Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:
«Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства»
08-53.МКР.022.00.000 ПЗ

Виконав: студент 2 курсу групи 2БС-22м
спеціальності 125 Кібербезпека
_____Анастасія РАДЕЦЬКА

Керівник: к. т. н., доцент каф. ЗІ
_____Леонід КУПЕРШТЕЙН
«12» 12 2023 р.

Опонент: к. т. н. доцент каф. ПЗ
_____Олена КОВАЛЕНКО
«13» 12 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«14» 12 2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д. т. н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«19» 09 2023 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Радецькій Анастасії Олександрівні

1. Тема роботи: «Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства»
керівник роботи: Куперштейн Леонід Михайлович, к. т. н., доцент кафедри ЗІ, затверджені наказом ректора ВНТУ від 18 вересня 2023 року №247.
2. Строк подання студентом роботи 13 грудня 2023 р.
3. Вихідні дані до роботи:
   - розроблена методика повинна забезпечити ефективну імплементацію серії стандартів ISO 27000 у систему управління інформаційною безпекою підприємства;
   - методика повинна чітко визначати сферу застосування та межі процесу системи управління інформаційною безпекою
4. Зміст текстової частини: Вступ. 1. Аналіз предметної області. 2. Розробка методики. 3. Реалізація методики. 4. Економічна частина. Висновки. Перелік використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Архітектура методики (плакат, А4). Алгоритм визначення меж та цілей застосування СУІБ (плакат, А4). Алгоритм оцінки ризиків (плакат, А4). Цінність інформаційних активів фінансового відділу (плакат, А4). Порівняльна характеристика систем збирання та обробки логів (плакат, А4). Порівняльна характеристика шлюзів безпеки електронної пошти (плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Леонід КУПЕРШТЕЙН к.т.н., доц. каф.ЗІ	19.09	25.09
2	Леонід КУПЕРШТЕЙН к.т.н., доц. каф.ЗІ	19.09	10.10
3	Леонід КУПЕРШТЕЙН к.т.н., доц. каф.ЗІ	19.09	26.10
4	Ольга РАТУШНЯК к.т.н., доц. каф ЕВПМ	19.09	27.11

7. Дата видачі завдання 1 вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
3	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
4	Науково-технічне обгрунтування	16.09.2023 – 22.09.2023	
5	Розробка технічного завдання	23.09.2023 – 29.09.2023	
6	Розробка рішень	30.09.2023 – 12.10.2023	
7	Практична реалізація, моделювання, експериментування, результати	14.10.2023 – 10.11.2023	
8	Розробка розділу економічного обгрунтування доцільності розробки	11.11.23 – 17.11.2023	
9	Аналіз виконання ТЗ, висновки	18.11.2023 – 24.11.2023	
10	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
11	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
12	Перевірка магістерської роботи на наявність плагіату	02.12.2023 – 10.12.2023	
13	Представлення МКР до захисту	11.12.2023 – 14.12.2023	

Студент _____ Анастасія РАДЕЦЬКА

Керівник роботи _____ Леонід КУПЕРШТЕЙН

АНОТАЦІЯ

УДК 004.56

Радецька А. О. Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2023. 81 с.

Укр. мовою. Бібліогр.: 49 назв; рис.: 6; табл.: 20.

Магістерська кваліфікаційна робота присвячена розробці Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства. В рамках роботи проведено аналіз основних понять та видів інформаційної безпеки та існуючих стандартів. Було здійснено розробку та опис методики впровадження серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства. Реалізовано практичне впровадження методики на підприємстві торгівлі.

Ілюстративна частина складається з 7 плакатів з демонстрацією результатів моделювання і проведених досліджень.

В економічному розділі проведено оцінку витрати на розробку методики та визначено її економічну доцільність.

Ключові слова: інформаційна безпека, система управління інформаційною безпекою, серія стандартів ISO 27000, заходи управління безпекою.

ABSTRACT

Radetska A. Methodology for implementing a series of ISO 27000 standards to improve enterprise information security. Master's qualification work in specialty 125 – Cybersecurity, educational program – Security of information and communication systems. Vinnytsia: VNTU, 2023. 81 p.

In Ukrainian. Bibliography: 49 titles; fig.: 6; tab.: 20.

The master's thesis is devoted to the development of the Methodology for the implementation of the ISO 27000 series of standards to improve the information security of the enterprise. As part of the work, the basic concepts and types of information security and existing standards were analyzed. The article develops and describes the methodology for implementing a series of ISO 27000 standards to improve the information security of an enterprise. The practical implementation of the methodology at a trade enterprise is realized.

The graphic part consists of 7 posters demonstrating the results of modeling and research.

The economic section estimates the cost of developing the methodology and determines its economic feasibility.

Keywords: information security, information security management system, ISO 27000 series of standards, security management measures

ЗМІСТ

ВСТУП **3**
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ **5**
1.1 Аналіз основних понять та видів інформаційної безпеки 5
1.2 Аналіз стандартів інформаційної безпеки 10
1.3 Формалізація вимог та постановка задачі 22
2 РОЗРОБКА МЕТОДИКИ **26**
2.1 Опис методики 26
2.2 Реалізація етапів методики 29
2.3 Методика оцінка ризиків 40
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДИКИ **44**
3.1 Збір даних про підприємство та інвентаризація активів 44
3.2 Визначення загроз та оцінка ризиків для підприємства 48
3.3 Визначення заходів управління для мінімізації ризиків 54
4 ЕКОНОМІЧНА ЧАСТИНА **59**
4.1 Проведення технологічного аудиту науково-технічної розробки 59
4.2 Оцінювання рівня конкурентоспроможності розробки 62
4.3 Розрахунок витрат на здійснення науково-дослідної роботи 64
4.4 Розрахунок економічної ефективності науково-технічної розробки від її впровадження 70
ВИСНОВКИ **75**
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ **77**
ДОДАТКИ **81**
Додаток А. Результат впровадження методики на підприємстві 82
Додаток Б. Протокол перевірки магвстерської кваліфікаційної роботи на наявність текстових запозичень 90
Додаток В. Ілюстративна частина 91

ВСТУП

В епоху, позначену швидким розвитком технологій і зростаючою залежністю підприємств від цифрових систем і даних, захист інформації та забезпечення її цілісності, конфіденційності та доступності стали першочерговими завданнями для організацій усіх розмірів і сфер діяльності. Інформаційна безпека у сучасному світі є однією з ключових складових успішної діяльності підприємств у цифровій епохі. Постійна загроза кібератак, витоків конфіденційної інформації та непередбачуваність технологічних ризиків наголошують на необхідності вдосконалення та зміцнення систем управління інформаційною безпекою. Серія стандартів ISO 27000 є визнаним міжнародним керівним документом, який надає чіткі настанови щодо управління та забезпечення безпеки інформації.

Актуальність даної магістерської дипломної роботи визначається нагальністю проблеми забезпечення інформаційної безпеки в умовах сучасного цифрового світу. Відсутність належного контролю над захистом інформації може призвести до серйозних наслідків для підприємств усіх галузей та розмірів.

Сьогоднішній світ характеризується стрімким розвитком технологій, підвищеним обсягом цифрових даних та швидким впровадженням цифрових платформ. У зв'язку з цим зростає кількість кібератак, витоків конфіденційної інформації та інших загроз, що ставлять під загрозу інформаційну безпеку підприємств. Кіберзлочинці намагаються використовувати слабкі місця у системах безпеки для незаконного доступу до конфіденційної інформації, що може призвести до фінансових втрат, порушення репутації, а також втрати довіри клієнтів і партнерів.

Серія стандартів ISO 27000 є загально визнаною світовою спільнотою фахівців у галузі інформаційної безпеки та відображає найкращі практики у даній сфері. Вона надає структуровану систему вимог для управління ризиками та забезпечення інформаційної безпеки в організаціях. Але попри існування

стандартів, необхідно розробити конкретні методики їх імплементації, адаптовані до особливостей конкретного підприємства, для забезпечення оптимального захисту інформації та мінімізації ризиків.

Об’єктом дослідження даної роботи є процес оцінювання інформаційної безпеки підприємства.

Предметом дослідження виступають методи та засоби оцінювання інформаційної безпеки підприємства.

Метою даної дипломної роботи покращення інформаційної безпеки підприємства за рахунок імплементації серії стандартів ISO 27000.

Для досягнення мети необхідно виконати наступні завдання:

– дослідити поняття інформаційної безпеки підприємства;
– провести аналіз існуючих стандартів інформаційної безпеки;
– розробити методику оцінки ІБ інформаційної безпеки підприємства;
– розробити алгоритм дій для кожного із етапів методики;
– здійснити реалізацію розробленої методики на основі підприємства;
– навести рекомендації стосовно покращення стану інформаційної безпеки підприємства за результатами проведеної оцінки.

Наукова новизна. Запропоновано методику імплементації серії стандартів ISO 27000, яка адаптована до конкретних вимог та особливостей підприємства, що дозволяє підвищити захищеність підприємства за рахунок систематизації активів та оцінки ризиків безпеки.

Практична цінність полягає у тому, що розроблено рекомендацій для практичного впровадження стандартів ISO 27000 на підприємствах певного типу, що дозволяє підвищити рівень інформаційної безпеки.

Результати здійснених досліджень під час виконання магістерської кваліфікаційної роботи доповідались на Міжнародній науково-практична конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи (МН-2024)» [1].

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз основних понять та видів інформаційної безпеки

У сучасному світі в усіх аспектах життя та діяльності людини задіяні інформаційні технології. Для реалізації будь-якого виду діяльності та проведення різноманітних операцій використовуються певні види інформації, що несуть корисне навантаження для їх реалізації. Саме тому надзвичайно важливим є питання організації та управління захисту ресурсів та активів як і багатомільонних корпорацій та державних установ, так і особистих даних певної особи чи групи людей. Для вирішення даної проблеми було розроблено концепцію інформаційної безпеки.

За визначенням NIST (Національного інституту стандартизації та технологій), під поняттям інформаційна безпека розуміється захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності [2].

Відповідно до ISO (Міжнародна організація зі стандартизації), інформаційна безпека – це збереження конфіденційності, цілісності та доступності інформації шляхом застосування процесу управління ризиками та надання впевненості в тому, що інформація захищена від несанкціонованого доступу, розкриття, зміни, знищення та порушення цілісності [3].

Визначення поняття інформаційної безпеки від ISACA (Асоціація аудиту та контролю інформаційних систем) виглядає наступним чином: інформаційна безпека охоплює політики, процеси, практики та технології, що використовуються для захисту критично важливої інформації від несанкціонованого доступу, розкриття, зміни, знищення або порушення [4].

У сучасній нормативно-правовій базі України не існує загального та однозначного офіційного визначення поняття "інформаційна безпека" в законодавчих актах. Однак, існують певні нормативні документи та стратегії, які

вказують на важливість та обов'язки щодо забезпечення інформаційної безпеки.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": Цей закон визначає правові основи захисту інформації в інформаційно-телекомунікаційних системах, встановлює вимоги до захисту конфіденційності, цілісності та доступності інформації [5].

Закон України "Про основні засади забезпечення кібербезпеки України": Цей закон встановлює основні засади забезпечення кібербезпеки в Україні, а також визначає організаційні та правові аспекти забезпечення кібербезпеки країни [6].

Закон України "Про інформацію": Цей закон визначає загальні засади збору, обробки, зберігання, захисту та поширення інформації, включаючи питання, пов'язані з комерційною та державною таємницею [7].

Стратегія забезпечення кібербезпеки України: Ця стратегія визначає стратегічні пріоритети та завдання у сфері кібербезпеки для забезпечення національної безпеки України в цифрову епоху [8].

Концепція національної безпеки України: Концепція визначає загальні засади та пріоритети національної безпеки України, включаючи аспекти інформаційної безпеки [9].

Тріада CIA (Конфіденційність, Цілісність Доступність) – це загальновизнана модель, яка лежить в основі інформаційної безпеки. Вона базується на трьох принципах, що необхідні для забезпечення захисту конфіденційних даних та належного функціонування інформаційних систем [10].

Конфіденційність. Цей принцип спрямований на захист конфіденційної інформації від несанкціонованого доступу та розголошення. Конфіденційність гарантує, що тільки авторизовані користувачі можуть отримати доступ до інформації, тоді як інші користувачі мають обмежений доступ. Методи, що використовуються для збереження конфіденційності, включають шифрування, захист паролем, автентифікацію користувачів, контроль доступу та впровадження суворих політик конфіденційності.

*Цілісність***.** Принцип цілісності гарантує, що інформація залишається

точною, повною і несуперечливою протягом усього її життєвого циклу. Він не дозволяє неавторизованим користувачам змінювати, підробляти або видаляти дані. Цілісність також гарантує, що авторизовані користувачі можуть вносити зміни лише у затверджений спосіб. Заходи для підтримки цілісності даних включають контрольні суми, цифрові підписи, контроль версій і суворий контроль доступу.

Доступність. Цей принцип гарантує, що інформація та системи будуть доступні авторизованим користувачам у разі потреби. Доступність має вирішальне значення для підтримки функціональності інформаційних систем, мінімізації простоїв і забезпечення доступу авторизованих користувачів до необхідних їм даних. Стратегії забезпечення доступності включають резервування, системи резервного копіювання, планування аварійного відновлення, надійну інфраструктуру та балансування мережевого навантаження.

Разом тріада CIA формує всеосяжну структуру, яка допомагає організаціям розробити надійні політики та процедури інформаційної безпеки. Для коректного та стабільного функціонування є надзвичайно важливо реалізовувати впровадження заходів, що стосуються кожного аспекту тріади. Це дозволить захистити кретині дані та зберегти довіру зацікавлених сторін.

Відповідно до сфер діяльності та функціонування інформації у системі роботи та обробки даних організацій та установ виділяють наступні види інформаційної безпеки [11]:

1) безпека програм;
2) хмарна безпека;
3) безпека інфраструктури;
4) криптографія;
5) реагування на інциденти;
6) управління вразливістю.

*Безпека додатків***.** Це, як правило, заходи, що вживаються для захисту програмних додатків від загроз і вразливостей, які можуть поставити під загрозу

конфіденційність, цілісність або доступність даних і систем, в яких вони працюють. Вона включає в себе проектування, розробку, тестування і розгортання додатків з урахуванням безпеки, а також впровадження засобів контролю для виявлення і реагування на інциденти, пов'язані з безпекою.

Хмарна безпека. Це набір політик, технологій і засобів контролю, спрямованих на захист хмарних компонентів та інформації від різноманітних загроз безпеці. Вона забезпечує захист, подібний до захисту додатків та інфраструктури, але з додатковим акцентом на вразливості, які виникають через сервіси, що виходять в Інтернет, та спільні середовища, такі як публічні хмари. Хмарна безпека також передбачає централізацію управління безпекою та інструментарію для підтримки видимості інформації та інформаційних загроз на розподілених ресурсах.

Мета хмарної безпеки – захистити хмарні активи від загроз. Одне з головних занепокоєнь щодо інформаційної безпеки полягає в тому, чи може вона захистити хмарні ресурси, особливо тому, що хмара стає все більш важливим компонентом бізнес-операцій. Хмарна безпека особливо важлива, оскільки хмарні обчислювальні середовища доступні з будь-якого місця, що робить їх вразливими до атак з будь-якої точки світу. Крім того, хмарні провайдери часто керують базовою інфраструктурою, що створює нові ризики безпеки для організацій, які покладаються на хмарні сервіси.

Безпека інфраструктури. Захищає фізичні активи, які підтримують мережу, включаючи сервери, мобільні пристрої, клієнтські пристрої та центри обробки даних. Зі зростанням взаємозв'язку між цими компонентами важливо вжити належних заходів для запобігання ризикам інформаційної безпеки. Ризик виникає через можливість поширення вразливостей між взаємопов'язаними системами. Якщо один компонент інфраструктури вийде з ладу або буде скомпрометований, це може вплинути на всі залежні компоненти. Тому однією з головних цілей безпеки інфраструктури є ізоляція компонентів і мінімізація залежностей при збереженні взаємозв'язку. Це допомагає локалізувати інциденти безпеки та запобігти їхньому поширенню на інші частини

інфраструктури.

Криптографія. Шифрування даних під час передачі та даних у стані спокою допомагає забезпечити конфіденційність і цілісність даних. Цифрові підписи зазвичай використовуються в криптографії для перевірки автентичності даних. Криптографія та шифрування стають все більш важливими. Хорошим прикладом використання криптографії є Advanced Encryption Standard (AES). AES — це симетричний ключовий алгоритм, який використовується для захисту секретної державної інформації.

*Реагування на інциденти***.** Це набір процедур та інструментів, які використовуються для виявлення, розслідування та реагування на порушення безпеки або події, що завдають шкоди. Основна мета реагування на інциденти - зменшити вплив інцидентів безпеки та якомога швидше відновити нормальну роботу бізнесу. Реагування на інциденти може включати в себе широкий спектр заходів, в тому числі:

– Ідентифікація та класифікація інцидентів безпеки на основі їх серйозності та потенційного впливу на організацію.

– Ізоляція уражених систем та видалення будь-якого шкідливого коду або шкідливого програмного забезпечення для запобігання подальшої шкоди.

– Судове розслідування – аналіз і збір доказів для визначення першопричини інциденту та виявлення вразливостей, які могли бути використані.

– Відновлення пошкоджених систем і даних до стану до інциденту та забезпечення відновлення нормальної роботи бізнесу.

– Аналіз після інциденту – проведення аналізу процесу реагування на інцидент з метою виявлення областей для вдосконалення та впровадження змін для запобігання подібних інцидентів у майбутньому.

Управління вразливостями. Це безперервний і активний процес, спрямований на захист комп'ютерних систем, мереж і корпоративних додатків від кібератак і витоку даних. Це важливий елемент загальної програми безпеки, оскільки він допомагає виявити, оцінити та усунути потенційні слабкі місця в

системі безпеки, щоб запобігти атакам і мінімізувати збитки в разі порушення безпеки. Основна мета управління вразливостями – зменшити загальний ризик для організації шляхом усунення якомога більшої кількості вразливостей. Це може бути складним завданням, враховуючи велику кількість потенційних вразливостей та обмеженість ресурсів, доступних для їх усунення. Таким чином, управління вразливостями – це безперервний процес, який повинен йти в ногу з новими і новими загрозами та мінливим середовищем.

1.2 Аналіз стандартів інформаційної безпеки

1.2.1 Серія стандартів ISO/IEC 27000

ISO/IEC 27000 – це серія або сімейство стандартів, опублікованих Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) [12]. Також скорочено "ISO27k", вона об'єднує низку стандартів інформаційної безпеки, що формують всеосяжну структуру, яка допомагає організаціям зміцнити свої системи управління інформаційною безпекою (СУІБ).

