Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Інтеграція методів причинно-наслідкового зв'язку та SWOT-аналізу щодо визначення інформаційних ризиків
(тема)

Виконав:
студентка 2 курсу, групи АМСЗІм-18-1
Подоляка Н.В.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського Добринін І.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2020 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентці Подоляці Наталії Віталіївні .
(прізвище, ім'я, по батькові)

1. Тема роботи: Інтеграція методів причинно-наслідкового зв'язку та SWOT-аналізу щодо визначення інформаційних ризиків.
затверджена наказом по університету від «17» березня 2020 р. № 465 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 10.05.2020 р.
3. Вихідні дані до роботи: сучасні методики оцінки інформаційних ризиків; методика факторного аналізу інформаційних ризиків; міжнародний стандарт ISO/IEC 31010; методика впровадження систем менеджменту інформаційної безпеки компанії IT-Grundshutz, SWOT-аналіз, міжнародний стандарт ISO/IEC 27001:2013
4. Перелік питань, що потрібно опрацювати в роботі:
1) Вимоги міжнародних стандартів щодо оцінки ризиків при створенні та функціонуванні систем менеджменту інформаційної безпеки
2) Аналіз сучасних підходів до визначення ризиків
3) Обґрунтування використання SWOT-аналізу для ідентифікації інформаційних ризиків
4) Інтеграція методів оцінки ризиків та SWOT-аналізу

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Добринін Ігор Станіславович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	17.02.2020	Виконано
2	Збір матеріалів для дослідження	28.02.2020	Виконано
3	Розробка 1 розділу	19.03.2020	Виконано
4	Розробка 2 розділу	03.04.2020	Виконано
5	Розробка 3 розділу	20.04.2020	Виконано
6	Розробка 4 розділу	01.05.2020	Виконано
7	Оформлення атестаційної роботи	10.05.2020	Виконано

Дата видачі завдання 17 лютого 2020 року

Студентка _____ Подоляка Н.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Добринін І.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 с., 5 рис., 13 табл., 1 додаток, 18 джерел.

ІНФОРМАЦІЙНА БЕЗПЕКА, ОЦІНКА РИЗИКІВ, ЗАГРОЗА, ВРАЗЛИВІСТЬ, SWOT-АНАЛІЗ, СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Об’єкт дослідження – процес створення та функціонування системи менеджменту інформаційної безпеки.

Предмет дослідження – ризики інформаційної безпеки.

Мета дипломної роботи – ідентифікація інформаційних ризиків на підставі використання SWOT-аналізу та методу причинно-наслідкових зв'язків.

Методи дослідження: емпіричний аналіз, формалізація та порівняння.

Дипломна робота присвячена всебічному аналізу існуючих підходів до оцінки ризиків інформаційної безпеки та підходів до створення та впровадження системи менеджменту інформаційної безпеки. Пропонується порівняння методологій кількісної та якісної оцінок ризиків інформаційної безпеки на підставі методології FAIR, OCTAVE, NIST, стандарту ISO/IEC 31010 та методу причинно-наслідкових зв'язків.

ABSTRACT

The report contains: 69 p., 5 fig., 13 tables, 1 aplication, 18 sources.

INFORMATION SECURITY RISK ASSESSMENT, THREAT, VULNERABILITY, SWOT-ANALYSIS, INFORMATION SECURITY MANAGEMENT SYSTEM.

A research object is a process of creation and functioning information security management system.

The subject of research is information security risks.

The purpose of the work is identification of information risks based on the use of SWOT-analysis and method of causation.

Methods of researches are empirical analysis, formalization and comparison.

The bachelor work is devoted to a comprehensive analysis of existing approaches to assessing information security risks. It is proposed to compare the methodologies of quantitative and qualitative information security risk assessments based on FAIR, OCTAVE, NIST, ISO/IEC 31010 and causation methodologies.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЄС – Європейський Союз
ІБ – інформаційна безпека
ІС – інформаційна система
НБУ – Національний банк України
ПЗ – програмне забезпечення
СМІБ – система менеджменту інформаційної безпеки
ЦО – цільові об’єкти
CISO – Chief Information Security Officer
FAIR – Factor Analysis of Information Risk
ISO – International Organization for Standardization
OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation

ВСТУП

Аналіз стандартів у сфері інформаційної безпеки свідчить про те, що створення ефективної системи менеджменту інформаційної безпеки (СМІБ) неможливе без ідентифікації та оцінки ризиків. Проте, в стандартах чітко не вказано, яким шляхом необхідно виконувати вказані процедури. Тобто, як державні, так і міжнародні стандарти не дають конкретної відповіді на те, яку саме методику слід використовувати. Зазвичай, це завдання покладається на керівників підприємств, або осіб, відповідальних за розробку, впровадження та підтримку СМІБ.

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

Метою дипломної роботи є ідентифікація інформаційних ризиків на підставі використання SWOT-аналізу та методу причинно-наслідкових зв'язків.

Для вирішення поставленої задачі, в першому розділі атестаційної роботи проведено ретельний аналіз популярних підходів до побудови систем менеджменту інформаційної безпеки.

Розглянуті найбільш вживані методології розробки та впровадження СМІБ, а саме:

– методологія, що надана у міжнародному стандарті ISO/IEC 27003:2017;

– методологія розробки та впровадження СМІБ від німецького федерального відомства з інформаційної безпеки BSI IT-Grundschutz;

– методологія розробки та впровадження СМІБ Національного банку України.

У другому розділі роботи проведено аналіз основних сучасних методик оцінки ризиків. Окреслено переваги та недоліки кожної з методик, надано певні рекомендації щодо їх застосування та передбачувані похибки в оцінці ризиків при розрахунку за цими методиками. Також проаналізовано одну з найбільш перспективних, за оцінками фахівців з інформаційної безпеки, методик оцінки ризиків - методологію FAIR. Показано, що розглянута методологія FAIR надає обґрунтовану і логічну основу для оцінки інформаційних ризиків.

У третьому розділі роботи розглянуто основні підходи, які використовуються при проведенні SWOT-аналізу, обґрунтовано його доцільність використання для оцінки інформаційних ризиків, а також розглянуті пов’язані зі SWOT-аналізом підходи, а саме SNW-аналіз, аналіз п’яти сил Портера та PEST-аналіз.

У четвертому розділі роботи проведена ідентифікація ризиків інформаційної безпеки технології «Розумного будинку» методом SWOT-аналізу, а також відображений результат методу причинно-наслідкових зв’язків на основі проведеного аналізу у вигляді діаграми Ісікави. В результаті була проведена комплексна ідентифікація інформаційних ризиків, яку доцільно використовувати разом з методологією FAIR для досягнення комплексної оцінки ризиків.

Окремі результати роботи опубліковано у [1 – 5].

1 ВИМОГИ МІЖНАРОДНИХ СТАНДАРТІВ ЩОДО ОЦІНКИ РИЗИКІВ ПРИ СТВОРЕННІ ТА ФУНКЦІОНУВАННІ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасному інформаційному світі щороку все більше уваги приділяється забезпеченню інформаційної безпеки та безпеці інформаційних технологій.

Дійсно, інформація є найважливішим стратегічним ресурсом не лише будь-якої країни, але й будь-якого бізнесу чи особи. А створення повноцінного та дієвого механізму забезпечення інформаційної безпеки стає можливим лише при правильному підході до управління та захисту даних, адже в системі інформаційної безпеки потрібно враховувати всі актуальні на сьогоднішній день загрози і вразливості.

Саме тому вагомий внесок в структуризацію управління бізнес-процесами і процесами захисту підприємств становить створення і впровадження систем менеджменту інформаційної безпеки (СМІБ). СМІБ – це одна з основних частин загальної системи менеджменту, яка заснована на підході бізнес-ризиків при створенні, впровадженні, функціонуванні, моніторингу, аналізі, підтримці і поліпшенні інформаційної безпеки.

У даному розділі будуть розглянуті найпопулярніші на сьогодні підходи до побудови системи менеджменту інформаційної безпеки, а особлива увага буде приділена ролі оцінки ризиків у кожному з них. Для дослідження було обрано наступні методології розробки та впровадження СМІБ:

– міжнародні стандарти ISO/IEC 27001:2013 Information technology Security techniques Information security management systems Requirements та ISO/IEC 27003:2017 Information Technology Security Techniques Information Security Management Systems Guidance;

– методологія розробки та впровадження систем менеджменту інформаційної безпеки німецького федерального відомства з інформаційної безпеки BSI IT-Grundschutz;

– вимоги Національного Банку України до побудови систем менеджменту інформаційної безпеки.

1.1 Аналіз вимог міжнародних стандартів ISO/IEC 27001:2013 та ISO/IEC 27003:2017 щодо створення систем менеджменту інформаційної безпеки

Стандартом ISO/IEC 27001:2013 визначаються вимоги для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи менеджменту інформаційною безпекою з урахуванням особливостей конкретної організації [6].

Цей стандарт призначений для забезпечення конфіденційності, цілісності та доступності інформації компанії (трьох принципів управління інформацією), а також спрямований на дотримання вимог законодавства. Це реалізується шляхом з'ясування потенційних проблем з інформацією, тобто оцінки ризиків, а потім визначення необхідних кроків для запобігання появи таких проблем, тобто зниження або обробки ризиків.

Даний стандарт є найбільш поширеним та фундаментальним підґрунтям при побудові СМІБ в усьому світі. Вимоги, викладені в ISO / IEC 27001 є загальними і призначені для застосування всіма організаціями, незалежно від їх типу, розміру і характеру. Структура і ризики кожної організації унікальні, внаслідок цього її специфічні вимоги впливають на впровадження СМІБ.

Відповідно до рекомендацій стандарту, СМІБ включає в себе повний комплекс дій по забезпеченню інформаційної безпеки, в тому числі організацію діяльності та управління ризиками, а також безпосереднє застосування заходів захисту інформації.

У стандарті ISO/IEC 27003:2017 знаходимо загальні керівні вказівки до найважливіших аспектів успішного проектування і впровадження СМІБ відповідно до вимог ISO/IEC 27001. Даний стандарт описує процес від початку проектування СМІБ і до розробки планів її впровадження.

Стандарт ISO/IEC 27003:2017 містить опис процесу отримання дозволу керівництва на впровадження СМІБ, специфікований проект впро- вадження СМІБ, а також надає рекомендації з планування проекту впровадження СМІБ.

Тобто метою цього стандарту є надання практичної допомоги при реалізації СМІБ у межах організації відповідно до загальної методології підходу забезпечення інформаційної безпеки в організації, описаної в стандарті ISO/IEC 27001.

Впровадження СМІБ є особливим видом діяльності організації і, зазвичай, виконується як проект. Стандарт ISO/IEC 27003:2017 описує процеси

впровадження СМІБ, при цьому особлива увага зосереджена на процесах ініціації, планування і визначення проекту. Процес остаточного планування впровадження СМІБ підрозділяється на п'ять наступних фаз, що мають схожу структуру:

- отримання дозволу керівництва на ініціацію проекту СМІБ;
- визначення області дії і політики СМІБ;
- проведення аналізу організації;
- виконання оцінки ризиків та планування їх обробки;
- проектування СМІБ.

Робити вибір тих чи інших способів захисту інформації слід на основі оцінки ризиків ІБ, тобто розміру можливих збитків від реалізації загроз конфіденційності, цілісності та доступності інформації. І, звичайно, виходячи з необхідності виконання нормативних зобов'язань перед державою, партнерами та іншими зацікавленими сторонами. Тому основна філософія ISO 27001 базується на управлінні ризиками: з'ясувати, де знаходяться ризики, а потім систематично обробляти їх.

Також саме оцінка ризиків є, мабуть, найбільш складною частиною впровадження ISO/IEC 27001:2013, але в той же час оцінка ризиків (а також їх обробка) є найбільш важливим кроком на початку кожного проекту побудови СМІБ в організації, так як він встановлює основи для інформаційної безпеки у будь-якій компанії.

Отже, спираючись на рекомендації стандарту ISO/IEC 27001:2013, можна точно сказати, що ключовим фактором в побудові ефективної СМІБ прийнято вважати саме пошук інцидентів, які можуть статися (тобто оцінка ризиків) і потім виявлення найбільш підходящих шляхів запобігання таких інцидентів, тобто обробка ризиків.

Крім того, необхідно оцінити важливість кожного ризику таким чином, щоб визначити їхню пріоритетність та мати можливість сфокусуватися на найбільш важливих ризиках. Відповідно до стандартів, які розглядаються, можна виділити 6 основних кроків, які необхідні для ефективного управління ризиками.

1) Методика оцінки ризиків.

Почати потрібно з визначення правил, за якими компанія в майбутньому буде виконувати управління ризиками, так як різні рівні, частини організації, а також її структурні підрозділи мають оцінювати ризики одним способом. Тому необхідно

визначити, буде це якісне чи кількісне оцінювання ризиків, які шкали будуть використовуватися для якісної оцінки, що буде прийнятним рівнем ризиків і т.д.

2) Впровадження оцінки ризиків.

У зв'язку з тим, що оцінювання ризиків інформаційної безпеки здійснюється стосовно до активів, пов'язаних із засобами, які опрацьовують інформацію, то перш за все, необхідно визначити та перерахувати всі активи компанії, а також усі потенційні загрози і вразливості, оцінити вплив і ймовірність для кожної сукупності актив - загроза - вразливість і, в кінцевому рахунку, обчислити рівень ризику.

3) Впровадження обробки ризиків.

Не всі виявлені ризики однаково важливі, а отже необхідно шляхом пріоритезації визначити найважливіші з них, вплив на які може завдати відчутної шкоди діяльності конкретної організації. І, відповідно, сфокусуватися на цих неприйнятних ризиках.

Далі розглянемо 4 варіанти, один з яких може бути обраний для нейтралізації кожного неприйнятного ризику:

– застосування засобів управління безпекою з Додатка А стандарту з метою зниження ризиків;

– передача ризику іншій стороні (наприклад, страховій компанії шляхом покупки страхового поліса);

– ухилення від ризику шляхом припинення діяльності, яка занадто ризикована, або шляхом виконання її повністю в іншій формі;

– прийняття ризику (наприклад, якщо вартість зниження даного ризику вища, ніж потенційно нанесений ним збиток).

На даному етапі необхідно обрати той з варіантів зниження ризику, який потребує мінімальну кількість ресурсів, тобто буде найоптимальнішим для організації.

4) Звіт з оцінки ризиків СМІБ.

Даний етап передбачає формування звіту, в якому задокументовано усі попередні кроки. Він може знадобитися як для аудиторської перевірки, так і для контролю та перевірки власних результатів.

5) Положення щодо застосовності.

Цей документ насправді показує профіль безпеки конкретної компанії - ґрунтуючись на результатах обробки ризиків необхідно перерахувати всі

впроваджені засоби управління безпекою, обґрунтувати їх доцільність та описати процес впровадження. Дане положення також є дуже важливим, тому що використовується в якості основного документу при проведенні аудиту.

