УДК 004.021
DOI: 10.31673/2409-7292.2022.023844

Чернявський І.Р., Якименко Ю.М.

РИЗИКООРІЄНТОВАНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

Стаття присвячена дослідженню проблем ризикоорієнтованого підходу в управлінні інформаційною безпекою підприємства. У статті проведено аналіз основних характеристик управління інформаційною безпекою на сучасному етапі; досліджено вимоги нормативно-методичних документів щодо організації управління інформаційною безпекою на підприємстві; розкриті основні процеси і складові організації управління; досліджено організація управління з використанням ризикоорієнтованого підходу.

Ключові слова: інформаційна безпека підприємства, система управління інформаційною безпекою, ризик, ризикоорієнтований підхід.

Вступ

Захист інформації на підприємстві є важливим завданням, що може впливати на фінансову та виробничу його діяльність і як наслідок на ринок, в якому існує. Для того, щоб забезпечити підприємству розвиток та конкурентоспроможність, необхідно створити надійну систему управління інформаційною безпекою. У інформаційну безпеку підприємства входить сукупність напрямів, методів, засобів і заходів, що знижують незахищеність інформації і не дає можливість зловмисникам доступу до інформації, її розповсюдженню або витоку. Для того, щоб підприємство функціонувало ефективно, необхідно ідентифікувати та управляти багатьма процесами, а саме управляти процесами забезпечення його інформаційної безпеки. Для кожного підприємства необхідно знаходити свої підходи до збільшення безпечного рівня захисту інформації від багатьох негативних факторів, створювати різні моделі ефективного управління інформаційною безпекою і в першу чергу розробляти та впроваджувати систему управління інформаційною безпекою. Саме тому досить актуальним є питання в дослідження підходів до організації управління інформаційною безпекою на підприємстві.

Мета роботи полягає у дослідженні організації управління інформаційною безпекою на підприємстві на основі ризикоорієнтованого підходу.

Використання ризикоорієнтованого підходу в управлінні інформаційною безпекою підприємства

Актуальність питань оцінки захищеності ІС в Україні почала зростати у 2005 р. з появою міжнародних стандартів з управління інформаційною безпекою, більшість з яких містять вимоги щодо оцінювання стану ІБ. Виникла потреба у сертифікації на відповідність стандартам ІБ для зміцнення авторитету підприємства серед партнерів та клієнтів. Процедура сертифікації неодмінно передбачає аудит стану ІБ організації.

Методика, яка запропонована в статті спирається на дослідження в області ІБ, українські національні та міжнародні стандарти з управління інформаційною безпекою та методики оцінювання ІБ. Для практичної реалізації методики для дослідження була застосована система управління інформаційною безпекою і програма «Матриця» [1].

Областю застосування пропонованої методики є аудит ІБ та оцінювання захищеності комп'ютерних систем. Призначеннями пропонованої методики є оцінювання загального рівня захищеності комп'ютерної системи, виявлення найбільш вразливих активів і найбільш небезпечних загроз для конкретної організації, визначення пріоритетів в усуненні вразливостей ІБ.

Процедура пропонованої методики заснована на оцінці ризиків ІБ та є наступною [1]:

1. Первинне опитування клієнта

На цьому етапі необхідно з'ясувати та визначити наступне:

структура мережі: фізична і логічна, розміщення устаткування, в т.ч. характеристика приміщень;

набір перевірок безпеки: бажані та рекомендовані;

активи: перелік та їх важливість для клієнта;

загрози: перелік та рівень небезпеки для клієнта;

облікові записи (необхідні для виконання обраних перевірок): імена користувачів, паролі, точки входу.

2. Визначення активів

Щоб визначити список активів цільової організації, слід перелічити усі малі об'єкти клієнта, що схильні до загроз інформаційної безпеки (а отже спричиняють ризики). Список активів повною мірою залежить від структури і особливостей цільової організації. Активами можуть бути не лише фізичні об'єкти (сервери, термінали, камери, друковані документи і т.п.), але й інформація (файли, згенеровані ключі і т.п.). Експерти перевіряючої сторони складають остаточний список активів на підставі первинного опитування.