Сімейство стандартів ISO 27000 можна умовно поділити на чотири категорії стандартів залежно від їхньої функції (табл. 1.1). Кожен з них має певну мету і може бути нормативним або інформативним.

Нормативні елементи використовуються для опису сфери застосування кожного стандарту та способів його дотримання. Ці елементи включають рекомендації, вимоги та можливості.

Інформативні елементи мають описовий характер і допомагають зрозуміти концепції. Вони надають контекст, передумови, додаткові рекомендації та зв'язок з іншими елементами. Лише нормативні стандарти можуть бути перевірені на відповідність.

Таблиця 1.1 – Класифікація стандартів серії ISO 27000

Категорія стандарту	Назва	Тип
Стандарти, що описують загальні принципи і термінологію	ISO 27000	Інформативні
Стандарти, що встановлюють вимоги	ISO 27001, ISO 27006, ISO 27009	Нормативні
Стандарти, що містять загальні рекомендації	ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27007, ISO 27013, ISO 27014, ISO 27021, TS 27008, TR 27016	Інформативні
Стандарти, що містять рекомендації для спеціальних областей	ISO 27010, ISO 27011, ISO 27017, ISO 27018, ISO 27019	Інформативні

Розглянемо детальніше кожен із стандартів.

ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary.

Цей стандарт містить загальні принципи, терміни та визначення, які використовуються у серії стандартів ISO/IEC 27000 для управління інформаційною безпекою [13].

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

Цей документ визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою в контексті організації. Цей документ також містить вимоги до оцінювання та управління ризиками інформаційної безпеки. Вимоги, викладені в цьому документі, є загальними і призначені для застосування до всіх організацій, незалежно від типу, розміру або характеру діяльності. Виключення будь-якої з

вимог, зазначених у пунктах 4-10, є неприйнятним, якщо організація претендує на відповідність цьому документу [14].

ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security manage.

Встановлює вимоги та надає настанови для органів, які проводять аудит та сертифікацію системи управління інформаційною безпекою, на додаток до вимог, що містяться в ISO/IEC 17021-1 та ISO/IEC 27001. Він призначений насамперед для підтримки акредитації органів з сертифікації, що надають послуги з сертифікації СУІБ [15].

ISO/IEC 27009:2020 Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 – Requirements

Описує вимоги до використання ISO 27001 в конкретному секторі. Він також визначає, як включати додаткові вимоги, уточнювати їх і додавати засоби контролю на додаток до тих, що зазначені в ISO 27001 [16].

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls

Посібник з вибору та впровадження загальних засобів контролю інформаційної безпеки для зміцнення системи управління інформаційною безпекою. Він містить найкращі практики та вказівки щодо використання цих засобів контролю [17].

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

Пояснює та вказує, як успішно впровадити СУІБ відповідно до ISO 27001 [18].

ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation

Спрямовує та допомагає організаціям оцінювати та вимірювати результативність СУІБ на відповідність вимогам ISO 27001:2022, 9.1 [19].

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection

– Guidance on managing information security risks

Надає організаціям рекомендації щодо впровадження управління ризиками відповідно до ISO 27001 [20].

ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing

Надає організаціям рекомендації щодо проведення аудитів СУІБ та компетентності аудиторів СУІБ відповідно до ISO 27001 [21].

ISO/IEC 27013:2021 Information security, cybersecurity and privacy protection Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Настанова для організацій, які мають намір

a) Впровадити ISO 27001, коли вже є ISO 20000-1 (стандарт на систему управління послугами), або впровадити останній (ISO 20000-1), коли є ISO 27001
b) Впровадити одночасно ISO/IEC 27001 та ISO/IEC 20000-1
c) інтегрувати свої системи менеджменту відповідно до ISO/IEC 27001 та ISO/IEC 20000-1.

Він також допомагає організаціям зрозуміти подібності та відмінності між цими двома стандартами [22].

ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection Governance of information security

Надає організаціям рекомендації щодо принципів і процесів моніторингу та управління інформаційною безпекою [23].

ISO/IEC 27021:2017 Information technology Security techniques Competence requirements for information security management systems professionals

Визначає вимоги до компетентності фахівців з СУІБ, які очолюють або беруть участь у створенні, впровадженні, підтримці та постійному вдосконаленні одного або декількох процесів системи управління інформаційною безпекою, що відповідає стандарту ISO/IEC 27001 [24].

ISO/IEC TS 27008:2019 Information technology Security techniques Guidelines for the assessment of information security controls

Містить настанови щодо перевірки та оцінювання впровадження та функціонування засобів контролю інформаційної безпеки, включаючи технічну оцінку засобів контролю інформаційних систем, відповідно до встановлених організацією вимог до інформаційної безпеки, включаючи технічну відповідність критеріям оцінювання, заснованим на вимогах до інформаційної безпеки, встановлених організацією [25].

ISO/IEC TR 27016:2014 Information technology Security techniques Information security management

Дозволяє організаціям оцінювати свої інформаційні активи, приймати обґрунтовані рішення щодо них у спосіб, який забезпечує економічну стійкість, а також отримувати уявлення про економічні наслідки своїх рішень [26].

ISO/IEC 27010:2015 Information technology Security techniques Information security management for inter-sector and inter-organizational communications

Надає вказівки та забезпечує контроль для ініціювання, впровадження, підтримки та покращення інформаційної безпеки з іншими організаціями та секторами [27].

ISO/IEC 27011:2016 Information technology Security techniques Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

Допомагає телекомунікаційним організаціям впроваджувати засоби контролю інформаційної безпеки. Це допомагає їм відповідати вимогам управління безпекою, таким як цілісність, конфіденційність та доступність [28].

ISO/IEC 27017:2015 Information technology Security techniques Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Допомагає постачальникам хмарних послуг впроваджувати засоби контролю безпеки відповідно до ISO 27002 [29].

ISO/IEC 27018:2019 Information technology Security techniques Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Встановлює цілі контролю, засоби контролю та настанови щодо захисту

персональних даних (PII) для хмарних обчислень відповідно до ISO 29100 [30].

ISO/IEC 27019:2017 Information technology Security techniques Information security controls for the energy utility industry

Застосовується до систем управління процесами, що використовуються в комунальному господарстві. Спрямовує їх на контроль і моніторинг виробництва, передачі, розподілу або генерації енергії [31].

1.2.2 COBIT

Control Objectives for Information and Related Technology (COBIT) – це структура, створена Асоціацією аудиту та контролю інформаційних систем (ISACA) як інструмент підтримки для менеджерів. Структура дозволяє подолати розрив між бізнес-ризиками, технічними проблемами та вимогами до контролю [32]. COBIT являє собою цілісну методологію, основним завданням якої є допомога у вирішенні завдань із керівництва та управління IT на підприємстві. COBIT надає можливість керувати і управляти IT в масштабах всього підприємства, як в областях функціональної відповідальності IT, так і бізнесу, а також дозволяє враховувати потреби в IT внутрішніх і зовнішніх зацікавлених сторін. Методологія COBIT універсальна і буде корисна підприємствам будь-якого масштабу і сфери діяльності: комерційним, громадським і державним.

Відповідно до опису, структура COBIT представляє 6 принципів для системи управління [33]:

1) Система управління необхідна для задоволення потреб зацікавлених сторін і створення цінності від використання I&T. Щоб створити вартість, підприємство має збалансувати вигоди, ризик і ресурси, а також розробити ефективну стратегію та систему управління.
2) Кілька компонентів будують систему управління. Вони можуть бути різних типів і повинні працювати разом цілісно.
3) Система управління має бути динамічною: якщо один або кілька факторів дизайну змінилися (наприклад, зміна стратегії чи технології), підприємство має розглянути, як це вплине на систему EGIT.
4) Діяльність і структури управління та управління відрізняються.

5) Для адаптації системи управління слід використовувати потреби підприємства. Для цього використовується набір факторів проектування для налаштування та пріоритезації компонентів системи управління.
6) Система управління включає всі функції підприємства, зосереджуючись на IT-функціях і всіх технологіях та інформації, які підприємство використовує для досягнення своїх цілей.

COBIT 2019 розглядається через призму 5 доменів, кожен з яких фокусується на різних аспектах управління IT в організаціях та складається із 40 високорівневих процесів [32].

Домен APO (Align, Plan, and Organize) зосереджений на тому, як організація має архітектурно планувати, організовувати та спрямовувати свою IT-інфраструктуру та процеси.

До нього входять наступні процеси:

– APO01 Управління підходом до управління IT
– APO02 Управління стратегією
– APO03 Управління архітектурою підприємства
– APO04 Управління інноваціями
– APO05 Управління портфелем інвестицій
– APO06 Управління бюджетом і витратами
– APO07 Управління персоналом
– APO08 Управління відносинами
– APO09 Управління угодами про послуги
– APO10 Управління підрядниками
– APO11 Управління якістю
– APO12 Управління ризиками
– APO13 Управління безпекою
– APO14 Управління даними

Домен BAI (Build, Acquire, and Implement) орієнтований на способи побудови, набуття та впровадження технологій для досягнення бізнес-цілей та

стратегій. Регламентовані процеси:

- BAI01 Управління програмами
- BAI02 Управління виявленням вимог
- BAI03 Управління вибором і впровадженням рішень
- BAI04 Управління доступністю і потужністю
- BAI05 Управління забезпеченням організаційних змін
- BAI06 Управління IT-змінами
- BAI07 Управління передачею і прийманням IT-змін
- BAI08 Управління знаннями
- BAI09 Управління активами
- BAI10 Управління конфігураціями
- BAI11 Управління проектами

Домен DSS (Deliver, Service, and Suppor) стосується управління постачанням та підтримкою IT-служб для задоволення бізнес-потреб та гарантування надійності.

- DSS01 Управління експлуатацією
- DSS02 Управління запитами на обслуговування і інцидентами
- DSS03 Управління проблемами
- DSS04 Управління безперервністю
- DSS05 Управління послугами безпеки
- DSS06 Управління контролями бізнес-процесів

Домен MEA (Monitor, Evaluate, and Assess) фокусується на процесах контролю, оцінки та оцінювання IT-забезпечення та його впливу на організацію.

- MEA01 Моніторинг, оцінка та аналіз продуктивності та відповідності
- MEA02 Моніторинг, оцінка та аналіз системи внутрішнього контролю
- MEA03 Моніторинг, оцінка та аналіз відповідності зовнішнім вимогам
- MEA04 Моніторинг, оцінка та аналіз страхування

Домен EDM (Evaluate, Direct, and Monitor) охоплює стратегічне управління ризиками, оцінювання загроз та визначення керівних принципів для їхнього управління.

– EDM01 Забезпечення створення та розвитку корпоративної системи
– управління IT
– EDM02 Забезпечення отримання вигоди
– EDM03 Забезпечення оптимізації ризиків
– EDM04 Забезпечення оптимізації ресурсів
– EDM05 Забезпечення прозорості для зацікавлених сторін

Ці домени надають організаціям універсальний фреймворк для управління IT, спрямований на забезпечення ефективності, ефективності та надійності в галузі інформаційних технологій.

1.2.3 NIST SP-800-53

NIST 800-53 – це стандарт відповідності вимогам безпеки, створений Міністерством торгівлі США та Національним інститутом стандартів у галузі технологій у відповідь на швидкий розвиток технологічних можливостей національних супротивників [34]. У ньому зібрані засоби контролю, рекомендовані Лабораторією інформаційних технологій (ITL) [35].

NIST 800-53 є обов'язковим для всіх федеральних інформаційних систем США, окрім тих, що стосуються національної безпеки, і є технологічно нейтральним. Однак його настанови можуть бути прийняті будь-якою організацією, що експлуатує інформаційну систему з чутливими або регульованими даними. Він надає перелік засобів контролю конфіденційності та безпеки для захисту від різноманітних загроз, стихійних лих та зловмисних атак. Організації та підприємства, які досягли відповідності NIST, можуть використовувати це як конкурентну перевагу під час маркетингу та переговорів про нові контракти. Відповідність демонструє, що організація має надійну систему безпеки та інвестує у створення та підтримку найкращих засобів контролю та процедур безпеки.

Метою стандарту є [36]:

– Забезпечити всеосяжний і гнучкий каталог засобів контролю для поточного і майбутнього захисту на основі мінливих технологій і загроз.

– Розробити основу для оцінки методів і процесів для визначення ефективності контролю.
– Покращити комунікацію між організаціями за допомогою спільного лексикону для обговорення концепцій управління ризиками.

Стандарт NIST 800-53 містить низку різних засобів контролю та рекомендацій для різних сімейств систем безпеки та контролю доступу, визначених відповідно до базового рівня впливу. Ці базові рівні розділені на [36]:

1) Низький - втрати матимуть обмежений негативний вплив.
2) Помірний - втрата матиме серйозний негативний вплив.
3) Високий - втрата матиме катастрофічні наслідки.

Елементи керування розподіляються на 20 родин безпеки та контролю [36]. Розглянемо кожен з них більш детально.

AC. Access control (Контроль доступу). Управління обліковими записами та моніторинг, дотримання принципу найменших привілеїв та розподіл обов'язків.

AT. Awareness and training. Забезпечення обізнаності та тренінгів з безпеки для працівників, а також підвищення технічної підготовки для більш привілейованих користувачів.

AU. Audit and accountability. Аудит записів і контенту, зберігання записів і надання відповідного аналізу та звітності.

CA. Assessment, authorization and monitoring. Тестування на проникнення та моніторинг підключень до публічних мереж і зовнішніх систем

CM. Configuration management. Впровадження контролю за змінами конфігурації та встановлення авторизованих програмних політик

CP. Contingency planning. Створення та тестування стратегій безперервності бізнесу, а також альтернативних сторін обробки та зберігання даних.

IA. Identification and authentication. Управління обліковими даними та налаштування політик і систем автентифікації для користувачів, пристроїв і сервісів.

IP. Individual participation. Отримання згоди та авторизація політик і практик конфіденційності.

IR. Incident response. Організація навчання з реагування на інциденти та налаштування відповідних систем моніторингу та звітності.

MA. Maintenance. Постійне обслуговування системи, персоналу та інструментів.

MP. Media protection. Забезпечення та захист доступу до медіа, їх використання, зберігання та транспортування.

PA. Privacy authorization. Встановлення політики щодо збору, використання та обміну інформацією, що дозволяє ідентифікувати особу (PII).

PE. Physical and environmental protection. Забезпечення доступу до аварійного живлення, забезпечення фізичного доступу та захист від фізичних ризиків і пошкоджень.

PM. Program management. Визначення стратегій управління ризиками, внутрішніми загрозами та архітектурою масштабування.

PL Planning. Наявність стратегій для комплексної архітектури безпеки (наприклад, глибинний захист і захист від сторонніх постачальників).

PS. Personnel security. Перевірка внутрішнього та зовнішнього персоналу, створення політик безпеки при звільненні та переведенні.

RA. Risk assessment. Сканування вразливостей, постійний вплив на конфіденційність та оцінка ризиків.

SA. System and services acquisition. Впровадження безпеки на всіх етапах життєвого циклу розробки системи, укладання контрактів з новими постачальниками.

SC. System and communications protection. Розподіл додатків, впровадження управління криптографічними ключами, захист паролів та інших конфіденційних даних.

SI. System and information integrit. Впровадження системного моніторингу, систем оповіщення та процесів усунення недоліків.

Проаналізувавши вище перераховані стандарти можна дійти висновку, що

ISO 27000, COBIT та NIST 800-53 – це стандарти, які відіграють важливу роль у сфері інформаційної безпеки та управління IT. Однак вони служать дещо різним цілям і мають відмінні характеристики.

Серія ISO 27000 зосереджена на системах управління інформаційною безпекою і є всесвітньо визнаним завдяки своєму широкому підходу до інформаційної безпеки. Вона забезпечує основу для створення, впровадження, підтримки та постійного вдосконалення СУІБ, а також орієнтована на процес і охоплює широкий спектр засобів контролю безпеки. Серія ISO 27000 може бути застосований до будь-якої організації, незалежно від її розміру або галузі, яка прагне створити та підтримувати СУІБ.

COBIT – це основа для управління та менеджменту IT. Хоча вона включає компоненти інформаційної безпеки, основна увага приділяється забезпеченню того, щоб IT підтримували бізнес-цілі організації. COBIT надає набір принципів і практик для управління та управління IT. Він включає домени, процеси та цілі контролю, які охоплюють широкий спектр діяльності. COBIT є цінним для організацій, які хочуть покращити загальне управління IT, управляти IT-ризиками та узгодити IT з бізнес-цілями. Це особливо корисно для великих підприємств зі складним IT-середовищем.

NIST SP 800-53 містить комплексний набір засобів контролю безпеки та керівних принципів, призначених в першу чергу для федеральних агентств США, але широко застосовується в різних секторах і може слугувати цінним довідником для впровадження контролю безпеки. Він зосереджується на засобах контролю безпеки та найкращих практиках для інформаційних систем та організацій, охоплюючи широкий спектр сфер безпеки.

Відповідно до даних про впровадження стандартів інформаційної безпеки на підприємствах серед країн Європи у 2022 році (рис. 1.1) найбільш поширеним є ISO 27000 [37].