6) План оброблення ризиків.

Розробка даного плану передбачає чітко визначити, хто буде впроваджувати кожен із засобів управління безпекою, в який проміжок часу, з яким бюджетом і т.д. Після цього необхідно отримати згоду власників ризиків на підтвердження плану оброблення ризиків інформаційної безпеки в організації.

Підсумовуючи, варто зазначити, що оцінка ризиків та їх обробка в системі управління інформаційною безпекою, побудованою на основі стандарту ISO 27001, є ключовим фактором успішної та ефективної роботи СМІБ в організації.

1.2 Аналіз методології розробки та впровадження системи менеджменту інформаційної безпеки IT-Grundschutz

IT-Grundschutz – це методика створення системи менеджменту інформаційної безпеки, розроблена німецьким федеральним відомством з інформаційної безпеки BSI [7].

Методологія IT-Grundschutz призначена для організацій будь-яких розмірів і типів (наприклад, для компаній, державних органів, інших державних та приватних організацій).

Її основне завдання – досягнення належного рівня захищеності інформації, наявної в організації. При цьому IT-Grundschutz використовує цілісний підхід. Для того, щоб досягти надійного рівня безпеки, що відповідає вимогам захисту інформації, що стосується бізнесу, необхідно реалізувати належне поєднання стандартних організаційних, кадрових, інфраструктурних та технічних гарантій безпеки.

Щоб надати організаціям допомогу у процесі визначення і впровадження заходів для захисту IT-систем, Федеральне управління з інформаційної безпеки (Bundesamt für Sicherheit in der Informationstechnik або BSI) розробило базовий набір стандартів щодо захисту інформаційних технологій (по-німецьки: IT-Grundschutz). До цих стандартів BSI входить:

– система менеджменту інформаційної безпеки (СМІБ) на основі стандартів ISO / IEC 27001 (стандарт BSI 200-1);

– методологія IT-Grundschutz, що описує налаштування і використання СМІБ (стандарт BSI 200-2);

– метод аналізу ризиків (стандарт BSI 200-3);

– каталоги IT-Grundschutz - стандартний набір потенційних загроз і заходів захисту від них для типовиого бізнес-середовища.

Методика BSI-Standard 200-3 аналізу ризиків включає сім етапів:

– попередня підготовка;

– підготовка опису загрози;

– визначення додаткових загроз.

– оцінка загрози (ОУ);

– обробка ризиків;

– консолідація концепції ІБ;

– зворотній зв'язок.

На першому етапі визначається область ІБ, вимоги до неї (нормальні, високі і дуже високі), які розглядаються з точки зору забезпечення конфіденційності, цілісності і доступності інформації. Також проводиться аналіз структури підприємства, додатковий аналіз ІБ, оцінюється її поточний рівень. За допомогою запропонованого в методиці списку загроз здійснюється їх аналіз для конкретного підприємства. Ідентифікуються модулі та цільові об'єкти (ЦО) захисту, які заносяться в таблицю. Вихідні дані. Кожен модуль пов'язаний зі списком загроз, а номер і їх назва відповідає конкретному ЦО. Результатом проходження етапу є список загроз конкретного об'єкта. Далі в узагальненій таблиці загрози упорядковано відповідно до кожного ЦО.

IT-Grundschutz додержується модульного підходу для покращення підготовки і структурування сильно неоднорідної області інформаційних технологій. Кожен модуль відображає типовий робочий процес у бізнес-процесах та області застосування IT. Всі модулі починаються з опису сценарію загрози, що очікується, при цьому включають описи типових загроз й загальні оцінки ймовірності їх появи.

Сценарій загрози - це основа для створення певного пакету гарантій безпеки для галузей інфраструктури, персоналу, організації, апаратного та програмного забезпечення, зв'язку та планування в разі надзвичайної ситуації.

Підхід IT-Grundschutz спрощує та робить ефективним процес складання концепцій безпеки IT. Якщо застосовувати традиційний аналіз ризику, то основні

загрози спочатку визначаються, а потім оцінюються з ймовірністю виникнення, щоб згодом можна було обрати певні гарантії безпеки і пізніше оцінити залишковий ризик.

В IT-Grundschutz ці кроки вже виконано для кожного модуля, й певні гарантії безпеки вже вибрані для типових сценаріїв застосування. При запровадженні IT-Grundschutz виконується аналіз шляхом цільового фактичного порівняння запобіжних засобів, рекомендованих в Каталогах IT-Grundschutz , та тими, що вже були впроваджені. Якщо будуть відсутні або ще не реалізовані гарантії, виявлені при цьому, то це буде вказувати на усування недоліків у безпеці за допомогою запропонованих гарантій. Але там, де підвищені вимоги до захисту, необхідно буде провести додатковий аналіз безпеки, ураховуючи економічну ефективність запровадження додаткових заходів. Але в даному випадку, зазвичай, достатнім буває доповнити гарантії, рекомендовані в Каталогах IT-Grundschutz, відповідними індивідуальними, більш якісними запобіжними засобами. Нескладний підхід для виконання цього описано у BSI Standard 200-3 Аналіз ризиків на основі IT-Grundschutz.

Каталоги IT-Grundschutz є цінною допомогою навіть для спеціальних компонентів чи середовищ додатків, що спеціально не оброблюються в Каталогах ITGrundschutz . Після цього необхідний додатковий аналіз можливо зосередити безпосередньо щодо конкретних загроз та гарантй безпеки для цих компонентів чи загальних умовах.

Перелічені в Каталогах IT-Grundschutz захисні засоби – це стандартні запобіжні засоби, тобто захисні засоби, які застосовуються щодо відповідних модулів згідно до нинішнього рівня техніки, реалізація якого необхідна для досягнення надійного базового рівня безпеки. При цьому, гарантії, що необхідні для отримання сертифікації відповідно до ISO 27001 на базі IT-Grundschutz , є мінімум з того, що повинно бути адекватно впроваджено у сфері гарантій безпеки. Ті засоби безпеки, що визначені "додатковими", теж практично підтвердили свою надійність, але спрямовані на застосування із більш високими вимогами до захисту.

Ті концепції безпеки, що засновані на IT-Grundschutz, зазвичай дуже компактні за своєю конструкцією, оскільки необхідно лише посилання на відповідні гарантії в Каталогах IT-Grundschutz в межах цієї концепції. Це забезпечує зрозумілість і чіткость понять. Для полегшення реалізації запропонованих гарантій, гарантії безпеки детально описані в Каталогах IT-

Grundschutz. При умові використання технічної термінології гарантується, що пояснення можуть зрозуміти ті, хто потребує запровадження гарантій.

Для того, щоб спростити запровадження гарантій Каталоги IT-Grundschutz, як і багато іншого, що стосується IT-Grundschutz , теж доступно в електронному вигляді. Крім цього, надаються ресурси та зразки рішень, які будуть корисними при запровадженні гарантії. Деякі з них були надані BSI, а деякі – отримані від користувачів ITGrundschutz.

Так як сфера IT занадто інноваційна й стрімко розвивається, то теперішні каталоги розроблені так, що їх можливо легко оновити та розширити. Федеральне управління з питань інформаційної безпеки постійно оновлює каталоги IT-Grundschutz та додає до них нові теми на основі відповідей на опитування користувачів.

BSI надає можливість кожному користувачу добровільно та безкоштовно зареєструватися. Користувачі, що зареєструвалися, постійно отримують інформацію стосовно актуальних тем щодо IT-Grundschutz й інформаційної безпеки. Реєстрація потрібна й для участі в опитуваннях користувачів. Каталоги можна переглядати та оновлювати лише за необхідності за допомогою безперервного обміну досвідом з користувачами IT-Grundschutz . Остаточна мета цих зусиль - це можливість показати актуальні рекомендації для вирішення типових проблем інформаційної безпеки. Рекомендовані гарантії, якщо вони не оновлюються та не розширюються постійно, дуже швидко застарівають.

Досвід показує, що стабільний рівень безпеки фактично неможливо мати без належного функціонування управління СМІБ. Тому стандарт BSI 200-1 "Системи управління інформаційною безпекою (ISMS)" описує, що має забезпечувати така система управління та завдання, що пов'язані з нею.

Кожен з модулів IT-Grundschutz містить стислий опис компонентів, що застосовуються, підходи та IT-системи, а також огляд сценарію загрози і запропоновані запобіжні заходи. Самою важливою частиною кожного модуля є розділ, що містить рекомендовані заходи безпеки.

У кожному модулі огляд теми розглянуто у вигляді життєвого циклу, де описано, які гарантії повинні бути реалізовані на якому етапі і з якою метою. Типові завдання, які будуть виконуватися для кожної гарантії в кожній з цих фаз вказані в таблиці 1.1.

Таблиця 1.1 – Етапи розробки, впровадження та експлуатації систем менеджменту інформаційної безпеки у відповідності з методологією IT-Grundschutz

Фаза	Типові завдання
Планування і проектування	Визначення й призначення. Специфікація експлуатаційних сценаріїв. Оцінка потенційного ризику. Документування прийнятих рішень. Створення концепції безпеки. Специфікація керівних принципів для використання.
Придбання (при необхідності)	Технічні вимоги щодо обладнання, яке буде придбане. Вибір відповідних продуктів.
Реалізація	Проектування і виконання тестових операцій. Установка і настройка відповідно до політики безпеки. Навчання і підвищення обізнаності для всіх тих, хто бере участь.
Операція	Гарантії безпеки для роботи персоналу. Постійне технічне обслуговування і уточнення. Управління змінами. Організація і проведення робіт з технічного обслуговування. Аудит.
Завершення терміну експлуатації (при необхідності)	Висновки щодо дозволів. Видалення ресурсів, даних та посилання на ці дані. Безпечне видалення носіїв даних.
Розподіл ресурсів	Проектування і організація резервного копіювання даних. Використання надлишкового обладнання для підвищення доступності. Поводження з інцидентами безпеки. Створення аварійного плану.

Управління безпеки і аудит впливають на всі фази, оскільки вони супроводжують і контролювати весь життєвий цикл.

Варто зазначити, що стандарт BSI IT-Grundschutz базується на основі стандарту ISO/IEC 27001, проте має більш поглиблену деталізацію процесів та процедур розробки, впровадження та підтримки функціювання СМІБ.

В той час як ISO/IEC 27001 зосереджується саме на процесі захисту інформації. Відповідні нормативні документи досить дефіцитні, не маючи навіть 50 сторінок тексту. Для компанії досить суттєво знайти та впровадити відповідні процедури та заходи, щоб знизити ідентифіковані та проаналізовані ризики до прийнятного рівня. Стандарт передбачає для цього 114 заходів, але усі вони досить не деталізовані.

Таким чином, процедура забезпечує більшу повноту у досягненні рівня захисту, який фактично є необхідним для власних потреб. Необхідно, однак, детально розробити дуже загальні специфікаційні норми та наповнити їх відповідним змістом. Основним є детальний аналіз ризиків та їх обробка. Саме для цього необхідні зусил-ля та ресурси значні.

Звичайно, стандарт, заснований на IT- Grundschutz, є альтернативою ISO/IEC 27001, адже також розглядає процеси захисту інформації. Проте типові загрози уже оцінені і викладені у кількох тисячах сторінок каталогів Grundschutz. Там також рекомендується велика кількість конкретних заходів для адекватного протидії таким загрозам. Лише коли йдеться про області, в яких є більша потреба у захисті, все ж потрібно провести власний аналіз загроз та ризиків та вжити додаткових або кардинально інших заходів захисту.

Методика IT-Grundschutz дозволяє створити СМІБ, яка відповідає вимогам ISO/IEC 27001, оскільки ця методика повністю сумісна з підходами, використаними в стандарті 27001. Проте методика IT-Grundschutz описує деякі питання, порушені в стандарті, більш детально і тому представляє більш дидактичний підхід для організацій, які впроваджують у себе СМІБ.

Методика IT- Grundschutz має значний потенціал для економії ресурсів при визначенні необхідних заходів, оскільки це виключає необхідність в повному аналізі ризику та розробці власних заходів. До того ж схематизація процедури дозволяє уникнути помилок у здійсненні.

Крім того, досягається об'єктивний рівень безпеки, окреслений методологією шляхом порівняння його з фактичним рівнем безпеки організації. Однак весь спектр питань, які слід розглянути, є значно ширшим, ніж у стандарті ISO/IEC 27001. Для порівняння стандартів ISO/IEC 27001та BSI IT-Grundschutz базові характеристики кожного з них зведені до таблиці 1.2.

Таблиця 1.2 – Відмінності між ISO/IEC 27001 та BSI-Grundschutz

ISO / IEC 27001	BSI IT-Grundschutz
Відповідні стандарти менше 50 сторінок	Каталоги GS на понад 4000 сторінок
Загальний підхід	Підхід, орієнтований на дії
Абстрактні вимоги до СМІБ	Конкретні вимоги до СМІБ
Потрібний повний аналіз ризику	Аналіз ризику лише з підвищеними вимогами до захисту

Безперечно в Україні є сенс сертифікувати СМІБ по міжнародному стандарту ISO/IEC 27001, в той же час федеральний стандарт BSI-Grundschutz використовувати виключно для полегшення процесу роботи над розробкою, впровадженням та підтримкою СМІБ.

1.3 Аналіз підходів Національного банку України до побудови систем менеджменту інформаційної безпеки

Згадаємо 2017 рік, який став переломним, а також дуже складним у розвитку банківської системи України. Навесні того року велика кількість банків були заражені глобальним вірусом-шифрувальником WannaCry, який масово вразив машини з операційною системою Microsoft Windows. Наслідком дії цієї шкідливої програми було масове виведення із ладу робочих місць касирів, менеджерів, операціоністів та інших банківських службовців.

Виглядає, що уже після цього випадку усі постраждалі банки мали прийняти низку рішень, які б стали поштовхом для впровадження серйозних заходів для підвищення захищеності банківських систем і мереж, а також для запобігання подібних атак в майбутньому.

Проте фактично реальність досить суттєво відрізнялась від наведеного вище очікуваного переліку подій, адже уже за кілька місяців вірус Petya.A вразив 70% банківської інфраструктури України. Даний інцидент призвів до фактичної зупинки роботи частини ключових банків, адже вони кілька годин не могли проводити платежі.

У ході цієї атаки постраждали не тільки робочі місця банківських службовців, як це сталося під час попередньої атаки, а й сервери та бази даних банківських установ, що звичайно є більш небезпечним та тягне за собою серйозні наслідки. Адже навіть через місяць після проведеної атаки вірусу Petya.A деякі банки продовжували роботи з відновлення порушених бізнес-процесів та втрачених даних.

І лише після цієї масштабної хакерської атаки, яка нанесла сильний удар банківській системі України в цілому, а також привернула значну увагу громадськості, Національний банк України (НБУ) почав розробку низку заходів, які в майбутньому дозволяли б запобігти подібним ситуаціям.

