МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ВПРОВАДЖЕННЯ ТА СЕРТИФІКАЦІЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗА СТАНДАРТОМ ISO/IEC 27001”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Євгеній КОРНІЄНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Євгеній КОРНІЄНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Корнієнку Євгенію Ігоровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Впровадження та сертифікація системи управління інформаційною безпекою за стандартом ISO/IEC 27001”,
керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій "Про закріплення тем випускних кваліфікаційних робіт та призначення наукових керівників на 2023-2024 н.р. за студентами першого (бакалаврського) рівня вищої освіти". № 36 від 27.02.24

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *система управління інформаційною безпекою організації, міжнародний стандарт ISO/IEC 27001, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати регуляторне середовище в контексті СУІБ.
4.2. Дослідити методику впровадження СУІБ в організації.
4.3. Провести аналіз методики сертифікації СУІБ на відповідність вимогам ISO/IEC 27001.
4.4. Розробити рекомендації щодо вибору доцільної стратегії впровадження СУІБ, досягнення та підтримки сертифікацій СУІБ.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних основ функціонування СУІБ	08.04.2024	
4.	Дослідження методики впровадження СУІБ	22.04.2024	
5.	Аналіз особливостей та підтримки сертифікації СУІБ	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ЕК.	__.06.2024	

Здобувач вищої освіти _____ Євгеній КОРНІЄНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Корнієнко Є.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Впровадження та сертифікація системи управління інформаційною безпекою за стандартом ISO/IEC 27001"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КОРНІЄНКО Євгеній у кваліфікаційній роботі проаналізував регуляторне середовище в контексті СУІБ; дослідив методику впровадження СУІБ в організації; провів аналіз методики сертифікації СУІБ на відповідність вимогам ISO/IEC 27001; розробив рекомендації щодо вибору доцільної стратегії впровадження СУІБ, досягнення та підтримки сертифікацій СУІБ.

КОРНІЄНКО Євгеній показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КОРНІЄНКА Євгенія на оцінку "_____" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Корнієнко Є.І. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КОРНІЄНКА Євгенія
на тему “ Впровадження та сертифікація системи управління інформаційною безпекою за стандартом ISO/IEC 27001”

Актуальність. Інформаційна безпека відіграє рішучу роль у добробуті суспільства й фінансовій безпеці окремих економічних суб’єктів та держави в цілому. Для належного захисту інформації та інформаційних активів організація повинна впровадити та підтримувати ефективну систему управління інформаційною безпекою. Для перевірки її ефективності та правильного використання заходів забезпечення інформаційної безпеки мають проводитися періодичні аудити, які дозволяють визначити поточний стан інформаційної безпеки та виявити потенційні вразливості та реальні недоліки, що можуть призвести до реалізації інцидентів, фінансових, репутаційних втрат, юридичних наслідків тощо. Наразі організації оперують великими обсягами конфіденційної інформації, за захист якої вони несуть відповідальність. З огляду на зазначене тема кваліфікаційної роботи є актуальною і своєчасною.

Позитивні сторони.

1. У роботі детально розглянуто алгоритм впровадження та сертифікації системи управління інформаційною безпекою організації.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: 43 публікації, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо ефективних стратегій впровадження системи управління інформаційною безпекою.

Недоліки.

Доцільно було б більш детально описати заходи, які відбуваються на кожному етапі аудиту СУІБ, із зазначенням технологій, методів та програмних інструментів, які при цьому використовуються.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “_____”, а здобувач КОРНІЄНКО Євгеній заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню впровадженню та сертифікації системи управління інформаційною безпекою за стандартом ISO/IEC 27001. Робота складається зі вступу, трьох розділів, що містять 18 рисунків, висновків і списку використаних джерел із 43 найменування. Загальний обсяг роботи становить 66 аркушів, з яких 5 аркушів займають перелік умовних позначень і скорочень та список використаних джерел.

Метою роботи є проведення аналізу стратегій впровадження, підтримки та сертифікації СУІБ за стандартом ISO/IEC 27001.

Об'єктом дослідження є процес функціонування системи управління інформаційною безпекою організації.

Предмет дослідження – особливості процесів впровадження, підтримки та сертифікації СУІБ за стандартом ISO/IEC 27001.

Методи дослідження. Методологія дослідження базується на комплексному підході, який включає аналіз літературних джерел, нормативних документів, а також практичних кейсів впровадження системи управління інформаційною безпекою за ISO/IEC 27001. Використовуються методи порівняння, системного аналізу, інтерв'ювання експертів та моделювання.

Як результат у роботі досліджено методики впровадження та сертифікації СУІБ на відповідність вимогам ISO/IEC 27001, розроблено рекомендації щодо вибору доцільної стратегії впровадження та підтримки сертифікації СУІБ.

Галузь застосування. Використання отриманих результатів дозволить здійснити обґрунтований вибір стратегії впровадження системи управління інформаційною безпекою та підвищити стан захищеності інформаційних активів організації шляхом ефективного аудиту та сертифікації системи управління інформаційною безпекою.

Ключові слова: СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, УПРАВЛІННЯ РИЗИКАМИ, СЕРТИФІКАЦІЯ, АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ABSTRACT

The qualification work is devoted to the study of the implementation and certification of the information security management system according to the ISO/IEC 27001 standard. The work consists of an introduction, three chapters containing 18 figures, conclusions and a list of 43 references. The total volume of the work is 66 pages, of which 5 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to analyze the strategies for implementing, maintaining and certifying the information security management system according to ISO/IEC 27001.

The object of the study is the process of functioning of an organization's ISMS.

The subject of the study is the peculiarities of the processes of implementation, maintenance and certification of the information security management system according to ISO/IEC 27001.

Research methods. The research methodology is based on an comprehensive approach, which includes an analysis of literary sources, regulatory documents, as well as practical cases of implementing an information security management system according to the ISO/IEC 27001 standard. The methods of comparison, system analysis, expert interviews and modelling are used.

As a result, the study investigates the methods of implementing and certifying ISMS for compliance with the requirements of ISO/IEC 27001, and develops recommendations for choosing an appropriate strategy for implementing and maintaining ISMS certification.

Field of application. The use of the obtained results will allow to make an informed choice of the strategy for implementing the information security management system and improve the security of the organization's information assets through effective audit and certification of the information security management system.

Keywords: INFORMATION SECURITY MANAGEMENT SYSTEM, RISK MANAGEMENT, CERTIFICATION, INFORMATION SECURITY AUDIT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ЗЗІБ	Заходи забезпечення інформаційної безпеки
ІА	Інформаційні активи
ІБ	Інформаційна безпека
ІС	Інформаційна система
ПЗ	Програмне забезпечення
СУІБ	Система управління інформаційною безпекою

ВСТУП

Актуальність теми. В сучасному світі ІБ стає все більш критичною складовою успішного функціонування будь-якої організації. Враховуючи зростаючі загрози з боку кіберзлочинців, важливо забезпечити надійний захист інформаційних активів. Впровадження та сертифікація СУІБ за стандартом ISO/IEC 27001 дозволяє компаніям забезпечити систематичний підхід до управління інформаційними ризиками, що є необхідним для підтримки довіри з боку клієнтів і партнерів.

З огляду на зазначене дослідження стратегій впровадження, підтримки та сертифікації СУІБ є актуальним науковим завданням.

Мета роботи полягає у проведенні аналізу стратегій впровадження, підтримки та сертифікації СУІБ за стандартом ISO/IEC 27001.

Об'єкт дослідження – процес функціонування СУІБ організації.

Предмет дослідження – особливості процесів впровадження, підтримки та сертифікації СУІБ за стандартом ISO/IEC 27001.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати регуляторне середовище в контексті СУІБ.
2. Дослідити методику впровадження СУІБ в організації.
3. Провести аналіз методики сертифікації СУІБ на відповідність вимогам ISO/IEC 27001.
4. Розробити рекомендації щодо вибору доцільної стратегії впровадження СУІБ, досягнення та підтримки сертифікації СУІБ.

Методи дослідження. Методологія дослідження базується на комплексному підході, який включає аналіз літературних джерел, нормативних документів, а також практичних кейсів впровадження СУІБ за стандартом ISO/IEC 27001. Використовуються методи порівняння, системного аналізу, інтерв'ювання експертів та моделювання.

Практичне значення одержаних результатів. Використання отриманих результатів дозволить здійснити обґрунтований вибір стратегії впровадження

системи управління інформаційною безпекою та підвищити стан захищеності інформаційних активів організації шляхом ефективного аудиту та сертифікації системи управління інформаційною безпекою. До того ж, результати роботи можуть бути використані для допомоги у підготовці до проведення внутрішніх аудитів СУІБ та незалежної сертифікації.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ СУІБ

Для всебічного розкриття теми кваліфікаційної роботи необхідно дослідити ключові терміни, принципи та особливості СУІБ, проаналізувати регуляторне середовище в контексті СУІБ, зокрема, вимоги стандарту ISO/IEC 27001.

1.1 Визначення фундаментальних принципів СУІБ

Інформація є ключовим ресурсом організацій та важливим бізнес-активом у сучасному ІТ-світі. Доступ до якісної, повної, точної та актуальної інформації є необхідним для підтримки процесу прийняття управлінських рішень, що веде до обґрунтованих висновків. Тому безпека ресурсів ІС має надзвичайно важливе значення для забезпечення належного захисту. Регламенти та політики конфіденційності і захисту даних накладають на організації певні зобов’язання. Організаціям необхідно використовувати СУІБ для ефективного управління своїми ІА. СУІБ складається з наборів політик, створених організацією для визначення, створення, розробки та підтримки безпеки на основі апаратних і програмних ресурсів, а також аудиту їх виконання.

Організації іноді витрачають значні кошти на брандмауери, проксі-сервери, антивіруси, механізми виявлення вторгнень, цифрові підписи, спеціальні мережеві пристрої та протоколи, вважаючи, що безпеку інформації можна забезпечити шляхом придбання цих технологій. Це є помилковим уявленням, оскільки управління безпекою – це більше про керування наскрізною системою, а не просто встановлення технічних рішень. Як і будь-яка інша повноцінна система, ця система має багато компонентів, включаючи людей, політику, процедури, процеси, стандарти та технології [1].

ІБ є критично важливою складовою будь-якої сучасної організації. СУІБ є комплексною структурою, яка охоплює організаційні, технічні та людські аспекти захисту інформації. У сучасному світі інформація стала важливим

ресурсом для будь-якої організації, незалежно від її розміру чи галузі діяльності. Забезпечення безпеки цього ресурсу є критичним завданням, яке впливає на стабільність, ефективність та конкурентоспроможність організації.

СУІБ охоплює сукупність політик, процесів та технічних засобів, що використовуються для захисту інформації від загроз. Мета СУІБ полягає у забезпеченні трьох основних принципів ІБ: конфіденційності, цілісності та доступності (табл. 1.1).

Таблиця 1.1.

Тріада ІБ [2]

Властивість інформації	**Визначення**
Конфіденційність	Забезпечення доступу до інформації тільки для уповноважених осіб. Це досягається через впровадження контрольних механізмів доступу, шифрування даних та інших засобів захисту.
Цілісність	Гарантія того, що інформація не була змінена або знищена без відповідного дозволу. Це забезпечується через використання цифрових підписів, контрольних сум, журналів аудиту та інших технологій.
Доступність	Забезпечення своєчасного і безперебійного доступу до інформації для уповноважених користувачів. Це досягається через резервне копіювання, відновлення після збоїв, дублювання критичних систем і інші методи.

Компоненти СУІБ включають в себе наступні складові: політики та процедури, управління ризиками, технічні засоби захисту, навчання та підвищення обізнаності, моніторинг та аналіз безпеки. Детальний опис компонентів СУІБ наведений на рис. А.1.

Для процесів СУІБ застосовується модель PDCA (рис. 1.1), яка складається з 4 ітеративних процесів:

- планування – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- виконання – етап реалізації та впровадження відповідних заходів;
- перевірка – фаза оцінки ефективності та продуктивності СУІБ;
- вплив – виконання превентивних і коригуючих дій.

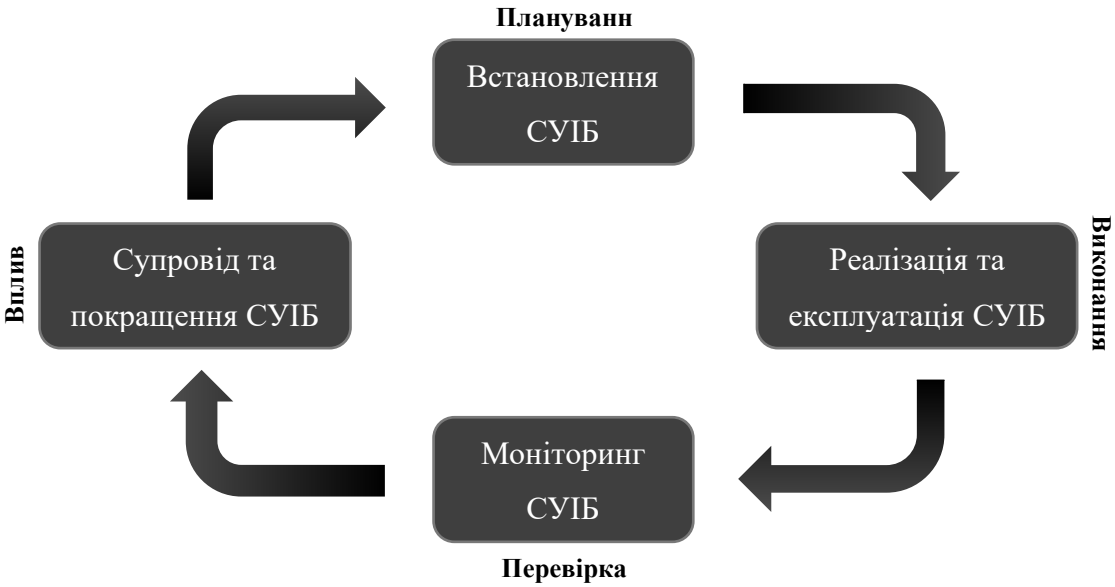

Рис. 1.1. Модель PDCA для СУІБ

Впровадження СУІБ є комплексним процесом, який включає декілька етапів, зокрема: [3]

1. Підготовчий етап;
2. Розробка політик та процедур;
3. Впровадження технічних засобів захисту;
4. Навчання персоналу;
5. Моніторинг і вдосконалення.

Підготовчий етап передбачає визначення цілей і завдань СУІБ і проведення ретельного аналізу поточного стану ІБ організації. Розробка політик і процедур передбачає розробку політик ІБ і встановлення протоколів для управління доступом, реагування на інциденти та інших важливих процедур. Реалізація заходів технічного захисту включає встановлення брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS), антивірусного програмного забезпечення та інших засобів безпеки. Проведення тренінгів та освітніх програм є важливою складовою навчання співробітників. Важливо постійно контролювати системи безпеки, проводити регулярні аудити та оновлювати політики та процедури [4].

Впровадження ефективної СУІБ в організації пропонує численні переваги,

такі як зниження ризику втрати інформації завдяки розгортанню надійних заходів безпеки, забезпечення дотримання нормативних вимог, що допомагає організації дотримуватися стандартів і правил у сфері ІБ, а також зниження ймовірності інцидентів, які можуть зашкодити репутації організації. Крім того, він підвищує довіру клієнтів і партнерів, демонструючи серйозну відданість захисту інформації.