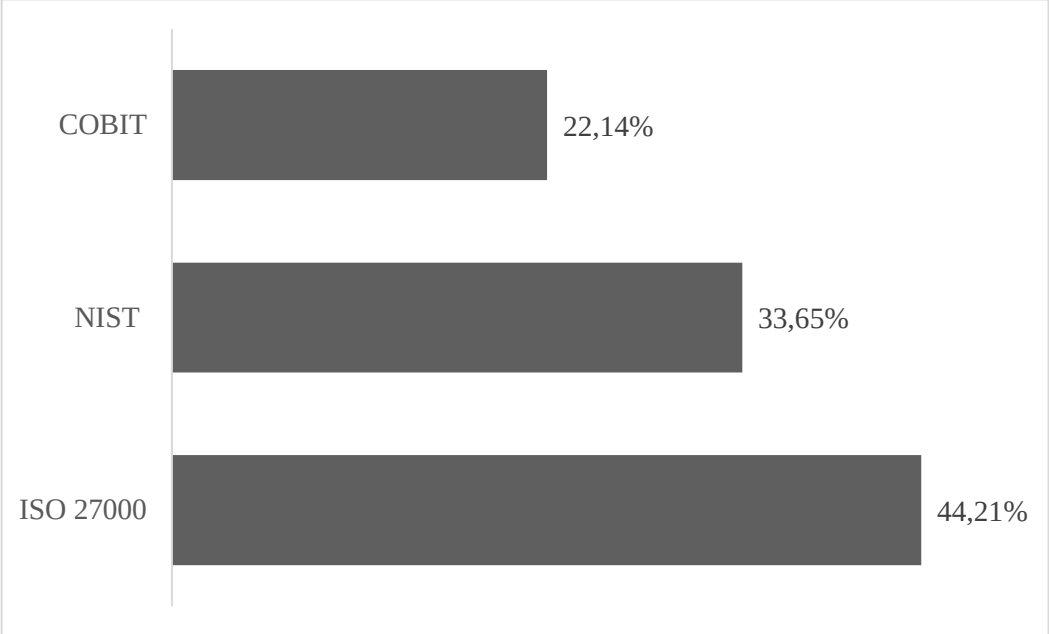


Рисунок 1.1 – Статистика використання стандартів інформаційної безпеки

Отже, базуючись на вище проведеному порівнянні стандартів інформаційної безпеки, можна зробити висновок, що для побудови та впровадження СУІБ на підприємстві найкращим стандартом є серія ISO/IEC 27000. Вона є найбільш популярною та загальноприйнятою для сертифікації у всьому світі та охоплює найбільше аспектів та питань з сфери інформаційної безпеки, ніж інші стандарти.

1.3 Формалізація вимог та постановка задачі

Питання порушення інформаційної безпеки викликає все більше занепокоєння. За останні роки спостерігається значне збільшення частоти випадків порушення інформаційної безпеки [38]. Відповідно до даних, що були зібрані та оприлюднені компанією Statista, у Європі протягом 2022 році 16312 підприємств та компаній зазнали порушень інформаційної безпеки [39]. Інформація про галузі що зазнали найбільше інцидентів представлена на рис.1.2.

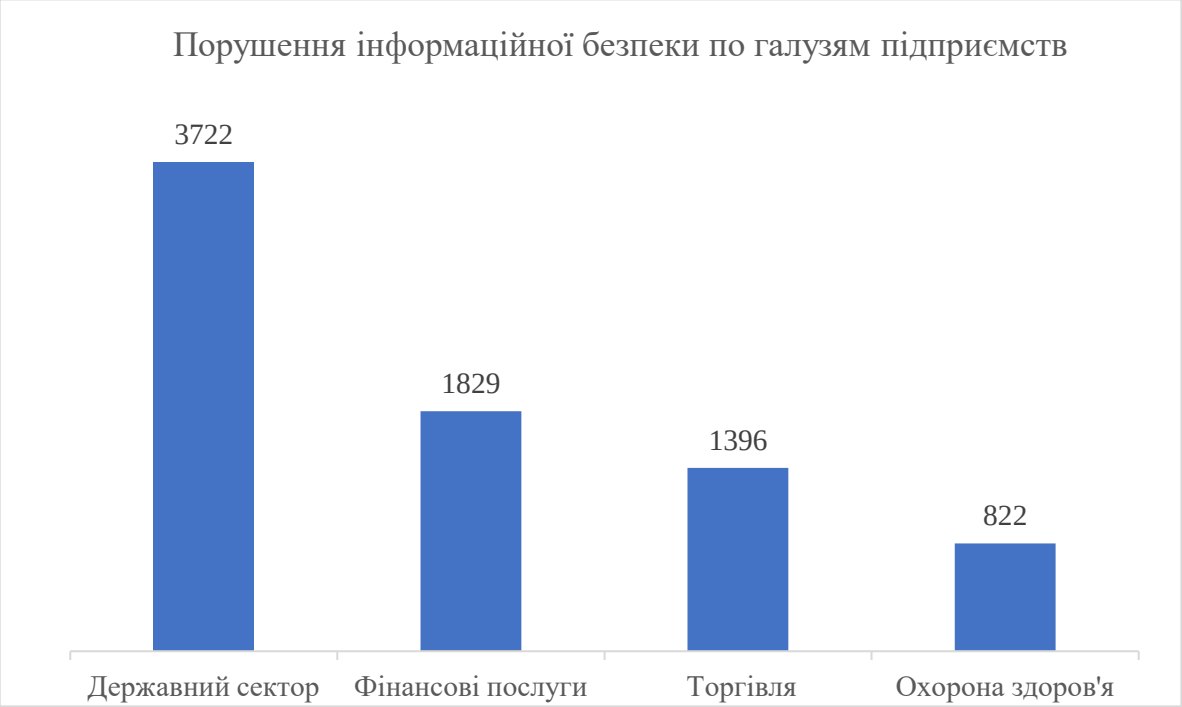


Рисунок 1.2 – Статистика порушень інформаційної безпеки

При чому у більшості із підприємств, що стали жертвами порушення безпеки було зафіксовано повну або часткову відсутність відповідності вимогам стандартів інформаційної безпеки [38].

Саме тому надзвичайно важливим для будь-якого підприємства є забезпечення побудови системи управління інформаційною безпекою на основі серії стандартів ISO/IEC 27000. Адже як видно із попереднього розділу саме дана серія стандартів є найбільш часто використовуваною та здатна забезпечити у ефективне управління інформаційною безпекою, охопивши всі важливі аспекти діяльності та бізнес-процесів організації.

Впровадження серії стандартів ISO/IEC 27000 у роботу підприємства має численні переваги, пов'язані з управлінням інформаційною безпекою і підвищенням ефективності бізнес-процесів. Ось деякі з найважливіших переваг.

Забезпечення інформаційної безпеки. Впровадження стандарту ISO 27000 допомагає організаціям захищати конфіденційність, цілісність та доступність інформації. Це допомагає уникнути витоків даних, несанкціонованого доступу та інших загроз інформаційній безпеці.

Управління ризиками. ISO 27000 надає методику для ідентифікації, оцінки та керування ризиками, пов'язаними з інформацією та інформаційною системою. Це допомагає зменшити вплив загроз та мінімізувати потенційні втрати.

Покращення процесів. Впровадження стандарту ISO 27000 сприяє покращенню управління інформаційною безпекою та інформаційною системою. Це включає в себе удосконалення процесів управління інцидентами, аудиту та відновлення після інцидентів.

Довіра споживачів і стейкхолдерів. Клієнти, партнери та стейкхолдери мають більше довіри до організацій, які впроваджують стандарти інформаційної безпеки. Це може покращити стосунки зі споживачами та сприяти розвитку бізнесу.

Виконання законодавства. В деяких країнах і галузях існують законодавчі вимоги щодо захисту інформації. ISO 27000 допомагає організаціям відповідати цим вимогам і уникати штрафів та інших юридичних наслідків.

Збільшення конкурентоспроможності. Запровадження стандартів інформаційної безпеки може відокремити підприємство від конкурентів та дозволити здобути перевагу на ринку.

Ефективність та продуктивність. ISO 27000 сприяє ефективнішому управлінню інформаційною безпекою та процесами в організації, що може призвести до покращення продуктивності та оптимізації витрат.

Міжнародне визнання. ISO 27000 є міжнародно визнаними стандартами, що дозволяє організаціям працювати в глобальному середовищі та дотримуватися міжнародних норм та вимог.

Саме тому метою даної роботи є покращення рівня інформаційної безпеки підприємства за рахунок впровадження серії стандартів ISO 27000 у систему управління інформаційною безпекою підприємства.

У якості досліджуваного підприємства було обрано підприємство, що працює у сфері роздрібної торгівлі та займається реалізацією продуктів широкого спектру, який включає продукти та товари для побуту. Для забезпечення конфіденційності критично важливих даних для функціонування

підприємства, уся інформація, яка використана під час виконання роботи, буде анонімізованою.

Для досягнення поставленої мети необхідно:

- проаналізувати вимоги стандартів серії ISO 27000;
- розробити методику імплементації даних стандартів;
- розробити алгоритми функціонування етапів методики;
- здійснити практичну реалізацію етапів методики на інформаційну систему підприємства;
- зробити висновки про виконану роботу.

Після здійснення аналізу предметної області та постановки задачі необхідно перейти до процесу розроблення методики.

2 РОЗРОБКА МЕТОДИКИ

2.1 Опис методики

Імплементація серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства – це серйозний і складний процес, який передбачає впровадження низки положень та заходів для захисту інформації в організації, а також дозволяє створити або покращити систему управління інформаційною безпекою (СУІБ)

Методика впровадження серії стандартів складається з 6 етапів, що дозволяють повною мірою покрити усі аспекти, пов’язані із специфікою бізнес-процесів підприємства (рис. 2.1):

- визначення меж та цілей застосування СУІБ;
- оцінка ризиків;
- визначення заходів управління;
- розробка політики безпеки;
- впровадження заходів;
- моніторинг та покращення.

Розглянемо детальніше кожен із даних етапів.

Етап 1. Визначення меж та цілей застосування СУІБ

Визначення меж та цілей застосування системи управління інформаційною безпекою (СУІБ) є важливим кроком у процесі розробки та впровадження системи, яка забезпечує безпеку інформації в організації. Цей крок допомагає чітко визначити обсяг та область застосування СУІБ та визначити основні цілі і завдання, які потрібно досягти.

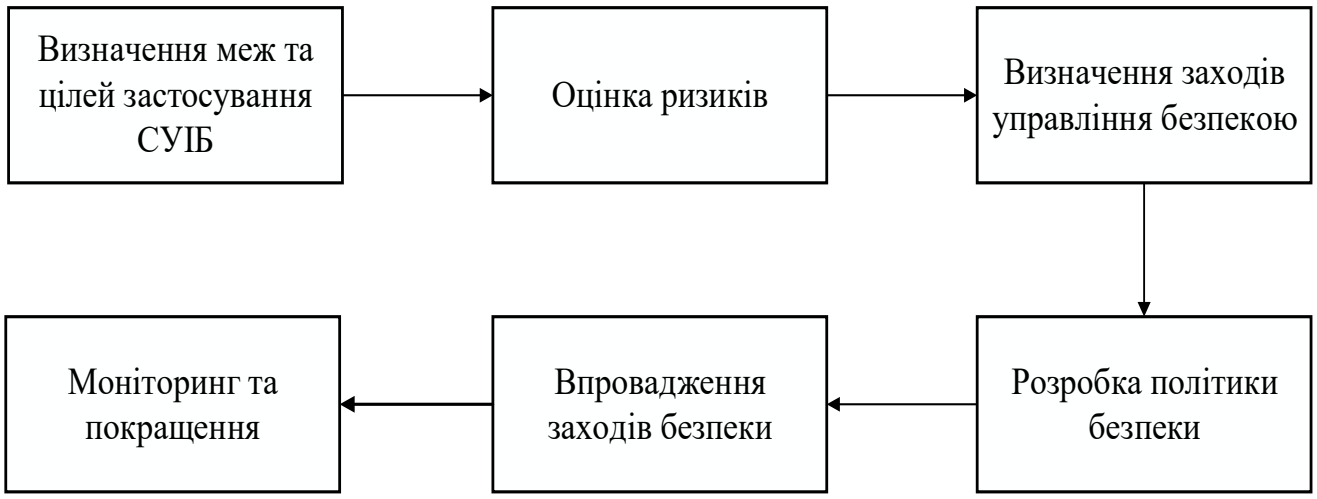


Рисунок 2.1 – Методика імплементація серії стандартів ISO 27000

Етап 2. Оцінка ризиків

Оцінка ризиків – це процес ідентифікації, аналізу та оцінки потенційних загроз і ризиків для інформаційної безпеки організації. Цей процес допомагає визначити, які ризики і загрози існують та які активи можуть бути вразливими.

Етап 3. Визначення заходів управління безпекою

Визначення заходів управління – це процес визначення конкретних дій та стратегій, які приймаються для зменшення або управління ризиками, ідентифікованими під час оцінки ризиків, а також для покращення бізнес-процесів. Ці заходи спрямовані на запобігання можливим інцидентам, забезпечення відповідності політиці інформаційної безпеки та модернізації етапів функціонування підприємства.

Етап 4. Розробка політики безпеки

На даному етапі здійснюється детальний опис дій, стратегій, процедур та правил, що необхідно реалізувати у межах системи управління інформаційною безпекою.

Етап 5. Впровадження заходів управління безпекою

Впровадження заходів – це процес втілення конкретних дій, стратегій і політик, спрямованих на забезпечення безпеки інформації в організації, що були визначені на попередньому кроці. Цей процес включає в себе всі кроки від розробки планів дій та аж до їх повного виконання.

Етап 6. Моніторинг та покращення

Моніторинг та аудит є важливою частиною системи управління інформаційною безпекою. На даному етапі реалізовано процеси, які дозволяють організації відстежувати та оцінювати ефективність її заходів управління безпекою, виявляти можливі відхилення, ідентифікувати слабкі місця. На основі отриманих даних здійснюється процес перегляду та модернізації усіх заходів реалізації СУІБ.

Важливо пам'ятати, що імплементація методики – це постійний процес, який вимагає постійного удосконалення та адаптації до змін у загрозах та технологіях. Саме тому для організації життєвого циклу розробленої методики СУІБ необхідно керуватися циклом PDCA (Plan-Do-Check-Act): планування, виконання, перевірка, вплив (управління, коригування) (рис. 2.2).

PDCA, також відомий як цикл Демінга – це ітеративний чотириетапний метод управління, який використовується в бізнесі для контролю та постійного вдосконалення процесів і продуктів [40].

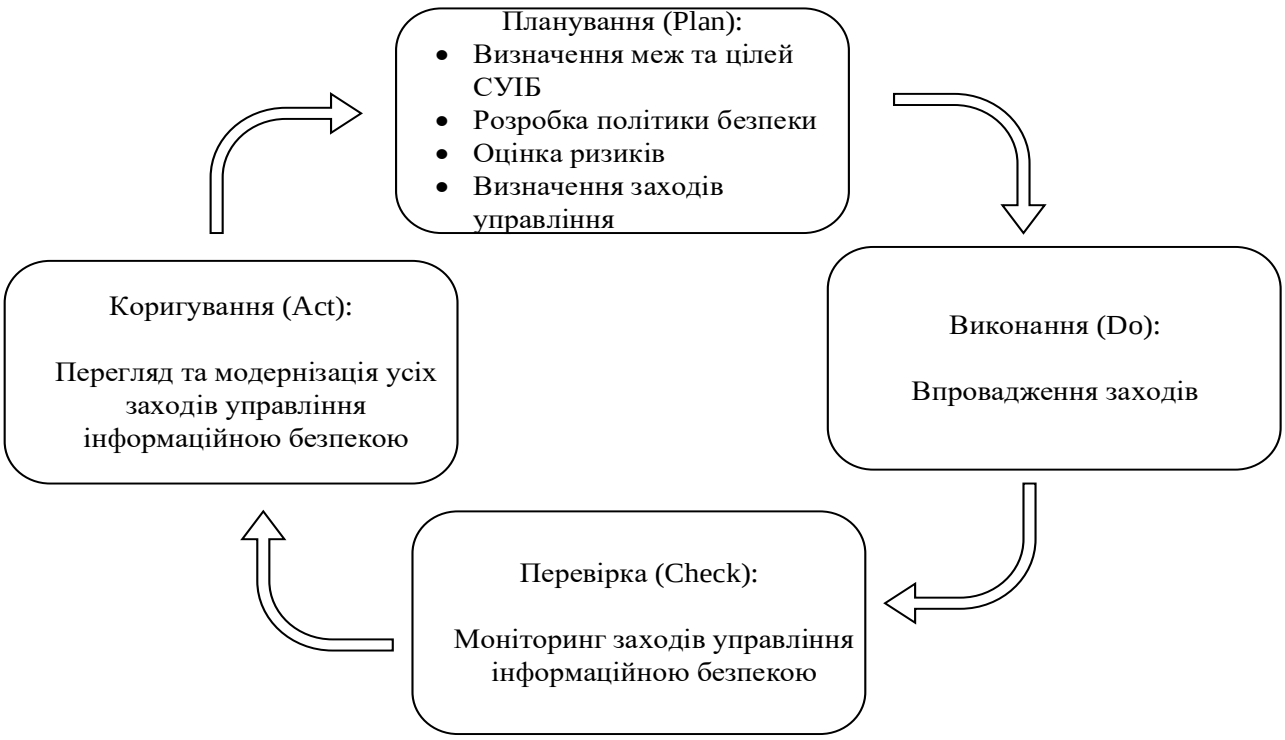


Рисунок 2.2 – Зв’язок етапів методики із циклом PDCA

Мепінг етапів методики імплементація серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства на цикл PDCA :

1) Планування – визначення меж та цілей застосування СУІБ; розробка політики безпеки; оцінка ризиків; визначення заходів управління.
2) Виконання – впровадження заходів.
3) Перевірка – моніторинг та покращення (на даному кроці циклу виконується лише частина цього етапу, що охоплює процеси моніторингу заходів управління інформаційною безпекою)
4) Коригування – моніторинг та покращення (на даному кроці циклу виконується частина цього етапу, що охоплює процеси перегляду та модернізації усіх заходів управління інформаційною безпекою)

Незважаючи на те, що процес створення системи управління інформаційною безпекою є циклічним, для більшості підприємств та компаній етапи визначення меж та цілей застосування СУІБ та розробка політики безпеки будуть проводитися із більшим періодом повторюваності, ніж інші етапи. Це пояснюється тим, що визначення меж та цілей застосування СУІБ та розробка політики безпеки стосуються більше стратегічних аспектів організації процесу роботи компанії або підприємства. Вони не потребують частого перегляду та змін, адже стратегії підприємства зазвичай не змінюються часто. У той же час інші етапи стосуються процесу управління ризиками, який потрібно регулярно переглядати та змінювати у відповідності до появи нових загроз системі.

2.2 Реалізація етапів методики

2.2.1 Визначення меж та цілей застосування СУІБ

Серія стандартів ISO 27000 визначає загальні принципи і вимоги для управління інформаційною безпекою в організаціях. Для визначення меж і цілей застосування системи управління інформаційною безпекою (СУІБ) в рамках цієї серії стандартів можна використовувати стандарт ISO/IEC 27001, який містить відповідні вимоги та вказівки.

На основі даного стандарту було здійснено розробку алгоритму, який описує послідовність дій для визначення меж та цілей застосування СУІБ (рис. 2.3)

Рисунок. 2.3 – Алгоритм визначення меж та цілей застосування СУІБ

Розглянемо детальніше кожен із кроків алгоритму.

Збір інформації. На даному кроці здійснюється збір всієї необхідної інформації про структуру та організацію бізнес-процесів підприємства. Визначаються активи (інформація, системи, обладнання, програмне забезпечення, люди), якими володіє організація, та здійснюється опис усіх інформаційних потоків, які впливають на інформаційну безпеку.