Результатом цієї роботи стало прийняття постанови №95 правлінням Національного банку України 28.09.2017, якою було затверджено Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [8].

Постановою № 95 вперше передбачається регулювання Національним банком питань безпеки інформації та кіберзахисту банківської системи України шляхом визначення обов'язкових вимог щодо організації заходів інформаційної безпеки, які поетапно мають впроваджуватися банками.

Вимоги, які наявні у постанові НБУ № 95, не є повністю оригінальною розробкою Національного банку України, адже їх джерелом послугували Міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002, PCI DSS, а також деякі із попередніх постанов НБУ, присвячені питанням інформаційної безпеки.

Дана постанова заснована на основі міжнародного стандарту ISO/IEC 27001:2013 і містить в собі 150 вимог щодо впровадження в банках інформаційної безпеки. Вона розроблена з метою вдосконалення вимог щодо захисту інформації в інформаційних системах банків з урахуванням актуальних кіберзагроз. Вимоги, викладені в постанові НБУ №95 передбачають області ІБ, зображені на рисунку 1.1.

Постановою № 95 також визначається поняття критичних бізнес-процесів банку з точки зору інформаційної безпеки та сфера застосування банками системи менеджменту інформаційної безпеки (СМІБ).

Крім того, відповідно до провідного світового досвіду з питань інформаційної безпеки, документ передбачає призначення в банках відповідальної особи за інформаційну безпеку (Chief Information Security Officer, CISO) та наділення її повноваженнями, достатніми для прийняття управлінських рішень.

Рисунок 1.1 – Області інформаційної безпеки, передбачені постановою Національного банку України №95

Також банки повинні сформувати окремі підрозділи з інформаційної безпеки виключно зі штатних працівників банку, які безпосередньо підпорядковуються CISO.

Далі розглянемо основні аспекти, які необхідно впровадити банку в свою інфраструктуру відповідно до постанови № 95.

1) Система захисту від вірусів та сучасних шпигунських програм. При цьому антивірусне програмне забезпечення повинно бути встановлено на всіх комп'ютерах і серверах банку.

2) Контроль використання змінних носіїв, таких як флешки, переносні жорсткі диски і т.д. Ця система повинна забезпечувати сувору ідентифікацію всіх тих, хто підключається до комп'ютерів банку, пристроїв зберігання інформації.

Основне завдання системи - запобігти несанкціонованому копіюванню банківських документів на змінні носії.

3) Системи контролю мережевого доступу. Ці системи відомі під іншими назвами: міжмережні екрани, фаерволи, брандмауери. Їх основне завдання - розділяти мережу банку на ізольовані сегменти і контролювати обмін даними між ними. Це дозволяє запобігти мережевим атакам і поширенню вірусів.

4) Система запобігання атак. Вона має виконувати постійний аналіз даних, що циркулюють в мережі, виявляти мережеві атаки і повідомляти про них фахівцям служби інформаційної безпеки. Особливо важливо, щоб така система виконувала моніторинг трафіку по периметру мережі банку.

5) Система захисту від атак, спрямованих на відмову в обслуговуванні. Такі атаки в теперішній час дуже поширені, і вони з легкістю можуть заблокувати роботу будь-якого банку, тому для захисту від них необхідно встановити спеціалізоване обладнання.

6) Система контролю підключення до банківської мережі. Така система повинна забезпечувати однозначну ідентифікацію обладнання при підключенні до мережі банку і блокувати роботу будь-яких сторонніх пристроїв, які не належать банку.

7) Система захисту електронної пошти. Всі вхідні й вихідні електронні листи банку необхідно перевіряти щодо вірусів, спаму, атак і несанкціонованого використання.

8) Система контролю інтернет-трафіку. Така система в банку повинна обмежувати доступ співробітників банку до тих сайтів, які можуть нести загрозу вірусного зараження або проникнення хакерів.

9) Система централізованого управління мережею банку. Вся мережа банку має управлятися з одного операційно-диспетчерського центру - Network Operation Centre.

10) Система централізованого управління параметрами операційних систем. Ті банки, де не впроваджена Microsoft Active Directory, зобов'язані використовувати її або аналогічні централізовані каталоги.

11) Система двофакторної аутентифікації. Співробітники банку при підключенні до будь-якої автоматизованої банківської системи, зобов'язані, крім імені та пароля, надавати смарт-карту або електронний ключ.

12) Централізована система управління обліковими записами. Така система забезпечує повну автоматизацію всього життєвого циклу облікових

записів користувачів. Функції, які реалізує ця система - надання, блокування і делегування доступу.

13) Система контролю адміністраторів. Така система дозволяє захиститися від атак і несанкціонованого доступу з використанням привілейованих облікових записів. Всі атаки останніх років, були успішні саме тому, що проникали в комп'ютери системних адміністраторів, а з них отримували доступ до всієї інфраструктури банку.

14) Система посиленого захисту серверів. Вона встановлюється на критичні сервери банку і дозволяє суттєво зміцнити їх захищеність від більшості атак за допомогою блокування будь-яких підозрілих дій.

15) Система підготовки тестових даних. За допомогою цієї системи є можливість сформувати набори деперсоніфікованих даних. Такі набори необхідно використовувати для тестування всіх банківських систем для того, щоб локалізувати можливість витоку реальних клієнтських даних.

16) Система моніторингу вразливостей і установки програмних оновлень. Завданням цієї системи є оперативне виявлення в мережі банку програмних вразливостей та надання допомоги фахівцям служби захисту інформації у їх закритті.

17) Система управління інцидентами інформаційної безпеки. Така система повинна дозволяти забезпечувати централізований збір інформації про всі події, що відбуваються в мережі банку, і своєчасно реагувати на позаштатні або підозрілі ситуації.

Впровадження норм, викладених у постанові НБУ № 95 дозволить:

– підвищити захищеність клієнтів, а також співробітників банку від актуальних кіберзагроз, встановивши для цього мінімально необхідні заходи захисту;

– підвищити рівень управління ІБ банківських установ, а також поглибити розуміння питань інформаційної безпеки керівництвом банку та всіма його співробітниками;

– проводити процес управління ризиками інформаційної безпеки з урахуванням специфіки банківського бізнесу;

– підвищити репутацію й інвестиційну привабливість банку.

Постанова №95 НБУ прийнята з метою удосконалення вимог до захисту інформації в інформаційних системах банків з урахуванням актуальних

кіберзагроз. Її норми відповідають принципам права Європейського Союзу та зобов’язанням України у сфері європейської інтеграції.

Документ визначає принципи забезпечення та управління інформаційною безпекою, які базуються на нових, уведених в дію з 01 січня 2017 року, національних стандартах України з питань інформаційної безпеки, та принципах забезпечення інформаційної безпеки і кіберзахисту, що притаманні міжнародній практиці.

Отже, спираючись, на обґрунтування, викладені у даному розділі, можна зробити висновок, що незалежно від того, яка саме система менеджменту створюється – система менеджменту якості, система менеджменту інформаційної безпеки чи будь-яка інша, незалежно від обраного підходу до її побудови, а найбільш популярні з них саме і були розглянуті в даному розділі, ми чітко бачимо, що оцінка ризиків являється фундаментом при побудові будь-якої з них. Адже ефективність процесів розробки, впровадження та функціонування СМІБ в організації першопочатково визначається саме точністю та повнотою аналізу і оцінкою факторів ризику.

2 АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ВИЗНАЧЕННЯ РИЗИКІВ

В основу сучасних стандартів у забезпеченні цілісності інформації закладений підхід, при якому здійснюється управління ризиками при їх наявності. Для того, щоб управляти цими ризиками, підприємству необхідно спочатку вибрати методику, за якою розраховувалася б оцінка ризиків. І цей крок, як правило, представляє складність з різних причин, адже не існує програмного комплексу, який би задовольняв за всіма параметрами.

Розвиток інформаційних технологій не стоїть на місці, а удосконалюється з кожним днем. Через це доводиться підвищувати і якість управління ризиками. Неминуче застарівають одні методики, інші - виникають і удосконалюються, в зв'язку з цим дуже важливо працювати з максимально актуальною на даний момент.

У результаті на ринку програм оцінювання ризиків сформувалися кілька постійних лідерів, які затьмарюють собою інші неефективні або рідко оновлюванні аналоги, а у самих методик з'являються відмінності, на яких і засновані всі переваги і недоліки програмних комплексів.

Так як обчислювальна мережа використовується на більшості підприємств, то актуальність проблеми інформаційної безпеки достатньо висока. В цьому розділі розглянемо і порівняємо основні системи аналізу інформаційних ризиків.

Призначення оцінки ризику полягає в забезпеченні отримання інформації та проведення аналізу на доказовій основі для прийняття обґрунтованих рішень про те, як обробляти конкретні ризики і як здійснювати вибір серед можливих варіантів.

Основні переваги, які дає змогу отримати проведення оцінки ризику, включають:

– забезпечення розуміння ризику та його потенційного впливу на цілі;

– надання інформації для осіб, які приймають рішення;

– поліпшення розуміння ризиків, що сприяє вибору варіантів їх обробки;

– можливість порівняння ризиків в альтернативних системах, технологіях або підходах;

– обмін інформацією про ризики і невизначеності;

– сприяння у встановленні пріоритетів;

– сприяння запобіганню нещасним випадкам, яке ґрунтується на розслідуванні минулих нещасних випадків;

– сприяння вибору серед різних форм обробки ризику;

– забезпечення відповідності обов'язковим вимогам;

– надання інформації, яка застосовується для оцінки можливості прийняття ризику при порівнянні з попередньо визначеними критеріями;

– оцінка ризиків, пов'язаних з утилізацією після закінчення терміну служби.

У наш час для вирішення задач з оцінки інформаційних ризиків можуть використовуватися кілька методологій. Найбільшу популярність завдяки масовому використанню здобули методологія OCTAVE, методологія NIST, методології, які зазначені в стандарті ISO/IEC 31010 та методологія FAIR. Стисло розглянемо основні підходи до оцінки ризиків, які були зазначені вище.

2.1 Аналіз методології OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation – "Оцінка операційно-критичних загроз, активів і вразливостей") – методика оцінки ризиків в організації особливістю якої є те, що весь процес аналізу проводиться силами самих співробітників організації, без залучення зовнішніх консультантів.

Методологія OCTAVE розроблена для організацій, які [9]:

– мають багатошарову ієрархію;

– підтримують свої власні обчислювальні інфраструктури;

– мають здатність запускати інструменти оцінки вразливості;

– мають здатність інтерпретувати результати оцінки вразливості.

Метод був розроблений з метою можливості подальшої адаптації організаціями, які прийняли його. Більшість організацій, які використовували метод OCTAVE адаптували підхід у відповідності зі своїми унікальними операційними середовищами.

При роботі з методологією OCTAVE відбувається активна участь власників інформації в процесі визначення найбільш незахищених інформаційних масивів та найбільш вірогідних ризиків. Методологія базується на послідовності спеціально організованих внутрішніх семінарів, а оцінка ризиків проводиться в три етапи,

перед якими пропонується узгодити графік семінарів, розпланувати дії учасників і призначити їм ролі.

Перший етап полягає в розробці профілів загроз, які відповідають мережі даної організації, а також законодавчій базі. На цьому етапі відбувається визначення інформаційних активів і їх важливості, а також стратегії їх захисту; ознайомлення з документами і вимогами безпеки і безпосередньо встановлення загроз, які можуть нанести шкоду інформаційним активам.

На другому етапі відбувається аналіз вразливостей систем підприємства по відношенню до загроз, профілі яких були складені на першому етапі.

Третій етап включає в себе оцінювання ризиків інформаційної безпеки, що полягає у встановленні ймовірності або ступеня заподіяння шкоди в разі здійснення загроз при існуючих вразливостях. Після закінчення проводиться прийняття рішень щодо обробки ризиків і розроблюється план зниження ризиків для критично важливих активів.

Отже, ключовими елементами OCTAVE є:

– ідентифікація критичних інформаційних активів;

– ідентифікація загроз для критичних інформаційних активів;

– визначення вразливостей, асоційованих з критичними інформаційними активами;

– оцінка ризиків, пов'язаних з критичними інформаційними активами.

OCTAVE передбачає високу ступінь гнучкості, яка досягається шляхом вибору критеріїв, які підприємство може використовувати при адаптації методології під власні потреби. Методологія розроблена для застосування у великих компаніях (300 і більше працівників), а її зростаюча популярність призвела до створення версії OCTAVE-S для невеликих підприємств (100 і менше працівників).

OCTAVE-S відрізняється від методу OCTAVE, так як він обслуговує більш дрібні організацій, які не мають достатньої кількості IT- персоналу або ресурсів для ефективного здійснення повномасштабної оцінки ризиків.

Згідно з посібником по впровадженню OCTAVE-S, невеликі організації отримають найбільшу вигоду від даного методу за умови, що команда, відповідальна за проведення процесу, складається всього з декількох чоловік, і ці люди володіють всіма знаннями, необхідними для виконання OCTAVE-S.

Існує ще один підхід - OCTAVE Allegro, який може бути використаний в умовах малого і середнього бізнесу, але він дещо відрізняється у виконанні. Так само, як OCTAVE та OCTAVE-S, OCTAVE Allegro спрямована на позиціонування оцінки ризиків в належному організаційному контексті.

Проте цей метод пропонує альтернативний підхід, спеціально направлений на інформаційні ресурси та їх пружність. Цей альтернативний підхід може поліпшити здатність організації до збереження інформаційних активів та виконувати оцінку ризиків шляхом, який надає результати більш ефективним і дієвим чином.

OCTAVE Allegro являє собою методологію, метою якої є спрощення і оптимізація процесу оцінки ризиків інформаційної безпеки. Разом з тим, організація може отримати достатні результати при невеликих затратах часу, людей і інших обмежених ресурсів.

Для аналізу ризиків по методиці OCTAVE Allegro пропонується підхід з восьми кроків:

- розробка критеріїв оцінки ризику;
- розробка переліку і профілю інформаційних активів;
- визначення місць зберігання і носіїв інформаційних активів;
- виявлення проблемних областей;
- визначення сценарію загроз;
- визначення ризику;
- аналіз ризику;
- визначення засобів обробки ризику.

Значною перевагою OCTAVE є адаптація методології до конкретних умов застосування, наприклад до розміру компанії, виду бізнесу, вимог законодавства та тих чи інших стандартів.

Хоча дана методика й реалізується вручну, без використання програмних засобів, проте аналітична команда, що складається з 3-5 чоловік, розглядає ризики організаційних активів в їх співвідношенні з цілями бізнесу, а кінцевим результатом методу є організаційно-спрямована стратегія безпеки і план щодо пом'якшення наслідків порушень ІБ. Проте відчутним моментом є і те, що при оцінці ризику дається тільки оцінка очікуваного збитку, без оцінки ймовірності.

