Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Розробка методології для оцінки ризиків інформаційної безпеки для агрохолдингу"

Виконала: студентка

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)

Костюк Катерина Олегівна
підпис (прізвище та ініціали)

Керівник Загородна Н.В.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Никитюк В.В.
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студентці Костюк Катерині Олегівні
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка методології для оцінки ризиків інформаційної безпеки для агрохолдингу

Керівник роботи Загородна Наталія Володимирівна к.т.н., доцент, завідувач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «20» 11 2024 року № 4/7-1112

2. Термін подання студентом завершеної роботи 23.12.2014

3. Вихідні дані до роботи Інтернет-джерела, технічна документація, регламентні документи

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ; Розділ 1. Методи ризиків інформаційної безпеки; Розділ 2. Розробка методології для оцінки ризиків інформаційної безпеки; Розділ 3. Практичне використання розробленої методології для оцінки ризиків інформаційної безпеки на прикладі агрохолдингу; Розділ 4. Охорона праці та безпека в надзвичайних ситуаціях; Висновки; Список використаних джерел; Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульний слайд; 2. Мета і завдання дослідження; 4. Актуальність та наукова новизна; 5. Методи оцінки ризиків; 6. Місія, оперативні цілі, фінансові цілі та зобов'язання; 7. Розробка методології для оцінювання ризиків інформаційної безпеки; 8. Критерії оцінки ризику; 9. Моделювання та оцінка ризиків; 10. Оцінка рекомендованих контролів; 11. Документування та звітування; 12. Заповнення реєстру ризиків інформаційної безпеки за розробленою методологією на прикладі агрохолдингу; 13. Оцінка розробленої методології та перспективи вдосконалення

Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 20.10.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з вимогами до кваліфікаційної роботи	20.11 – 21.11	Виконано
2.	Затвердження теми кваліфікаційної роботи	21.11 – 22.11	Виконано
3.	Аналіз літератури та нормативної бази відповідно до		
	теми роботи	22.11 – 23.11	Виконано
4.	Написання першого розділу звіту	23.11 – 24.11	Виконано
5.	Ідентифікація активів	24.11 – 25.11	Виконано
6.	Вибір контрольних заходів захисту	25.11 – 26.11	Виконано
7.	Розробка критеріїв оцінки ризику	26.11 – 27.11	Виконано
8.	Визначення етапів моделювання та оцінки ризиків	28.11 – 29.11	Виконано
9.	Проведення оцінки рекомендованих контролів	29.11 – 30.11	Виконано
10.	Написання другого розділу звіту	01.12 – 02.12	Виконано
11.	Заповнення реєстру ризиків інформаційної безпеки за		
	розробленою методологією	03.12 – 04.12	Виконано
12.	Оцінка розробленої методології	05.12 – 06.12	Виконано
13.	Написання третього розділу звіту	06.12 – 07.12	Виконано
14.	Ознайомлення з літературою про забезпечення охорони		
	та безпеки в надзвичайних ситуаціях	08.12 – 09.12	Виконано
15.	Написання четвертого розділу звіту	09.12 – 10.12	Виконано
16.	Оформлення кваліфікаційної роботи	10.12 – 12.12	Виконано
17.	Нормоконтроль	13.12 – 14.12	Виконано
18.	Перевірка на плагіат	15.12 – 16.12	Виконано
19.	Попередній захист кваліфікаційної роботи	23.12.2024	Виконано
20.	Захист кваліфікаційної роботи	28.12.2024	

Студент _____ Костюк К.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Загородна Н.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка методології для оцінки ризиків інформаційної безпеки для агрохолдингу // ОР «Магістр» // Костюк Катерина Олегівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-62 // Тернопіль, 2024 // С. 84, рис. – 18, табл. – 0 , кресл. – 0, додат. – 4.

Ключові слова: управління ризиками, інформаційна безпека, інформаційні технології, інформаційні активи, оцінка ризиків, контролі, очікуваність, вплив.

Кваліфікаційна робота присвячена розробці методології для оцінки ризиків інформаційної безпеки агрохолдингу. У роботі розглянуто сучасні методології оцінки ризиків, такі як ISO/IEC 27005, FAIR та DoCRA, і їх застосування в контексті оцінки ризиків інформаційної безпеки. Запропонована методологія розроблена відповідно до вимог замовника, яким є ″Контінентал Фармерс Груп″.

Методологія включає розробку критеріїв оцінки, моделювання ризиків, обробку та документування. Апробація методології проведена на прикладі аграрного підприємства, що дозволило протестувати її ефективність у реальних умовах.

Результати дослідження мають вагоме практичне значення для фахівців у сфері інформаційної безпеки, адже розроблена методологія, завдяки своїй гнучкості, може бути адаптована до потреб організацій різною галузевою специфікою, забезпечуючи універсальність та широкі можливості застосування.

ABSTRACT

Development of a Methodology for Information Security Risk Assessment for an Agricultural Holding // Thesis of educational level "Master"// Kateryna Kostiuk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-62 // Ternopil, 2024 // P. 84, figs. 18, tables 0, drawings 0, added. – 4.

Keywords: risk management, information security, information technology, information assets, risk assessment, controls, likelihood, impact.

The qualifying work is devoted to the development of a methodology for assessing the information security risks of an agricultural holding. The paper considers modern risk assessment methodologies, such as ISO/IEC 27005, FAIR and DoCRA, and their application in the context of information security risk assessment. The proposed methodology was developed in accordance with the requirements of the client, Continental Farmers Group.

The methodology encompasses the development of assessment criteria, risk modeling, risk treatment, and documentation. Its testing was conducted on an agricultural enterprise, allowing its effectiveness to be evaluated in real-world conditions.

The results of the research hold significant practical value for information security professionals, as the developed methodology, owing to its flexibility, can be adapted to the needs of organizations across various industries, ensuring its versatility and broad applicability.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VCDB	—	VERIS Community Database
VERIS	—	Vocabulary for Event Recording and Incident Sharing
DBIR	—	Data Breach Investigations Report
ISO	—	International Organization for Standardization
IEC	—	International Electrotechnical Commission
DoCRA	—	Duty of Care Risk Analysis
COBRA	—	Consultative, Objective and Bi-functional Risk Analysis
NIST	—	National Institute of Standards and Technology
FAIR	—	Factor Analysis of Information Risk
CRAMM	—	CCTA Risk Analysis and Management Method
ІБ	—	Інформаційна безпека
ІТ	—	Інформаційні технології

ВСТУП

У сучасних умовах стрімкої цифровізації, що стає основою розвитку бізнесу, інформаційна безпека набуває вирішального значення для забезпечення стабільності, ефективності та конкурентоспроможності організацій. Особливого значення це набуває для агрохолдингів, які активно використовують інформаційні системи для управління виробничими процесами, фінансами та логістикою. Захист інформаційних активів у цьому контексті є ключовою умовою збереження стратегічних інтересів організацій.

Аграрний сектор, як і інші галузі, стикається з такими загальними небезпеками, як кібератаки, витоки конфіденційних даних та збої в роботі інформаційних систем, які можуть призвести до значних фінансових втрат і порушення бізнес-процесів. Водночас існуючі методології оцінки ризиків нерідко виявляються недостатньо адаптованими до особливостей окремих галузей, що ускладнює їх застосування у практичній діяльності аграрного сектору. Це створює потребу у розробці нових підходів, для забезпечення ефективного управління ризиками.

Враховуючи зазначені проблеми, було розроблено методологію, яка відповідає вимогам одного з найбільших агрохолдингів Західної України – Контінентал Фармерс Груп. Методологія розроблена з урахуванням міжнародних стандартів, що дозволяє впроваджувати заходи безпеки ефективно й раціонально, забезпечуючи належний рівень захисту інформаційних активів без порушення бізнес-процесів.

Метою даного дослідження є створення методології для оцінки ризиків інформаційної безпеки, яка забезпечує збалансований підхід до впровадження заходів безпеки, враховує вимоги бізнесу та може бути адаптована для використання в різних галузях.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– Провести аналіз сучасних методологій оцінки ризиків інформаційної безпеки.

– Визначити критерії оцінки ризиків, враховуючи очікуваність загроз і їхній вплив на бізнес-процеси.

– Розробити адаптовану методологію оцінки ризиків, інтегруючи під міжнародні стандарти та галузеві особливості.

– Виконати апробацію розробленої методології на прикладі аграрного підприємства.

– Запропонувати напрями для подальшого вдосконалення методології.

Об’єктом дослідження є процеси управління ризиками інформаційної безпеки в аграрному секторі.

Предметом дослідження є методологія оцінки ризиків інформаційної безпеки.

Новизна роботи полягає у створенні методології оцінки ризиків інформаційної безпеки, яка вперше дозволяє враховувати вплив ризиків окремо на ключові аспекти діяльності організації: місію, фінансові цілі, операційні процеси та зобов'язання. Методологія базується на принципі визначення ризику за найбільш значущим впливом, що забезпечує пріоритезацію заходів безпеки з урахуванням стратегічних та операційних пріоритетів організації.

Хоча методологія розроблена відповідно до вимог конкретної компанії, її гнучкість робить її придатною для адаптації до потреб інших галузей. Це створює потенціал для її комерційного застосування, дозволяючи організаціям впроваджувати ефективний баланс між заходами безпеки та бізнес-цілями.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: XII науково-технічна конференція «Інформаційні моделі, системи та технології» (м. Тернопіль, Україна).

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 МЕТОДИ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття ризиків інформаційної безпеки

У сучасному світі інформаційні технології стали невіддільною складовою функціонування будь-якої організації, що все частіше використовують цифрові системи для управління виробничими процесами, ресурсами та даними.

Діяльність будь-якого підприємства завжди пов’язана з різними ризиковими подіями. Аналізуючи саме поняття «ризик» слід виділити дослідження авторів Гросул В. А. та Усової М. О. [1], які зазначають, що ризик підприємства – це об’єктивно-суб’єктивна категорія, що характеризує невизначеність у сучасному економічному просторі внаслідок дії факторів бізнес-середовища, які мають як прямий, так і непрямий вплив на діяльність підприємства.

У контексті інформаційної безпеки, вважаємо, що ризик визначається як ймовірність того, що загрози та вразливості призведуть до втрати конфіденційності, цілісності чи доступності інформаційних ресурсів бізнесу.

Поняття інформаційного ризику розкрито в статті Ілляшко К.В [2] як ризик втрат, що виникли у результаті впливу навмисних або спадкових подій на інформаційні системи.

На думку авторів Карпович І.М., Гладка О.М., Наконечна Ю.А. [3] ефективність захисту інформації залежить від підходу до її організації та правильного вибору методів розрахунку ризиків інформаційної безпеки.

Визначаючи поняття інформаційної безпеки, слід звернутись до наукової праці автора Гончарова М.В. [4], який говорить, що суть інформаційної безпеки доволі розмита.

Тому найбільш актуальним, вважаємо визначення авторів Акімова Н. С., Кирильєва Л. О., Наумова Т. А. [5], які розкривають інформаційну безпеку як процес створення відповідних умов щодо формування ефективної системи захисту та обміну інформацією на підприємстві.

Розглядаючи принципи інформаційної безпеки, на яких вона базується, вважаємо доцільним виділити три основні які було зазначено на сайті компанії Microsoft [6] (див. рисунок 1.1).

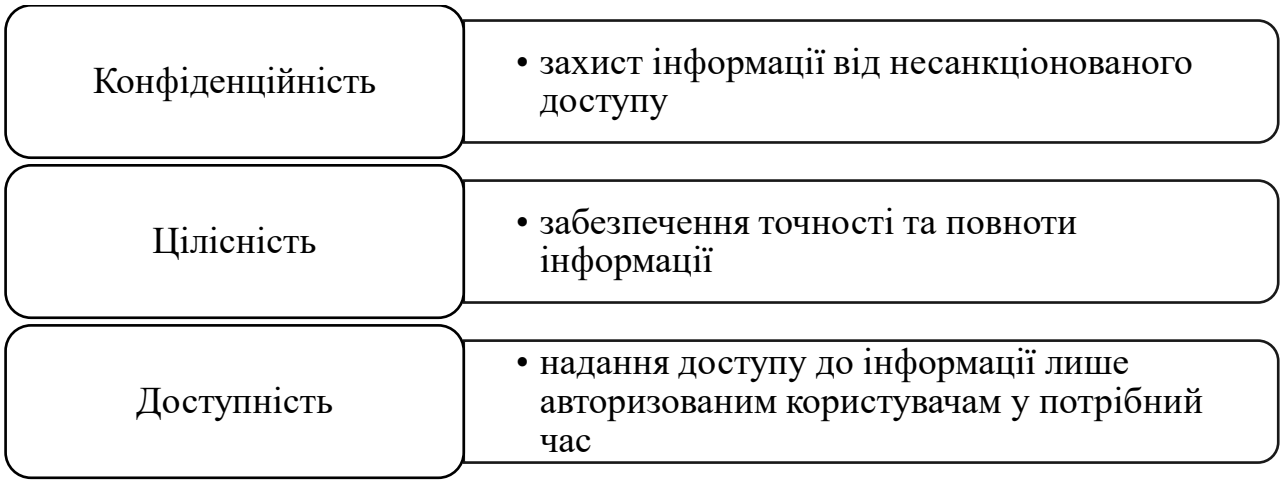

Рисунок 1.1 – Принципи інформаційної безпеки

Отже, ризики інформаційної безпеки виникають тоді, коли існує потенційна загроза, що може реалізуватися через вразливість та вплинути на функціонування інформаційних систем та порушенні таких важливих принципів як захист інформації від несанкціонованого доступу, забезпечення точності та повноти інформації і надання доступу тільки авторизованим користувачам.

1.2 Управління ризиками в інформаційній безпеці

Управління ризиками інформаційної безпеки є критично важливим для будь-якого сучасного бізнесу, оскільки інформація стала одним із ключових активів організацій.

Сьогодні підприємства залежать від інформаційних систем, які слугують для управління процесами, планування та прийняття стратегічних рішень. В умовах цифровізації будь-який інцидент у сфері інформаційної безпеки може спричинити серйозні наслідки для підприємства, включаючи фінансові втрати, зупинку операційної діяльності та втрату конкурентних переваг.

Тому, основна мета управління ризиками – це досягнення балансу між витратами на безпеку та рівнем прийнятного ризику для бізнесу.

Процес управління ризиками в інформаційній безпеці є досить важливим та багатокомпонентним, тому розглянем її за допомогою рисунку 1.2.

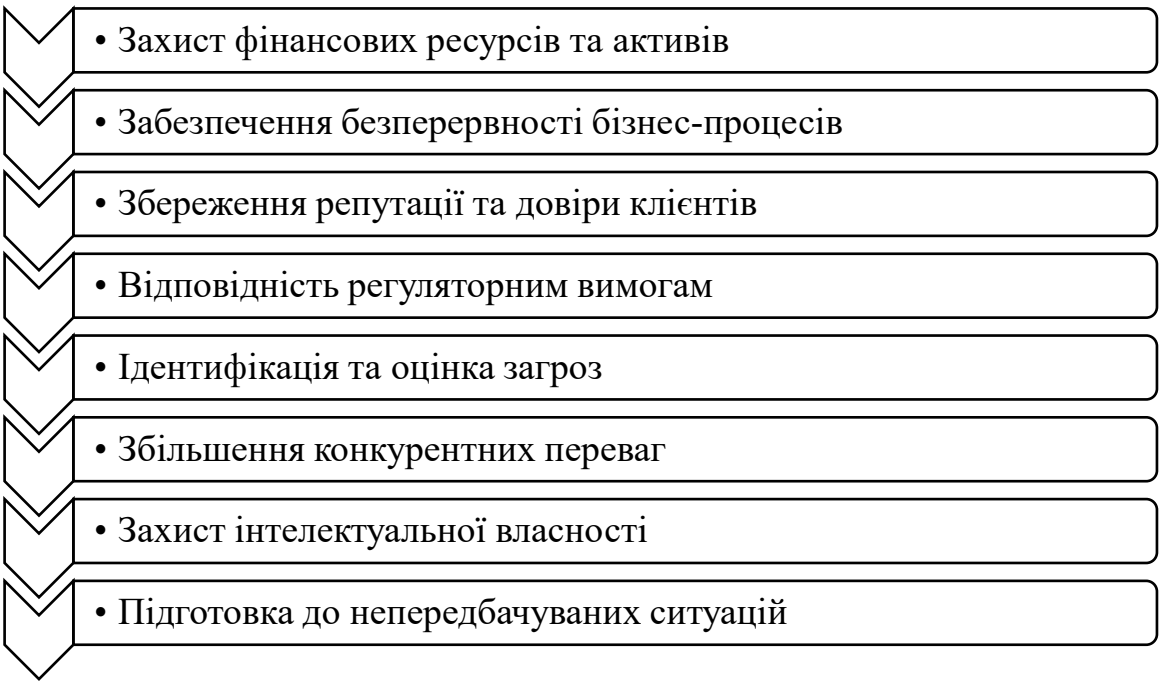

Рисунок 1.2 – Показники важливості управління ризиками в інформаційній безпеці для бізнесу

Розкриваючи більш детально кожен з показників, слід зазначити, що перший – захист фінансових ресурсів та активів є важливим, адже кібератаки, зокрема віруси, зловмисне програмне забезпечення та несанкціонований доступ, можуть призвести до фінансових втрат через крадіжку даних, зупинку виробництва чи виплату викупу (наприклад, у випадку Ransomware). Управління ризиками допомагає виявити потенційні загрози і вжити заходів для їх мінімізації.