Визначення меж застосування. Здійснюється формування меж

застосування СУІБ, у яких чітко окреслюється як буде поширюватися система управління інформаційною безпекою: на усе підприємство або ж лише на окремі його підрозділи. Визначаються які активи, проєкти, процеси, або інформаційні потоки включаються і виключаються із зони поширення СУІБ.

Визначення цілей застосування. На даному кроці здійснюється формулювання цілей та завдання СУІБ. У якості цілей ставиться забезпечення конфіденційності, цілісності та доступності інформації, зменшення ризиків, забезпечення відповідності нормативним вимогам, забезпечення безперервності бізнесу та покращення обізнаності персоналу у сфері інформаційної безпеки. При формуванні цілей необхідно використовувати метод SMART [41]. Цілі повинні бути конкретними, вимірюваними, досяжними, реалістичними та часово визначеними.

Визначення відповідальних осіб. На даному етапі здійснюється визначення осіб, які будуть відповідати за реалізацію та управління СУІБ. Формується перелік членів команди, керівництва та інших учасників, що відповідальна за інформаційну безпеку. Здійснюється розподіл обов'язків та повноважень між усіма працівниками.

Розробка документації. Здійснюється фіксація визначених межі та цілей в документах. Уся документація обов’язково затверджується керівництвом організації. Вміст документів доноситься до усіх працівників та є загальнодоступним у будь-який час.

2.2.2 Оцінка ризиків

При розробці алгоритму оцінки ризиків опорним нормативним документом був стандарт ISO 27005.

ISO 27005 – це загальновизнаний стандарт управління ризиками інформаційної безпеки. Він забезпечує структуровану основу для оцінки та управління ризиками інформаційної безпеки в організації. ISO 27005 не встановлює конкретного математичного алгоритму для розрахунку ризику. Замість цього він заохочує організації адаптувати свої методи оцінки ризиків до конкретних потреб і можливостей. Саме тому у розділі 2.3 наведено опис

математичного алгоритму розрахунку ризику.

Розроблений алгоритм оцінки ризиків представлено на рис. 2.4.

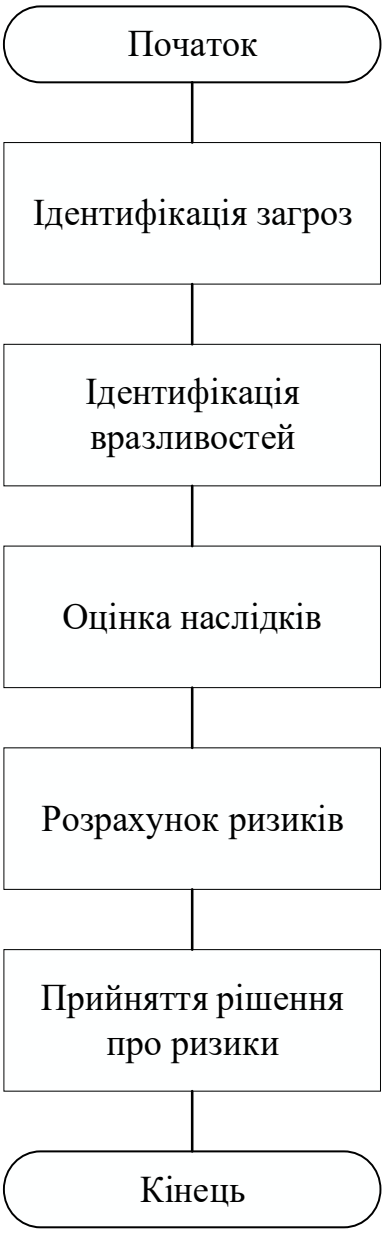


Рисунок 2.4 – Алгоритм оцінки ризиків

Розглянемо детально кожен із кроків алгоритму

Ідентифікація загроз. Визначення усіх можливих загрози, які можуть вплинути на інформаційні активи. Загрози можуть бути технічними, природними, людськими тощо.

Ідентифікація вразливостей. Визначення вразливостей, які існують в системах, процесах та обладнанні, і які можуть бути використані загрозами для

здійснення атак.

Оцінка наслідків. Визначення можливих наслідків, які можуть виникнути в результаті реалізації загроз на інформаційні активи.

Оцінка ризиків. Оцінювання ризиків, використовуючи визначені раніше активи, загрози, вразливості, наслідки і ймовірність.

Прийняття рішення про ризики. Визначення того, які ризики є прийнятними для підприємства, а які потребують подальшого управління. Усі результати прийнятих рішень представляються на розгляд керівництву компанії та обов'язково мають бути ним затверджені.

2.2.3 Визначення заходів управління

На основі проведеної оцінки ризиків та потреб підприємства здійснюється процес визначення заходів управління інформаційною безпекою. У рамках серії стандартів ISO 27000 для реалізації даного етапу методики необхідно використовувати стандарт ISO 27002.

Відповідно до ISO 27002 усі заходи правління інформаційною безпекою поділяються на 4 групи:

- організаційні заходи захисту;
- заходи захисту персоналу;
- фізичні заходи захисту;
- технологічні заходи захисту.

Кожна із категорій охоплює певну частину системи управління інформаційною безпекою та допомагає підприємству організувати максимально можливий рівень захисту.

Організаційні заходи

Організаційні заходи захисту включають в себе різні стратегії, процедури та практики, які допомагають забезпечити безпеку і конфіденційність інформації в організації. До них можна віднести:

Контроль доступу – це процес управління і регулювання доступу користувачів, пристроїв і систем до інформації та ресурсів в організації. Для

його реалізації необхідно запровадити процедури ідентифікації та аутентифікації усіх користувачів систем. Також потрібно реалізувати процедуру управління правами доступу, що включає в себе встановлення ролей та груп доступу для усіх працівників компанії за принципом найменших привілеїв, та їх регулярний перегляд. Необхідно здійснювати моніторинг і аудиту активності користувачів у системах підприємства та фіксувати усі їх дії

Управління інцидентами інформаційної безпеки дозволить організації швидко та своєчасно виявляти та реагувати на виникнення подій, що порушують цілісність, конфіденційність та доступність будь-якої інформації чи системи. Для виявлення інцидентів порушення інформаційної безпеки необхідно використовувати SIEM та IDS/IPS системи. SIEM – це комплексна технологія та підхід до кібербезпеки, що надає організаціям централізовану систему моніторингу, управління та аналізу подій та інформації про безпеку в їхній IT-інфраструктурі [42]. Системи IDS та IPS призначені для виявлення та реагування на інциденти та загрози безпеці в режимі реального часу [43]. Системи IDS генерують сповіщення при виявленні підозрілих дій. Адміністратори безпеки переглядають ці сповіщення, щоб дослідити потенційні загрози. Системи IPS вживають заходів після виявлення загроз.

Окрім систем моніторингу інцидентів необхідно визначити групу осіб, яка б реагувала на них та здійснювала їх ліквідацію. Потрібно встановити швидку та ефективну комунікацію між групою реагування та рештою співробітників. Також необхідно запровадити процедуру детального документування усіх інцидентів та порядку реагування на них. Визначити перелік дій для відновлення нормальної роботи після інцидентів, а також запровадити регулярне навчання персоналу щодо виявлення інцидентів та його дій у випадку інцидентів.

Заходи захисту персоналу

Заходи захисту персоналу є надзвичайно важливими для організації надійної системи управління інформаційною безпекою. Адже левова частка успішності реалізації СУІБ залежить від того, наскільки працівники компанії обізнані у правилах інформаційної безпеки та дотримуються їх.

Під час проведення процесу найму співробітників необхідно запровадити перевірку на достовірність наданої потенційним кандидатом інформації. Це дозволить уникнути ряду проблем пов'язаних із репутаційними та ресурсними витратами. Перевірка допомагає переконатися, що правильних людей, із належною компетенцією наймають на відповідну роботу.

Усі працівники компанії мають бути ознайомлені із процедурами та правилами політики безпеки. Необхідно запровадити процедуру підписання договорів, у яких чітко буде прописано усі посадові обов'язки працівників, їх рівні доступу до інформації та вказано вимоги щодо нерозголошення конфіденційних даних.

Потрібно запровадити процедуру регулярного проведення навчання та підвищення рівня обізнаності співробітників у галузі інформаційної безпеки. Також необхідно реалізувати процедури контролю отриманих знань та навичок. Для цього можна використати систему тестування або ж усного опитування, ще одним із способів перевірки є створення тестової ситуації порушення інформаційної безпеки, для контролю дій співробітників.

Фізичні заходи захисту

Фізичні заходи захисту стосуються захисту фізичного оточення, де зберігається або оброблюється уся важлива для підприємства інформація.

Для реалізації фізичного захисту необхідно здійснити контроль доступу на територію та до приміщень організації. Для цього необхідно забезпечити наявність контрольованих зон за допомогою систем відеоспостереження, сигналізацій, пропускних карток та перепусток.

Доступ до серверів та комунікаційного обладнання потрібно обмежити шляхом їх розміщення у спеціальних закритих приміщеннях, або ж у спеціальних коробах та захисних ящиках. Доступ до них повинен бути лише у обмеженого кола осіб, у чиї посадові обов'язки входить робота з даним видом обладнання.

Слід впровадити необхідні запобіжні заходи, щодо мінімізації ризиків, що пов'язані із загрозами фізичній безпеці від навколишнього середовища. Для

мінімізації наслідків пожежі потрібно встановити та налаштувати системи, здатні виявляти пожежі на ранній стадії та надсилати сигнали тривоги або запускати системи пожежогасіння. Для захисту від повені чи підтоплення слід здійснити встановлення систем, здатних виявляти затоплення на ранній стадії під підлогою зон, що містять носії інформації або системи обробки інформації. Водяні насоси або еквівалентні засоби повинні бути наявними та легкодоступними на випадок затоплення. Для захисту від загроз, пов’язаних електроенергією потрібно встановити системи безперебійного аварійного живлення та захисту від стрибків напруги.

Потрібно запровадити політику чистого столу та екрану. Всі співробітники мають залишали свої робочі столи чистими і порожніми після завершення робочого. Необхідно прибрати зі столу всі документи, записи, ключі, карти доступу та інші матеріали, які можуть містити конфіденційну інформацію. Після завершення робочого сеансу слід блокувати екран або вимикати комп'ютер. Важливо забезпечити фізичний захист документів, для цього їх необхідно зберігати у закритих шафах або сейфах.

Технологічні заходи захисту

Технологічні заходи захисту спрямовані на захист інформаційних активів організації від різних технологічних загроз і вразливостей.

За допомогою криптографічних методів реалізується захист конфіденційності, цілісності та достовірності інформації. До них відноситься використання процесу шифрування даних, що передаються або ж зберігаються у інформаційних системах підприємства та цифрових підписів для перевірки автентичності та цілісності.

Для забезпечення мережевої безпеки необхідно використовувати брандмауери, системи виявлення та запобігання вторгненням, сканери мережевої активності а також сегментацію мережі. Брандмауери діють як бар'єр між надійною внутрішньою мережею та ненадійними зовнішніми мережами, такими як Інтернет. Вони перевіряють і контролюють вхідний і вихідний мережевий трафік на основі політики безпеки організації [44]. Мережеві сканери

– це інструменти та програмні додатки, призначені для сканування та оцінки безпеки комп'ютерних мереж, систем і пристроїв [45]. Вони відіграють вирішальну роль у виявленні вразливостей, неправильних конфігурацій і потенційних слабких місць в інфраструктурі мережі. Сегментація мережі дозволить зменшити ризик для несанкціонованого доступу під час мережевих атак.

Необхідно здійснити реалізацію захисту від шкідливого програмного забезпечення, такого як віруси, хробаки, трояни та інше шкідливе програмне забезпечення. Для цього слід забезпечити наявність на усіх пристроях підприємства встановленого антивірусного програмного забезпечення. Необхідно здійснювати регулярне сканування на наявність шкідливого програмного забезпечення усіх файлів та програм, що передаються та надсилаються у мережі компанії.

Необхідно здійснювати виявлення технічних вразливостей у встановлених операційних системах та програмному забезпечені. Для цього слід запровадити використання сканерів вразливостей та здійснення регулярного тестування на проникнення. Сканери вразливостей – це автоматизовані інструменти, які використовуються для виявлення, оцінки та повідомлення про потенційні вразливості безпеки в комп'ютерних системах, мережах і додатках [46]. Ці інструменти відіграють вирішальну роль у підтримці та посиленні інформаційної безпеки організації шляхом виявлення слабких місць, які можуть бути використані зловмисниками. Тестування на проникнення – це процес оцінки безпеки, в якому фахівці з кібербезпеки імітують реальні кібератаки на інформаційні системи, додатки та мережі організації з метою виявлення вразливостей і слабких місць [47]. Основна мета тестування на проникнення – оцінити безпеку активів та інфраструктури організації шляхом імітації зловмисних дій хакерів.

Для запобіганню витоку конфіденційних та критично важливих даних слід впровадити використання DLP рішень. DLP (Data Loss Prevention) – інструменти та рішення для запобігання втраті даних покликані допомогти організаціям

запобігти несанкціонованому розкриттю конфіденційної інформації та запобігти витоку даних [48]. Рішення DLP необхідні для захисту конфіденційної інформації, такої як дані клієнтів, інтелектуальна власність, фінансова звітність та інші конфіденційні дані. Вони пропонують широкий спектр можливостей, включаючи виявлення даних, моніторинг, забезпечення дотримання правил та реагування на інциденти.

Для збереження цілісності та доступності інформації слід запровадити виконання процедури резервного копіювання даних. Копіювання даних слід здійснювати регулярно для всіх критичних інформаційних систем та даних. Необхідно забезпечити безпечне та захищене зберігання резервних копій даних від фізичних і кіберзагроз. Усі скопійовані дані мають зберігатися у зашифрованому вигляді. Доступ до резервних копій потрібно забезпечити лише авторизованим співробітникам.

Необхідно встановити контроль над кінцевими точками та способами віддаленого підключення до мережі та систем підприємства. Під кінцевими точками в цьому контексті зазвичай маються на увазі окремі пристрої, такі як робочі станції, ноутбуки, сервери та мобільні пристрої в мережі організації. Для забезпечення безпеки кінцевих точок слід використовувати технологію EDR. EDR (Endpoint Detection and Response) – це технологія і підхід до кібербезпеки, спрямовані на виявлення, розслідування та реагування на інциденти безпеки на рівні кінцевих точок [49]. Рішення EDR призначені для забезпечення видимості в реальному часі діяльності кінцевих точок, виявлення потенційних загроз і швидкого реагування на інциденти. Для віддаленого підключення до мережі підприємства слід використовувати VPN. Технологія VPN використовується для забезпечення безпечного та зашифрованого з'єднання, тим самим гарантуючи конфіденційність при передані інформації.

2.2.4 Впровадження заходів управління безпекою та моніторинг і покращення

Впровадження заходів управління безпекою здійснюється на основі документації, політики правил та процедур що були створені на попередньому

етапі.

Згідно з ISO 27001, після впровадження заходів управління, необхідно організувати неперервний процес моніторингу та покращення інформаційної безпеки в організації. Цей процес є ключовим для забезпечення ефективності системи управління інформаційною безпекою (СУІБ). Даний процес можливо реалізувати за допомогою наступних кроків.

Визначення показників інформаційної безпеки. Проєктування та визначення ключових показників інформаційної безпеки, які допоможуть оцінювати ефективність розробленої СУІБ. Ці показники можуть включають в себе інциденти безпеки, відхилення від політики безпеки, результати аудитів, витрати на заходи забезпечення безпеки.

Моніторинг та збір інформації. Забезпечення постійного моніторингу інформації, пов'язаної з інформаційною безпекою. Даний процес включає в себе відстеження подій та виявлення можливих інцидентів безпеки, а також збір інформації щодо дійсних станів і результатів процесів інформаційної безпеки.

Оцінка ризиків та відхилень. Проведення оцінки ризиків та виявлення відхилень від встановлених вимог інформаційної безпеки. Оцінка серйозності імовірних загроз і ризиків.

Покращення та коригування. На основі результатів оцінки ризиків та відхилень необхідно приймати коректівні заходи. Вони включають в себе розробку планів дій для виправлення виявлених проблем і запобігання подібним проблемам у майбутньому.

Проведення аудитів. Необхідно регулярно проводити аудити наявної СУІБ, щоб переконатися, що вона відповідає вимогам стандарту ISO 27001 і забезпечує високий рівень інформаційної безпеки.

Документування та звітність. Необхідно детально документувати усі проведені заходи моніторингу та покращення, включаючи виявлені відхилення та вжиті процедури. Потрібно організувати процес створення звітів із проведених робіт та зберігати їх для отримання детальної інформації про зміни під час наступних аудитів.

Навчання персоналу. Необхідно організовувати процес навчання усіх працівників підприємства щодо важливості дотримання інформаційної безпеки і внутрішніх політик та процедур. Потрібно обов'язково проводити додаткове навчання у випадку внесення змін у структуру СУІБ.

Процес моніторингу та покращення є циклічним і повинен продовжуватися неперервно, щоб забезпечити високий рівень інформаційної безпеки в організації. Такий підхід допомагає адаптувати систему управління інформаційною безпекою до змінних умов і загроз.

2.3 Методика оцінка ризиків

Після визначення усіх інформаційних активів підприємства та ідентифікації можливих загроз та вразливостей, необхідно здійснити процес оцінки ризиків, що може зазнати підприємство внаслідок порушення інформаційної безпеки активів.

Оцінка ризиків здійснюється у контексті визначення величини рівня завдання збитку, що може нанести процес реалізації загрози для певного активу.

