МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ МЕТОДИКА ВПРОВАДЖЕННЯ СТАНДАРТІВ ISO/IEC 27001 У СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ”

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

_____ Олександр ЛОЗА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Олександр Лоза
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Юрій ПЕПА
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лозі Олександру Дмитровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методика впровадження стандартів ISO/IEC 27001 у системи управління інформаційною безпекою”,
керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, к.т.н., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, міжнародні стандарти, наукова та технічна література.*
4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати сучасний стан систем управління інформаційною безпекою.
   4.2. Проаналізувати вимоги та принципи стандарту ISO/IEC 27001.
   4.3. Розробити методику впровадження стандарту в системи управління інформаційною безпекою.
   4.4. Оцінити ефективність впровадження стандарту в системи управління інформаційною безпекою.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз сучасний стан систем управління інформаційною безпекою	08.04.2025	
4.	Дослідження вимог та принципів стандарту ISO/IEC 27001	15.04.2025	
5.	Розробити методику впровадження стандарту в системи управління інформаційною безпекою та оцінити ефективність її впровадження	29.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	15.05.2025	
7.	Оформлення роботи.	22.05.2025	
8.	Оформлення презентації.	29.05.2025	
9.	Отримання рецензії на роботу.	05.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Олександр ЛОЗА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Лоза О.Д. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Методика впровадження стандартів ISO/IEC 27001 у системи управління інформаційною безпекою ”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ЛОЗА Олександр у кваліфікаційній роботі проаналізував загрози інформаційній безпеці та сучасні підходи до її управління, вивчив вимоги та принципи стандарту ISO/IEC 27001, розробив методику впровадження стандарту в систему управління інформаційною безпекою, яка включає, яка включає аналіз ризиків, розробку політик та процедур безпеки, вибір інструментів для підтримки СУІБ та оцінку та оцінив ефективність впровадження.

ЛОЗА Олександр показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЛОЗИ Олександра на оцінку “відмінно” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Лоза О.Д. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувач вищої освіти ЛОЗА Олександр
на тему “ Методика впровадження стандартів ISO/IEC 27001 у системи управління інформаційною безпекою ”

Актуальність. В умовах стрімкої цифровізації бізнесу та зростання кіберзагроз, забезпечення інформаційної безпеки є критично важливим для будь-якої організації. Стандарти ISO/IEC 27001 відіграють ключову роль у побудові ефективних систем управління інформаційною безпекою (СУІБ). Дослідження методик впровадження цих стандартів є актуальним завданням, особливо в контексті адаптації до специфічних потреб підприємств та постійних змін у ландшафті кіберзагроз.

Позитивні сторони.

1. У роботі проведено ґрунтовний аналіз існуючих систем управління інформаційною безпекою та загроз.
2. Кваліфікаційна робота має чітку структуру, виклад матеріалу логічний та послідовний. Автором продемонстровано розуміння ключових концепцій та вимог стандарту ISO/IEC 27001.
3. У роботі запропоновано структуровану методику впровадження стандарту ISO/IEC 27001, яка включає аналіз ризиків, розробку політик та процедур безпеки, вибір інструментів для підтримки СУІБ та оцінку ефективності впроваджених заходів.
4. Автором опрацьовано значну кількість літературних джерел, що свідчить про глибоке дослідження теми.

Недоліки.

Вважаю, що розділ, присвячений вибору інструментів для підтримки СУІБ, міг би бути розширений. Зокрема, доцільно було б надати більш детальний огляд сучасних систем управління ризиками, SIEM-систем та засобів моніторингу, їх порівняльний аналіз та критерії вибору.

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

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

Рецензент: _____ Юрій Пепа
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методики впровадження міжнародного стандарту ISO/IEC 27001:2022 у систему управління інформаційною безпекою підприємства. Робота складається зі вступу, чотирьох розділів, що містять 6 рисунків, висновків і списку використаних джерел із 62 найменувань. Загальний обсяг роботи становить 71 аркуш, з яких 8 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка та обґрунтування методики впровадження ISO/IEC 27001:2022 у СУІБ організації.

Об'єктом дослідження є процеси управління інформаційною безпекою.

Предмет дослідження – методи, інструменти та етапи впровадження стандарту.

Методи дослідження. Застосовано системний аналіз, порівняння, класифікацію, аналіз ризиків, вивчення нормативної бази та практичний досвід.

В роботі проаналізовано підходи до СУІБ, вимоги ISO/IEC 27001, управління активами, ризиками, інцидентами та політики безпеки.

Як результат у роботі Проаналізовано сучасний стан систем управління інформаційною безпекою, вимоги та принципи стандарту ISO/IEC 27001; Розробив методику впровадження стандарту в системи управління інформаційною безпекою та оцінив ефективність впровадження стандарту.

Галузь застосування. Результатом є структурована методика впровадження СУІБ за ISO/IEC 27001:2022 з урахуванням специфіки підприємства. Результати будуть використанні при створенні/модернізації СУІБ для відповідності стандартам при проведенні сертифікації.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ISO/IEC 27001, СИСТЕМА УПРАВЛІННЯ, ПОЛІТИКА БЕЗПЕКИ, УПРАВЛІННЯ РИЗИКАМИ, СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ABSTRACT

Qualification work is dedicated to the study of the methodology for implementing the international standard ISO/IEC 27001:2022 in the enterprise information security management system. The work consists of an introduction, four chapters, conclusions, and a list of references with 62 titles. The total volume of the work is 64 pages, of which 8 pages are occupied by the list of abbreviations and the list of references.

The aim of the work is to develop and justify the methodology for implementing ISO/IEC 27001:2022 in the organization's ISMS.

The object of the study is the processes of information security management.

The subject of the study is the methods, tools, and stages of standard implementation.

Research methods. System analysis, comparison, classification, risk analysis, study of regulatory framework, and practical experience were applied.

The work analyzes approaches to ISMS, ISO/IEC 27001 requirements, asset management, risks, incidents, and security policies.

As a result, the work analyzes the current state of information security management systems, the requirements and principles of the ISO/IEC 27001 standard; develops a methodology for implementing the standard in information security management systems and evaluates the effectiveness of standard implementation.

Application area. The result is a structured methodology for implementing ISMS according to ISO/IEC 27001:2022, taking into account the specifics of the enterprise. The results will be used in the creation/modernization of ISMS to comply with standards during certification.

Keywords: INFORMATION SECURITY, ISO/IEC 27001, MANAGEMENT SYSTEM, SECURITY POLICY, RISK MANAGEMENT, INFORMATION SECURITY STANDARDS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

APT	Розвинена постійна загроза (Advanced Persistent Threat)
CIA	Принципи конфіденційності, цілісності та доступності (Confidentiality, Integrity, Availability)
CISA	Агентство з кібербезпеки та інфраструктурної безпеки США (Cybersecurity and Infrastructure Security Agency)
DLP	Захист від витоків даних (Data Loss Prevention)
DoS/DDoS	Відмова в обслуговуванні
GDPR	Загальний регламент про захист даних
ISMS	Система управління інформаційною безпекою (СУІБ)
NIST RMF	Рамкова модель управління ризиками Національного інституту стандартів і технологій США
OCTAVE	Методика оцінки загроз, активів і вразливостей (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
PDCA	Цикл покращення: Плануй–Роби–Перевіряй–Дій (Plan–Do–Check–Act)
SIEM	Система управління інформацією та подіями безпеки (Security Information and Event Management)
SOC	Центр моніторингу безпеки (Security Operations Center)
VPN	Віртуальна приватна мережа (Virtual Private Network)

ВСТУП

Актуальність теми. Сучасний світ дедалі більше залежить від інформаційних технологій, а отже й від надійності, захищеності та цілісності інформаційних систем, які забезпечують безперервність функціонування бізнес-процесів, державних установ та критичної інфраструктури. У зв'язку з цим проблематика інформаційної безпеки набула ключового значення для будь-якої організації, незалежно від галузі чи масштабу діяльності [1]. В епоху цифрових трансформацій, коли обсяги даних стрімко зростають, а кількість кіберзагроз постійно еволюціонує [2], зростає потреба у впровадженні систем управління інформаційною безпекою, що базуються на визнаних міжнародних стандартах.

Одним із найбільш авторитетних та поширених стандартів у сфері управління інформаційною безпекою є ISO/IEC 27001. Цей стандарт встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Він надає організаціям чітку методологію, яка дозволяє не лише ефективно керувати інформаційними ризиками, а й демонструвати свою відповідність вимогам безпеки перед партнерами, замовниками, аудиторами та регуляторними органами. В умовах зростання регуляторного тиску та юридичної відповідальності за порушення конфіденційності даних, дотримання вимог стандарту ISO/IEC 27001 стає важливим фактором забезпечення довіри та стійкості організації.

Питання впровадження ISO/IEC 27001 набуває особливої актуальності в українському контексті, де організації стикаються не лише з загальносвітовими кіберзагрозами, а й з унікальними ризиками, пов'язаними з гібридною війною, кібератаками на державні та комерційні структури, а також обмеженими ресурсами на впровадження комплексних заходів захисту. На фоні цих викликів особливу цінність мають структуровані, адаптовані до місцевих умов методики, що дозволяють ефективно інтегрувати вимоги стандарту у практику управління безпекою.

Метою дослідження є розробка методики впровадження стандартів ISO/IEC 27001 для створення, підтримки та вдосконалення системи управління інформаційною безпекою в організації з урахуванням сучасних кіберзагроз та нормативних вимог. Така методика має сприяти не лише технічному та організаційному впровадженню положень стандарту, а й формуванню корпоративної культури безпеки, що включає залучення персоналу, управління інцидентами, проведення внутрішніх аудитів і постійне вдосконалення процедур.

Об'єктом дослідження є процеси управління інформаційною безпекою в організаціях, які відповідають або прагнуть відповідати стандарту ISO/IEC 27001. Ці процеси охоплюють широкий спектр дій – від оцінки ризиків і розробки політик до контролю за виконанням заходів та аналізу результатів.

Предметом дослідження є методи, підходи та інструменти впровадження ISO/IEC 27001 у систему управління інформаційною безпекою.

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

1. Проаналізувати сучасний стан систем управління інформаційною безпекою.

2. Проаналізувати вимоги та принципи стандарту ISO/IEC 27001.

3. Розробити методику впровадження стандарту в системи управління інформаційною безпекою.

4. Оцінити ефективність впровадження стандарту.

Особлива увага приділяється аналізу ризиків, формуванню політик безпеки, процедурі аудиту відповідності та вибору ефективних заходів з кіберзахисту. Дослідження також охоплює питання оцінки ефективності впроваджених заходів та рекомендацій щодо подальшого розвитку СУІБ [3] у контексті зростаючих викликів цифрового середовища.

Дослідження базується на комплексному підході, який поєднує аналіз нормативних документів, методів управління ризиками, інструментів технічного та організаційного характеру, а також практичного досвіду впровадження стандартів інформаційної безпеки в різних організаціях.

Методи дослідження. Для досягнення мети використовуються методи системного аналізу, порівняльного аналізу, моделювання процесів, експертного оцінювання, а також емпіричні методи, що базуються на дослідженні конкретного прикладу впровадження.

Практичне значення одержаних результатів роботи полягає у створенні адаптованої до сучасних українських реалій методики впровадження стандарту ISO/IEC 27001, яка може бути використана підприємствами, установами та організаціями для підвищення рівня захищеності інформаційних активів. Запропоновані в роботі підходи дозволяють не лише скоротити ризики кіберінцидентів, а й забезпечити стійке функціонування організацій в умовах цифрової трансформації та зростаючої залежності від інформаційних технологій.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

РОЗДІЛ 1 АНАЛІЗ СТАНУ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Основні загрози інформаційній безпеці організацій

У сучасному цифровому світі інформація стала одним з найцінніших ресурсів організацій. Її захист є пріоритетним завданням для керівництва, технічних спеціалістів і фахівців з інформаційної безпеки [4]. З розвитком технологій та зростанням залежності від інформаційних систем збільшується і кількість загроз, що здатні порушити цілісність, конфіденційність і доступність інформаційних активів [5]. Ці загрози можуть мати різне походження, рівень складності, вплив на організацію, але всі вони створюють суттєві ризики, які потребують ретельного аналізу та управління.

Серед найпоширеніших загроз інформаційній безпеці організацій слід виокремити зовнішні атаки з боку кіберзлочинців, які спрямовані на отримання несанкціонованого доступу до корпоративних ресурсів [6]. Напади типу DoS/DDoS, фішинг, експлуатація вразливостей у програмному забезпеченні, розповсюдження шкідливого коду та використання соціальної інженерії є лише частиною арсеналу сучасного зловмисника. Кібератаки стають дедалі складнішими, часто організовуються на високому професійному рівні, мають політичне, економічне або промислове підґрунтя. Такі атаки не лише спричиняють втрати даних, а й можуть паралізувати роботу компанії, нанести репутаційної шкоди [7], призвести до фінансових збитків або штрафів за порушення законодавства [8].

Внутрішні загрози також є значною складовою ризиків для інформаційної безпеки. Найбільш небезпечними вважаються інсайдери – співробітники, які мають доступ до критичних систем і навмисно або ненавмисно порушують встановлені правила. Причиною таких порушень можуть бути недбалість, невдоволення умовами праці, бажання отримати вигоду або відсутність належного контролю. Навіть несвідомі дії персоналу, наприклад відкриття

фішингового листа чи використання незахищеного носія, можуть спричинити серйозні наслідки. Велику загрозу становить недостатня обізнаність працівників у сфері безпеки та відсутність культури захисту інформації в організації.

Технічні вразливості, пов'язані з неправильним налаштуванням систем, застарілим програмним забезпеченням, використанням слабких паролів або відсутністю багатофакторної аутентифікації, відкривають додаткові можливості для зловмисників. Часто такі вразливості залишаються невиявленими впродовж тривалого часу, що дає змогу хакерам безперешкодно діяти в межах корпоративної мережі. Коли організація не виконує регулярне оновлення програмного забезпечення або ігнорує рекомендації з безпеки, рівень ризику зростає в геометричній прогресії.

Організації також стикаються із загрозами, що виникають через взаємодію з постачальниками, підрядниками та партнерами. Використання хмарних сервісів, інтеграція з зовнішніми платформами, спільне оброблення даних – усе це потребує ретельного контролю, перевірки безпеки зовнішніх систем, аудитів третьої сторони [9]. Недостатній рівень захисту у контрагентів може стати причиною проникнення в основну систему організації, оскільки ланцюг безпеки є настільки сильним, наскільки захищено його найслабшу ланку.

Також варто враховувати загрози фізичної безпеки – несанкціонований доступ до серверних приміщень, крадіжки носіїв інформації, природні катастрофи, пожежі та інші події, що можуть знищити або пошкодити інформаційні ресурси. Без комплексного підходу до безпеки, який охоплює як цифрові, так і фізичні аспекти, неможливо гарантувати захищеність організації в цілому.

Сучасні організації змушені враховувати і регуляторні загрози – вплив міжнародного та національного законодавства на правила обробки, зберігання та захисту інформації. Недотримання таких вимог, як GDPR, ISO/IEC 27001 або національні нормативні акти [10], може призвести до юридичних санкцій, втрати ліцензій або дискредитації на ринку.

Зростаюча складність інформаційного середовища, поява нових векторів атак, людський фактор та обмежені ресурси організацій роблять завдання управління загрозами надзвичайно складним. Без системного підходу, який базується на сучасних методологіях, стандартах і технологічних рішеннях, забезпечення інформаційної безпеки стає неможливим. Саме з цієї причини впровадження стандарту ISO/IEC 27001 є надзвичайно важливим кроком, оскільки він дозволяє побудувати системний підхід до виявлення, аналізу та мінімізації загроз, що постійно змінюються.

Особливої уваги заслуговують загрози, пов’язані з цілеспрямованими атаками на конкретні об'єкти, які відомі як APT. Це складні, довготривалі атаки, за якими часто стоять добре організовані угруповання, що мають значні ресурси та глибокі технічні знання. Вони спрямовані на проникнення в інформаційні системи [34] для отримання доступу до стратегічно важливої інформації, промислових секретів, персональних даних або елементів інфраструктури. Такі атаки можуть залишатися непоміченими місяцями, використовувати комбінації методів проникнення і утримувати контроль над системою навіть після виявлення. Вони несуть особливу небезпеку для критично важливих об’єктів, державних установ, фінансових структур та підприємств оборонного сектору.

У контексті цифрової трансформації варто звернути увагу на загрози, пов’язані з Інтернетом речей. Зростання кількості підключених до мережі пристроїв створює нові вектори атак, оскільки багато з них мають обмежені функції безпеки, відкриті порти або стандартні паролі, які не змінюються після встановлення. Зловмисники можуть використовувати такі пристрої для організації ботнет-мереж, збирання інформації або проникнення у внутрішню мережу організації. Недостатній рівень захисту IoT-пристроїв часто стає ключовим фактором успішності атаки, оскільки їх важко контролювати централізовано, а механізми оновлення часто відсутні або не застосовуються вчасно.