Наступний показник – забезпечення безперервності бізнес-процесів є не менш важливим, адже будь-яке порушення роботи інформаційних систем може призвести до зупинки основних бізнес-процесів, а ефективне управління ризиками дозволяє завчасно розробити плани безперервності (Business Continuity Plans) та швидко реагувати на інциденти.

Збереження репутації та довіри клієнтів є основою для будь-якої компанії, тому управління ризиками інформаційної безпеки дозволяє мінімізувати ці загрози та підтримувати позитивний імідж компанії.

Відповідність регуляторним вимогам також є важливим, оскільки сучасний бізнес повинен дотримуватися численних законодавчих норм та стандартів у сфері інформаційної безпеки, таких як GDPR (захист персональних даних), ISO/IEC 27001 (системи управління безпекою інформації) тощо. Невиконання цих вимог може призвести до штрафів та юридичної відповідальності.

Для бізнесу важлива ідентифікація та оцінка загроз, а управління ризиками дозволяє системно ідентифікувати загрози, оцінювати їх вплив і визначати найбільш критичні вразливості.

Підприємства, що ефективно управляють ризиками інформаційної безпеки, забезпечують надійність своїх операцій і стають більш конкурентоспроможними на ринку.

До прикладу, для агрохолдингів, критичною є інформація про інноваційні технології, нові методи вирощування культур або розробки у сфері автоматизації виробництва. Управління ризиками допомагає зменшити ймовірність крадіжки інтелектуальної власності.

Управління ризиками включає розробку планів реагування на інциденти (Incident Response Plans), що дозволяє швидко реагувати на загрози, мінімізуючи їх вплив на бізнес.

Таким чином, управління ризиками інформаційної безпеки є не лише необхідністю, а й важливим інструментом для стратегічного розвитку та конкурентоспроможності бізнесу. У випадку підприємств, що працюють з великими обсягами даних і цифровими інфраструктурами, це питання стає критично важливим для забезпечення ефективної та безперебійної діяльності.

1.3 Процес оцінки ризиків інформаційної безпеки

Для ефективного функціонування підприємства необхідно розробити та впровадити дієві системи управління й оцінки ризиків інформаційної безпеки.

Одним із ключових елементів успішного управління ризиками є система оцінки ризиків інформаційної безпеки, оскільки вона дозволяє застосовувати математичні методи та моделі для систематизації й об’єктивного аналізу даних. Це сприяє отриманню більш точних, обґрунтованих і послідовних результатів, завдяки чому керівництво може приймати своєчасні та ефективні рішення для мінімізації ризиків інформаційної безпеки [8].

Щоб захистити свої дані від кіберзлочинності та підвищити загальну безпеку, потрібна комплексна програма захисту інформаційних технологій [9].

Усі організації, які використовують IT-інфраструктуру, повинні проводити оцінку ризиків кібербезпеки, яку доцільно проводити за наведеного алгоритму, розробленого авторами Яцків Н.Г. та Вівчар Д.В. на рисунку 1.3.

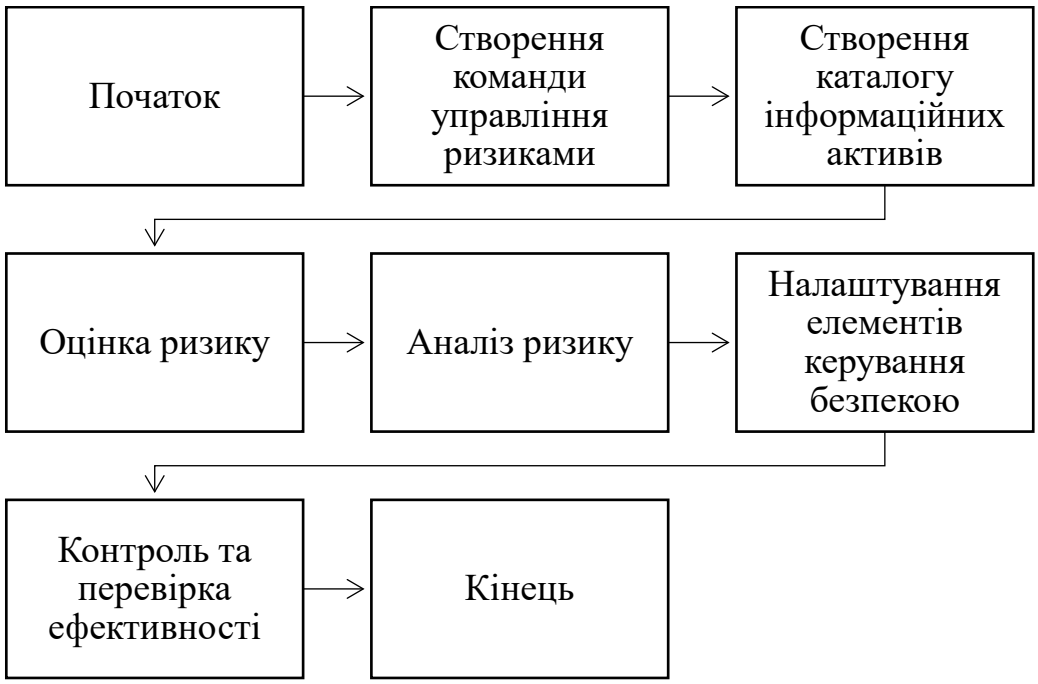

Рисунок 1.3 - Алгоритм оцінки ризиків

Процес оцінки ризику включає чотири основні етапи, які зазначає автори Яцків Н.Г. та Вівчар Д.В. [9]:

1) Підготовка до проведення оцінки.
2) Безпосереднє виконання оцінки.
3) Представлення результатів оцінки.
4) Підтримка та актуалізація оцінки.

Детальна структура етапів процесу оцінки ризику та відповідні завдання наведені на рисунку 1.4.

Рисунок 1.4 – Процес оцінки ризику

Кожен крок алгоритму розділений на набір завдань. Для кожного завдання керівництво надає додаткову інформацію для організацій, які проводять оцінку ризиків.

Крім того, процес розрахунку оцінок ризиків інформаційної безпеки підприємства передбачає визначення потенційних загроз, вразливих місць та можливих наслідків їх реалізації.

Нижче представлено основні формули, які використовуються для обчислення оцінок ризику інформаційної безпеки:

Рівень ризику (R) можна розрахувати за формулою [8]:

$$R = P \times I \tag{1.1}$$

де:

R - рівень ризику,

P - ймовірність виникнення загрози ($0 \leq P \leq 1$),

I - потенційний збиток від реалізації загрози.

Ймовірність виникнення загрози (P) розраховується так:

$$P = T \times V \tag{1.2}$$

де:

P - ймовірність виникнення загрози ($0 \leq P \leq 1$),

T - ймовірність виникнення джерела загрози ($0 \leq T \leq 1$),

V - ймовірність вразливості системи до загрози ($0 \leq V \leq 1$).

Співвідношення ризиків (RR) можна розрахувати за формулою:

$$RR = (R1 - R2) / R1 \quad (1.3)$$

де:

RR - співвідношення ризиків,

R1 - рівень ризику до впровадження контрольних заходів,

R2 - рівень ризику після впровадження контрольних заходів.

Ці формули та алгоритми можна використовувати як основу для розрахунку оцінок ризику інформаційної безпеки підприємства.

1.4 Аналіз існуючих методологій для оцінки ризиків інформаційної безпеки

Оцінка та управління ризиками інформаційної безпеки стають важливими завданнями, що потребують комплексного підходу та адаптованих до галузі методологій.

Вибір методології залежить від специфіки бізнесу, масштабів організації, доступних ресурсів та глибини необхідного аналізу [15] .

На сьогодні існує багато методологій для оцінки ризиків інформаційної безпеки, що відрізняються підходами, рівнем деталізації та сферою застосування. Серед найпоширеніших можна виділити:

– OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) фокусується на ідентифікації критично важливих активів та оцінці загроз.

– COBRA (Consultative, Objective and Bi-functional Risk Analysis) дозволяє організаціям проводити швидкий і точний аналіз ризиків, адаптуючи процес до їхніх конкретних потреб.

– ISO/IEC 27005 є стандартизованим підходом до оцінки ризиків на основі міжнародних стандартів управління безпекою.

– FAIR (Factor Analysis of Information Risk) є кількісною моделю оцінки ризиків, що розраховує фінансові наслідки ризику.

– NIST SP 800-30 є керівництвом для оцінки ризиків, що використовується для організацій у США.

– DoCRA (Duty of Care Risk Analysis) є методологією, що фокусується на балансуванні між витратами на управління ризиками та їхнім впливом на бізнес.

Розглянемо детальніше кожну з методологій для оцінки ризиків інформаційної безпеки.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)– це методологія, розроблена дослідницьким центром SEI (Software Engineering Institute). Вона орієнтована на організації для проведення самооцінки ризиків інформаційної безпеки. OCTAVE дозволяє виявити критичні активи, потенційні загрози та вразливості.

Особливості методології OCTAVE засновані на [10]:

1) Орієнтації на бізнес-цілі організації.
2) Використанні процесу самооцінки
3) Процес оцінки ризиків включає:

– Ідентифікацію активів та загроз.

– Аналіз інфраструктури та визначення вразливостей.

– Розробку плану управління ризиками.

OCTAVE підходить для середніх та великих підприємств, які мають достатній ресурс для самостійного аналізу загроз.

COBRA (Consultative, Objective and Bi-functional Risk Analysis) є методологією, яка базується на структурованому підході до аналізу ризиків інформаційної безпеки з використанням автоматизованих інструментів [10].

COBRA включає такі етапи:

1) Визначення контексту, а саме аналіз бізнес-процесів, ідентифікація ключових активів та цілей безпеки.

2) Використання програмного забезпечення для ідентифікації загроз, оцінки їхнього впливу та ймовірності.

3) Формування рекомендацій для мінімізації ризиків (технічні, організаційні, правові).

4) Повторний аналіз після впровадження заходів для оцінки їх ефективності.

COBRA є популярним вибором для організацій, які прагнуть знизити трудомісткість оцінки ризиків, зберігаючи високий рівень точності та об'єктивності.

ISO/IEC 27005 – є міжнародним стандартом для управління ризиками інформаційної безпеки. Він є частиною серії стандартів ISO/IEC 27000 і надає інструкції для реалізації процесу управління ризиками, що відповідають вимогам ISO/IEC 27001 [11].

Основним аспектом ISO/IEC 27005 є те, що воно:

1) Підходить для всіх типів організацій, незалежно від їх розміру.

2) Містить повний цикл управління ризиками:

– Ідентифікація активів, загроз та вразливостей.

– Оцінка ймовірності та потенційного впливу ризиків.

– Розробка стратегії для їх обробки (уникнення, зменшення, прийняття чи перенесення ризику).

3) Використовує кількісні та якісні методи оцінки ризиків.

FAIR (Factor Analysis of Information Risk) – це методологія, що надає кількісний підхід до аналізу ризиків інформаційної безпеки. Розроблена для того, щоб оцінити фінансовий вплив ризиків на організацію [12].

Головними особливостями FAIR можна зазначити:

1) Фокусування на вимірюванні ризику в грошовому еквіваленті.

2) Дозволяє пріоритизувати ризики на основі їх фінансового впливу.

3) Процес оцінки ризиків включає:

– Ідентифікацію активів і загроз.

– Визначення ймовірності реалізації загроз.

– Обчислення фінансових наслідків.

FAIR є корисним для організацій, які хочуть обґрунтувати свої інвестиції в інформаційну безпеку на основі кількісного аналізу.

NIST SP 800-30 – це керівництво з управління ризиками, створене Національним інститутом стандартів і технологій США (NIST). Воно широко використовується для оцінки ризиків в інформаційній безпеці.

Ключовими аспектами NIST SP 800-30 можна зазначити такі [13]:

1) Ґрунтується на циклічному процесі управління ризиками.

2) Процес включає наступні етапи:

– Ідентифікація загроз, активів і вразливостей.

– Аналіз ймовірності та впливу загроз.

– Визначення рівня ризику.

– Пропонування заходів з мінімізації ризиків.

– Підходить для державних установ та приватних організацій.

Методологія NIST є детальною і гнучкою, що дозволяє її адаптувати під конкретні потреби підприємства.

DoCRA (Duty of Care Risk Analysis) – це методологія, що допомагає організаціям оцінювати ризики, враховуючи як безпеку, так і фінансові інтереси бізнесу [16].

Основна мета DoCRA полягає у забезпеченні прийнятного рівня ризиків, який відповідає інтересам бізнесу, співробітників, клієнтів і регуляторів. Ця методологія ґрунтується на принципах збалансованого аналізу ризиків та врахуванні не лише технічних, але й економічних, юридичних і репутаційних аспектів [14].

Ключовими етапами аналізу ризиків за DoCRA є:

1) Ідентифікація загроз і вразливостей.

2) Визначення критичних активів підприємства та потенційні ризики для їхньої безпеки.

3) Оцінка ймовірності та наслідків - аналіз, наскільки ймовірно, що ризик реалізується, і які будуть наслідки для бізнесу та зацікавлених сторін.

4) Вибір розумних заходів включає такі заходи безпеки, які мінімізують ризик до прийнятного рівня, але не створюють надмірного фінансового навантаження.

5) Визначення меж допустимого ризику на основі аналізу рівня ризику.

Основними особливостями DoCRA є те, що:

– Балансує між потребами в захисті інформаційних активів і бізнес-цілями.

– Враховує інтереси організації, її клієнтів та регуляторів.

– Оцінка ризиків здійснюється на основі принципів «розумного ризику», тобто ризики мають бути обґрунтовані та не перевищувати допустимих витрат на їх усунення.

– Підходить для підприємств, які прагнуть оптимізувати витрати на управління ризиками.

– DoCRA є корисною для бізнесу завдяки своїй орієнтації на баланс між витратами на безпеку та необхідним рівнем захисту.

– DoCRA враховує галузеві стандарти, нормативно-правові акти та юридичні вимоги. Це допомагає організації уникнути штрафів та юридичної відповідальності.

Перераховані методології мають свої переваги та сфери застосування. DoCRA є найбільш орієнтованою на баланс між бізнес-вимогами та інформаційною безпекою.

DoCRA є особливо важливою для підприємств, які хочуть не лише захистити свої дані, а й оптимізувати витрати на безпеку. Наприклад, великі організації, як-от агрохолдинги, мають багато інформаційних активів, які потрібно захистити. У той же час надмірні витрати на безпеку можуть негативно вплинути на фінансові результати. Методологія DoCRA допомагає знайти цей баланс, забезпечуючи оптимальний рівень безпеки за обґрунтовані витрати.

Тож, саме методологія DoCRA найбільше відповідає вимогам сучасного бізнесу, проте для агрохолдингів вона є недостатньо гнучкою та універсальною. Тому виникає необхідність розробки нової методології оцінки ризиків інформаційної безпеки, що враховуватиме специфіку аграрного сектору, масштабність діяльності та унікальні потреби агрохолдингів.

РОЗДІЛ 2 РОЗРОБКА МЕТОДОЛОГІЇ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ АГРОХОЛДИНГУ

2.1 Опис запропонованої методології

Методологія оцінки ризиків інформаційних технологій та інформаційної безпеки (ІТ та ІБ) розроблена для можливості обґрунтувати інвестиції та забезпечити «доцільне» (reasonable) впровадження заходів контролів. Вона допомагає визначити прийнятний рівень ризику, а також пріоритезувати контролі для управління ризиками.

Методологія передбачає наступні активності:

– розробка критеріїв оцінки ризику та критеріїв прийняття ризику, а саме встановлення та визначення критеріїв оцінки та прийняття ризику;

– моделювання ризиків, яке включає оцінку поточної реалізації контролів, які б запобігали або виявляли передбачувані загрози;

– оцінювання ризиків, яке є визначенням очікуваності і впливу порушень безпеки та отриманням кількісного значення оцінки ризиків для визначення, чи є виявлені ризики прийнятними;

– рекомендація контролів включає вибір контролів, які б зменшили неприйнятні ризики;

– оцінка рекомендованих контролів визначає аналіз доцільності рекомендованих контролів, щоб переконатися, що вони створюють прийнятно низькі ризики, не створюючи при цьому обтяження.

Для моделювання ризиків використовуються інформаційні активи або класи активів та контролі, визначені у стандарті «ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги.» (див. Додаток Б) і становлять основу для кожного аналізу. Аналіз ризиків на основі активів допомагає моделювати ризики, спочатку поставивши запитання: «ми повинні захистити всі ці активи, але за допомогою яких контролів і чому?».

2.2 Принципи та практики методології

Методологія управління ризиками інформаційних технологій (IT) та інформаційної безпеки (ІБ) базується на принципах «DoCRA (Duty of Care Risk Analysis)», що дозволяють збалансувати захист інформаційних активів і інтереси зацікавлених сторін, а саме [16]:

– аналіз ризиків повинен враховувати інтереси всіх сторін, які можуть постраждати від ризику;

– ризики мають бути знижені до рівня, який не вимагатиме відшкодування будь-якій стороні;

– контролі не повинні бути більш обтяжливими, ніж ризики, від яких вони захищають.

