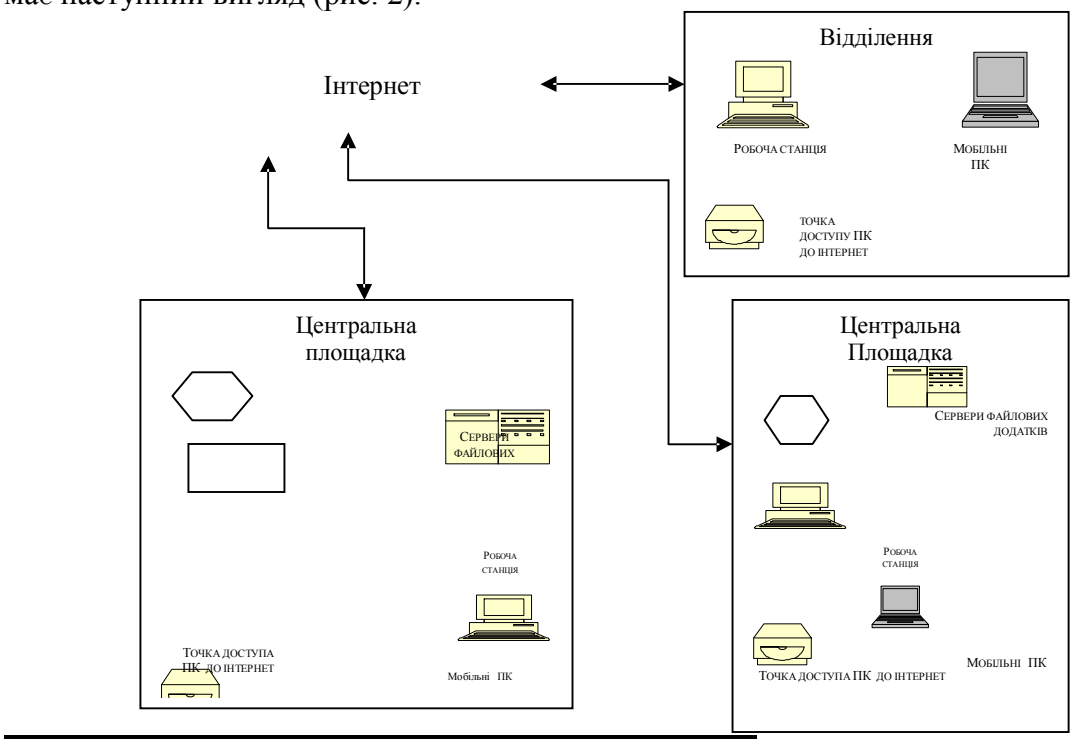


Рис.2. Приклад інформаційної структури підприємства

В інформаційній системі використовують систему корпоративної пошти на базі Postfix 2.1.5 і Lotus Domino Enterprise 8.0.2. В інформаційній системі використовуються магістральні цифрові канали Frame Relay, від 64 Kbit/s до 10 Mbit/s. Поштові сервера Lotus Domino використовуються в якості «транспорту» для автоматизованої системи формування оперативної звітності цеху основного виробництва (20 робочих місць, інвентарний номер 2121-2141, 100% від загальної кількості робочих місць), клієнтами системи також є органи

управління (3 робочих місця, інвентарний номер 1741-1744, 24% від загальної кількості робочих місць) і склад (1 робоче місце, інвентарний номер 1417, 30% від загальної кількості робочих місць).

Ризикова вартість автоматизованої системи визначається як добуток вираженого в рівних долях використання автоматизованої системи в діяльності підрозділу підприємства і граничного значення ризику для нього. Розглянемо приклад визначення ризикової вартості автоматизованої системи формування оперативної звітності цеху основного виробництва (табл.2 ).

Активи підприємства (підрозділи) це власність підприємства, яка відображена в активі балансу.