Підсумовуючи, СУІБ є критично важливим елементом для успішної роботи будь-якої сучасної організації, забезпечуючи надійний захист її інформаційних активів і сприяючи стабільному розвитку та конкурентоспроможності на ринку [5].

1.2 Аналіз регуляторного середовища в контексті СУІБ

Аналіз регуляторного середовища в контексті СУІБ є важливою складовою процесу забезпечення ІБ в організації. Регуляторне середовище включає нормативні акти, стандарти, правила та вимоги, які встановлюють обов'язки організацій щодо захисту інформації. Дотримання цих вимог є критичним для забезпечення правової відповідності, уникнення штрафів та збереження довіри клієнтів та партнерів.

Слід розглянути детальніше ключові та найпопулярніші стандарти, які допомагають встановлювати обов’язки організацій щодо захисту інформації.

Основним стандартом в цій галузі є стандарт ISO/IEC 27001. Він є міжнародним стандартом, який визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення СУІБ. Він надає систематизований підхід до управління ІБ, зосереджуючись на управлінні ризиками та забезпеченні безпеки інформаційних активів. Стандарт охоплює різні аспекти, включаючи політики безпеки, організаційні структури, управління активами, управління доступом, криптографію, фізичну безпеку, безпеку персоналу, управління інцидентами та відповідність нормативним вимогам. Стандарт має значні переваги, порівнюючи з іншими, схожими стандартами (рис. А.2).

Також, варто взяти до уваги стандарт ISO/IEC 27002. Він є доповненням до ISO/IEC 27001 і надає практичні рекомендації щодо впровадження засобів управління ІБ, описаних у стандарті ISO/IEC 27001. Він охоплює найкращі практики для різних аспектів ІБ, включаючи політики, управління ризиками, навчання персоналу та технічні засоби захисту. Цей стандарт встановлює настанови та загальні принципи щодо започаткування, впровадження, підтримки та вдосконалення управління ІБ в організації. Цілі, окреслені в цьому стандарті, надають основні настанови щодо загальноприйнятих цілей управління ІБ. Цілі заходів забезпечення ІБ (ЗЗІБ) цього стандарту призначені для впровадження з метою задоволення вимог, ідентифікованих оцінкою ризику. Цей стандарт може слугувати практичною настановою для розвитку стандартів безпеки в організації та практики ефективного управління безпекою, і для допомоги в побудові конфіденційності в діяльності організації [6].

Основні відмінності між стандартами ISO/IEC 27001 та ISO/IEC 27002 зображені на рис. 1.2.

Рис. 1.2. Відмінності між стандартами ISO/IEC 27001 та ISO/IEC 27002

Окремо слід взяти до уваги стандарт NIST SP 800-53. Він представляє собою спеціальну публікацію від Національного інституту стандартів і технологій (NIST) США надає набір ЗЗІБ для захисту інформаційних систем (ІС) федеральних установ США. Вона включає вимоги щодо безпеки, конфіденційності та забезпечення доступу до ІС. NIST SP 800-53 охоплює широкий спектр ЗЗІБ, включаючи управління ризиками, захист систем та комунікацій, управління ідентифікацією та автентифікацією, а також управління інцидентами. Зокрема, спеціальна публікація NIST 800-53 охоплює кроки в структурі управління ризиками, які стосуються вибору ЗЗІБ для федеральних ІС відповідно до вимог безпеки Федерального стандарту обробки інформації (FIPS) 200. Це включає вибір початкового набору базових ЗЗІБ на основі аналізу найгіршого сценарію впливу FIPS 199, адаптація базових ЗЗІБ та доповнення ЗЗІБ на основі організаційної оцінки ризику. Правила безпеки охоплюють 20 сфер, включаючи контроль доступу, реагування на інциденти, безперервність бізнесу та аварійне відновлення [7].

Ключовою частиною процесу оцінки та авторизації (раніше – сертифікації та акредитації) для федеральних інформаційних систем є вибір і впровадження підмножини ЗЗІБ (запобіжних заходів) із Каталогу контролю безпеки (NIST 800-53, Додаток F). Ці ЗЗІБ є управлінськими, операційними та технічними заходами (або контрзаходами), призначеними для інформаційної системи для захисту конфіденційності, цілісності та доступності системи та її інформації. Щоб запровадити необхідні ЗЗІБ, агентства повинні спочатку визначити категорію безпеки своїх інформаційних систем відповідно до положень FIPS 199 «Стандарти категоризації безпеки федеральної інформації та інформаційних систем». Категорія безпеки інформаційної системи (низька, помірна або висока) визначає базовий набір ЗЗІБ, які необхідно впроваджувати та контролювати. Агентства мають можливість налаштовувати ці елементи керування ЗЗІБ та пристосовувати їх до цілей своєї організації чи середовища.

Незважаючи на те, що будь-яка приватна організація може прийняти використання NIST 800-53 як керівну структуру для своєї практики безпеки, усі

федеральні урядові установи США та підрядники зобов'язані дотримуватися цієї структури, щоб захистити свої важливі дані. План дій щодо впровадження стандарту NIST SP 800-53 зображено на рис. А.3. [8].

Говорячи про передові стандарти ІБ, варто згадати також про COBIT (Control Objectives for Information and Related Technology). Це відкритий IT-стандарт, який в свою чергу містить ряд документів зі стандартами щодо оптимізації управління IT: аудитом IT та IT-безпекою. Він був створений Асоціацією з аудиту та контролю інформаційних система (ISACA) спільно із Інститутом управлінням IT (ITGI). Стандарт сприяє чіткішій координації дій IT-департаменту та керівництва компанії, об'єднує в собі ряд інших стандартів, що дозволяє на високому рівні якості отримувати інформацію про стан IT та управляти цілями і задачами IT.

Завдання COBIT полягає в ліквідації розриву між керівництвом компанії з їх баченням бізнес-цілей і IT-департаментом, що здійснює підтримку інформаційної інфраструктури, яка повинна сприяти досягненню цих цілей. В COBIT детально описані принципи управління, об'єкти управління, чітко визначені всі IT-процеси (завдання), що протікають в компанії, і вимоги до них, описаний можливий інструментарій (практики) для їх реалізації. В описі IT-процесів також приведені рекомендації по управлінню IT-безпекою [9].

Ключові поняття стандарту COBIT зображені на рис. 1.3.

Рис. 1.3. Ключові поняття стандарту COBIT 5

Окрім стандартів, є необхідним дотримання регуляторних вимог в різних галузях, таких як фінансовий сектор, охорона здоров’я, енергетичний сектор.

Для фінансового сектору ключовими є базельські принципи – це принципи Базельського комітету з банківського нагляду спрямовані на підвищення стабільності та безпеки фінансових установ. Вони включають вимоги до управління ризиками, в тому числі й інформаційними. Варто також взяти до уваги PCI DSS – це стандарт безпеки даних індустрії платіжних карток (Payment Card Industry Data Security Standard), який встановлює вимоги до захисту даних платіжних карток і використовується для забезпечення безпеки транзакцій у фінансовому секторі [10].

Розглядаючи сектор охорони здоров’я, варто взяти до уваги HIPAA. Це закон про портативнічсть і підзвітність медичного страхування (Health Insurance Portability and Accountability Act), який вимагає захисту конфіденційності та безпеки медичної інформації. Організації, що обробляють медичні дані, зобов'язані дотримуватись суворих вимог щодо захисту цієї інформації [11].

Обов’язковим є дотримання національних законодавчих актів, як закон України, так і законів та регламентів ЄС.

Зокрема, це закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Цей закон встановлює основні принципи та вимоги до захисту інформації в інформаційно-телекомунікаційних системах, що використовуються на території України. Він визначає обов'язки суб'єктів у сфері захисту інформації та передбачає відповідальність за порушення цих вимог [12].

Розглядаючи закони ЄС, варто взяти до уваги GDPR. GDPR (Загальний регламент про захист даних) – це регламент Європейського Союзу, що встановлює вимоги до захисту персональних даних. GDPR впливає на всі організації, які обробляють персональні дані громадян ЄС, незалежно від їх місця розташування. Він передбачає суворі вимоги до забезпечення конфіденційності, прозорості та права суб'єктів даних [13].

Окрім нього, варто також виділи Cybersecurity Act. Він представляє собою закон ЄС, спрямований на підвищення рівня кібербезпеки в країнах-членах ЄС.

Він встановлює вимоги до забезпечення безпеки мереж та інформаційних систем, включаючи критичну інфраструктуру. Європейський акт про кібербезпеку (Регламент (ЄС) 2019/881) набув чинності 27 червня 2019 року. Основні елементи цього Регламенту включають постійний мандат Агентства Європейського Союзу з кібербезпеки (ENISA), що супроводжується запровадженням єдиного Європейського рамки сертифікації продуктів, послуг і процесів ІКТ. Вони мають бути сертифіковані відповідно до різних критеріїв і мають бути призначені попередньо визначені рівні безпеки «низький», «середній» і «високий» [14].

Після публікації запропонованого Регламенту у вересні 2017 року Федеральне відомство з інформаційної безпеки (BSI) надало ґрунтовну підтримку переговорам і консультаціям, проведеним у редакційних комітетах. Ці внески допомогли забезпечити перенесення успішних існуючих систем сертифікації в новий Регламент. Країни-члени ЄС також продовжують відігравати ключову роль у сертифікації додатків з високим рівнем безпеки.

Рамки сертифікації, викладені в статті III Регламенту, також суттєво змінюють процедуру розробки схем сертифікації та видачі сертифікатів у межах Європейського Союзу. Будучи членом таких організацій, як Європейська група сертифікації кібербезпеки (ECCG), BSI робить значний внесок у нові процеси, створені Регламентом. Як і раніше, BSI також продовжує тісно співпрацювати з європейськими партнерами у сфері сертифікації кібербезпеки.

Організації повинні дотримуватися регуляторних вимог та стандартів для забезпечення належного рівня ІБ. Тому аналіз регуляторного середовища є невід'ємною частиною процесу управління ІБ. Відповідність нормативним вимогам та стандартам забезпечує не тільки захист інформаційних активів організації, але й підвищує її репутацію, довіру з боку клієнтів та партнерів, а також знижує ризики фінансових втрат та юридичних наслідків. Організації повинні постійно слідкувати за змінами в регуляторному середовищі та адаптувати свої СУІБ відповідно до нових вимог і стандартів. Ключові вимоги, яких повинні дотримуватися організації, наведені в табл. 1.2.

Таблиця 1.2.

Ключові вимоги забезпечення належного рівня ІБ [15]

Вимога	Призначення
Проводити регулярні аудити та оцінки безпеки	Внутрішні та зовнішні аудити допомагають виявити слабкі місця та відповідність встановленим вимогам.
Розробляти плани управління інцидентами	План управління інцидентами повинен включати процедури виявлення, аналізу, реагування та відновлення після інцидентів безпеки.
Підвищувати обізнаність персоналу	Проведення навчальних програм та тренінгів для підвищення рівня знань працівників щодо ІБ та регуляторним вимогам.
Впроваджувати політики безпеки	Створення та впровадження політик, що регулюють доступ до інформації, використання ресурсів та інші аспекти ІБ
Виконувати моніторинг та аналіз безпеки	Постійний моніторинг систем та аналіз журналів подій для своєчасного виявлення та реагування на загрози.
Забезпечувати фізичну безпеку	Впровадження заходів фізичної безпеки, таких як контроль доступу до приміщень, системи відеоспостереження та сигналізації.
Управляти доступом до інформації	Впровадження механізмів управління доступом, таких як системи автентифікації та авторизації, контроль прав доступу до інформаційних ресурсів.
Виконувати резервне копіювання даних	Регулярне створення резервних копій критичних даних та перевірка можливості їх відновлення.
Оцінювати та управляти ризиками	Проведення оцінки ризиків інформаційної безпеки та впровадження заходів для їх зниження.
Підтримувати відповідність законодавству та стандартам	Забезпечення дотримання вимог законодавства, нормативних актів та стандартів, що регулюють інформаційну безпеку.

1.3 Аналіз ключових принципів та вимог стандарту ISO/IEC 27001

ISO/IEC 27001 є міжнародним стандартом, що встановлює вимоги до СУІБ. Він надає систематизований підхід до управління конфіденційністю, цілісністю та доступністю інформаційних активів, з акцентом на управління ризиками. Стандарт застосовується до всіх типів організацій, незалежно від їх розміру, галузі чи географічного розташування.

Ключові принципи ISO/IEC 27001 наведені в табл. 1.3.

Таблиця 1.3.

Ключові принципи ISO/IEC 27001 [16]

Вимоги	Призначення
Систематизований підхід до управління ІБ	Стандарт визначає процеси, що забезпечують постійний моніторинг, аналіз, впровадження та вдосконалення заходів безпеки
Управління ризиками	Визначення, оцінка та управління ризиками є основними складовими ISO/IEC 27001. Стандарт вимагає ідентифікації інформаційних ризиків та впровадження засобів контролю для їх мінімізації
Залучення керівництва	Важливою умовою успішного впровадження СУІБ є активна участь керівництва організації, яке має забезпечити необхідні ресурси та підтримку
Контекст організації	Стандарт вимагає врахування внутрішнього та зовнішнього контексту організації, включаючи законодавчі, регуляторні та інші вимоги.
Підхід на основі процесів	ISO/IEC 27001 передбачає використання процесного підходу для управління та вдосконалення СУІБ
Постійне вдосконалення	Стандарт акцентує увагу на необхідності постійного вдосконалення СУІБ через регулярний моніторинг, аналіз та коригувальні дії

Основні вимоги та можливості стандарту ISO/IEC 27001 зображені на рис. 1.4.

Рис. 1.4. Вимоги та можливості стандарту ISO/IEC 27001

Окремо варто розглянути та виділити важливі вимоги, серед них: контекст організації, лідерство, планування, підтримка, операційна діяльність, оцінка результативності та вдосконалення.

В контексті організації ключову роль грають визначення зовнішніх і

внутрішніх факторів, що можуть вплинути на здатність організації досягати цілей ІБ, а також визначення зацікавлених сторін та їх вимог до ІБ. Лідерство має на меті відповідальність вищого керівництва за встановлення політики ІБ, забезпечення ресурсами та призначення відповідальних осіб, активну участь керівництва в підтримці та вдосконаленні СУІБ. Важливо планувати та визначати цілі ІБ та планів їх досягнення, враховуючи ризики та можливості для забезпечення результативності СУІБ. Варто забезпечити наявність необхідних ресурсів, компетенцій та обізнаності для впровадження та підтримки СУІБ та документування процесів і процедур, пов'язаних з ІБ. Сюди ж відноситься впровадження ЗЗІБ для управління ідентифікованими ризиками, планування, впровадження та контроль операційних процесів ІБ. Не обійдеться без оцінки результативності, а саме моніторинг, вимірювання, аналіз та оцінка результативності СУІБ. Заключним етапом є покращення результативності, а саме виявлення невідповідності та вжиття коригувальних дій, постійне вдосконалення СУІБ.

Розглядаючи детально стандарт ISO/IEC 27001, варто виділити Додаток А, який містить цей стандарт, він включає набір ЗЗІБ, згрупованих у 4 розділи, а саме: організаційні заходи (А.5), людські заходи (А.6), фізичні заходи (А.7) та технологічні заходи (А.8).

Деякі з них наведені в табл. 1.4.

Таблиця 1.4.