3. Визначення важливості активів за словесною шкалою

Визначення важливості активів відбувається за словесною шкалою. Дані первинного опитування клієнта рецензуються на підставі думок експертів перевіряючої сторони та офіційних документів (наприклад, стандартів ІБ або бюлетенів Microsoft). Наприкінці цього етапу кожен актив повинен мати словесну оцінку важливості. *Рекомендовані ступені важливості:* Критичний, Важливий, Рядовий, Маловажливий, Неважливий. Приклад результату даного етапу наведений в табл. 1.

Таблиця 1

Рекомендована шкала оцінок важливості активів

Важливість активу	Збиток при реалізації загроз (умовна оцінка)
Критичний	5
Важливий	4
Рядовий	3
Маловажливий	2
Неважливий	1

4. Пошук вразливостей визначених активів

Пошук вразливостей визначених активів виконується у відповідності до спектру доступних перевірок:

перевірка на проникнення (penetration test);

визначення зловмисників серед співробітників цільової організації (insiders);

аналіз налаштувань (конфігурації);

аналіз фізичного доступу до об'єктів комп'ютерної мережі;

інші перевірки ІБ.

5. Визначення загроз, що походять від знайдених вразливостей

Одна вразливість може бути джерелом декількох загроз (наприклад, фізичний доступ до сервера може бути причиною як знищення так і захоплення устаткування). Тому слід визначити загрози для кожної знайденої вразливості на підставі думок експертів перевіряючої сторони та офіційних документів (наприклад, стандартів ІБ або бюлетенів Microsoft). Наприкінці цього етапу має бути складений перелік загроз.

6. Визначення ступеня небезпеки знайдених загроз за словесною шкалою

Визначення рівня небезпеки загроз відбувається за словесною шкалою. Дані первинного опитування клієнта рецензуються на підставі думок експертів перевіряючої сторони та офіційних документів (наприклад, стандартів ІБ або бюлетенів Microsoft). Наприкінці цього етапу кожна загроза повинна мати словесну оцінку рівня небезпеки. *Рекомендовані міри оцінки важливості*: Критичний, Важливий, Середній, Низький, Малоймовірний.

Існує приклад перекладу важливості активів та ступеня небезпеки загроз в кількісні оцінки. Так для автоматизованої оцінки ризиків можна перевести попередньо отримані словесні оцінки активів і загроз в кількісні. Для цього використовуютьр екомендовані шкали оцінок, які представлені приведені в табл. 1 та 2. Отриманий результат даного етапу наведений в табл. 3 та 4 [2].

Таблиця 2.

Рекомендована шкала оцінок ступеня небезпеки загроз

Рівень небезпеки загрози	Вірогідність реалізації (умовна оцінка)
Критичний	5
Важливий	4
Середній	3
Низький	2
Малоймовірний	1

Таблиця 3.

Приклад оцінок важливості активів

Актив	Важливість	Збиток
Сервер доступу до Інтернет	Критичний	5
Сервер 1С:Підприємство, термінал.сервер	Критичний	5
Головний контролер домену	Критичний	5
Поштовий сервер	Важливий	4
Запасний контролер домену, сервер БД	Важливий	4

Таблиця 4.