Визначення ризикованої вартості автоматизованої системи Таблиця 2

| Найменування підрозділу | Значення граничного ризику, в грн. | Рівень використання автоматизованої системи | Ризикова ватість автоматизованої системи, в грн. |
|---|---|---|---|
| Органи управління підприємством | 12 000 | 0,24 | 2 880 |
| Невиробничі служби | 30 000 | 0 | 0 |
| Цех основного виробництва | 150 000 | 1 | 150 000 |
| Склад | 20 000 | 0,3 | 6 000 |
| Інші організації | 5 000 | 0 | 0 |

В основному існують три види активів: 1) поточні активи; 2) основний капітал з тривалим терміном служби; 3) інші активи.

Оцінка активів, полягає в їх ідентифікації, визначенні рівня їх доступності, цілісності і конфіденційності, визначенні важливості ресурсів (узагальнення — характеристик ресурсу).

В якості класів інформаційних ресурсів може бути запропоновано: робоча станція, сервер додатків, поштовий сервер, точка доступу/шлюз до Інтернет, і так далі. Оцінка проводиться для кожного позначеного класу ресурсу. Схематично процес оцінки ресурсів проілюстрований на рис. 3.

Процес визначення рівня доступності, цілісності та конфіденційності ідентифікованих ресурсів, а також процес визначення їх важливості супроводжується визначенням їх вагових коефіцієнтів. В якості прикладу оціночна шкала, яка пов’язана з характеристикою ресурсу, виражена в привласненні йому ідентифікатора належності до певної групи використаних наступних шкал:

*При визначенні рівня доступності*: ресурс повинен бути доступний завжди; ресурс може бути недоступний протягом 1 години; ресурс може бути недоступний протягом 4 годин; ресурс може бути недоступний протягом 8 годин.

*При визначенні рівня цілісності*: порушення цілісності припиняє працездатність системи; порушення цілісності блокує працездатність системи; порушення цілісності уповільнює працездатність системи; порушення цілісності не впливає на працездатність системи.

*При визначенні рівня важливості ресурсу*: втрата ресурсу припиняє працездатність системи; втрата ресурсу блокує працездатність системи; втрата ресурсу уповільнює працездатність системи; втрата ресурсу не впливає на працездатність системи. Чим більший ваговий коефіцієнт, тим більший негативний вплив чиниться на ресурс. Як приклад, вага одиниці вагового коефіцієнта приймається за 0,0625. Сумарна оцінка ресурсу в даному прикладі не повинна перевищувати 1.

Першим етапом повинна використовуватись оцінка ідентифікації ресурсів, подальша послідовність пропонується як рекомендована.

Результатом цього процесу являється оцінка ресурсу $O_p$, який розраховується як сума коефіцієнтів, отриманих на кожному із етапів оцінки:

$$O_p = O_{Д} + O_К + O_{Ц} + O_В,$$

де $O_{Д}$ — оцінка рівня доступності;

$O_К$ — оцінка рівня конфіденційності;

$O_{Ц}$ — оцінка рівня цілісності;

$O_В$ — оцінка рівня важливості.

Надалі, значення оцінки ресурсу $O_p$, будемо використовувати для визначення значення ризику розглядуваного ресурсу, який дорівнює 0,875.

Для оцінки (розрахунку) ймовірності реалізації загроз для автоматизованих систем визначимо поняття загроз, яке грунтується на способі негативної дії на систему або її компоненти. Загальноприйняті в області ІТ—безпеки поняття загрози і уразливості в даному документі об'єднані в поняття загроза. Набір загроз і уразливостей формується на етапі розробки моделі загроз.

Формування переліку загроз і уразливостей, які актуальні для елементів (рівень клієнтів) задіяних в роботі автоматизованої системи визначається на етапі формування моделі загроз.

Для однієї уразливості може існувати декілька загроз.

Множина потенційних загроз і множина уразливостей є кінцевою множиною, визначеною на етапі формування моделі загроз.