Інформаційні системи стають мішенню не лише для професійних хакерів, а й для недержавних акторів, які переслідують ідеологічні, політичні або

деструктивні цілі. Хактивісти можуть атакувати ресурси організацій, які, на їхню думку, порушують етичні норми, або з метою публічного тиску. Такі атаки можуть супроводжуватись витоками конфіденційної інформації та блокуванням послуг. Наслідки подібної активності негативно впливають на імідж компанії, призводять до втрати довіри клієнтів, скорочення ринкової частки та зниження капіталізації.

Інформаційна безпека також опиняється під загрозою через недоліки в управлінні життєвим циклом програмного забезпечення. Якщо в процесі розробки не враховуються вимоги до захищеності, у коді залишаються критичні вразливості. Публікація вихідного коду, використання відкритих бібліотек без перевірки, недостатнє тестування призводять до появи точок входу для зловмисників. Впровадження незахищеного програмного забезпечення [11] в інфраструктуру організації створює потенційну загрозу, яка може реалізуватися у будь-який момент.

Також слід згадати про загрози, пов’язані з людським фактором на рівні прийняття управлінських рішень. Керівники організацій не завжди мають належну підготовку в питаннях інформаційної безпеки, що призводить до хибної оцінки ризиків або відмови від інвестування у відповідні заходи. Відсутність підтримки з боку топ менеджменту часто стає перешкодою на шляху до побудови ефективної системи захисту. Недостатнє фінансування, нехтування політиками безпеки [12], пріоритетність комерційних інтересів над питаннями захисту інформації створюють сприятливе середовище для реалізації загроз.

Ще одним джерелом небезпеки є техногенні та природні катастрофи, які можуть порушити роботу інформаційної інфраструктури. Пожежі, повені, перебої з електропостачанням, землетруси чи інші форс-мажорні обставини можуть призвести до втрати даних, пошкодження серверів, порушення ланцюгів зв'язку. Відсутність планів реагування на надзвичайні ситуації, бекапів або систем резервування ускладнює відновлення роботи і підвищує вразливість до зовнішніх впливів.

Сукупність усіх вищезазначених факторів формує складне і динамічне середовище, в якому організаціям доводиться функціонувати. Постійна зміна ландшафту загроз, поява нових технологій, зростаючі очікування клієнтів і жорсткі нормативні вимоги вимагають від підприємств розробки гнучких, масштабованих та стандартизованих рішень, які здатні забезпечити ефективне управління ризиками. Впровадження стандарту ISO/IEC 27001 дає змогу структурувати процес захисту, ідентифікувати критичні активи, визначити пріоритети, виявити загрози та реалізувати необхідні контрзаходи. Це створює фундамент для формування зрілої системи управління інформаційною безпекою, здатної протистояти сучасним викликам.

Поява нових технологій, зокрема штучного інтелекту, машинного навчання, блокчейн-рішень та автоматизованих систем прийняття рішень, створює нові виклики для інформаційної безпеки. Інструменти на основі штучного інтелекту здатні як посилити захист [13], так і бути використані зловмисниками для обходу традиційних засобів контролю.

Автоматизовані системи аналізу можуть допомагати у виявленні аномалій, однак у разі компрометації або неправильного налаштування самі стають джерелом загрози. Неправильно реалізовані алгоритми, навчання моделей на некоректних або маніпульованих даних, відсутність контролю за процесами ухвалення рішень – усе це може призвести до втрати контролю над критичними процесами та даними.

Варто звернути увагу на зростаючу кількість атак на критичну інфраструктуру, включаючи енергетичні, транспортні, фінансові, телекомунікаційні та медичні системи. Такі атаки можуть мати катастрофічні наслідки не лише для окремих організацій, а й для цілих регіонів або держав. Збільшення масштабів цифрової взаємозалежності між секторами економіки означає, що порушення функціонування в одній галузі може спричинити каскадні наслідки в інших. Стратегії кібербезпеки [14] повинні враховувати ці аспекти та передбачати заходи з між секторального реагування.

Загрози, пов’язані з обробкою персональних даних, набувають особливого значення у зв’язку з підвищенням уваги суспільства до захисту приватності. Організації, які збирають, зберігають або обробляють персональні дані клієнтів, співробітників, партнерів, зобов’язані забезпечити їхню цілісність і недоторканність. Витоки персональних даних, як правило, призводять до серйозних фінансових і репутаційних втрат. Джерелом таких витоків можуть бути не лише зовнішні атаки, а й неналежне поводження з інформацією всередині організації – зберігання даних без шифрування, передача через незахищені канали, надання доступу без обґрунтованої потреби.

Ще одним серйозним ризиком є використання застарілого обладнання або програмного забезпечення, яке більше не підтримується виробниками. Така техніка не отримує оновлень безпеки, має обмежену сумісність із сучасними засобами захисту, що робить її легкою ціллю для атак. Організації часто не оновлюють своє обладнання з міркувань економії, не усвідомлюючи масштабу загроз, які виникають через цю практику. Відсутність планування життєвого циклу IT-інфраструктури, недостатній моніторинг активів і неефективне управління конфігураціями призводять до поступового накопичення вразливостей, які рано чи пізно будуть експлуатовані.

Зміна характеру трудових процесів, перехід до віддаленої роботи і використання персональних пристроїв (BYOD) стали ще однією причиною зростання загроз. Коли працівники використовують власні ноутбуки, смартфони або інші пристрої для виконання службових обов’язків, організація втрачає повний контроль над середовищем, у якому обробляються її дані. Відсутність корпоративного антивірусу, брандмауера, захищених каналів зв'язку, контролю доступу – все це призводить до збільшення ризиків [15,16]. Без належної політики безпеки та її дотримання співробітниками організація втрачає здатність оперативно реагувати на інциденти.

Соціальні мережі, месенджери, публічні хмари – ще одна категорія платформ, які активно використовуються в діловій комунікації, але при цьому залишаються зоною високого ризику. Через ці канали може відбуватися витік

інформації, фішинг, пересилання шкідливих файлів, несанкціонований доступ до службових ресурсів. Практика використання неофіційних каналів для обговорення важливих питань створює додаткові труднощі в контролі за інформаційними потоками.

Уся сукупність загроз, з якими стикаються організації, вимагає не лише технічних, а й організаційних рішень. Створення чіткої структури управління інформаційною безпекою, проведення навчання для співробітників, впровадження стандартів захисту, регулярна оцінка ризиків, застосування автоматизованих засобів моніторингу – це лише частина відповідей на сучасні виклики. Системний підхід до аналізу загроз і побудова ефективної стратегії управління ризиками дає змогу забезпечити стабільність роботи організації, зберегти її репутацію та відповідати вимогам сучасного цифрового середовища.

1.2 Підходи до управління інформаційною безпекою та міжнародні стандарти

Управління інформаційною безпекою стало стратегічним елементом діяльності сучасних організацій, оскільки порушення захисту інформаційних активів несе серйозні фінансові, репутаційні та правові наслідки [17]. З огляду на це, сформувалися різноманітні підходи до забезпечення безпеки інформації, які базуються на принципах системного аналізу, управління ризиками, політиках доступу, стандартизації процесів і постійному моніторингу. Ці підходи мають на меті побудову такої системи безпеки, яка здатна не лише захистити від існуючих загроз, а й адаптуватися до нових умов, реагувати на інциденти, мінімізувати наслідки порушень і забезпечити стійкість організації.

Одним із фундаментальних підходів є концепція управління ризиками. Її суть полягає у виявленні, аналізі та оцінці ризиків, які можуть вплинути на інформаційні ресурси, та реалізації заходів для їхнього мінімізації до прийнятного рівня. Управління ризиками передбачає чітке розуміння того, які активи є критичними, які загрози можуть бути на них спрямовані, якими є

вразливості в існуючій інфраструктурі [18], а також які можуть бути наслідки реалізації ризиків. Цей підхід дозволяє зосередити зусилля на найнебезпечніших аспектах, раціонально розподіляти ресурси і приймати обґрунтовані рішення щодо пріоритетів у сфері захисту інформації.

Іншим важливим підходом є впровадження політик безпеки, які регламентують поведінку співробітників, порядок доступу до інформаційних систем, зберігання і передачу даних, відповідальність за порушення правил. Політики безпеки створюють єдині правила гри всередині організації, підвищують обізнаність персоналу і формують культуру відповідального ставлення до інформації. Чітко прописані правила дозволяють знизити ризики випадкових помилок, несанкціонованого доступу, витоку конфіденційної інформації або навмисного порушення встановлених норм.

Технологічна складова управління безпекою включає застосування засобів контролю доступу, антивірусного захисту, міжмережевий екран (Firewall), засобів шифрування, систем виявлення вторгнень, моніторингу подій, аналізу логів, резервного копіювання та інших інструментів, які забезпечують технічну реалізацію політик і процедур [19]. Усі ці засоби повинні працювати як єдина система, інтегруючись у загальну архітектуру безпеки організації. Технології не є самодостатніми – їх ефективність залежить від того, наскільки правильно вони впроваджені, підтримуються та інтегровані у бізнес-процеси.

На рівні глобального регулювання і стандартизації ключову роль відіграють міжнародні стандарти, які визначають найкращі практики у сфері інформаційної безпеки. Одним із найвідоміших і найавторитетніших є стандарт ISO/IEC 27001, який встановлює вимоги до створення, впровадження, експлуатації, моніторингу, аналізу, підтримки та вдосконалення системи управління інформаційною безпекою. Він орієнтований на принцип циклічного процесу управління (PDCA), що дозволяє організації постійно вдосконалювати свою систему захисту. ISO/IEC 27001 визначає обов’язкові елементи СУІБ, серед яких політики безпеки, управління ризиками, оцінка відповідності, внутрішній

аудит, реагування на інциденти та інші компоненти, що мають бути документально зафіксовані та інтегровані у структуру управління.

До інших поширених стандартів і підходів належать NIST Cybersecurity Framework, COBIT, ITIL, PCI DSS, CIS Controls, які розроблені для різних сфер і потреб. Наприклад, NIST CSF широко використовується у США і базується на п’яти ключових функціях: ідентифікація, захист, виявлення, реагування та відновлення. Він пропонує набір гнучких і адаптивних заходів, які організація може застосувати відповідно до свого профілю ризику. COBIT орієнтований на управління IT-процесами з акцентом на цілісність бізнесу, а ITIL фокусується на управлінні IT-послугами. Кожен з цих підходів має власну методологію, документообіг і філософію, але всі вони визнають необхідність системного підходу, який інтегрує безпеку в усі рівні організаційної діяльності.

У межах Європейського Союзу особливу роль відіграє загальний регламент захисту персональних даних (GDPR), який встановлює жорсткі вимоги до зберігання, обробки і передачі персональної інформації. Його дотримання вимагає від організацій впровадження низки технічних і організаційних заходів безпеки, документального підтвердження дій, ведення реєстрів обробки даних, підготовки до інцидентів порушення захисту та інформування про них національних органів і суб’єктів даних.

У контексті інтеграції в міжнародне співтовариство та підвищення рівня кіберзахисту в Україні також активно впроваджуються міжнародні стандарти. Національні нормативні документи поступово гармонізуються з ISO/IEC 27001, NIST, GDPR та іншими міжнародними вимогами. Це дозволяє організаціям діяти відповідно до світових практик, брати участь у міжнародних проєктах, відповідати умовам співпраці з партнерами з інших країн та демонструвати високий рівень відповідальності за захист інформації.

Сучасні підходи до управління інформаційною безпекою ґрунтуються на розумінні, що ефективний захист можливий лише в умовах цілісної системи, яка враховує як технічні, так і організаційні аспекти, а також поведінкові чинники. Вони мають спиратися на стандартизовані процеси, постійне оновлення знань,

адаптацію до змін і побудову зрілої корпоративної культури безпеки. Тільки за наявності таких умов можна досягти належного рівня інформаційної стійкості і готовності до реагування на нові виклики.

Особливу роль у формуванні підходів до управління інформаційною безпекою відіграє концепція «захисту в глибину», яка передбачає створення багаторівневої системи оборони. Кожен рівень такої системи виконує окрему функцію, і навіть у випадку, коли одна лінія захисту буде зламана, інші залишаються здатними стримувати розвиток загрози або мінімізувати її наслідки. Це включає фізичний контроль доступу, обмеження на рівні мережі, захист кінцевих точок, криптографічний захист даних, моніторинг дій користувачів, реагування на інциденти та навчання персоналу. Такий підхід дозволяє будувати гнучкі системи, які можуть бути адаптовані під реальні потреби організації і її ризик-профіль.

Формування ефективної системи управління інформаційною безпекою вимагає інтеграції безпекових процесів у всі етапи життєвого циклу інформаційних систем – від проектування до експлуатації та виведення з обігу. Це означає, що безпека має враховуватися вже на етапі планування архітектури, вибору платформ, розробки програмного забезпечення, створення політик доступу і бізнес-логіки. Такий підхід часто називають «безпека за задумом» (security by design). Він дозволяє виявляти та усувати потенційні вразливості до того, як система буде введена в експлуатацію, а не вже після виявлення інциденту. Багато сучасних стандартів безпеки підтримують цю ідею, закликаючи до створення інфраструктури, де безпека є частиною проєктного мислення, а не реакцією на зовнішні чинники.

Надзвичайно важливою складовою підходів до управління інформаційною безпекою є забезпечення безперервності бізнесу та відновлення після надзвичайних ситуацій. Організація повинна мати плани дій у разі збоїв у роботі інформаційних систем, кібератак, втрати даних або знищення фізичної інфраструктури. Ці плани включають чітко визначені ролі, відповідальність,

канали комунікації, процедури резервного копіювання, відновлення даних, перевірку цілісності систем після інциденту.

Спроможність організації швидко відновити свою діяльність після кризи є важливим показником зрілості системи управління інформаційною безпекою. Міжнародні стандарти, зокрема ISO/IEC 27031 та ISO 22301, надають структуру і рекомендації для формування такої здатності.

Ще одним критичним напрямом у підходах до управління інформаційною безпекою є людський фактор. Велика частина інцидентів спричинена діями працівників, які не дотримуються політик безпеки, нехтують правилами доступу або стають жертвами соціальної інженерії. Підвищення обізнаності персоналу, регулярне навчання, симуляції фішингових атак, тестування знань із безпеки є обов'язковими елементами ефективного захисту. Навіть найдосконаліші технічні рішення не зможуть гарантувати безпеку, якщо співробітники не володіють навичками розпізнавання загроз або не розуміють наслідків своїх дій. Підходи, орієнтовані на розвиток культури інформаційної безпеки, передбачають не лише освітні заходи, а й формування корпоративної політики, яка підтримує відкритий діалог, взаємодію між підрозділами, залучення керівництва до процесів безпеки.

Усі сучасні підходи до управління інформаційною безпекою сходяться на тому, що ефективна система має бути динамічною, адаптивною, інтегрованою та керованою. Її основою є нормативно-правова база, стандарти, внутрішні політики, процедури, навчання, технічні засоби і регулярна оцінка результатів. Такий підхід дозволяє будувати середовище, в якому інформація захищена на кожному етапі свого життєвого циклу, де кожен учасник процесу усвідомлює свою роль у системі захисту, а всі дії базуються на принципах прозорості, відповідальності та безперервного вдосконалення.

1.3 Огляд стандарту ISO/IEC 27001: структура, основні вимоги та принципи

Стандарт ISO/IEC 27001 є фундаментальним документом у сфері інформаційної безпеки, який визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою в організації. Його цінність полягає в уніфікації підходів до захисту інформаційних активів незалежно від типу, розміру чи сфери діяльності організації. Стандарт забезпечує рамкову структуру, яка дозволяє адаптувати заходи безпеки до конкретних умов підприємства, базуючись на принципах управління ризиками та безперервного вдосконалення.

ISO/IEC 27001 належить до серії стандартів ISO/IEC 27000, які охоплюють різні аспекти інформаційної безпеки, але саме 27001 є сертифікаційним стандартом, тобто організація, яка його впроваджує, може пройти аудит і отримати офіційне підтвердження відповідності. Це відкриває нові можливості для бізнесу, включаючи участь у міжнародних тендерах, зміцнення довіри партнерів і клієнтів, демонстрацію дотримання найвищих стандартів у сфері безпеки.

Структура стандарту базується на моделі PDCA, що передбачає чотири основні фази: планування, реалізація, перевірка та дія (Рис. 1.2).

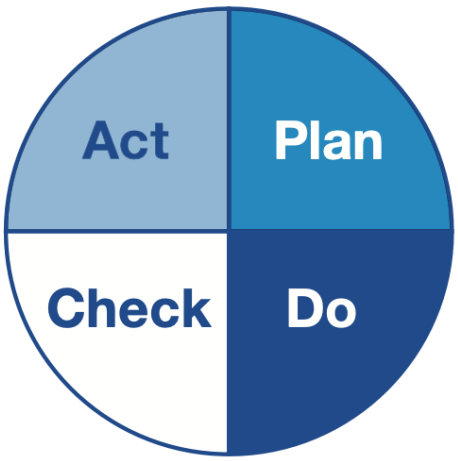

Рис. 1.2. PDCA

На етапі планування визначаються цілі інформаційної безпеки, формуються політики, аналізуються ризики, ідентифікуються активи та загрози, а також встановлюються методи управління ризиками. Наступна фаза включає реалізацію заходів, що були визначені на попередньому етапі, впровадження контролів, навчання персоналу, розробку процедур і технічне забезпечення захисту. Після цього слідує перевірка, яка охоплює внутрішні аудити, моніторинг подій, оцінку результатів і виявлення відхилень. Завершальний етап полягає в корекції виявлених недоліків, оновлених політик і процедур, а також у вдосконаленні всієї системи на основі отриманих даних.