Приклад оцінок рівня небезпеки загроз

Загроза	Рівень небезпеки	Частота
Переповнення буфера	Критичний	5
Несанкціоноване отримання прав	Важливий	4
Виток інформації	Важливий	4
Віддалене виконання коду	Середній	3
Відмова в обслуговуванні	Низький	2

8. Підрахування оцінок ризиків

Для автоматизованого підрахування оцінок ризиків в СУІБ «Матриця», слід виконати наступні дії у пункті головного меню «Списки елементів»:

1. Ввести в СУІБ виявлені активи у вигляді списку, що містить назви активів і значення збитку, згідно з вибраною шкалою оцінок.
2. Ввести в СУІБ виявлені загрози у вигляді списку, що містить назви загроз і їх частоти (вірогідність реалізації), згідно з вибраною шкалою оцінок.
3. Сформувати список ризиків шляхом призначення загроз активам. Автоматичне перехресне об'єднання активів з загрозами недоступне, оскільки можуть бути утворені неіснуючі, незначні, або навіть неможливі ризики (наприклад, фізичне пошкодження цифрових підписів).

Оцінки ризиків розраховуються автоматично шляхом множення значення збитку активу на значення частоти загрози:

$$R = W \times n \quad (1)$$

де R - ризик, W - збиток, n - частота.

У пункті головного меню «Оцінка ризиків» зведена діаграма надає огляд ризиків, а зведена таблиця - розподіл загроз за активами і навпаки, з сумарними оцінками по кожному активу і кожній загрозі.

Сумарна оцінка ризику (у зведеній таблиці ризиків) потрібна для періодичного оцінювання. Вона дає можливість відстежити зміни загального рівня ризику з плином часу. Приклади зведеної таблиці та зведеної діаграми ризиків наведені відповідно на рис. 1 та рис 2.

Оцінка ризиків

Відображення: Таблиця / Діаграма

Загроза	Актив: Головний контро/ Оцінка ризику	Запасний контрол Оцінка ризику	Поштовий сервер Оцінка ризику	Сервер 1С:Підпри/ Оцінка ризику	Сервер доступу до Оцінка ризику	Общие итоги Оцінка ризику
Виток інформації	20	16	16	20	20	92
Віддалене виконання коду	15	12	12	15	15	69
Відмова в обслуговуванні	10	8	8	10	10	46
Несанкціоноване отримання прав	20	16	16	20	20	92
Переповнення буфера	25	20	20	25		90
Общие итоги	90	72	72	90	65	389

Рис. 1. Приклад зведеної таблиці ризиків [1]