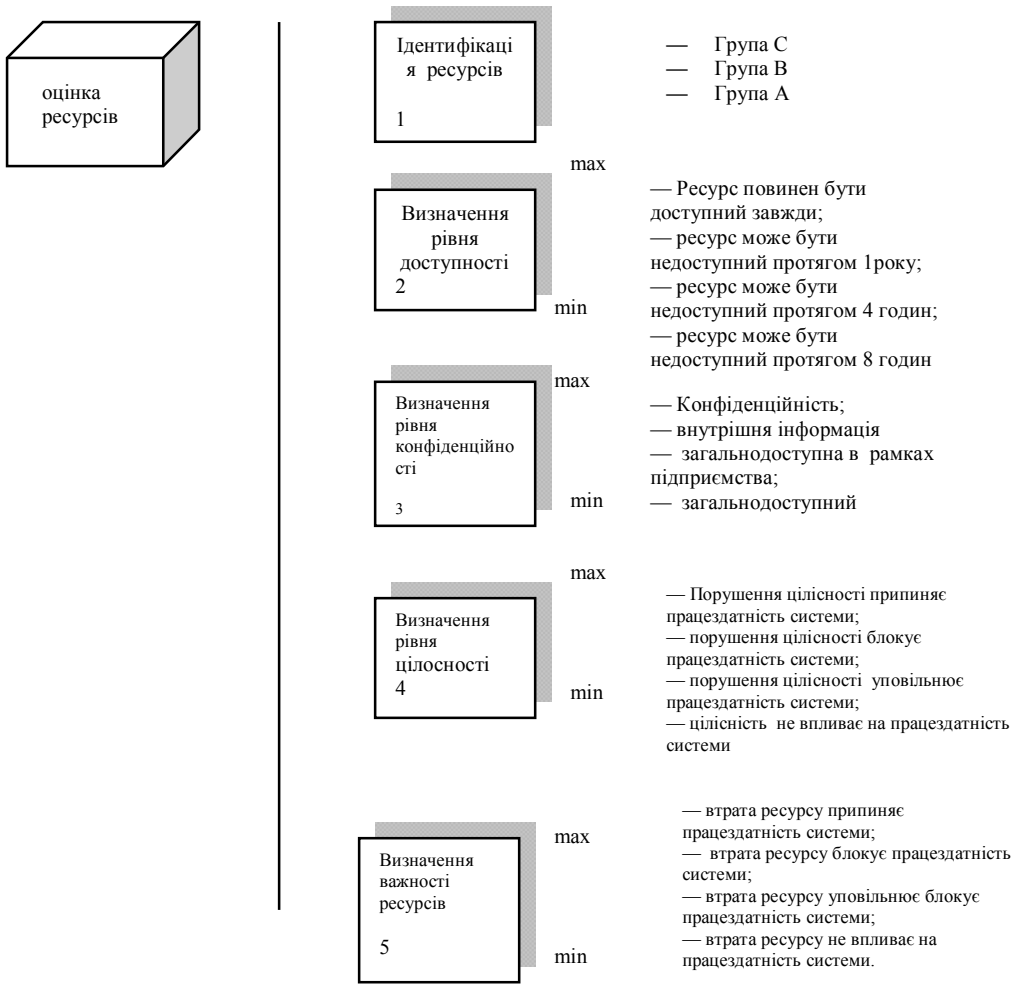


Рис. 3. Процес оцінки ресурсів

Обидві множини є динамічними і підлягають періодичному перегляду. Як інтервал, після якого множину необхідно переглядати, рекомендується використовувати часовий проміжок 1 рік.

Множина засобів захисту є динамічна нескінчена множина, яка підлягає постійній актуалізації. Інтервал актуалізації, що рекомендується, — раз на квартал.

Між загрозою і існуючими захисними заходами повинен існувати логічний зв'язок, який визначає експерт або група експертів, що формують моделі або кінцеву оцінку.

Результатом процесу оцінки загрози є числове значення ймовірності реалізації конкретного виду загроз виходячи з наявності уразливостей, засобів захисту та відомого досвіду.

На етапі ухвалення рішення про наявність загрози визначається ймовірність їх реалізації та проводиться розрахунок для кожного виявленого виду загроз. Результатом позитивної оцінки (наявність загрози, уразливості, засобу) на етапі 2, 3 і 5 є 1.

Якщо на кожному з цих етапів в результаті проведеної оцінки отримаємо 1, то ймовірність реалізації цього виду загроз дорівнює 1, якщо на одному з цих етапів отримано негативний результат — 0, імовірність реалізації цього виду загрози дорівнює 0,5, в інших випадках імовірність реалізації цього виду загрози дорівнює 0,01.