Для досягнення цих принципів застосовуються наступні практики:

– аналіз ризиків враховує ймовірність того, що загрози можуть призвести до значних наслідків;

– межі прийнятності викладені простою мовою і застосовуються до кожної категорії впливу та показника впливу в аналізі ризиків;

– оцінки впливу та очікуваності мають якісний компонент, який стисло формулює інтереси зацікавлених сторін та організації, що проводить оцінку;

– оцінки впливу та очікуваності обчислюються шляхом кількісних розрахунків, що дозволяє порівнювати всі оцінені ризики, контролі та критерії прийнятності ризиків;

– визначення впливу забезпечує, що величина шкоди для однієї сторони прирівнюється до величини шкоди для інших сторін;

– визначення впливу повинне мати чітку межу між тими величинами, які є прийнятними для всіх сторін, і тими, які не є прийнятними;

– визначення впливу охоплює місію організації або її цілі, що пояснює, чому організація та інші сторони взаємодіють із ризиком, а також власні інтереси організації та її зобов'язання щодо захисту інших від шкоди;

– аналіз ризиків ґрунтується на принципах ретельності для аналізу поточних та рекомендованих контролів;

– ризики аналізуються експертами, які використовують фактичні дані для оцінки ризиків та контролів;

– оцінка ризиків не може врахувати всі передбачувані ризики, тому вона повторюється для виявлення та обробки нових ризиків з часом.

Отже, методологія управління ризиками ІТ та ІБ забезпечує збалансований підхід до аналізу, оцінки та зниження ризиків, враховуючи інтереси всіх сторін і стратегічні цілі організації.

2.3 Розробка критеріїв оцінки ризику

2.3.1 Визначення категорій та показників впливу

Категорії впливу визначаються як ключові аспекти діяльності організації, на які можуть вплинути реалізовані ризики. Ці категорії використовуються для оцінки можливих наслідків інцидентів інформаційної безпеки. Основні категорії впливу, які розглядаються в рамках даної методології, включають:

– місія - основна функція або призначення організації, що визначає, чому вона існує і на що вона спрямовує свою діяльність;

– операційні цілі - досягнення гарантій того, що організація може захистити себе від шкоди, спричиненої інцидентами інформаційної безпеки або надмірними контролями;

– фінансові цілі - досягнення фінансових результатів, включаючи доходи, витрати та рентабельність;

– зобов'язання - виконання юридичних, регуляторних або договірних зобов'язань перед іншими сторонами, які можуть постраждати від інцидентів інформаційної безпеки або від непередбачуваних наслідків застосування контролів.

Для вимірювання ступеня шкоди, яку може зазнати організація в результаті реалізації загроз, використовуються показники впливу. Показники впливу визначаються за шкалою від 1 до 5, де:

1) Незначний вплив (1) - місія, цілі або зобов'язання організації майже не постраждають;

2) Прийнятний вплив (2) - вплив на організацію є незначним, але прийнятним (діяльність може продовжуватися без значних збоїв);

3) Неприйнятний вплив (3) - вплив викликає серйозні наслідки для місії або операційної ефективності організації, але відновлення можливе;

4) Високий вплив (4) - вплив суттєво порушує діяльність організації, і для відновлення потрібні значні ресурси;

5) Катастрофічний вплив (5) - непоправна шкода для місії або цілей організації, що може призвести до зупинки діяльності або невиконання зобов'язань.

Показники впливу повинні відповідати на наступні запитання:

– Якими є видимі докази того, що у випадку реалізації загрози зазначена категорія впливу не постраждає?

– Якими є видимі докази того, що у випадку реалізації загрози зазначена категорія впливу буде скомпрометована, але це не потребуватиме корекції?

– Якими є видимі докази того, що у випадку реалізації загрози зазначена категорія впливу буде скомпрометована таким чином, що це вимагатиме виправлення, але воно може бути досягнуто в ході звичайного ведення бізнесу?

– Якими є видимі докази того, що у випадку реалізації загрози зазначена категорія впливу буде скомпрометована настільки, що для її відновлення знадобляться значні зусилля?

– Якими є видимі докази того, що у випадку реалізації загрози зазначена категорія впливу буде скомпрометована настільки, що її неможливо буде досягти?

2.3.2 Визначення критеріїв властивого ризику

Властивий ризик - це потенційний максимальний вплив, який може статися за відсутності контролів. Властивий ризик визначається для кожного інформаційного активу або класу активів.

Критерієм властивого ризику є максимальне значення впливу, який інформаційні активи (класи активів) можуть спричинити для місії, цілей та зобов'язань.

Для оцінки ризиків можуть розглядатися класи та підкласи активів (див. рисунок 2.1).

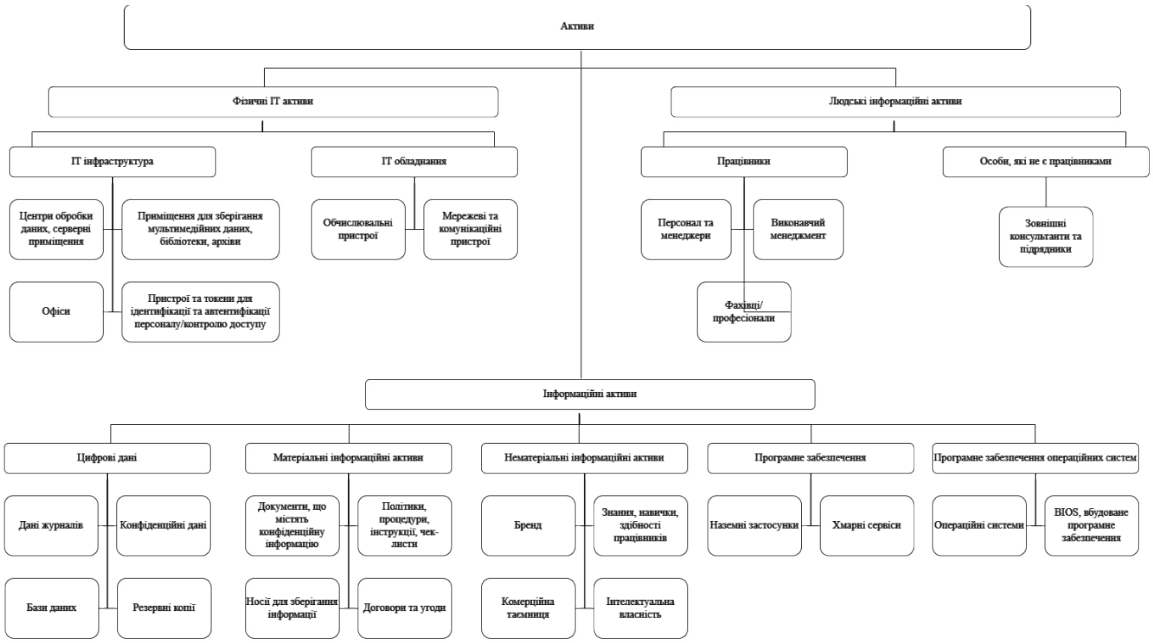

Рисунок 2.1 – Класи та підкласи активів

За необхідності, окремі інформаційні активи можуть бути виділені з класу активів (наприклад, конкретна інформаційна система, яку необхідно оцінити окремо, може бути виділена з класу «Програмне забезпечення»).

2.3.3 Визначення критеріїв очікуваності

Критерії очікуваності використовуються для оцінки ймовірності реалізації загрози або інциденту інформаційної безпеки та базуються на правилі, згідно з

яким очікуваність визначається зв'язком між можливостями контролю (з огляду на рівень його зрілості) та поширеністю загрози, на запобігання якої він спрямований.

Очікуваність визначається за шкалою від 1 до 5:

1) Вкрай малоймовірно (1) - контроль надійно запобігатиме загрозі.

2) Малоймовірно (2) - контроль запобігатиме більшості випадків реалізації загрози.

3) Настільки ймовірно, наскільки ні (3) - контроль запобігатиме стільком випадкам реалізації загрози, скільки й пропустить.

4) Ймовірно (4) - контроль запобігатиме деяким проявам загрози.

5) Точно відбудеться (5) - контроль не здатен запобігти реалізації загрози.

Оцінка зрілості контролів визначається з використанням такої шкали [19]:

1) Неіснуючий (1) - контроль не впроваджено або впроваджено не послідовно (заходи безпеки виконуються частково, з порушеннями, без дотримання встановлених правил або застосовуються лише в окремих випадках).

2) Обмежений (2) - контроль повністю впроваджений на деяких інформаційних активах або частково впроваджений на всіх інформаційних активах.

3) Визначений (3) - контроль впроваджений на всіх інформаційних активах.

4) Керований (4) - контроль регулярно тестується, а виявлені недоліки виправляються.

5) Оптимізований (5) - контроль забезпечений механізмами, які гарантують, що він буде виконуватися стабільно і безперервно протягом тривалого часу (контроль не деградує з часом і завжди забезпечує очікуваний рівень безпеки).

Для визначення поширеності загроз використовується база даних VCDB словника для запису подій та обміну інформацією про інциденти (VERIS).

За допомогою бази даних VCDB [17] визначається індекс VCDB, який відображає співвідношення кількості повідомлених інцидентів безпеки до

загальної кількості загроз, що були виявлені у відповідному класі інформаційних активів. Перелік визначених індексів VCDB в розрізі класів активів можна побачити в Додатку В, а співвідношення оцінки рівнів зрілості контролів до індексів VCDB для визначення очікуваності в Додатку Г.

2.3.4 Визначення критеріїв прийнятність ризику

Прийнятність ризику визначає рівень ризику, який організація готова прийняти без вжиття додаткових заходів, та визначається за формулою 2.1:

$$\text{Прийнятний ризик} < \text{Неприйнятний} \times \text{Неприйнятна очікуваність} \quad (2.1)$$

Ризики вважаються прийнятними, якщо їх розрахункове значення є меншим за встановлене порогове значення (наприклад, якщо показник неприйнятного впливу та неприйнятної очікуваності = 3, усі ризики зі значенням <9 вважаються прийнятними, а ≥9 неприйнятними та потребують обробки).

2.4 Моделювання та оцінка ризиків

Моделювання ризиків здійснюється шляхом ідентифікації інформаційних активів або класів активів (включаючи дані, інформаційні системи, мережеве обладнання, пристрої та інші ресурси), визначення контрольних заходів, які їх захищають, та аналізу можливих вразливостей, що можуть виникнути внаслідок відсутності або неналежного впровадження контролів.

Моделювання ризиків включає наступні етапи:

1) Ідентифікація та вибір інформаційних активів або класів інформаційних активів для оцінки.
2) Визначення контролів, які захищають ці інформаційні активи.
3) Оцінка рівня зрілості контролів.
4) Ідентифікація вразливостей на основі оцінки зрілості існуючих контрольних заходів і виявлення слабких місць або недоліків у їхньому

впровадженні чи функціонуванні, які можуть призвести до потенційних порушень безпеки.

5) Фіксація результатів ідентифікації у реєстрі ризиків для подальшої оцінки та обробки.

Моделювання ризиків повинне здійснюватися не рідше одного разу на рік, в разі значних змін в інформаційних системах або бізнес-процесах, або при виявленні нових загроз чи вразливостей. Виявлені нові ризики або зміни в існуючих повинні бути задокументовані та внесені до реєстру ризиків для подальшої оцінки.

Оцінювання ризиків є ключовим етапом оцінки ризиків, що дозволяє визначити рівень ризику для інформаційного активу або класу інформаційних активів, враховуючи результати моделювання.

Процедура оцінки ризиків повинна включати:

– оцінку очікуваності на основі поширеності загроз (індексу VCDB) та зрілості контролів;

– оцінювання ризиків на основі очікуваності та найбільшого впливу на категорії впливу (властивий ризик);

– класифікацію ризиків за рівнями критичності: низький, середній, високий, критичний.

Критерії оцінки ризиків встановлюються відповідно до наступних показників:

– вплив ризику (max): визначення можливих наслідків для місії, цілей та зобов’язань компанії;

– очікуваність реалізації ризику: оцінка ймовірності того, що ризик реалізується з урахуванням впроваджених контролів (або їх відсутності).

Для оцінювання ризиків використовується формула добутку властивого ризику (max) та очікуваності.

Результатом оцінювання ризиків є значення від 1 до 25, яке дозволяє забезпечити пріоритезацію обробки ризиків (чим більше значення ризику – тим більш пріоритетною повинна бути його обробка). Результати оцінки ризиків, нижчі за визначений рівень прийнятного ризик, автоматично вважаються

прийнятними. Ризики, які отримали оцінки, вищі за критерії прийнятності ризику, повинні бути зменшені шляхом підвищення зрілості існуючих контролів або впровадження нових.

Класифікація ризиків повинна базуватися на прийнятному рівні ризику, наприклад:

– низький рівень ризику (Low) містить оцінку від 1 до 8 – прийнятні ризики;

– середній рівень ризику (Medium) містить оцінку від 9 до 16 — ризики, що потребують додаткових заходів з обробки, але не є терміновими;

– високий рівень ризику (High) містить оцінку від 17 до 24 — ризики, що потребують першочергової обробки;

– критичний рівень ризику (Critical) містить оцінку 25 — ризики, що вимагають негайних і суттєвих заходів з обробки.

Незважаючи на використання кількісної оцінки, рівень ризику не завжди точно відповідає числовому значенню. Остаточна класифікація ризику може бути скоригована залежно від контексту, наприклад, якщо інформаційний актив є критично важливим для досягнення цілей, або якщо ефективність контролів суттєво впливає на ймовірність реалізації загрози.

Результати оцінки ризиків повинні бути задокументовані у реєстрі ризиків із зазначенням рівня ризику для пріоритезації подальшої обробки, а також повинні використовуватися для пріоритезації ризиків з метою визначення послідовності та терміновості їх обробки відповідно до рівня критичності кожного ризику (чим вища кількісна оцінка ризику – тим частіше пов’язані загрози матимуть високий вплив, і тим вищим повинен бути пріоритет).

2.5 Оцінка рекомендованих контролів

Ризики, які за результатами оцінювання отримали неприйнятно високі значення, повинні бути зменшені шляхом вдосконалення (підвищення рівня зрілості) існуючих контролів, або застосування нових. Це передбачає вибір щодо того, які контролі будуть використовуватися для зменшення ризиків, а також

оцінка рекомендованих контролів, щоб переконатися, чи будуть вони ефективно зменшувати ідентифіковані ризики, не створюючи при цьому нових, неприйнятних ризиків.

Вибір контролів не повинен розглядатися як такий, що обов'язково забезпечить зниження усіх ризиків, оскільки вдосконалені або нові контролі можуть зменшити ризики в одній сфері (традиційно вважається, що це «залишковий ризик»), однак потенційно створити ризики в інших. Саме тому в методології замість терміну «залишковий ризик» використовується термін «ризик контролю».

Поширеними прикладами контролів, які підвищують ризики, є: нові засоби контролю безпеки, які сповільнюють продуктивність, заохочуючи персонал до пошуку небезпечних обхідних шляхів, суворий контроль доступу до інформації, необхідної в критичних ситуаціях, захист даних, який перешкоджає співпраці та дослідженням, шифрування, яке заважає моніторингу, або надмірно дорогі контролі.

Все це можна вважати «ризиками контролів», які можуть зашкодити місії, цілям та зобов'язанням. Тому контролі повинні впроваджуватися таким чином, щоб вони відповідали меті зниження ризиків, не створюючи при цьому нових ризиків (забезпечуючи доцільність).

Рекомендовані контролі оцінюються з використанням тих самих критеріїв оцінки ризиків, які були застосовані для оцінки ризиків, шляхом визначення:

- зрілості контролю після впровадження/покращення;
- очікуваності після впровадження;
- впливу після впровадження;
- значень ризику після впровадження.

В рамках оцінки рекомендованих контролів також може здійснюватися аналіз раціональності, що забезпечується шляхом порівняння очікуваних витрат на контролі в межах визначеного періоду з «прийнятним» показником впливу на фінансові цілі.

2.6 Обробка ризиків

Обробка ризиків здійснюється для зниження ризиків до прийнятного рівня або забезпечення умов для ефективного управління ними. Для кожного виявленого ризику повинен бути визначений метод обробки ризику, який може включати наступні варіанти:

– прийняття ризику застосовується, якщо рівень ризику є прийнятним для компанії без додаткових заходів;

– зниження ризику передбачає впровадження нових контролів або підвищення ефективності існуючих для зменшення очікуваності;

– уникнення ризику передбачає зміну бізнес-процесів або припинення діяльності, що спричиняє ризик;

– передача ризику передбачає передачу відповідальності за ризик третій стороні (наприклад, через страхування або аутсорсинг).

Обрані методи обробки ризиків повинні фіксуватися в плані обробки ризиків разом з:

– запропонованими контролями (або іншими заходами обробки) та описом їх впровадження;

– відповідальними особами за реалізацію плану;

– оцінку витрат на впровадження заходів обробки;

– терміном виконання заходів обробки ризиків.