Заходи безпеки Додатку А стандарту ISO/IEC 27001:2022 [16]

Номер	**Положення**	**Опис**
А.5.1	Політики ІБ	Політика ІБ та тематичні політики повинні бути визначені, схвалені керівництвом, опубліковані, доведені до відома та переглянуті.
А.5.2	Обов'язки у сфері ІБ	Обов'язки у сфері ІБ повинні бути визначені та розподілені відповідно до потреб організації.
А.7.2	Фізичний вхід	Безпечні зони повинні бути захищені відповідними контрольно-пропускними пунктами і точками доступу.

Продовження таблиці 1.4.

Номер	Положення	Опис
A.7.8	Розміщення і захист обладнання	Обладнання повинно бути розміщене і захищене належним чином.
A.7.10	Носії інформації	Управління носіями інформації повинно здійснюватися протягом їх життєвого циклу – від придбання до використання, транспортування та утилізації.
A.8.5	Безпечна автентифікація	Технології та процедури безпечної автентифікації повинні бути реалізовані на основі обмежень доступу до інформації та політики управління доступом.
A.8.13	Резервне копіювання інформації	Резервні копії інформації, ПЗ та систем повинні підтримуватися та регулярно тестуватися у відповідності з політикою резервного копіювання.
A.8.26	Вимоги безпеки додатків	Вимоги до ІБ повинні бути визначені, задокументовані та затверджені під час розробки або придбання додатків.
A.5.8	ІБ в управлінні проєктами	ІБ повинна бути інтегрована в управління проєктами.
A.5.14	Передача інформації	Правила передачі інформації, процедури або угоди повинні діяти для всіх типів засобів передачі всередині організації та між організацією та іншими сторонами.
A.6.2	Умови працевлаштування	В трудових договорах повинні бути вказані обов'язки персоналу та організації щодо забезпечення ІБ.
A.6.7	Віддалена робота	Заходи безпеки повинні бути реалізовані, коли персонал працює віддалено, для захисту інформації, до якої здійснюється доступ, яка обробляється або зберігається за межами організації.

Стандарт ISO/IEC 27001 надає комплексний підхід до управління ІБ, враховуючи всі аспекти, від політики та планування до операційної діяльності та покращення. Впровадження цього стандарту допомагає організаціям ефективно захищати свої інформаційні активи, мінімізувати ризики та забезпечувати відповідність законодавчим та нормативним вимогам.

Висновки до розділу 1

У розділі розглянуто теоретичні аспекти СУІБ, що є важливими для розуміння основних принципів та вимог, які лежать в основі забезпечення ІБ в організаціях.

Огляд основних концепцій ІБ дозволив зрозуміти сутність і значущість

захисту конфіденційності, цілісності та доступності інформації. ІБ включає різноманітні заходи та процеси, що забезпечують захист від несанкціонованого доступу, порушень точності даних та забезпечення доступності інформації у потрібний час.

В результаті аналізу розвитку стандартів управління ІБ було виявлено, що розвиток цих стандартів був обумовлений зростаючими потребами організацій у систематизованому підході до управління ІБ. Від британського стандарту BS 7799:1995 до міжнародного стандарту ISO/IEC 27001:2022, процес стандартизації сприяв поширенню найкращих практик управління ІБ на глобальному рівні.

Було проаналізовано основні положення стандарту ISO/IEC 27001, які включають широкий спектр заходів, від політики ІБ до управління інцидентами та забезпечення безперервності бізнесу. Ці положення визначають основні напрями і методи, які організації можуть використовувати для забезпечення ефективного управління ІБ.

Загалом, теоретичні аспекти СУІБ, розглянуті у розділі, забезпечують ґрунтовну основу для подальшого дослідження практичних аспектів впровадження та сертифікації СУІБ за стандартом ISO/IEC 27001. Вони демонструють важливість комплексного підходу до управління ІБ , що включає не лише технічні, але й організаційні та людські фактори.

Розділ 2 ДОСЛІДЖЕННЯ МЕТОДИКИ ВПРОВАДЖЕННЯ СУІБ

Для досягнення мети кваліфікаційної роботи необхідно проаналізувати особливості та кращі практики процесу впровадження СУІБ та визначити ключові особливості управління ризиками ІБ як важливого фактору ефективного функціонування СУІБ.

2.1 Аналіз особливостей процесів планування та ініціювання впровадження СУІБ

Процес планування та ініціювання впровадження СУІБ є критично важливим етапом, який закладає основу для успішного функціонування всієї системи. Цей процес включає визначення цілей, аналіз поточного стану інформаційної безпеки, розробку стратегії впровадження та залучення керівництва і співробітників до роботи над забезпеченням безпеки інформаційних активів. Етапи ефективного планування впровадження СУІБ зображені на рис. 2.1.

Рис. 2.1. Етапи ефективного планування впровадження СУІБ

Перш за все, варто провести визначення цілей, які повинна досягнути СУІБ, таких як забезпечення конфіденційності, цілісності та доступності ІА, відповідність законодавчим та нормативним вимогам, підвищення довіри клієнтів та партнерів. Важливо визначити обсяг впровадження меж СУІБ, тобто які підрозділи, процеси та ІА будуть включені в систему. Це може бути вся організація або її окремі частини.

Аналіз поточного стану ІБ включає в себе оцінку поточних практик, аналіз існуючих політик, процедур та засобів захисту інформації, виявлення сильних та слабких сторін поточної системи безпеки, а також ідентифікація та оцінка ризиків, пов'язаних з ІА організації. Це включає аналіз загроз, вразливостей та потенційних наслідків реалізації ризиків.

Впровадження СУІБ має на меті вибір методології та підходів до впровадження СУІБ, таких як використання міжнародних стандартів, в даному випадку ISO/IEC 27001, або внутрішніх розробок. Розробка детального плану впровадження має включати етапи, терміни, ресурси та відповідальних осіб. План повинен враховувати всі необхідні заходи для досягнення цілей СУІБ (табл. 2.1).

Таблиця 2.1.

План заходів для досягнення цілей СУІБ [17]

Заходи	**Дії**
Графік робіт	Встановлення термінів для кожного етапу впровадження, від початкової оцінки до повної інтеграції СУІБ в організацію.
Розподіл завдань	Чітке визначення відповідальності за кожен етап та завдання, призначення відповідальних осіб.
Критерії успіху	Визначення чітких критеріїв, за якими буде оцінюватись успіх впровадження кожного етапу проекту.
Ризики проекту	Ідентифікація можливих ризиків під час впровадження та розробка планів їхнього управління.

Забезпечення та залучення підтримки з боку вищого керівництва організації буде грати ключову роль, оскільки керівники повинні розуміти важливість СУІБ і бути готовим надавати необхідні ресурси та інформувати всі зацікавлені сторін про цілі, обсяги та плани впровадження СУІБ. Це включає

внутрішні комунікації зі співробітниками, а також зовнішні комунікації з клієнтами, партнерами та регуляторними органами.

Ініціювання провадження СУІБ включає в себе певні процеси, такі як формування команди проекту, розробку політики ІБ, ідентифікацію ІА, оцінку ризиків, розробку плану управління ризиками, навчання та підвищення обізнаності персоналу.

Для успішного впровадження СУІБ необхідно створити команду проекту, яка буде відповідати за виконання всіх завдань. Основні ролі, які можуть включати в команді, зазначені на рис. 2.2.

Рис. 2.2. Основні ролі команди проекту впровадження СУІБ [18]

Детальний огляд кожної ролі та визначення їх обов’язків зазначено нижче в табл. 2.2.

Таблиця 2.2.

Ролі та обов’язки команди проєкту [18]

Роль	Обов’язки
Керівник проєкту	Відповідальний за загальну координацію проєкту, управління ресурсами та звітність перед керівництвом
Фахівець з ІБ	Здійснює технічний нагляд за впровадженням СУІБ, розробляє і впроваджує заходи безпеки
Юридичний консультант	Забезпечує відповідність правовим вимогам та рекомендаціям
ІТ-адміністратори	Відповідають за технічну інфраструктуру, включаючи мережеву безпеку, захист даних і управління доступом
Представники бізнес-підрозділів	Забезпечують врахування вимог і потреб різних підрозділів організації

Окрім цього, впровадження СУІБ вимагає відповідного фінансування. Бюджет має включати такі основні моменти, як:

1. Витрати на навчання персоналу;
2. Придбання обладнання та програмного забезпечення;
3. Консультаційні послуги;
4. Інші витрати.

Детальний приклад розподілення фінансування наведено в табл. 2.3.

Таблиця 2.3.

Розподіл витрат при впровадженні СУІБ [19]

Об’єкт фінансування	Витрати
Навчання персоналу	Проведення тренінгів і семінарів для підвищення рівня обізнаності співробітників щодо ІБ.
Придбання обладнання	Закупівля необхідних засобів захисту інформації, таких як міжмережеві екрани, системи виявлення та запобігання вторгнень, засоби шифрування.
Консультаційні послуги	Залучення зовнішніх експертів для проведення аудиту, оцінки ризиків та розробки стратегії впровадження.
Інші витрати	Витрати на сертифікацію, оновлення нормативної документації та управління проєктом.

Ефективна комунікація між усіма зацікавленими сторонами, включаючи керівництво, відділ ІБ, ІТ-відділ та інші підрозділи, є необхідною складовою успішного впровадження СУІБ. Така комунікація забезпечує своєчасний обмін інформацією про загрози, вразливості та інциденти, що дозволяє миттєво

реагувати на ризики. Крім того, механізми для постійного вимірювання та оцінки ефективності заходів з ІБ допомагають підтримувати високий рівень безпеки в організації, забезпечуючи відповідність вимогам стандарту ISO/IEC 27001 та покращуючи загальну ІБ. Приклад ефективної комунікації наведено на рис. 2.3.

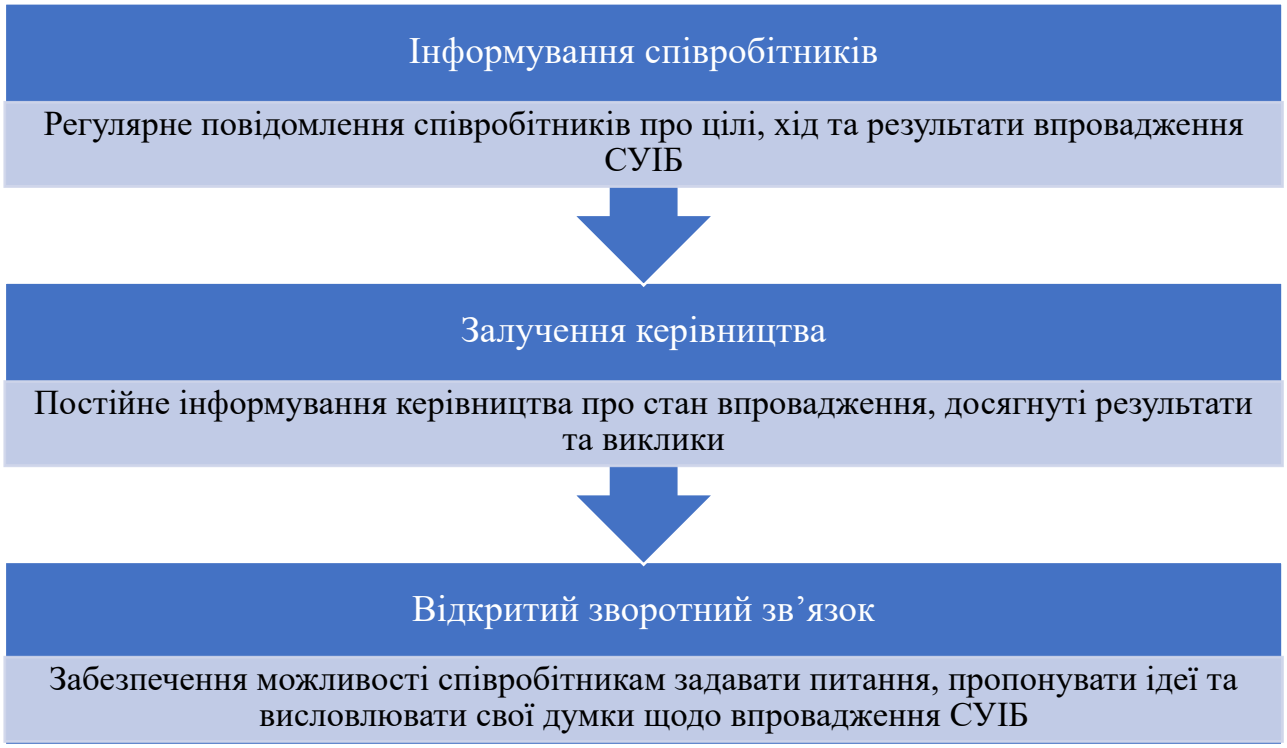

Рис. 2.3. Приклад ефективної комунікації на підприємстві

Оцінка ефективності заходів з ІБ є критично важливим аспектом для забезпечення їхньої дієвості та відповідності змінним умовам. Вимірювання та оцінка включають регулярне відстеження прогресу впровадження заходів, аналіз результатів, проведення внутрішніх та зовнішніх аудитів, а також впровадження коригувальних дій за потреби. Етапи вимірювання та оцінки ефективності заходів наведено в табл. 2.4.

Таблиця 2.4.

Етапи вимірювання та оцінки ефективності заходів з ІБ [20]

Етап	Оцінка ефективності
Моніторинг виконання плану	Регулярне відстеження прогресу щодо виконання плану впровадження, виявлення відхилень та коригування дій
Оцінка результативності	Використання встановлених критеріїв для оцінки ефективності заходів з ІБ.
Періодичні аудити	Проведення внутрішніх та зовнішніх аудитів для оцінки відповідності СУІБ вимогам стандарту ISO/IEC 27001.

Під час планування та ініціювання впровадження СУІБ в організації можуть виникати різного типу виклики та ризики. Приклади деяких викликів наведені на рис. 2.4.

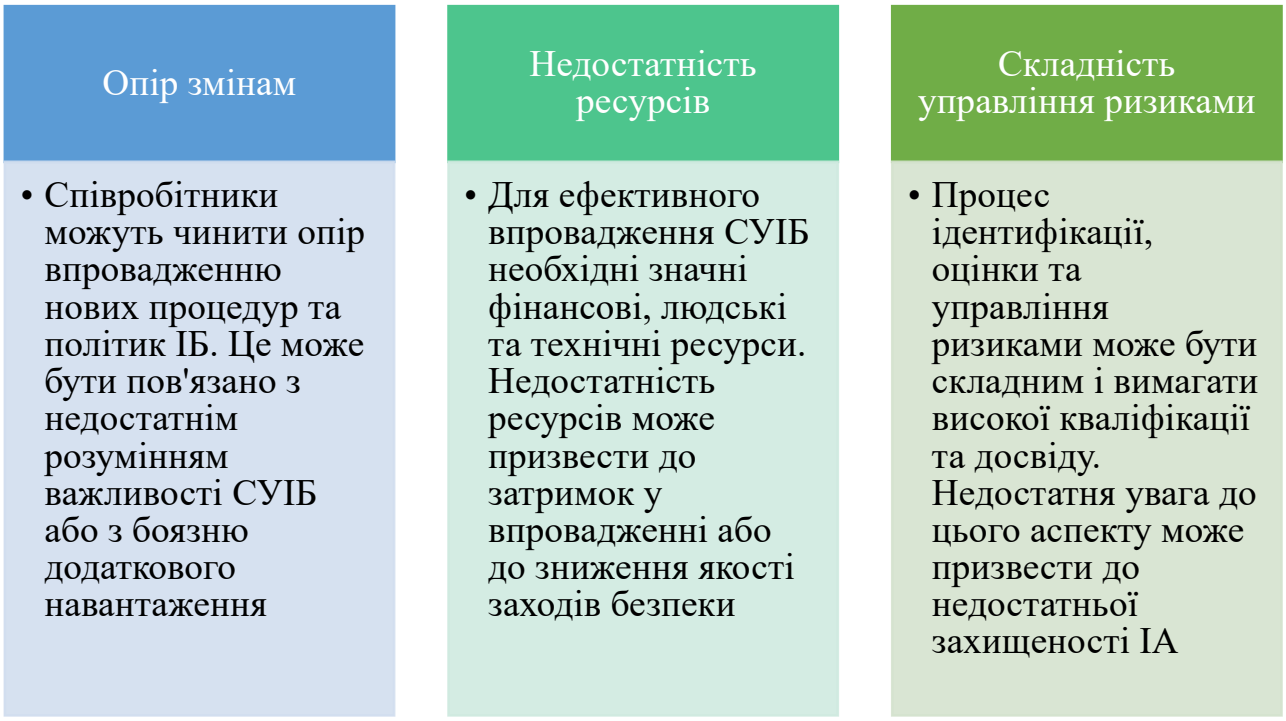

Рис. 2.4. Виклики при впровадженні СУІБ

Обов’язкова документація СУІБ є важливою складовою для забезпечення належного функціонування системи та відповідності вимогам стандарту ISO/IEC 27001. До такої документації відносяться: політика ІБ, оцінка ризиків, SoA (Statement of Applicability), план управління ризиками, процедури управління (інцидентами, доступом, активами), BCP (Business continuity planning), внутрішні

аудити та звіти, навчальні матеріали та програми підвищення обізнаності. У табл. 2.5 наведені детальні описи кожної з документацій, їхні зміст та мету.