Величина ризику від реалізації загрози обчислюється як добуток збитків від одноразової реалізації ризику на коефіцієнт, що характеризує ймовірність реалізації певної загрози протягом одного року (2.1).

$$R = L \cdot P \qquad (2.1)$$

де R – ризик від реалізації загрози, спрямованої на вразливість місця зберігання активу;

L – фінансовий збиток від одноразової реалізації загрози, спрямованої на місце, де зберігається актив;

P – середньорічна частота реалізації загрози $P \in \{1, 2, 3\}$

Критерії для визначення частоти реалізації загрози наведено у табл. 2.1

Таблиця 2.1 – Середньорічна частота реалізації загрози

Значення	Рівень частоти реалізації загрози	Опис
1	Низький	Здатність реалізувати загрозу низька, джерело загрози недостатньо мотивоване. Діючі засоби захисту ускладнюють реалізацію загрози. Відсутня статистика або інша інформація, яка б вказувала, що інцидент може статися.
2	Середній	Джерело загрози мотивоване, існують передумови для реалізації загрози. Інформація про уразливість опублікована для широкої аудиторії, проте необхідні спеціальні технічні засоби для реалізації загрози.
3	Високий	Інформація про уразливість опублікована для широкої аудиторії. Існує статистика або інша інформація, яка вказує на те, що загроза скоріше за все здійсниться або можуть існувати серйозні причини або мотиви атакуючого, щоб здійснити такі дії

Величина фінансових збитків від одноразової реалізації загрози, спрямованої на місце зберігання активу визначається за формулою 2.2.

$$L = \sum C_{ass} \cdot L_R \tag{2.2}$$

де L – фінансовий збиток від одноразової реалізації загрози, спрямованої на вразливість місця зберігання активу;

C_{ass} – вартість активу;

L_R – рівень наслідків при порушенні конфіденційності, цілісності та доступності активу, $L_R \in \{0…1\}$.

Вартість активу C_{ass} виражається у грошових одиницях, що в залежності від його типу обчислюється на основі наступних факторів:

– вартість утримання активу;
– вартість заміни або відновлення активу;
– витрати в разі недоступності активу;
– шкода репутації організації;
– зниження річного доходу;
– зниження рівня конкурентоспроможності;
– зниження рівня ефективності проведення бізнес процесів;
– штрафи та санкції за порушення законодавчих норм та вимог.

Рівень наслідків при порушенні конфіденційності, цілісності та доступності активу визначається за формулою 2.3.

$$L_R = max\{C_c, C_i, C_a\} \quad (2.3)$$

де L_R – рівень наслідків від порушення конфіденційності, цілісності та доступності активу;

C_c – рівень наслідків шкоди при порушенні конфіденційності;

C_i – рівень наслідків шкоди при порушенні цілісності;

C_a – рівень наслідків шкоди при порушенні доступності.

Значення рівня наслідків шкоди визначається за допомогою таблиці 2.2.

Щоб оцінити отриману величина ризику від реалізації загрози *R*, визначимо певний поріг витрат збитку від діяльності підприємства. В даному випадку значення прогу становить 5% від чистого прибутку підприємства. Базуючись на цьому значені можливо визначити величину ризику: високий, середній або низький (табл. 2.3).

Таблиця 2.2 – Наслідки при порушенні конфіденційності, цілісності та доступності активу

Значення рівня порушення	Опис
0	Порушення не мають відчутних наслідків
0,1-0,3	Незначний рівень фінансових збитків; мінімальна шкода для бізнес процесів підприємства; погіршення іміджу та втрата довіри деяких клієнтів і партнерів.
0,4-0,6	Середній рівень фінансових збитків; середня шкода для бізнес процесів підприємства; середнє погіршення іміджу та втрата довіри деяких клієнтів і партнерів.
0,7-0,9	Фінансовий рівень відчутно зменшився; завдано значної шкоди усім бізнес процесам підприємства; значне погіршення іміджу та втрата довіри значної клієнтів і партнерів.
1	Фінансовий рівень критично зменшився; завдано критичної шкоди усім бізнес процесам підприємства; критичне погіршення іміджу та втрата довіри клієнтів і партнерів.

Таблиця 2.3 – Визначення величини ризику

Рівень ризику	Величина матеріального збитку
Високий	≥ 5% від прибутку підприємства
Середній	від 2% до 5% прибутку підприємства
Низький	≤ 2% від прибутку підприємства

Підприємство приймає та запобігає ризикам із високим та середнім рівнем. Відносно ризиків низького рівня застосовується процес уникнення.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДИКИ

3.1 Збір даних про підприємство та інвентаризація активів

Досліджуване підприємство А працює у сфері продаж та займається реалізацією товару широкого спектру вжитку. На теперішній час у підприємстві нараховується близько 45 тисяч співробітників. Прибуток за 2022 рік становить 6000 мільйонів гривень.

Очолює підприємство генеральний директор. До організаційної структури підприємства входять наступні підрозділи:

- рада директорів;
- юридичний відділ;
- відділ безпеки;
- ІТ відділ;
- фінансовий відділ;
- відділ торгівлі;
- логістичний відділ;
- відділ маркетингу;
- відділ управління персоналом;
- відділ контролю якості товарів;
- відділ бізнес-аналітики;
- відділ закупівель;
- відділ управління нерухомістю;
- відділ технічного проектування та розвитку;
- відділ цифрової торгівлі.

Оскільки процес імплементації серії стандартів ISO 27000 на систему управління інформаційною безпекою підприємства – дуже тривалий та масштабний процес, у рамках даної роботи буде висвітлено лише його реалізацію у рамках фінансового відділу.

Фінансовий відділ володіє та обробляє наступні інформаційні активи:

1) фінансова звітність;
2) інформація про операційні доходи;
3) дані про витрати на закупівлю товарів;
4) кошториси і плани фінансування;
5) бухгалтерська документація;
6) дані про облік запасів товарів;
7) інформація про цінову політику;
8) фінансові проекції та прогнози;
9) дані про фінансові ризики;
10) інформація про облік та управління заборгованостями клієнтів;
11) аналіз фінансових показників;
12) дані про оподаткування та податкові зобов’язання;
13) фінансові контракти з постачальниками;
14) фінансові зобов’язання перед постачальниками;
15) дані про операційні витрати;
16) фінансова інформація про платіжні системи;
17) інформація про інвестиційні можливості;
18) дані про розрахунковий обіг та готівкові операції;
19) дані про фінансові ресурси та їх розподіл;
20) інформація про фінансову аналітику;
21) фінансові договори з банками чи фінансовими установами;
22) дані про плани стратегічного розвитку;
23) дані про фінансові зв'язки з іншими підприємствами та партнерами;
24) дані про майно компанії.

До місць зберігання інформаційних активів, якими володіє фінансовий відділ підприємства відносяться:

- ПК працівників;
- система електронного документообігу;
- паперові носії;
- система Business Intelligence;

– поштовий сервер.

Детальна інформація про інвентаризацію перерахованих інформаційних активів розміщена у таблиці А.1 додатку А. Для кожного із активів зазначено їх вартість та вказано місце зберігання та обробки у загальній системі функціонування підприємства.

Визначимо цінність інформаційних активів та їх рівень критичності для підприємства, а також наслідки при порушенні конфіденційності, цілісності та доступності активу (табл. 3.2).

Для визначення цінності та критичності інформаційних активів було використано шкалу з таблиці 3.1. На основі цих даних було визначено наслідки при порушенні конфіденційності, цілісності та доступності активу, шкала оцінювання наведена у таблиці 2.2 (див. розділ 2). Відповідні значення для кожного із активів було визначено на основі власної експертної думки, що базувалася на даних, зібраних у процесі вивчення специфіки роботи підприємства та проведені інтерв'ю із працівниками та керівниками фінансового відділу.

Таблиця 3.1 – Класифікація інформаційних активів за ступенем їх впливу на функціонування підприємства

Цінність інформаційних активів	Рівень критичності
8-10	К1 (особливо критична інформація)
5-7	К2 (критична інформація)
2-4	К3 (інформація середньої критичності)
0-1	К4 (некритична інформація)

Таблиця 3.2 – Цінність інформаційних активів фінансового відділу

№	Інформаційний актив	Цінність	Рівень критичності	Рівень наслідків від порушення КЦД		
				К	Ц	Д
1	Фінансова звітність	9	К1	0,9	0,9	0,9
2	Інформація про операційні доходи	6	К2	0,5	0,7	0,7
3	Дані про витрати на закупівлю товарів	4	К3	0,3	0,7	0,7

Продовження таблиці 3.2

№	Інформаційний актив	Цінність	Рівень критичності	Рівень наслідків від порушення КЦД		
				К	Ц	Д
4	Кошториси і плани фінансування	8	К1	0,6	0,8	0,8
5	Бухгалтерська документація	9	К1	0,9	0,9	0,9
6	Дані про облік запасів товарів	5	К2	0,2	0,7	0,6
7	Інформація про цінову політику	4	К3	0,3	0,5	0,5
8	Фінансові проекції та прогнози	8	К1	0,8	0,8	0,8
9	Дані про фінансові ризики	9	К1	0,9	0,9	0,9
10	Інформація про облік та управління заборгованостями	7	К2	0,8	0,7	0,8
11	Аналіз фінансових показників	5	К2	0,6	0,7	0,6
12	Дані про оподаткування та податкові зобов’язання	9	К1	0,1	0,8	0,8
13	Фінансові контракти з постачальниками	5	К2	0,9	0,9	0,9
14	Фінансові зобов’язання перед постачальниками	5	К2	0,6	0,7	0,7
15	Дані про операційні витрати	6	К2	0,6	0,7	0,7
16	Фінансова інформація про платіжні системи	7	К2	0,6	0,8	0,8
17	Інформація про інвестиційні можливості	7	К2	0,9	0,9	0,9
18	Дані про розрахунковий обіг та готівкові операції	6	К2	0,6	0,7	0,7
19	Дані про фінансові ресурси та їх розподіл	8	К1	0,6	0,8	0,7
20	Інформація про фінансову аналітику	7	К2	0,9	0,8	0,8
21	Договори з банками чи фінансовими установами	8	К1	0,7	0,7	0,7
22	Дані про плани стратегічного розвитку	8	К1	0,8	0,8	0,8

Після проведення інвентаризації інформаційних активів перейдемо до етапу оцінки ризиків.

3.2 Визначення загроз та оцінка ризиків для підприємства

Для реалізації процесу ідентифікації загроз та вразливостей було здійснено аудит наявних на підприємстві засобів контролю безпеки та процесу організації та виконання співробітниками бізнес-процесів. Отримання необхідної інформації було реалізовано шляхом проведення інтерв'ю із співробітниками фінансового відділу та IT відділу. Був здійснений додатковий аудит налаштувань безпеки на всіх рівнях інформаційних систем, таких як операційні системи, бази даних та програмні додатки.

Після проведення аудиту фінансового відділу підприємства було виявлено наступні загрози:

- втрата або крадіжка місця збереження інформаційних активів;
- випадкове розголошення конфіденційних даних працівником підприємства або підрядником;
- свідоме розголошення конфіденційних даних працівником підприємства або підрядником;
- неочікувані наслідки в результаті впровадження нових бізнес-процесів, змін у програмному забезпеченні та обладнані;
- проникнення зловмисника в інформаційну систему з метою отримання доступу до конфіденційної інформації, порушення функціональності системи та спричинення інших негативних наслідків.

Для визначених загроз було здійснено опис наявних вразливостей у системі управління інформаційною безпекою фінансового відділу досліджуваного підприємства торгівлі. Визначено на які конкретно місця зберігання інформаційних активів впливає та чи інша загроза. На основі цієї інформації було визначено можливі ризики та наслідки від їх реалізації для підприємства (табл. 3.3).

Таблиця 3.3 – Опис загроз, вразливостей та ризиків

Загроза	Місце зберігання активу	Вразливість	Ризик
Втрата або крадіжка місця збереження інформаційних активів	ПК працівників	Проблеми в процесі шифрування конфіденційної інформації на пристроях. Відповідальність за шифрування даних покладається на кінцевих користувачів.	Отримання несанкціонованого доступу до конфіденційної інформації підприємства внаслідок крадіжки чи втрати обладнання з важливими даними через відсутність або недоліки у процесах та інструментах шифрування інформації.
	Паперові носії	Відсутні контроль та відповідальність за фізичний захистом документів при їх пересилці. На підприємстві користуються послугами декількох служб доставок, з якими не укладено жодного договору, у якому було б чітко окреслено засоби захисту документів від фізичної втрати чи пошкодження та нерозголошення їх змісту	Крадіжка документів, які містять важливу інформацію, як з боку представників кур'єрських служб, так і зловмисників, через відсутність контролю під час пересилання документів та недоліки у системі відповідальності за фізичний захист цих матеріалів.
	Паперові носії	Недотримання політики чистого столу у процесі роботи з документацією	Крадіжка документів, на через недотримання правил контролю за ними на робочих місцях працівників
Випадкове розголошення конфіденційних даних працівником підприємства або підрядником	ПК працівників	Недотримання політики чистого столу	Розголошення даних шляхом отримання доступу неуповноважених осіб до пристрою

Продовження таблиці 3.3

Загроза	Місце зберігання активу	Вразливість	Ризик
Випадкове розголошення конфіденційних даних працівником підприємства або підрядником	Паперові носії	Недотримання політики чистого столу, відсутність контролю за друком на мережевому принтері	Розголошення конфіденційних даних шляхом отримання доступу неуповноважених осіб вмісту документів
	Поштовий сервер	Не реалізовано контроль за відправкою листів, що містять конфіденційні дані	Розголошення конфіденційних даних шляхом відправки листа помилковому отримувачу
Свідоме розголошення конфіденційних даних працівником	Поштовий сервер	Відсутні засоби контролю за надсиланням конфіденційних даних по пошті, у випадку шифрування вмісту листа	Розголошення конфіденційних даних шляхом відправки листа, через відсутність функціоналу системи запобігання витоку даних із аналізом зашифрованої інформації
Неочікувані наслідки в результаті впровадження нових бізнес-процесів, змін у програмному забезпеченні та обладнані	Business Intelligence	Відсутній контроль за доступом розробників до продуктивного середовища та дотримання ними вимог безпечної інсталяції та конфігурації програмних додатків	Розголошення конфіденційних даних у видку отримання невідповідних прав доступу до інформації в процесі розробки, тестування або внесення змін у інформаційну систему
Несанкціонований доступ до даних в хмарному середовищі	Business Intelligence	Недостатній контроль за доступу до інформаційних активів в орендованому хмарному середовищі, з боку решти орендарів хмари та адміністратора сервісу	Крадіжка конфіденційних даних через недоліки в управлінні доступом до інформації,, що зберігається і обробляється в хмарних сервісах

Продовження таблиці 3.3

Загроза	Місце зберігання активу	Вразливість	Ризик
Загроза безпеці електронної пошти	Поштовий сервер	Недостатній контроль за масовими розсилками та опрацюванням спаму, виявленням ШПЗ в електронних листах	Конфіденційна інформація може бути вкрадена, а інформаційні системи втратити непрацездатність через шкідливе програмне забезпечення або соціальну інженерію, що розсилаються через електронну пошту працівникам підприємства
Несанкціонований доступ до системи	Система електронного документообігу	Поточні вимоги до паролю не відповідають вимогам безпеки: мінімальна довжина паролю задана 7 символів, відсутнє обмеження на кількість спроб вводу паролю	Отримання зловмисником доступу до системи через реалізації атаки brute force
Використання небезпечного ПЗ	ПК працівників	Відсутність чітко визначеного списку дозволеного ПЗ та контролю за встановленими програмами	Крадіжка або модифікація даних, порушення працездатності інформаційної системи шляхом використання ПЗ з уразливостями
Використання стандартних налаштувань та облікових записів за замовчуванням	Business Intelligence	Використання інформаційних систем з обліковими записами та паролями за замовчуванням. Відсутність процесу стандартизації безпечного налаштування систем та мережевого обладнання (перелік дозволених портів, протоколів та сервісів)	Витік конфіденційних даних через з використання вразливостей інформаційної системи та мережевого обладнання

Продовження таблиці 3.3

Загроза	Місце зберігання активу	Вразливість	Ризик
Несанкціонований доступ до системи. Порушення конфіденційності та цілісності даних.	Система електронного документообігу	Надання неузгоджених або невідповідних прав доступу до системи. Права доступу визначають адміністратори на підставі свого досвіду або раніше наданих прав співробітникам. Відсутні вимоги стосовно проведення перевірок раніше виданих прав доступу	Витік конфіденційних даних або порушення працездатності системи через отримання несанкціонованого доступу, що реалізується шляхом використання недоліків у процесі надання прав доступу.
	Система електронного документообігу	Помилки у процесі обмеження доступу до системи при звільненні співробітника. Права доступу обмежується вручну адміністратором на підставі даних, що надані відділом управління персоналом. Відсутній процес реалізації перевірок вчасного блокування доступу. Документація про блокування доступу не ведеться	Розголошення конфіденційних даних та порушення працездатності системи співробітниками, доступ яких був не вчасно заблокований

На основі отриманої інформації проведемо розрахунок рівня ризику та визначимо його величину.

Оскільки річний прибуток підприємства становить 6000 млн. грн., то ризик значення якого більше 300 млн. грн. вважається високим, від 120 до 300 млн. грн. – середнім, нижче 120 млн. грн. – низьким. Оброблятися будуть лише ризики із високим та середнім рівнем.

Ризик для загрози втрати або крадіжки місця збереження інформаційних

активів, що спрямована на місце зберігання активу ПК працівників розраховується відповідно до формул наведених у пункті 2.3.

Розрахуємо фінансовий збиток від реалізації загрози, спрямованої на місце зберігання активу *L*. Вартість активів, що зберігаються на ПК працівників зазначена у таблиці А.1 додатку А, рівень наслідків від порушення конфіденційності, цілісності та доступності активу вказано у табл. 3.2.

Фінансовий збиток від одноразової реалізації загрози, спрямованої на місце зберігання активу становить:

$$L=20,9\cdot0,9+9,15\cdot0,7+7,1\cdot0,7+16,34\cdot0,9+16,21\cdot0,8+19,03\cdot0,9+17,11\cdot0,8+$$
$$+20,3\cdot0,8=104,91 \text{ млн грн.}$$

Середньорічна частота реалізації загрози становить 1. Тоді ризик від реалізації загрози становить:

$$R=104,91\cdot1=104,91 \text{ млн грн.}$$

Дане значення становить менше 2% від річного прибутку підприємства (120 млн. грн.), тому він є низьким і не потребує жодних дій

Усі результати проведених обчислень значення рівнів представлено у таблиці А.2 додатку А.

За результатами оцінки ризиків було виявлено, що високий рівень ризиків пов’язаний із загрозами:

1) Несанкціонований доступ до системи. Стосуються місця зберігання активів – системи електронного документообігу.
2) Використання небезпечного ПЗ. Стосуються місця зберігання активів – ПК працівників.
3) Порушення конфіденційності та цілісності даних і стосується наступних місць зберігання. Стосуються місця зберігання активів – системи електронного документообігу

Середній рівень ризиків стосується наступних загроз:

1) Випадкове розголошення конфіденційних даних працівником підприємства або підрядником. Місця зберігання активів, на які впливає ризик:

- ПК працівників;
- паперові носії.