Основними вимогами стандарту (табл. 1) є встановлення політики інформаційної безпеки, визначення ролей і відповідальності, проведення аналізу ризиків, управління інцидентами, проведення навчання та підвищення обізнаності працівників, моніторинг ефективності заходів, проведення внутрішніх аудитів, перегляд з боку керівництва та постійне вдосконалення системи.

Таблиця 1

Вимоги розробки політики згідно стандарту

A.5. Політики інформаційної безпеки	A.5.1.1 Розробка та перегляд політик
A.6. Організація інформаційної безпеки	A.6.1.1 Ролі, обов'язки та розподіл відповідальності
	A.6.2.1 Мобільні пристрої та віддалена робота
A.7. Безпека людських ресурсів	A.7.1.1 Перевірка при прийомі на роботу та умови працевлаштування
	A.7.2.1 Обізнаність, навчання та дисциплінарні заходи
	A.7.3.1 Припинення або зміна трудових відносин
A.8. Управління активами	A.8.1.1 Інвентаризація та володіння активами
	A.8.2.1 Класифікація, маркування та поводження з інформацією
	A.8.3.1 Управління носіями інформації
A.9. Контроль доступу	A.9.1.1 Політика контролю доступу та доступ до мереж
	A.9.2.1 Управління правами доступу користувачів
	A.9.3.1 Управління автентифікаційною інформацією
	A.9.4.1 Контроль доступу до інформації та систем

Продовження таблиці 1

A.10. Криптографія	A.10.1.1 Політика використання криптографії та управління ключами
A.11. Фізична безпека та безпека довкілля	A.11.1.1 Зони безпеки та фізичний захист
	A.11.2.1 Фізичний контроль входу та захист обладнання
A.12. Безпека операцій	A.12.1.1 Операційні процедури та управління змінами
	A.12.2.1 Захист від шкідливого ПЗ, резервне копіювання та реєстрація подій
	A.12.3.1 Захист цілісності інформації
	A.12.4.1 Безпека мереж
	A.12.5.1 Управління сеансом та обмін інформацією
	A.12.7.1 Поводження з інформацією та угоди про нерозголошення
A.13. Безпека комунікацій	A.13.1.1 Мережева безпека
	A.13.2.1 Передача інформації та політики використання
A.14. Придбання, розробка та супровід систем	A.14.1.1 Вимоги безпеки систем та безпека розробки
	A.14.2.1 Безпека сервісів додатків
	A.14.3.1 Захист даних тестування
A.15. Відносини з постачальниками	A.15.1.1 Політика безпеки відносин з постачальниками та угоди
	A.15.2.1 Моніторинг та управління змінами сервісів постачальників
A.16. Управління інцидентами інформаційної безпеки	A.16.1.1 Управління інцидентами, звітність та реагування
A.17. Аспекти інформаційної безпеки управління безперервністю бізнесу	A.17.1.1 Планування, впровадження та перевірка безперервності
A.18. Дотримання вимог	A.18.1.1 Дотримання правових та договірних вимог, захист даних
	A.18.2.1 Перегляд інформаційної безпеки та відповідність політикам

Кожен із цих компонентів повинен бути документально зафіксований, мати відповідальних осіб і регулярно перевірятися. Особливу увагу приділено інтеграції процесів безпеки в загальну систему управління організацією, що дозволяє уникнути фрагментації та забезпечує узгодженість усіх дій.

Додаток А стандарту містить перелік рекомендованих заходів контролю безпеки, які розподіляються за тематичними групами, серед яких управління активами, контроль доступу, криптографічний захист, фізична безпека, безпека

персоналу, управління інцидентами, безпека комунікацій, розробка та обслуговування систем, що представлено в табл. 1. Усі ці контролі носять рекомендаційний характер, проте організація має обґрунтувати вибір або невикористання кожного з них залежно від результатів аналізу ризиків. Такий підхід забезпечує гнучкість у впровадженні, дозволяючи адаптувати вимоги до специфіки бізнесу, фінансових можливостей та організаційної структури.

Принципи, на яких базується ISO/IEC 27001, охоплюють комплексність, орієнтацію на ризики, системність, залучення всіх рівнів організації, прозорість процесів, доказову базу для прийняття рішень і безперервне вдосконалення. Стандарт не є лише набором технічних вимог, а вимагає створення корпоративної культури безпеки, в якій кожен працівник усвідомлює значення захисту інформації і діє відповідально. Без участі керівництва, без підкріплення рішень з боку вищого менеджменту та без інтеграції безпеки у стратегію організації досягти відповідності стандарту неможливо.

ISO/IEC 27001 виступає не лише інструментом захисту інформації, а й засобом управління ризиками [20], оптимізації бізнес-процесів, підвищення ефективності діяльності, зниження витрат у разі інцидентів та зміцнення репутації на ринку. Його впровадження створює основу для довгострокового розвитку організації, забезпечує відповідність правовим вимогам, підвищує конкурентоспроможність і дає змогу відповідати викликам глобального цифрового середовища.

1.4 Проблеми та виклики впровадження ISO/IEC 27001 у сучасних організаціях

Впровадження стандарту ISO/IEC 27001 у сучасних організаціях супроводжується рядом труднощів, які пов’язані з організаційними, технічними, фінансовими та культурними аспектами функціонування підприємств. Хоча цей стандарт пропонує чітку і логічну структуру для побудови системи управління інформаційною безпекою, його впровадження часто виявляється складним [21],

тривалим і потребує серйозної підготовки з боку керівництва та всього персоналу (Рис. 1.3) .

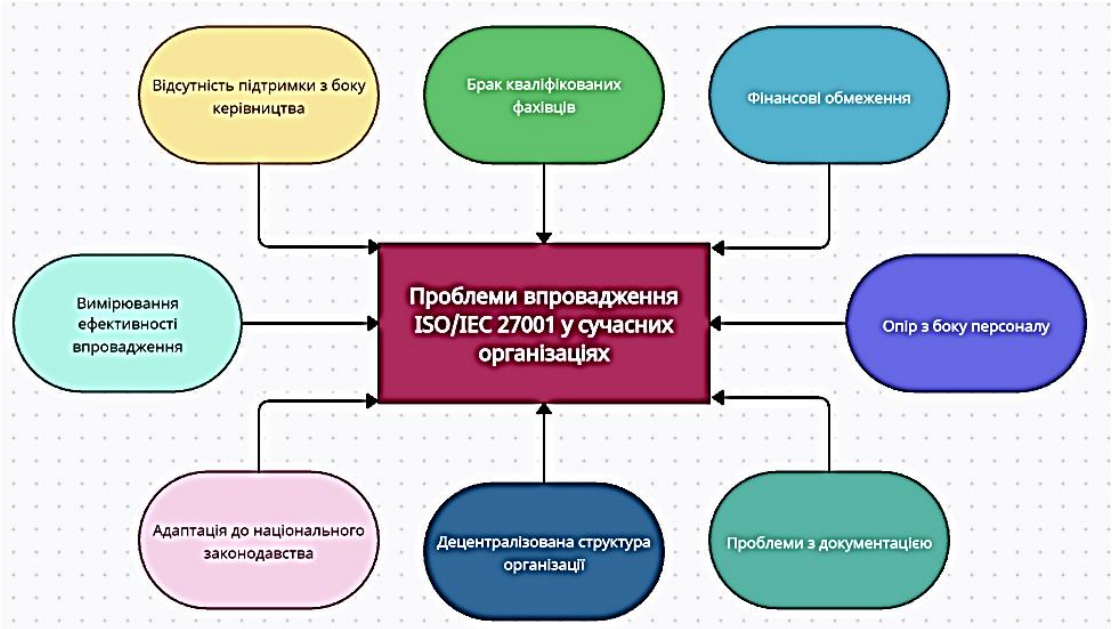

Рис. 1.3. Проблеми впровадження стандарту ISO

Однією з головних проблем є відсутність розуміння реальної цінності інформаційної безпеки на рівні керівників організацій. Без належної підтримки з боку топ менеджменту будь-які ініціативи, спрямовані на реалізацію вимог стандарту, втрачають стратегічне значення і зводяться до формальностей. Якщо керівництво не готове інвестувати в безпеку, не бере участі в перегляді політик, не ставить безпеку в пріоритет, система залишається поверхневою і не має внутрішнього ресурсу для розвитку. Часто впровадження починається під тиском зовнішніх обставин, таких як вимоги партнерів чи тендерні умови, і не супроводжується глибокою внутрішньою трансформацією.

Серйозною перешкодою стає брак кваліфікованих фахівців у сфері інформаційної безпеки, які мають досвід саме з впровадження ISO/IEC 27001. Більшість IT-працівників мають технічну підготовку, але не знайомі з принципами управління ризиками, підготовкою документації, проведенням аудитів та організаційною частиною безпеки [22]. Навіть у великих компаніях, які мають IT-департаменти, може не бути жодного спеціаліста, здатного

самостійно ініціювати й реалізувати проєкт впровадження стандарту. Це призводить до необхідності залучення зовнішніх консультантів, що збільшує витрати і ускладнює контроль за процесом.

Фінансові обмеження також є критичним фактором. Впровадження стандарту вимагає витрат на навчання персоналу, створення нових посад, закупівлю технічних засобів, розробку документів, сертифікацію та підтримку відповідності. У багатьох випадках організації не мають окремого бюджету на інформаційну безпеку, що змушує впроваджувати лише найнеобхідніше або відкладати реалізацію на невизначений термін. При цьому витрати на безпеку часто сприймаються як тягар, а не як інвестиція у стабільність і надійність бізнесу.

Ще одним викликом є опір з боку персоналу. Будь-які зміни, які вимагають дотримання нових процедур, проходження навчання, зміни звичок, обмеження доступу або використання додаткових засобів автентифікації [23], часто викликають негативне ставлення. Якщо співробітники не розуміють, навіщо вводяться ті чи інші політики, або якщо вони вважають, що це заважає виконанню їхніх обов’язків, вони можуть почати ігнорувати правила або шукати способи їх обходу. Відсутність культури безпеки в колективі створює середовище, де формальна відповідність стає самоціллю, а не частиною реального захисту.

Проблемним аспектом впровадження стандарту стає також ведення та оновлення документації. ISO/IEC 27001 вимагає створення великої кількості документів, серед яких політики, процедури, плани, звіти, реєстри активів, протоколи аудитів, оцінки ризиків, плани реагування на інциденти [24]. Без автоматизації та чіткої організації документообігу ці процеси стають надмірно ресурсоємними, схильними до помилок і неефективними. Організації, які не мають досвіду ведення такого рівня документації, часто припускаються неточностей, пропусків або надмірної формалізації, що знижує ефективність впроваджених заходів.

Особливі труднощі виникають у компаніях з децентралізованою структурою, філіями, віддаленими офісами або міжнародною присутністю. В таких випадках стає складно забезпечити однаковий рівень виконання вимог у всіх підрозділах, уніфікувати політики, організувати навчання та внутрішній аудит. Відсутність централізованого контролю або належного IT-інструментарію призводить до фрагментації системи і втрати керованості.

Певні проблеми пов'язані з необхідністю адаптації стандарту до національного законодавства. У різних країнах існують різні вимоги до зберігання, обробки і передачі персональних даних, і не всі вимоги стандарту можуть бути реалізовані без конфлікту з місцевими нормами. Це вимагає залучення юристів, перегляду процедур, узгодження політик на кількох рівнях і часто ускладнює сертифікацію.

Немаловажною є складність у вимірюванні ефективності впровадженої системи. Багато організацій не мають чітких метрик [25], які б дозволили оцінити, наскільки впровадження ISO/IEC 27001 дійсно зменшило ризики або підвищило рівень захищеності. Без механізмів оцінки результатів складно обґрунтовувати подальші інвестиції або перегляд стратегії безпеки.

Всі ці виклики не зменшують значення стандарту, а навпаки, підтверджують, що його впровадження вимагає системного підходу, залучення всіх рівнів управління, наявності кваліфікованих кадрів і довгострокової стратегії. Успішне подолання зазначених проблем забезпечує організації стійкий захист інформаційних активів, зміцнення репутації та відповідність вимогам сучасного інформаційного середовища.

Висновок до розділу 1

Загрози інформаційній безпеці організацій є комплексними та постійно еволюціонують разом із розвитком технологій. Від зовнішніх атак кіберзлочинців до внутрішніх загроз, таких як порушення з боку інсайдерів, організації повинні враховувати всі можливі ризики, включаючи технічні, людські та регуляторні фактори. Врахування фізичних загроз та важливість

партнерської безпеки також є критичними для збереження цілісності даних. В умовах зростаючої цифрової взаємозалежності та нових технологій, впровадження міжнародних стандартів, таких як ISO/IEC 27001, дозволяє організаціям систематизувати захист, оптимізувати управління ризиками та забезпечити безпеку на всіх рівнях.

Для ефективного управління інформаційною безпекою необхідно використовувати підходи, засновані на комплексному аналізі загроз, системному управлінні ризиками та впровадженні політик безпеки. Це дозволяє не лише захищати організацію від існуючих загроз, а й адаптуватися до нових викликів, забезпечуючи стійкість і стабільність роботи компанії в умовах постійних змін.

РОЗДІЛ 2 МЕТОДИКА ВПРОВАДЖЕННЯ ISO/IEC 27001

2.1 Загальний алгоритм впровадження системи управління інформаційною безпекою

Впровадження системи управління інформаційною безпекою відповідно до вимог ISO/IEC 27001 є складним і багатоступеневим процесом, який охоплює всі рівні організаційної структури та вимагає системного підходу. Алгоритм впровадження СУІБ не має універсальної форми, оскільки повинен бути адаптований до особливостей конкретної організації, однак існують загальні етапи, які є обов'язковими для забезпечення відповідності вимогам стандарту і досягнення реальної ефективності системи (Рис. 2.1).

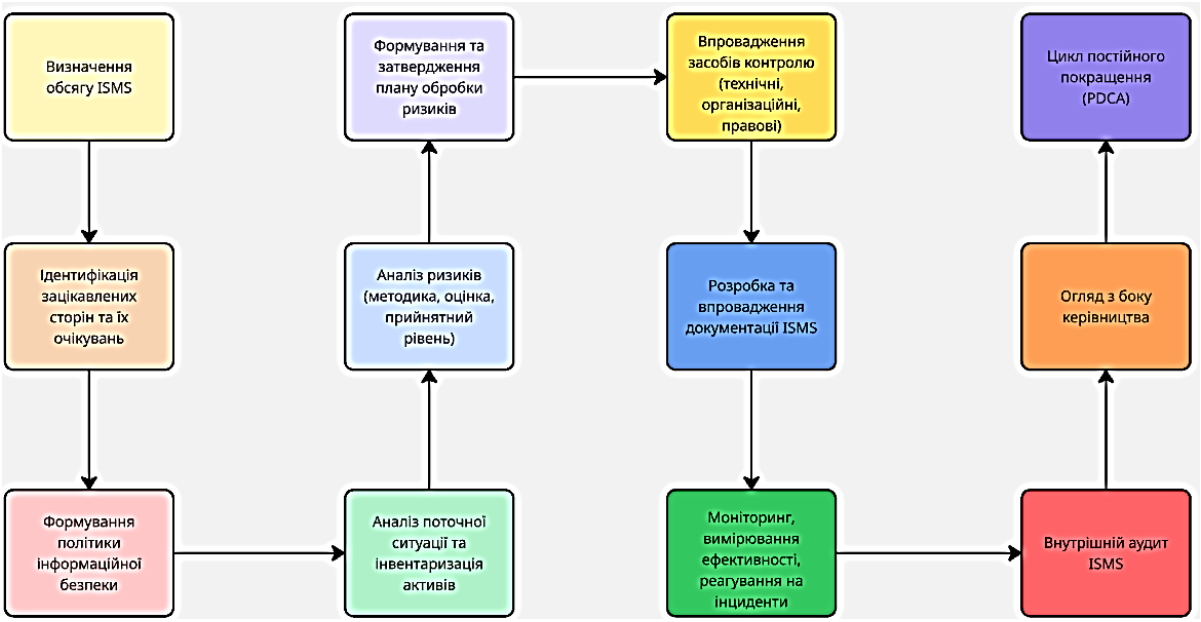

Рис. 2.1 Алгоритм впровадження СУІБ

Першим кроком у процесі впровадження є визначення обсягу СУІБ. Організація має чітко встановити, які саме підрозділи, інформаційні ресурси, процеси та активи будуть охоплені системою управління.

Визначення меж застосування СУІБ дозволяє сфокусувати зусилля на критично важливих елементах, уникнути надмірної бюрократизації та

забезпечити більш точне управління ризиками [26]. На цьому етапі необхідно також провести ідентифікацію зацікавлених сторін – партнерів, клієнтів, постачальників, регуляторних органів, акціонерів, внутрішніх користувачів – і визначити їх очікування щодо безпеки інформації.