В ідеалі необхідно отримати не тільки задовільні результати оцінювання, а й зручний у використанні програмний комплекс, який би був інструментом при

такому оцінюванні. Зрозуміле бажання власників таких підприємств отримати не лише ясні результати дослідження, а також рекомендації щодо зниження ризиків. Метод відображає зв'язок між ризиками і причинами, що призводять до цих ризиків. Саме ці вимоги найбільш задовольняє OCTAVE.

2.2 Аналіз підходів, зазначених стандартом NIST щодо визначення інформаційних ризиків

Стандарт NIST SP 800-30 детально розглядає питання управління інформаційними ризиками [10]. Основні стадії, які відповідно до стандарту NIST 800-30 повинен включати процес управління ризиками:

- характеристика системи;
- ідентифікація загрози;
- ідентифікація вразливості;
- аналіз управління;
- визначення ймовірності;
- аналіз впливу;
- визначення ризику;
- рекомендації управління;
- документація результатів.

На стадії «Характеристика системи» визначаються цілі створення інформаційної системи, її межі, інформаційні ресурси, вимоги в області інформаційної безпеки і до компонентів управління інформаційної системи, і до самого режиму інформаційної безпеки.

На стадії «Ідентифікація загрози» здійснюється побудова моделі порушника, де описується, хто може виступати в якості порушника, можливості і мотиви порушника, сценарій реалізації загрози. Підсумком цього є перелік актуальних для інформаційної системи загроз.

В результаті виконання ідентифікації вразливостей складається список потенційних вразливостей інформаційної системи. Для існуючої інформаційної системи при складанні списків вдаються до ряду джерел: мережеві сканери вразливостей, каталоги вразливостей різних організацій.

При оцінці рівня вразливості беруть до уваги існуючі процедури та методи забезпечення режиму інформаційної безпеки, дані внутрішнього аудиту та результати аналізу мали місце інцидентів.

Потім вибирають шкали для оцінки параметрів ризиків. Найбільш поширеною є якісна шкала з декількома градаціями. Оцінка проводиться експертно. Використовуючи шкали оцінюють тяжкість наслідків порушення інформаційної безпеки та ймовірності реалізації загроз.

Потім вимірюють рівень ризиків, комбінуючи ймовірності реалізації загрози і тяжкості наслідків її реалізації. Рівень ризику залежить від рівнів загроз, вразливостей і ціни можливих наслідків. Ризики повинні бути розподілені за ступенем їх небезпеки.

Наступним кроком є вироблення рекомендацій з управління ризиками. Рекомендації щодо зменшення ризиків до допустимого рівня необхідні. Вони повинні бути комплексними і враховувати можливі міри різних рівнів.

Результати оцінки ризиків оформлюються у вигляді звітних документів.

2.3 Аналіз підходів стандарту ISO/IEC 31010 щодо визначення інформаційних ризиків

Серія стандартів ISO 31000 містить керівні принципи, які стосуються вибору і застосування систематичних методик оцінки ризику. Оцінка ризику включає основні елементи процесу менеджменту ризику, які визначені в ISO 31000, і містить наступні елементи: обмін інформацією та консультування, встановлення контексту, оцінку ризику (що включає ідентифікацію ризику, аналіз ризику та оцінювання ризику), обробку ризику, моніторинг і аналіз [11].

Важливим моментом є те, що оцінка ризику не є окремим видом діяльності, вона повинна бути невід'ємною частиною інших складових процесу ризик-менеджменту.

Оцінку ризику можна проводити з різним ступенем глибини і деталізації та із застосуванням одного або кількох методів від простих до складних. Необхідно приводити обґрунтування вибору методики з урахуванням її доцільності і придатності.

Після прийняття рішення про проведення оцінки ризику і встановлення цілей і сфери застосування необхідно вибрати методики, ґрунтуючись на таких факторах, як:

– цілі дослідження, так як цілі оцінки безпосередньо впливають на вибір методик, які будуть застосовані (наприклад, якщо проводять порівняльне дослідження різних варіантів, то може бути цілком прийнятним застосування менш деталізованих моделей наслідків для частин системи, на які не впливають відмінності);

– потреби осіб, які приймають рішення, так як у деяких випадках високий рівень деталізації потрібен для прийняття оптимального рішення, а в інших - буде достатньо загального розуміння;

– тип і діапазон ризиків, які аналізуються;

– потенційна значимість наслідків, так як рішення про степінь, до якої слід проводити оцінку ризику, має відображати початкове сприйняття наслідків (хоча степінь можна змінити після завершення попереднього оцінювання);

– потреба кваліфікованих експертів, персоналу та інших ресурсів, тобто простий метод, якщо він відповідає цілям і області застосування оцінки, застосований належним чином, може дати кращі результати, аніж більш складна, проте недостатньо відпрацьована процедура;

– наявність інформації і даних, так як деякі методики вимагають більше інформації і даних, ніж інші;

– необхідність зміни або удосконалення оцінки ризику, так як в майбутньому може виникнути необхідність у зміні або удосконаленні оцінки, то деякі методики є більш гнучкими в цьому плані, ніж інші;

– будь-які обов'язкові і договірні вимоги.

2.4 Аналіз методології факторного аналізу інформаційних ризиків з метою визначення інформаційних ризиків

Розглянуті у даному розділі методики дають чітке розуміння якісної оцінки інформаційних ризиків, в той час як сучасний ринок вимагає іще й кількісних показників. Особи, які керують ризиками, хочуть оперувати не лише якісними показниками, а і конкретними цифрами.

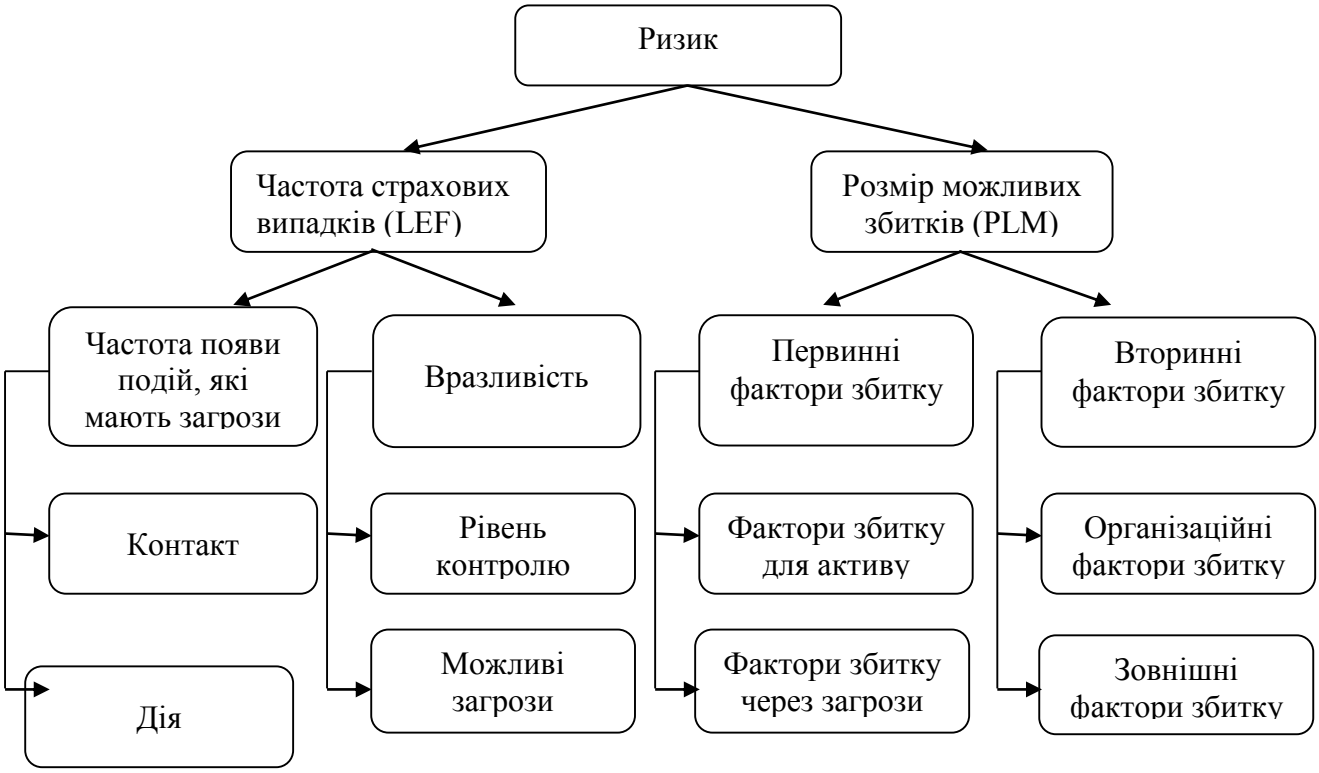
Якісний підхід не дозволяє визначити чисельну величину ризику. Він є основою для проведення подальших досліджень за допомогою кількісних методів, що широко використовують математичний апарат теорії ймовірностей, математичної статистики, теорії дослідження операцій.

Якісні (експертні) методи засновані на суб'єктивному аналізі ризику, який дозволяє розділити виявлені ризики на такі класи, як: високий, середній, низький; прийнятний повністю, частково прийнятний, неприйнятний; допустимий, критичний, катастрофічний.

У більшості існуючих методологій та стандартів основна увага приділяється побудові комплексного процесу управління ризиками. В той час як питання безпосередньої оцінки ризиків розглядаються досить поверхнево. Методологія FAIR розроблена саме для усунення цього недоліку.

Вона містить детальну класифікацію факторів, що обумовлюють виникнення ризику, визначає їх вплив один на одного і взаємозв'язок між ними. Це дозволяє адекватно оцінити частоту реалізації ризиків і масштаби втрат - саме те, що найчастіше викликає труднощі.

Методика FAIR визначає ризик як сукупність елементів, представлених на рисунку 2.1 [12]:



LEF - Loss Event Frequency

PLM - Probable Loss Magnitude

TEF -Threat Event Frequency

Рисунок 2.1 – Графічна інтерпретація методології факторного аналізу інформаційних ризиків

Варто зазначити, що FAIR призначений для доповнення і поліпшення існуючих методологій аналізу ризиків, а не для їх заміни [13]. В цілому методологія FAIR складається з 4 етапів і реалізується загалом в 10 кроків.

Перший етап - ідентифікація об'єктів оцінки.

1) Встановлення активів під загрозою.

Задля того, щоб оцінити ціннісні характеристики, та характеристики захисних засобів в межах аналізу ризику, аналітик має перш за все визначити актив (об’єкт), який ми оцінюємо. Якщо виконується багаторівневий аналіз, аналітику буде необхідно встановити і оцінити основний актив (об’єкт) під загрозою і всі мета-об’єкти, що існують між основним активом і общиною загроз. Результатом виконання даного кроку має бути складений перелік активів під загрозою.

2) Встановлення общини загроз, що розглядається.

Задля того, щоб оцінити частоту подій реалізації загрози та можливість загрози, певна община загроз має першочергово бути встановлена. Як мінімум, оцінюючи ризик, пов'язаний зі зловмисними діями, аналітик має вирішити, община загроз є людиною чи шкідливим програмним забезпеченням, внутрішньою чи зовнішньою. У більшості випадків доречно визначити общину загроз більш конкретно – наприклад, мережевих інженерів, команди прибиральників та ін., та охарактеризувати очікуваний характер общини.

Результатом завершення даного кроку має бути визначена та чітко охарактеризована община загроз.

Другий етап – оцінка частоти подій, що призводять до втрат (оцінка частоти виникнення збитків):

3) Оцінка вірогідної частоти подій реалізації загрози, варіант якої надано у табл. 2.1.

Таблиця 2.1 - Шкала для визначення частоти появи подій, що містять загрози

Оцінка	Опис
Дуже висока (ДВ)	Більше 100 разів у рік
Висока (В)	Від 10 до 100 разів у рік
Середня (С)	Від 1 до 10 разів у рік
Низька (Н)	Від 0,1 до 1 разу в рік
Дуже низька (ДН)	Менше 0,1 разу в рік (менше 1 разу в 10 років)

Вірогідна частота, в межах певного проміжку часу, що агент загрози діятиме проти активу. Фактори, що сприяють цьому: частота контакту і ймовірність дії. Оцінити вірогідну частоту подій реалізації загрози можна за шкалою, наведеною в табл.2.1 [14].

4) Оцінка можливості загрози.

Ймовірний рівень сили, яку агент загрози може застосувати проти активу. Фактори, які сприяють: уміння та ресурси. Шкала для визначення можливості загрози подана на рис.2.2 [14].

Rating	✓	Description
Very High (VH)		Top 2% when compared against the overall threat population
High (H)		Top 16% when compared against the overall threat population
Moderate (M)		Average skill and resources (between bottom 16% and top 16%)
Low (L)		Bottom 16% when compared against the overall threat population
Very Low (VL)		Bottom 2% when compared against the overall threat population

Рисунок 2.2 - Шкала для визначення можливості загрози

5) Оцінка сил захисних засобів.

Очікувана ефективність захисних засобів, протягом певного проміжку часу, в зіставлені з базовим рівнем сили. Фактори, що сприяють: сила та упевненість. Шкала для визначення сили захисних засобів подана на рис.2.3 [14].

Rating	✓	Description
Very High (VH)		Protects against all but the top 2% of an avg. threat population
High (H)		Protects against all but the top 16% of an avg. threat population
Moderate (M)		Protects against the average threat agent
Low (L)		Only protects against bottom 16% of an avg. threat population
Very Low (VL)		Only protects against bottom 2% of an avg. threat population

Рисунок 2.3 - Шкала для визначення сили захисних засобів

6) Встановлення походження уразливості.

Вірогідність того, що актив не зможе протистояти діям агенту загрози. Значення розраховується на основі показників можливості загрози і сили захисних

засобів, отриманих на кроці 4 і 5. Результатом виконання даного кроку є значення уразливості, яке розраховується за допомогою матриці визначення уразливості, поданої в табл. 2.2 [14].

Таблиця 2.2 - Матриця визначення уразливості

Вразливість						
Можливість загрози	ДВ	ДВ	ДВ	ДВ	В	С
	В	ДВ	ДВ	В	С	Н
	С	ДВ	В	С	Н	ДН
	Н	В	С	Н	ДН	ДН
	ДН	С	Н	ДН	ДН	ДН
		ДН	Н	С	В	ДВ
	Сила захисних засобів					

7) Виведення частоти подій, що приводить до втрат.

Вірогідна частота, в межах певного проміжку часу, з якою агент загрози завдасть шкоди активу. Значення розраховується на основі показників частоти подій реалізації загрози і уразливості, отриманих на кроці 3 і 6. Результатом виконання даного кроку є значення частоти подій, що призводить до втрат, яке розраховується за допомогою матриці частоти подій, що призводять до втрат, поданої у табл. 2.3 [14].