Таблиця 2.5.

Опис документації стандарту ISO/IEC 27001 [21]

Документація	**Зміст**	**Мета**
Політики ІБ	Загальні принципи, цілі та підходи до управління ІБ.	Встановити єдині правила для захисту ІА організації.
Оцінка ризиків	Процес ідентифікації, оцінки та управління ризиками ІБ.	Виявлення та мінімізація потенційних загроз для ІА.
SoA	Перелік заходів контролю та обґрунтування їх вибору або відмови від них.	Забезпечити прозорість у виборі заходів контролю.
План управління ризиками	Заходи для управління ідентифікованими ризиками, включаючи терміни та відповідальних осіб.	Ефективне управління ризиками ІБ та їх мінімізація.
Процедура управління інцидентами	Інструкції щодо виявлення, аналізу, реагування та усунення інцидентів безпеки.	Забезпечити швидке та ефективне реагування на інциденти.
Процедура управління доступом	Правила та процедури надання, контролю та відкликання доступу до ІС та даних.	Захист конфіденційності, цілісності та доступності інформаційних активів.
Процедура управління активами	Процеси ідентифікації, класифікації, інвентаризації та управління ІА.	Ефективне управління ІА та зниження ризиків втрати або пошкодження даних.
BCP	Заходи та процедури для забезпечення безперервності бізнес-процесів в умовах інцидентів.	Мінімізувати перерви у бізнес-процесах та забезпечити їх безперервність.
Внутрішні аудити та звіти	Процедури проведення внутрішніх аудитів, включаючи плани, методологію, результати та коригувальні дії	Постійний моніторинг та вдосконалення СУІБ
Навчальні матеріали та програми підвищення обізнаності	Програми навчання та підвищення обізнаності персоналу з питань ІБ	Підвищення обізнаності співробітників та їх відповідальності за захист ІА

Ведення необхідної документації має свої певні вимоги. Вона повинна відображати поточний стан ІБ та враховувати останні зміни. Документи повинні бути доступні для всіх співробітників, які потребують їх для виконання своїх обов’язків. Необхідно забезпечити захист документації, що містить чутливу

інформацію. Обов’язковим є призначення відповідальних осіб за розробку, затвердження, оновлення та зберігання документації, забезпечення належного зберігання архівних версій матеріалів.

Документація є основою для ефективного функціонування СУІБ. Вона систематизує процеси, підвищує прозорість та обізнаність співробітників, допомагає дотримуватися нормативних вимог і стандартів, а також сприяє підвищенню рівня ІБ в організації. Вимоги стандарту ISO 27001 включають створення та підтримку документації, яка відображає політики, процедури, плани управління ризиками та інші ключові аспекти СУІБ, що забезпечує відповідність нормативним вимогам та ефективне управління ІБ [22].

2.2 Дослідження кращих практик моніторингу та вдосконалення СУІБ

Моніторинг та вдосконалення СУІБ є критично важливим для забезпечення її ефективності та відповідності змінним умовам зовнішнього та внутрішнього середовища організації. У цьому розділі досліджені кращі практики, які забезпечують постійне покращення СУІБ та допомагають організаціям швидко реагувати на нові виклики і загрози.

Слід почати з встановлення чітких KPI та метрик. KPI (Ключові показники ефективності) – це всі фінансові та нефінансові показники, які допомагають оцінити ефективність поточної діяльності. Їхнє значення, виміряне за певний період часу та виражене в цифрах, є зворотним зв'язком про те, чи була досягнута поставлена мета. Сама по собі постановка цілей – це тільки половина справи. Ефективний моніторинг прогресу в їх досягненні не менш важливий. KPI – це конкретні цифри, виділені з об’єму інших даних. Вони дають змогу швидко дізнатися й оцінити поточний стан конкретної мети, що полегшує визначення пріоритетів і ухвалення рішень. До них можуть входити кількість інцидентів безпеки, час реагування на інциденти, кількість успішних ідентифікацій загроз тощо. Метрики дозволяють отримати числове значення деяких властивостей ПЗ, відображає оперативну інформацію про його поточний стан. Це має на меті

забезпечити можливість кількісної оцінки ефективності заходів безпеки та виявлення областей, які потребують вдосконалення [23].

Постійний, регулярний моніторинг, збір та аналіз логів від різних систем та додатків допоможуть у виявленні аномальної поведінки або потенційних інцидентів безпеки. Його метою є швидке виявлення та реагування на потенційні загрози для забезпечення безпеки ІА.

Особливо важливим варто зазначити використання систем виявлення та запобігання вторгнень, таких як IDS/IPS. Це програмні або апаратні системи, що забезпечують мережну та комп'ютерну безпеку. IDS – це пасивна система виявлення, яка у режимі реального часу аналізує весь трафік і за необхідності повідомляє про можливі загрози. Вона ніяк не модифікує мережеві пакети даних і не впливає на роботу мережевої інфраструктури, в той час як IPS здатна запобігти доставці пакетів подібно до того, як це робить брандмауер. IPS, будучи системою запобігання вторгненням, також націлена на постійний аналіз трафіку, ось тільки повноважень у цієї служби більше – за необхідності вона може відхиляти отримання пакетів, якщо системний аналіз виявить загрозу. Для виявлення загроз використовується актуальна база даних сигнатур, отже її рекомендується регулярно оновлювати, щоб система належним чином виконувала свої функції. Впровадження та налаштування систем IDS/IPS для моніторингу мережевого трафіку та виявлення підозрілої активності допоможе забезпечити активний захист ІС від несанкціонованих вторгнень та атак [24].

Сюди ж варто додати впровадження інструментів для автоматизованого моніторингу безпеки, таких як SIEM, для централізованого збору, аналізу та кореляції даних про інциденти. Це набір інструментів і методів для дослідження подій, важливих для кібербезпеки, у середовищі, де застосовується ця система. SIEM складається з двох технологій, які розвивалися окремо одна від одної – Керування подіями безпеки (Security Event Management, SEM) і Керування інформацією про безпеку (Security Information Management, SIM). SEM відповідає за моніторинг та сповіщення про вхідні події в мережі (нові підключення, можливі проблеми та сумнівна поведінка). З іншого боку, SIM

займається аналізом журналів подій і наданням відповідних висновків команді аналітиків. SIEM поєднує обидва ці підходи, пропонуючи одночасну реєстрацію всіх подій у системі та їх аналіз. Ця технологія дозволяє командам кібербезпеки стежити за подіями, виявляти загрози та реагувати на них. Насправді реакція зазвичай вимагає як навичок, так і програмного забезпечення, яке дає змогу захистити певні ділянки мережі [25].

Розглядаючи дослідження кращих практик вдосконалення СУІБ, варто приділити увагу регулярному тренування та навчання персоналу, оскільки працівники – це головна рушійна сила організації. Від роботи та дій працівників залежить успішна робота компанії, саме тому варто приділяти велику увагу розвитку та організації регулярних тренувань та навчальних програм для підвищення обізнаності та компетенцій співробітників у сфері ІБ. Це забезпечить їх готовність до реагування на інциденти безпеки. Як варіант, можна організувати періодичне проведення інформаційних симуляцій та тестувань на проникнення (пентестів) для виявлення вразливостей у системах та процесах. Це дозволить виявляти слабкі місця у захисті та допоможе в розробці заходів для їх усунення.

Не менш важливим є аналіз проведеної роботи, а саме аналіз інцидентів та впровадження коригувальних дій. Проведення детального аналізу кожного інциденту безпеки для визначення його причин та розробка планів щодо запобігання подібним інцидентам у майбутньому допоможе покращити процеси та процедури на основі отриманого досвіду.

Варто підкреслити важливість та необхідність залучення зовнішніх експертів та консультантів. Співпраця з ними допоможе провести незалежну оцінку СУІБ та отримати рекомендації щодо їх вдосконалення. Отримання свіжого, стороннього погляду та експертних знань буде перевагою для покращення функціонування СУІБ.

Впровадження СУІБ в організацію здійснюється за допомогою різних методик, що дозволяють структурувати та систематизувати цей процес. В табл. 2.6 наведені конкретні методики впровадження СУІБ, які можуть бути

застосовані в організації.

Таблиця 2.6.

Методики впровадження СУІБ [26]

Методика	Призначення
GAP-аналіз	Дозволяє виявити розриви між поточним станом ІБ організації та вимогам ISO/IEC 27001
OCTAVE	Ризик-орієнтована методика, що фокусується на ідентифікації, оцінці та управління ризиками ІБ
ITIL	Комплексний підхід до управління IT-послугами, включаючи аспекти ІБ

Алгоритм впровадження методик на прикладі GAP-аналізу зображено на рис 2.5.

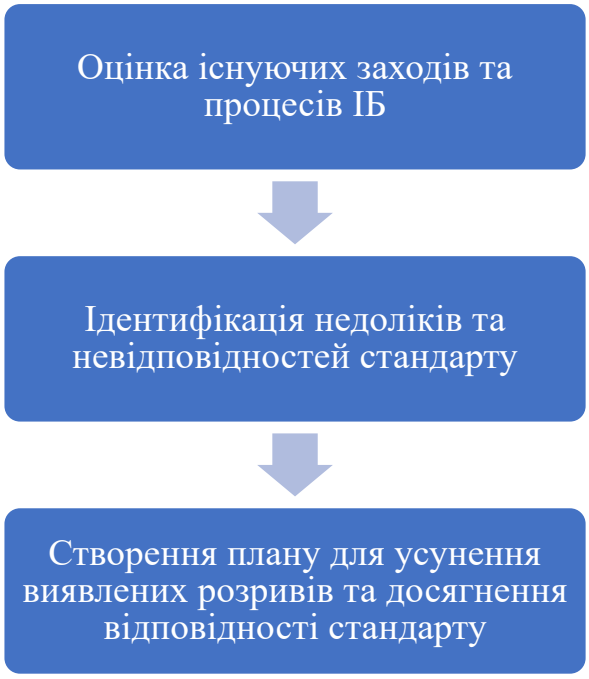

Рис. 2.5. Алгоритм впровадження методики на основі GAP-аналізу

Кожна з цим методик має свої переваги та може бути адаптована до специфіки вашої організації для забезпечення ефективного впровадження СУІБ. Вибір методики залежить від розміру організації, її галузі, рівня зрілості ІБ та доступних ресурсів.

Підсумувавши, можна з впевненістю зазначити, що моніторинг та вдосконалення СУІБ є безперервними процесами, які потребують

систематичного підходу та постійної уваги. Використання кращих практик допомагає організаціям забезпечувати високий рівень захисту ІА, відповідати нормативним вимогам та швидко адаптуватися до змінних умов зовнішнього середовища. Ефективний моніторинг та вдосконалення СУІБ сприяють підвищенню стійкості організації до кіберзагроз та забезпеченню її конкурентоспроможності на ринку. На завершення варто додати, що не зайвим буде визначення контексту організації на етапі планування, що дасть змогу впровадити СУІБ за кращими умовами (рис. 2.6).

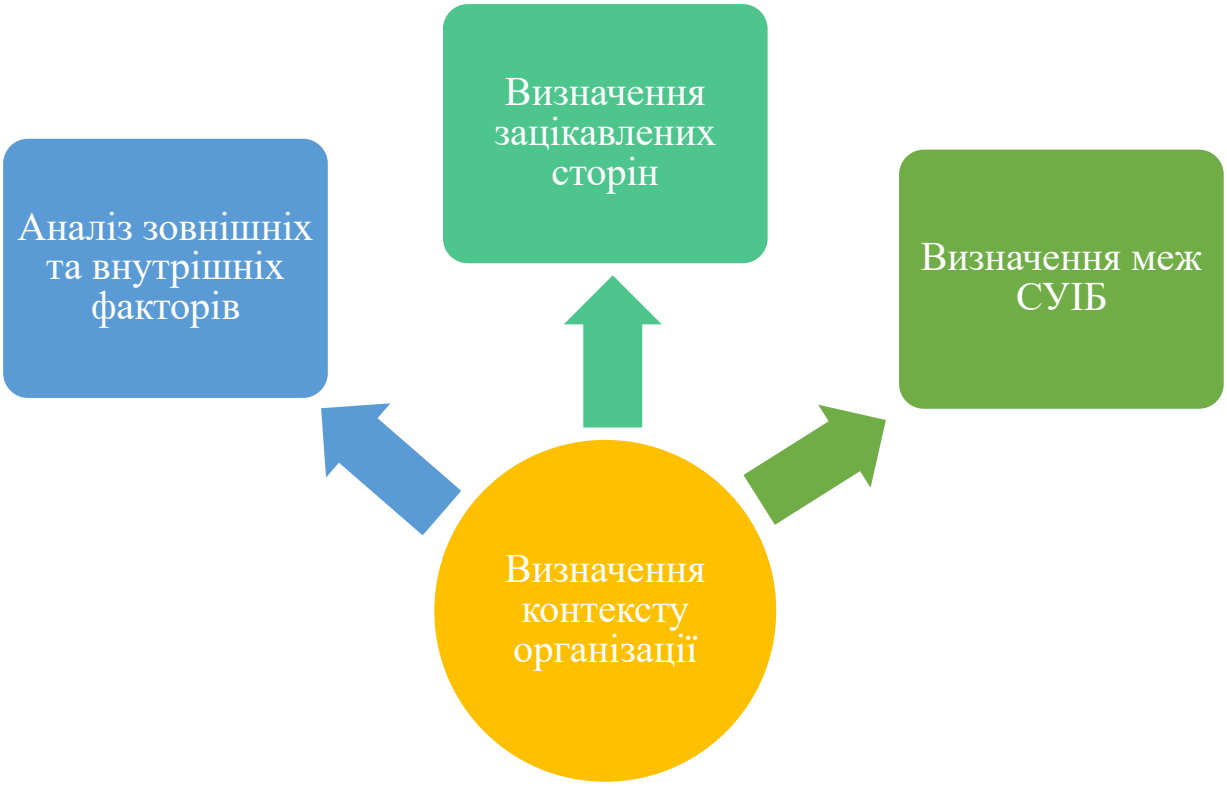

Рис. 2.6. Визначення контексту організації при впровадженні СУІБ [27]

Зацікавленими сторонами можуть бути різні групи користувачів, які мають вплив або на яких може бути вплив за рахунок впровадження СУІБ. Детальний приклад наведені на рис. 2.7.