Заходи обробки ризиків повинні впроваджуватися відповідно до рівня критичності ризиків:

– для критичних ризиків заходи повинні бути впроваджені у найкоротший можливий термін (не більше одного місяця);

– для високих ризиків заходи повинні бути впроваджені протягом трьох місяців;

– для середніх ризиків термін впровадження заходів не повинен перевищувати шість місяців;

– для низьких ризиків заходи не вимагають впровадження, однак за необхідності можуть бути впроваджені у термін до одного року.

Оптимальні терміни для впровадження заходів обробки ризиків повинні встановлюватися на основі аналізу рівня ризику, складності заходів та наявності ресурсів для їх виконання. Перед затвердженням, плани обробки ризиків повинні бути задокументовані та проаналізовані на предмет доцільності та раціональності.

Аналіз доцільності повинен здійснюватися шляхом оцінки очікуваних:

– зрілості контролю після обробки ризику;
– значень очікуваності після обробки ризику;
– значень впливу після обробки ризику;
– якісних та/або кількісних значень ризику.

Аналіз раціональності повинен здійснюватися шляхом порівняння очікуваних витрат на впровадження заходів обробки в межах року з «прийнятним» показником впливу на фінансові цілі. Якщо за результатами аналізу плани обробки ризиків виявилися не раціональними та/або не доцільними, заходи обробки повинні переглядатися, та, за необхідності, розглядатися додаткові/альтернативні рішення.

Для забезпечення контролю за впровадженням заходів обробки ризиків та оцінки їх ефективності, повинен здійснюватися їх регулярний моніторинг, частота якого визначається рівнем критичності ризику (не рідше одного разу на місяць для високих та критичних ризиків, та не рідше одного разу на три місяці для середніх ризиків). Результати моніторингу повинні документуватися та надаватися менеджменту компанії для аналізу і, за необхідності, коригування планів обробки ризиків. Якщо результати моніторингу демонструють, що заходи обробки не призводять до зниження ризику до прийнятного рівня, повинні розглядатися додаткові або альтернативні рішення.

У разі порушення відповідальними особами термінів впровадження заходів обробки ризиків повинні бути вжиті заходи, включаючи:

– перегляд причин затримки, оцінка можливого впливу на компанію через невчасне впровадження заходів, та, за необхідності, притягнення до адміністративної та/або дисциплінарної відповідальності відповідальних осіб;

– перенесення термінів із затвердженням та узгодженням нових строків виконання;

– визначення додаткових заходів для прискорення впровадження у разі, якщо затримка стосується критичних або високих ризиків.

Всі зміни у термінах впровадження заходів обробки ризиків повинні бути задокументовані та погоджені з відповідальними особами. Всі результати обробки ризиків, включаючи застосовані заходи, відповідальних осіб, терміни виконання та результати оцінки ефективності, повинні бути зафіксовані в реєстрі ризиків для забезпечення прозорості та контролю.

2.7 Моніторинг і повторна оцінка ризиків

Моніторинг ризиків повинен здійснюватися регулярно з метою забезпечення актуальності оцінки ризиків, своєчасного виявлення нових ризиків або змін у рівнях існуючих, а також перевірки ефективності впроваджених заходів обробки ризиків. Для моніторингу ризиків можуть використовуватися автоматизовані системи для збору та аналізу даних у режимі реального часу, що дозволяє оперативно виявляти інциденти та реагувати на загрози.

Моніторинг ризиків повинен здійснюватися на основі рівня критичності ризиків:

– критичні ризики – щомісяця;

– високі ризики – кожні 3 місяці;

– середні ризики: кожні 6 місяців;

– низькі ризики: щороку.

Моніторинг ризиків повинен включати:

– виявлення нових загроз та вразливостей, які можуть вплинути на рівень ризику;

– оцінку змін у ризиках після впровадження заходів обробки («ризик контролю»);

– аналіз ефективності впроваджених контролів з урахуванням нових умов або змін у бізнес-середовищі.

Позаплановий моніторинг ризиків може здійснюватися у разі виявлення значних інцидентів або змін у зовнішньому середовищі, що можуть суттєво вплинути на рівень ризику.

Повторна оцінка ризиків повинна здійснюватися:

– за результатами моніторингу;

– у разі суттєвих змін в інформаційних системах, бізнес-процесах або регуляторних вимогах;

– після впровадження нових технологій;

– у разі змін щодо ризик-апетиту компанії;

– на вимогу менеджменту компанії або у випадках порушення термінів впровадження заходів обробки;

– у разі значних змін щодо методології оцінки ризиків.

Під час повторної оцінки ризиків повинна здійснюватися переоцінка рівня ризику, зокрема очікуваності його реалізації та можливого впливу на місію, цілі та зобов’язання компанії. У разі виявлення нових ризиків або змін у існуючих ризиках, а також якщо моніторинг демонструє неефективність заходів обробки ризику, повинні бути переглянуті та оновлені заходи обробки ризиків відповідно до нових даних.

Результати моніторингу та повторної оцінки ризиків повинні бути задокументовані у реєстрі ризиків, включаючи зміни у рівнях ризиків, ризики контролів та ефективність заходів обробки ризиків.

2.8 Документування та звітування

Всі результати моніторингу ризиків, оцінок ризиків та заходів з обробки ризиків повинні бути задокументовані в реєстрі ризиків з метою забезпечення прозорості процесу управління ризиками, своєчасного інформування менеджменту компанії про поточний стан ризиків та їх обробку, а також збереження всіх відповідних даних для подальшого аналізу та аудиту. Для кожного ризику, виявленого в процесі ідентифікації, оцінки та обробки, повинен

бути створений окремий запис у реєстрі ризиків. Запис у реєстрі ризиків повинен включати:

– інформаційні активи або класи активів, що піддаються ризику, та їх вплив на місію, цілі та зобов’язання компанії;

– показник поширеності загроз для класів активів (індекс VCDB);

– контролі, що знижують ризик, опис їхнього впровадження та оцінку зрілості;

– виявлені вразливості;

– оцінку очікуваності;

– оцінку та рівень ризику;

– метод обробки ризику та опис запланованих заходів;

– вартість впровадження заходів з обробки;

– терміни впровадження заходів;

– оцінку доцільності та раціональності методу обробки та запланованих заходів;

– відповідальних осіб за ризик;

– дату останньої оцінки ризику.

Будь-які зміни до реєстру ризиків повинні фіксуватися в реєстрі змін для можливості аудиторських перевірок або аналізу. Реєстр ризиків повинен бути доступним лише менеджменту компанії та відповідальним працівникам, які задіяні у процесі управління ризиками, для подальшого аналізу і прийняття необхідних рішень. Результати моніторингу ризиків повинні надаватися менеджменту компанії щоквартально за результатами проведення регулярних оцінок у формі звіту з інформацією щодо:

– списку усіх ризиків із зазначенням їх поточного рівня критичності (низький, середній, високий, критичний);

– прогресу впровадження заходів обробки ризиків для кожного критичного та високого ризику;

– оцінка ризиків контролів для кожного активу після впровадження заходів обробки;

– пропозицій щодо коригувальних дій у випадку виявлення неефективності заходів обробки.

У разі виявлення ризиків високого або критичного рівня, інформація повинна бути негайно передана менеджменту компанії для оперативного прийняття рішень щодо їх обробки.

РОЗДІЛ 3 ПРАКТИЧНЕ ВИКОРИСТАННЯ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПРИКЛАДІ АГРОХОЛДИНГУ

3.1 Визначення місії, зобов’язань, операційних і фінансових цілей агрохолдингу

Для ефективного застосування запропонованої методології першочерговим етапом є визначення базових характеристик компанії-замовника, в нашому випадку – агрохолдингу "Контінентал Фармерс Груп", зокрема місії, зобов’язань, операційних та фінансових цілей. Ці аспекти формують основу для подальшого моделювання ризиків та оцінки їх впливу на бізнес-процеси компанії.

Провівши всебічний аналіз діяльності компанії, її бізнес-процесів, ключових цінностей та пріоритети розвитку компанії, стало зрозуміло, що місією компанії є забезпечення сталого розвитку через ефективну організацію польових робіт, впровадження передових технологій і гарантування надійності бізнес-процесів. Додатково, забезпечує свою цінність для партнерів і суспільства через прозоре управління, екологічну відповідальність і дотримання найвищих стандартів безпеки та якості.

Згідно з запропонованою методологією, місія визначає, які основні бізнес-функції повинні бути захищені, щоб забезпечити стійкість і безперервність роботи організації. У даному випадку це ключові аграрні процеси, такі як автоматизовані системи моніторингу врожайності, управління ланцюгами постачання, а також підтримка цифрових платформ для обліку та аналізу даних. Ці процеси критично залежать від безпеки інформаційних активів, що забезпечують їхню безперебійну роботу.

Зобов’язання компанії визначають основу для ідентифікації зовнішніх вимог та потенційних ризиків, здатних вплинути на стейкхолдерів. Враховуючи специфіку діяльності "Контінентал Фармерс Груп", основні зобов’язання компанії включають:

– використання інноваційних і сталих агротехнологій, спрямованих на збереження природних ресурсів і мінімізацію екологічного впливу;

– реалізація довгострокових ініціатив, спрямованих на розвиток місцевих громад через створення робочих місць, підтримку соціальних програм і підвищення економічного добробуту регіону;

– забезпечення своєчасного та якісного виконання польових робіт;

– захист інформаційних активів компанії та забезпечення стійкості бізнес-процесів від зовнішніх та внутрішніх загроз;

– дотримання національних і міжнародних стандартів у сфері безпеки, якості продукції та екології.

Зобов’язання в рамках методології формують основу для оцінки ризиків, спрямованих на підтримання довіри стейкхолдерів до компанії, захист її репутації, фінансової стійкості та безперервності операційної діяльності.

Операційні цілі компанії відображають, як вона планує забезпечити ефективність своїх бізнес-процесів і мінімізувати вплив потенційних загроз. Основні операційні цілі агрохолдингу включають:

– забезпечення стабільного виконання планів польових робіт із точністю до 95% термінів;

– забезпечення безперебійної роботи критичних інформаційних систем із доступністю на рівні 99,9%;

– впровадження автоматизованих систем моніторингу для виявлення та запобігання кіберзагрозам;

– оптимізація логістичних процесів із метою скорочення витрат на транспортування на 15%;

– розвиток цифрових компетенцій співробітників через навчання та підвищення кваліфікації.

В межах методології, ці операційні цілі слугують основою для визначення прийнятного рівня ризиків, зокрема оцінки того, наскільки потенційні інциденти інформаційної безпеки можуть вплинути на безперервність бізнесу.

Фінансові цілі компанії визначають економічні рамки, в межах яких відбувається управління ризиками. Основні фінансові цілі "Континентал Фармерс Груп" включають:

– досягнення щорічного приросту доходу на рівні 10% за рахунок підвищення операційної ефективності;

– скорочення операційних витрат на 5% шляхом впровадження автоматизації процесів;

– інвестування 15% річного прибутку в інноваційні технології, зокрема інформаційної безпеки та автоматизації;

– формування резервного фонду для покриття ризиків, пов’язаних із кіберзагрозами та іншими бізнес-ризиками.

Методологія використовує фінансові цілі для оцінки потенційного впливу ризиків на економічні показники компанії та встановлення пріоритетів у впровадженні заходів безпеки.

Визначення місії, зобов’язань, операційних та фінансових цілей є ключовим етапом методології. Ці параметри забезпечують зв’язок між бізнес-цілями компанії та ризиками інформаційної безпеки, дозволяючи оцінити вплив потенційних інцидентів на інформаційні активи та обґрунтувати доцільність впровадження відповідних заходів контролю.

3.2 Заповнення реєстру ризиків інформаційної безпеки за розробленою методологією

Заповнення реєстру ризиків інформаційної безпеки є важливим етапом у застосуванні розробленої методології для оцінки ризиків інформаційної безпеки після визначення категорій впливу. Реєстр ризиків представляє собою Excel-таблицю, яка є практичним інструментом для систематизації інформації про активи, впроваджені контрольні заходи та потенційні ризики. Важливо зазначити, що реєстр складається з двох основних частин: аналізу ризиків (Risk Analysis) та обробки ризиків (Risk Treatment). Така структура дозволяє створити основу для прийняття об’єктивних рішень у сфері управління інформаційною безпекою.

Початковим етапом є співставлення активів з відповідними контрольними заходами, що дозволяє забезпечити прозорість процесу та чітко визначити рівень

впровадженості заходів безпеки. На основі отриманих даних здійснюється розрахунок ключових показників ризику, які включають ймовірність реалізації ризику (Expectancy Score), вплив на місію організації (Impact to Mission), операційну діяльність (Impact to Operational Objectives), фінансові показники (Impact to Financial Objectives) та нормативні зобов'язання (Impact to Obligations). Вкінці формується інтегральний показник ризику (Risk Score), на основі якого визначається рівень ризику (Risk Level).

Цей поетапний підхід забезпечує глибоке розуміння поточного стану інформаційної безпеки організації та дозволяє ефективно визначати пріоритети в управлінні ризиками.

3.2.1 Визначення відповідності між активами та контрольними заходами

У розділі 2 було виконано ідентифікацію активів на категорії, ці категорії класифікуємо на відповідні класи й підкласи. Класи активів, такі як дані (Data), документація (Documentation), користувачі (Users), програмне забезпечення (Software), пристрої (Devices) та мережа (Network). Кожен з цих класів активів має бути захищеним через впровадження відповідних контрольних заходів, які забезпечують цілісність, конфіденційність та доступність даних і ресурсів організації. Детальний аналіз активів та їх характеристик дозволяє чітко співставити кожен клас активів з необхідними заходами безпеки.

У процесі аналізу визначаються основні групи активів, на які спрямований контроль, а також додаткові групи активів, для яких вплив контролю є менш вираженим. При цьому є класи активів, на які контроль не має прямого впливу.

Розглянемо організаційні контролі (Organizational controls), які спрямовані на створення, впровадження та моніторинг політик і процедур, що забезпечують управління інформаційною безпекою. Як видно з рисунку 3.1, де чорний кружечок у таблиці вказує на основний вплив контролю, білий кружечок — на додатковий вплив різних контролів один на одного, а порожнє поле означає відсутність впливу, ці контролі охоплюють широкий спектр активів, забезпечуючи їхню захищеність від потенційних ризиків.

Organizational controls						
Control	**Data**	**Documentation**	**Users**	**Software**	**Devices**	**Network**
Policies for information security		●	○			
Information security roles and responsibilities		○	●			
Segregation of duties		○	●			
Management responsibilities		○	●			
Contact with authorities		●				
Contact with special interest groups		●				
Threat intelligence	●	○				
Information security in project management		●				
Inventory of information and other associated assets	○	●			○	
Acceptable use of information and other associated assets		●	○			
Return of assets	○				●	
Classification of information	●	○				
Labelling of information	●					
Information transfer	●					○
Access control	●		○			
Identity management			●			
Authentication information			●			
Access rights	●		○			
Information security in supplier relationships		●				
Addressing information security within supplier agreements		●				
Managing information security in the ICT supply-chain		●				
Monitoring, review and change management of supplier services		●				
Information security for use of cloud services	●			○		
Information security incident management planning/preparation		●				
Assessment and decision on information security events		●				
Response to information security incidents		●	○			
Learning from information security incidents		●				
Collection of evidence	●					
Information security during disruption		●				
ICT readiness for business continuity					●	○
Legal, statutory, regulatory and contractual requirements		●				
Intellectual property rights	●					
Protection of records	●					
Privacy and protection of PII	●					
Independent review of information security		●				
Compliance with policies, rules and standards		●				
Documented operating procedures		●				

Рисунок 3.1 – Покриття організаційними контролями класів активів

Наприклад, організаційні контролі мають основний вплив на документацію (Documentation), дані (Data) та користувачів (Users). Серед ключових заходів, що застосовуються до цих активів, можна виділити політики інформаційної безпеки

(Policies for information security), ролі та обов'язки в галузі інформаційної безпеки (Information security roles and responsibilities), інвентаризація інформації та інших пов'язаних активів (Inventory of information and other associated assets), дотримання політик, правил та стандартів (Compliance with policies, rules and standards). Ці заходи дозволяють регламентувати робочі процеси, розподіл відповідальності та створення чітких вимог до збереження інформації.

На деякі класи активів, такі як пристрої (Devices), програмне забезпечення (Software) та мережа (Network), організаційні контролі мають обмежений або відсутній вплив. Це пов'язано з тим, що ці активи більше залежні від технічних або фізичних заходів захисту.

Розглянемо клас контролів, що стосуються персоналу (People controls). Як видно з рисунку 3.2, ці контролі спрямовані на управління ризиками, пов'язаними з людським фактором та забезпеченням інформаційної безпеки через політики, процеси та підвищення обізнаності.