Таблиця 2.3 - Матриця визначення частоти подій, що призводять до втрат

Частота подій, що приводить до втрат						
Частота подій реалізації загрози	ДВ	С	В	ДВ	ДВ	ДВ
	В	Н	С	В	В	В
	С	ДН	Н	С	С	С
	Н	ДН	ДН	Н	Н	Н
	ДН	ДН	ДН	ДН	ДН	ДН
		ДН	Н	С	В	ДВ
	Вразливість					

Третій етап – підрахунок вірогідної величини втрат.

8) Оцінка втрати в найгіршому випадку.

Оцінити величину втрати в найгіршому випадку можливо, виконуючи наступні три пункти:

– визначити дію загрози, що скоріш за все призведе до результату найгіршого випадку;

– визначити величину для кожної форми втрати, пов’язаної з тією дією загрози;

– підсумувати величини кожної форми втрат.

9) Оцінка вірогідних втрат.

Оцінити вірогідну величину втрат можна наступним чином:

– встановити найбільш ймовірну дію(ї) общини загроз;

– визначити величину втрат для кожної форми втрат;

– підсумувати величини.

Саме на цьому етапі відбувається зіставлення якісних і кількісних показників. Для визначення рівня збитків варто скористатися шкалою, поданою в табл. 2.4 [14].

Таблиця 2.4 - Шкала для визначення рівня збитків

Величина	Нижня межа діапазону	Верхня межа діапазону
Критична	$ 10 000 000	--
Висока	$ 1 000 000	$9 999 999
Значна	$ 100 000	$999 999
Середня	$ 10 000	$99 999
Низька	$ 1 000	$9 999
Дуже низька	$ 0	$999

Таблиця 2.5 [14] використовується для відображення якісних оцінок для кожного виду збитку у разі реалізації перелічених загроз або однієї з них.

Четвертий етап – встановлення походження ризику, чітке формулювання ризику та оцінка величини потенційних збитків.

10) Встановлення походження та чітке формулювання ризику.

Фактично на даному кроці підсумовуються усі отримані на попередніх кроках дані. На основі отриманих даних встановлюються вірогідна частота та вірогідна величина майбутніх втрат.

Таблиця 2.5 - Шаблон для оцінки ймовірних величини втрат у разі дії загроз

	Види втрат					
Дія загрози	Продуктивність	Реакція	Заміна	Штрафи, рішення	Реклама компанії	Репутація
Доступ						
Зловживання						
Розголошення						
Модифікація						
Відмова в доступі						

Добре сформульовані аналізи ризику забезпечать осіб, які приймають рішення, принаймні двома ключовими елементами інформації:

– підрахована частота подій, що призводить до втрат;

– підрахована вірогідна величина втрат.

Ця інформація може передаватися текстом, графіками, або ж і тим, і іншим способом. У більшості випадків бажано також надавати підрахований потенціал щодо втрат найвищого рівня для того, щоб особа, яка приймає рішення, була проінформована щодо сценарію втрат у найгіршому випадку.

Таблиця 2.6 - Матриця визначення величини ризику

Ризик						
Вірогідна величина втрати	Критична	В	В	К	К	К
	Висока	С	В	В	К	К
	Значна	С	С	В	В	К
	Середня	Н	С	С	В	В
	Низька	Н	Н	С	С	С
	Дуже низька	Н	Н	С	С	С
		ДН	Н	С	В	ДВ
	Частота подій, що приводить до втрат					

Тобто на цьому етапі мають бути чітко визначені наступні величини: частота подій, що приводить до втрат; вірогідні втрати; втрати в найгіршому випадку.

За допомогою табл.2.6 [14] встановлюється величина ризику, а її значення розшифровується за допомогою таблиці 2.7 [14].

Таблиця 2.7 - Шкала ризику

Значення	Рівень ризику
К	Критичний
В	Високий
С	Середній
Н	Низький

В окремих випадках, для уточнення оцінки інформаційних ризиків, може бути застосований підхід, заснований на переході від якісної до кількісної оцінки інформаційних ризиків, як це зазначено у [15].

Отже, в даному розділі був проведений аналіз різноманітних методик для оцінки інформаційних ризиків. Описані програми досить популярні серед організацій, причиною чого може слугувати цілий ряд переваг кожної з методологій. Вони розрізняються ступенем деталізації, вимогами до підготовки персоналу і необхідними ресурсами. Проте кожне підприємство визначає для себе пріоритетні напрямки, за якими і вибирає методику.

Дані критерії також свідчать і про те, що у кожного комплексу є і свої недоліки. Тому проблема наразі лишається актуальною - немає універсальної методології, яка б відповідала всім критеріям і задовольняла всі потреби підприємств. Наявність такої є важливим моментом, так як до сих пір деякі керівники не розуміють важливості проведення оцінки інформаційних ризиків у їхніх мережах, в тому числі і з причини неповного досконалості наявних на ринку програм.

В той же час методологія FAIR надає обґрунтовану і логічну основу для оцінки інформаційних ризиків, яка виражена в наступних моментах:

– класифікація факторів, з яких складається інформаційний ризик. Це забезпечує концептуальне розуміння інформаційного ризику, без чого ми не зможемо розумно і обґрунтовано зробити все інші кроки. Класифікація також дає набір стандартних визначень для наших термінів;

– методика вимірювання факторів, які ведуть до появи інформаційного ризику, в тому числі частота реалізації загрози, вразливість і збитки;

– схема розрахунків, яка дозволяє отримати величину ризику шляхом математичного моделювання взаємозв'язків між вимірюваними факторами;

– імітаційна модель, яка дозволяє застосовувати класифікацію, методику вимірювання та схему розрахунків з метою побудови і аналізу сценаріїв ризику практично будь-якого розміру та складності.

Тому варто підсумувати, що FAIR не є ідеальним вирішенням проблеми оцінювання інформаційних ризиків, так як це в принципі досить складний предмет. Проте ідеального рішення на даний момент взагалі не існує. Тим не менше, FAIR дає можливість раціонально, ефективно та обґрунтовано вирішити цю проблему.

3 ОБҐРУНТУВАННЯ ВИКОРИСТАННЯ SWOT-АНАЛІЗУ ДЛЯ ІДЕНТИФІКАЦІЇ ІНФОРМАЦІЙНИХ РИЗИКІВ

На сьогоднішній день для оцінки інформаційних ризиків організації використовують широкий спектр різноманітних методик, найпопулярніші з яких були розглянуті у попередньому розділі. Проведений аналіз дав чітке розуміння того, що кожна з розглянутих методологій має не лише переваги, а й недоліки.

Ідентифікація ризиків являється критично важливим етапом в процесі управління ризиками організації. Адже ризик, який не був виявлений на даному етапі не буде включений в подальший аналіз.

Також ризик, який був ідентифікований поверхнево, може помилково бути прийнятий несуттєвим, неактуальним, що в майбутньому призведе до похибок в процесі оцінювання ризиків та в подальшому помилок при їх обробці. І саме це являється суттєвим недоліком розглянутих у попередньому розділі методологій, незважаючи на те, що у більшості з них основна увага приділяється саме побудові комплексного підходу до управління ризиками.

Саме тому в даному розділі атестаційної роботи буде розглянутий один із найбільш популярних підходів до ідентифікації ризиків, а саме метод комплексної оцінки внутрішніх і зовнішніх факторів, які впливають на розробку та провадження проекту (продукту) в організації - SWOT-аналіз, а також пов’язані з ним підходи SNW-аналіз, аналіз п’яти сил Портера та PEST-аналіз.

3.1 Аналіз методології SWOT-аналізу

SWOT-аналіз – це метод стратегічного планування, який полягає у виявленні факторів внутрішнього і зовнішнього середовища організації і поділі їх на чотири категорії: Strengths (сильні сторони), Weaknesses (слабкі сторони), Opportunities (можливості) і Threats (загрози) [16]. Також це інструмент стратегічного аналізу, який використовується для оцінки конкурентоспроможності продукту компанії.

Об'єктом SWOT-аналізу може бути не тільки організація, а й інші соціально-економічні об'єкти (наприклад, галузі економіки, міста, державно-громадські інститути, наукова сфера, політичні партії, некомерційні організації, окремі фахівці, персони і т. д.).

SWOT-аналіз допомагає проаналізувати внутрішні ресурси і зовнішнє середовище компанії, провести аналіз ризиків, оцінити конкурентоспроможність та створити конкурентну перевагу оцінюваного продукту компанії.

Сильні (S) і слабкі (W) сторони є факторами внутрішнього середовища об'єкта аналізу, (тобто тими, на що сам об'єкт здатний вплинути), в той час як можливості (O) і загрози (T) є факторами зовнішнього середовища (тобто тими, що може вплинути на об'єкт ззовні і при цьому не контролюється об'єктом).

Тобто методологія SWOT-аналізу передбачає виявлення внутрішніх сильних і слабких сторін організації та зовнішніх можливостей і загроз, а також встановлення зв’язків між ними. Розглянемо далі їх більш детально.

Сильні сторони – це такі внутрішні характеристики компанії (її товару або послуги), які забезпечують конкурентну перевагу на ринку або більш вигідне становище порівняно з конкурентами, іншими словами ті області, в яких товар компанії відчуває себе краще і стабільніше конкурентів.

Сильні сторони мають вагоме значення для компанії в стратегічному плануванні так, як за рахунок сильних сторін компанія може збільшувати рівень продажу, прибутку і частку на ринку, сильні сторони забезпечують виграшне становище товару або послуги в порівнянні з конкурентами. Сильні сторони необхідно постійно зміцнювати, покращувати, використовувати в спілкуванні зі споживачем ринку.

Слабкі сторони або недоліки товару або послуги – це такі внутрішні характеристики компанії, які ускладнюють ріст бізнесу, заважають товару лідирувати на ринку, є неконкурентоспроможними на ринку.

Важливо, також об’єктивно оцінювати значення й слабких сторін для компанії в стратегічному плануванні, адже вони заважають зростанню продажів і прибутку та тягнуть компанію назад.

Саме за рахунок слабких сторін компанія може втратити частку ринку в довгостроковій перспективі і втратити конкурентоспроможність. Тому необхідно відстежувати області, в яких компанія не досить сильна, покращувати їх, розробляти спеціальні програми для мінімізації ризиків впливу слабких сторін на ефективність компанії.

Можливості компанії – це сприятливі фактори зовнішнього середовища, які можуть впливати на зростання бізнесу в майбутньому. Їх значення для компанії в стратегічному плануванні складно недооцінити, так як саме можливості ринку уособлюють джерела зростання бізнесу.

Можливості необхідно аналізувати, оцінювати і розробляти план заходів по їх використанню з залученням сильних сторін компанії.

Загрози компанії – це такі негативні фактори зовнішнього середовища, які можуть послабити конкурентоспроможність компанії на ринку в майбутньому і привести до зниження продажів і втрати частки ринку.

Значну увагу варто звертати саме на значення ринкових загроз для компанії в стратегічному плануванні, так як саме вони означають можливі ризики компанії в майбутньому. Кожна загроза повинна бути оцінена з точки зору ймовірності виникнення в короткостроковому періоді та з точки зору можливих втрат для компанії. Проти кожної загрози повинні бути запропоновані рішення для їх мінімізації.

Технологія застосування SWOT-аналізу складається з таких кроків [16]:

– проведення аналізу оточуючого середовища компанії, товару чи послуги в розрізі зовнішніх і внутрішніх факторів;

– формування переліку сильних і слабких сторін, загроз і можливостей на основі проведеного аналізу;

– створення SWOT-матриці на основі отриманих параметрів;

– формування висновків про необхідні дії з вказанням пріоритетів виконання та термінів на основі побудованої SWOT-матриці.

Тобто при проведенні SWOT-аналізу бажано притримуватися послідовності дій, зображеної на рисунку 3.1 [16].

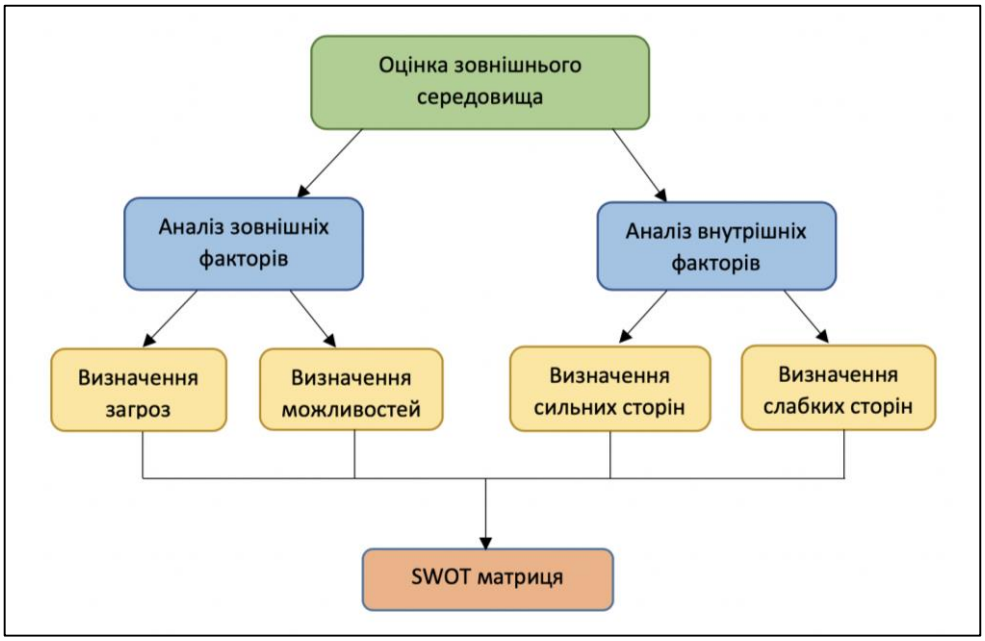


Рисунок 3.1. – Послідовність дій при SWOT-аналізі

SWOT-аналіз входить до числа найбільш часто використовуваних аналітичних методів. Спеціалізована література зазвичай включає лише результат останнього етапу SWOT-аналізу, тобто матрицю SWOT (див. рис. 3.1). Під час SWOT-аналізу необхідно визначити мету його використання, тобто для чого будуть використані його результати. SWOT-аналіз може бути використаний для однієї або декількох з наступних цілей [17]:

- як основа для розробки бачення організації;
- як основа для визначення стратегічної мети або цілей;
- як основа для першого покоління стратегічних альтернатив;
- визначення критичних областей.

Багато організацій закінчують SWOT-аналіз детальним переліком сильних, слабких сторін, можливостей та загроз. Однак якщо виявлені факти не використовуються для цілей, зазначених вище, результати в основному марні.

Питання полягає в тому, яка мета виявлення слабких сторін організації (наприклад, у забезпеченні інформаційних систем, якщо організація вже не працює з такою інформацією). Багато організацій проводять аналіз SWOT лише для того, щоб стверджувати, що він був завершений, наприклад, під час підготовки кризового плану безпеки інформаційних систем.

Однак той факт, що план не відображає результати аналізу, не враховується. Тому при впровадженні SWOT-аналізу необхідно враховувати його мету та подальше використання результатів.