2) Неочікувані наслідки в результаті впровадження нових бізнес-процесів, змін у програмному забезпеченні та обладнані. Стосуються місця зберігання активів – системи Business Intelligence.
3) Загроза безпеці електронної пошти. Стосуються місця зберігання активів – поштовий сервер.
4) Використання стандартних налаштувань та облікових записів за замовченням. Стосуються місця зберігання активів – Business Intelligence

На основі отриманої інформації здійснимо визначення заходів управління інформаційною безпекою, які потрібно впровадити або покращити у існуючу СУІБ підприємства для мінімізації ризиків.

3.3 Визначення заходів управління для мінімізації ризиків

Більшість виявлених ризиків на підприємстві пов’язані із відсутністю відповідних нормативних документів, які визначають безпечні налаштування компонентів інфраструктури у інформаційній системі підприємства, процедури надання прав доступу та порушення політики чистого столу.

Необхідно запровадити управління та контроль за програмним забезпеченням, що використовується на підприємстві. Для цього слід:

1) Створити повний перелік усього програмного забезпечення, що дозволено для використання.
2) Здійснювати контроль над ліцензіями програмного забезпечення, термінами їх дії та відновленням.
3) Забезпечити своєчасне оновлення програмного забезпечення для збереження безпеки та функціональності.
4) Заборонити працівникам самостійно установлювати програмне забезпечення, шляхом надання прав адміністратора лише

уповноваженим працівникам.

5) Запровадити процес ведення журналу зміни та аудиту програмного забезпечення.
6) Здійснювати регулярну перевірку установленого програмного забезпечення на відповідність переліку дозволеного. Вести журнал перевірки, де вказувати її результати та наявність не дозволених програм. Видаляти усі програми, що порушують встановлені правила.

Не потребує фінансових витрат, усе можливо реалізувати за рахунок наявних на підприємстві ресурсів.

Слід покращити наявні на підприємстві процедури надання прав доступу до інформаційних систем шляхом:

1) Розробити документацію, яка б чітко описувала вимоги надання, зміни та блокування прав доступу до інформаційних систем під час реалізації процедури управління доступом.
2) Впровадити процес управління привілеями користувачів відповідно наступних вимог:
   - надання користувачеві тільки необхідних привілеїв для виконання їхніх обов'язків, за принципом найменших привілеїв;
   - визначення рівнів доступу до різних частин інформаційної системи на основі потреб користувачів та їхніх обов'язків, створити матриці доступів до інформаційних систем
3) Запровадити наступні вимоги ідентифікації користувачів у системі:
   - присвоїти кожному працівникові унікальний ідентифікатор.
   - замінити усі облікові записи за замовчуванням;
   - задокументувати усі наявні облікові записи.
4) Запровадити наступні вимоги аутентифікації користувачів у системі:
   - присвоїти кожному працівникові унікальний пароль.
   - довжина паролю не менше 14 символів;
   - пароль має містити літери верхніх і нижніх регістрів, цифри та спецсимволи;

- змінювати пароль необхідно раз на 90 днів, новий пароль має не повторюватися із 10 попередніми.
- Здійснювати блокування облікового запису після трьох невдалих спроб введення паролю.

5) Запровадити процедуру логування для відслідковування дій користувачів у системі.
6) Здійснювати регулярну перевірку наявних прав доступу працівників відповідно до їх потреб та обов'язків. У виявлені невідповідності змінювати вносити зміни їх налаштування.

Фінансові витрати становлять 175$ на місяць для оплати ліцензії на використання системи логування ELK Stack. Дану систему було обрано через ряд переваг над іншими можливими варіантними на ринку. Порівняння наведено у таблиці 3.4.

Таблиця 3.4 – Порівняльна характеристика систем збирання та обробки логів

Критерій	ELK Stack	Splunk	Sumo Logic	Graylog
Функціональність	Широкий функціонал збору, зберігання та візуалізації логів. Kibana для аналізу.	Гнучкий функціонал для аналізу даних, включаючи логи.	Фокус на безпеці та моніторингу, інструменти для виявлення загроз.	Відкрите ПЗ з потужними інструментами для фільтрації та аналізу логів.
Масштабованість	Для великих обсягів даних необхідні додаткові конфігурації	Для великих обсягів даних необхідні потужні серверів та ресурсів.	Хмарний сервіс, який може легко масштабуватися в залежності від потреб.	Для великих обсягів даних необхідні додаткові конфігурації
Інтеграція	Має широкий спектр інтеграцій з іншими інструментами моніторингу та аналізу даних.	Значний перелік інтеграцій, але є обмежена підтримка для деяких систем.	Інтеграція з багатьма іншими інструментами	Значний перелік інтеграцій, але є обмежена підтримка для деяких систем.
Ціна	175$/місяць	275$/місяць	442$/місяць	510$/місяць

ELK Stack є найкращим вибором, оскільки має широкий функціонал,

низьку ціну та здатності до інтеграції з іншими інструментами.

Потрібно розробити та задокументувати процедури дотримання політики чистого столу та екрану. Для цього слід:

1) Запровадити регулярне видалення чутливих документів, які більше не потрібні.
2) Організувати зберігання важливих документів у безпечних місцях, таких як сейфи, шафи та тумби із замками, які обмежують несанкціонований доступ до документів.
3) У випадку залишення робочого місця без нагляду слід прибирати усі важливі документи із поверхні робочого столу.
4) Забезпечити процес блокування комп'ютера під час відсутності користувача або його не активності протягом 5 хвилин.
5) Здійснювати регулярне очищення робочого простору від зайвих документів та об'єктів.
6) Запровадити та розробити процедури навчання персоналу щодо збереження конфіденційності та управління даними на робочому місці.
7) Визначити відповідальних осіб за контроль дотримання політики чистого столу та розробити дисциплінарні заходи, що будуть застосовуватися до працівників у випадку порушення.

Фінансові витрати становлять 7000-15000 $. Та складаються із наступних витрат:

– 5000-10000$ – створення підрядниками LMS системи для організації навчання персоналу;
– Від 2000$ – розробка матеріалу для проведення навчань та тренінгів із інформаційної безпеки.

Для уникнення ризику, пов’язаного із електронною поштою слід запровадити використання шлюзу безпеки електронної пошти (Cisco Email Security Appliance). Фінансові витрати становлять 1000-2500$. Дану систему було обрано через ряд переваг над іншими можливими варіантними на ринку. Порівняння наведено у таблиці 3.5.

Таблиця 3.5 – Порівняльна характеристика шлюзів безпеки електронної пошти

Критерії	Cisco Email Security	Proofpoint Email Protection	Barracuda Email Security	Sophos Email Security
Захист від фішингу	Використовує штучний інтелект для виявлення та блокування фішингових атак	Пропонує захист від атак фішингу, виявлення зловмисних посилань.	Включає захист від фішингу та спаму	Забезпечує захист від фішингу та інших загроз
Блокування спаму	Забезпечує фільтрацію спаму та блокування небажаних повідомлень	Пропонує захист від спаму та небажаних повідомлень	Блокує спам та небажані листи	Захищає від спаму та небажаних повідомлень
Виявлення вірусів	Має механізми виявлення та блокування вірусів у електронній пошті	Забезпечує захист від вірусів у пошті	Включає захист від вірусів у електронній пошті	Має захист від вірусів та інших загроз
Штучний інтелект	Використовує механізми штучного інтелекту для аналізу та блокування загроз	Має розвинуті алгоритми для виявлення та блокування загроз	Має певні функції штучного інтелекту для виявлення та блокування загроз	Має інструменти штучного інтелекту для виявлення та блокування загроз
Ціна	1000-2000$	1500-2500$	2,66$/місяць за 1 користувача	55,30$/місяць

З урахуванням перелічених критеріїв Cisco Email Security видається найбільш підходящим варіантом, оскільки він володіє розвинутими можливостями захисту від фішингу, спаму, вірусів і використовує штучний інтелект для ефективної блокування загроз у електронній пошті, а також має оптимальну ціну.

Перелічені заходи управління допоможуть мінімізувати вплив ризиків на інформаційну систему підприємства. Однак для забезпечення ефективної протидії загрозам слід регулярно здійснювати контроль їх ефективності та відповідності стану організації інформаційної системи підприємства.

4 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження, якщо вона відповідає вимогам часу, як в напрямку науково-технічного прогресу та і в плані економіки. Тому для науково-дослідної роботи необхідно оцінювати економічну ефективність впровадження розробки на підприємстві торгівлі.

Для оцінки розробленої методики імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства необхідно здійснити:

1) проведення технологічного аудиту власної науково-технічної розробки, тобто встановлення її науково-технічного рівня;
2) розрахунок витрат на здійснення науково-технічної розробки;
3) розрахунок економічної ефективності науково-технічної розробки у випадку її впровадження на підприємстві та обґрунтування економічної доцільності впровадження розробленого у магістерській кваліфікаційній роботі науково-технічного проекту.

4.1 Проведення технологічного аудиту науково-технічної розробки

Метою проведення технологічного аудиту дослідження за темою «Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства» є оцінювання науково-технічного рівня розробки, створеної в результаті науково-технічної діяльності. Оцінювання науково-технічного рівня розробки рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 4.1 [50].

Для проведення технологічного аудиту залучені 3 незалежних експерти: Баришев Ю. В, Куперштейн Л. М., Войтович О. П. Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки зведено до таблиці 4.2.

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня розробки та бальна оцінка.

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів нижча за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижча за ціни аналогів	Ціна продукту значно нижча за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування

Продовження таблиці 4.1

10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5- ти років. Термін окупності інвестицій більший 5- ти років	Термін реалізації ідеї менший 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менший 3-х років. Термін окупності інвестицій менший 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що потребує значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту потребує незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Таблиця 4.2 – Результати оцінювання науково-технічного рівня розробки

Критерії	Експерти		
	Баришев Ю. В,	Куперштейн Л. М.,	Войтович О. П
	Бали		
1. Технічна здійсненність концепції	2	3	3
2. Ринкові переваги (наявність аналогів)	2	2	2
3. Ринкові переваги (ціна продукту)	4	3	3
4. Ринкові переваги (технічні властивості)	3	2	2
5. Ринкові переваги (експлуатаційні витрати)	4	4	4
6. Ринкові перспективи (розмір ринку)	2	2	2
7. Ринкові перспективи (конкуренція)	3	4	3
8. Практична здійсненність (наявність фахівців)	3	4	3
9. Практична здійсненність (наявність фінансів)	3	3	3
10. Практична здійсненність (необхідність нових матеріалів)	4	3	4
11. Практична здійсненність (термін реалізації)	4	4	4
12. Практична здійсненність (розробка документів)	3	4	3
Сума балів	37	38	36
Середньоарифметична сума балів $СБ_c$	37		

За результатами розрахунків, наведених в таблиці 4.2, робиться висновок щодо науково-технічного рівня розробки. При цьому використовують рекомендації, наведені в табл. 4.3.

Таблиця 4.3 – Науково-технічні рівні розробки

Середньоарифметична сума балів СБ, розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вищий середнього
21…30	Середній
11…20	Нижчий середнього
0…10	Низький

Згідно проведених досліджень науково-технічний рівень розробки становить 37 балів, що, відповідно до таблиці 4.3, свідчить про важливість проведення даних досліджень (рівень потенціалу розробки вище середнього).

4.2 Оцінювання рівня конкурентоспроможності розробки

Проведемо порівняння технічних та економічні параметрів аналога та нової науково-технічної розробки, результати наведено таблиці 4.4.

Таблиця 4.4 – Технічні та економічні параметри аналога та нової науково-технічної розробки

Параметр	Одиниця виміру	Аналог	Нова розробка	Індекс зміни значення параметра	Коефіцієнт вагомості
Технічні					
Кількість факторів впливу	од.	4	5	1,25	0,6
Складність розрахунків	бал.	2	4	2	0,3
Кількість виконання необхідних етапів	од.	8	6	1,3	0,1
Економічні					
Витрати на ПЗ для проведення розрахунків	Грн	2000	1500	0,75	1

Розрахуємо груповий показник конкурентоспроможності за нормативними параметрами за формулою [50]:

$$I_{НП} = \prod_{i=1}^{n} q_i, \tag{4.1}$$

де $I_{нп}$ – загальний показник конкурентоспроможності за нормативними параметрами;

q_i – одиничний (частинний) показник за і-м нормативним параметром;

n – кількість нормативних параметрів, які підлягають оцінюванню.

$I_{нп}$=1,25·2·1,3·0,75=2,4375

Розрахуємо значення групового параметричного індексу за технічними параметрами з урахуванням вагомості (частки) кожного параметра:

$$I_{ТП} = \sum_{i=1}^{n} q_i \cdot \alpha_i, \tag{4.2}$$

де $I_{ТП}$ – груповий параметричний індекс за технічними показниками (порівняно з аналогом);

q_i – одиничний параметричний показник і-го параметра;

α_i – вагомість і-го параметричного показника;

n – кількість технічних параметрів, які підлягають оцінюванню. ·

$I_{ТП}$=1,25·0,6+2·0,3+1,3·0,1=1,48

Розрахуємо значення групового параметричного індексу за економічними параметрами:

$$I_{ЕП} = \sum_{i=1}^{m} q_i \cdot \beta_i \tag{4.3}$$

де $I_{ЕП}$ – груповий параметричний індекс за економічними показниками;

q_i – економічний параметр і-го виду;

β_i – частка і-го економічного параметра;

m – кількість технічних параметрів, які підлягають оцінюванню.

$I_{ЕП}$=0,75·1=0,75

На основі групових параметричних індексів за нормативними, технічними та економічними показниками розрахуємо інтегральний показник конкурентоспроможності за формулою:

$$К_{ІНТ} = I_{НП} \cdot \frac{I_{ТП}}{I_{ЕП}}, \quad (4.4)$$

$К_{ІНТ}$=2,4375*1,48/0,75=4,81

За результатами проведених розрахунків інтегральний показник конкурентоспроможності становить 4,81 та має високий рівень конкурентоспроможності ($К_{ІНТ}$ > 1).

4.3 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.3.1 Витрати на оплату праці

Витрати на основну заробітну плату дослідників (Зо) розраховуємо у відповідності до посадових окладів працівників, за формулою [50]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (4.5)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

Проведені розрахунки зведемо до таблиці (табл. 4.5).

Таблиця 4.5 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Кількість днів роботи	Витрати на заробітну плату, грн
Керівник	30000	1428,5	28	40 000
Розробник	25000	1 190,5	28	33 333
Всього				73 333

Витрати на основну заробітну плату робітників ($З_р$) за відповідними розраховуємо за формулою:

$$З_{\text{р}} = \sum_{i=1}^{n} C_i \cdot t_i, \tag{4.6}$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника на виконання певної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{\text{зм}}}, \tag{4.7}$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо M_M=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду;

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих;

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 дн;

$t_{зм}$ – тривалість зміни, год. $t_{зм}$=8 год.

Проведені розрахунки зведемо до таблиці (табл. 4.6).

Таблиця 4.6 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Розробка	20	5	1,7	111,8	2 236
Тестування	8	4	1,5	98,7	789,6
Впровадження	5,30	3	1,35	88,8	470,64
Всього					3 496,24

Додаткову заробітну плату дослідників та робітників ($З_{дод}$) розраховуємо як 10…12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.8)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. $Н_{дод}$ =11%.

$З_{дод}$=(73 333+3 496,24)·11/100%=8 451,2 грн

4.3.2Відрахування на соціальні заходи

До статті «Відрахування на соціальні заходи» належать відрахування внеску на загальнообов’язкове державне соціальне страхування та для здійснення заходів щодо соціального захисту населення (ЄСВ – єдиний соціальний внесок). Нарахування на заробітну плату дослідників та робітників розраховується як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%}, \quad (4.9)$$

де $Н_{зп}$ – норма нарахування на заробітну плату.

$З_н$=(73 333+3 496,24+8 451,2)·22/100%=18 761,6 грн.

4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби й предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень.

Витрати на матеріали (*М*) у вартісному вираженні розраховуються окремо для кожного виду матеріалів за формулою:

$$\text{М} = \sum_{j=1}^{n} \text{Н}_j \cdot \text{Ц}_j \cdot \text{К}_j - \sum_{j=1}^{n} \text{В}_j \cdot \text{Ц}_{\text{в}j}, \tag{4.10}$$

де Н_j – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

Ц_j – вартість матеріалу j-го найменування, грн/кг;

К_j – коефіцієнт транспортних витрат, (К_j = 1,1 … 1,15);

В_j – маса відходів j-го найменування, кг;

$\text{Ц}_{\text{в}j}$ – вартість відходів j-го найменування, грн/кг.

Проведені розрахунки зведемо до таблиці (табл. 4.7).

Таблиця 4.7 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір офісний Zoom A4 80 г/м	260	1	0	0	286
Набір канцелярський Milan Silver (08737)	249	1	0	0	273,9
Органайзер настільний H-Tone (JJ41220)	260	1	0	0	286
Всього					845,9

4.3.4 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з

використанням прямолінійного методу амортизації за формулою:

$$А_{обл} = \frac{Ц_б}{Т_в} \cdot \frac{t_{вик}}{12}, \quad (4.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$Т_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

Проведені розрахунки зведено до таблиці (табл.4.8)

Таблиця 4.8 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Ноутбук HP Envy DV7	32420	2	2	2 593,6
Оргтехніка	6750	4	2	270
ОС Windows 11	8570	2	2	685,6
Прикладний пакет Microsoft Office 2019	7825	2	2	626
Приміщення лабораторії	632000	20	2	50 560
Всього				1581,6

4.3.5 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (Ве) розраховують за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_е \cdot К_{впі}}{\eta_i}, \quad (4.12)$$

де W_{yi} – встановлена потужність обладнання на певному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_е$ – вартість 1 кВт-години електроенергії, грн (вартість електроенергії

визначається за даними енергопостачальної компанії);

$К_{впі}$ – коефіцієнт, що враховує використання потужності, $К_{впі}$ <1;

$\eta_і$ – коефіцієнт корисної дії обладнання, $\eta_і$ <1.

Проведені розрахунки зведено до таблиці (табл.4.8)

Таблиця 4.8 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук HP Envy DV7	0,3	160	297,60
Оргтехніка	0,5	3	9,30
Всього			306,9

4.3.6 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.13)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», $Н_{ів}$=50%.

$І_в$=(73 333+3 496,24)·50/100=38 414,62 грн.

4.3.7 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.14)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», $Н_{нзв}$=100%.