People controls						
Control	**Data**	**Documentation**	**Users**	**Software**	**Devices**	**Network**
Screening			●			
Terms and conditions of employment		●	○			
Information security awareness, education and training		○	●			
Disciplinary process		○	●			
Responsibilities after termination/change of employment		○	●			
Confidentiality or non-disclosure agreements		●				
Remote working			●		○	
Information security event reporting	○		●			

Рисунок 3.2 – Покриття людськими контролями класів активів

Людські контролі створенні щоб захищати саме користувачів (Users), а не інші групи активів. Основні заходи включають перевірку (Screening), підвищення обізнаності, навчання та тренування з питань інформаційної безпеки (Information security awareness, education and training), обов’язки після завершення або зміни трудових відносин (Responsibilities after termination/change of employment), дисциплінарний процес (Disciplinary process). Такі заходи дозволяють мінімізувати ризики, пов'язані з людським фактором, шляхом

ретельного відбору персоналу, впровадження умов працевлаштування та навчання. Умови та положення трудових відносин (Terms and conditions of employment) та угоди про конфіденційність або нерозголошення (Confidentiality or non-disclosure agreements) спрямовані на забезпечення безпеки конфіденційної інформації та документації організації.

Додатковий вплив людські контролі мають на документацію (Documentation) та дані (Data). Наприклад, заходи підвищення обізнаності, навчання та тренування з питань інформаційної безпеки (Information security awareness, education and training) та дисциплінарний процес (Disciplinary process) спрямовані на підвищення обізнаності працівників щодо політик безпеки та відповідальності за захист конфіденційної інформації. Ці заходи також підтримують формування культури безпеки в організації, що допомагає мінімізувати ризики, пов'язані з людськими помилками або недотриманням правил.

Розглянемо клас фізичних контролів, які відіграють не менш важливу роль у забезпеченні безпеки активів (див. рисунок 3.3).

Physical controls						
Control	**Data**	**Documentation**	**Users**	**Software**	**Devices**	**Network**
Physical security perimeters					●	
Physical entry			○		●	
Securing offices, rooms and facilities		○			●	
Physical security monitoring		○			●	
Protecting against physical/environmental threats					●	
Working in secure areas			○		●	
Clear desk and clear screen	●		○			
Equipment siting and protection					●	
Security of assets off-premises	○				●	
Storage media	●					
Supporting utilities					●	
Cabling security						●
Equipment maintenance					●	
Secure disposal or re-use of equipment	○				●	

Рисунок 3.3 – Покриття фізичними контролями класів активів

Фізичні контролі забезпечують переважно захист пристроїв (Devices), де такі заходи, як фізичні межі безпеки (Physical security perimeters), фізичний доступ (Physical entry), захист офісів, приміщень і об'єктів (Securing offices, rooms

and facilities), моніторинг фізичної безпеки (Physical security monitoring) та обслуговування обладнання (Equipment maintenance), мають основний вплив. Наприклад, контроль фізичні межі безпеки (Physical security perimeters) має основний вплив на пристрої, забезпечуючи їх фізичний захист від несанкціонованого доступу. Аналогічно, контроль обслуговування обладнання (Equipment maintenance) гарантує стабільну роботу обчислювальної техніки шляхом регулярного обслуговування.

Лише додатковий вплив фізичні контролі мають на документацію (та користувачів. Це пов’язано з тим, що ці активи менше залежать від фізичної безпеки порівняно з іншими класами активів. Наприклад, заходи захисту офісів, приміщень і об'єктів (Securing offices, rooms and facilities) або політика чистого столу та чистого екрану (Clear desk and clear screen) забезпечують базовий рівень захисту для документації та облікових записів користувачів, але їхній вплив є обмеженим у порівнянні з впливом на пристрої.

На деякі класи активів фізичні контролі не мають прямого впливу, наприклад, програмне забезпечення (Software). Це пояснюється тим, що фізичні заходи зосереджені переважно на забезпеченні фізичної безпеки обладнання та інфраструктури, а не на управлінні обліковими записами чи функціонуванням програмного забезпечення.

Розглянемо клас технічних контролів, які є одними з основних інструментів забезпечення інформаційної безпеки, вони спрямовані на захист різних класів активів з різною мірою впливу.

Як бачимо з рисунку 3.4, група технічних контролів захищає різні групи активів, але найкраще - програмне забезпечення. Такі контролі як: безпечний життєвий цикл розробки (Secure development life cycle), вимоги до безпеки застосунків (Application security requirements), безпечна архітектура та інженерія систем (Secure system architecture and engineering), безпечне програмування (Secure coding), тестування безпеки у процесі розробки та приймання (Security testing in development and acceptance), розробка на аутсорсингу (Outsourced development), розділення середовищ розробки, тестування та експлуатації (Separation of development, test and production environments), управління змінами

(Change management), використання привілейованих утиліт (Use of privileged utility programs), інсталяція програмного забезпечення на операційні системи (Installation of software on operational systems), захист інформаційних систем під час аудиторських перевірок (Protection of information systems during audit tests), доступ до вихідного коду (Access to source code), захист від шкідливого програмного забезпечення (Protection against malware), управління технічними вразливостями (Management of technical vulnerabilities) та управління конфігурацією (Configuration management) в комплексі, забезпечують надійний захист програмного забезпечення (Software) та інших груп активів.

Technological controls						
Control	**Data**	**Documentation**	**Users**	**Software**	**Devices**	**Network**
User end point devices					●	
Privileged access rights	○		●			
Information access restriction	●					
Access to source code				●		
Secure authentication			●			
Capacity management					●	○
Protection against malware				●		
Management of technical vulnerabilities				●		
Configuration management				●		
Information deletion	●					
Data masking	●					
Data leakage prevention	●					
Information backup	●					
Redundancy of information processing facilities					●	
Logging	●					
Monitoring activities	●					
Clock synchronization					●	
Use of privileged utility programs			○	●		
Installation of software on operational systems				●		
Networks security	○					●
Security of network services	○					●
Segregation of networks	○					●
Web filtering			○			●
Use of cryptography	●					
Secure development life cycle		○		●		
Application security requirements				●		
Secure system architecture and engineering				●		
Secure coding				●		
Security testing in development and acceptance		○		●		
Outsourced development		○		●		
Separation of development, test and production env				●		
Change management		○		●	○	
Test information	●					
Protection of information systems during audit test	○			●		

Рисунок 3.4 – Покриття технічними контролями класів активів

Водночас технічні контролі мають найменший і здебільшого додатковий вплив на документацію. Наприклад, заходи для забезпеченя безпечного життєвого циклу розробки (Secure development life cycle), тестування безпеки у процесі розробки та приймання (Security testing in development and acceptance), розробка на аутсорсингу (Outsourced development), управління змінами (Change management) спрямовані лише на мінімізацію можливих ризиків, пов'язаних із документацією.

Такий підхід дозволяє організації забезпечити ефективний розподіл контрольних заходів між різними класами активів, враховуючи їх специфіку. Це сприяє створенню стійкої системи інформаційної безпеки, яка здатна адаптуватися до змін та забезпечувати безперервність бізнес-процесів.

3.2.2 Деталізація класів активів для визначення відповідностей контролям

У попередньому підрозділі було розглянуто, які класи активів охоплюють контрольні заходи та окреслено основні та додаткові області застосування контролів. Це дозволило сформувати загальне розуміння зв’язку між класами активів і контрольними заходами, що є критично важливим для подальшого аналізу ризиків. Однак, для якісної оцінки ризиків та побудови ефективного реєстру ризиків інформаційної безпеки необхідно переходити до більш детального аналізу активів.

Кожен актив організації має специфічні характеристики, залежно від яких визначається його рівень критичності та необхідний рівень впровадження контролів. Зважаючи на це, на наступному етапі аналізу акцент буде зроблено на оцінці ризиків для кожного підкласу активу.

Попередній підготовчий етап із визначення покриття контролями класів активів полегшує детальну оцінку, оскільки забезпечує розуміння, які контролі є релевантними для кожного класу активів. Це значно спрощує процес переходу від загального до конкретного аналізу, дозволяючи зосередитись на найбільш критичних активах.

Asset Class	Asset Subclass	ISO Control	ISO Control Title	Control Type	Cybersecurity concepts	Operational capabilites
Device	Computing and storage devices	A.5.3	Segregation of duties	Preventive	Protect	Governance Identity and access management
Documents	Policies, procedures, guidelines, checklists	A.5.2	Information security roles and responsibilities	Preventive	Identify	Governance
Documents	Policies, procedures, guidelines, checklists	A.5.3	Segregation of duties	Preventive	Protect	Governance Identity and access management
Software	On-premises applications	A.5.3	Segregation of duties	Preventive	Protect	Governance Identity and access management
Software	Cloud services	A.5.3	Segregation of duties	Preventive	Protect	Governance Identity and access management
Users	Specialists/professionals	A.5.2	Information security roles and responsibilities	Preventive	Identify	Governance
Users	Staff and managers	A.5.2	Information security roles and responsibilities	Preventive	Identify	Governance
Users	Specialists/professionals	A.5.3	Segregation of duties	Preventive	Protect	Governance Identity and access management
Users	Staff and managers	A.5.3	Segregation of duties	Preventive	Protect	Governance Identity and access management

Рисунок 3.5 – Фрагмент таблиці з результатами аналізу зв’язків між класами активів, їх підкласами та контролями

У межах магістерської роботи демонстрація застосування методології буде обмежена одним із розділів стандарту ISO — організаційними контролями A.5.2-A.5.3.

Фрагмент таблиці, зображеної на рисунку 3.5, демонструє результати попереднього аналізу зв’язку між класами активів та їх підкласами з відповідними контрольними заходами. Також відображено тип контролю (Control Type), концепції кібербезпеки (Cybersecurity concepts) та відповідні операційні можливості (Operational capabilites), що сприяють реалізації заходів інформаційної безпеки.

Тип контролю (Control Type) вказує на характер заходу безпеки, наприклад, профілактичний (Preventive). Це дає змогу класифікувати контролі за їхньою роллю в управлінні ризиками, такими як запобігання, виявлення чи реагування на загрози.

Концепції кібербезпеки (Cybersecurity concepts) відображають основні принципи безпеки, яких дотримуються під час впровадження заходів. На рисунку 3.5 представлені концепції, такі як "Protect" (захист) та "Identify" (виявлення), які відповідають ключовим завданням у рамках загального підходу до безпеки.

Операційні можливості (Operational Capabilities) - конкретні механізми або процеси, які забезпечують реалізацію заходів безпеки. Наприклад, "Governance" (управління) стосується управління політиками та процедурами, а "Identity and Access Management" (керування ідентифікацією та доступом) охоплює управління доступом та ідентифікацією.

Проведений аналіз дозволяє встановити чіткий зв’язок між активами та контрольними заходами, враховуючи їхню роль у забезпеченні інформаційної безпеки. Це створює основу для подальшого глибокого аналізу ризиків

3.1.3 Визначення показника зрілості контрольних заходів

На основі попереднього аналізу зв’язку між класами активів і контрольними заходами, наступним етапом є оцінка зрілості контрольних заходів. Для оцінки зрілості контрольних заходів важливо перевірити три ключові аспекти: рівень впровадженості заходів, наявність доказів їх реалізації та потенційні вразливості. Лише через комплексну перевірку цих компонентів можна визначити поточний стан системи безпеки.

Рівень впровадженості контрольних заходів відображає, наскільки контрольні механізми реалізовані в організації відповідно до прийнятих стандартів, політик та процедур. Для аналізу було здійснено детальне вивчення регламентуючих документів, технічних інструкцій та процесів, що діють у компанії. Наприклад, рольові матриці доступу, які застосовуються для

управління правами доступу до інформаційних систем, виявилися впровадженими лише для окремих систем, що вказує на необхідність їх повної інтеграції в організаційні процеси. Крім того, впровадження деяких контролів залишається на низькому рівні через відсутність регулярного перегляду регламентуючих документів.

Перевірка доказів впровадження спрямована на підтвердження того, що контрольні заходи не лише формально впроваджені, але й реально функціонують. Для цього було проаналізовано широкий спектр документів, включаючи регламенти, журнали доступу, протоколи аудиту та шаблони договорів. Наприклад, шаблони договорів включають положення про конфіденційність інформації, однак ці положення не завжди стандартизовані та відображені у всіх документах. Схожа ситуація спостерігається з доступом до пристроїв: хоча формальне розмежування доступу існує, відсутні документальні підтвердження цього процесу, що знижує рівень надійності впровадження.

Аналіз документації та процесів дозволив ідентифікувати ключові вразливості, що впливають на ефективність впровадження контрольних заходів. Серед основних проблем було виявлено:

– відсутність регулярного оновлення політик та регламентуючих документів;

– недостатню деталізацію вимог безпеки в існуючих шаблонах договорів;

– брак документації, яка формалізує існуючі процеси контролю доступу до активів.

Наприклад, доступ до пристроїв розмежовано, однак його формалізація потребує доопрацювання для відповідності вимогам стандартів.

Розрахунок показника зрілості (Safeguard Maturity Score) здійснюється на основі сукупного аналізу трьох зазначених аспектів. Для цього кожен контроль оцінюється за шкалою від 1 до 5 відповідно до критеріїв таблиці зрілості:

1) Неіснуючий (1) - контроль відсутній або не визначений. Процеси не розроблені, документація та докази реалізації відсутні.

2) Обмежений (2) - контроль визначений, але реалізований частково або на окремих активах.

3) Визначений (3) - контроль визначений і задокументований, але відбувається не завжди або нерегулярно. Процеси існують і описані, але їх належне виконання та якість не забезпечуються.

4) Керований (4) - контроль повністю впроваджений та функціонує відповідно до задокументованих процедур.

5) Оптимізований (5) - контроль постійно вдосконалюється на основі регулярного моніторингу.

Після розрахунку показника зрілості контрольних заходів, було отримано таблицю, що відображає результати оцінки зрілості для кожного активу. Ця таблиця (див. рисунок 3.6) стає базою для подальшого аналізу ризиків, бо демонструє взаємозв’язок між реалізацією контрольних заходів (Our Implementation), доказами їх впровадження (Evidence of Implementation) та виявленими вразливостями (Vulnerabilities).

В стовпці наша реалізація (Our Implementation) описується, як саме реалізовані контрольні заходи в організації. Наприклад, доступ до пристроїв розмежовано, але не задокументовано, або рольові матриці доступу використовуються для налаштування прав доступу в деяких системах.

Стовпець з доказами впровадження (Evidence of Implementation) містить підтвердження впровадження заходів безпеки, такі як наявність матриць доступу, додаткових документів (регламентів, стандартів, СОПів), які забезпечують нормативну основу для реалізації контрольних заходів.

Вразливості (Vulnerabilities) містять виявлені прогалини або недоліки. Наприклад, відсутність матриць доступу до пристроїв чи інформаційних систем. У випадках, де вразливості не виявлено, зазначається "не виявлено".

Така структура дозволяє ідентифікувати ключові аспекти впровадження заходів безпеки, оцінювати рівень відповідності вимогам та виявляти потенційні слабкі місця. Наприклад, відсутність документування для певних заходів, таких як доступ до пристроїв, може призвести до ускладнень у контролі доступу, що є важливим для усунення.

Asset Class	Asset Subclass	ISO Control	ISO Control Title	Our Implementation	Evidence of Implementation	Vulnerabilities	Safeguard Maturity Score
Device	Computing and storage devices	A.5.3	Segregation of duties	Доступ до пристроїв розмежовано, але не задокументовано	Відсутні	Відсутні матриці доступу до пристроїв	***2***
Documents	Policies, procedures, guidelines, checklists	A.5.2	Information security roles and responsibilities	Ролі учасників процесів інформаційної безпеки визначаються в рамках додаткових документів Положення	Додаткові документи положення (регламенти, стандарти, СОПи)	Не виявлено	***5***
Documents	Policies, procedures, guidelines, checklists	A.5.3	Segregation of duties	Політики та додаткові документи чітко описують обов'язки учасників процесів	Додаткові документи положення (регламенти, стандарти, СОПи)	Не виявлено	***5***
Software	On-premises applications	A.5.3	Segregation of duties	Для частини систем з розробленими рольовими матрицями доступу налаштування прав доступу здійснюється у відповідності до матриць	Матриці доступу до інформаційних систем	Відсутні матриці доступу до усіх інформаційних систем	***2***
Software	Cloud services	A.5.3	Segregation of duties	Для частини систем з розробленими рольовими матрицями доступу налаштування прав доступу здійснюється у відповідності до матриць	Матриці доступу до інформаційних систем	Відсутні матриці доступу до усіх хмарних інформаційних систем	***2***
Users	Specialists / professionals	A.5.2	Information security roles and responsibilities	Ролі учасників процесів інформаційної безпеки визначаються в рамках додаткових документів Положення	Додаткові документи положення (регламенти, стандарти, СОПи)	Не виявлено	***5***
Users	Staff and managers	A.5.2	Information security roles and responsibilities	Політика інформаційної безпеки та її процеси доносяться до усіх працівників при впровадженні або змінах, дотримання відстежується в рамках процесів	Додаткові документи положення (регламенти, стандарти, СОПи)	Не виявлено	***5***
Users	Specialists/professionals	A.5.3	Segregation of duties	Технічні кроки в процесах розподілені між фахівцями для уникнення конфлікту інтересів	Додаткові документи положення (регламенти, стандарти, СОПи)	Не виявлено	***5***
Users	Staff and managers	A.5.3	Segregation of duties	Здійснюється чітке визначення розподілу обов'язків в межах процесів ІБ над різними етапами процесів	Додаткові документи положення (регламенти, стандарти, СОПи)	Не виявлено	***5***

Рисунок 3.6 – Фрагмент таблиці після визначення показника зрілості контролів

Таким чином, проведений аналіз дозволяє чітко визначити рівень впровадження контрольних заходів, їх зрілість та вразливості, які потребують усунення. Ці результати є основою для обчислення показника зрілості контрольних заходів (Safeguard Maturity Score) та формування наступних етапів

оцінки ризиків, включаючи оцінку очікуваності (Expectancy Score), оцінку впливу (Impact Score) та інші.