Узагальнена таблиця значень ймовірності реалізації загроз для ресурсу залежно від уразливостей і засобів представлено в таблиці 3.

Узагальнена таблиця значень ймовірності реалізації загроз Таблиця 3

| Імовірність загрози $P_y$ | Подія мало-ймовірна або підприємство із загрозою не зустрічалось | Подія теоретично можлива | Із загрозою зустрічалось підприємство-партнер | Подія можлива | Розповсюджена подія або підприємство зустрічалось с загрозою |
|---|---|---|---|---|---|
| Загроза/ уразливість/ засіб | 0,01 | 0,35 | 0,5 | 0,75 | 1 |
| Загроза/ уразливість | 0,005 | 0,175 | 0,25 | 0,375 | 0,5 |
| Загроза | 0,0001 | 0,0035 | 0,005 | 0,0075 | 0,01 |

Значення ймовірності менше 0,01 вважаються мінімальними і можуть бути виключені з подальшого розгляду.

До розгляду пропонується наступна шкала вразливостей: Люди; Користувачі; Співробітники підрозділів; Адміністратори; Співробітники служби захисту інформації; Керівники; Хакери; Програми; Устаткування. При цьому рівень загрози (ваговий коефіцієнт) з критерію люди відповідають рівню визначеному при формуванні моделі загроз. На етапі визначення ймовірності реалізації, повинний враховуватися світовий досвід або досвід підприємства в області інформаційної безпеки. Як джерело, що враховує світовий досвід, рекомендовано застосовувати доступні результати досліджень в конкретній області (області інформаційної безпеки). наприклад, дослідження, які проводилися Gartner, Inc., The Forrester Wave або або інші доступні дослідження.

В якості прикладу пропонується використовувати результати досліджень Gartner, Inc., 21.12.2008, ID Number G00153291. Пропонуються наступна шкала потенційних загроз: Відмова — П; Вірус; НСД—ЛВС: Переадресація; Нав'язування; Ресурси ОС; Ресурси КЗ; Прослуховування; Читання — З; Копіювання; Імітація; НСД — РС; НСД — П; Злом; Перехоплення; Закладка — П; Перешкоди; Підміна; Дезорганізація.

Виходячи з представленої в них інформації, шкала, що враховує вагу певного виробника в конкретній області (світовий досвід), від більшого до меншого, матиме наступний вигляд: Bi9; eEye Digital Securiti; Big Fix; Webroot Software; LAN Desk; Kaspersky

Lab; Check Point Software Technologies; Panda Securiti; IBM; F-Secure; CA; Sophos; Mikrosoft Trend; Mikro; Symantec; McAfee

При цьому ймовірність, яка враховує світовий досвід $P_0$, розраховується як приватний рівень відповідного досвіду розглядуваного виробника і максимального значення цього рівня із всього представленого набору значень (для представленого випадку 16). У випадку якщо застосовується декілька засобів захисту, в подальших розрахунках приймається менша ймовірність реалізації, яка відповідає більшому досвіду виробника в побудові систем захисту. Результуюча ймовірність реалізації $P_{PEÇ}$ визначається як добуток ймовірності загрози, ймовірності уразливості і ймовірності, що враховує світовий досвід. Приклад результатів ймовірності реалізації загроз і вразливостей «програми» представлено в табл.4.

З результатів оцінки кожного підрозділу підприємства складається зведена матриця ймовірності загроз.