Рис. 2.7. Основні групи зацікавлених сторін [27]

Діяльність з визначення груп зацікавлених сторін і їхніх вимог включає в себе:

- визначення вимог клієнтів до ІБ, їхніх очікувань щодо конфіденційності, цілісності та доступності інформації;
- аналіз вимог постачальників і партнерів, їхнього впливу на ІБ організації, а також необхідність узгодження політики ІБ;
- визначення ролі співробітників у забезпеченні ІБ, їхніх потреб у навчанні та обізнаності, а також мотивації до дотримання політики ІБ;
- ідентифікація вимог регуляторних органів, які контролюють діяльність організації, зокрема вимог щодо звітності та відповідності стандартам;
- інтереси акціонерів та їхні очікування щодо захисту ІА, які можуть впливати на репутацію та вартість організації.

Внутрішній аудит та аналіз з боку керівництва є ключовими елементами процесу моніторингу та вдосконалення СУІБ. Вони допомагають забезпечити відповідність СУІБ вимогам стандартів, виявляти та усувати недоліки, а також підвищувати загальну ефективність системи. Внутрішній аудит – це систематичний, незалежний та документований процес оцінки відповідності СУІБ встановленим вимогам, політикам та процедурам.

Внутрішній аудит включає в себе етапи, серед яких:

1. Планування;
2. Підготовка;
3. Проведення аудиту;
4. Аналіз результатів;
5. Звіт про аудит;
6. Моніторинг коригувальних дій.

Початковим процесом є визначення цілей, обсягу, критеріїв та методів аудиту. План повинен включати перелік підрозділів, процесів та активів, які підлягають аудиту, а також вибір незалежних і кваліфікованих аудиторів, які не мають конфлікту інтересів щодо об’єктів аудиту. В подальшому йде ознайомлення з політиками, процедурами та попередніми звітами про аудити. Це допомагає аудиторам зрозуміти контекст та специфіку СУІБ організації. На цьому етапі розробляється списки питань та пунктів для перевірки, які будуть використовуватися під час аудиту. Наступним кроком проводиться інтерв’ю зі співробітниками, спостереження за процесами та перевірка документів для оцінки відповідності встановленим вимогам, збір об’єктивних доказів відповідності або невідповідності вимогам, політикам та процедурам. Слід провести порівняння зібраних доказів з встановленими критеріями для визначення відповідності або виявлення невідповідностей, розробку рекомендацій щодо усунення виявлених невідповідностей та покращення СУІБ. Необхідно скласти звіт про результати аудиту, включаючи виявлені невідповідності, їхні причини та рекомендації щодо покращення. Проводиться передача звіту вищому керівництву для коригувальних дій. Останнім кроком має бути моніторинг впровадження коригувальних дій, визначених у звіті про аудит, для забезпечення усунення невідповідностей та покращення СУІБ [28].

Аналіз з боку керівництва – це регулярний процес оцінки ефективності та результативності СУІБ, що проводиться вищим керівництвом організації. В основному під цим процесом мається на увазі підготовка та проведення аналізу, а саме оцінка зібраних даних та звітів для визначення ефективності СУІБ,

виявлення тенденцій та проблемних областей, порівняння результатів роботи СУІБ з визначеними цілями та планами. Найголовнішим є визначення необхідних коригувальних та запобіжних дій для усунення виявлених проблем та покращення СУІБ та пріоритезація дій на основі їх важливості та впливу на ІБ організації. Кінцевим процесом буде документування результатів аналізу з боку керівництва, включаючи висновки та рішення щодо покращення СУІБ, інформування відповідальних осіб та підрозділів про результати аналізу та заплановані коригувальні дії. Для закріплення хорошого результату, має бути організований моніторинг виконання визначених коригувальних та запобіжних дій, оцінка їхньої ефективності та впливу на СУІБ.

У висновку, внутрішній аудит та аналіз з боку керівництва є невід'ємними компонентами систематичного підходу до моніторингу та вдосконалення СУІБ. Вони забезпечують незалежну оцінку відповідності та ефективності заходів ІБ, допомагають виявляти слабкі місця та розробляти рекомендації для їхнього усунення. Були розроблені рекомендації методик, які допоможуть впровадити СУІБ в організацію виходячи з її особливостей. Впровадження цих практик сприяє підвищенню рівня ІБ в організації, забезпечує відповідність нормативним вимогам та стандартам, а також підтримує постійне вдосконалення процесів управління ІБ [29].

2.3 Забезпечення ефективності процесів ризик-менеджменту як важливого фактору успішного функціонування СУІБ

Ефективність процесів ризик-менеджменту є критично важливим фактором успішного функціонування СУІБ. Ризик-менеджмент дозволяє ідентифікувати, оцінювати та керувати ризиками, пов'язаними з ІА організації. Це забезпечує захист конфіденційності, цілісності та доступності інформації, що є основою для стабільного та безпечного функціонування організації. У цьому розділі досліджено ключові аспекти забезпечення ефективності процесів ризик-менеджменту.

Першим етапом процесу ризик-менеджменту є ідентифікація ризиків, що включає виявлення потенційних загроз і вразливостей, які можуть вплинути на ІА організації. Для ефективної ідентифікації ризиків використовуються різні методи, деякі з них наведені в табл. 2.7.

Таблиця 2.7.

Методи ідентифікації ризиків [30]

Етап	**Дія**
Аналіз активів	Ідентифікація всіх ІА організації, які потребують захисту. Це можуть бути дані, ПЗ, апаратні засоби, мережеві ресурси та інші активи.
Визначення загроз	Виявлення всіх можливих загроз, які можуть вплинути на ІА. Загрози можуть бути внутрішніми або зовнішніми, навмисними або випадковими. Приклади загроз включають хакерські атаки, природні катастрофи, помилки співробітників, крадіжку даних та інші.
Визначення вразливостей	Ідентифікація вразливостей ІА, які можуть бути використані загрозами для реалізації атак. Вразливості можуть бути технічними (наприклад, недоліки в ПЗ), організаційними (наприклад, відсутність політик безпеки) або людськими (наприклад, недостатня обізнаність співробітників).

Після ідентифікації ризиків проведено їхній аналіз. Аналіз ризиків включає оцінку ймовірності реалізації кожного ризику та можливих наслідків. Основні етапи аналізу ризиків включають оцінку ймовірності, оцінку наслідків та розрахунок рівня ризику.

Спочатку визначено ймовірність реалізації кожного ідентифікованого ризику. Це було зроблено на основі статистичних даних, експертних оцінок та аналізу історичних інцидентів. Ймовірність може оцінюватись якісно (наприклад, висока, середня, низька) або кількісно (наприклад, у відсотках).

Наступним кроком проведено оцінку можливих наслідків реалізації кожного ризику. Це включало фінансові втрати, порушення бізнес-процесів, втрату даних, шкоду репутації та інші наслідки. Наслідки також можуть оцінюватись якісно (критичні, суттєві, незначні) або кількісно (у грошових одиницях). Було застосовано форму рівня ризику. Це документ, який використовується для оцінки та документування ризиків ІБ. Це допомагає класифікувати ризики за рівнем критичності та пріоритетності. Детальний опис наведено в табл. 2.8.

Таблиця 2.8.

Складові форми рівня ризику [31]

Опис	Дія
Опис ризику	Короткий опис ризику, який включає в себе його джерело, актив, який він може зашкодити та потенційні наслідки
Рівень ймовірності	Оцінка ймовірності того, що ризик станеться. Ймовірність може бути оцінена як низька, середня або висока
Рівень впливу	Оцінка впливу ризику, якщо він станеться. Вплив може бути оцінений як незначний, помірний або значний
Загальний рівень ризику	Сукупна оцінка ймовірності та впливу ризику. Загальний рівень ризику може бути оцінений як низький, середній або високий
Заходи з пом'якшення ризику	Опис заходів, які можуть бути вжиті для зменшення ймовірності або впливу ризику

Оцінка ризиків включає визначення того, які ризики є прийнятними для організації, а які потребують управління. Основні етапи оцінки ризиків включають:

- встановлення критеріїв прийнятності ризиків, які організація повинна визначити, які рівні ризиків є прийнятними, виходячи з її стратегії, ресурсів. Це можуть бути встановлені порогові значення для ймовірності, наслідків або рівня ризику;
- класифікація ризиків, на основі критеріїв прийнятності ризиків, ідентифіковані ризики класифікуються на прийнятні та неприпустимі. Прийнятні ризики — це ті, які не потребують подальших дій, оскільки їхній рівень є допустимим для організації;
- визначення стратегії управління ризиками, а саме для кожного неприпустимого ризику розробляється стратегія управління.

Управління ризиками включає розробку та впровадження заходів для мінімізації або усунення ідентифікованих ризиків. Було з'ясовано основні стратегії управління ризиками, які включають:

1. Вибір та впровадження заходів контролю для зменшення ймовірності реалізації загроз або зниження їхнього вплив, це може включати технічні заходи (шифрування, системи виявлення вторгнень), організаційні заходи (політики доступу, навчання співробітників) та фізичні заходи (контроль доступу до

приміщень);

2. Постійний моніторинг та оцінка ефективності впроваджених заходів контролю, включає регулярні аудити, тестування на проникнення та аналіз інцидентів безпеки;

3. Розробка планів реагування на інциденти, які визначають дії у разі реалізації ризиків, тобто процедури виявлення, аналізу, реагування та відновлення після інцидентів.

Результати оцінки ризиків повинні були ретельно задокументовані для забезпечення прозорості та подальшого аналізу. Приклад документації наведений на рис. 2.8.

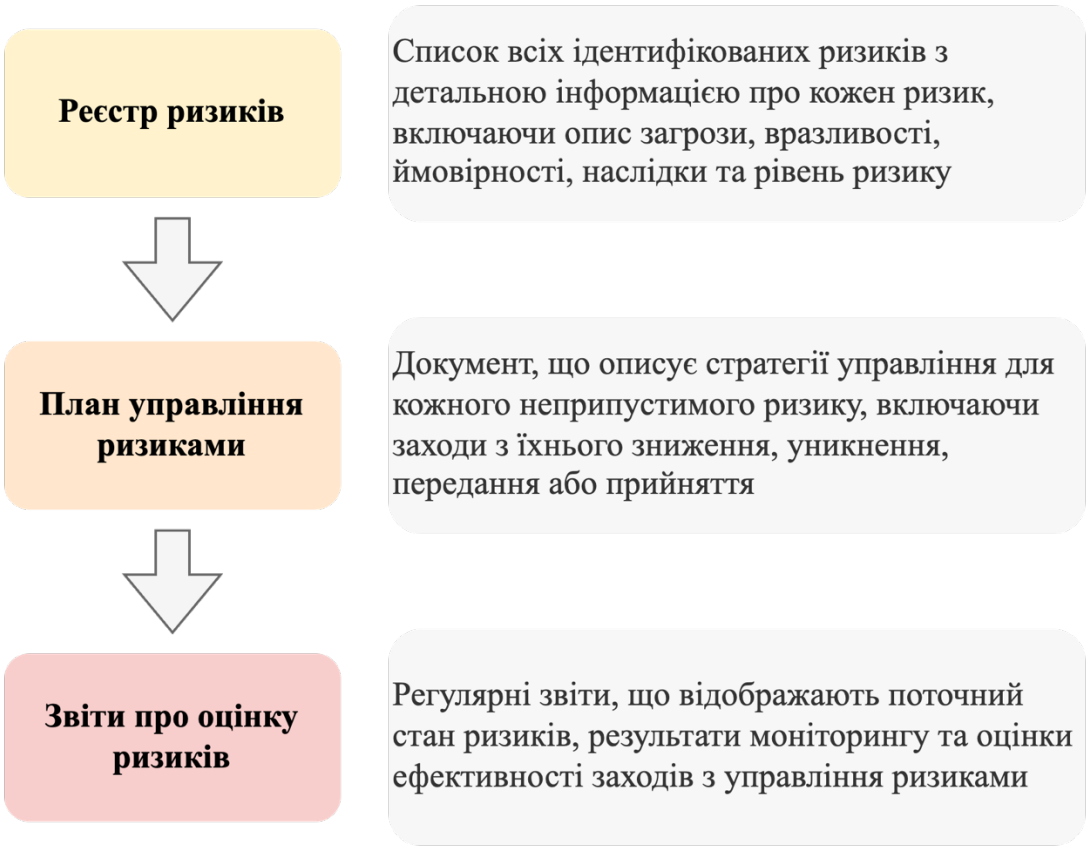

Рис. 2.8. Документація результатів оцінки ризиків [32]

Оцінка ризиків є безперервним процесом, який постійно контролюється та переглядається. Основні етапи моніторингу включають:

1. Проведення регулярних переглядів ризиків для виявлення нових загроз

і вразливостей, а також оцінки змін у ймовірностях та наслідках існуючих ризиків;

2. Оцінку ефективності впроваджених заходів з управління ризиками для забезпечення їхньої дієвості;

3. Оновлення реєстру ризиків на основі результатів моніторингу та перегляду, а також внесення змін у план управління ризиками.

Ефективна оцінка ризиків допомагає організації ідентифікувати та усувати потенційні загрози для ІБ, забезпечуючи захист ІА і підтримування відповідність вимогам стандарту ISO/IEC 27001 [33].

Окрім цього, ефективність процесів ризик-менеджменту залежить від їх постійного вдосконалення. Дії по вдосконаленню процесів ризик-менеджменту, які застосовані на підприємстві ТОВ «Бізнестехніка», наведені на рис. 2.9.

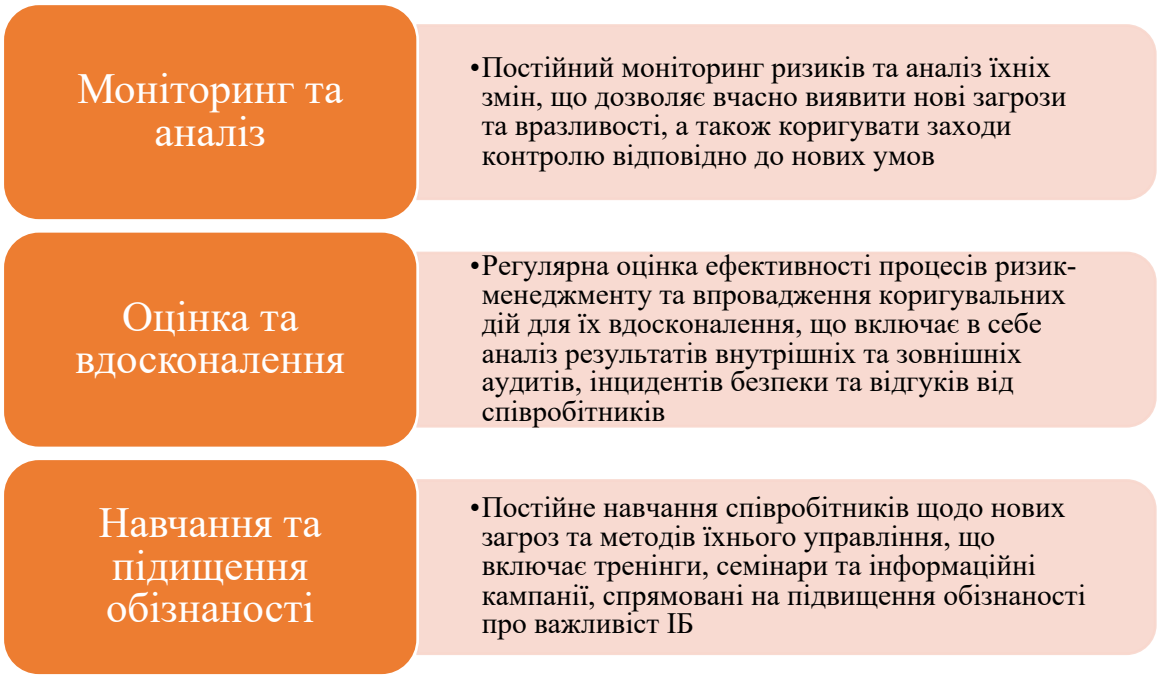

Рис. 2.9. Процеси вдосконалення ризик-менеджменту

З’ясовано, що забезпечення ефективності процесів ризик-менеджменту є ключовим фактором успішного функціонування СУІБ в межах організації. Вони дозволяють ідентифікувати, оцінювати та керувати ризиками, забезпечуючи захист ІА. Ефективний ризик-менеджмент сприяє мінімізації втрат від інцидентів безпеки, підвищенню операційної ефективності та забезпеченню

відповідності нормативним вимогам. Постійне вдосконалення процесів ризик-менеджменту допомагає організаціям адаптуватися до змінних умов та нових викликів, забезпечуючи стабільний та безпечний розвиток [34].