3.1.4 Визначення критеріїв впливу

Для ефективної оцінки ризиків недостатньо обмежуватися аналізом зрілості контрольних заходів. Необхідно також визначити вплив потенційних інцидентів на ключові аспекти функціонування організації. У цьому розділі розглядаються основні критерії впливу, зокрема VCDB індекс, оцінка очікування (Expectancy Score), вплив на місію (Impact to Mission), вплив на оперативні цілі (Impact to Operational Objectives), вплив на фінансові цілі (Impact to Financial Objectives), вплив на зобов'язання (Impact to Obligations). Ці показники є важливими елементами для формування комплексної оцінки ризиків та розробки дієвих стратегій їхнього управління.

VCDB індекс є показником, що характеризує частоту інцидентів безпеки для кожного класу активів. Він базується на кількісному аналізі історичних даних про інциденти, зокрема інформації з бази DBIR. Для кожного класу активів було визначено відсоткову частку інцидентів від загальної кількості та відповідний індекс [18].

Таблиця визначених індексів VCDB у розрізі класів активів попередньо була сформована в розділі 2, а саму таблицю подано в додатку Б. Як видно з таблиці, класи активів підприємство (Enterprise), дані (Data) та користувачі (Users) мають найвищі індекси "3", що свідчить про високий рівень ризику. Натомість класи мережа (Network) і пристрої (Devices) мають найнижчі індекси "1", що вказує на відносно низьку частоту інцидентів. Оскільки такий індекс присвоюється класу активів, то автоматично кожен підклас отримує такий же індекс.

Очікуваність (Expectancy Score) визначає ймовірність реалізації ризику для кожного активу, враховуючи рівень зрілості впроваджених контрольних заходів (Safeguard Maturity Score) та індекс VCDB. Цей показник є ключовим у процесі

оцінки ризиків, оскільки дозволяє визначити, наскільки вразливим є актив до потенційних інцидентів.

Для спрощення розрахунків та підвищення точності аналізу, в розділі 2 була розроблена таблиця, яка зіставляє оцінки зрілості контрольних заходів (від 1 до 5) з індексами VCDB (від 1 до 5) для визначення очікуваності (Expectancy Score). Ця таблиця подана у додатку В.

Процедура визначення очікуваності (Expectancy Score):

1) Для кожного активу визначається його VCDB індекс, що був попередньо розрахований у розділі 2 (див. таблицю у додатку Б).

2) Встановлюється рівень зрілості контролів (Safeguard Maturity Score) для кожного контрольного заходу на основі результатів аналізу у розділі 3.1.3.

3) За допомогою таблиці у додатку В знаходиться відповідний рівень очікуваності (Expectancy Score) на основі співвідношення VCDB індексу та зрілості контролів (Safeguard Maturity Score).

Оцінка очікуваності (Expectancy Score) інтерпретується за шкалою:

– Непередбачувано (1).
– Передбачувано, але неочікувано (2).
– Очікувано, але не часто (3).
– Досить часто (4).
– Може траплятися прямо зараз (5).

		Safeguard Maturity Score				
VCDB index		1	2	3	4	5
	1	4	3	1	1	1
	2	4	3	2	2	1
	3	5	4	3	2	1
	4	5	4	4	3	2
	5	5	5	5	3	2

Рисунок 3.7 – Матриця Expectancy Score

Основні закономірності, що можемо побачити на рисунку 3.7:

– Високий рівень зрілості контрольних заходів (4 або 5) забезпечує низький рівень очікуваності інцидентів навіть для активів з високими індексами VCDB.

– Низький рівень зрілості контрольних заходів (1 або 2) значно підвищує очікуваність інцидентів, особливо для активів з індексами VCDB 3, 4 та 5.

– Середній рівень зрілості (3) формує помірний рівень очікуваності, який варіюється залежно від критичності активу та частоти інцидентів.

– Кожна клітинка матриці, на перетині параметрів, містить значення Expectancy Score, яке визначається залежно від взаємозв'язку цих двох параметрів.

Отже, можемо зробити висновок, що чим надійніше впроваджений контроль, тим менш очікувано, що поширена загроза стане причиною інциденту безпеки (див. рисунок 3.8).

Asset Class	Asset Subclass	ISO Control	ISO Control Title	Safeguard Maturity Score	VCDB Index	Expectancy Score
Device	Computing and storage devices	A.5.3	Segregation of duties	***2***	1	3
Documents	Policies, procedures, guidelines, checklists	A.5.2	Information security roles and responsibilities	***5***	3	1
Documents	Policies, procedures, guidelines, checklists	A.5.3	Segregation of duties	***5***	3	1
Software	On-premises applications	A.5.3	Segregation of duties	***2***	2	3
Software	Cloud services	A.5.3	Segregation of duties	***2***	2	3
Users	Specialists / professionals	A.5.2	Information security roles and responsibilities	***5***	3	1
Users	Staff and managers	A.5.2	Information security roles and responsibilities	***5***	3	1
Users	Specialists/professionals	A.5.3	Segregation of duties	***5***	3	1
Users	Staff and managers	A.5.3	Segregation of duties	***5***	3	1

Рисунок 3.8 – Фрагмент таблиці після обчислення значень очікуваності

Після того як було визначено показник очікуваності (Expectancy Score) для розуміння чи зможе саме цей контроль захистити групу активів, наступним кроком є оцінка впливу потенційних інцидентів (див. рисунок 3.9). Вплив оцінюється за чотирма критеріями:

– Вплив на місію (Impact to Mission) характеризує, рівень впливу на здатність організації виконувати свої стратегічні завдання та ключові функції. Це може включати вплив на основну діяльність, репутацію чи здатність підтримувати безперервність роботи.

– Вплив на операційні цілі (Impact to Operational Objectives) визначає вплив на основні бізнес-процеси організації, такі як логістика, виробництво, обслуговування клієнтів чи підтримка інформаційних систем.

– Вплив на фінансові цілі (Impact to Financial Objectives) оцінює потенційні фінансові наслідки, включаючи втрати доходів, штрафи, витрати на усунення.

– Вплив на зобов’язання (Impact to Obligations) визначає вплив на виконання організацією нормативних, договірних або етичних зобов’язань перед клієнтами, партнерами чи регуляторами.

Для кожної категорії впливу визначено шкалу оцінок від 1 до 5:

1) Незначний (1) - мінімальний або несуттєвий вплив, який не створює суттєвих перешкод для операцій чи зобов’язань.

2) Прийнятний (2) - прийнятний вплив, що може викликати деякі труднощі, але не призводить до серйозних наслідків.

3) Неприйнятний (3) - вплив, що вимагає значних коригувальних дій або ресурсів для мінімізації наслідків.

4) Високий (4) - значний вплив, який може бути відновлений, але викликає серйозні перешкоди у виконанні ключових функцій.

5) Катастрофічний (5) - катастрофічний вплив, що призводить до незворотних наслідків або суттєво порушує діяльність організації.

Asset Class	Asset Subclass	ISO Control	ISO Control Title	Safeguard Maturity Score	VCDB Index	Expectancy Score	Impact to Mission	Impact to Operational Objectives	Impact to Financial Objectives	Impact to Obligations
Device	Computing and storage devices	A.5.3	Segregation of duties	***2***	1	3	4	4	4	4
Documents	Policies, procedures, guidelines, checklists	A.5.2	Information security roles and responsibilities	***5***	3	1	5	5	5	5
Documents	Policies, procedures, guidelines, checklists	A.5.3	Segregation of duties	***5***	3	1	5	5	5	5
Software	On-premises applications	A.5.3	Segregation of duties	***2***	2	3	4	4	4	4
Software	Cloud services	A.5.3	Segregation of duties	***2***	2	3	4	4	4	4
Users	Specialists / professionals	A.5.2	Information security roles and responsibilities	***5***	3	1	5	5	5	5
Users	Staff and managers	A.5.2	Information security roles and responsibilities	***5***	3	1	4	4	4	3
Users	Specialists/professionals	A.5.3	Segregation of duties	***5***	3	1	5	5	5	5
Users	Staff and managers	A.5.3	Segregation of duties	***5***	3	1	4	4	4	3

Рисунок 3.9 – Фрагмент таблиці після оцінки впливу потенційних інцидентів

Додатково, критерії впливу дозволяють організаціям проводити фінансове обґрунтування ризиків, оцінюючи, які витрати є виправданими для зменшення певного рівня впливу. Цей підхід робить аналіз ризиків не лише технічним, але й економічно доцільним.

3.1.5 Визначення рівня ризику

Після того як значення очікуваність (Expectancy Score) та вплив (Impact Score) було визначено для кожного активу, наступним етапом є розрахунок значення ризику (Risk Score). Ця величина дозволяє кількісно оцінити ризик для кожного активу на основі його очікуваності та впливу потенційних інцидентів. Методологія пропонує модель для інтеграції цих критеріїв у загальний процес оцінки ризиків, яка базується на формулі добутку впливу та очікуваності для обчислення значення ризику.

Під час розрахунку значення ризику (Risk Score) вибирається найбільше значення серед усіх категорій впливу (Impact Score), яке підставляється у формулу разом із значенням очікуваності (Expectancy Score). Таким чином,

формула враховує як очікуваність реалізації ризику, так і його найсерйозніший можливий наслідок для організації.

Результатом розрахунку значення ризику (Risk Score) є числове значення в межах від 1 до 25, яке потім інтерпретується відповідно до рівня ризику (Risk Level), використовуючи триколірну шкалу: зелений, жовтий та червоний кольори. Ця шкала дозволяє швидко ідентифікувати ризики, які мають найбільший пріоритет, та приймати обґрунтовані рішення щодо їх мінімізації.

Матриця ризиків (risk map), зображена на рисунку 3.10, є інструментом для візуалізації співвідношення між очікуваністю (Expectancy Score) та впливом (Impact Score). Вона допомагає визначити:

– Зелені зони позначають прийнятні ризики з низьким рівнем очікуваності та/або впливу (Low).

– Жовті зони позначають ризики середнього рівня, які потребують подальшої уваги (Medium).

– Червоні зони позначають високі та критичні ризики, які потребують негайного втручання (High/Critical).

Expectancy / Impact	1	2	3	4	5
1					
2					
3					
4					
5					

Рисунок 3.10 – Матриця ризиків

Прийнятний рівень ризику в нашому випадку встановлено до "9". Усі ризики з оцінкою "9" і вище вимагають відповідних дій для їх мінімізації. Особливу увагу слід приділяти ризикам, які мають найвищі значення ризику (Risk Score) і належать до червоних зон, оскільки вони становлять найвищу

загрозу для організації і потребують невідкладного втручання (див. рисунок 3.11).

Asset Class	Asset Subclass	ISO Control	ISO Control Title	Safeguard Maturity Score	VCDB Index	Expectancy Score	Impact to Mission	Impact to Operational Objectives	Impact to Financial Objectives	Impact to Obligations	Risk Score	Risk Level
Device	Computing and storage devices	A.5.3	Segregation of duties	***2***	1	3	4	4	4	4	12	Medium
Documents	Policies, procedures, guidelines, checklists	A.5.2	Information security roles and responsibilities	***5***	3	1	5	5	5	5	5	Low
Documents	Policies, procedures, guidelines, checklists	A.5.3	Segregation of duties	***5***	3	1	5	5	5	5	5	Low
Software	On-premises applications	A.5.3	Segregation of duties	***2***	2	3	4	4	4	4	12	Medium
Software	Cloud services	A.5.3	Segregation of duties	***2***	2	3	4	4	4	4	12	Medium
Users	Specialists / professionals	A.5.2	Information security roles and responsibilities	***5***	3	1	5	5	5	5	5	Low
Users	Staff and managers	A.5.2	Information security roles and responsibilities	***5***	3	1	4	4	4	3	4	Low
Users	Specialists / professionals	A.5.3	Segregation of duties	***5***	3	1	5	5	5	5	5	Low
Users	Staff and managers	A.5.3	Segregation of duties	***5***	3	1	4	4	4	3	4	Low

Рисунок 3.11 – Фрагмент таблиці після обчислення значень ризику

Розрахунок оцінки ризику (Risk Score) та рівня ризику (Risk Level) є важливим для ефективного управління ризиками в організації. Він дозволяє наочно визначити рівень загрози для кожного активу, спираючись на числові значення очікуваності та впливу. Завдяки цьому організація отримує чіткі орієнтири для пріоритетизації ризиків, а також можливість визначити, які заходи з мінімізації необхідно реалізувати першочергово. Цей розрахунок створює основу для подальшого вдосконалення системи інформаційної безпеки.

3.1.6 Планування заходів обробки ризиків

Після завершення заповнення першої частини реєстру ризиків – аналізу ризиків, приступаємо до другої частини – обробки ризиків. В цій частині реєстру

ризиків формується план обробки ризиків, який забезпечує впровадження ефективних заходів з мінімізації або усунення визначених ризиків. В реєстрі ризиків враховуються різноманітні параметри, що дозволяють забезпечити прозорість і контроль на кожному етапі реалізації заходів. Розглянемо основні поля реєстру ризиків, що використовуються для планування заходів з управління ризиками, а також їх практичне значення.

Asset Class	Asset Subclass	Risk Score	Risk Level	Risk Treatment Option	Risk Treatment Control	Risk Treatment Control Title	Risk Treatment Safeguard Description
Device	Computing and storage devices	12	Medium	Reduce	A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.
Documents	Policies, procedures, guidelines, checklists	5	Low	Accept	A.5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.
Documents	Policies, procedures, guidelines, checklists	5	Low	Accept	A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.
Software	On-premises applications	12	Medium	Reduce	A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.
Software	Cloud services	12	Medium	Reduce	A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.
Users	Specialists / professionals	5	Low	Accept	A.5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.
Users	Staff and managers	4	Low	Accept	A.5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.
Users	Specialists / professionals	5	Low	Accept	A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.
Users	Staff and managers	4	Low	Accept	A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.

Рисунок 3.12 – Фрагмент частини полів планування заходів таблиці-реєстру ризиків

На рисунку 3.12 можемо бачити таблицю, яка відображає частину процесу обробки ризиків інформаційної безпеки для різних класів активів. Вона включає

нові, раніше не відомі поля: варіант обробки ризику (Risk Treatment Option), контроль для обробки ризику (Risk Treatment Control), назва контрольного заходу (Risk Treatment Control Title), опис заходу безпеки (Risk Treatment Safeguard Description).

Варіант обробки ризику (Risk Treatment Option) вказує на обрану стратегію управління ризиком. Наприклад, "Reduce" означає зменшення ризику, а "Accept" - прийняття ризику.

Контроль для обробки ризику (Risk Treatment Control) - конкретний контрольний захід, що застосовується для управління ризиком. У таблиці це зазначено через посилання на стандарт ISO: A.5.2 або A.5.3.

Назва контрольного заходу (Risk Treatment Control Title) описує контрольний захід відповідно до стандарту ISO. Наприклад, розподіл обов'язків (Segregation of duties) або ролі та обов'язки з інформаційної безпеки (Information security roles and responsibilities).

Опис заходу безпеки (Risk Treatment Safeguard Description) - деталізує, як реалізується конкретний контрольний захід, наприклад ролі та обов’язки в сфері інформаційної безпеки повинні бути визначені та розподілені відповідно до потреб організації.

Заплановане впровадження (Our Planned Implementation) - короткий опис того, як захід буде впроваджено та використовуватиметься в організації.

Оцінка зрілості заходу безпеки (Risk Treatment Safeguard Maturity Score), очікувана оцінка заходу безпеки (Risk Treatment Safeguard Expectancy Score), вплив заходу на місію (Risk Treatment Safeguard Impact to Mission), вплив заходу на операційні цілі (Risk Treatment Safeguard Impact to Operational Objectives), вплив заходу на фінансові цілі (Risk Treatment Safeguard Impact to Financial Objectives), вплив заходу на зобов'язання (Risk Treatment Safeguard Impact to Obligations), оцінка ризику заходу безпеки (Risk Treatment Safeguard Risk Score) – всі ці поля обраховуються ідентично то тих, що визначались в першій частині реєстру ризиків – в аналізі ризиків, лиш зараз розраховується як плановані значення, після виконання запланованих впроваджень контролів.

Після обрахунку планованих значень оцінки ризику можна вирішувати чи є впровадження таких контролів прийнятне, якою буде вартість впровадження такого заходу безпеки та встановити терміни впровадження. Фрагмент таблиці в якому містяться фінальні розрахунки доцільності впровадження контролів для захисту активів знаходиться на рисунку 3.13.