Досі аналіз не мав чіткої методологічної бази. Переважно в спеціалізованій літературі публікується загальна інформація про процедуру SWOT - аналізу, а не окремі етапи, що супроводжують її практичну реалізацію.

Під час SWOT-аналізу слід дотримуватися наступних принципів [17].

1) Мета повинна враховуватися весь час під час аналізу; процедури та результати не можна механічно застосувати до іншої проблеми.

2) Необхідно зосередитися на суттєвих фактах; виклад стратегії ускладнюється у випадку надмірної кількості інформації. SWOT, як частина стратегічного аналізу, повинен визначати лише "стратегічні" факти, тобто довгострокові явища.

3) Аналіз повинен бути об'єктивним - цього можна досягнути якнайбільшою кількістю людей, залученою в його проведення.

4) Доцільно використовувати систему оцінки сили факторів, наприклад за допомогою точкових шкал.

Найчастіше використовуються такі методи та інструменти SWOT-аналізу [18]:

– використання даних оціночних та аналітичних звітів та досліджень - це звичайно контент-аналіз розроблених документів, що включає певний тип аналізу, або аналіз початкового стану або прогноз майбутнього розвитку;

– впровадження творчих методів (наприклад, мозковий штурм, дискусія) та процедур, заснованих на професійних прогнозах, зроблених компетентними структурами;

– впровадження відповідних форм, матриць, графіків і точкових шкал.

Для проведення SWOT-аналізу не потрібна формальна підготовка. Будь-менеджер, який орієнтується в справах компанії і знайомий з ринком, може скласти просту форму SWOT.

Але ця простота і легкість застосування має і зворотну сторону. Є ризик неправильного використання, поспішних і безглуздих висновків, використання невизначених і двозначних понять. До того ж, не варто забувати, що для об'єктивності картини треба використовувати для аналізу тільки актуальну, перевірену і свіжу інформацію, про що багато користувачів просто забувають.

Ось кілька нескладних правил, які допоможуть уникнути подібних помилок і дістати максимум користі з SWOT-аналізу.

1) Для об'єктивного SWOT-аналізу бізнес треба сегментувати за сферами або конкретним ринкам. Загальний аналіз, який охоплює весь бізнес - це недоцільно, так як результати вийдуть занадто узагальненими і марними. Фокусування SWOT-аналізу на конкретному сегменті забезпечить виявлення найбільш важливих сильних і слабких сторін компанії, можливостей і загроз.

2) Треба віддавати собі звіт в тому, що елементи SWOT істотно відрізняються один від одного, зокрема щодо походження і сфер впливу. Наприклад, сильні і слабкі сторони - це внутрішні характеристики компанії, отже, вони підконтрольні їй. Можливості та загрози - це зовнішні, об'єктивні, незалежні характеристики ринкового середовища, і вони непідвладні впливу організації.

3) Сильні і слабкі сторони компанії - це поняття суб'єктивні. Але думки з приводу цих характеристик повинні висловлювати не керівники і навіть не конкуренти, а клієнти, покупці, партнери, інвестори. Як вони вважають і

сприймають дані елементи - так воно і є. Сильні сторони буде вважатися такими до тих пір, поки ринок їх сприймає як конкурентоспроможні.

4) Для об'єктивного аналізу слід використовувати різнобічні вхідні дані. Навіть якщо немає можливості отримати результати великих маркетингових досліджень, це не означає, що достатньо обмежитися напрацюваннями однієї людини.

Для точності і глибини аналізу найкраще організувати групову дискусію з обміном ідеями, дізнатися і врахувати точки зору усіх функціональних підрозділів компанії. Будь-яка інформація або вихідні дані повинні бути підкріплені аргументованими доказами (офіційні листами, підтверджені цитати, статистика по галузі, звіти в пресі, відомості від дилерів, думки і коментарі покупців, урядові публікації).

5) Чим точніше формулювання, тим кориснішим буде аналіз. Отже, треба уникати розлогих, не конкретизованих і двозначних заяв.

3.2 Модель аналізу п'яти конкурентних сил Майкла Портера

Стратегічна модель аналізу 5 сил конкуренції була описана Майклом Портером в 1979 році. Майкл Портер за допомогою п'яти структурних одиниць, властивих для кожної галузі, описав способи формування конкурентної переваги і довгострокової прибутковості товару, а також способи, за допомогою яких компанія в довгостроковому періоді може утримувати свою прибутковість і зберігати конкурентоспроможність.

Метод дозволяє організації визначити свої головні конкурентні переваги і, змінивши стратегію, досягти більш вигідного положення на ринку. Тобто, метою розробки стратегії є адаптація до конкурентного середовища.

Метод призначений для вивчення зовнішнього контексту організації і надає дані для SWOT-аналізу в частині можливостей та загроз, з якими може зіштовхнутися організація у галузі.

Теорія конкуренції Майкла Портера говорить про те, що на ринку існує п'ять рушійних сил, які визначають можливий рівень прибутку на ринку. Кожна сила в моделі Майкла Портера являє собою окремий рівень конкурентоспроможності товару:

– ринкова влада покупців

- ринкова влада постачальників
- загроза появи на ринку нових учасників
- загроза появи замінників товарів чи послуг
- рівень конкурентної боротьби або внутрішньогалузева конкуренція

Майкл Портер вважав, що дані елементи ринку є рушійними силами ринкової конкуренції, що і лягло в назву моделі - модель п'яти сил конкуренції по Портеру.

Конкурентний аналіз галузі по Майклу Портеру допомагає визначити інтенсивність і вираженість конкурентних сил в галузі, знайти таку позицію, в якій компанія буде максимально захищена від впливу конкурентних сил і зможе зі свого боку впливати на них.

Золоте правило теорії п'яти сил конкуренції Майкла Портера полягає наступному: чим слабкіший вплив конкурентних сил, тим більше можливостей для отримання високого прибутку в галузі має компанія. І навпаки, чим вище вплив конкурентних сил, тим вище ймовірність, що жодна компанія не в змозі буде забезпечити високу прибутковість від капіталовкладень. А середня прибутковість галузі визначається найбільш впливовими конкурентними силами.

Найбільш ефективно даний вид аналізу застосовується в маркетингових дослідженнях та при стратегічному плануванні в організаціях.

Далі розглянемо більш детально кожну із п’яти сил Портера [17].

1) Загроза появи на ринку нових учасників.

Зазвичай нові учасники привносять на ринок нові виробничі потужності, нові технології, нові ресурси, що може бути потрясінням для галузі, може змінювати поведінку споживачів та задавати нові стандарти роботи для існуючих гравців.

Сила впливу нових гравців залежить від вхідних бар'єрів галузі і швидкості впливу існуючих гравців ринку. Якщо бар'єри входу в галузь високі і рівень протидії існуючих в галузі компаній високий, то вплив нових претендентів на прибуток в галузі буде мінімальним. Тому при роботі з новими гравцями важливо правильно вибудувати вихідні бар'єри.

2) Ринкова влада покупців.

Покупці можуть впливати на конкурентоспроможність товару компанії на ринку, так як за фактом є споживачами готового товару і забезпечують за рахунок задоволення своїх потреб існування ринку. Компанія при розробці стратегії повинна вибирати тих покупців, які є найменш впливовими на ринку.

Споживачі можуть посилювати конкуренцію за рахунок пред'явлення більш високих вимог до якості товару, до рівня сервісу, чинити тиск на рівень цін. Більш високі вимоги, пропоновані до готового товару, змушують виробників галузі підвищувати якість виробленого продукту за рахунок збільшення витрат (більш якісну сировину, додаткові умови обслуговування і т.д.), а отже, скорочувати свій рівень прибутку.

3) Ринкова влада постачальників.

Постачальники можуть впливати на конкурентоспроможність товару компанії на ринку, так як є власниками ресурсів для виробництва товарів галузі. Зростання цін на сировину і укладання угод на невигідних для компанії умовах призводить до зростання собівартості готової продукції, зростання витрат виробництва. У разі неможливості підвищення роздрібних цін на готові товари на порівнянному з ростом сировини рівні - в галузі знижується прибутковість від реалізації товарів або послуг.

4) Поява замінників товарів і послуг.

Замінники товарів чи послуг обмежують потенціал ринку з точки зору зростання цін. Зазвичай товари-замінники впливають на встановлення верхньої межі ринкових цін, що в умовах зростання витрат виробництва і сировини знижує рентабельність компаній. Поки гравці ринку не зможуть підвищити якість продукції і диференціювати свій товар від товарів-замінників - в галузі матиме місце невисока прибуток і обмежений зростання ринку.

5) Внутрішньогалузева конкуренція.

Суперництво серед існуючих конкурентів зводиться до прагнення будь-якими силами поліпшити своє становище на ринку, завоювати споживачів ринку. Інтенсивна конкуренція призводить до цінової конкуренції, збільшення витрат на просування товару, іноді до підвищення якості продукції, збільшення інвестицій в нові розробки. Все це знижує прибутковість галузі.

Для визначення величини кожної із сил Портера проводиться оцінка її складових. На підставі даних оцінки роблять висновки про привабливість галузі та положення організації в галузі і приймаються відповідні рішення.

3.3. Аналіз SNW підходу

SWOT-аналіз є одним з найбільш відомих і традиційних підходів до проведення стратегічного аналізу внутрішнього середовища організації, як її

особливого ресурсу, але тільки в секторі SW, тобто з позиції слабких і сильних сторін організації.

При проведенні традиційного SW-підходу формуються наступні висновки: слабкі сторони організації (як поганий внутрішній ресурс) ліквідувати; сильні сторони організації (як хороший ресурс) зберегти і, можливо, додатково підсилити.

Тому, певні первинні елементи сильних сторін, які були виявлені в результаті проведення стратегічного аналізу внутрішнього середовища, необхідні як первинні "блоки" побудови конкурентних переваг саме цієї компанії. І, з іншого боку, певні складові слабких сторін, які були виявлені даним стратегічним аналізом, тобто базисну основу конкурентного недоліку даної організації, необхідно ліквідувати.

Так, при SNW-підході до проведення стратегічного аналізу внутрішнього середовища тій чи іншій організації зберігається і SW-підхід (в квадрантах сил і слабкостей). Однак SNW-аналітика - це все-таки і інша якість аналізу, і інший зміст.

SNW аналіз - це сукупна оцінка організації, в процесі якої оцінюється її внутрішнє середовище за трьома значеннями: S - сильна сторона; N - нейтральна сторона; W - слабка сторона [17]. В якості нейтральної сторони (позиції) найчастіше приймається середній по ринку («нульовий») стан для даної конкретної ситуації.

SNW аналіз, в цілому, схожий з методом SWOT аналізу, але з додаванням «нейтрального» аспекту. Відповідно, при проведенні SNW аналізу всі раніше викладене про SW підході зберігається, але ще додається особлива нейтральна (N) сторона. Зазвичай SNW-аналіз застосовують для більш глибокого вивчення внутрішнього середовища організації після проведення SWOT-аналізу.

При проведенні стратегічного аналізу внутрішнього середовища організації, як показує практика, найкраще в якості нейтральної позиції встановлювати ситуаційний середньоринковий стан - для аналізованої конкретної ситуації.

По-перше, всі достоїнства SW-підходу залишаються в силі при SNW-підході. По-друге, і це головне, по кожному конкретному аналізованого ресурсу при SNW-підході чітко визначається середньоринковий стан, тобто своєрідний ситуаційний усереднений стан конкурентоспроможності на даному ринку по конкретному ресурсу.

Тому в конкурентній боротьбі для перемоги достатнім може виступати стан ринку, коли конкретна організація щодо всіх ринкових конкурентів за всіма

ключовими ресурсним позиціях (крім однієї) знаходиться в точці N (нейтральна) і тільки по одній з позицій в стані S (сильна).

Саме такий сильний (особливий ситуаційний S-ресурс організації) відповідно до практики і теорії стратегічного SNW-аналізу, виступає ключовим ресурсним елементом конкурентної переваги даної організації в даній ситуації.

3.4 Аналіз методу PEST-аналізу

PEST аналіз - простий і зручний метод для аналізу макросередовища (зовнішнього середовища) організації. Даний метод аналізу широко застосовується в стратегічному плануванні та управлінні великими організаціями, а також для оцінки інвестиційних ризиків [17].

Результати PEST аналізу можна використовувати для визначення списку потенційних загроз і можливостей при складанні SWOT аналізу компанії. PEST аналіз є інструментом довгострокового стратегічного планування і складається на 3-5 років вперед, з щорічним оновленням даних.

В процесі PEST аналізу визначаються політичні (P - political), економічні (E - economic), соціальні (S - social) і технологічні (T - technological) фактори зовнішнього середовища і оцінюється їх вплив на організацію. Вплив факторів оцінюється в балах або інших одиницях виміру. За результатами аналізу складається зведена матриця.

Далі розглянемо більш детально кожну групу факторів.

P (Political) - фактори політико-правового середовища компанії. При аналізі політико - правового оточення галузі, ринку або країни рекомендується відповісти на питання щодо ключових змін в області політичної стабільності і правового регулювання.

E (Economical) - фактори економічного стану ринку. В ході аналізу даної групи факторів необхідно визначити 6 ключових параметрів, що характеризують стан економіки країни / ринку, на якому функціонує компанія, а саме:

- динаміка розвитку економіки - спад, зростання, стагнація;
- зміна курсів валют, вартості капіталу;
- зміна рівня безробіття;
- зміна рівня інфляції;
- зміна наявного доходу на душу населення;

– тенденції в банківській сфері.

S (Socio - cultural) - фактори соціального та культурного стану ринку. В ході аналізу даної групи факторів необхідно описати 5 ключових параметрів:

– зміна демографічного стану: рух населення (спад або зростання), статево-вікова структура ринку, зміна расової приналежності;

– рівень освіченості населення, в тому числі рівень кваліфікованості кадрів;

– особливості менталітету, культурні цінності;

– зміна соціальних верств населення;

– зміна смаків і уподобань аудиторії, усталені міфи й упередження.

T (Technological) - фактори, що характеризують технологічний прогрес в галузі. Дана група чинників вимагає детального аналізу, так як в епоху технологічного процесу саме зміна в технології може кардинально змінити усталену ситуацію ринку. У ході аналізу технологічних факторів необхідно звернути увагу на 4 параметра:

– можливі зміни в ключових технологіях, використовуваних на ринку (інновації в обладнанні, матеріалах, в бізнес-моделях і методах ведення бізнесу);

– вплив інтернет на розвиток ринку;

– вплив мобільних технологій на розвиток ринку;

– Інновації в інформаційних технологіях, що дозволяють більш ефективно конкурувати на ринку.

Таким чином, переваги SWOT-аналізу полягають в тому, що він дозволяє досить просто, в правильному розрізі поглянути на становище компанії, товару або послуги в галузі, надати деталізовану оцінку ідентифікації ризиків і тому є одним із найбільш популярних інструментів в управлінні ризиками та прийнятті управлінських рішень.