Висновки до розділу 2

У розділі було детально розглянуто методику впровадження СУІБ в організаціях, що включає аналіз процесів планування та ініціювання впровадження, дослідження кращих практик моніторингу та вдосконалення, а також забезпечення ефективності процесів ризик-менеджменту. Окрім цього, досліджені методики, які допомагають під кожну організацію індивідуально підібрати метод впровадження СУІБ, виходячи з її поточного стану ІБ. Це такі методики як GAP-аналіз, OCTAVE, ITIL, NIST.

Впровадження СУІБ розпочато з ретельного планування та ініціювання, що включало визначення цілей, аналізу поточного стану ІБ, розробку стратегії впровадження та залучення керівництва й співробітників. Важливим етапом була розробка обов'язкової документації, яка встановлює політики, процедури та стандарти для захисту ІА. До основної документації включено політика ІБ, оцінка ризиків, заява про застосовність, план управління ризиками, процедури управління інцидентами та доступом, план безперервності бізнесу та інші. Ці документи допомогли забезпечити систематизацію процесів, підвищення прозорості та відповідності нормативним вимогам.

Проаналізувавши ефективний моніторинг та вдосконалення СУІБ, було визначено, що він включає встановлення чітких KPI та метрик, регулярний моніторинг логів, використання систем виявлення та запобігання вторгнень (IDS/IPS), проведення регулярних внутрішніх та зовнішніх аудитів, а також використання автоматизованих засобів моніторингу. Важливу роль відігравали внутрішні аудити та аналіз з боку керівництва, які забезпечують незалежну оцінку відповідності та ефективності заходів ІБ, виявляють слабкі місця та допомагають розробляти рекомендації для їх усунення. Постійне вдосконалення

СУІБ досягається через цикл PDCA, регулярні тренування та навчання персоналу, проведення інформаційних симуляцій та тестувань на проникнення, аналіз інцидентів та коригувальні дії, а також оновлення політик та процедур.

З’ясовано, що ефективність процесів ризик-менеджменту є ключовим фактором успішного функціонування СУІБ. Це включає в себе ідентифікацію ризиків, оцінку ймовірності та впливу загроз, класифікацію ризиків, розробку та впровадження заходів контролю, а також оцінку їхньої ефективності. Важливими етапами є також розробка планів реагування на інциденти, моніторинг ризиків та їхніх змін, оцінка та вдосконалення процесів ризик-менеджменту, а також постійне навчання та підвищення обізнаності персоналу. Забезпечення ефективності ризик-менеджменту дозволяє організаціям мінімізувати втрати від інцидентів безпеки, підвищити операційну ефективність та забезпечити відповідність нормативним вимогам.

Таким чином, в результаті дослідження методики впровадження СУІБ визначено, що успішне функціонування СУІБ залежить від систематичного підходу до планування та ініціювання, впровадження кращих практик моніторингу та вдосконалення, а також забезпечення ефективного управління ризиками. Ці елементи допомагають організаціям адаптуватися до змінних умов, забезпечувати захист ІА та підтримувати стабільний розвиток.

Розділ 3 ОСОБЛИВОСТІ ПІДТРИМКИ ТА СЕРТИФІКАЦІЇ СУІБ

Для досягнення мети дослідження необхідно провести аналіз методики сертифікації СУІБ на відповідність вимогам ISO/IEC 27001 та розробити рекомендації щодо вибору доцільної стратегії впровадження СУІБ, досягнення та підтримки сертифікації СУІБ.

3.1 Аналіз методики сертифікації СУІБ на відповідність вимогам ISO/IEC 27001

Сертифікація СУІБ на відповідність вимогам стандарту ISO/IEC 27001 є важливим етапом для організацій, що прагнуть офіційно підтвердити відповідність своєї СУІБ міжнародним стандартам. Процес сертифікації включає кілька ключових етапів, кожен з яких вимагає ретельного планування, підготовки та виконання.

Сертифікація СУІБ на відповідність вимогам стандарту ISO/IEC 27001 включає в себе декілька етапів. Детально досліджено та проаналізовано кожен з них.

Першим етапом є підготовка до сертифікації. Організації потрібно визначити обсяги сертифікації, тобто які підрозділи, процеси та інформаційні активи будуть включені в сертифікацію. Це включає оцінку меж СУІБ і визначення ключових активів, що підлягають захисту. Також необхідний детальний аналіз поточного стану СУІБ для виявлення відповідності вимогам стандарту ISO 27001. Це включає оцінку політик, процедур, технічних засобів захисту та організаційних заходів. Після аналізу визначено необхідні коригувальні дії для усунення виявлених невідповідностей та вдосконалення СУІБ. План дій включає конкретні заходи, терміни виконання та відповідальних осіб [35].

Після проведеної підготовки організації впроваджено деякі заходи для відповідності вимогам стандарту. Це такі заходи як:

- оновлення політик та процедур;
- навчання та підвищення обізнаності персоналу;
- впровадження технічних заходів захисту.

На організацію також чекало проведення внутрішнього та зовнішнього сертифікаційного аудиту. Внутрішній аудит включав в себе деякі процеси пов’язані з підготовкою, проведенням та документуванням аудиту. Що стосується зовнішнього аудиту, тут організація повинна вибрати сертифікаційний орган, який має акредитацію, і яким буде проведений сам аудит на відповідність вимогам стандарту.

Сам аудит має бути розділений на декілька етапів, такі як:

1. Проведення попереднього аудиту (Stage 1 Audit), на якому сертифікаційний орган проводить попередній аудит для оцінки;

2. Готовності організації до основного аудиту, що включає перевірку документації, аналіз ризиків та планування основного аудиту;

3. Проведення основного аудиту (Stage 2 Audit), який включає детальну перевірку відповідності СУІБ вимогам ISO 27001. Аудитори аналізують документи, проводять інтерв'ю зі співробітниками та спостерігають за процесами;

4. За результатами аудиту складається звіт із виявленими невідповідностями та рекомендаціями. Після проведених операцій організації дається можливість на виправлення усіх невідповідностей, тобто усунути всі виявлені під час основного аудиту невідповідності та надати докази сертифікаційному органу;

5. Після успішного виправлення невідповідностей та повторної перевірки сертифікаційний орган видає сертифікат відповідності ISO 27001. Цей сертифікат буде дійсний протягом трьох років, після чого необхідно проходити повторну сертифікацію.

Після пройдених етапів і успішного отримання сертифікату відповідності організація отримає ряд переваг, деякі з яким наведені в табл. 3.1.

Таблиця 3.1.

Приклади отриманих переваг після отримання сертифікату [36]

Перевага	Опис
Підвищення довіри клієнтів та партнерів	Демонструє прихильність організації до забезпечення високого рівня ІБ, що сприяє підвищенню довіри з боку клієнтів, партнерів
Відповідність нормативним вимогам	Сертифікація допомагає забезпечити відповідність нормативним та законодавчим вимогам у сфері ІБ
Зниження ризиків	Сертифікація СУІБ сприяє ефективному управлінню ризиками, що дозволяє знизити ймовірність інцидентів безпеки та їхні негативні наслідки
Підвищення операційної ефективності	Систематичний підхід до управління ІБ сприяє підвищенню операційної ефективності та зменшенню витрат, пов'язаних з інцидентами безпеки
Покращення іміджу організації	Сертифікація ISO 27001 підвищує репутацію організації на ринку, демонструючи її відповідальність та професіоналізм у сфері ІБ

Сертифікація СУІБ на відповідність вимогам ISO 27001 є важливим кроком для будь-якої організації, що прагне забезпечити високий рівень захисту ІА та підвищити свою конкурентоспроможність. Процес сертифікації включає підготовку, впровадження заходів для відповідності вимогам стандарту, проведення внутрішніх та зовнішніх аудитів, а також виправлення невідповідностей. Сертифікація приносить значні переваги, включаючи підвищення довіри клієнтів та партнерів, відповідність нормативним вимогам, зниження ризиків, підвищення операційної ефективності та покращення іміджу організації. Успішне проходження сертифікації підтверджує, що СУІБ організації відповідає міжнародним стандартам, що є ключовим фактором для стабільного та безпечного розвитку в умовах сучасного інформаційного середовища. Детальні кроки кожного етапу методики сертифікації СУІБ на відповідність вимогам ISO/IEC 27001 зображені на рис. 3.1.

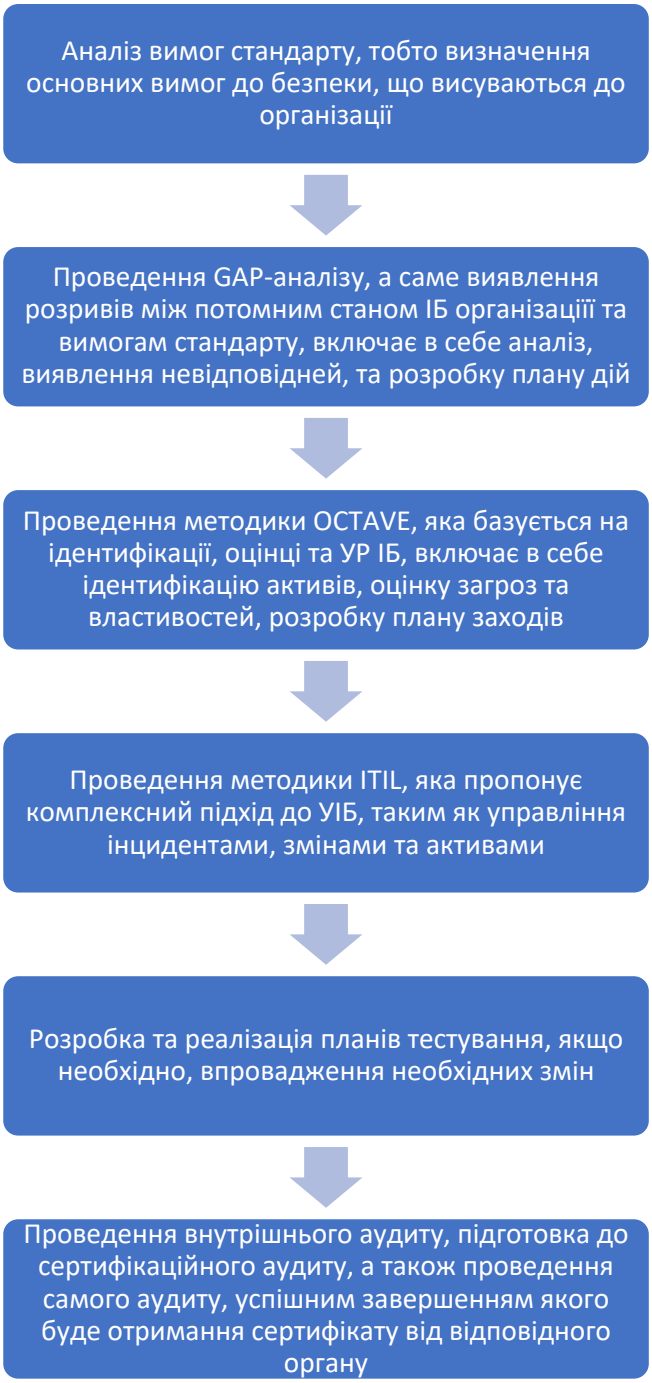

Рис. 3.1. Етапи методики сертифікації СУІБ [37]

3.2 Розробка рекомендацій щодо вибору доцільної стратегії впровадження СУІБ

Вибір доцільної стратегії впровадження СУІБ є важливим етапом, що визначає ефективність захисту ІА організації. Успішне впровадження СУІБ вимагає врахування багатьох факторів, включаючи розмір та галузь організації,

наявні ресурси, специфіку ІА, нормативні вимоги та потенційні ризики.

У цьому розділі було досліджено рекомендації щодо вибору стратегії впровадження СУІБ, що базуються на кращих практиках та стандартах ІБ, а саме:

- проведення попереднього аналізу та оцінки ризиків. Цей крок включає в себе ідентифікацію всіх ІА, таких як апаратне та програмне забезпечення, людські ресурси, ІС та інфраструктура, окремо визначення критичних активів організації – сервери, бази даних з інформацією про клієнтів та секретною інформацією; ідентифікацію загроз та вразливостей, розробку сценаріїв актуальних загроз із врахуванням існуючих вразливостей та моделі порушника, визначення критичних загроз; для критичних активів та загроз – проведення кількісної та якісної оцінки ризиків;
- визначення цілей та обсягу впровадження СУІБ відповідно до організації, обрання відповідної методології. Цілі мають враховувати захист ІА, зниження ризиків, підвищення обізнаності персоналу, ефективності бізнесу, довіри з боку клієнтів, законодавчим вимогам, пошук взаємозв’язку між цілями та стратегією, визначення області застосування; включення як всієї компанії так і окремих підрозділів, що залежить від критичності процесів, ризиків, ресурсів, вимогам нормативних актів;
- залучення керівництва та зацікавлених сторін. Залучення CEO, CISO, CIO, керівників підрозділів, партнерів, клієнтів, регуляторів, менеджера ризиків: всі вони мають взаємодіяти між собою, а також мають значний вплив на роботу всієї організації, тому надважливо забезпечити спільну зацікавленість для ефективної роботи; важливо підтримувати комунікацію з керівництвом, пояснювати важливість їхнього залучення та вплив на стан ІБ;
- розробка детального плану впровадження політик, процедур та заходів безпеки. План має включати аналіз та оцінку поточного стану ІБ, визначення обсягу СУІБ, цілей ІБ, планування ресурсів, розробку політик та процедур, моніторинг та оцінка ефективності, коригувальні дії та постійне вдосконалення, документування звітності; призначення відповідальним за виконання плану

проектного менеджера, який буде збирати та аналізувати зворотній зв'язок, а також аналізувати результати та вносити зміни;

- навчання, підвищення обізнаності та розвиток персоналу. Відповідальний за це HR-менеджер, який відповідальний за обов’язкове проведення оцінки обізнаності персоналу щонайменше раз на квартал, проведення важливе для всіх правників організації залежно від їх рівня знань та посади;
- моніторинг, оцінка ефективності та коригувальні дії для постійного вдосконалення. Здійснюється за допомогою систем IDS/IPS, SIEM систем, антивірусного ПЗ, моніторингу мережевого трафіку, проводиться збір та аналіз інформації. Застосовуються показники ефективності, такі як кількість інцидентів, вразливостей, частота оновлень безпеки, рівень дотримання політик безпеки, оцінка ризиків; постійне вдосконалення, проведення навчальних програм, оновлення знань, інформування керівництва та отримання зворотного зв’язку;
- підготовка до сертифікації. Підготовлення документів з цілями, політиками ІБ, обсягом СУІБ, заяву з переліком контролів, що застосовуються, звіти внутрішніх аудитів, процедури УР, результати management review; забезпечення наявності ключових співробітників, таких як CISO, CIO, системного адміністратора, менеджера по роботі з ризиками; внутрішні аудити мають проводитись як мінімум раз на рік внутрішніми аудиторами, а також варто залучати зовнішніх аудиторів для забезпечення об’єктивності.