Asset Class	Asset Subclass	Risk Treatment Control	Risk Treatment Control Title	Risk Treatment Safeguard Maturity Score	Risk Treatment Safeguard Expectancy Score	Risk Treatment Safeguard Impact to Mission	Risk Treatment Safeguard Impact to Operational Objectives	Risk Treatment Safeguard Impact to Financial Objectives	Risk Treatment Safeguard Impact to Obligations	Risk Treatment Safeguard Risk Score	Reasonable and Acceptable	Risk Treatment Safeguard Cost	Implementation Quarter	Implementation Year
Device	Computing and storage devices	A.5.3	Segregation of duties	4	4	2	1	2	1	8	YES	5 000 ₴	II	2025
Documents	Policies, procedures, guidelines, checklists	A.5.2	Information security roles and responsibilities	5	5	1	1	1	1	5	NO	-	-	-
Documents	Policies, procedures, guidelines, checklists	A.5.3	Segregation of duties	5	5	1	1	1	1	5	NO	-	-	-
Software	On-premises applications	A.5.3	Segregation of duties	4	4	1	1	2	1	8	YES	8 000 ₴	II	2025
Software	Cloud services	A.5.3	Segregation of duties	4	4	2	2	1	2	8	YES	6 000 ₴	I	2025
Users	Specialists / professionals	A.5.2	Information security roles and responsibilities	5	5	1	1	1	1	5	NO	-	-	-
Users	Staff and managers	A.5.2	Information security roles and responsibilities	4	4	1	1	1	1	4	NO	-	-	-
Users	Specialists / professionals	A.5.3	Segregation of duties	4	5	1	1	1	1	5	NO	-	-	-
Users	Staff and managers	A.5.3	Segregation of duties	4	2	1	2	1	1	4	NO	-	-	-

Рисунок 3.13 – Фрагмент обробки ризиків в реєстрі ризиків

Обґрунтованість та прийнятність (Reasonable and Acceptable) – поле для визначення того, чи є запланований захід безпеки обґрунтованим і прийнятним для реалізації в організації.

Вартість заходу безпеки (Risk Treatment Safeguard Cost) - оцінка вартості, яку передбачається витратити на впровадження запланованого заходу безпеки.

Квартал та рік впровадження (Implementation Quarter and Year) – квартал та рік, у якому планується завершити впровадження заходу безпеки.

Заповнення перечислених полів реєстру ризиків вимагає залучення спеціалістів різних напрямків. ІТ-відділ відповідає за технічну реалізацію, фінансовий відділ — за оцінку витрат і вигод, а керівництво — за стратегічне

ухвалення рішень. Такий підхід дозволяє врахувати всі аспекти ризиків і забезпечити ефективну реалізацію заходів.

3.2 Оцінка розробленої методології та перспективи вдосконалення

Розроблена методологія управління ризиками демонструє значний потенціал у забезпеченні прозорості, структурованості та адаптивності процесів оцінки та мінімізації ризиків. Вона забезпечує:

– Використання чітко визначених критеріїв та шкал для оцінки ризиків дозволяє уникнути суб’єктивності в аналізі та створює основу для уніфікованого підходу до управління ризиками. Це сприяє підвищенню довіри до результатів оцінки серед внутрішніх і зовнішніх зацікавлених сторін.

– Послідовність у процесі ідентифікації ризиків, оцінки їхнього впливу та очікуваності, а також вибору відповідних заходів для зменшення ризиків. Вона враховує всі ключові аспекти діяльності організації — від місії до фінансових цілей і зобов’язань.

– Гнучкість та легку адаптацію до потреб організації, враховуючи галузеві особливості, розмір компанії та регуляторні вимоги.

– Орієнтацію на проактивне управління замість фокусування на реагуванні на події, які вже сталися, а також дозволяє прогнозувати ризики, оцінювати їхній вплив і впроваджувати заходи для їхнього мінімізації ще до настання інцидентів.

– Підтримку прийняття обґрунтованих рішень завдяки чітким критеріям оцінки ризиків і матриці ризиків, що сприяє прийняттю стратегічно важливих рішень, спрямованих на зменшення ризиків до прийнятного рівня.

Попри значний потенціал, методологія має низку напрямів для подальшого вдосконалення, які можуть підвищити її ефективність і адаптивність:

– Використання сучасних програмних інструментів для автоматизації розрахунків і моніторингу ризиків. Це дозволить зменшити вплив людського фактора, підвищити точність оцінок і спростити обробку великих обсягів даних.

– Розширення критеріїв оцінки з можливістю додавання нових критеріїв, таких як вплив на репутацію чи вартість відновлення після інциденту. Це дозволить отримати більш повну картину ризиків і їхнього потенційного впливу.

– Регулярний перегляд і адаптація методології, щоб враховувати нові загрози, технології та регуляторні вимоги.

– Крос-функціональна інтеграція із залученням інших департаментів, таких як фінансовий, юридичний чи HR, до процесу управління ризиками для підвищення ефективності впроваджених заходів і оптимізації їхньої вартості.

Розроблена методологія є ефективним інструментом для системного управління ризиками в організації. Вона забезпечує як прозорість і стандартизацію процесів, так і можливість адаптації до змінюваних умов. Водночас її подальше вдосконалення дозволить зробити її ще більш ефективною та корисною для організацій різного масштабу і галузі.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

У процесі розробки методології для оцінки ризиків інформаційної безпеки аграрного підприємства значну увагу було приділено питанням охорони праці, дотримання техніки безпеки та протипожежної безпеки. Ці аспекти є невід'ємною частиною процесу розробки, оскільки забезпечують не лише фізичну безпеку працівників, а й їхнє здоров'я та комфорт під час використання методології в реальних умовах діяльності підприємства. Методологія оцінки ризиків є комплексним інструментом, що інтегрує вимоги охорони праці в усі етапи її реалізації, гарантуючи відповідність чинному законодавству та забезпечуючи безпечні умови праці на всіх рівнях взаємодії з інформаційними системами.

Ключовим законодавчим актом, який було враховано під час розробки методології, є Закон України "Про охорону праці" (№ 2694-XII від 14.10.1992 р.). Згідно з цим законом, роботодавець зобов'язаний створити безпечні умови праці, забезпечити належну організацію робочих місць та запровадити заходи, спрямовані на запобігання виробничим ризикам [20]. Методологія містить рекомендації щодо роботи з інформаційними системами, які відповідають стандартам ДСТУ CEN ISO/TR 9241-514:2023 "Ергономіка взаємодії людина-система". Ці стандарти включають положення про розташування обладнання, допустиме освітлення та організацію робочого простору, що зменшує ризики професійних захворювань.

Особливу увагу приділено виконанню вимог Закону України "Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин" (ДСанПіН 3.3.2.007-98). Цей документ регламентує норми тривалості роботи за комп'ютером, умови освітлення, а також ергономічні параметри робочого місця [21].

Окрім цього, дотримання належного мікроклімату в робочих приміщеннях передбачено стандартами ДБН В.2.5-67:2013 "Опалення, вентиляція та кондиціонування". Це дозволяє забезпечити комфортну температуру, адекватний рівень вологості та належний повітрообмін, що безпосередньо впливає на продуктивність працівників і їхнє загальне самопочуття. Наприклад, у приміщеннях з обладнанням, що генерує тепло (серверні кімнати), передбачено встановлення кондиціонерів з автоматичним регулюванням температури [22].

Не менш важливим аспектом є забезпечення електробезпеки. Працівники, які взаємодіють із технічними засобами, повинні дотримуватись ПТЕЕС (Правила технічної експлуатації електроустановок споживачів). Методологія передбачає рекомендації щодо регулярної перевірки справності електрообладнання та проведення інструктажів згідно з НПАОП 40.1-1.21-98 (Правила безпечної експлуатації електроустановок). Наприклад, співробітники, які мають доступ до серверного обладнання, повинні бути забезпечені діелектричними рукавичками та іншими засобами захисту [23].

Особлива увага приділяється приміщенням, де зосереджено критичне обладнання, таке як сервери, джерела безперебійного живлення та інші технічні засоби. Для забезпечення належного рівня безпеки рекомендовано встановлення сучасних систем автоматичного пожежогасіння відповідно до стандарту ДСТУ EN 54-4:2019 "Системи пожежної сигналізації". Крім того, методологія передбачає регулярне тестування та перевірку системи пожежної сигналізації, забезпечення приміщень вогнегасниками, а також проведення навчань і інструктажів для персоналу з питань дій у разі виникнення пожежі [24]. Це дозволяє мінімізувати ризики виникнення надзвичайних ситуацій та забезпечити оперативне реагування, що має вирішальне значення для захисту життя і здоров'я працівників.

Методологія також акцентує увагу на необхідності проведення навчальних інструктажів із питань охорони праці, що передбачено НПАОП 0.00-4.12-05 "Типове положення про навчання з питань охорони праці". Це дозволяє працівникам оволодіти необхідними знаннями та навичками для безпечного виконання своїх обов'язків [25]. Наприклад, нові співробітники повинні

проходити первинний інструктаж із подальшими періодичними перевірками знань.

Завдяки інтеграції сучасних стандартів кібербезпеки, таких як ISO/IEC 27001:2022, розроблена методологія не лише гарантує інформаційну безпеку, але й сприяє створенню безпечного робочого середовища для співробітників, які працюють із цією системою. Впровадження таких заходів, як автоматичні оновлення програмного забезпечення та постійний моніторинг безпеки, мінімізує ризики кіберзагроз, що можуть негативно вплинути на стабільність робочих процесів. Це забезпечує захист від потенційних кібератак, що в свою чергу сприяє безпечному виконанню трудових обов'язків, запобігаючи виникненню ситуацій, які можуть загрожувати здоров'ю та безпеці працівників.

Таким чином, розроблена методологія оцінки ризиків інформаційної безпеки для аграрного підприємства є інноваційним інструментом, який повністю відповідає сучасним вимогам охорони праці, техніки безпеки та протипожежної безпеки. Вона базується на дотриманні як національного законодавства України, так і міжнародних стандартів, що дозволяє гарантувати безпечне та комфортне середовище для працівників. Інтеграція цих аспектів у процес оцінки ризиків забезпечує не лише відповідність нормативним вимогам, а й сприяє підвищенню ефективності виконання поставлених завдань, захищаючи при цьому здоров’я та життя співробітників.

4.2 Безпека в надзвичайних ситуаціях

Державна система моніторингу довкілля (далі – система моніторингу) – це система спостережень, збирання, оброблення, передавання, збереження та аналізу інформації про стан довкілля, прогнозування його змін і розроблення науково-обгрунтованих рекомендацій для прийняття рішень про запобігання негативним змінам стану довкілля та дотримання вимог екологічної безпеки [26].

Система моніторингу є складовою частиною національної інформаційної інфраструктури, сумісної з аналогічними системами інших країн.

Система моніторингу – це відкрита інформаційна система, пріоритетами функціонування якої є захист життєво важливих екологічних інтересів людини і суспільства; збереження природних екосистем; відвернення кризових змін екологічного стану довкілля і запобігання надзвичайним екологічним ситуаціям.

Створення і функціонування системи моніторингу з метою інтеграції екологічних інформаційних систем, що охоплюють певні території, грунтується на принципах:

– узгодженості нормативно-правового та організаційно-методичного забезпечення, сумісності технічного, інформаційного і програмного забезпечення її складових частин;

– систематичності спостережень за станом довкілля та техногенними об'єктами, що впливають на нього;

– своєчасності отримання, комплексності оброблення та використання екологічної інформації, що надходить і зберігається в системі моніторингу;

– об'єктивності первинної, аналітичної і прогнозної екологічної інформації та оперативності її доведення до органів державної влади, органів місцевого самоврядування, громадських організацій, засобів масової інформації, населення України, заінтересованих міжнародних установ та світового співтовариства.

Моніторинг довкілля здійснюється Мінагрополітики, Мінприроди, ДАЗВ, Держгеонадрами, Мінрегіоном, ДКА (Державне космічне агентство), а також ДСНС (Державною службою України з надзвичайних ситуацій), Держсанепідслужбою, Держлісагентством, Держводагентством, Держземагентством та їх територіальними органами, підприємствами, установами та організаціями, що належать до сфери їх управління, обласними, міськими держадміністраціями, а також, до окупації, органом виконавчої влади Автономної Республіки Крим з питань охорони навколишнього природного середовища.

Наприклад, спостереження за станом атмосферного повітря здійснюються Державною службою України з надзвичайних ситуацій (на пунктах державної системи гідрометеорологічних спостережень), Міністерством охорони здоров’я

України (у місцях проживання і відпочинку населення), а Державною екологічною інспекцією України проводиться вибірковий відбір проб на джерелах викидів.

З метою забезпечення інформацією про стан навколишнього природного середовища, в областях функціонує регіональна система моніторингу довкілля. Так, спостереження за станом об'єктів довкілля проводяться суб'єктами регіональної системи моніторингу довкілля, а екологічне інформаційне забезпечення здійснюється органами державної влади.

Крім того, відповідно до ст. 22 Закону України „Про охорону навколишнього природного середовища‖ спостереження за станом навколишнього природного середовища, рівнем його забруднення здійснюється підприємствами, установами та організаціями, діяльність яких призводить або може призвести до погіршення стану навколишнього природного середовища.

Фінансування робіт із створення і функціонування системи моніторингу та її складових частин здійснюється відповідно до порядку фінансування природоохоронних заходів за рахунок коштів, передбачених у державному та місцевих бюджетах згідно із законодавством.

Покриття певної частини витрат на створення і функціонування складових частин і компонентів системи моніторингу може здійснюватися за рахунок інноваційних фондів у межах коштів, передбачених на природоохоронні заходи, міжнародних грантів та інших джерел фінансування.

Система моніторингу спрямована на:

– підвищення рівня вивчення і знань про екологічний стан довкілля;

– підвищення оперативності та якості інформаційного обслуговування користувачів на всіх рівнях;

– підвищення якості обгрунтування природоохоронних заходів та ефективності їх здійснення;

– сприяння розвитку міжнародного співробітництва у галузі охорони довкілля, раціонального використання природних ресурсів та екологічної безпеки.

Основними завданнями суб'єктів системи моніторингу є:

– довгострокові систематичні спостереження за станом довкілля;

– аналіз екологічного стану довкілля та прогнозування його змін;

– інформаційно-аналітична підтримка прийняття рішень у галузі охорони довкілля, раціонального використання природних ресурсів та екологічної безпеки;

– інформаційне обслуговування органів державної влади, органів місцевого самоврядування, а також забезпечення екологічною інформацією населення країни і міжнародних організацій.

Отже, система моніторингу довкілля є важливим інструментом для забезпечення екологічної безпеки та попередження надзвичайних ситуацій. Вона об’єднує зусилля різних установ і дозволяє оперативно реагувати на загрози, сприяючи захисту довкілля та здоров’я населення. Для її ефективності необхідні належне фінансування, технічна модернізація та використання сучасних технологій, що підвищать рівень екологічної безпеки.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було досягнуто поставлену мету — розроблено методологію оцінки ризиків інформаційної безпеки відповідно до вимог замовника. Методологія дозволяє оцінювати ризики з урахуванням їхнього впливу на місію, фінансові цілі, операційні процеси та зобов'язання організації. Результати дослідження підтвердили актуальність обраної теми та її практичну значущість, оскільки ефективне управління ризиками є основою забезпечення стійкості бізнесу та збереження його конкурентоспроможності.

Проведені дослідження дозволили зробити такі основні висновки:

– Аналіз сучасних методологій оцінки ризиків, таких як ISO/IEC 27005, FAIR, NIST SP 800-30 та DoCRA, показав, що вони забезпечують загальні принципи оцінки ризиків, проте потребують адаптації для практичного застосування в організаціях різних галузей, включаючи аграрний сектор.

– Розроблено критерії оцінки ризиків, які базуються на врахуванні очікуваності реалізації загроз та їхнього впливу окремо на ключові аспекти діяльності організації.

– Запропонована методологія оцінки ризиків вирізняється високою гнучкістю та адаптивністю. Вона передбачає оцінку ризиків для класів активів, таких як дані, обладнання, мережі чи документація. Водночас методологія дозволяє виділяти окремі критично важливі активи з відповідного класу для проведення більш детальної оцінки, що забезпечує підвищену точність у визначенні ризиків та пріоритезації заходів для їхньої обробки.

– Апробація розробленої методології на прикладі агрохолдингу підтвердила її ефективність у реальних умовах. Застосування методології забезпечило точне визначення ризиків, їхню пріоритезацію та розробку заходів для мінімізації впливу на бізнес-процеси. Це сприяло підвищенню загальної стійкості інформаційної системи підприємства.

– Практичне впровадження методології дозволяє забезпечити прозорість процесу управління ризиками, оптимізувати витрати на заходи з

кібербезпеки та підвищити рівень довіри з боку зацікавлених сторін. Крім того, регулярний моніторинг і повторна оцінка ризиків забезпечують актуальність і ефективність обраних підходів.

Результати роботи мають суттєве теоретичне та практичне значення. Запропонована методологія може застосовуватися для підвищення рівня кіберзахисту як в аграрному секторі, так і в інших галузях, завдяки її універсальності та здатності адаптуватися до різних бізнес-середовищ. Крім того, методологія може стати базою для подальших наукових досліджень, спрямованих на вдосконалення підходів до оцінки та управління ризиками інформаційної безпеки.

Напрями для подальшого дослідження:

– Інтеграція автоматизованих інструментів для підвищення точності та швидкості оцінки ризиків.

– Розробка механізмів фінансової оцінки витрат на впровадження заходів контролю.