$В_{нзв}$=(73 333+3 496,24)·100/100=76 829,24 грн

Витрати на проведення науково-дослідної роботи розраховуються як сума всіх попередніх статей витрат за формулою:

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + А_{обл} + В_е + І_в + В_{нзв} \quad (4.15)$$

$В_{заг}$=73333+3496,24+8451,2+18 761,6+845,9+1581,6+306,9+38 414,62+ +76 829,24=222 020,3 грн.

Загальні витрати ЗВ на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{В_{заг}}{\eta}, \quad (4.16)$$

де η – коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, η=0,9.

ЗВ=222 020,3/0,9=246 689,2 грн.

4.4 Розрахунок економічної ефективності науково-технічної розробки від її впровадження

Розрахуємо економічну ефективність Розробки та впровадження методики імплементації серії стандартів ISO 27000 для підприємства торгівлі.

В цьому випадку майбутній економічний ефект та ефективність буде формуватися на основі використання показника $\Delta П_я$ – зростання прибутку

підприємства внаслідок зниження витрат на оплату праці працівників, які виконують окремі інформаційно-технічні управлінські функції.

$$\Delta П_{Я} = \frac{ЧП \cdot ЗП \cdot 12}{N} - \frac{(0{,}2 \ldots 0{,}6) \cdot ЗВ}{\Delta N_i}, \quad (4.17)$$

де ЧП – чисельність працівників, які виконують певні функції вручну, осіб. ЧП=6;

ЗП – середня заробітна плата працівника, який виконує відповідну функцію вручну, грн. ЗП=25000 грн;

ЗВ – приблизні витрати на розробку автоматизованої системи управління, грн. ЗВ=246 689,2 грн;

N – кількість функцій, які виконуються вручну у році до впровадження результатів нової науково-технічної розробки, шт. N=20;

ΔN_i – прогнозоване зростання кількості виробничих чи інформаційно-технічних управлінських функцій, виконання яких автоматизується, в аналізованому році (відносно року до впровадження цієї розробки), шт. ΔN_i=10.

$\Delta П_я$=6·25000·12/20-0,2·246689,2/10=85066,216 грн.

Прибуток ($П_я$), який отримує підприємство від автоматизації виконання окремої інформаційно-технічної управлінської функції у кожному із років після впровадження науково-технічної розробки, грн можна приблизно оцінити, виходячи з формули:

$$П_{Я} = \frac{\Delta ЧП \cdot ЗП \cdot 12}{N}, \quad (4.18)$$

де ΔЧП – економія чисельності працівників, виконання виробничої чи управлінської функції яких було автоматизовано в аналізованому році, осіб. ΔЧП=3.

$П_я$=3·25000·12/20=45 000 грн.

Розрахуємо можливе збільшення чистого прибутку підприємства $\Delta П_і$ для кожного із років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, за формулою:

$$\Delta П_і = \Delta П_я \cdot N + П_я \cdot \Delta N \quad (4.19)$$

$\Delta П_і$=85 066,216·20+45 000·10=2 151 324,32 грн.

Розрахуємо приведену вартість збільшення всіх чистих прибутків ПП, що їх може отримати підприємство від можливого впровадження науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_і}{(1+\tau)^t}, \quad (4.20)$$

де $\Delta П_і$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

Т – період часу, протягом якого очікується отримання позитивних результатів від впровадження науково-технічної розробки, роки. Т=1

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні. τ =0,15;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання підприємством збільшеної величини чистого прибутку в аналізованому році. t=2 1,3225

ПП=2 151 324,32/(1+0,15)^2=1 626 710,26 грн.

Розрахуємо величину початкових інвестицій PV , які необхідно вкласти для здійснення науково-технічної розробки, за формулою:

$$PV = k_{розр} \cdot ЗВ, \quad (4.21)$$

де $k_{розр}$ – коефіцієнт, що враховує витрати на впровадження науково-технічної розробки. $k_{розр}$=2;

ЗВ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

PV=2·246 689,2=493 378,4 грн.

Розрахуємо абсолютний економічний ефект $Е_{абс}$ від можливого впровадження науково-технічної розробки:

$$Е_{абс} = ПП - PV \quad (4.22)$$

$Е_{абс}$=1 626 710,26-493 378,4=1 133 331,86 грн.

Величина $Е_{абс}$ має велике додатне значення, це може свідчити про потенційну доцільність у впровадженні цієї науково-технічної розробки.

Для остаточного прийняття рішення в необхідно розрахувати внутрішню економічну дохідність $Е_в$ за формулою:

$$Е_в = \sqrt[Т_ж]{1 + \frac{Е_{абс}}{PV}} - 1, \quad (4.23)$$

де $Е_{абс}$ – абсолютний економічний ефект вкладених інвестицій, грн;

PV – теперішня вартість початкових інвестицій, грн;

$Т_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, роки. $Т_ж$=4.

$Е_в$=(1+1 133 331,86/493 378,4)$^{1/4}$-1=0,35.

Розрахуємо період окупності інвестицій $Т_{ок}$, які можуть бути вкладені у впровадження та комерціалізацію науково-технічної розробки:

$$Т_{ок} = \frac{1}{Е_в} \quad (4.24)$$

$Т_{ок}$=1/0,35=2,8 роки.

$Т_{ок}$ < 3-х років, що свідчить про економічну ефективність впровадження науково-технічної розробки.

Згідно проведених досліджень науково-технічний рівень розробки за темою «Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства» становить 37 балів, що, свідчить про важливість проведення даних досліджень (рівень потенціалу розробки вище середнього). При оцінюванні інтегрального показника конкурентоспроможності науково-технічна розробка переважає існуючі аналоги приблизно в 2,68 рази.

При оцінюванні рівня конкурентоспроможності було встановлено, що узагальнений коефіцієнт конкурентоспроможності розробки дорівнює 4,81. Дане значення вказує на високий рівень конкурентоспроможності.

Загальні витрати на завершення науково-технічної роботи становлять 246 689,2 грн. Період окупності інвестицій, які можуть бути вкладені у впровадження та комерціалізацію науково-технічної розробки становить 2,8 р., що менше 3-х років, та свідчить про економічну ефективність впровадження науково-технічної розробки.

Отже можна зробити висновок про доцільність проведення науково-технічної роботи за темою «Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства».

ВИСНОВКИ

Під час виконання магістерської кваліфікаційної роботи було здійснено розробку методики імплементації серії стандартів ISO 27000 для підвищення рівня інформаційної безпеки підприємства. Для цього було проведено постановку основних задач та завдань, що дозволяють провести розробку методики. У ході виконання роботи усі визначені задачі та завдання було успішно виконано. Розроблена дипломна робота є комплексним дослідженням, спрямованим на аналіз та практичне застосування принципів інформаційної безпеки.

В результаті проведеного аналізу предметної області було виявлено та детально проаналізовано основні поняття та види інформаційної безпеки. Визначено основні стандарти у галузі інформаційної безпеки, на основі яких здійснюється побудова системи управління інформаційною безпекою. Проведено їх порівняльний аналіз та здійснено дослідження частоти їх застосування. На основі отриманих даних було доведено, що серія стандартів ISO 27000 є найбільш оптимальним вибором у якості нормативної бази для організації інформаційної безпеки підприємства. Було здійснено аналіз випадків порушення інформаційної безпеки у компаніях та організаціях та визначено, що однією із основних причин є не відповідність стандартам безпеки наявних на підприємствах систем захисту інформації. Даний факт ще раз підкреслює актуальність та доцільність проведення розробки методики.

Було проведено розробку та опис методики імплементації серії стандартів ISO 27000 для підвищення рівня інформаційної безпеки підприємства. Здійснено детальний опис кожного із етапів методики та розроблено алгоритми дій для їх реалізації. Наведено спосіб оцінки ризиків інформаційної безпеки для підприємства, що дозволяє провести їх ефективну оцінку з точки зору нанесення матеріальної та репутаційної шкоди компанії. Розроблена методика впровадження серії стандартів ISO 27000 являє собою системний підхід до

управління ризиками та заходами захисту інформаційної системи підприємства.

Проведено практичну реалізацію розробленої методики у контексті підприємства, що працює у сфері торгівлі. Здійснено аналіз структури підприємства, його основних активів та бізнес-процесів. Визначено можливі загрози та ризики, наведено їх оцінку. На основі отриманих даних розроблено конкретні стратегії з управління для мінімізації цих ризиків, що відповідають вимогам стандартів серії ISO 27000.

У економічній частині роботи було здійснено оцінювання науково-технічного рівня розробки, визначення її конкурентоспроможності, розраховано загальну вартість реалізації розробленої методики та її економічну ефективність. виявив важливість розгляду проблеми інформаційної безпеки з позицій не лише технічної, але й економічної доцільності. За результатами визначення та обчислення усіх критеріїв було визначено, що розроблена методика є доцільною та ефективною з точки зору економіки.

Отже, виходячи із проведених досліджень та практичних висновків, розроблена методика імплементації серії стандартів ISO 27000 для підвищення рівня інформаційної безпеки підприємства є актуальною та ефективною. Вона надає можливість застосувати комплексний підхід до вирішення проблем інформаційної безпеки та мінімізації наслідків від їх виникнення. Що в свою чергу має значний вплив на підвищення ефективності захисту інформації в сучасному світі технологій та бізнесу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Радецька А. О. Визначення заходів управління інформаційною безпекою підприємства на основі страндарту ISO 27002. м. Вінниця. URL: https:// conferences.vntu.edu.ua/index.php/mn/mn2024/paper/view/19600 (дата звернення: 08.12.2023).

2. NIST SP 800-53 Rev. 5. Effective from 2020-12-10.

3. ISO/IEC 27001. Effective from 2022.

4. Information security. ISACA. URL: https://www.isaca.org/search#q= information%20security&sort=relevancy (дата звернення: 18.09.2023).

5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР : станом на 1 лип. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 18.09.2023).

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/ show/2163-19#Text (дата звернення: 18.09.2023).

7. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 18.09.2023).

8. Про Стратегію кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 21.05.2021 р. URL:https://www.rnbo.gov.ua/files/2021/ STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 18.09.2023).

9. Про Стратегію національної безпеки України : Рішення Ради нац. безпеки і оборони України від 30.12.2021 р. URL: https://www.president.gov.ua/ documents/562022-41377 (дата звернення: 16.10.2023).

10. Whitman M. E., Mattord H. J. Principles of Information Security. 4th ed. 2011. 658 p.

11. What Is Information Security?. CISCO. URL: https://www.cisco.com/

c/en/us/products/security/what-is-information-securityinfosec.html (дата звернення: 19.09.2023).

12. ISO/IEC 27000 family. ISO. URL: https://www.iso.org/standard/iso-iec-27000-family (дата звернення: 19.09.2023).

13. ISO/IEC 27000:2018. ISO. URL: https://www.iso.org/standard/7390 6.html (дата звернення: 20.09.2023).

14. ISO/IEC 27001:2022. ISO. URL: https://www.iso.org/standard/73906 .html (дата звернення: 20.09.2023).

15. ISO/IEC 27006:2015. ISO. URL: https://www.iso.org/standard/7390 7.html (дата звернення: 20.09.2023).

16. ISO/IEC 27009:2020. ISO. URL: https://www.iso.org/standard/7390 7.html (дата звернення: 20.09.2023).

17. ISO/IEC 27002:2022. ISO. URL: https://www.iso.org/standard/7565 2.html (дата звернення: 20.09.2023).

18. ISO/IEC 27003:2017. ISO. URL: https://www.iso.org/standard/6341 7.html (дата звернення:20.09.2023).

19. ISO/IEC 27004:2016. ISO. URL: https://www.iso.org/standard/6412 0.html (дата звернення: 20.09.2023).

20. ISO/IEC 27005:2022. ISO. URL: https://www.iso.org/standard/80585.html (дата звернення: 20.09.2023).

21. ISO/IEC 27007:2020. ISO. URL: https://www.iso.org/standard/77802.html (дата звернення: 20.09.2023).

22. ISO/IEC 27013:2021. ISO. URL: https://www.iso.org/standard/78752.html (дата звернення: 20.09.2023).

23. ISO/IEC 27014:2020. ISO. URL: https://www.iso.org/standard/74046.html (дата звернення: 20.09.2023).

24. ISO/IEC 27021:2017. ISO. URL: https://www.iso.org/standard/61003.html (дата звернення: 20.09.2023).

25. ISO/IEC TS 27008:2019. ISO. URL: https://www.iso.org/standard/67397 .html (дата звернення: 20.09.2023).

26. ISO/IEC TR 27016:2014. ISO. URL: https://www.iso.org/standard/43756.html (дата звернення:20.09.2023).

27. ISO/IEC 27010:2015. ISO. URL: https://www.iso.org/standard/68427.html (дата звернення: 20.09.2023).

28. ISO/IEC 27011:2016. ISO. URL: https://www.iso.org/standard/64143.html (дата звернення: 20.09.2023).

29. ISO/IEC 27017:2015. ISO. URL: https://www.iso.org/standard/43757.html (дата звернення: 20.09.2023).

30. ISO/IEC 27018:2019. ISO. URL: https://www.iso.org/standard/76559.html (дата звернення: 20.09.2023).

31. ISO/IEC 27019:2017. ISO. URL: https://www.iso.org/standard/68091.html (дата звернення: 20.09.2023).

32. COBIT. ISACA. URL: https://www.isaca.org/resources/cobit (дата звернення: 20.09.2023).

33. COBIT 2019 Framework: Governance and Management Objectives. Вид. офіц. 2019. 114 с.

34. NIST SP 800-53. Rev. 5. NIST. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (дата звернення:21.09.2023).

35. Information Technology Laboratory (ITL). URL: https://www.erdc.usace.army.mil/Locations/ITL/ (дата звернення: 21.09.2023).

36. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Чинний від 2020-10-12. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

37. Utilizing Cyber Security Standards And Frameworks. Cyber Security Hub. URL: https://www.cshub.com/security-strategy/articles/utilizing-cyber-security-standards-and-frameworks (дата звернення: 21.09.2023).

38. Beamer T. What Industries Are Most Vulnerable to Cyber Attacks In 2022. Tech Business News. 2023. URL: https://www.techbusinessnews.com.au/ what-industries-are-most-vulnerable-to-cyberattacks-in-2022/(дата звернення: 30.09.2023)

39. Global number of cybercrime incidents by industry and organization size.

Ststista, 2023. URL: https://www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/ (дата звернення: 30.09.2023)

40. WHAT IS THE PLAN-DO-CHECK-ACT (PDCA) CYCLE?. ASQ. URL: https://asq.org/quality-resources/pdca-cycle (дата звернення: 30.09.2023).

41. Bogue R. Use S.M.A.R.T. goals to launch management by objectives plan. TechRepublic. 2018. (дата звернення: 02.10.2023).

42. What is SIEM?.IBM. URL: https://www.ibm.com/topics/siem (дата звернення: 02.10.2023).

43. Intrusion Detection and Prevention System. Spiceworks. URL: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-isid ps/ (дата звернення: 22.09.2023).

44. What is a Firewall?. Checkpoint. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ (дата звернення: 02.10.2023).

45. Network Scanning Tools. Intellipaat. URL:https://intellipaat.com/blog/ network- scanning-tools/ (дата звернення: 03.10.2023).

46. Vulnerability Scanning Tools. OWASP. URL: https://www.cshub.com/security-strategy/articles/utilizing-cyber-security-standards-and-frameworks (дата звернення: 03.10.2023).

47. Penetration Testing. Penetration Testing. URL: https://www.synopsys.com/ glossary/what-is-penetration-testing.html (дата звернення: 03.10.2023).

48. Data Loss Prevention. Netskope. URL: https://www.netskope.com/security-defined/what-is-data-loss-prevention-dlp (дата звернення: 03.10.2023).

49. Endpoint Detection and Response (EDR) Tools. Cynet. URL: https://www.cynet.com/endpoint-protection-and-edr/top-6-edr-tools-compar ed/ (дата звернення: 03.10.2023

50. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

ДОДАТКИ

Додаток А Результат впровадження методики на підприємстві

Таблиця А.1 – Інвентаризація активів підприємства

№	Інформаційний актив	Вартість, млн. грн	Місце зберігання активів				
			ПК працівників	Система електронного документообігу	Паперові носії	Система Business Intelligence	Поштовий сервер
1	Фінансова звітність	2,90	Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій Підрозділ податкової звітності Підрозділ інвестицій	Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій Підрозділ податкової звітності Підрозділ інвестицій	Підрозділ звітності Підрозділ проведення розрахунків	Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій Підрозділ податкової звітності Підрозділ інвестицій	Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій Підрозділ податкової звітності Підрозділ інвестицій
2	Інформація про операційні доходи	9,15	Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій	Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій	
3	Дані про витрати на закупівлю товарів	7,1	Підрозділ обліку товарів Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій	Підрозділ обліку товарів Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій		Підрозділ обліку товарів Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій	

Продовження таблиці А.1

№	Інформаційний актив	Вартість, млн. грн	Місце зберігання активів				
			ПК працівників	Система електронного документообігу	Паперові носії	Система Business Intelligence	Поштовий сервер
4	Кошториси і плани фінансування	12,5		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ інвестицій	Підрозділ звітності Підрозділ проведення розрахунків Підрозділ інвестицій		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ інвестицій
5	Бухгалтерська документація	16,34	Підрозділ звітності Підрозділ ЗП Підрозділ податкової звітності Підрозділ розрахункових операцій	Підрозділ звітності Підрозділ ЗП Підрозділ податкової звітності Підрозділ розрахункових операцій	Підрозділ звітності Підрозділ ЗП Підрозділ податкової звітності Підрозділ розрахункових операцій		
6	Дані про облік запасів товарів	7,5		Підрозділ обліку товарів		Підрозділ обліку товарів	
7	Інформація про цінову політику	4,53		Підрозділ проведення розрахунків Підрозділ обліку товарів			Підрозділ проведення розрахунків Підрозділ обліку товарів
8	Фінансові проекції та прогнози	10,2				Підрозділ звітності Підрозділ інвестицій	
9	Дані про фінансові ризики	19,8		Підрозділ звітності		Підрозділ звітності	
10	Інформація про облік та управління заборгованостями	8,6		Підрозділ звітності Підрозділ проведення розрахунків		Підрозділ звітності Підрозділ проведення розрахунків	Підрозділ звітності Підрозділ проведення розрахунків