Дослідження проводилось на підприємстві ТОВ «Бізнестехніка» під час проходження переддипломної практики.

Організація проводила детальну оцінку поточного стану ІБ, це є перший кроком у розробці стратегії впровадження СУІБ. Вона проводиться на основі: інвентаризації активів, оцінки ризиків та аналізі поточних заходів безпеки.

На основі оцінки поточного стану ІБ організація вибрала відповідний підхід до впровадження СУІБ. Основні та загальні підходи по вибору стратегії

зазначені в табл. 3.2.

Таблиця 3.2

Рекомендації по вибору стратегії впровадження СУІБ [38]

Стратегія	**Переваги**
Інтеграція з вже існуючими системами управління	Забезпечує узгодженість з іншими системами управління (наприклад, системами управління якістю або екологічного менеджменту), що може зменшити дублювання зусиль і підвищити ефективність
Поетапне впровадження	Дає змогу поступово впроваджувати СУІБ, що може бути менш ресурсомістким і дозволяє вносити коригування на основі отриманого досвіду
Комплексне впровадження	Забезпечує швидке досягнення повної відповідності вимогам стандарту ISO 27001. Може бути доцільним для організацій, що потребують швидкої сертифікації або мають високий рівень ризиків

Кожна з запропонованих стратегій має свої рекомендації по впровадженню. Наприклад, організація, яка вже має впроваджену систему управління, може інтегрувати СУІБ з існуючими системами для забезпечення узгодженості підходів та використання наявних ресурсів. Якщо ж організація має обмежені ресурси, або впроваджує СУІБ вперше, їй краще підійде поетапне впровадження. Для неї початкові етапи можуть включати впровадження основних політик та процедур, а подальші етапи – розширення функціональності системи. Для великих організацій та тих, які працюють з широким спектром інформації або у високо ризикованих галузях, рекомендоване комплексне впровадження, де ІБ є критично важливою.

Організацією обрано стратегію комплексного впровадження. Це обумовлене багатьма факторами, зокрема тим, що нашій організації було необхідне швидке досягнення результату та наближення до відповідним вимогам стандарту. Компанія не мала високий рівень ризиків, проте вона обробляє великий обсяг інформації, такої як: персональні данні клієнтів, стратегічно важливу інформацію компанії, секретні розробки та впровадження. Це зіграло ключову роль при виборі стратегії по впровадження стандарту. Мушу зазначити, що вибір саме такого варіанту було найкращим рішенням для покращення роботи та усунення можливих ризиків для організації.

Загалом, вибір доцільної стратегії впровадження СУІБ є складним і багатоетапним процесом, який вимагає ретельного планування та врахування специфічних особливостей організації. Проте є основні, загальні рекомендації щодо вибору стратегії, які включають:

1. Проведення детального аналізу поточного стану ІБ для виявлення сильних та слабких сторін, визначення критичних активів та оцінка ризиків;
2. Вибір відповідного підходу до впровадження СУІБ на основі оцінки ресурсів, специфіки ІА та ризиків;
3. Створення детального плану впровадження, що включає визначення цілей, розподіл ролей і відповідальностей, розробку політик та процедур, навчання співробітників, впровадження технічних засобів захисту, моніторинг та оцінку ефективності, проведення внутрішніх аудитів;
4. Забезпечення постійного вдосконалення СУІБ шляхом регулярного моніторингу, оцінки результатів, проведення аудитів та навчання співробітників.

Впровадження СУІБ, що відповідає вимогам стандарту ISO 27001, дозволяє організації ефективно захищати свої ІА, мінімізувати ризики та забезпечувати відповідність нормативним вимогам. Це сприяє підвищенню довіри клієнтів та партнерів, покращенню операційної ефективності та підтриманню конкурентоспроможності на ринку [39].

3.3 Розробка рекомендацій щодо досягнення та підтримки сертифікації СУІБ за ISO/IEC 27001

Досягнення та підтримка сертифікації СУІБ за стандартом ISO/IEC 27001 є невід’ємним етапом для організацій, які прагнуть офіційно підтвердити відповідність своєї СУІБ міжнародним стандартам. Сертифікація не лише підвищує рівень захисту ІА, але й сприяє зміцненню довіри з боку клієнтів, партнерів та регуляторів. У цьому розділі були розглянуті та досліджені рекомендації щодо досягнення та підтримки сертифікації СУІБ за стандартом ISO/IEC 27001 на прикладі ТОВ «Бізнестехніка», а саме:

- усунення незначних та вагомих невідповідностей: аналізувати причини, розроблювати коригувальні заходи, перевіряти ефективність, документувати результати.
- проведення щорічних наглядових аудитів: перевіряти ключові елементи СУІБ, включаючи УР, політики, процедури, технічні засоби та реагування на інциденти, щорічно протягом трьох років після отримання сертифікату; залучення зовнішніх аудиторів до об'єктивності та достовірності результатів; підготовка звітів та документації про результати аудиту;
- проведення ресертифікаційного аудиту: вимагає визначення мети, створення плану аудиту; залучення зовнішніх аудиторів для його проведення відповідно до стандарту ISO/IEC 27001.

Загалом етапи проведення та підготовки до ресертифікаційного аудиту нічим не відрізняються від проведення основного сертифікаційного аудиту, проте він необхідний задля продовження дії сертифікату на відповідність стандарту ISO/IEC 27001.

Вимоги до органів, які можуть проводити сертифікацію СУІБ:

- сертифікаційні органи мають бути акредитовані відповідно до стандарту ISO/IEC 17021, який визначає вимоги до органів, що проводять аудит та сертифікацію систем управління;
- вони повинні бути акредитовані національними органами з акредитації, до прикладу Національним агентством з акредитації України.

В Україні існують певні організації, які здійснюють сертифікацію СУІБ, серед них найпопулярнішими є: Bureau Veritas Certification Ukraine, SGS Ukraine, Intertek Ukraine, DNV GL Ukraine.

Після успішного завершення сертифікаційного аудиту за стандартом ISO/IEC 27001 організація отримала сертифікат, який підтверджує її відповідність вимогам стандарту. Однак отримання сертифікату – це лише початок процесу. Для забезпечення постійної відповідності стандарту та підтримання сертифікату організація повинна здійснювати ряд заходів з

моніторингу, оцінки та вдосконалення своєї СУІБ.

Досягнення сертифікації СУІБ складалося з рідних етапів та заходів. Приклад процесу успішної сертифікації ТОВ «Бізнестехніка» зображений на рис. 3.2. Створення детального плану дій, що включає конкретні заходи, терміни виконання та відповідальних осіб, визначення всіх аспектів СУІБ, що потребують вдосконалення допомогло у якісному отриманні сертифікату. Після проведення внутрішнього аудиту в організації були виявлені деякі недоліки у технічному захисті. Саме тому, перед основним аудитом було додатково встановлено та налаштовано додаткові технічні засоби захисту (брандмауери, IDS/IPS, антивірусне ПЗ) та впроваджено організаційні заходи (контроль доступу, резервне копіювання). На етапі проведення зовнішнього аудиту співробітники були максимально підготовленим і сконцентрованим, оскільки від них залежало отримання майбутнього сертифікату на відповідність дотримання стандартів.

Рис. 3.2. Процес успішної сертифікації [40]

Було проаналізовано результати процесу успішного впровадження та отримання сертифікату СУІБ на підприємстві ТОВ «Бізнестехніка».

Співробітниками продемонстровано успішну роботу процедур, які передбачає стандарт. На власному досвіді, я усвідомив важливість та престижність отримання даного сертифікату, а також впевнився у не легкому підтриманні зазначених вимог.

Підтримання сертифікату ISO/IEC 27001 це відповідальний і необхідний процес для підприємства. Приклад заходів, які є невід'ємною частиною у підтриманні сертифікату наведені на рис. 3.3.

Рис. 3.3. Заходи, спрямовані на підтримання сертифікації [41]

З моменту сертифікації, організація націлена на постійний моніторинг своєї СУІБ для виявлення можливих недоліків та негайного їх усунення.

Зокрема, це необхідно для того, щоб через три роки, коли треба поновлювати дію сертифікату, організація вже не мала суттєвих проблем при підготовці до нового аудиту, та могла підтримувати СУІБ у належному стані.

Сертифікаційний орган також проводить регулярні наглядові аудити для підтвердження постійної відповідності організації вимогам стандарту. Наглядові аудити зазвичай проводяться щорічно протягом трьох років після отримання сертифікату. Під час наглядових аудитів перевіряється виконання вимог стандарту, впровадження коригувальних заходів та ефективність СУІБ. ТОВ «Бізнестехніка» зобов'язалась регулярно переглядати та оновлювати свої політики, процедури та інші документи для забезпечення їхньої актуальності та відповідності вимогам стандарту. Це включає врахування змін у зовнішньому та внутрішньому середовищі, нових загроз та технологічних змін.

Було впроваджено систему регулярних тренінгів, семінарів та інформаційних кампаній для всіх співробітників, які працюють в організації. Компанія зробила акцент на розвиток співробітників, оскільки знання та досвід це головна рушійна сила будь якої компанії.

Після проходження сертифікації організація розробила ефективні процедури управління інцидентами ІБ для швидкого виявлення, реагування та усунення інцидентів. Я досліджував розробку планів для розслідування інцидентів, аналіз причин та впровадження коригувальних заходів для запобігання повторенню. Було ініційовано проведення регулярних внутрішніх аудитів для оцінки відповідності нашої СУІБ вимогам стандарту та виявлення можливостей для вдосконалення. Внутрішні аудити допомагають підтримувати високий рівень відповідності та готовності до наглядових аудитів [42].

Через три роки після отримання сертифікату організація буде проходити процес ресертифікації для підтвердження відповідності вимогам стандарту ISO/IEC 27001. Процес ресертифікації включає повний аудит, подібний до основного аудиту, що проводився під час первинної сертифікації. Саме тому дуже важливим є дотримання всіх вимог протягом всього часу дії сертифікату. Якщо організація успішно проходить ресертифікацію, їй видається новий

сертифікат на наступні три роки.

Отримання та підтримання сертифікату ISO/IEC 27001 є важливим елементом забезпечення високого рівня ІБ в організації. Постійний моніторинг, регулярні аудити, оновлення політик та навчання персоналу забезпечують відповідність вимогам стандарту та підтримання довіри з боку клієнтів і партнерів [43].

Висновки до розділу 3

У цьому розділі детально розглянуто процес сертифікації за стандартом ISO/IEC 27001, який включає підготовку до сертифікації, проведення аудиту та отримання та підтримання сертифікату. Ці етапи є критично важливими для забезпечення відповідності вимогам міжнародного стандарту та підтримання високого рівня ІБ в організації.

Розроблено рекомендації по вибору стратегії та підтримки сертифікації СУІБ, що базуються на індивідуальних складових організації, зокрема залежить від обсягу ІА, що обробляє та зберігає організація, створення детального плану дій по підтримці сертифікації, який містить в собі етапи навчання персоналу, профілактичних заходів, та оновленні систем.

Була проведена підготовка до сертифікації проведенням внутрішньої оцінки відповідності та впровадження коригувальних заходів. Цей етап включав ретельний аналіз документації, оцінку ІА та ризиків, а також впровадження необхідних змін для усунення виявлених невідповідностей. Проведення внутрішнього аудиту перед сертифікаційним аудитом дозволило організації оцінити свою готовність та впевнитися у відповідності вимогам стандарту.

Було проведено детальне дослідження процесів проведення аудиту, який складався з двох основних етапів: попереднього аудиту (етап 1) та основного аудиту (етап 2). Попередній аудит допоміг оцінити готовність організації до основного аудиту, виявив можливі невідповідності, які успішно було усунено. Основний аудит включав детальну перевірку всієї СУІБ на відповідність

вимогам ISO/IEC 27001. Успішне проходження основного аудиту та усунення всіх виявлених невідповідностей було необхідною умовою, яка допомогла отримати сертифікат.

Отримання сертифікату ISO/IEC 27001 є важливим досягненням нашої організації, оскільки підтверджує її відповідність міжнародним стандартам ІБ. Однак, підтримання сертифікату вимагає постійного моніторингу, оцінки та вдосконалення СУІБ. Було розроблено детальний план для якісного підтримання сертифікату. Це такі процедури, як: регулярні наглядові аудити, оновлення політик та процедур, навчання персоналу та управління інцидентами ІБ, є невід'ємними компонентами підтримання високого рівня захисту ІА.

Заплановано підготовку до ресертифікації через три роки після отримання сертифікату, яка складається з проведення внутрішніх аудитів, усунення невідповідностей та оновлення документації. Ресертифікаційний аудит підтверджує постійну відповідність організації вимогам стандарту та забезпечує продовження дії сертифікату на наступні три роки.

Таким чином, процес сертифікації за стандартом ISO/IEC 27001 був складним та багатоступеневим, але він забезпечує створення та підтримання ефективної системи управління ІБ. Це сприяє підвищенню довіри з боку клієнтів, партнерів та інших зацікавлених сторін, а також забезпечує відповідність нормативним вимогам та кращим світовим практикам у сфері ІБ.

ВИСНОВКИ

У кваліфікаційній роботі було здійснено комплексне дослідження та аналіз стратегій впровадження, підтримки та сертифікації СУІБ за ISO/IEC 27001.

У першому розділі розглянуто теоретичні основи функціонування СУІБ та визначено ключові принципи та вимоги стандарту ISO/IEC 27001:2022, що дозволило перейти до аналізу стратегій та методів впровадження СУІБ.

У другому розділі проведено аналіз особливостей процесів планування та ініціювання впровадження СУІБ, проаналізована основна документація СУІБ. Досліджено та визначено кращі практики моніторингу та вдосконалення СУІБ, проаналізовано етапи внутрішнього аудиту та аналізу з боку керівництва, визначено роль ризик-менеджменту.

У третьому розділі проведено аналіз методики сертифікації СУІБ на відповідність вимогам ISO/IEC 27001, представлено алгоритм її проведення, який включає в себе такі етапи, як: аналіз вимог стандарту; проведення GAP-аналізу; розробка плану усунення розривів на основі результатів GAP-аналізу та плану аудиту; розробка та реалізація планів тестування; впровадження необхідних змін; проведення внутрішнього аудиту; підготовка до сертифікаційного аудиту; проведення сертифікаційного аудиту; формування результатів та звітів; отримання сертифікації та її підтримка.