Цей метод, у порівняні з розглянутими у другому розділі методологіями, дає більш точний розрахунок впливу зовнішніх і внутрішніх факторів на роботу організації. Адже оцінка відбувається в бальній системі і результати являються наглядними та реально вказують на важливість кожного з факторів.

На основі цього можемо зробити висновок, що підходи, які використовуються при проведені SWOT-аналізу можуть бути використані в тому числі і для ідентифікації інформаційних ризиків, так як дозволяють більш якісно ідентифікувати ризики.

4 ІНТЕГРАЦІЯ МЕТОДІВ ОЦІНКИ РИЗИКІВ ТА SWOT-АНАЛІЗУ

У сучасному світі все більшого поширення та популярності набувають автоматизовані системи управління будинком, їх більш популярна назва - системи «Розумного будинку».

Вони дозволяють значно полегшити і автоматизувати процес використання устаткування інженерних, мультимедійних, охоронних та інших систем будівель і споруд, а також значно підвищити ефективність їх роботи.

Проте, все ще існує проблема, пов'язана з недостатнім опрацюванням та дослідженням загроз інформаційній безпеці користувачів «Розумного будинку», саме тому дана система була обрана для ідентифікації ризиків інформаційної безпеки методом SWOT-аналізу та інтеграції отриманих результатів з методом оцінки ризиків причинно-наслідковим зв’язком та методологією FAIR.

Загрозами інформаційній безпеці системам «Розумного будинку» є класичні загрози - порушення конфіденційності, цілісності та доступності інформації, яка використовується в процесі роботи.

Конфіденційність - це відсутність можливості витоку інформації закритого або особистого характеру користувачів системи «Розумного будинку», через його компоненти.

Доступність - можливість авторизованим користувачам і самій системі «Розумного будинку» виконувати різні дії, прописані в сценарії роботи системи «Розумного будинку». В іншому випадку виникає проблема неможливості реагувати на події і здійснювати дії, що передбачаються програмною складовою системи «Розумного будинку».

Цілісність в контексті «Розумного будинку» - це достовірність інформації, одержуваної від датчиків або інших джерел, включаючи користувача.

4.1 Ідентифікація ризиків з використанням SWOT-аналізу

На основі методу SWOT-аналізу, детально розглянутого у 3 розділі даної атестаційної роботи, був проведений аналіз інформаційної безпеки технології «Розумний будинок».

Процедуру здійснення SWOT-аналізу доцільно почати із загальних принципів впровадження SWOT-аналізу. На основі методології SWOT-аналізу,

детально розглянутої у 3 розділі, можемо виокремити чотири основні фази SWOT-аналізу (незалежно від того, буде він впроваджений у виробничому секторі, державному управлінні чи інформаційній системі).

1) Підготовка до SWOT-аналізу.

2) Визначення та оцінка сильних і слабких сторін організації та/або її областей.

3) Виявлення та оцінка можливостей та загроз з боку зовнішнього середовища.

4) Розробка SWOT-матриці.

Індивідуальні фази SWOT-аналізу далі поділяються на окремі види діяльності та етапи. Описана процедура впровадження кожного етапу SWOT-аналізу базується на перевіреному практичному досвіді та не є обов'язковою.

Оскільки метод не має фіксованої методологічної бази, можна вносити зміни до запропонованої процедури відповідно до потреб та усталених практик організації та рівня стратегії, для якої використовується SWOT-аналіз.

Для успішного проведення SWOT-аналізу в організації до його початку пропонується виконати такі чотири кроки:

– чітке визначення мети SWOT-аналізу;
– визначення областей, які підлягають аналізу;
– створення аналітичних груп;
– стандартизація методології роботи та мотивація членів команди.

Для визначення сильних і слабких сторін пропонується виконання двох послідовних кроків, які більш докладно описані нижче.

1) Ідентифікація сильних і слабких сторін.

Сильні та слабкі сторони аналізованої області організації можуть бути визначені декількома способами, наприклад через контент-аналіз вихідних даних та наступну реалізацію творчих методів, напр. мозковий штурм, консультації та керовані дискусії, спрямовані на виявлення або визначення сильних і слабких сторін аналізованої області організації. Необхідно відповідним чином записувати сильні та слабкі сторони, напр. у формі, включаючи обґрунтування результату. Приклад форми для виявлення слабких сторін показаний у таблиці 4.1.

2) Оцінка сильних і слабких сторін.

Визначення сильних і слабких сторін аналізованої області зазвичай виконується шляхом визначення їх відповідності з точки зору їх наслідків для

аналізованої області. Актуальність сильних і слабких сторін оцінюється окремо за допомогою методу парного порівняння або методу 100 балів.

Таблиця 4.1. - Приклад форми для виявлення слабких сторін

Аналізована область організації: напр. безпека інформаційної системи організації	
Слабка сторона	Обґрунтування (чому ми вважаємо даний фактор слабкістю)
Недосконале оновлення інформаційної системи	Пробіли в безпеці виникають через недосконале оновлення інформаційної системи. Потім зловмисне програмне забезпечення може проникнути в таку інформаційну систему.
Інфільтрація (проникнення) персоналу	Навряд чи керівництво компанії виявить персонал, який маючи доступ до інформаційної системи організації, буде здійснювати несанкціонований до неї доступ. Тому несанкціоноване використання даних в інформаційній системі є досить великим.
Слабка інформаційна інфраструктура	Потоки даних неправильно запрограмовані в інформаційній системі. Це може призвести до ненавмисного та серйозного витоку даних.
Слабка комунікаційна інфраструктура	Невчасне оновлення обладнання може призвести до можливих помилок безпеки, які дозволяють зловмисним проникнути в інформаційну систему через незахищені порти.

Процедура визначення відповідності або порядку окремих сильних і слабких сторін методом парного порівняння виглядає наступним чином (див. табл. 4.2.).

– виявлені сильні / слабкі сторони порівнюються парами та визначається їх відповідність стосовно аналізованої області, а потім важливіший елемент кожної пари записується в таблиці;

– підраховується частота більшої відповідності, тобто підраховується кількість переваг у парі при порівнянні, а значення підсумовуються як у рядках, так і у стовпцях;

– релевантність (актуальність або доречність) - масштабність кожної сили / слабкості обчислюється діленням кількості переваг певної сили / слабкості

на загальну кількість переваг (наприклад, релевантність першої слабкості, наведеної у таблиці 4.1. є = 2/6 = 0,33).

Таблиця 4.2. - Визначення відповідності методу парного порівняння виявлених сильних і слабких сторін

Процес визначення відповідності	a)				b)	c)
Сильна / Слабка сторона	A	B	C	D	Кількість переваг	Актуальність (доречність)
A. Недосконале оновлення інформаційної системи		B	A	A	2	0,33
B. Інфільтрація персоналу			B	B	3	0,5
C. Слабка інформаційна інфраструктура				D	0	0
D. Слабка комунікаційна інфраструктура					1	0,17
Загально					6	1,0

У випадку використання методу ста балів, кожен член команди ділить 100 балів серед індивідуальних сильних сторін. Чим більше балів відведено заданій сильній стороні, тим більш актуальною вона вважається відносно аналізованої області.

100 балів аналогічно розділяються і між слабкими сторонами. Відповідність може бути потім обчислена як середнє арифметичне за окремими оцінками членів аналітичної групи. Якщо оцінка будь-якої сильної / слабкої сторони значно відрізняється серед членів команди, краще досягти консенсусу, а не використовувати середнє арифметичне.

Після виявлення сильних і слабких сторін вони розташовуються в порядку відповідності за результатами оцінки. Таким чином, створюютсья два списки, починаючи з першої найбільш актуальної сильної / слабкої сторони і до останньої як найменш релевантної, яка може мати з найменші або і взагалі відсутні наслідки для аналізованої області.

Порядок слабких сторін складається на основі результатів оцінки даних, наданих у табл. 4.2 та відповідно до їх важливості.

1) Інфільтрація персоналу.

2) Недосконале оновлення інформаційної системи.

3) Слабка комунікаційна інфраструктура.

4) Слабка інформаційна інфраструктура.

У ході дослідження, було з’ясовано, що сучасний «Розумний будинок» оснащений системою охорони, відеоспостереження, системами розпізнавання, а також багатьма іншими технологіями (в залежності від виробника), які гарантують серйозний захист від фізичного доступу.

Тому, до сильних сторін даної технології, по праву віднесені фактори, які захищають будинок від фізичного несанкціонованого доступу сторонніх осіб, а отже однозначно зменшують шанси зловмисників заволодіти інформацією.

Проте, незважаючи, на достатньо ефективний рівень захисту від фізичного вторгнення, було виявлено серйозні недоліки у функціонуванні системи, які загрожують інформаційній безпеці даної технології, а отже і ставлять під загрозу безпеку користувачів таких систем.

В першу чергу варто зазначити підключення системи до мережі Інтернет та до локальної мережі. Дані моменти уже дають розуміння про достатньо велику кількість потенційних вразливостей та загроз, які можуть бути реалізовані шляхом несанкціонованого доступу до мережі.

Крім того, варто пам’ятати, що кожен із пристроїв, який підключений до системи Розумного будинку має задовольняти вимоги безпеки, необхідні для ефективного функціонування технології. А також варто здійснювати пошук та аналіз вразливостей кожного окремого виділеного об’єкта такої системи.

Іще одним досить важливим і суттєвим недоліком є передача інформації від системи управління до кінцевих пристроїв автоматизації у відкритому вигляді. Це надає особливу простоту зловмиснику у разі несанкціонованого доступу до системи модифікувати дані і таким чином змінити поведінку систему «Розумного будинку» у своїх цілях.

Далі пропонується три послідовні кроки для ідентифікації та оцінки загроз і можливостей із зовнішнього середовища, які більш докладно описані нижче.

1) Ідентифікація загроз та можливостей зовнішнього середовища.

Загрози та можливості зовнішнього середовища можуть бути визначені декількома способами для аналізованої області організації. Їх можна ідентифікувати за допомогою контент-аналізу вихідних даних з подальшими деякими творчими методами, наприклад, мозковий штурм, консультації, керована дискусія, спрямована на виявлення або визначення загроз та можливостей

аналізованої області організації. Необхідно відповідним чином записувати загрози та можливості, наприклад у формі, включаючи обґрунтування результатів. Зразок форми для ідентифікації загроз представлений у таблиці 4.3.

Таблиця 4.3. - Приклад ідентифікації форми загрози

Аналізована область організації: напр. безпека інформаційної системи організації	
Загроза	Обґрунтування (чому ми вважаємо даний фактор загрозою)
Моніторинг мережі	Можуть бути виявлені слабкі сторони та отримані дані з інформаційної системи з метою підготовки майбутніх атак або компрометації користувачів інформаційної системи.
Зміна відправлених даних	Дані фальсифікуються з метою впровадження дезінформації в інформаційну систему.
Вставлення дезінформації в інформаційну систему	Пряме вставлення дезінформації (надлишкової інформації) в інформаційну систему з метою компрометації споживачів системи.
Перевантаження інформаційної системи	Можливість зробити інформаційну систему недоступною, відключивши її від комунікаційної інфраструктури та комп'ютерної мережі з метою відмови в обслуговуванні.

2) Оцінка загроз.

Оцінка загроз насамперед спрямована на визначення релевантності наслідків загроз із зовнішнього середовища для аналізованої області, якщо вони виникають. А також виявляється ймовірність виникнення окремих загроз. Рівень ризику, що дана загроза вплине на аналізовану область організації, потім буде обчислюватися як продукт загрози та відповідність її наслідків для організації та ймовірності її виникнення. Чим вище рівень ризику, тим більше стратегічне значення він має. Потім ризики для аналізованої області розташовуються відповідно до їх рівнів.

3) Оцінка можливостей.

Даний крок включає визначення привабливість наслідків можливостей із зовнішнього середовища на аналізовану область у разі їх виникнення, а також визначається ймовірність виникнення індивідуальних можливостей. Вигода кожного можливості може бути визначена на основі двох згаданих вище змінних.

Можливість визначається як продукт привабливості наслідків можливості та ймовірності її виникнення. Чим більша вигода, тим більше стратегічне значення вона має. Тоді переваги для аналізованої області розташовуються відповідно до їх рівнів.

Далі розглянемо два ключові кроки, які повинні бути виконані під час розробки SWOT-матриці:

– запис факторів, що мають стратегічне значення;

– формування альтернативних стратегій.

Запис факторів стратегічної значущості - це облік сильних і слабких сторін, що мають велике значення, а також можливостей та загроз високих значень (тобто можливостей та ризиків високого рівня), які мають стратегічне значення. Отже, це вибір тих факторів (сильних, слабких сторін, можливостей та загроз), які будуть використані для формування альтернативних стратегій.

Формування альтернативних стратегій базується на поєднанні сильних і слабких сторін (внутрішніх факторів) з виявленими загрозами та можливостями (зовнішні фактори). Потім розробка чотирьох стратегій є логічним продовженням матриці SWOT. Матриця SWOT включає наступні чотири стратегії.

1) Стратегія WO - стратегія пошуку. Ця стратегія спрямована на подолання (усунення) слабких місць шляхом використання можливостей. Ця стратегія вимагає отримання додаткових ресурсів для використання можливостей.

2) Стратегія SO - стратегія використання переваг. Ця стратегія використовує переваги на користь можливостей, виявлених у зовнішньому середовищі. Цей квадрант визначає бажану умову, до якої спрямовується організація. Зрозуміло, що ця стратегії є основою для визначення бачень і цілей. Складність її визначення та реалізації зумовлена тим, що комбінація SO зустрічається рідко в реальному житті.

3) Стратегія WT - стратегія уникнення. Це оборонна стратегія, спрямована на усунення (подолання) слабких місць та уникнення зовнішньої загрози. Це "потреба на виживання" для організації. Якщо стратегія використовується для розробки концепцій, вона є ключовою для підтримання основних функцій організації, необхідних для виконання її місії.

4) Стратегія ST - стратегія протиборства. Цю стратегію можливо реалізувати, якщо організація достатньо сильна, щоб зіткнутися з загрозою - в

основному одна група організації вимагає, щоб інша група організації дотримувалася принципів сталого розвитку.

У ході проведення аналізу, була складена SWOT-матриця (див. табл. 4.4.), яка відображає сильні та слабкі сторони інформаційної безпеки технології «Розумний будинок», а також її загрози та можливості.

Під час проведення SWOT-аналізу було проаналізовано багато джерел та досліджень стосовно безпеки інформації, яка циркулює в системі «Розумного будинку». Дана технологія дає можливість досить широко оцінити фактори, які мають вплив на оцінку ризиків.

Кількість сильних та слабких сторін, переваг та недоліків технології «Розумний будинок» однозначно не обмежується даними, поданими у таблиці 4.4. У ході аналізу був сформований їх перелік у порядку пріоритетності, як було заначено вище, і саме найбільш важливі та можливі з них подані у вигляді підсумкової матриці SWOT-аналізу.