Наступним етапом є формування політики інформаційної безпеки, яка виступає основним документом, що фіксує позицію керівництва щодо захисту інформаційних активів. Цей документ встановлює загальні принципи, обов'язки працівників, напрями розвитку СУІБ, вимоги до конфіденційності, цілісності та доступності інформації. Без затвердженої політики неможливо організувати узгоджену діяльність підрозділів і забезпечити системність у прийнятті управлінських рішень у сфері безпеки.

Далі організація повинна здійснити аналіз існуючої ситуації, який включає інвентаризацію інформаційних активів, оцінку поточного рівня захисту, виявлення вразливостей, оцінку відповідності чинним вимогам і стандартам. Такий аналіз є фундаментом для подальшого управління ризиками [27], оскільки дозволяє сформувати чітке уявлення про те, що саме потребує захисту, і які потенційні загрози можуть бути реалізовані. Ідентифікація активів є однією з найвідповідальніших задач, адже помилка на цьому етапі може призвести до того, що критичні елементи залишаться поза межами захисту.

Наступний важливий крок – проведення аналізу ризиків. Організація повинна визначити методику оцінювання, яка дозволяє встановити ймовірність реалізації загроз, їхній потенційний вплив [28], ступінь вразливості, рівень прийнятного ризику та пріоритетність заходів реагування. На основі цього формується план обробки ризиків, який містить перелік заходів з їх уникнення, зниження, перенесення або прийняття. План має бути узгоджений з керівництвом, мати чіткі терміни виконання, відповідальних осіб і критерії оцінки ефективності.

Після затвердження плану ризик-менеджменту починається етап впровадження засобів контролю. Це може включати технічні, адміністративні, організаційні або правові заходи, спрямовані на мінімізацію імовірності

реалізації загроз. До таких заходів належать впровадження антивірусного програмного забезпечення, систем виявлення вторгнень, обмеження доступу до даних, політики управління паролями, розмежування прав доступу, резервне копіювання, шифрування інформації, ведення журналів подій, розробка інструкцій для персоналу, підвищення обізнаності працівників щодо загроз інформаційної безпеки.

Важливою складовою процесу є розробка документації, яка регламентує діяльність у сфері інформаційної безпеки. Стандарт ISO/IEC 27001 вимагає наявності задокументованих процедур, інструкцій, реєстрів, протоколів, які фіксують дії, що мають бути виконані у стандартних і нестандартних ситуаціях. Документація має бути доступною, актуальною, перевіреною, а також відповідати вимогам внутрішнього і зовнішнього аудиту.

Після впровадження контролів і процедур організація повинна запустити процес моніторингу та вимірювання ефективності СУІБ. Це передбачає регулярне збирання та аналіз інформації про виконання заходів, дотримання політик, стан технічних засобів захисту, виявлення інцидентів [29], поведінку користувачів. Збір статистики дозволяє виявити слабкі місця, оцінити динаміку змін, формулювати обґрунтовані рішення щодо вдосконалення системи.

На завершальному етапі здійснюється внутрішній аудит системи управління інформаційною безпекою, який має на меті перевірку відповідності встановленим політикам, процедурним вимогам, цілям та критеріям ефективності. Аудит проводиться незалежними фахівцями, які аналізують як технічні аспекти, так і організаційну структуру, управління персоналом, реакцію на інциденти, документацію та планування безпеки. За результатами аудиту керівництво організації повинно розглянути звіт і ухвалити рішення щодо вдосконалення СУІБ.

Фінальним кроком є цикл постійного покращення, в якому виявлені недоліки та нові ризики враховуються для оновлення політик [30], впровадження нових заходів, перегляду пріоритетів і підвищення загального рівня зрілості системи. Весь процес впровадження СУІБ є безперервним і має бути частиною

загальної стратегії управління організацією, а не одноразовою дією або формальною процедурою.

Разом із загальним алгоритмом, що представлений на Рис. 2.1, для впорядкування процесу впровадження СУІБ широко використовується модель PDCA, яка дозволяє представити послідовність дій у структурованій формі. Для більш глибокого розуміння реалізації процесу нижче наведено деталізовану блок-схему, яка відображає основні етапи впровадження СУІБ з урахуванням практичної реалізації вимог стандарту ISO/IEC 27001 (Рис. 2.2).

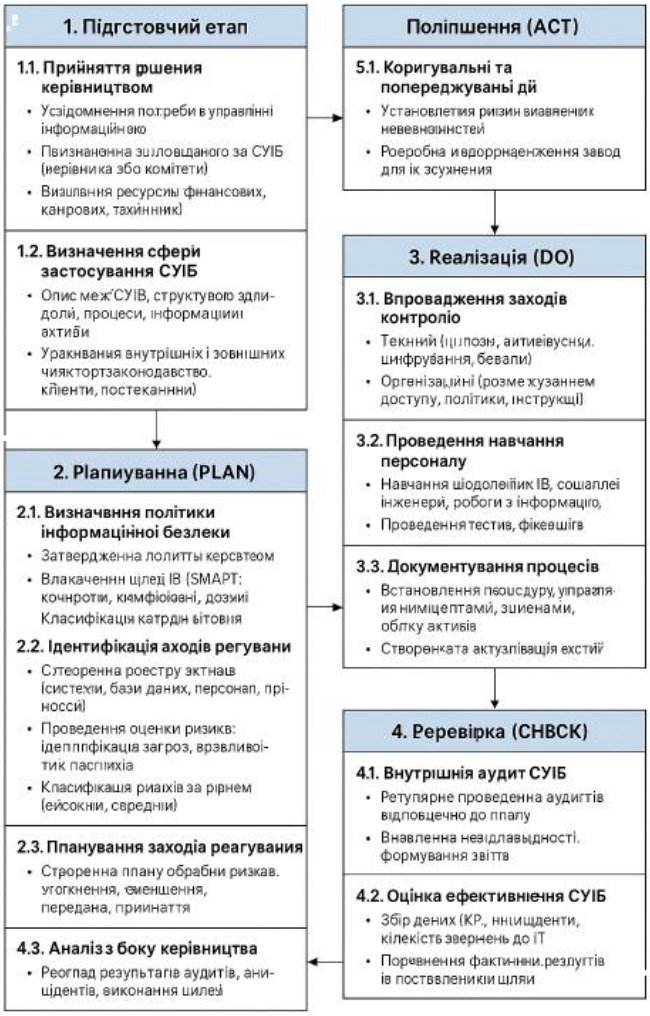

Рис.2.2. Етапи впровадження системи управління інформаційною безпекою (СУІБ) за циклом PDCA

2.2 Аналіз ризиків у контексті ISO/IEC 27001 (методи OCTAVE, NIST,RMF)

Аналіз ризиків є центральним елементом побудови ефективної системи управління інформаційною безпекою відповідно до стандарту ISO/IEC 27001. Саме він визначає логіку вибору заходів захисту, допомагає виявити найуразливіші місця в інформаційній системі [31], встановлює пріоритети для реалізації контролів і формує основу для прийняття обґрунтованих рішень керівництвом. Без якісного аналізу ризиків система управління перетворюється на набір декларативних заходів, які не відповідають реальним загрозам та специфіці функціонування організації.

Відповідно до ISO/IEC 27001 організація повинна визначити критерії прийнятного ризику, обрати методику ідентифікації, аналізу та оцінювання ризиків, а також здійснити документовану оцінку, яка враховує активи, загрози, вразливості, можливі наслідки і ймовірність реалізації загроз. Оцінка має охоплювати не лише технічні аспекти, а й організаційні процеси, людський фактор, юридичні ризики, залежність від постачальників та інші зовнішні обставини, які можуть впливати на функціонування інформаційної системи.

Один з методів, що широко застосовується у сфері інформаційної безпеки [32], є OCTAVE. Цей метод розроблений в Carnegie Mellon University і орієнтований на організації, які хочуть самостійно управляти своїми ризиками без залучення сторонніх консультантів. Він базується на глибокому [59] розумінні бізнес-процесів, активній участі ключових працівників і враховує контекст функціонування підприємства. Метод OCTAVE складається з трьох основних фаз: визначення інформаційних активів і організаційного контексту, ідентифікація вразливостей і потенційних загроз, формування стратегій управління ризиками. Особливістю цього підходу є акцент на організаційних аспектах безпеки, таких як політики, процедури, поведінка працівників, а також включення суб’єктивної оцінки значущості активів. Методика дозволяє

сформувати якісну картину ризиків і підвищити рівень усвідомлення інформаційної безпеки серед персоналу.

Інший потужний підхід до управління ризиками представлений у вигляді NIST Risk Management Framework (RMF) [33], розробленого Національним інститутом стандартів і технологій США. Ця методика призначена для державних установ США, але отримала широке визнання в усьому світі і застосовується в багатьох галузях. NIST RMF має сім послідовних етапів, кожен з яких деталізовано і передбачає чітку процедуру документування: підготовка, категоризація інформаційних систем, вибір заходів контролю, впровадження, оцінка ефективності, авторизація на використання і постійний моніторинг. Цей підхід дозволяє створити чітку, керовану і добре задокументовану систему, що постійно адаптується до змін зовнішнього середовища і внутрішніх умов.

Методологія NIST орієнтується на оцінку впливу інциденту на конфіденційність, цілісність і доступність інформації, при цьому враховує як можливу шкоду, так і важливість активів для досягнення цілей організації. На відміну від OCTAVE, яка більше фокусується на якісній оцінці і суб'єктивному підході, RMF вимагає точного визначення параметрів загроз, ймовірностей і заходів контролю. Завдяки цьому вона підходить для організацій, які прагнуть високого рівня деталізації і структурованості.

Існують також інші методики оцінки ризиків, серед яких CRAMM, MEHARI, ISO/IEC 27005 [34], які можуть застосовуватись залежно від обраної стратегії, специфіки діяльності і рівня зрілості системи управління. Стандарт ISO/IEC 27001 не вимагає використання конкретної методики, залишаючи вибір за організацією, але наголошує на необхідності обґрунтування обраного підходу, його узгодженості з цілями безпеки та його інтеграції у загальний процес управління.

Незалежно від обраного методу, процес аналізу ризиків передбачає обов'язкову участь різних категорій працівників, включаючи IT-фахівців, керівників підрозділів, юристів, менеджерів з якості та аудиторів. Така

міжфункціональна взаємодія дозволяє отримати повну картину загроз, які можуть виникнути на стику бізнесу, технологій і регулювання.

Результати оцінки ризиків мають бути задокументовані у вигляді реєстру ризиків, який містить опис кожного ризику, джерело його виникнення, оцінку впливу, імовірність, рівень ризику, обґрунтування прийняття або неприйняття, запропоновані заходи реагування та відповідальних осіб [35]. Регулярне оновлення цього реєстру забезпечує динамічність системи і дозволяє організації вчасно реагувати на нові виклики.

Правильно організований аналіз ризиків стає не лише основою для вибору засобів захисту, а й потужним управлінським інструментом, який допомагає організації приймати стратегічні рішення, підвищувати ефективність витрат, дотримуватись вимог законодавства та підтримувати довіру клієнтів. Без постійного аналізу ризиків і вдосконалення методик оцінки неможливо забезпечити стабільне функціонування системи управління інформаційною безпекою на рівні, що відповідає сучасним загрозам і стандартам.

Аналіз ризиків, будучи центральною складовою системи управління інформаційною безпекою, є не одноразовим процесом, а безперервним циклом, який супроводжує організацію на всіх етапах її діяльності. У динамічному середовищі, де змінюються бізнес-процеси, технології, ринки, нормативні вимоги і профілі загроз, постійне оновлення даних про ризики є обов’язковим. Стандарт ISO/IEC 27001 вимагає не лише початкової оцінки ризиків на етапі впровадження СУІБ [36], але й періодичного перегляду та перегрупування ризиків залежно від змін у зовнішньому і внутрішньому середовищі.

Важливо розуміти, що оцінка ризиків повинна охоплювати всі категорії інформаційних активів, включаючи як матеріальні, так і нематеріальні ресурси. Серед них можуть бути сервери, комп’ютери, мережеве обладнання, програмне забезпечення, бази даних, конфіденційні документи, контракти, розробки, знання персоналу, ліцензії, доступ до інформації, довіра клієнтів, ділова репутація. Недооцінка або неврахування певного класу активів призводить до

викривлення реальної картини загроз і, як наслідок, до неадекватної реакції на них.

Особливої уваги потребує врахування людського чинника під час аналізу ризиків. Люди залишаються найбільш непередбачуваним елементом інформаційної безпеки, тому ризики, пов’язані з помилками, навмисними діями або недостатнім розумінням політик безпеки, мають оцінюватися нарівні з технічними [37]. Зловмисна активність співробітників, необережне поводження з документами, несвоєчасне оновлення програмного забезпечення, порушення процедур автентифікації, відкриття шкідливих вкладень у листах – усе це створює сприятливе середовище для реалізації загроз і має враховуватись у матриці ризиків.

Методика OCTAVE дозволяє проводити оцінку ризиків із залученням різних груп персоналу, що підвищує рівень внутрішнього залучення до процесу і сприяє глибшому розумінню важливості захисту інформації. Цей підхід фокусується на знанні організації про себе саму, використовуючи внутрішні ресурси для створення цілісного профілю ризиків [38]. Він не вимагає високої технологічної оснащеності, але натомість потребує зрілості організаційної культури, спроможності до самоаналізу і чесного ставлення до виявлення слабких місць.

На відміну від OCTAVE, NIST RMF значно деталізує технічну сторону управління ризиками. Цей підхід є ідеальним для організацій, які мають високі вимоги до безпеки, великі обсяги інформації, складну інфраструктуру та потребу в документальній точності. NIST RMF не тільки надає логіку аналізу ризиків, а й вимагає детальної звітності на кожному етапі. Це дозволяє забезпечити прозорість рішень, обґрунтування бюджету на заходи безпеки та можливість подальшої сертифікації або перевірки відповідності.

Обидві методики – і OCTAVE, і NIST RMF – є ефективними інструментами у процесі створення СУІБ, проте вибір між ними залежить від ресурсів організації, рівня підготовки персоналу, цілей управління безпекою і регуляторних вимог. Нерідко організації комбінують елементи з різних методик,

адаптуючи процес оцінки ризиків до власних реалій. Це дозволяє забезпечити гнучкість, уникнути зайвого навантаження і сконцентруватися на ключових напрямках захисту.

Процес аналізу ризиків не завершується після складання реєстру. Кожен ризик повинен мати свій життєвий цикл, що включає моніторинг, перегляд, перегрупування за пріоритетністю, виконання запланованих заходів, оцінку ефективності контролів. Без цього система перетворюється на статичну структуру [39], не здатну реагувати на динаміку зовнішніх і внутрішніх змін. Деякі ризики можуть зменшуватись або зникати після впровадження заходів, інші, навпаки, зростають у зв’язку з новими загрозами, технологічними змінами або людськими помилками.

Ефективність управління ризиками в межах ISO/IEC 27001 залежить не лише від обраної методики, а й від здатності організації інтегрувати оцінку ризиків у всі ключові процеси. Коли оцінка ризиків проводиться ізольовано або виконується один раз на початку проєкту [40], її результативність різко знижується. Тільки за умови її інтеграції у щоденну діяльність, у прийняття рішень, у планування змін, у бюджетування і в навчальні програми вона стає живим інструментом, який підтримує безпеку системи на належному рівні.

2.3 Розробка політик та процедур безпеки

Розробка політик та процедур безпеки є невід'ємною складовою впровадження системи управління інформаційною безпекою згідно зі стандартом ISO/IEC 27001. Цей процес має стратегічне значення, оскільки саме політики формують нормативну основу функціонування СУІБ, визначають рамки поведінки працівників, встановлюють вимоги до захисту інформаційних активів і забезпечують єдину мову для взаємодії між підрозділами організації. Без чітко визначених правил та інструкцій система безпеки втрачає керованість і послідовність, що значно знижує її ефективність.

Політика інформаційної безпеки є базовим документом, який декларує принципи, на яких ґрунтується підхід організації до захисту даних. У цьому документі відображаються стратегічні цілі в галузі безпеки, відповідальність керівництва за впровадження та підтримку заходів захисту, основні обов'язки працівників, загальні вимоги до безпеки інформаційних активів, орієнтири для оцінювання ефективності СУІБ. Цей документ має бути затвердженим на найвищому рівні управління і доступним для всіх співробітників. Він слугує основою для подальшої деталізації процесів у вигляді процедур, інструкцій, регламентів і положень.

Процедури безпеки деталізують, як саме виконуються вимоги, що закладені в політиках. Вони мають бути чіткими, зрозумілими і такими, що піддаються перевірці. Наприклад, процедура управління користувачами визначає порядок створення облікових записів, надання прав доступу, блокування неактивних облікових записів, ревізії доступу і його відкликання після звільнення співробітника. Процедура управління інцидентами містить порядок виявлення, фіксації, класифікації, ескалації та реагування на порушення інформаційної безпеки [41]. Процедура резервного копіювання описує алгоритм створення, зберігання, перевірки і відновлення копій критичних даних. Кожна з процедур повинна мати визначену періодичність перегляду, відповідальних осіб і механізми контролю виконання.

Розробка політик вимагає ретельного аналізу чинного законодавства, вимог галузевих нормативів, контрактних зобов'язань і внутрішніх потреб організації. Вони мають враховувати специфіку діяльності, тип оброблюваної інформації, рівень зрілості корпоративної культури, технічні можливості і наявні ресурси. Не можна просто взяти шаблон політики і застосувати його без адаптації, оскільки це може призвести до формального дотримання вимог без реального ефекту. Політики мають бути релевантними, доцільними, узгодженими між собою і такими, що не створюють зайвого навантаження на персонал.