Розроблено рекомендації щодо вибору доцільної стратегії впровадження СУІБ:

- проведення попереднього аналізу та оцінки ризиків, в т.ч. ідентифікація критичних активів, розробка сценаріїв актуальних загроз, проведення кількісної оцінки ризиків для критичних активів;
- визначення цілей та обсягу впровадження СУІБ відповідно до цілей організації, обрання відповідної методології на основі критичності бізнес-процесів, рівня ризиків, наявних ресурсів та застосовних вимог;
- залучення керівництва та зацікавлених сторін, в т.ч. CEO, CISO, CIO, керівників підрозділів, партнерів, клієнтів, регуляторів.

- розробка детального плану впровадження політик, процедур та заходів безпеки;
- навчання, підвищення обізнаності та розвиток персоналу, в т.ч. визначення відповідальних за ці процеси, частоти їх проведення, цільової аудиторії, структури плану та програми обізнаності;
- моніторинг, оцінка ефективності та коригувальні дії для постійного вдосконалення за допомогою таких технологій, як системи IDS/IPS, SIEM-системи, антивірусне ПЗ, моніторинг мережевого трафіку та таких показників, як кількість інцидентів, вразливостей, частота оновлень безпеки, рівень дотримання політик безпеки;
- підготовка до сертифікації, а саме підготовка відповідних документів, забезпечення наявності ключових співробітників, належне проведення внутрішніх аудитів.

Розроблено рекомендації щодо підтримки сертифікації СУІБ за ISO/IEC 27001, а саме:

- вчасне усунення виявлених значних і незначних невідповідностей;
- проведення щорічних наглядових аудитів;
- проведення ресертифікаційного аудиту з можливістю розширення області дії СУІБ та області аудиту;
- вибір акредитованих органів для сертифікації СУІБ.

На прикладі ТОВ «Бізнестехніка» помічено важливість комплексної стратегії по впровадженню стандарту ISO/IEC 27001 для сертифікації СУІБ, оскільки для більшості партнерів цей пункт є важливим. Це допомогло забезпечити успішне функціонування в сучасному інформаційному просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шарай. Р. О. Організація систем управління інформаційною безпекою. 2022. С. 1-3. URL: https://atestor.ua/uk/poleznye-stati/organizaciya-sistemi-upravlinnya-informaciinoyu-bezpekoyu/

2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник. Дніпро, ДДУВС, 2020. С. 104-110.

3. Чунарьова А.О., Чунарьов А.І. СУІБ на базі міжнародних стандартів серії ISO: навч. посібник. Київ, НАУ, 2021. С. 50-56.

4. Полторак В. І., Корзаченко О.В. Методологічні засади щодо вибору IDS/IPS для організації: монографія. Київ, КНЕУ, 2019. С. 4-8.

5. Яремчук Ю.Є., Павловський П.В., Катаєв В.С., Сінюгін В.В. Комплексні системи захисту інформації: навчальний посібник. Вінниця, ВНТУ, 2020. Розділ 1.2.2. С. 5-9.

6. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Official edition, 2022. С. 12-20.

7. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53). Official edition, 2021. С.10-35.

8. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Security Systems and Organizations. Release 5.1.1, 2023. С.10-55.

9. Christopher Anoruo. COBIT 2019 Framework. Governance and Management Objectives. ISACA, 2019. С. 5-20.

10. Steven De Haes and Wim Van Grembergen. Enterprise Governance of Information Technology. Achieving Alignment and Value, Featuring COBIT 5. Springer, 2021. С. 10-30.

11. Lisa M. Boyle, Paul Knag. A Guide to Healthcare Privacy and Security Law. (ISBN: 9781454859814). HIPAA, 2022. С. 24-39.

12. Про захист інформації в інформаційно-комунікаційних системах: ЗАКОН УКРАЇНИ від 16.12.2020 р. № № 3549-IX : станом на 16 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

13. Rayan Carter. General Data Protection Regulation (EU) 2019/679. ISBN: 9789403511450. Official Journal of the European Union, 2019. URL: https://gdpr-info.eu/

14. Cybersecurity Act. European Regulation on Cybersecurity. ISBN: 9789403513508. ENISA, 2021. С. 2-8.

15. Cyber Security Act. BSI, Federal office of cybersecurity, 2019. URL: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/Cyber-Security-Act/cyber-security-act_node.html

16. Steve G. Watkins. ISO/IEC 27001:2022. An introduction to information security and the ISMS standard (ISBN: 9781787784031). It-gp, 2022. С. 5-50.

17. Mastering ISO/IEC 27001. A 10-Step Guide to Seamless Implementation. PECB, 2022. URL: https://pecb.com/article/mastering-isoiec-27001-a-10-step-guide-to-seamless-implementation

18. Alan Calder. Nine Steps to Success: An ISO 27001 Implementation Overview. IT Governance Publishing, 2023. С. 23-44.

19. Alan Calder. The case for ISO 27001. IT Governance Publishing, 2020. С. 52-64.

20. Peltier T. R. Information Security Policies and Procedures: A Practitioner's Reference, 2019. С. 50-70.

21. A Guide to ISO 27001 Mandatory Documents. Hicomply, 2021. URL: https://hicomply.com/iso-27001/iso-27001-documentation

22. Dejan Kosutic. A Business Guide to Implementing ISO 27001 On Your Own. Advisera Expert Solutions Ltd, 2023. С. 30-40.

23. Key Performance Indicators (KPI). IT enterprise, 2023. URL: https://www.it.ua/knowledge-base/technology-innovation/key-performance-indicators-kpi

24. Snort IDS/IPS Explained: What - Why you need - How it works. Zenarmor, 2022. URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-snort

25. An IDS, IPS, SIEM Guide for the Non-Technical. Ntiva, 2024. URL: https://www.ntiva.com/blog/ids-ips-siem-decoded-for-non-techs

26. Bridget Kenyon. ISO 27001 controls – A guide to implementing and auditing. IT Governance Publishing, 2019. C. 32-45.

27. Abhishek Chopra and Mukund Chaudhary. Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines. Apress, 2019. C. 12-35.

28. Mastering ISO 27001 Internal Audits: A Step-by-Step Guide. IT Governance, 2022. C. 10-25.

29. Tipton H. F., Krause M. Information Security Management Handbook. Auerbach Publications, 2019. C. 75-100.

30. Mark Darby. Information Security Risk Management Explained ─ ISO 27001. ISMS.online, 2019. URL: https://www.isms.online/iso-27001/information-security-risk-management-explained/

31. Dejan Kosutic. ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide. Advisera, 2023. URL: https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/

32. How To Do Risk Assessment ISO 27001. SecureFrame, 2023. C. 14-37. URL: https://secureframe.com/hub/iso-27001/risk-assessment

33. ISO 27001 & the Risk Management Process. Apomatix, 2022. C. 45-67. URL: https://www.apomatix.com/blog/iso-27001-and-the-risk-management-process/

34. Alan Calder, Steve Watkins. Information Security Risk Management for ISO 27001/ISO 27002, Third edition. IT Governance, 2019. C. 29-38.

35. Dejan Kosutic. ISO 27001 certification - Everything you need to know about getting ISO 27001 certified. Advisera, 2023. URL: https://advisera.com/27001academy/iso-27001-certification/

36. ISO 27001 Certification: The Ultimate Guide To Success. Hightable, 2021. URL: https://hightable.io/iso-27001-certification/

37. ISO 27001 certification process. A step-by-step guide. Vanta, 2022. URL: https://www.vanta.com/collection/iso-27001/iso-27001-risk-assessment

38. Dejan Kosutic. ISO 27001 Implementation Guide: Checklist of Steps, Timing, and Costs involved. Advisera, 2023. URL: https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/

39. ISO 27001 – Implementation & Leadership Support. Standard Fusion, 2021. URL: https://www.standardfusion.com/blog/iso-27001-implementation-leadership-support/

40. What You Need To Know About Undertaking ISO 27001 Certification. Data Center Evolved, 2024. URL: https://www.databank.com/resources/blogs/what-you-need-to-know-about-undertaking-iso-27001-certification/

41. ISO 27001: 10 ways to achieve continual improvement. Evalian, 2023. URL: https://evalian.co.uk/iso-27001-10-ways-to-achieve-continual-improvement/

42. Information Security Management courses ISO/IEC 27001 Training. DSI, 2024. URL: https://www.bsigroup.com/en-US/ISO-IEC-27001-Information-Security/Training-courses-for-ISO-27001/

43. ISO 27001 Security Awareness Training: A Complete Guide. Guardey, 2023. URL: https://www.guardey.com/iso27001-security-awareness-training/

ДОДАТКИ

ДОДАТОК А

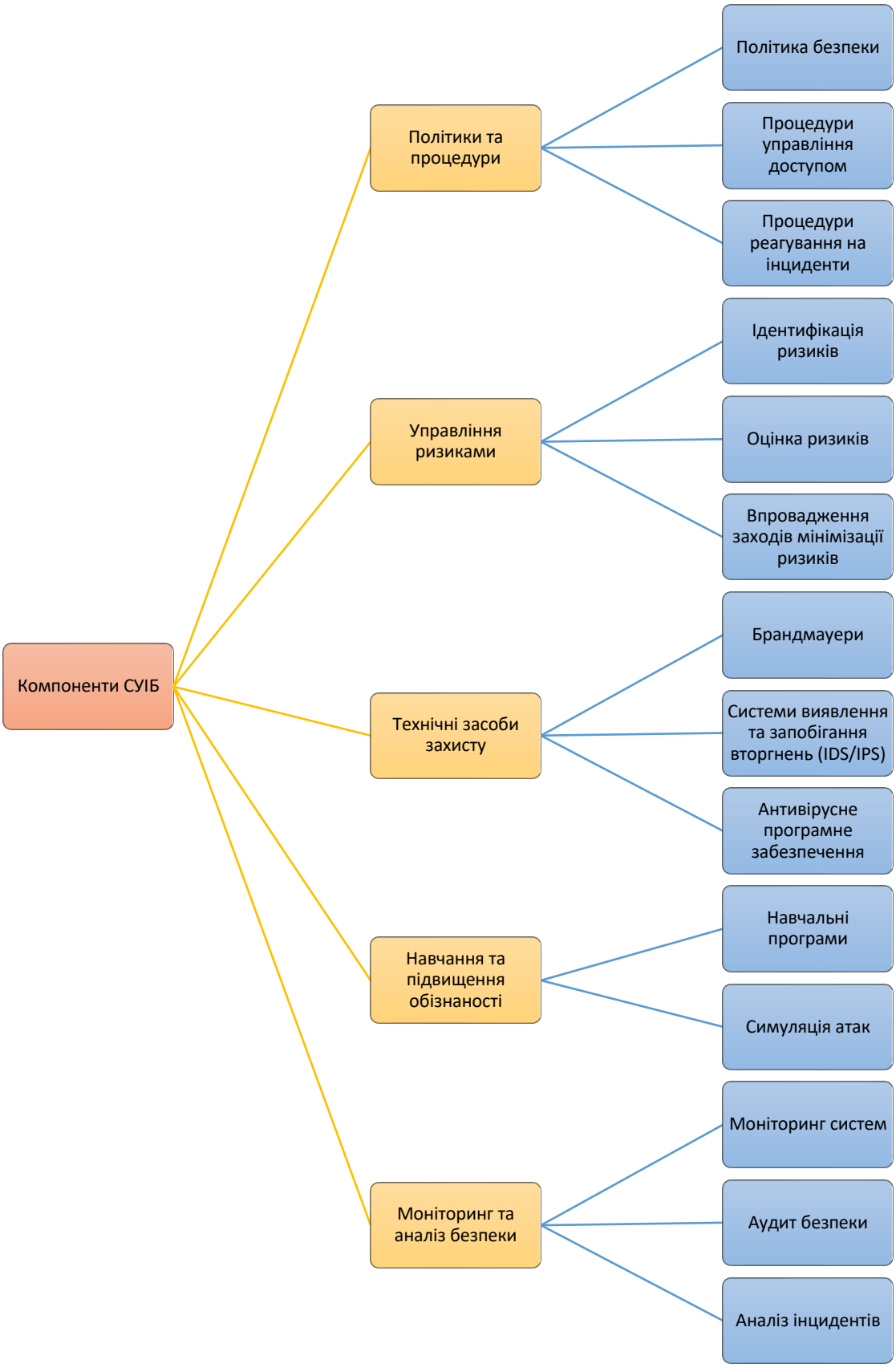

Рис. А.1. Компоненти СУІБ

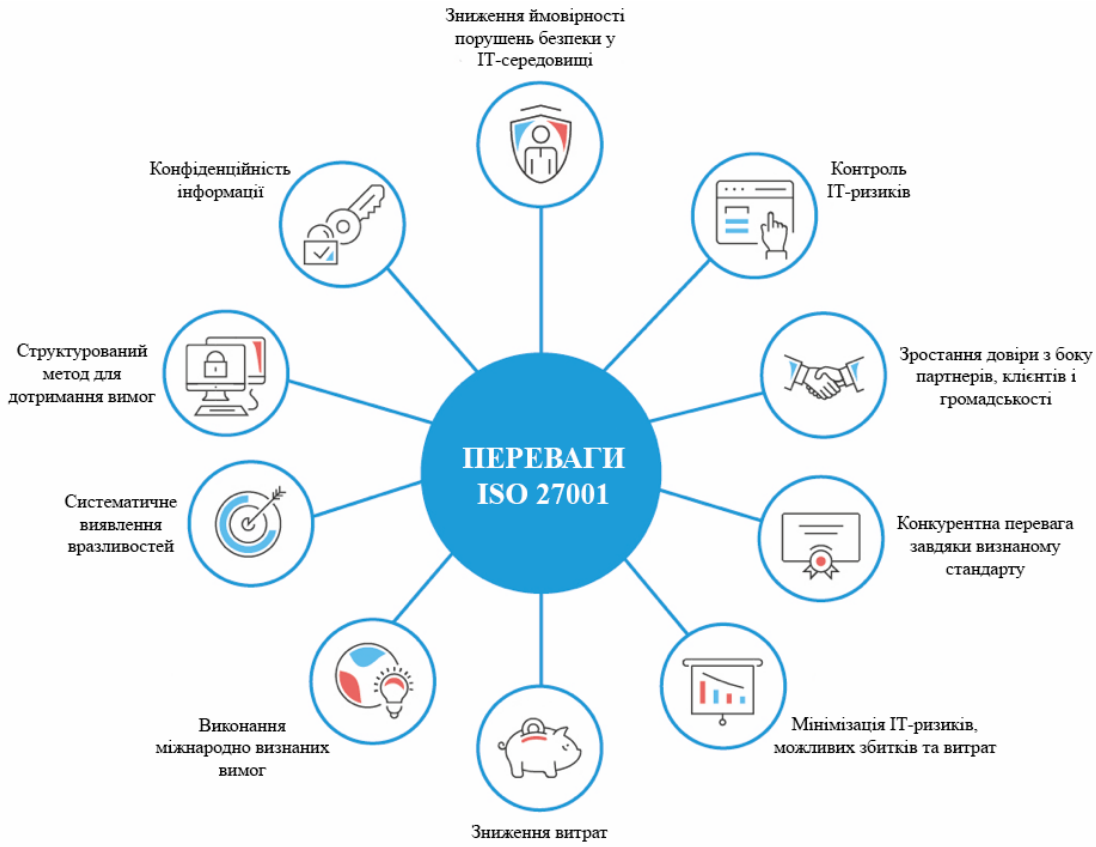

Рис. А.2. Переваги стандарту ISO/IEC 27001

Рис. А.3. План впровадження NIST SP 800-53