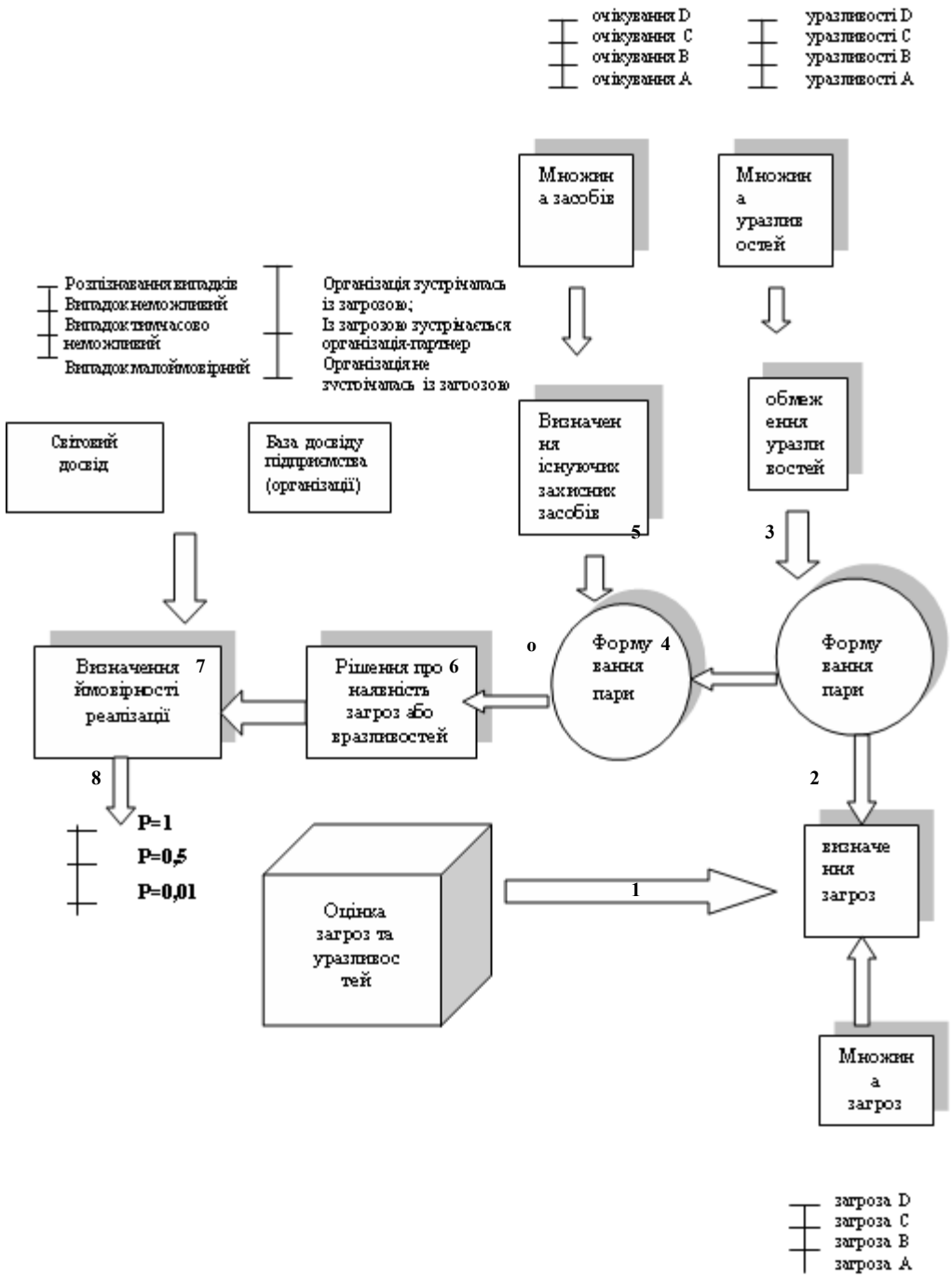


Рис.4. Процес оцінки загроз та вразливостей

Інформаційний ризик для підрозділу підприємства розраховується як добуток ризикової вартості автоматизованої системи, результату оцінки ресурсу і ймовірності реалізації конкретного виду загроз.