Однією з найважливіших політик є політика управління доступом. Вона визначає принципи, за якими встановлюються права доступу до інформаційних ресурсів, встановлює правила розмежування повноважень, ведення обліку доступу, контроль за обліковими записами, аудит змін у правах. Без чітких правил доступу організація наражається на ризик несанкціонованого доступу, витоку конфіденційної інформації або саботажу з боку незадоволених працівників [42]. Політика управління доступом повинна бути підкріплена технічними засобами контролю, такими як багатофакторна автентифікація, автоматизовані системи надання доступу, журналювання дій користувачів.

Ще однією ключовою політикою є політика класифікації інформації. Вона регламентує порядок присвоєння рівнів конфіденційності документам, електронним листам, файлам, базам даних. У цій політиці зазначається, які категорії інформації є публічними, внутрішніми, конфіденційними або критичними, хто має право встановлювати рівень доступу і як саме повинна поводитися інформація на кожному рівні захисту [43]. Така політика допомагає структурувати інформаційні потоки, забезпечити відповідний рівень контролю над особливо важливими активами і уникнути несанкціонованого розповсюдження.

Процес розробки політик повинен супроводжуватись навчанням персоналу. Недостатньо просто створити документ і опублікувати його на внутрішньому порталі. Працівники мають розуміти зміст політик, знати, як їх застосовувати у щоденній роботі, і відчувати власну відповідальність за дотримання правил. Для цього проводяться інформаційні кампанії, тренінги, перевірки знань, практичні навчання у вигляді моделювання інцидентів. Зворотний зв’язок від користувачів допомагає вдосконалити політики і зробити їх реальним інструментом підвищення безпеки.

Документи, які входять до складу СУІБ, мають постійно оновлюватися. Нові загрози, зміни в законодавстві, технологічний розвиток, нові бізнес-процеси вимагають перегляду підходів до безпеки. Організація повинна мати чіткий графік ревізії політик і процедур, проводити регулярні перевірки їх актуальності,

вносити зміни на основі результатів внутрішніх аудитів, інцидентів і змін у структурі підприємства [44]. Це дозволяє зберігати релевантність нормативної бази і забезпечувати її відповідність реальним умовам.

Без грамотно сформованих, затверджених і підтримуваних політик неможливо забезпечити ефективне функціонування системи управління інформаційною безпекою. Вони є основою для побудови довіри, забезпечення прозорості, дотримання регуляторних вимог і формування корпоративної культури відповідального поводження з інформацією.

Створення політик та процедур безпеки передбачає не лише документальне оформлення вимог, а й забезпечення їх життєздатності у реальному робочому середовищі. Вони мають бути інтегровані у всі бізнес-процеси організації, не створюючи зайвих перешкод для продуктивності, але при цьому гарантувати стабільність і контроль. Успішна реалізація цього завдання потребує взаємодії між підрозділами, участі керівництва, підтримки з боку IT-фахівців і активного залучення служби безпеки.

Особливу увагу слід приділяти адаптації політик до змін, які відбуваються всередині організації. Зміна структури, впровадження нових технологій, розширення діяльності, відкриття нових філій, переведення персоналу на дистанційну роботу – все це повинно знайти відображення у відповідних процедурах. Наприклад, поява нових типів мобільних пристроїв або використання хмарних сервісів вимагає створення окремих політик щодо BYOD або захищеного використання публічних хмар. Без такої гнучкості документи втрачають актуальність, а їх формальне дотримання не забезпечує реального захисту.

Політики безпеки не повинні дублювати одне одного або суперечити між собою. Їх зміст має бути узгодженим, логічно побудованим і впорядкованим за рівнями доступу та пріоритетності. Існує базова політика інформаційної безпеки, яка встановлює загальні принципи [45], і на її основі будуються всі тематичні документи, що деталізують окремі напрями – політика управління інцидентами, політика шифрування, політика управління мобільними пристроями, політика

роботи з постачальниками. Кожна з них повинна бути прив'язана до відповідних ризиків і бути частиною комплексної стратегії захисту.

Не менш важливою є процедура прийняття політик, яка має бути прозорою, структурованою і передбачати механізми узгодження з усіма зацікавленими сторонами. Відповідальні особи за розробку, погодження, затвердження, поширення і перегляд політик мають бути визначені заздалегідь. Бажано, щоб розробка політик відбувалася на міждисциплінарному рівні з урахуванням поглядів IT-департаменту, юридичної служби, відділу кадрів, керівників підрозділів і кінцевих користувачів. Це дозволяє врахувати практичні аспекти їх застосування і уникнути надмірної формальності.

Процес реалізації політик повинен супроводжуватися автоматизацією, де це можливо. Системи управління документами, платформи контролю доступу, засоби моніторингу виконання процедур, інструменти електронного погодження документів значно спрощують дотримання політик і зменшують навантаження на персонал. Автоматизація дозволяє швидко реагувати на зміни, оновлювати документи, відслідковувати відповідальність і вчасно інформувати користувачів про нові вимоги.

Інтеграція політик у внутрішні процеси організації забезпечує цілісність підходу до інформаційної безпеки. Вони повинні враховуватись під час навчання нових співробітників, у щорічних оцінках знань [46], у процесах розробки нових продуктів, при прийнятті рішень щодо закупівель, під час перевірки контрагентів. Це дозволяє сформувати єдине середовище, в якому безпека не є окремим напрямом, а є складовою корпоративної культури.

Якісна розробка політик та процедур забезпечує стабільність, передбачуваність і керованість інформаційної безпеки. Вона дозволяє мінімізувати вплив людського фактора, структурувати заходи захисту, уніфікувати дії співробітників у стандартних і нестандартних ситуаціях. Політики створюють простір, у якому безпека перестає бути абстракцією і набуває чітких форм, вимог, правил та механізмів реалізації. Усі ці чинники

забезпечують сталість роботи організації, відповідність міжнародним стандартам, конкурентоспроможність і готовність до зовнішнього аудиту.

2.4 Вибір інструментів для підтримки СУІБ (системи управління ризиками, SIEM, засоби моніторингу)

Після створення фундаменту системи управління інформаційною безпекою відповідно до стандарту ISO/IEC 27001 організація стикається з необхідністю вибору технічних і програмних інструментів, які дозволять підтримувати ефективність СУІБ на постійній основі [47]. Без сучасного інструментарію неможливо забезпечити належний рівень автоматизації, своєчасне виявлення загроз, контроль за виконанням процедур безпеки та оперативне реагування на інциденти. Інструменти, які застосовуються в межах СУІБ, повинні відповідати реальним потребам організації, бути інтегрованими в її IT-інфраструктуру, масштабованими, гнучкими та такими, що можуть підтримувати процес безперервного вдосконалення.

Однією з найважливіших категорій інструментів є системи управління ризиками, які забезпечують централізоване ведення реєстрів ризиків, автоматизують процес їх оцінювання, дозволяють створювати карти ризиків, встановлювати зв’язки між активами, загрозами та заходами контролю. Такі системи допомагають організації візуалізувати ризики, аналізувати їх динаміку, контролювати виконання планів реагування і формувати звіти для керівництва. Найпоширеніші рішення в цій галузі включають платформу LogicManager, MetricStream, RSA Archer, RiskWatch, які надають широкий набір функцій для інтеграції з іншими компонентами СУІБ. Вони дозволяють спростити процеси аудиту, управління відповідністю, звітності і стратегічного планування в сфері безпеки.

Не менш важливою є категорія інструментів, що забезпечують виявлення інцидентів і централізований моніторинг подій безпеки. Тут ключову роль відіграють SIEM-системи (Security Information and Event Management), які

здійснюють збір, нормалізацію, кореляцію та аналіз логів з різноманітних джерел. Вони дозволяють виявляти аномальну активність, зловмисні дії, спроби проникнення або порушення політик доступу у реальному часі. SIEM-системи виступають центральним компонентом для команд реагування на інциденти, забезпечують історичний аналіз подій, формування дашбордів і автоматизоване повідомлення про загрози.

Найбільш відомими рішеннями є Splunk, IBM QRadar, ArcSight, Microsoft Sentinel, які підтримують інтеграцію з хмарними платформами, мережевими пристроями, серверними системами і системами автентифікації.

До інструментів, що відіграють важливу роль у підтримці СУІБ, належать також засоби моніторингу стану систем, журналювання дій користувачів, контроль за конфігураціями, аналіз вразливостей і управління патчами. Вони дозволяють виявляти відхилення від стандартних сценаріїв, фіксувати зміни в критичних файлах, забезпечувати контроль за доступом до конфіденційних даних. Серед таких рішень слід відзначити Nagios, Zabbix, SolarWinds, OpenVAS, Tenable Nessus, які підтримують гнучке налаштування, автоматизацію перевірок і створення звітів. Засоби моніторингу допомагають зберігати постійний контроль над інфраструктурою, попереджати інциденти і забезпечувати відповідність вимогам стандарту ISO/IEC 27001 щодо моніторингу, аналізу і вдосконалення заходів безпеки.

Інструменти для управління активами та конфігураціями також мають важливе значення. Вони забезпечують повну інвентаризацію IT інфраструктури, зберігають відомості про апаратне та програмне забезпечення, ліцензії, версії, відповідальних осіб. Такі системи дозволяють встановити зв’язок між активами і ризиками, виявляти незареєстровані пристрої, контролювати відповідність конфігурацій політикам безпеки. Рішення на кшталт GLPI, Lansweeper, ManageEngine ServiceDesk Plus допомагають централізувати інформацію, підвищити прозорість управління активами і забезпечити обґрунтованість при прийнятті рішень щодо їх модернізації або заміни.

У контексті побудови захищеного середовища важливо також використовувати засоби багатофакторної автентифікації, управління привілейованими обліковими записами, засоби контролю доступу до мережі, системи шифрування даних у транзиті та на носіях, рішення для резервного копіювання та відновлення [48]. Всі ці інструменти мають бути об’єднані в єдину архітектуру, підпорядковану політикам безпеки і підтримувану належним рівнем адміністрування.

Інструментальна база СУІБ має постійно переглядатися і вдосконалюватися. Поява нових загроз, оновлення нормативних вимог, зміни в архітектурі ІТ-середовища потребують відповідного оновлення використовуваних технологій. Важливу роль у цьому відіграє регулярна оцінка ефективності інструментів, тестування на проникнення, аналіз інцидентів і отриманий досвід практичного реагування. Лише ті засоби, які довели свою ефективність і відповідають потребам конкретної організації, можуть стати основою стабільної системи захисту.

Інтеграція інструментів підтримки СУІБ у щоденні операційні процеси організації дозволяє не лише виконувати вимоги ISO/IEC 27001, а й підвищити рівень зрілості системи [49], забезпечити прозорість прийняття рішень, скоротити час реагування на інциденти і знизити ймовірність реалізації ризиків, що загрожують критичним інформаційним активам.

Висновок до розділу 2

Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до стандарту ISO/IEC 27001 є багаторівневим і системним процесом, який охоплює всі аспекти діяльності організації – від технічних рішень до управлінських підходів. Ключовими етапами є визначення меж системи, формування політики безпеки, ідентифікація інформаційних активів, аналіз ризиків, впровадження контролів, документування процедур, моніторинг ефективності та безперервне вдосконалення. Особливої уваги заслуговує аналіз

ризиків, який виступає основою для прийняття обґрунтованих рішень щодо заходів захисту.

Різні методики аналізу ризиків – такі як OCTAVE і NIST RMF – дозволяють організаціям обрати найбільш відповідний підхід залежно від розміру, структури та рівня зрілості. OCTAVE орієнтована на організаційні аспекти та участь персоналу, тоді як NIST RMF передбачає високий рівень деталізації й суворе документування. Обидва підходи можуть бути ефективно використані для забезпечення комплексного управління ризиками в межах СУІБ.

Таким чином, ефективне впровадження СУІБ потребує не лише формального дотримання стандарту, а й усвідомлення його стратегічної ролі в управлінні організацією. Безперервний аналіз ризиків, залучення персоналу, адаптація до змін зовнішнього середовища та орієнтація на реальні загрози є необхідними умовами побудови стійкої системи інформаційної безпеки.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ВПРОВАДЖЕННЯ ISO/IEC 27001

3.1 Аналіз поточного стану інформаційної безпеки на об’єкті дослідження

Оцінювання поточного стану інформаційної безпеки є початковим і надзвичайно важливим етапом практичного впровадження системи управління інформаційною безпекою згідно з вимогами стандарту ISO/IEC 27001. Воно дозволяє отримати об'єктивне уявлення про наявні механізми захисту, виявити прогалини [50], визначити рівень зрілості організаційної культури безпеки, проаналізувати існуючі політики, технічні засоби, процедури і відповідність нормативним вимогам. Без цього кроку неможливо коректно сформувати план впровадження СУІБ, оскільки будь-яка подальша діяльність повинна базуватись на достовірному аналізі реального стану справ.

Перш за все, увага зосереджується на виявленні і класифікації інформаційних активів організації. Це дозволяє зрозуміти, які саме об'єкти потребують захисту, як вони використовуються, до кого належать, які системи забезпечують їх обробку і зберігання. У процесі інвентаризації фіксуються сервери, робочі станції, бази даних, документообіг, резервні носії, мережеве обладнання, програми, електронна пошта, сховища, мобільні пристрої, а також нематеріальні активи – такі як репутація, конфіденційна інформація, угоди з партнерами, інтелектуальна власність. Кожен актив отримує визначення щодо його критичності, власника, рівня конфіденційності та необхідного ступеня захисту.

У рамках аналізу поточного стану також здійснюється оцінка організаційних заходів, які діють у межах підприємства. Вивчаються наявні політики безпеки, посадові інструкції, процедури реагування на інциденти, регламенти з управління паролями, правила обробки персональних даних, документи з обліку активів і процедур доступу. Визначається ступінь формалізації процесів, наявність підписаних працівниками зобов’язань про

нерозголошення інформації, перевіряється рівень обізнаності співробітників щодо вимог безпеки. Проводяться бесіди, опитування, аналіз журналів, спостереження за поведінкою користувачів у процесі щоденної роботи.

Окремо проводиться технічний аудит, який охоплює аналіз стану інфраструктури, виявлення відкритих портів, перевірку актуальності оновлень програмного забезпечення, оцінку конфігурацій серверів, брандмауерів, маршрутизаторів, антивірусного захисту, шифрування, систем контролю доступу. Вивчається структура доменів, моделі автентифікації, використання багатофакторних механізмів, політики журналювання подій, інтеграція SIEM-систем, наявність резервного копіювання і політик зберігання логів. Аналізується, чи виконуються основні технічні вимоги, передбачені стандартом, і які існують відхилення або слабкі місця, що створюють потенційну загрозу.

Особливу увагу приділяють аспектам фізичної безпеки, яка включає захист серверних приміщень, доступ до технічних засобів, системи відеонагляду, контроль відвідувачів, облік обладнання [51]. Аналізуються дії у випадку надзвичайних ситуацій, наявність планів відновлення, інструкцій для персоналу на випадок збоїв, пожеж, аварійного відключення живлення або витоку даних. Проводиться огляд засобів контролю кліматичних умов, протипожежної безпеки, автономного живлення, фізичної ідентифікації.

Значною складовою оцінки є перевірка відповідності законодавчим вимогам і зовнішнім стандартам, які можуть діяти в галузі, де працює організація. Враховується національне законодавство, міжнародні договори, галузеві регламенти, вимоги партнерів, правила обробки персональних даних, положення щодо зберігання комерційної інформації, специфікації безпеки, що закріплені в контрактах або тендерах [9]. У результаті формується загальна картина відповідності і виявляються розриви між фактичним станом системи безпеки і вимогами стандарту ISO/IEC 27001.

Підсумком цього етапу є підготовка аналітичного звіту, в якому узагальнюються виявлені проблеми, надається опис існуючих загроз, встановлюється перелік невиконаних вимог, оцінюється рівень готовності до

впровадження СУІБ. На основі цього звіту визначається план першочергових дій, розробляється стратегія усунення критичних вразливостей, проводиться ранжування ризиків і встановлюються ключові цілі для наступного етапу реалізації стандарту. Такий підхід забезпечує обґрунтованість подальших рішень, знижує ймовірність хибних управлінських кроків, допомагає раціонально розподілити ресурси і забезпечити фокус на найбільш критичних аспектах захисту.

3.2 Впровадження основних заходів відповідно до вимог стандарту

Впровадження основних заходів безпеки згідно з вимогами стандарту ISO/IEC 27001 є ключовим етапом на шляху створення повноцінної системи управління інформаційною безпекою (Рис 3.2).