– Врахування нових загроз, пов'язаних із розвитком сучасних технологій.

Отже, проведене дослідження підтвердило, що запропонована методологія є ефективним інструментом для системного управління ризиками інформаційної безпеки, сприяє забезпеченню стійкості бізнесу та відповідає викликам сучасних загроз у сфері кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гросул В. А., Усова М. О. Ризик: сутність, причини виникнення та основні види. Економічний простір № 176, 2021. С.58-64. DOI: https://doi.org/10.32782/2224-6282/176-9

2. Ілляшко К.В. Інформаційна безпека обліково-аналітичних процесів. URL: http://feb.tsatu.edu.ua/wp-content/uploads/2019/01/5-1-1.pdf

3. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства // Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. 2020. №5. Т. 31 (70). С. 69-74

4. Гончаров М.В. Дослідження поняття «інформаційна безпека» Серія ПРАВО. Науковий вісник Ужгородського Національного Університету, 2024. Випуск 82: частина 1. DOI: https://doi.org/10.24144/2307-3322.2024.82.1.4

5. Акімова Н. С., Кирильєва Л. О., Наумова Т. А. Інформаційна безпека підприємств торгівлі в умовах становлення глобального інформаційного суспільства. Підприємництво і торгівля : збірник наукових праць. № 35 (2023). DOI: https://doi.org/10.32782/2522-1256-2023-35-01

6. Що таке інформаційна безпека (InfoSec)? Сайт: URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec

7. Скіцько Олексій, Ширшов Роман. Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об’єктів критичної інфраструктури. International Science Journal of Engineering & Agriculture. Vol. 2, No. 6, 2023, pp. 12-22. doi: 10.46299/j.isjea.20230206.02

8. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

9. Яцків Н.Г., Вівчар Д.В. Аналіз підходів до оцінки ризиків. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ – 2022), Тернопіль, 2022. – С. 10-12.

10. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

11. Сидоренко В.; Положенцев А. Метод управління ІТ-загрозами на об'єктах критичної інформаційної інфраструктури. Наукоємні технології, 2024, 62.2: 143-153.

12. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.

13. Користін О. О. Щодо дослідження систем та методологій управління ризиками у сфері кібербезпеки. Напрям № 1 Воєнна наука. Національна безпека, 2024, 29. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/20834/1/zbirnyk_tez_22.05.2024.pdf#page=29

14. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

15. ISO 31000:2018. *ISO*. URL: https://www.iso.org/iso-31000-risk-management.html (дата звернення: 15.10.2024).

16. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

17. VERIS Community Database (VCDB). Інформаційна база даних для реєстрації подій та обміну інформацією про інциденти. URL: https://veriscommunity.net (дата звернення: 22.10.2024).

18. The VERIS Framework. *The VERIS Framework*. URL: https://verisframework.org (date of access: 22.10.2024).

19. Derkach, M., Skarga-Bandurova, I., Matiuk, D., & Zagorodna, N. (2022, December). Autonomous quadrotor flight stabilisation based on a complementary filter and a PID controller. In 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-7). IEEE.

20. Закон України “Про охорону праці” від 14.10.92 р. № 2694-XII. URL: https://zakon.rada.gov.ua/laws/show/2694-12#Text (дата звернення: 24.11.2024).

21. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. URL: https:// https://zakon.rada.gov.ua/rada/show/v0007282-98#Text (дата звернення: 24.11.2024).

22. Портал Єдиної державної електронної системи у сфері будівництва - ДБН В.2.5-67:2013 "Опалення, вентиляція та кондиціонування". URL: https://e-construction.gov.ua/laws_detail/3074971619479783152?doc_type=2 (дата звернення: 25.11.2024).

23. Про затвердження Правил безпечної експлуатації електроустановок споживачів (ДНАОП 0.00-1.21-98). URL: https://zakon.rada.gov.ua/laws/show/z0093-98#Text (дата звернення: 26.11.2024).

24. Про затвердження Правил улаштування та експлуатації систем оповіщення про пожежу та управління евакуацією людей в будинках та спорудах. URL:https://zakon.rada.gov.ua/laws/show/z0506-09#Text (дата звернення: 26.11.2024).

25. Про затвердження Типового положення про навчання з питань охорони праці. URL:https://zakon.rada.gov.ua/laws/show/z0506-09#Text (дата звернення: 27.11.2024).

26. Про затвердження Положення про державну систему моніторингу довкілля. URL: https://zakon.rada.gov.ua/laws/show/391-98-%D0%BF#Text (дата звернення: 28.11.2024).

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 004.77

Катерина Костюк, студентка гр.СБм-52
Тернопільський національний технічний університет імені Івана Пулюя

РОЗРОБКА МЕТОДОЛОГІЇ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕ АГРОХОЛДИНГУ

Kateryna Kostiuk, student of gr. СБм-52

DEVELOPMENT OF A METHODOLOGY FOR INFORMATION SECURITY RI ASSESSMENT FOR AN AGRICULTURAL HOLDING

Швидкий розвиток цифрових технологій в аграрному секторі відкриває нові мож але водночас збільшує вразливість до інформаційних загроз. Інциденти в інформаційній можуть мати серйозні наслідки для бізнесу: фінансові втрати, збої у виробничих пр погіршення репутації. У таких умовах постає необхідність розробки методології оцінки яка враховувала б специфіку агрохолдингів, зокрема їхню залежність від технологій, се операцій і широке використання автоматизованих систем.

Запропонована методологія побудована на основі аналізу сучасних підходів, ISO/IEC 27005 [1], NIST [2], DoCRA [3] і інших визнаних стандартів, адаптованих до аграрного бізнесу. Її мета — забезпечити системний підхід до управління ризикам дозволяє врахувати баланс між безпекою та ефективністю бізнес-процесів.

Особливістю методології є структурований підхід до ідентифікації активів, вразливостей, оцінки їхнього впливу та надання рекомендацій щодо пріоритетності управління ризиками. Вона базується на принципах, що узгоджуються з міжна стандартами безпеки, та орієнтована на відповідальне управління ризиками з урахуванням цілей організації [4].

Апробація методології на прикладі одного з провідних агрохолдингів України до провести комплексну оцінку ризиків інформаційної безпеки. У результаті було ідентифі ключові загрози, визначено їхній вплив на критичні активи та надано рекомендаці пріоритетів у подальшому управлінні ризиками [5].

Запропонована методологія демонструє високу ефективність у контексті ан бізнесу, забезпечуючи можливість комплексної оцінки ризиків, оптимального плануванн безпеки та підвищення стійкості інформаційних систем. Її впровадження сприяє мі ризиків і забезпечує стабільність бізнес-процесів в умовах сучасних небезпек.

Таким чином, запропонована методологія демонструє високу ефективність у к аграрного бізнесу, забезпечуючи комплексний підхід до управління ризиками інфор безпеки. Її впровадження сприятиме мінімізації втрат від кіберзагроз, забезпеченню стаб операційної діяльності та підвищенню конкурентоспроможності компанії.

Література:

1. ISO/IEC 27005:2018 Information Security Risk Management. URL: https://www.iso.org/standard/75281.html
2. NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. URL: https://csrc.nist.gov/pubs/sp/800/30/r1/final
3. The Duty of Care Risk Analysis Standard. URL: https://www.docra.org/
4. Critical Asset Identification. URL: https://www.emagined.com/blog/critical-asset-identification
5. CRR Implementation Guide Asset Management FINAL. URL: https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-AM

Додаток Б Перелік контролів ДСТУ ISO/IEC 27001:2023

Секція	Перелік контролів ДСТУ ISO/IEC 27001:2023	Перелік контролів ISO/IEC 27001:2023 (оригінал)
A5	**Організаційні контролі**	**Organizational controls**
A.5.1	Політика інформаційної безпеки	Policies for information security
A.5.2	Ролі та обов'язки в інформаційній безпеці	Information security roles and responsibilities
A.5.3	Розподіл обов'язків	Segregation of duties
A.5.4	Обов'язки керівництва	Management responsibilities
A.5.5	Контакт з органами влади	Contact with authorities
A.5.6	Контакт з групами спеціальних інтересів	Contact with special interest groups
A.5.7	Розвідка загроз	Threat intelligence
A.5.8	Інформаційна безпека в управлінні проектами	Information security in project management
A.5.9	Інвентаризація інформації та інших пов'язаних активів	Inventory of information and other associated assets
A.5.10	Прийнятне використання інформації та інших пов'язаних з нею активів	Acceptable use of information and other associated assets
A.5.11	Повернення активів	Return of assets
A.5.12	Класифікація інформації	Classification of information
A.5.13	Маркування інформації	Labelling of information
A.5.14	Передача інформації	Information transfer
A.5.15	Контроль доступу	Access control
A.5.16	Управління ідентифікацією	Identity management
A.5.17	Інформація про автентифікацію	Authentication information
A.5.18	Права доступу	Access rights
A.5.19	Інформаційна безпека у відносинах з постачальниками	Information security in supplier relationships
A.5.20	Вирішення питань інформаційної безпеки в угодах з постачальниками	Addressing information security within supplier agreements
A.5.21	Управління інформаційною безпекою в ланцюжку постачання інформаційно-комунікаційних технологій (ІКТ)	Managing information security in the information and communication technology (ICT) supply-chain

Секція	Перелік контролів ДСТУ ISO/IEC 27001:2023	Перелік контролів ISO/IEC 27001:2023 (оригінал)
A.5.22	Моніторинг, аналіз та управління змінами послуг постачальників	Monitoring, review and change management of supplier services
A.5.23	Інформаційна безпека при використанні хмарних сервісів	Information security for use of cloud services
A.5.24	Планування та підготовка до управління інцидентами інформаційної безпеки	Information security incident management planning and preparation
A.5.25	Оцінка та прийняття рішень щодо подій інформаційної безпеки	Assessment and decision on information security events
A.5.26	Реагування на інциденти інформаційної безпеки	Response to information security incidents
A.5.27	Навчання на основі інцидентів інформаційної безпеки	Learning from information security incidents
A.5.28	Збір доказів	Collection of evidence
A.5.29	Інформаційна безпека під час збоїв	Information security during disruption
A.5.30	Готовність ІКТ до безперервності бізнесу	ICT readiness for business continuity
A.5.31	Правові, законодавчі, регуляторні та договірні вимоги	Legal, statutory, regulatory and contractual requirements
A.5.32	Права інтелектуальної власності	Intellectual property rights
A.5.33	Захист записів	Protection of records
A.5.34	Конфіденційність та захист персональної інформації, що ідентифікує особу (PII)	Privacy and protection of personal identifiable information (PII)
A.5.35	Незалежна перевірка інформаційної безпеки	Independent review of information security
A.5.36	Дотримання політик, правил та стандартів інформаційної безпеки	Compliance with policies, rules and standards for information security
A.5.37	Задокументовані операційні процедури	Documented operating procedures
A6	**Контролі над людськими ресурсами**	**People controls**
A.6.1	Скринінг	Screening
A.6.2	Умови працевлаштування	Terms and conditions of employment
A.6.3	Поінформованість, освіта та навчання з питань інформаційної безпеки	Information security awareness, education and training

Секція	Перелік контролів ДСТУ ISO/IEC 27001:2023	Перелік контролів ISO/IEC 27001:2023 (оригінал)
A.6.4	Дисциплінарний процес	Disciplinary process
A.6.5	Обов'язки після звільнення або зміни місця роботи	Responsibilities after termination or change of employment
A.6.6	Угоди про конфіденційність або нерозголошення	Confidentiality or non-disclosure agreements
A.6.7	Дистанційна робота	Remote working
A.6.8	Звітування про події інформаційної безпеки	Information security event reporting
A7	**Фізичні контролі**	**Physical controls**
A.7.1	Фізичні периметри безпеки	Physical security perimeters
A.7.2	Фізичний вхід	Physical entry
A.7.3	Охорона офісів, приміщень та об'єктів	Securing offices, rooms and facilities
A.7.4	Моніторинг фізичної безпеки	Physical security monitoring
A.7.5	Захист від фізичних та екологічних загроз	Protecting against physical and environmental threats
A.7.6	Робота в безпечних зонах	Working in secure areas
A.7.7	Чистий стіл і чистий екран	Clear desk and clear screen
A.7.8	Розміщення та захист обладнання	Equipment siting and protection
A.7.9	Безпека активів за межами офісу	Security of assets off-premises
A.7.10	Носії інформації	Storage media
A.7.11	Підтримка інженерних мереж	Supporting utilities
A.7.12	Захист кабелів	Cabling security
A.7.13	Обслуговування обладнання	Equipment maintenance
A.7.14	Безпечна утилізація або повторне використання обладнання	Secure disposal or re-use of equipment
A8	**Технологічні контролі**	**Technological controls**
A.8.1	Кінцеві пристрої користувачів	User end point devices
A.8.2	Привілейовані права доступу	Privileged access rights
A.8.3	Обмеження доступу до інформації	Information access restriction
A.8.4	Доступ до вихідного коду	Access to source code
A.8.5	Безпечна аутентифікація	Secure authentication
A.8.6	Керування ресурсами	Capacity management
A.8.7	Захист від шкідливих програм	Protection against malware

Секція	Перелік контролів ДСТУ ISO/IEC 27001:2023	Перелік контролів ISO/IEC 27001:2023 (оригінал)
A.8.8	Управління технічними вразливостями	Management of technical vulnerabilities
A.8.9	Управління конфігурацією	Configuration management
A.8.10	Видалення інформації	Information deletion
A.8.11	Маскування даних	Data masking
A.8.12	Запобігання витоку даних	Data leakage prevention
A.8.13	Резервне копіювання інформації	Information backup
A.8.14	Резервування засобів обробки інформації	Redundancy of information processing facilities
A.8.15	Ведення журналів	Logging
A.8.16	Моніторинг діяльності	Monitoring activities
A.8.17	Синхронізація годинника	Clock synchronization
A.8.18	Використання привілейованих службових програм	Use of privileged utility programs
A.8.19	Встановлення програмного забезпечення на операційні системи	Installation of software on operational systems
A.8.20	Безпека мережі	Networks security
A.8.21	Безпека мережевих сервісів	Security of network services
A.8.22	Сегрегація мереж	Segregation of networks
A.8.23	Веб-фільтрація	Web filtering
A.8.24	Використання криптографії	Use of cryptography
A.8.25	Безпечний життєвий цикл розробки	Secure development life cycle
A.8.26	Вимоги до безпеки додатків	Application security requirements
A.8.27	Безпечна системна архітектура та інженерні принципи	Secure system architecture and engineering principles
A.8.28	Безпечне кодування	Secure coding
A.8.29	Тестування безпеки при розробці та прийнятті	Security testing in development and acceptance
A.8.30	Аутсорсинг розробка	Outsourced development
A.8.31	Розділення середовищ розробки, тестування та виробництва	Separation of development, test and production environments
A.8.32	Управління змінами	Change management
A.8.33	Тестова інформація	Test information

Додаток В Перелік визначених індексів VCDB в розрізі класів активів

Клас активів	**Підклас активів**	**Кількість інцидентів для класу**	**Відсоток**	**Індекс**
Підприємство	1.2.2 Договори та угоди 1.2.3 Політики, процедури, інструкції, чек-листи 1.3.1 Бренд 1.3.2 Знання, навички, здібності працівників 1.3.3 Комерційна таємниця 1.3.4 Інтелектуальна власність 3.1.2 Виконавчий менеджмент	4458	50%	3
Програмне забезпечення	1.4.1 Наземні застосунки 1.4.2 Хмарні сервіси 1.5.1 Операційні системи 1.5.2 BIOS, вбудоване програмне забезпечення	1253	14%	2
Дані та інформація	1.1.1 Дані журналів 1.1.2 Конфіденційні дані (персональні, фінансові, юридичні, комерційні тощо) 1.1.3 Бази даних 1.1.4 Резервні копії 1.2.1 Документи, що містять конфіденційну інформацію	4458	50%	3

Клас активів	Підклас активів	Кількість інцидентів для класу	Відсоток	Індекс
	1.2.3 Носії для зберігання інформації			
Пристрої	2.2.1 Обчислювальні пристрої 2.2.2 Мережеві та комунікаційні пристрої 2.1.4 Пристрої та токени для ідентифікації та автентифікації персоналу/контролю доступу	798	9%	1
Мережа	2.2.2 Мережеві та комунікаційні пристрої 2.1.1 Центри обробки даних, серверні приміщення	62	1%	1
Людські інформаційні активи	3.1.1 Персонал та менеджери 3.1.2 Виконавчий менеджмент 3.1.3 Фахівці/професіонали 3.2.1 Зовнішні консультанти та підрядники	4458	50%	3
Інші	n/a	863	10%	1

Додаток Г Співвідношення оцінки рівнів зрілості контролів до індексів VCDB для визначення очікуваності

Оцінка зрілості контролю	**Індекс VCDB**	**Очікуваність**
5	1	1
5	2	1
5	3	1
5	4	2
5	5	2
4	1	1
4	2	2
4	3	2
4	4	3
4	5	3
3	1	1
3	2	2
3	3	3
3	4	4
3	5	5
2	1	3
2	2	3
2	3	4
2	4	4
2	5	5
1	1	4
1	2	4
1	3	5
1	4	5
1	5	5