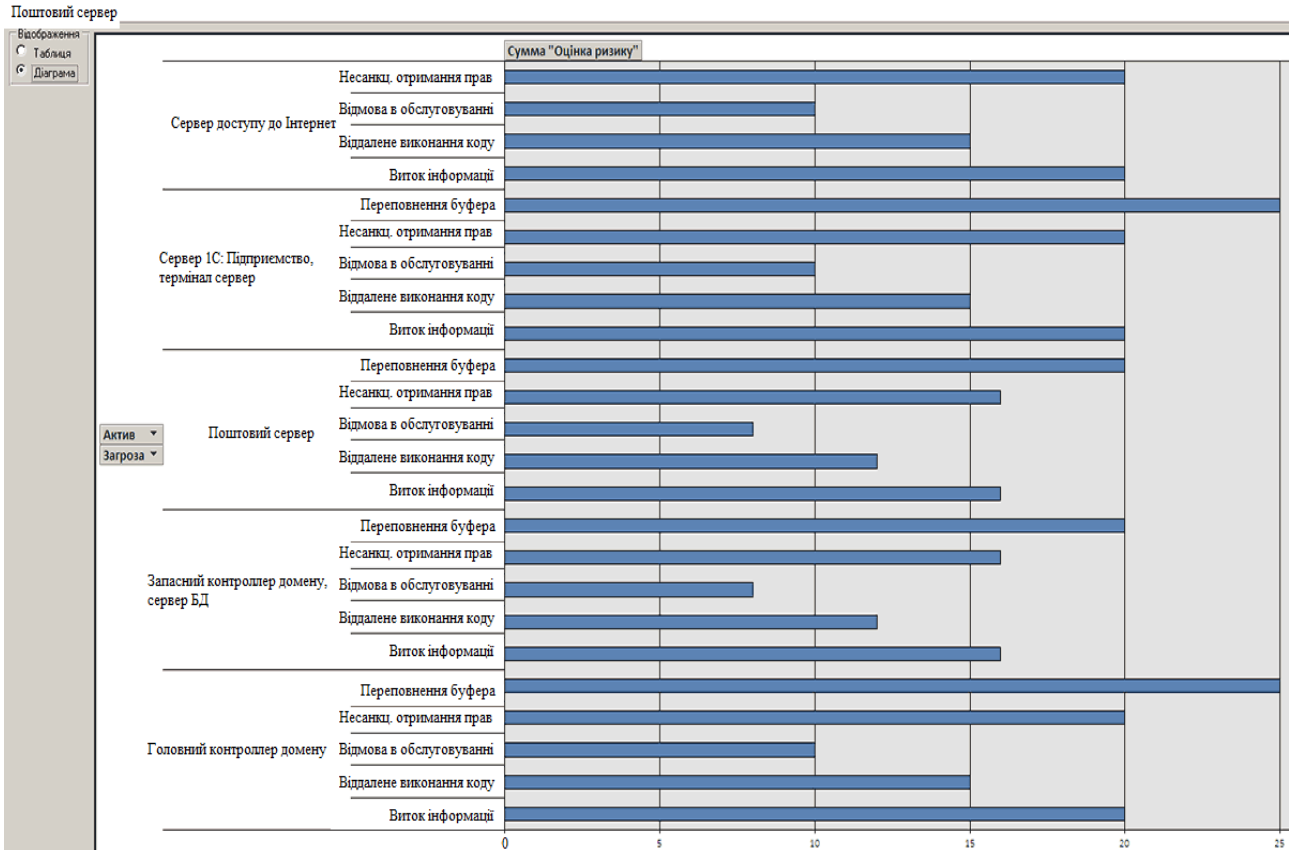

Рис. 2. Приклад зведеної діаграми ризиків [1]

9. Визначення найбільш вразливих активів та найбільш небезпечних загроз

У зведеній діаграмі «Оцінка ризиків», прибираючи по черзі поля з області даних, отримати спочатку графік сумарних оцінок за активами, потім за загрозами. Приклади графіків сумарних оцінок за активами та за загрозами наведені відповідно на рис. 3 та рис. 4.

Зробити висновки про найвразливіші активи та найбільш небезпечні загрози (вони матимуть найвищі сумарні оцінки ризику) [3].

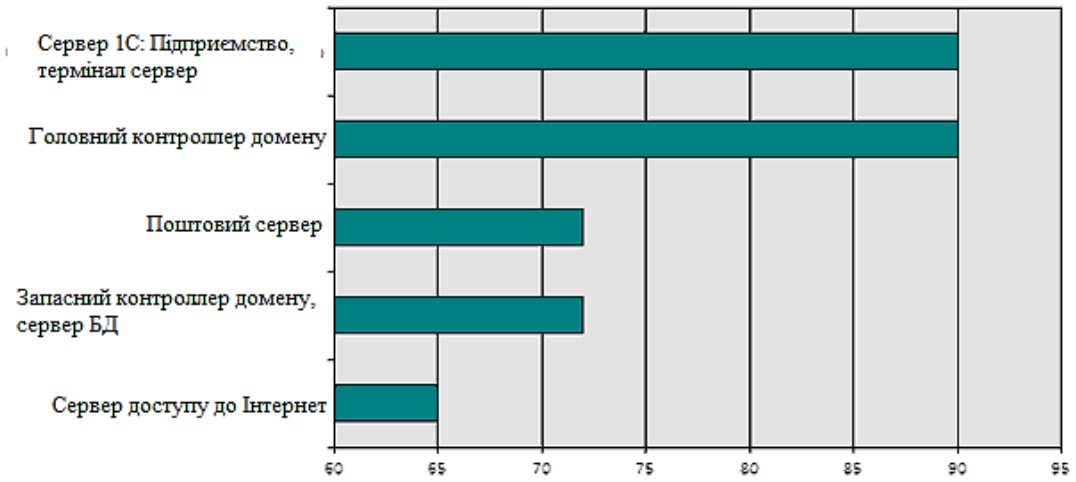

Рис. 3. Приклад графіку сумарних оцінок за активами [1]