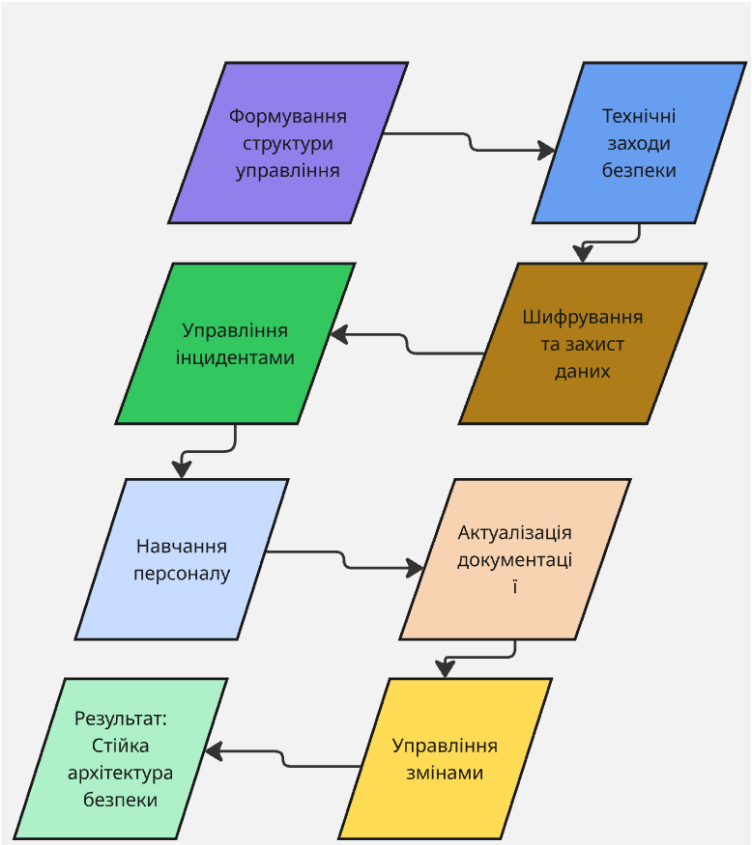

Рис 3.2 Впровадження основних заходів безпеки

Цей процес передбачає не лише технічні дії, а й глибоку організаційну перебудову, інтеграцію політик безпеки в повсякденну діяльність, зміну підходів до обробки інформації [52], побудову культури відповідального поводження з цифровими активами. Основне завдання полягає в тому, щоб на основі результатів попереднього аналізу запровадити комплекс взаємопов'язаних заходів, які у сукупності створять надійне середовище для захисту даних, процесів і технологій.

На першому рівні реалізації заходів впроваджується оновлена структура управління інформаційною безпекою. Формується або трансформується підрозділ, відповідальний за координацію всіх процесів СУІБ, призначаються особи, які відповідають за безпеку в межах своїх підрозділів, розробляється і затверджується регламент взаємодії між службами [53]. Встановлюються постійно діючі комісії, які приймають рішення з питань доступу, інцидентів, змін у процедурних документах, а також здійснюється контроль за впровадженням рішень з боку керівництва.

На рівні технічної інфраструктури реалізуються заходи, спрямовані на зниження ризиків, пов'язаних з несанкціонованим доступом до інформації. Впроваджується багатофакторна автентифікація для всіх критичних систем, встановлюються обмеження за ролями, часовими рамками, місцем доступу. Використовуються централізовані служби каталогів, системи керування правами, аудиту доступу, автоматичні механізми зміни паролів. Налаштовуються міжмережевий екран, ізолюються сегменти мережі, створюються віртуальні приватні мережі для віддалених користувачів. Для підвищення рівня контролю над користувацькою активністю впроваджуються системи журналювання подій і автоматичної фіксації аномальної поведінки.

Для забезпечення цілісності та конфіденційності даних запроваджуються засоби шифрування. Всі канали передачі інформації переводяться на протоколи, що підтримують захист даних на транспортному рівні [54]. Внутрішні сервіси використовують шифрування баз даних, а файли, що містять критичну інформацію, зберігаються на зашифрованих носіях. Забезпечується ізоляція

резервних копій, доступ до яких мають лише уповноважені особи, а самі копії зберігаються у захищених середовищах з контрольованим доступом.

Особливу роль відіграють процедури управління інцидентами. Створюється централізований механізм реєстрації, класифікації, розслідування та усунення інцидентів, пов'язаних з інформаційною безпекою. Визначаються ролі учасників процесу реагування, розробляються шаблони дій для типових ситуацій, налаштовуються канали швидкого інформування відповідальних осіб. Проводяться тренування персоналу, створюються навчальні сценарії, що дозволяють перевірити готовність до реагування у випадку порушення захисту. Кожен випадок аналізується з точки зору запобігання повторному виникненню.

З метою підвищення обізнаності працівників організовується серія навчальних заходів, які охоплюють не лише загальні питання інформаційної безпеки, а й специфіку роботи в умовах дотримання політик СУІБ. Кожен працівник має бути ознайомлений із вимогами, які стосуються його функціональних обов'язків, а також з базовими правилами кібергігієни [55], поведінки у випадку інциденту, порядком звернення до служби підтримки. Навчання супроводжується перевірками знань, створенням навчальних матеріалів, поширенням пам'яток та інструкцій.

Усі зміни супроводжуються актуалізацією документації. Розробляються нові політики, вносяться зміни до існуючих процедур, оновлюються посадові інструкції, створюються реєстри активів, матриці доступу, журнали інцидентів. Вся документація зберігається у захищених сховищах, забезпечується її контрольована доступність, впроваджується система регулярного перегляду і затвердження.

Впровадження заходів включає також побудову процесу управління змінами, що стосуються інформаційної безпеки. Кожна зміна у системах, обладнанні, програмному забезпеченні, процедурі або структурі доступу повинна проходити через механізм аналізу впливу на безпеку. Це дозволяє уникнути неузгоджених рішень, які можуть створити вразливості або порушити відповідність встановленим вимогам.

Результатом цього етапу має стати створення стійкої і адаптивної архітектури безпеки, яка відповідає реаліям діяльності організації, інтегрується в усі бізнес-процеси, підтримується на всіх рівнях і забезпечує виконання вимог стандарту ISO/IEC 27001 у щоденній практиці. Така система не лише знижує ризики, а й підвищує довіру клієнтів, знижує ймовірність фінансових втрат, сприяє проходженню зовнішніх аудитів та створює основу для подальшого вдосконалення.

3.3 Оцінка ефективності запропонованих заходів

Після впровадження основних заходів безпеки, передбачених вимогами стандарту ISO/IEC 27001, виникає необхідність об’єктивної оцінки їх ефективності. Така оцінка дозволяє не лише підтвердити досягнення поставлених цілей, а й виявити недоліки, прогалини, неочікувані наслідки або недосконалості в реалізації окремих рішень [56]. Без цього процесу система управління інформаційною безпекою залишається незавершеною, оскільки немає зворотного зв’язку, що дозволяє визначати, наскільки прийняті заходи відповідають фактичним викликам і ризикам.

Оцінювання ефективності повинно проводитись комплексно, із застосуванням як кількісних, так і якісних методів. Передусім розглядається ступінь виконання встановлених вимог і відповідність реалізованих заходів політикам, процедурам і запланованим результатам. Перевіряється наявність усієї необхідної документації, правильність її ведення, дотримання затверджених процедур, виконання контрольних дій і рівень залучення відповідальних осіб до процесів підтримки системи безпеки. Для кількісної оцінки ризиків, що залишилися після впровадження заходів, може бути використана базова формула:

$$R = P * V\ , \qquad (1)$$

де R - ризик, P – імовірність впливу (0-1) V – вплив.

Здійснюється аналіз журналів подій, звітів SIEM-систем, систем моніторингу, результатів сканування вразливостей, відомостей про збої, спроби вторгнень, інциденти, які були зафіксовані за певний період часу. Кількість виявлених спроб несанкціонованого доступу, їх успішність, швидкість реагування на події, тривалість виведення з ладу систем, ступінь впливу інцидентів на основну діяльність організації – усі ці фактори формують загальну картину реального стану захисту. Особливу увагу приділяють повторюваним подіям, які свідчать про наявність системних проблем або про неефективність застосованих заходів.

Ефективність заходів оцінюється також через співвідношення виявлених ризиків і реального впливу інцидентів. Якщо система працює правильно, то реалізовані загрози не повинні виходити за межі прийнятного ризику, а план обробки ризиків – бути здатним запобігати порушенням. Для оцінки потенційних фінансових втрат від реалізації ризиків може бути використана формула очікуваних річних втрат:

$$V_o = O_v * \omega_{pod} , \quad (2)$$

де Vo очікувані річні втрати, O_v- очікувані одноразові втрати, а ω_{pod} - річна частота виникнення події.

Порівнюються показники до і після впровадження СУІБ, аналізується динаміка змін, зменшення кількості критичних інцидентів, покращення часу виявлення загроз, зростання кількості навчань персоналу, підвищення рівня захищеності інфраструктури (Рис 3.3).

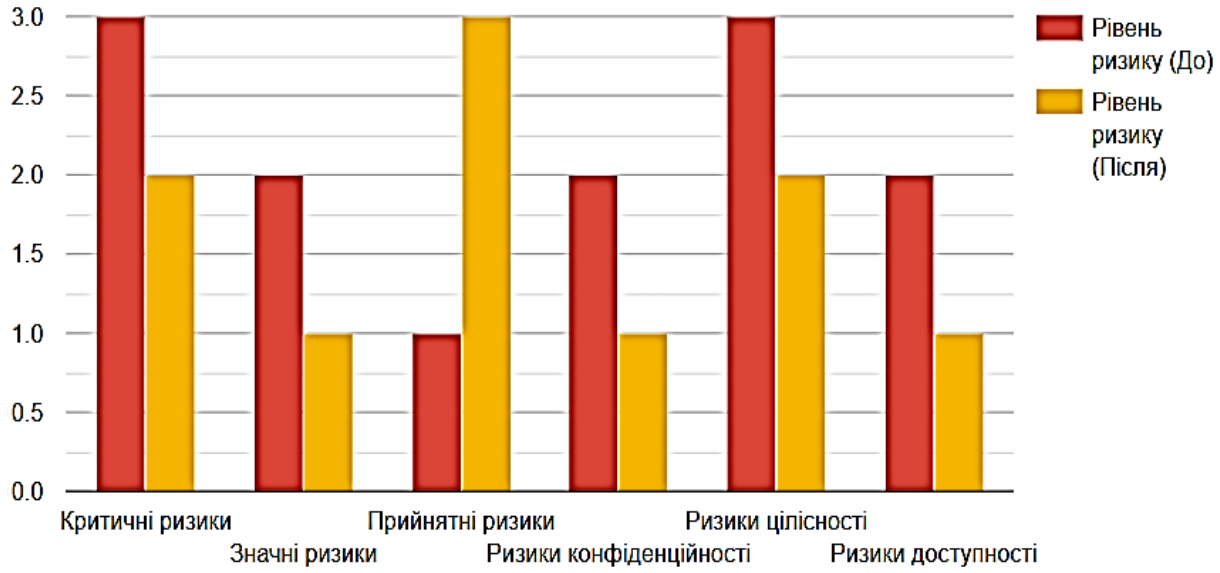

Рис 3.3. Порівняльні показники до і після впровадження СУІБ

Оцінювання має враховувати і людський фактор, зокрема обізнаність працівників, їхню поведінку в ситуаціях, що потребують дотримання вимог безпеки, здатність ідентифікувати підозрілі дії, дотримання політик, рівень відповідальності. Проводяться анонімні опитування, інтерв'ю, тести, які дозволяють з'ясувати, чи справді персонал розуміє вимоги стандарту і чи готовий їх виконувати на практиці. Важливим є і ступінь ініціативності з боку співробітників, готовність повідомляти про інциденти, дотримання процедур звітування.

Оцінка ефективності неможлива без аналізу витрат (3), пов'язаних із впровадженням заходів. Економічний аспект розглядається не тільки через призму витрат на засоби захисту, навчання та аудит, а й через показники потенційно зекономлених ресурсів у випадку успішного запобігання інцидентам. Основні критерії та результати оцінювання ефективності впровадження стандарту ISO/IEC 27001 представлено в табл.3.

Таблиця 3

Результати оцінювання ефективності впровадження стандарту ISO/IEC 27001

№	Критерій оцінки	Опис	Максимальний бал	Фактичний бал
1	Документована політика ІБ	Наявність, актуальність, затвердження керівництвом	5	4
2	Визначення сфери застосування СУІБ	Чітке окреслення меж, активів, процесів	5	5
3	Проведення оцінки ризиків	Визначення, аналіз, оцінка ризиків ІБ	10	7
4	План обробки ризиків	Прийняття заходів щодо зниження ризиків	10	5
5	Впровадження контрольних заходів (Annex A)	Відповідність впроваджених контролів потребам	10	6
6	Проведення внутрішніх аудитів	Регулярність, глибина, реагування на виявлені невідповідності	10	8
7	Участь керівництва	Надання ресурсів, участь у прийнятті рішень	5	4
8	Навчання та обізнаність персоналу	Курси, інструктажі, тестування знань	5	5
9	Реагування на інциденти	Наявність планів, фіксація, аналіз інцидентів	10	9
10	Досягнення цілей ІБ	Відповідність фактичних результатів встановленим цілям	10	10
11	Коригувальні/попереджувальні дії	Вчасне усунення невідповідностей, аналіз першопричин	10	7
12	Постійне покращення СУІБ	Оновлення документів, практик, заходів	5	5
13	Підготовка та результати сертифікаційного аудиту	Відсутність критичних/серйозних невідповідностей	5	4

$$E = (L_0 - L_1 - C) / C \quad (3)$$

Ця формула (3) відображає економічну ефективність впровадження заходів безпеки, де L0 - очікувані втрати до впровадження, L1 - очікувані втрати після впровадження, а C - вартість впровадження.

Якщо заходи дозволили уникнути витоків інформації, втрати даних, штрафів або зупинок у діяльності [57], це свідчить про їхню дієвість і виправданість інвестицій. На основі таких оцінок розраховуються показники рентабельності впровадження, формуються аргументи для подальшого фінансування заходів безпеки.

Окремий блок уваги приділяється аналізу процедур реагування на інциденти. Розглядається, наскільки швидко і якісно були проведені дії після виявлення порушень, чи була забезпечена безперервність роботи систем, чи вдалося ідентифікувати причини інциденту, чи було проведено розслідування та впроваджено коригувальні заходи. Якість зворотного зв'язку після інциденту є важливим показником зрілості системи безпеки.

Результатом процесу оцінки ефективності є підготовка звіту, в якому відображено сильні сторони, наявні проблеми, пріоритетні напрямки вдосконалення, нові загрози або ризики, що з'явилися в ході реалізації заходів. Такий звіт є основою для перегляду стратегії, оновлення політик, коригування планів, визначення нових цілей. Він слугує інструментом для підвищення прозорості управлінських рішень, аргументованості бюджетних запитів, підготовки до зовнішніх аудитів або сертифікації.

Оцінка ефективності заходів безпеки має стати регулярною практикою, що повторюється у визначені періоди або після значних змін в інфраструктурі, організаційній структурі, нормативному полі або технологічному середовищі. Такий підхід дозволяє не лише підтримувати належний рівень захисту, а й забезпечити безперервне вдосконалення СУІБ, як цього вимагає структура стандарту ISO/IEC 27001.

3.4 Проведення внутрішнього аудиту СУІБ та підготовка рекомендацій

Внутрішній аудит системи управління інформаційною безпекою є обов'язковим компонентом підтримки і розвитку СУІБ відповідно до вимог

стандарту ISO/IEC 27001 (Рис. 3.4). Його проведення забезпечує систематичну оцінку стану реалізації вимог стандарту, виявлення відхилень, аналіз ефективності заходів, визначення зон для вдосконалення та підтвердження готовності до зовнішньої сертифікації. Внутрішній аудит має не лише виявляти недоліки, а й формувати конструктивні рекомендації для підвищення рівня захищеності організації.

Рис. 3.4. Послідовність проведення внутрішнього аудиту

Підготовка до аудиту починається з формування плану, який охоплює всі аспекти функціонування СУІБ у межах визначеної області застосування. У плані зазначаються об’єкти перевірки, строки проведення, відповідальні особи, обсяг аналізованої документації, методи збору інформації, джерела даних та очікувані результати. Аудит може охоплювати як окремі процеси – управління доступом, реагування на інциденти, моніторинг, захист персональних даних, так і всю систему в цілому. Для забезпечення об’єктивності аудиту важливо, щоб аудитори не були безпосередньо залучені до діяльності підрозділів, які перевіряються.

Основним джерелом інформації для аудиторів є внутрішня документація СУІБ. Аналізу підлягають політики, інструкції, протоколи, звіти, реєстри активів, плани управління ризиками, результати навчань, журнали інцидентів, записи про оновлення систем, зміни в конфігураціях, заходи з відновлення після надзвичайних ситуацій. Особлива увага приділяється відповідності змісту документів вимогам стандарту, їхньої актуальності, повноті і наявності підтверджень практичного виконання встановлених вимог.

Під час аудиту також проводяться інтерв’ю з працівниками, що дозволяє оцінити рівень обізнаності, розуміння процедур, готовність до дій у разі інциденту, дотримання політик у щоденній роботі. Спостереження за виконанням процесів дає змогу порівняти задекларовані підходи з реальною практикою. Якщо у документах описано одну модель поведінки, а в реальності застосовується інша, це сигнал про невідповідність і необхідність перегляду підходів або посилення контролю.