При виконанні SWOT-аналізу кожен аналітик повинен переконатися, що результати оцінки є найбільш об'єктивними. Це справедливо і в разі оцінки системи інформаційної безпеки організації саме з позицій безпеки за допомогою SWOT-аналізу.

Рівень суб'єктивності в аналітичному процесі мінімізується шляхом впровадження вище представлених методів, що підвищує якість набутої інформації. Об'єктивні результати допомагають організації отримати більш точний огляд перспектив подальшого розвитку.

Оцінка ризиків та можливостей є підходящим способом отримання об'єктивних результатів при оцінці зовнішніх факторів. Він ґрунтується на оцінці двох основних критеріїв, релевантності чи привабливості наслідків та ймовірності їх настання.

Реалізація SWOT-аналізу в основному базується на конкретних методах та інструментах, що реалізуються при виявленні зовнішніх та внутрішніх факторів, а також їх оцінці. Тому доцільно проаналізувати можливості впровадження методів та інструментів для конкретних типів організацій на окремих етапах SWOT-аналізу.

Таблиця 4.4. – Сформована SWOT-матриця

Сильні сторони	**Слабкі сторони**
Відеоспостереження (постійний контроль за будинком і прилеглою територією у режимі онлайн)	Доступ до мережі Інтернет та локальної мережі
Охорона будинку від несанкціонованого доступу сторонніх осіб	Недостатній рівень захищеності потоку даних між системою управління та кінцевими пристроями автоматизації
Імітація людської присутності	Збір певних видів персональних даних користувачів системи
Система пожежогасіння	Людський фактор (збереження паролів за замовчуванням, вимкнення частини системи автентифікації і т.д.)
Системи розпізнавання	Залежність функціонування системи від подачі електроенергії
Загрози	**Можливості**
Перехоплення та підміна сигналу між елементами мережі	підвищення обізнаності користувачів систем «Розумний дім» щодо необхідності захисту інформаційної безпеки їх систем
Підключення до мережі несанкціонованого користувача	Впровадження шифрування даних під час їх передачі
Віруси та троянські програми	Підвищення рівня захисту мережі від несанкціонованого доступу
Атака хакерів	Виявлення та усунення вразливостей пристроїв, які входять до складу системи
Збої в системі електропостачання	Забезпечення неможливості вільного доступу до апаратної частини системи

До переваг використання SWOT-аналізу організації можемо віднести:

– універсальність методу - підходить всім організаціям;

– гнучкість методу, що передбачає вільний вибір аналізованих факторів в залежності від поставлених цілей;

– простота використання методу - не вимагає спеціальних знань і вузькопрофільної освіти;

Також варто зазначити і недоліки використання SWOT-аналізу:

– трудомісткість методу - потрібно зібрати великий обсяг інформації з самих різних сфер;

– суб'єктивність результатів - як правило, залежать від бачення і знань людини, яка його проводить;

– висновки на основі SWOT аналізу, найчастіше, носять описовий характер без установки пріоритетів і рекомендацій.

4.2 Встановлення причинно-наслідкових зв’язків на основі проведення SWOT-аналізу

Аналіз причинно-наслідкових зв'язків - це структурований метод, який застосовується для визначення можливих причин небажаної події чи проблеми. Він систематизує можливі чинники, які мають вплив в узагальнені категорії таким чином, що дозволяє розглядати всі можливі гіпотези.

Однак, метод не вказує на фактичні причини, оскільки вони можуть бути визначені тільки шляхом фактичного засвідчення та емпіричної перевірки гіпотез. Інформацію представляють у вигляді діаграми Ісікави (званої також «риб'яча кістка»), а іноді - у вигляді деревоподібної схеми.

Аналіз причинно-наслідкових зв'язків дозволяє отримати структуроване графічне відображення переліку причин конкретного впливу. Вплив може бути позитивним або негативним (проблема), в залежності від контексту.

Даний метод застосовується для розгляду всіх можливих сценаріїв і причин, зазначених групою експертів, і дозволяє встановити необхідний консенсус щодо найбільш ймовірних причин, які потім можливо перевірити дослідним шляхом або за допомогою оцінювання наявних даних. Застосування даного методу доцільно на початку аналізу для більш широкого розгляду можливих причин і подальшого встановлення можливих гіпотез для подальшого формального аналізу.

Складання діаграми причинно-наслідкових зв'язків доцільно при необхідності:

– виявити можливі початкові причини конкретного впливу, проблеми або стану;

– виділити і співвіднести деякі з взаємозв'язків серед факторів, що впливають на конкретний процес;

– проаналізувати існуючі проблеми так, щоб можна було зробити коригувальну дію.

Складання діаграми причинно-наслідкових зв'язків має такі переваги:

– привернення уваги фахівців, які проводять аналіз, до конкретної проблеми;

– сприяння визначенню початкових причин проблеми із застосуванням структурованого підходу;

– сприяння співробітництву в групі і більш повному використанню знань групи про продукцію або процес;

– застосування простого для сприйняття типу діаграми для відображення причинно-наслідкових зв'язків;

– виявлення можливих причин змін в процесі;

– встановлення областей, в яких слід збирати дані для подальшого вивчення.

Аналіз причинно-наслідкових зв'язків може застосовуватися в якості методу проведення аналізу першопричини.

Основними етапами проведення причинно-наслідкового аналізу є:

– встановлення впливу, який необхідно проаналізувати, і включення його в блок на діаграмі. Вплив може бути позитивним або негативним (проблема), в залежності від обставин;

– визначення основних категорій причин, що відображаються в блоках на діаграмі Ісікави. При аналізі систем зазвичай виділяють наступні категорії причин: персонал, обладнання, середовище, процеси та ін. Категорії визначають відповідно до конкретного контексту;

– відображення можливих причин для кожної основної категорії з відгалуженнями для опису взаємозв'язку між ними;

– продовження аналізу за допомогою питання «Чому?» Або «Чим це викликано?» для встановлення зв'язку між причинами;

– аналіз всіх відгалужень для забезпечення узгодженості та повноти, а також того, що дані причини відносяться до основного впливу;

– визначення найбільш ймовірних причин на підставі думки групи і наявних свідчень.

Результати зазвичай відображають у вигляді діаграми Ісікави («риб'ячої кістки»). Діаграма Ісікава будується шляхом підрозділу причин на основні категорії (представлені лініями, що відходять від «Скелета риби») з відгалуженнями, які описують більш конкретні причини в даних категоріях.

На основі проведеного SWOT-аналізу, а також методу причинно-наслідкових зв'язків для встановлення причин, які загрожують порушенню конфіденційності, цілісності та доступності інформаційних активів, які циркулюють в мережі системи «Розумний дім», побудуємо діаграму Ісікави, які чітко відобразить усі існуючі загрози.

В якості виконання даного етапу, у додатку А надана розроблена автором діаграма основних відповідностей ризиків інформаційної безпеки системи «Розумний дім» конкретним факторам порушенню інформаційної безпеки, які були досліджені та ідентифіковані методом SWOT-аналізу. У таблиці представлені основні категорії можливих загроз та шляхи їхньої реалізації (тобто фактори).

Діаграма Ісікави або причинно-наслідкова діаграма є ефективним інструментом при оцінюванні ризиків в СМІБ, так як наглядно демонструє причинно-наслідкові зв’язки між об’єктом аналізу, в нашому випадку це інформаційна безпека системи «Розумний дім» та факторами, які на нього впливають.

Таким чином, у ході даного розділу атестаційної роботи була продемонстрована інтеграція методу SWOT-аналізу та методу встановлення причинно-наслідкових зв’язків для ідентифікації та встановлення ризиків інформаційної безпеки системи «Розумний дім».

Ґрунтуючись на дане дослідження та досвід інтеграції методу причинно-наслідкових зв’язків та методології факторного аналізу інформаційних ризиків, який був детально викладений у матеріалах моєї бакалаврської атестаційної роботи, можемо говорити покращення, посилення та деталізацію даного підходу до оцінки ризиків інформаційної безпеки.

Адже на основі результатів SWOT-аналізу та методу причинно-наслідкових зв’язків, можемо стверджувати про вдале розширення та покращення, обраного в моїй попередній роботі, комплексного підходу до оцінки ризиків за методологією FAIR.

ВИСНОВКИ

Завдання на атестаційну роботу виконано у повному обсязі. У даній роботі вирішено задачу щодо обґрунтування підходу до ідентифікації інформаційних ризиків на підставі використання SWOT-аналізу та методу причинно-наслідкових зв'язків.

Проведено ретельний аналіз підходів до оцінки інформаційних ризиків за рахунок використання SWOT-аналізу, методу причинно-наслідкового аналізу та методології факторного аналізу інформаційних ризиків.

На цей час актуальним є питання забезпечення інформаційної безпеки. В свою чергу, для забезпечення інформаційної безпеки як окремих систем, технологій чи підприємств, так і держави в цілому важливим є питання оцінки ризиків, які виникають в процесі діяльності підприємств. Для оцінки ризиків інформаційної безпеки використовуються різні методики і стандарти управління інформаційними ризиками.

Оцінка ризику дає можливість особам, які приймають рішення, та відповідальним сторонам, поліпшити розуміння ризиків, що може сприяти досягненню цілей, а також адекватності і результативності здійснюваного управління. Оцінка ризику забезпечує основу для прийняття рішень про вибір найбільш доцільного підходу, застосовуваного для обробки ризиків.

Вихідні дані оцінки ризику є вхідними даними для процесів прийняття рішень в організації. У роботі був проведений аналіз різних підходів до побудови системи менеджменту інформаційної безпеки, який дав чітке розуміння, що саме оцінка ризиків – є фундаментальним кроком при будь-якому із них.

У роботі проведено аналіз найбільш відомих методик оцінки інформаційних ризиків. Встановлено, що існуючі методики недостатньо повно враховують фактори, що мають вплив на ризик.

Однією з найбільш перспективних методик оцінки ризиків є методика FAIR, яка представляє собою детально розроблений процес оцінки ризиків з урахуванням основних факторів, що мають вплив на актив, загрозу та організацію в цілому.

Ретельний аналіз даної методології показав, що в розрахунках інформаційних ризиків вона передбачає матричний підхід та переведення кількісних значень параметрів до якісних за допомогою відповідних шкал.

Незважаючи на те, що методологія FAIR дає якісну оцінку ризику, цей підхід може застосовуватися достатньо ефективно. Проте, для того, щоб він застосовувався найбільш ефективно, доцільно спочатку ідентифікувати ризики за допомогою SWOT-аналізу, а потім формувати причинно-наслідкові зв'язки, які були розроблені в роботі по відношенню до інформаційної безпеки технології «Розумний дім».

Даний підхід дозволяє сформувати модель загроз, точно ідентифікувати ризики та спростити застосування методології FAIR для оцінки інформаційних ризиків.

Результати роботи можуть бути корисні для спеціалістів в області інформаційної безпеки, а також для керівників підприємств, які цікавляться оцінкою ризиків інформаційної безпеки.

Окремі результати роботи опубліковано у [1 – 5].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Подоляка Н. В. Пропозиції щодо використання методу причинно-наслідкових зв'язків для визначення ризиків елементів корпоративних мереж / Н. В. Подоляка. // Матеріали XXII міжнародного молодіжного форуму Радіоелектроніка та молодь у XXI столітті. – 2018. – С. 136–137.

2. Кавуненко Я.О., Подоляка Н. В. Исследование и обоснование выбора методов многофакторной аутентификации / Я.О. Кавуненко, Н. В. Подоляка. // Матеріали міжнародної науково-практичної конференції «Інформаційна безпека та інформаційні технології». – 2019. – С. 11.

3. Подоляка Н. В., Кавуненко Я.О. Комплексний підхід при виборі методології оцінки ризиків серверної кімнати як об’єкту підвищеного ризику компанії / Подоляка Н. В., Кавуненко Я.О. // Матеріали XXIV міжнародного молодіжного форуму Радіоелектроніка і молодь у XXI столітті. – 2020.

4. Lisova V.P., Podoliaka N.V. Suggestions of protection confidential data from insider attacks / V.P. Lisova, N.V. Podoliaka // Матеріали XLIII міжнародної науково-практичної інтернет – конференції «Сучасні виклики та проблеми науки». – 2020 р. – Ч. 3, С. 23.

5. Подоляка Н. В. Ідентифікація інформаційних ризиків для елементів корпоративних мереж методом причинно-наслідкового аналізу: бак. атест. роб.: 6.170103 «Управління інформаційною безпекою» / Подоляка Наталія Віталіївна – Харків, ХНУРЕ, 2018. – 55 с.

6. ISO/IEC 27003:2017 / Information technology – Security techniques – Information security management systems – Guidance // – 2017.

7. Каталоги BSI IT-Gundschutz [Електронний ресурс] – Режим доступу до ресурсу: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_15_EL_EN_Draft.pdf?__blob=publicationFile&v=2

8. Постанова № 95 Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України від 28 вересня 2017 року.

9. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process / A. C. Richard, F. S. James, R. W. William. – Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2007. – 141с.

10. Stoneburner G. Risk Management Guide for Information Technology

Systems / G. Stoneburner, A. Goguen, A. Feringa. – Gaithersburg: National Institute of Standards and Technology, 2002. – 56 c. – (NIST Special Publication 800-30).

11. Менеджмент риска. Методики оценки риска. // ISO/IEC 31010:2009, IDT. – 2009.

12. Добринін І. С. Вдосконалення методики факторного аналізу інформаційних ризиків / І. С. Добринін, Н. О. Мальцева. // Системи обробки інформації. – 2017. – №3. – С. 146–150.

13. Практика ИБ \ FAIR - методология анализа рисков [Електронний ресурс]. – 2011. – Режим доступу до ресурсу: http://dorlov.blogspot.com/2011/10/fair-1.html.

14. Freund J. Введение в факторный анализ информационных рисков (FAIR) / J. Freund, J. Jones. – 87 с.

15. Dobrynin I., Radivilowa T., Maltseva N., Ageyev D., Use of Approaches to the Methodology of Factor Analysis of Information Risks for the Quantitative Assessment of Information Risks Based on the Formation of Cause-And-Effect Links, 2018 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), p. 229-233, DOI: 10.1109/INFOCOMMST. 2018.8632022.

16. Как выполняется SWOT-анализ [Електронний ресурс]. – Режим доступу до ресурсу: https://ivan-shamaev.ru/doing-swot-analysis/

17. Метод SWOT анализа в стратегическом управлении [Електронний ресурс]. –Режим доступу до ресурсу: http://powerbranding.ru/biznes-analiz/swot/

18. Rehak D. The Ways of Assessing the Security of Organization Information Systems through SWOT Analysis / D. Rehak, M. Grasseova // Cases on E-Readiness and Information Systems Management in Organizations: Tools for Maximizing Strategic Alignment / D. Rehak, M. Grasseova., 2012. – (1). – С. 162–184.