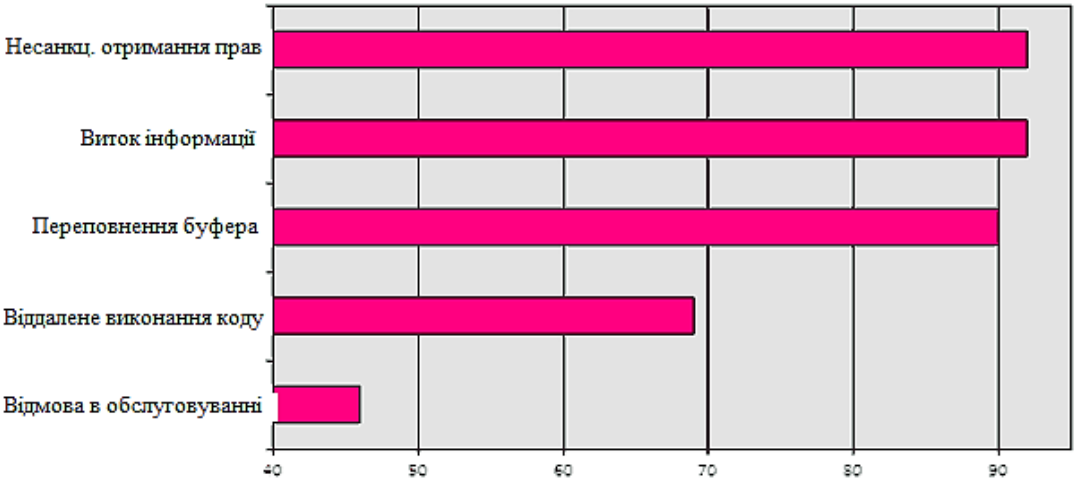

Рис. 4. Приклад графіку сумарних оцінок за загрозами [1]

10. Ранжування вразливостей кожного активу

Слід згрупувати вразливості по активах і вирахувати сумарні оцінки ризику для кожної вразливості кожного активу. Слід мати на увазі, що кожна вразливість може бути джерелом однієї або декількох загроз.

Сумарна оцінка ризику для вразливості вираховується для кожного активу, оскільки для однакових загроз активи мають різну цінність.

Числова сумарна оцінка ризику для вразливості конкретного активу обчислюється як сума оцінок ризиків від кожної загрози, джерелом якої є ця вразливість для цього активу:

$$V_a = \sum R_a = W_a \times \sum n_a \qquad (2)$$

де V_a - вразливість активу, R_a - ризик активу, W_a - збиток активу, n_a – частота загрози.

Приклад розрахунку числової сумарної оцінки ризику для однієї вразливості наведений в табл. 5.

Таблиця 5.

Приклад розрахунку числової сумарної оцінки ризику від вразливості активу «Головний контролер домену»

Вразливість	Загроза для даного активу	Оцінка ризику загрози для даного активу	Числова сумарна оцінка ризику вразливості
Не встановлені критичні оновлення Windows: MS04-012, MS08-061, MS08-063, MS08-064.	Несанкціоноване отримання прав	20	70
	Віддалене виконання коду	15	
	Відмова в обслуговуванні	10	
	Переповнення буфера	25	

Отримавши кількісні сумарні оцінки ризику для усіх вразливостей, відсортувати їх за спаданням, а потім перевести в словесні за рекомендованою шкалою оцінок, що представлена в табл. 6.

Таблиця 6.