Результати аудиту оформлюються у вигляді звіту "(Додаток 1)", в якому фіксуються як відповідності, так і невідповідності, а також надаються зауваження, рекомендації, приклади кращих практик, виявлені резерви для вдосконалення. У звіті має бути чітко зазначено, які пункти стандарту були перевірені, яка інформація була проаналізована, які порушення виявлені, які висновки зроблені. Важливо, щоб за кожною виявленою невідповідністю стояли конкретні факти, а не загальні припущення. Звіт аудитора повинен бути підставою для управлінських рішень, тому його об’єктивність, точність і повнота є критично важливими.

На основі результатів аудиту формується перелік коригувальних і попереджувальних дій. Для кожної з виявлених проблем визначаються причини, масштаби, ризики, заходи усунення, відповідальні особи і строки виконання. Цей перелік має бути інтегрований у загальну систему управління, підлягати контролю з боку керівництва і супроводжуватися постійним моніторингом виконання. Усі зміни, що впроваджуються внаслідок аудиту, повинні бути задокументовані, оцінені на предмет ефективності і, за потреби, перевірені повторно.

Рекомендації, підготовлені за результатами внутрішнього аудиту, мають бути не лише технічними, а й організаційними. Наприклад, якщо було виявлено недостатню обізнаність працівників, необхідно оновити програму навчання, якщо політики не відповідають реаліям роботи – провести їх перегляд за участі ключових підрозділів, якщо система реагування на інциденти надто складна –

спростити або оптимізувати її логіку. Важливо, щоб рекомендації не сприймалися як критика, а були інструментом покращення та розвитку.

Аудит завершується аналізом результатів на рівні керівництва, яке повинно розглянути звіт, ухвалити рішення про необхідні зміни, виділити ресурси для їх реалізації та встановити пріоритети. Це закріплює безпеку як частину загальної управлінської політики, інтегрує її у стратегічне планування і формує культуру постійного вдосконалення. Повторний аудит або перевірка виконання рішень дозволяє контролювати стан усунення недоліків, забезпечити прозорість та відповідальність.

Внутрішній аудит СУІБ не є одноразовою подією, а має бути постійною практикою, яка дозволяє організації не просто підтримувати відповідність стандарту, а й рухатися вперед, реагувати на зміни в середовищі, зміцнювати довіру до себе з боку клієнтів, партнерів, регуляторних органів. Такий підхід робить безпеку не лише вимогою, а й конкурентною перевагою.

Висновок до розділу 3

Комплексне впровадження системи управління інформаційною безпекою (СУІБ) згідно зі стандартом ISO/IEC 27001 потребує поетапного і всебічного підходу, що охоплює аналіз поточного стану безпеки, впровадження цільових заходів і подальшу оцінку їх ефективності. На першому етапі, шляхом інвентаризації активів, аналізу організаційних та технічних заходів, було сформовано об'єктивне уявлення про стан захисту, виявлено прогалини та визначено вразливості. Це дозволило розробити обґрунтований план дій із впровадження необхідних змін.

У процесі реалізації заходів було впроваджено низку організаційних, технічних та процедурних рішень, спрямованих на підвищення рівня безпеки даних, доступу, інцидент-менеджменту та обізнаності персоналу. Забезпечено відповідність ключовим вимогам стандарту, інтегровано заходи у бізнес-процеси, актуалізовано нормативну документацію та розгорнуто систему внутрішнього контролю.

Завершальним етапом стала оцінка ефективності впроваджених змін, яка показала зниження рівня ризиків, підвищення стійкості до загроз і покращення безпекової культури в організації. Проведений аналіз підтвердив доцільність вжитих заходів і створив підґрунтя для постійного вдосконалення СУІБ. Такий підхід не лише підвищує загальну захищеність, а й сприяє довірі з боку клієнтів, партнерів та регуляторних органів.

РОЗДІЛ 4 ОЦІНКА РЕЗУЛЬТАТІВ ТА РЕКОМЕНДАЦІЇ

4.1 Вплив впровадження стандартів ISO/IEC 27001 на інформаційну безпеку організації

Впровадження стандарту ISO/IEC 27001 справляє комплексний вплив на систему інформаційної безпеки організації, трансформуючи не лише технічні аспекти захисту даних [58], а й управлінські, організаційні та культурні компоненти. Цей стандарт передбачає побудову системи, яка функціонує на основі чітко визначених процедур, політик, відповідальностей і механізмів контролю, що дозволяє створити єдину архітектуру безпеки на всіх рівнях діяльності організації.

Реалізація вимог стандарту сприяє формуванню системного підходу до захисту інформаційних активів, що означає перехід від фрагментарних і часто реактивних заходів до комплексної стратегії, яка охоплює всі аспекти роботи з інформацією. Організація отримує можливість виявляти, класифікувати та контролювати свої активи, встановлювати пріоритети в управлінні ризиками, координувати дії різних структурних підрозділів, підтримувати ефективну комунікацію між службами, що відповідають за IT, безпеку, юридичні питання, персонал і управління якістю.

На практичному рівні впровадження стандарту приводить до зменшення кількості інцидентів, пов’язаних з порушеннями інформаційної безпеки. Це досягається через застосування контрольованих засобів автентифікації, шифрування, моніторингу, системного управління вразливостями, резервного копіювання та обмеження доступу до інформаційних ресурсів. Завдяки цим заходам значно підвищується стійкість інфраструктури до зовнішніх атак, зменшується ризик втрати або витоку конфіденційної інформації, скорочується час на виявлення та реагування на інциденти.

Іншим важливим результатом впровадження є підвищення обізнаності персоналу щодо ролі кожного співробітника в забезпеченні інформаційної

безпеки. Навчальні програми, внутрішні комунікаційні кампанії, тестування, практичні тренування з реагування на інциденти створюють культуру відповідального поводження з інформацією. Персонал починає розуміти ризики, які виникають при порушенні встановлених процедур, вчиться розпізнавати фішингові листи, несанкціоновані запити на доступ, підозрілу активність у системах.

Важливим ефектом є також підвищення довіри з боку клієнтів, партнерів, постачальників і регуляторів. Наявність сертифікованої системи управління інформаційною безпекою свідчить про відповідальність компанії, її здатність дотримуватися міжнародних вимог, системно управляти ризиками, захищати інтереси зацікавлених сторін. Це часто стає умовою співпраці в міжнародних проєктах, підвищує конкурентоспроможність компанії, дозволяє брати участь у тендерах, де вимагається наявність впровадженого стандарту.

Фінансовий аспект також демонструє позитивну динаміку після впровадження ISO/IEC 27001. Зменшення кількості інцидентів знижує витрати на їх ліквідацію, зменшує ризики штрафів за порушення законодавства, сприяє уникненню втрат репутації, які можуть мати довгострокові наслідки. Інвестиції в безпеку перестають бути просто витратами і починають розглядатися як захід, що забезпечує стабільність, безперервність діяльності і довготривалу ефективність.

Важливим стратегічним наслідком впровадження стандарту є підвищення гнучкості та адаптивності організації до змін. Система СУІБ, побудована відповідно до ISO/IEC 27001, дозволяє вчасно реагувати на нові виклики, змінювати внутрішні процедури з урахуванням змін у технологіях, законодавстві чи бізнес-середовищі. Така система є живою, вона не є застиглою бюрократичною конструкцією, а дозволяє організації розвиватися, не втрачаючи контроль над інформаційною безпекою.

Підвищується рівень зрілості процесів [59], оскільки реалізація вимог стандарту вимагає їх опису, регламентації, документування, що автоматично підвищує дисципліну, прозорість і передбачуваність роботи. Процеси стають

краще структурованими, взаємодія між підрозділами – більш ефективною, система прийняття рішень – більш обґрунтованою. Це сприяє не лише інформаційній безпеці, а й загальному управлінню організацією, що підвищує її конкурентоспроможність і привабливість на ринку.

Впровадження стандарту також стимулює організацію до розвитку внутрішнього аудиту, моніторингу, аналітики, оцінки ризиків, що формує культуру вдосконалення, орієнтовану на постійний аналіз і поліпшення. Такий підхід сприяє довготривалому зміцненню безпеки, робить захист частиною повсякденної діяльності, а не винятковим реагуванням на вже реалізовані загрози.

4.2 Аналіз досягнутого рівня відповідності стандарту

Аналіз досягнутого рівня відповідності стандарту ISO/IEC 27001 є критично важливою складовою завершального етапу впровадження системи управління інформаційною безпекою. Такий аналіз дозволяє встановити, наскільки впроваджена система відповідає вимогам стандарту, які елементи реалізовані повністю, які частково, а які потребують доопрацювання або перегляду. Він формує об’єктивну картину зрілості СУІБ в межах організації, допомагає підготуватися до зовнішньої сертифікації та забезпечує основу для подальшого розвитку.

Оцінка відповідності проводиться на основі порівняння наявних практик, документів, процесів та інструментів з конкретними пунктами стандарту ISO/IEC 27001. Кожна вимога аналізується на предмет її реалізації в контексті діяльності організації. Враховується не лише наявність процедур, а й їх реальне застосування, підтверджене доказовими матеріалами, такими як звіти, журнали, протоколи, записи тренінгів, акти перевірок, внутрішні аудити. Саме факт практичного застосування стандарту має ключове значення для підтвердження відповідності.

У процесі аналізу вивчаються основні обов’язкові вимоги стандарту, серед яких визначення контексту організації, потреб і очікувань зацікавлених сторін, формування політики безпеки, управління ризиками, призначення відповідальностей, оцінка ефективності заходів, забезпечення навчання персоналу, внутрішній аудит, аналіз з боку керівництва та постійне вдосконалення СУІБ. Для кожного з цих елементів складається оцінка, яка враховує повноту реалізації, рівень формалізації, глибину впровадження і наявність результатів, що підтверджують функціонування системи.

Окрему увагу приділено додатку А до стандарту, який містить перелік контрольних заходів, згрупованих за темами. Аналізується, які з рекомендованих контролів були впроваджені, які визнані неактуальними в контексті організації, які реалізовані частково. Для кожного заходу має бути наявне обґрунтування – чому саме він був або не був впроваджений, яке рішення приймалося на основі оцінки ризиків, якими документами підтверджується такий підхід. Це демонструє логіку управління безпекою, відповідність процесу моделі управління ризиками, що є основою ISO/IEC 27001 [60].

Важливою частиною аналізу відповідності є перевірка наскрізної інтеграції СУІБ в операційну діяльність організації. Система має бути не ізольованим набором документів і інструментів, а частиною щоденної роботи всіх структурних підрозділів. Розглядається, наскільки політики безпеки інтегровані у кадрові процедури, ІТ-інфраструктуру, закупівлі, управління проєктами, юридичну практику, взаємодію з контрагентами. Оцінюється, як система адаптується до змін – наприклад, як реалізується управління змінами, яким чином виявляються нові ризики, наскільки швидко приймаються рішення про оновлення заходів захисту.

Аналіз охоплює і культуру безпеки, яка склалася в організації внаслідок впровадження стандарту. Розглядається залученість керівництва, активність працівників, рівень виконання вимог без примусового контролю, ініціативність персоналу щодо повідомлення про інциденти або пропозицій удосконалення. Високий рівень відповідності стандарту передбачає не лише наявність

інструментів, а й сформовану поведінку, яка базується на усвідомленні важливості інформаційної безпеки як загальної цінності. Узагальнення результатів аналізу оформлюється у вигляді підсумкового звіту, який демонструє рівень досягнутої відповідності представлено в табл. 4.

Таблиця 4

Шкала оцінювання ефективності впровадження стандартів

Загальний бал	**Рівень ефективності**	**Рекомендації**
90–100	Високий	СУІБ працює ефективно, відповідає ISO 27001
75–89	Достатній	Необхідні незначні покращення
60–74	Середній	Потрібно вдосконалити ключові процеси
40–59	Низький	СУІБ має серйозні недоліки, потрібна глибока перебудова
<40	Критично недостатній	Впровадження ISO/IEC 27001 не реалізовано належно

Аналіз відповідності стандарту ISO/IEC 27001 на об’єкті практики показав, що впровадження СУІБ оцінюється на **73%**, що відповідає *середньому рівню ефективності* згідно зі шкалою інтерпретації. Система має основні елементи управління безпекою, зокрема політики, базові процедури управління ризиками та внутрішній аудит, однак потребує вдосконалення в частині інтеграції в операційну діяльність, систематизації документації та розвитку культури інформаційної безпеки. Рекомендовано зосередити подальші дії на поглибленні реалізації вимог стандарту та підготовці до сертифікації. У ньому мають бути відображені сильні сторони, які підтверджують відповідність критичним

вимогам стандарту, а також виявлені слабкі місця, що потребують додаткової уваги. Звіт є основою для підготовки до сертифікації, а також для формування стратегії подальшого вдосконалення СУІБ. Його слід представити керівництву для прийняття відповідних рішень, встановлення пріоритетів, бюджетування і планування наступних етапів розвитку системи безпеки.

Аналіз досягнутого рівня відповідності має періодично повторюватися, оскільки середовище, в якому функціонує організація, постійно змінюється. Це дозволяє зберігати динамічність СУІБ, підтримувати її актуальність і забезпечити готовність організації до нових викликів та зовнішніх перевірок у будь-який момент.

4.3 Розробка рекомендацій для подальшого вдосконалення СУІБ

Після проведення аналізу досягнутого рівня відповідності стандарту ISO/IEC 27001 настає етап формування практичних рекомендацій, які дозволяють удосконалити систему управління інформаційною безпекою, зробити її більш адаптивною, ефективною та орієнтованою на довгостроковий розвиток. Рекомендації мають ґрунтуватися на реальному досвіді експлуатації СУІБ, результатах внутрішніх аудитів, зворотному зв’язку від персоналу, виявлених інцидентах, зміні зовнішнього середовища, появі нових загроз і змін у нормативному регулюванні. Їхня реалізація повинна стати логічним продовженням роботи над підтримкою і розвитком системи.

Першочерговим напрямом для вдосконалення є розширення процесів аналізу ризиків. Вони повинні стати більш гнучкими, динамічними, адаптивними до змін у бізнес-середовищі, впровадженні нових технологій, трансформації внутрішніх процесів. Рекомендовано переглянути періодичність аналізу ризиків, залучити більшу кількість учасників до процесу оцінки [48], розширити коло активів, які підлягають класифікації та моніторингу. Варто вдосконалити критерії прийнятного ризику, оновити методику розрахунку впливу і

ймовірності, запровадити автоматизовані інструменти для візуалізації ризик-профілю.

Наступним важливим кроком є посилення інтеграції СУІБ у всі бізнес процеси організації. Необхідно забезпечити, щоб вимоги безпеки враховувалися ще на етапах розробки нових продуктів, послуг, впровадження технологій, зміни інфраструктури. Рекомендовано створити механізми взаємодії між департаментами на рівні розробки та погодження проєктів, де безпека є невіддільною частиною планування. Такий підхід зменшує витрати на усунення вразливостей після впровадження, підвищує якість процесів і робить захист інформації невід'ємною складовою корпоративної стратегії.

Суттєве вдосконалення слід реалізувати в напрямку підвищення рівня автоматизації контролю за виконанням політик та процедур. Варто розглянути впровадження нових інструментів для моніторингу, виявлення аномалій, аналізу журналів подій, управління інцидентами, оновлення політик безпеки у відповідності до змін. Автоматизація дозволяє зменшити людський фактор, пришвидшити реагування, забезпечити точність та повноту обліку подій, забезпечити безперервний контроль у реальному часі. Особливу увагу слід приділити інтеграції інструментів із наявною IT-інфраструктурою, зокрема з хмарними сервісами, мобільними платформами, засобами віртуалізації та зовнішніми постачальниками.

Рекомендації мають також стосуватись удосконалення системи навчання і підвищення обізнаності персоналу. Ефективність заходів безпеки значною мірою залежить від того, наскільки користувачі розуміють свої ролі і відповідальність. Необхідно оновити навчальні матеріали, впровадити індивідуалізований підхід до різних категорій працівників, організовувати регулярні тренінги, симуляції атак, перевірки знань, тематичні ігри, інтерактивні модулі. Підвищення рівня обізнаності має стати не періодичною акцією, а постійною освітньою практикою.

Особливу увагу слід звернути на підвищення ефективності системи внутрішнього аудиту. Необхідно оновити критерії перевірки, забезпечити

прозорість і незалежність аудиторського процесу, навчити нових аудиторів, створити базу знань з результатами попередніх аудитів, рекомендаціями та прикладами кращих практик. Аудит має перетворитися на інструмент розвитку, а не бути формальною процедурою перевірки. Результати аудиту повинні активно використовуватися для прийняття управлінських рішень, формування стратегічних напрямів вдосконалення системи.

Система управління інцидентами потребує розширення як з погляду швидкості реагування, так і з точки зору якості документування та аналізу причин. Рекомендовано впровадити автоматизовану систему реєстрації інцидентів, створити механізми їх пріоритезації, вдосконалити сценарії реагування, визначити зони відповідальності та налагодити комунікаційні канали між учасниками реагування. Варто переглянути плани реагування на найпоширеніші загрози, забезпечити їх практичну апробацію, проводити тренування в умовах, максимально наближених до реальних.

Рекомендації також повинні включати вдосконалення системи управління змінами в СУІБ. Кожна зміна в інфраструктурі, політиках, штатному розкладі, процесах має проходити через процедуру аналізу її впливу на інформаційну безпеку. Доцільно створити централізовану базу змін, в якій фіксуватимуться їх ініціатори, обґрунтування, очікувані наслідки, оцінка ризиків та план реагування.