Продовження таблиці А.1

№	Інформаційний актив	Вартість, млн. грн	Місце зберігання активу				
			ПК працівників	Система електронного документообігу	Паперові носії	Система Business Intelligence	Поштовий сервер
11	Аналіз фінансових показників	9,8				Підрозділ звітності Підрозділ проведення розрахунків	
12	Дані про оподаткування та податкові зобов’язання	16,21	Підрозділ звітності Підрозділ податкової звітності	Підрозділ звітності Підрозділ податкової звітності	Підрозділ звітності Підрозділ податкової звітності		Підрозділ звітності Підрозділ податкової звітності
13	Фінансові контракти з постачальниками	16,85			Підрозділ звітності Підрозділ проведення розрахунків Підрозділ інвестицій		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ інвестицій
14	Фінансові зобов’язання перед постачальниками	14,9			Підрозділ звітності Підрозділ проведення розрахунків Підрозділ		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ інвестицій
15	Дані про операційні витрати	16,7		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій	
16	Фінансова інформація про платіжні системи	9,12		Підрозділ звітності Підрозділ розрахункових операцій	Підрозділ звітності Підрозділ розрахункових операцій		

Продовження таблиці А.1

№	Інформаційний актив	Вартість, млн. грн	Місце зберігання активу				
			ПК працівників	Система електронного документообігу	Паперові носії	Система Business Intelligence	Поштовий сервер
17	Інформація про інвестиційні можливості	19,03	Підрозділ інвестицій	Підрозділ інвестицій		Підрозділ інвестицій	Підрозділ інвестицій
18	Дані про розрахунковий обіг та готівкові операції	20,13		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій		Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій	
19	Дані про фінансові ресурси та їх розподіл	17,11	Підрозділ обліку активів	Підрозділ звітності Підрозділ обліку активів	Підрозділ обліку активів	Підрозділ звітності Підрозділ обліку активів	
20	Інформація про фінансову аналітику	19,9				Підрозділ звітності Підрозділ проведення розрахунків Підрозділ розрахункових операцій	
21	Договори з банками чи фінансовими установами	17,15		Підрозділ звітності Підрозділ проведення розрахунків			Підрозділ звітності Підрозділ проведення розрахунків
22	Дані про плани стратегічного розвитку	20,30	Підрозділ інвестицій		Підрозділ інвестицій Підрозділ звітності		

Таблиця А.2 – Оцінка рівня ризиків

Загроза	Місце зберігання активу	Вразливість	Ризик	L, млн грн	P	R, млн грн	Рівень ризику
Втрата або крадіжка місця збереження інформаційних активів	ПК працівників	Проблеми в процесі шифрування конфіденційної інформації на пристроях. Відповідальність за шифрування даних покладається на кінцевих користувачів.	Отримання несанкціонованого доступу до конфіденційної інформації підприємства внаслідок крадіжки чи втрати обладнання з важливими даними через відсутність або недоліки у процесах та інструментах шифрування інформації.	104,91	1	104,91	Низький
	Паперові носії	Відсутні контроль та відповідальність за фізичний захистом документів при їх пересилці. На підприємстві користуються послугами декількох служб доставок, з якими не укладено жодного договору, у якому було б чітко окреслено засоби захисту документів від фізичної втрати чи пошкодження та нерозголошення їх змісту	Крадіжка документів, які містять важливу інформацію, як з боку представників кур'єрських служб, так і зловмисників, через відсутність контролю під час пересилання документів та недоліки у системі відповідальності за фізичний захист цих матеріалів.	109,30	1	109,30	Низький
	Паперові носії	Недотримання політики чистого столу у процесі роботи з документацією	Крадіжка документів, на через недотримання правил контролю за ними на робочих місцях працівників	109,30	1	109,30	Низький

Продовження таблиці А.2

Загроза	Місце зберігання активу	Вразливість	Ризик	L, млн грн	P	R, млн грн	Рівень ризику
Випадкове розголошення конфіденційних даних працівником підприємства або підрядником	ПК працівників	Недотримання політики чистого столу	Розголошення даних шляхом отримання доступу неуповноважених осіб до пристрою	104,91	2	209,82	Середній
	Паперові носії	Недотримання політики чистого столу, відсутність контролю за друком на мережевому принтері	Розголошення конфіденційних даних шляхом отримання доступу неуповноважених осіб вмісту документів	109,30	2	218,6	Середній
	Поштовий сервер	Не реалізовано контроль за відправкою листів, що містять конфіденційні дані	Розголошення конфіденційних даних шляхом відправки листа помилковому отримувачу	101,17	1	101,17	Низький
Свідоме розголошення конфіденційних даних працівником	Поштовий сервер	Відсутні засоби контролю за надсиланням конфіденційних даних по пошті, у випадку шифрування вмісту листа	Розголошення конфіденційних даних шляхом відправки листа, через відсутність функціоналу системи запобігання витоку даних із аналізом зашифрованої інформації	101,17	1	75,88	Низький
Неочікувані наслідки в результаті впровадження нових бізнес-процесів, змін у програмному забезпеченні та обладнані	Business Intelligence	Відсутній контроль за доступом розробників до продуктивного середовища та дотримання ними вимог безпечної інсталяції та конфігурації програмних додатків	Розголошення конфіденційних даних у видку отримання невідповідних прав доступу до інформації в процесі розробки, тестування або внесення змін у інформаційну систему	109,66	2	219,32	Середній

Продовження таблиці А.2

Загроза	Місце зберігання активу	Вразливість	Ризик	L, млн грн	P	R, млн грн	Рівень ризику
Несанкціонований доступ до даних в хмарному середовищі	Business Intelligence	Недостатній контроль за доступу до інформаційних активів в орендованому хмарному середовищі, з боку решти орендарів хмари та адміністратора сервісу	Крадіжка конфіденційних даних через недоліки в управлінні доступом до інформації,, що зберігається і обробляється в хмарних сервісах	109,66	1	109,66	Низький
Загроза безпеці електронної пошти	Поштовий сервер	Недостатній контроль за масовими розсилками та опрацюванням спаму, виявленням ШПЗ в електронних листах	Конфіденційна інформація може бути вкрадена, а інформаційні системи втратити непрацездатність через шкідливе програмне забезпечення або соціальну інженерію, що розсилаються через електронну пошту працівникам підприємства	101,17	2	202,34	Середній
Несанкціонований доступ до системи	Система електронного документообігу	Поточні вимоги до паролю не відповідають вимогам безпеки: мінімальна довжина паролю задана 7 символів, відсутнє обмеження на кількість спроб вводу паролю	Отримання зловмисником доступу до системи через реалізації атаки brute force	105,97	3	317,91	Високий
Використання небезпечного ПЗ	ПК	Відсутність чітко визначеного списку дозволеного ПЗ та контролю за встановленими програмами	Крадіжка або модифікація даних, порушення працездатності інформаційної системи шляхом використання ПЗ з уразливостями	104,91	3	314,73	Високий

Продовження таблиці А.2

Загроза	Місце зберігання активу	Вразливість	Ризик	L, млн грн	P	R, млн грн	Рівень ризику
Використання стандартних налаштувань та облікових записів за замовченням	Business Intelligence	Використання інформаційних систем з обліковими записами та паролями за замовчуванням. Відсутність процесу стандартизації безпечного налаштування систем та мережевого обладнання (перелік дозволених портів, протоколів та сервісів)	Витік конфіденційних даних через з використання вразливостей інформаційної системи та мережевого обладнання	109,66	3	328,98	Середній
Несанкціонований доступ до системи. Порушення конфіденційності та цілісності даних.	Система електронного документообігу	Надання неузгоджених або невідповідних прав доступу до системи. Права доступу визначають адміністратори на підставі свого досвіду або раніше наданих прав співробітникам. Відсутні вимоги стосовно проведення перевірок раніше виданих прав доступу	Витік конфіденційних даних або порушення працездатності системи через отримання несанкціонованого доступу, що реалізується шляхом використання недоліків у процесі надання прав доступу.	105,97	3	317,91	Високий
	Система електронного документообігу	Помилки у процесі обмеження доступу до системи при звільненні співробітника. Права доступу обмежується вручну адміністратором на підставі даних, що надані відділом управління персоналом. Відсутній процес реалізації перевірок вчасного блокування доступу. Документація про блокування доступу не ведеться	Розголошення конфіденційних даних та порушення працездатності системи співробітниками, доступ яких був не вчасно заблокований	105,97	3	317,91	Високий

Додаток Б
ПРОТОКОЛ ПЕРЕВІРКИ
МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Методика імплементації серії стандартів ISO 27000 для покращення інформаційної безпеки підприємства

Автор роботи: Радецька Анастасія Олександрівна

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 91,68 %. Схожість – 8,32 %.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Валентина КАПЛУН
(підпис)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Анастасія РАДЕЦЬКА
(підпис)

Керівник роботи _____ Леонід КУПЕРШТЕЙН
(підпис)

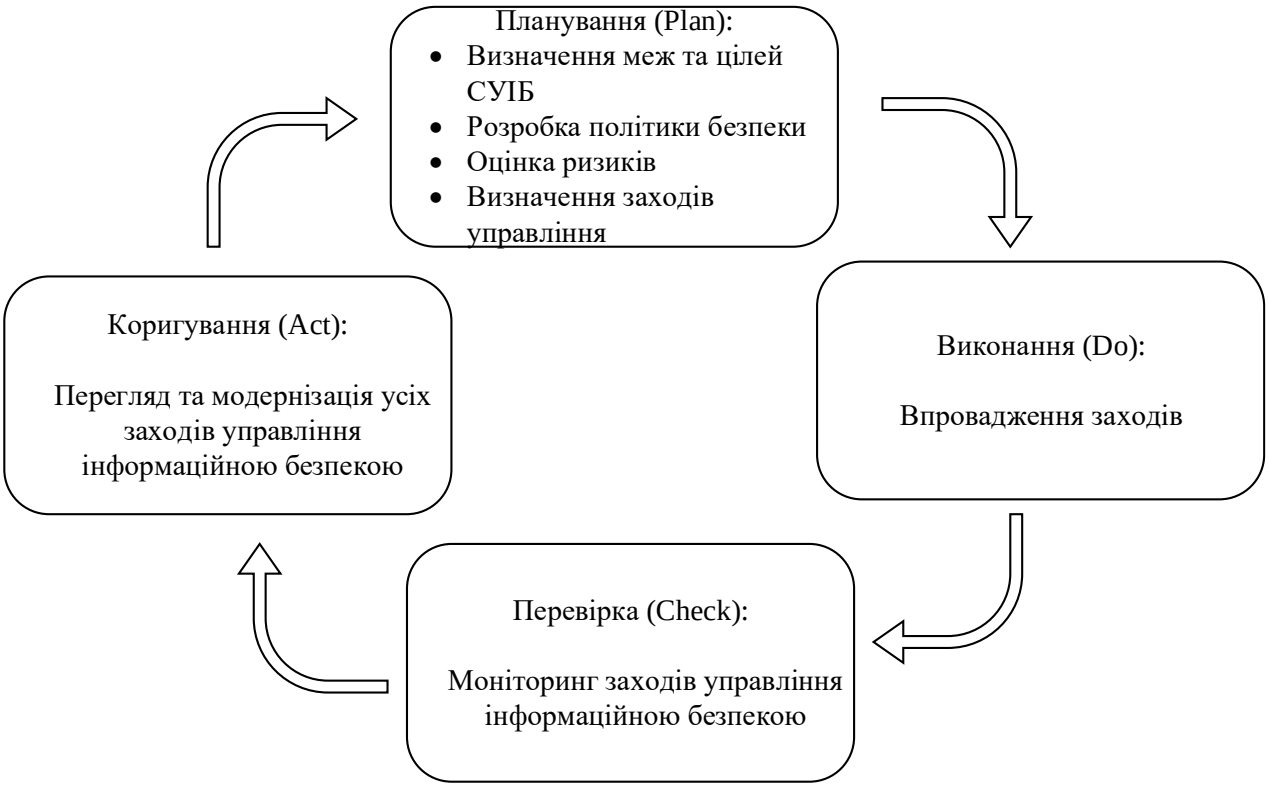
Додаток В

ІЛЮСТРАТИВНА ЧАСТИНА

МЕТОДИКА ІМПЛЕМЕНТАЦІЇ СЕРІЇ СТАНДАРТІВ ISO 27000 ДЛЯ ПОКРАЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

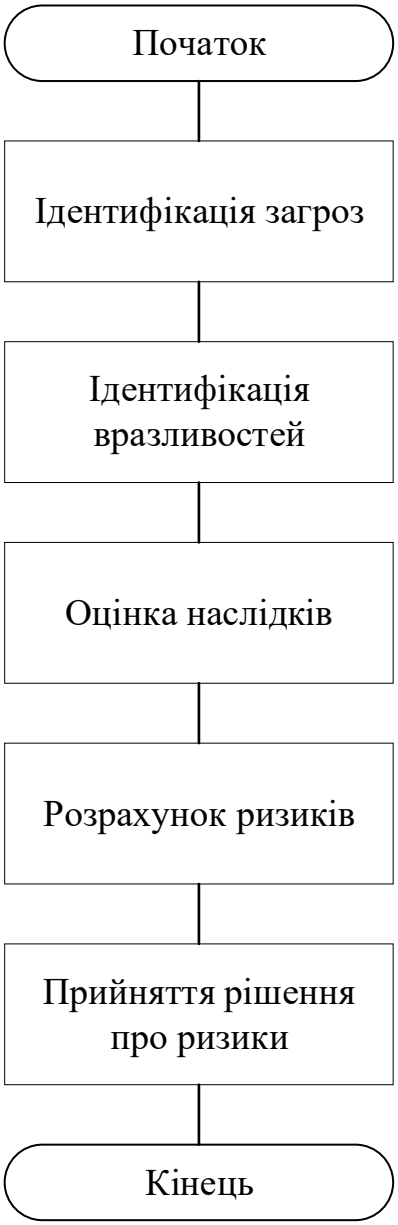
МЕТОДИКА ІМПЛЕМЕНТАЦІЯ СЕРІЇ СТАНДАРТІВ ISO 27000

ЗВ’ЯЗОК ЕТАПІВ МЕТОДИКИ ІЗ ЦИКЛОМ PDCA



АЛГОРИТМ ВИЗНАЧЕННЯ МЕЖ ТА ЦІЛЕЙ ЗАСТОСУВАННЯ СУІБ

АЛГОРИТМ ОЦІНКИ РИЗИКІВ



ЦІННІСТЬ ІНФОРМАЦІЙНИХ АКТИВІВ ФІНАНСОВОГО ВІДДІЛУ

№	Інформаційний актив	Цінність	Рівень критичності	Рівень наслідків від порушення КЦД		
				К	Ц	Д
1	Фінансова звітність	9	К1	0,9	0,9	0,9
2	Інформація про операційні доходи	6	К2	0,5	0,7	0,7
3	Дані про витрати на закупівлю товарів	4	К3	0,3	0,7	0,7
4	Кошториси і плани фінансування	8	К1	0,6	0,8	0,8
5	Бухгалтерська документація	9	К1	0,9	0,9	0,9
6	Дані про облік запасів товарів	5	К2	0,2	0,7	0,6
7	Інформація про цінову політику	4	К3	0,3	0,5	0,5
8	Фінансові проекції та прогнози	8	К1	0,8	0,8	0,8
9	Дані про фінансові ризики	9	К1	0,9	0,9	0,9
10	Інформація про облік та управління заборгованостями	7	К2	0,8	0,7	0,8
11	Аналіз фінансових показників	5	К2	0,6	0,7	0,6
12	Дані про оподаткування та податкові зобов’язання	9	К1	0,1	0,8	0,8
13	Фінансові контракти з постачальниками	5	К2	0,9	0,9	0,9
14	Фінансові зобов’язання перед постачальниками	5	К2	0,6	0,7	0,7
15	Дані про операційні витрати	6	К2	0,6	0,7	0,7
16	Фінансова інформація про платіжні системи	7	К2	0,6	0,8	0,8
17	Інформація про інвестиційні можливості	7	К2	0,9	0,9	0,9
18	Дані про розрахунковий обіг та готівкові операції	6	К2	0,6	0,7	0,7
19	Дані про фінансові ресурси та їх розподіл	8	К1	0,6	0,8	0,7
20	Інформація про фінансову аналітику	7	К2	0,9	0,8	0,8
21	Договори з банками чи фінансовими установами	8	К1	0,7	0,7	0,7
22	Дані про плани стратегічного розвитку	8	К1	0,8	0,8	0,8

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА СИСТЕМ ЗБИРАННЯ ТА ОБРОБКИ ЛОГІВ

Критерій	ELK Stack	Splunk	Sumo Logic	Graylog
Функціональність	Широкий функціонал збору, зберігання та візуалізації логів. Kibana для аналізу.	гнучкий функціонал для аналізу даних, включаючи логи.	Фокус на безпеці та моніторингу, інструменти для виявлення загроз.	Відкрите ПЗ з потужними інструментами для фільтрації та аналізу логів.
Масштабованість	Для великих обсягів даних необхідні додаткові конфігурації	Для великих обсягів даних необхідні потужні серверів та ресурсів.	Хмарний сервіс, який може легко масштабуватися в залежності від потреб.	Для великих обсягів даних необхідні додаткові конфігурації
Інтеграція	Має широкий спектр інтеграцій з іншими інструментами моніторингу та аналізу даних.	Значний перелік інтеграцій, але є обмежена підтримка для деяких систем.	Інтеграція з багатьма іншими інструментами	Значний перелік інтеграцій, але є обмежена підтримка для деяких систем.
Ціна	175$/місяць	275$/місяць	442$/місяць	510$/місяць

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ШЛЮЗІВ БЕЗПЕКИ ЕЛЕКТРОННОЇ ПОШТИ

Критерії	Cisco Email Security	Proofpoint Email Protection	Barracuda Email Security	Sophos Email Security
Захист від фішингу	Використовує штучний інтелект для виявлення та блокування фішингових атак	Пропонує захист від атак фішингу, виявлення зловмисних посилань.	Включає захист від фішингу та спаму	Забезпечує захист від фішингу та інших загроз
Блокування спаму	Забезпечує фільтрацію спаму та блокування небажаних повідомлень	Пропонує захист від спаму та небажаних повідомлень	Блокує спам та небажані листи	Захищає від спаму та небажаних повідомлень
Виявлення вірусів	Має механізми виявлення та блокування вірусів у електронній пошті	Забезпечує захист від вірусів у пошті	Включає захист від вірусів у електронній пошті	Має захист від вірусів та інших загроз
Штучний інтелект	Використовує механізми штучного інтелекту для аналізу та блокування загроз	Має розвинуті алгоритми для виявлення та блокування загроз	Має певні функції штучного інтелекту для виявлення та блокування загроз	Має інструменти штучного інтелекту для виявлення та блокування загроз
Ціна	1000-2000$	1500-2500$	2,66$/місяць за 1 користувача	55,30$/місяць