Рекомендована шкала сумарних оцінок ризику вразливості

Числова сумарна оцінка ризику вразливості	Словесна оцінка	Опис для клієнта
>100	Критична	Несе найбільшу кількість загроз для даного активу; найбільший збиток у разі використання зловмисниками.
51-100	Важлива	Несе серйозні загрози і, ймовірно, буде використана зловмисниками.
25-50	Середня	Представляє небезпеку, проте її використання зловмисниками малоймовірно.
<25	Низька	Малоймовірні загрози, або мінімальний збиток.

Складання рекомендацій щодо усунення вразливостей та оформлення звіту

Скласти типові рекомендації по усуненню виявлених вразливостей на підставі офіційних документів (наприклад, стандартів ІБ або бюлетенів Microsoft). Потім, доповнити рекомендації на підставі думок і досвіду експертів перевіряючої сторони. Скласти таблиці вразливостей для кожного активу з колонками: Вразливість, Загрози, Важливість (словесна оцінка сумарного ризику вразливості), Рекомендації.

Скласти звіт з наступних розділів, що відображатимуть основні етапи оцінювання ризиків інформаційної безпеки за даною методикою:

1. Терміни, визначення і скорочення, використані в звіті.
2. Цілі та сфера дослідження.
3. Дослідження вразливостей: виявлені вразливості та зведені дані щодо оцінок ризиків.
4. Рекомендації щодо усунення вразливостей.
5. Додаткові розділи (за потреби).
6. Загальні висновки.

Таким чином, запропонована методика оцінювання захищеності ІС за допомогою СУІБ «Матриця» забезпечує отримання кількісних оцінок стану ІБ і оцінку ефективності функціонування СУІБ. В свою чергу, завдяки кількісним оцінкам забезпечується точний вибір пріоритетів в усуненні вразливостей ІБ, в підвищенні можливостей управлінні ними і в забезпеченні ефективності управління безпекою підприємства в цілому. Запропонована методика є універсальною з точки зору розміру та профілю підприємства [1].

Висновки

У статті показано, що використання ризикоорієнтованого підходу в дослідженні управлінських процесів в СУІБ має істотні переваги в порівнянні з іншими підходами. Розкрита сутність СУІБ, як цілісний механізм, в якому об'єднуються всі засоби, методи та заходи, що використовуються для захисту інформації. СУІБ сприймається іноді як варіант у вигляді документованої системи управління, яка визначена в рамках підприємства. Показано структурне включення в таку СУІБ, в якої виділені головні місця Політиці інформаційної безпеки і оцінці та аналізу ризиків безпеки.

Проведено дослідження з використанням системного підходу в управлінні інформаційною безпекою підприємства. Для практичної реалізації дослідження була застосована система управління інформаційною безпекою і програма СУІБ «Матриця». Процедура використаної методики заснована на оцінці ризиків ІБ, за допомогою якої було отримана кількісна оцінка стану ІБ і оцінка ефективності функціонування СУІБ на прикладі. В свою чергу, завдяки кількісним оцінкам забезпечується точний вибір пріоритетів в усуненні вразливостей ІБ, в підвищенні можливостей управлінні ними і в забезпеченні ефективності управління безпекою підприємства в цілому.

Застосування напрацювань статті дає змогу здійснити обґрунтований вибір методів і засобів в проведенні досліджень, спрямованих на розробку і вдосконалення системи управління інформаційною безпекою у відповідності до цілей бізнесу, можливостей та ресурсів будь-якого підприємства.

Перелік посилань

1. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ «Матриця». URL: http://www.epos.ua/view.php/about_pubs_archive

2. Управление безопасностью предприятий в условиях рыночной экономики URL: http://bezopasnik.org/article/60.htm

3. Информационные технологии - Методы и средства обеспечения безопасности Системы менеджмента информационной безопасности – Общие сведения и словарь. URL: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2014.pdf

4. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник / Ю.М.Якименко, В.А. Савченко, С.В. Легомінова//. Київ: ДУТ, 2022. -308 с.

Надійшла: 10.06.2022 Рецензент: д.т.н., професор Савченко В.А.