Результати ймовірності реалізації загроз і уразливостей Таблиця 4

| Уразливості | | Загроза | | Світовий досвід | | Результуюча ймовірність |
|---|---|---|---|---|---|---|
| Найменування | Ймовірність | Найменування | Ймовірність | Найменування | Ймовірність | |
| | | Відмова — П | 0,35 | Trend Micro | 0,1875 | 0,065625 |

| | | | | | | |
|---|---|---|---|---|---|---|
| П Р О Г Р А М И | 1. | Вірус | 1 | Trend Micro | 0,1875 | 0,1875 |
| | | НСД—ЛВС | 0,35 | Trend Micro | 0,1875 | 0,065625 |
| | | Переадресація | 0,35 | Trend Micro | 0,1875 | 0,065625 |
| | | Нав'язування | 0,5 | Trend Micro | 0,1875 | 0,09375 |
| | | Ресурси ОС | 0,75 | Trend Micro | 0,1875 | 0,140625 |
| | | Ресурси КЗ | 0,75 | Trend Micro | 0,1875 | 0,140625 |
| | | Прослуховування | 0,5 | Trend Micro | 0,1875 | 0,09375 |
| | | Читання — З | 0,35 | Trend Micro | 0,1875 | 0,065625 |
| | | Копіювання | 0,75 | Trend Micro | 0,1875 | 0,140625 |
| | | Імітація | 0,5 | Trend Micro | 0,1875 | 0,09375 |
| | | НСД — РС | 0,35 | Trend Micro | 0,1875 | 0,065625 |
| | | НСД — П | 0,35 | Trend Micro | 0,1875 | 0,065625 |
| | | Злом | 0,75 | Trend Micro | 0,1875 | 0,140625 |
| | | Перехоплення | 0,35 | Trend Micro | 0,1875 | 0,065625 |
| | | Закладка — П | 0,75 | Trend Micro | 0,1875 | 0,140625 |
| | | Перешкоди | 0,35 | Trend Micro | 0,1875 | 0,065625 |
| | | Підміна | 0,35 | Trend Micro | 0,1875 | 0,065625 |
| | | Дезорганізація | 0,5 | Trend Micro | 0,1875 | 0,09375 |

З результатів розрахунку складається результуюча матриця ризиків для підрозділів підприємства (табл.5).

Матриця ризиків для підрозділів підприємства Таблиця 5

| Підрозділи | Ризикована вартість, в грн. | Оцінка ресурсу | Результуюча ймовірність загрози | | Значення ризику, в грн. |
|---|---|---|---|---|---|
| | | | Найменування | Значення | |
| ЦЕХ ОСНОВНОГО ВИРОБНИЦТВА | 150 000 | 0,875 | Відмова — П | 0,065625 | 8 613. 28 |
| | | | Вірус | 0,1875 | 24 609.38 |
| | | | НСД—ЛВС | 0,065625 | 8 613. 28 |
| | | | Переадресація | 0,065625 | 8 613. 28 |
| | | | Нав'язування | 0,09375 | 12 304.69 |
| | | | Ресурси ОС | 0,140625 | 18 457.03 |
| | | | Ресурси КЗ | 0,140625 | 18 457.03 |
| | | | Прослуховування | 0,09375 | 12 304.69 |
| | | | Читання — З | 0,065625 | 8 613. 28 |
| | | | Копіювання | 0,1875 | 18 457.03 |
| | | | Імітація | 0,09375 | 12 304.69 |
| | | | НСД — РС | 0,065625 | 8 613. 28 |
| | | | НСД — П | 0,065625 | 8 613. 28 |
| | | | Злом | 0,140625 | 18 457.03 |
| | | | Перехоплення | 0,065625 | 8 613. 28 |
| | | | Закладка — П | 0,140625 | 18 457.03 |
| | | | Перешкоди | 0,065625 | 8 613. 28 |
| | | | Підміна | 0,065625 | 8 613. 28 |
| | | | Дезорганізація | 0,09375 | 12 304.69 |

**Висновки.** У результаті проведення оцінки запропонованої методики підприємство отримує не якісну (високий, середній, низький), а кількісну (виражену в грошах) оцінку ризиків, що дозволить керівництву підприємства реально оцінити свої інформаційні активи і об'єктивно вибрати методи та засоби їх захисту.

**Список літератури**

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

2. Андрєєв В.І., Хорошко В.О., Шелест М.Є. Основи інформаційної безпеки / за ред.. проф.. В.О. Хорошка. 2-е вид., доп. і перероб. – К.: ДУІКТ, 2009. – 292 с.

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

Надійшла: 17.05.2011 р.

Рецензент: д.т.н., проф. Кузнецов Г.В.