Розроблені рекомендації мають бути структурованими, пріоритезованими і закріпленими за конкретними виконавцями. Для кожної рекомендації слід визначити терміни реалізації, очікувані результати, метрики ефективності, ресурси, що будуть задіяні, і відповідальних осіб. Такий підхід дозволить не лише сформувати план вдосконалення, а й забезпечити його практичну реалізацію в межах життєвого циклу СУІБ.

4.4 Перспективи розвитку стандартів ISO/IEC 27001 у контексті глобальної кібербезпеки

Перспективи розвитку стандартів ISO/IEC 27001 у контексті глобальної кібербезпеки базу, яка визнається всіма сторонами і забезпечує взаємну довіру. Стандарти ISO/IEC 27001 сприяють створенню єдиного інформаційного простору, де організації можуть обмінюватися даними, спільно реалізовувати проєкти, делегувати функції без ризику порушення конфіденційності, цілісності або доступності критичної інформації.

Інтенсивний розвиток цифрової економіки, появи нових технологічних рішень і посилення загроз з боку організованих кіберзлочинних угруповань вимагають постійного оновлення підходів до управління інформаційною безпекою. У зв'язку з цим важливу роль відіграє активна робота міжнародних технічних комітетів, зокрема ISO/IEC JTC 1/SC 27, які відповідають за розробку і перегляд стандартів у сфері IT-безпеки.

Періодичне оновлення ISO/IEC 27001, а також пов'язаних з ним документів ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27017 та інших, дозволяє підтримувати актуальність вимог, враховувати нові категорії ризиків і впроваджувати найкращі практики, що підтвердили свою ефективність у реальних умовах.

У майбутньому очікується ще більша персоналізація стандартів під окремі галузі, зокрема охорону здоров'я, фінансові послуги, енергетику, телекомунікації, транспорт. Кожна з цих сфер має власну специфіку, типові загрози, характерні типи інформаційних активів, рівень допустимого ризику і вимоги до часу реагування. Розробка спеціалізованих профілів відповідності на базі ISO/IEC 27001 дозволить адаптувати систему управління безпекою до практичних умов кожної галузі, підвищити ефективність її реалізації і пришвидшити процес сертифікації.

Розвиток стандарту ISO/IEC 27001 також йде в напрямку посилення акценту на відповідальності вищого керівництва за функціонування системи. Роль топ менеджменту у підтримці політик, виділенні ресурсів, участі в аудитах, прийнятті рішень щодо ризиків стає ключовою умовою успішного функціонування СУІБ. Вимоги щодо залучення керівництва все більше закріплюються в оновлених версіях стандарту і відображають [61] тенденцію до інтеграції інформаційної безпеки у стратегічне управління організацією.

Ще одним перспективним напрямом є розвиток цифрових платформ для автоматизованої підтримки ISO/IEC 27001. Впровадження програмних рішень, які забезпечують збирання та аналіз інформації про стан безпеки, контроль за виконанням політик, ведення документації, проведення внутрішніх аудитів, розрахунок показників ефективності – дозволяє значно підвищити продуктивність і точність управлінських дій. У майбутньому такі платформи можуть стати обов'язковим компонентом сертифікації, що ще більше стандартизує підхід до безпеки на міжнародному рівні.

У контексті глобальної кібербезпеки зростає роль стандартів як інструменту дипломатії, координації зусиль між державами, розбудови цифрового суверенітету, захисту критичної інфраструктури. ISO/IEC 27001 дедалі більше розглядається не лише як технічний документ, а як частина загальної політики інформаційної безпеки країн, яка формує правила для державних установ, приватного сектору, міжнародних корпорацій та операторів критичних сервісів.

У довгостроковій перспективі можна очікувати появу механізмів обміну інформацією між організаціями, сертифікованими за ISO/IEC 27001, що дозволить швидше реагувати на нові типи загроз [62], попереджати інциденти, узгоджувати захисні заходи та посилювати глобальну стійкість кіберпростору. Взаємне визнання сертифікатів, створення реєстрів відповідності, участь у глобальних мережах обміну кіберінформацією може суттєво підвищити рівень міждержавної взаємодії у сфері кіберзахисту.

Розвиток стандарту ISO/IEC 27001 не лише слугує інструментом забезпечення внутрішньої стабільності окремої організації, а й стає частиною ширшої інфраструктури міжнародної кібербезпеки, яка вимагає постійного вдосконалення, координації і стратегічного бачення на рівні світової спільноти.

Висновок до розділу 4

У розділі було всебічно проаналізовано вплив впровадження стандарту ISO/IEC 27001 на систему управління інформаційною безпекою організації, оцінено досягнутий рівень відповідності та сформовано практичні рекомендації для її подальшого вдосконалення.

Впровадження стандарту ISO/IEC 27001 дозволило організації перейти від фрагментарного захисту до системного управління інформаційними ризиками. Це охопило не лише технічні аспекти, але й управлінські, організаційні та поведінкові елементи, сприяючи створенню цілісної культури безпеки. Стандартизовані політики, процедури, відповідальності та контрольні заходи забезпечили інтеграцію інформаційної безпеки в усі бізнес-процеси, підвищили стійкість до загроз, зменшили кількість інцидентів та підвищили рівень обізнаності персоналу.

Проведений аналіз відповідності стандарту засвідчив, що ключові вимоги ISO/IEC 27001 реалізовані в значній мірі, хоча деякі аспекти потребують подальшого вдосконалення. Було виявлено сильні сторони, такі як ефективне управління ризиками, активна участь керівництва та функціональність основних процедур, а також визначено зони, де необхідні додаткові заходи – зокрема в автоматизації, інтеграції, внутрішньому аудиті та навчанні персоналу.

Рекомендації, сформовані за підсумками аналізу, спрямовані на підвищення адаптивності, гнучкості та ефективності системи управління інформаційною безпекою. Зокрема, пропонується удосконалити підходи до ризик-менеджменту, автоматизувати контрольні процеси, розширити навчальні програми, посилити взаємодію між підрозділами та вдосконалити внутрішній аудит. Це дозволить організації підтримувати високий рівень безпеки,

оперативно реагувати на нові виклики та забезпечити безперервність діяльності в умовах динамічного середовища.

Таким чином, впровадження та розвиток СУІБ на основі стандарту ISO/IEC 27001 є ефективною стратегією забезпечення надійного та сталого захисту інформаційних активів, що прямо впливає на конкурентоспроможність і довгостроковий успіх організації.

ВИСНОВКИ

У результаті проведеного дослідження було досягнуто поставлену мету – розроблено методику впровадження стандарту ISO/IEC 27001 у систему управління інформаційною безпекою організації з урахуванням сучасних кіберзагроз і нормативних вимог. Виявлено, що стандарт ISO/IEC 27001 є не лише технічним регламентом, а цілісною управлінською моделлю, яка дозволяє побудувати ефективну, адаптивну та стійку систему захисту інформації в умовах зростаючої складності IT-середовища.

Проведений аналіз існуючих загроз інформаційній безпеці дозволив деталізувати сучасні виклики, які стоять перед організаціями в цифрову епоху, та продемонструвати необхідність переходу від фрагментарних заходів до структурованого управління на основі міжнародних норм. Особливу увагу в роботі приділено інструментам аналізу ризиків, зокрема методикам OCTAVE і NIST RMF, які дозволяють гнучко адаптувати систему до специфіки конкретної організації. Це підкреслює важливість індивідуалізованого підходу до впровадження СУІБ.

У процесі дослідження було здійснено комплексну оцінку поточного стану інформаційної безпеки на об’єкті впровадження, визначено ключові вразливості, реалізовано базові заходи відповідно до вимог стандарту та здійснено внутрішній аудит. На основі результатів оцінки запропоновано низку рекомендацій щодо вдосконалення системи, які охоплюють як технічні, так і організаційні аспекти. Акцент зроблено на безперервності розвитку СУІБ, необхідності її адаптації до змін зовнішнього середовища, появи нових технологій та загроз.

Дослідження показало, що впровадження СУІБ на основі ISO/IEC 27001 дає змогу організаціям знижувати рівень інформаційних ризиків, забезпечуючи стратегічну сталість, підвищення конкурентоспроможності, довіру з боку партнерів, клієнтів і регуляторів. Аналіз процесів управління ризиками, розробка політик, вибір технічних інструментів, побудова механізмів реагування на

інциденти та моніторингу безпеки створюють основу для практичної реалізації принципів стандарту. Практична частина роботи довела, що при системному підході, належному рівні підтримки з боку керівництва та залученні персоналу впровадження стандарту є цілком досяжною і результативною метою.

Практична значущість дослідження полягає у створенні уніфікованого алгоритму, визначеному в таблиці 3.1. впровадження стандарту ISO/IEC 27001, який може бути використаний як методичний інструмент впровадження для організацій різних галузей.

Результати дослідження можуть застосовуватись під час побудови або модернізації системи управління інформаційною безпекою, а також під час підготовки до сертифікації відповідно до міжнародних вимог.

Проведене дослідження засвідчило, що дотримання стандарту ISO/IEC 27001 є не просто вимогою, а необхідністю для сучасної організації, яка прагне забезпечити надійний захист інформаційних активів, відповідати законодавчим і контрактним зобов’язанням, а також формувати довгострокову репутацію в середовищі цифрової довіри.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білецький І. П. Інформаційна безпека: навч. посіб. Львів: Львівська політехніка, 2021. 210 с.

2. Павлюк, О. В. Кібербезпека: теоретичні основи та практичні аспекти. Львів: Видавництво ЛНУ, 2021. 220 с.

3. IT Ukraine Association. Cybersecurity Guide для бізнесу. Київ: IT Ukraine, 2023. 34 с. URL: https:.itukraine.org.ua (дата звернення: 12.03.2025)

4. Семенов, В. І. Управління інформаційною безпекою підприємства: навч. посіб. Харків: ХНЕУ ім. С. Кузнеця, 2022. 312 с.

5. Хілько, Д. С. Менеджмент інформаційної безпеки: стратегія, політика, аудит. Одеса: ОНУ ім. Мечникова, 2023. 264 с.

6. РНБО України. Доктрина інформаційної безпеки України: офіційна редакція. Київ, 2022. URL: https:.www.rnbo.gov.ua (дата звернення: 22.03.2025)

7. PwC Ukraine. Cybersecurity Outlook 2022: Стан кіберзахисту українського бізнесу. Київ, 2022.

URL:https:.www.pwc.com/ua/uk/publications/cyber-outlookukraine2022.html (дата звернення: 23.03.2025)

8. Григоренко, І. М., & Лобанова, Н. О. Аудит інформаційної безпеки на підприємстві. Дніпро: Університет митної справи та фінансів, 2023. 145 с.

9. Андрущенко, В. П., Козлов, Д. В., & Тарасов, С. І. Інформаційна безпека в інформаційно-комунікаційних системах: навч. посіб. КНУ імені Тараса Шевченка, 2021. 248 с.

10. Smith, J., & Johnson, R. Implementing ISO/IEC 27001: A Practical Guide to Securing Information. London: IT Governance Publishing, 2023. 198 p.

11. Про інформацію : Закон України від 02.10.1992 № 2657-XII.

URL: https:.zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 29.03.2025)

12. Про захист інформації в інформаційно-телекомунікаційних системах Закон України від 05.07.1994 № 80/94-ВР.

URL: https:.zakon.rada.gov.ua/laws/show/80/94-вр

13. НД ТЗІ 2.5-010-03. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Держспецзв'язку України, 2003. 28 с.

14. Концепція забезпечення кібербезпеки України : Розпорядження КМУ № 962-р від 15.10.2020. URL: https:.zakon.rada.gov.ua/laws/show/962-2020-р (дата звернення: 01.04.2025)

15. Міністерство цифрової трансформації України. Національна стратегія з кібербезпеки України на 2021–2025 роки. Київ, 2021. URL: https:.cip.gov.ua/ua/news/strategiya-kyberbezpeky (дата звернення: 01.04.2025)

16. NIST SP 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: NIST, 2020. URL: https:.nvlpubs.nist.gov (дата звернення: 01.04.2025)

17. Доктрина інформаційної безпеки України: РНБО України. офіційна редакція. Київ, 2022. URL: https:.www.rnbo.gov.ua (дата звернення: 01.04.2025)

18. ISO/IEC 27001:2022. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Женева: ISO, 2022.

19. ISO/IEC 27002:2022. Інформаційні технології. Методи захисту. Кодекс практики для заходів інформаційної безпеки. Женева: ISO, 2022.

20. Чернуха, В. М. Технічні засоби захисту інформації: сучасні рішення. Львів: Видавництво ЛНТУ, 2023. 138 с.

21. ISO/IEC 27005:2018. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. Женева: ISO, 2018.

22. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Київ: ДП «УкрНДНЦ», 2016. 26 с.

23. ДСТУ ISO/IEC 27002:2017. Інформаційні технології. Методи захисту. Кодекс практики для заходів інформаційної безпеки. Київ: ДП «УкрНДНЦ», 2017. 106 с.

24. ProZorro. Вимоги до інформаційної безпеки у державних тендерах: методичні рекомендації. Київ, 2021. URL: https:.prozorro.gov.ua (дата звернення: 10.04.2025)

25. ISO/IEC 27019:2022. Інформаційна безпека для енергетичних об'єктів. Женева: IEC, 2022.

26. Von Solms, B., & van Niekerk, J. Information Security Governance. Cham: Springer, 2020. 95 p.

27. NIST SP 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: NIST, 2020. URL: https:.nvlpubs.nist.gov (дата звернення: 15.04.2025)

28. Петрик І. М. Методологія побудови системи управління інформаційною безпекою організації на основі міжнародних стандартів. Інформаційні технології та комп'ютерна інженерія. 2021. № 3(63). С. 45–53.

29. Сидоренко Л. О. Практичне впровадження стандарту ISO/IEC 27001 у сфері державного управління . Електронне урядування в Україні. 2020. № 2. С. 33–40.

30. Гончаренко С. В. Забезпечення кіберстійкості організації через впровадження ISO/IEC 27001: аналіз ефективності. Збірник наукових праць НАСОА. 2022. № 1(50). С. 112–119.

31. Швець О. О. Практика застосування ISO/IEC 27001 на підприємствах України: проблеми і рішення . Вісник Національного університету «Львівська політехніка». Серія: Інформаційні системи та мережі. 2022. № 3(137). С. 89–96.

32. ISO/IEC 27003:2017. Information technology – Security techniques – Information security management system implementation guidance. Geneva: ISO, 2017.

33. Іванченко М. Роль міжнародних стандартів у формуванні політики інформаційної безпеки державного сектору України . Державне управління: теорія та практика. 2021. № 2. С. 54–61.

34. Савчук І. Ю. Роль інформаційної безпеки у цифровій трансформації бізнесу: ISO/IEC 27001 як стратегічний інструмент . Бізнес-інформ. 2022. № 11. С. 135–140.

35. Громов В. Є. Інформаційна безпека в умовах гібридної війни: нормативно-правове забезпечення в Україні . Юридичний журнал України. 2023. № 4. С. 27–33.

36. Козлов С. В. Управління інформаційною безпекою в умовах цифрової трансформації . Інформаційні технології і засоби навчання. 2021. № 5(89). С. 29–39.

37. Мінаєва І. В. Ризикоорієнтований підхід до управління інформаційною безпекою організації . Управління розвитком складних систем. 2021. № 47. С. 123–130.

38. Шаповал А. В. ISO/IEC 27001 як інструмент стратегічного управління безпекою в українських компаніях . Вісник ХНУРЕ. 2020. № 1(59). С. 102–109.

39. Кабінет Міністрів України. Концепція забезпечення кібербезпеки України. Розпорядження КМУ № 962-р від 15.10.2020. URL: https:.zakon.rada.gov.ua/laws/show/962-2020-p (дата звернення: 15.04.2025)

40. Кривуля С. О. Аналіз практики впровадження ISO/IEC 27001 у вітчизняних підприємствах . Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління проектами. 2022. № 2(1402). С. 84–90.

41. Ткаченко С. І. Захист інформації в сучасному цифровому середовищі: загрози, інструменти, стандарти . Інформаційне суспільство. 2021. № 3. С. 44–50.

42. Процик В. О. Побудова інформаційної безпеки підприємства згідно з вимогами ISO/IEC 27001 . Збірник наукових праць «Економіка та держава». 2023. № 2. С. 75–79.

43. Рекомендації щодо впровадження системи управління інформаційною безпекою згідно з вимогами ISO/IEC 27001. Державна служба спеціального зв’язку та захисту інформації України. Київ, 2020. URL: https:.cip.gov.ua/ua/news/rekomendaciyi-27001 (дата звернення: 15.04.2025)

44. Марков В. А. Практичні аспекти адаптації міжнародних стандартів інформаційної безпеки в Україні . Економіка. Фінанси. Право. 2022. № 4. С. 57–60.

45. Войцехівський О. І. Інформаційна безпека в цифровій економіці: принципи, стандарти, стратегії . Економіка та суспільство. 2023. № 51. С. 212–218.

46. Коваленко А. С. Забезпечення відповідності міжнародним стандартам у галузі інформаційної безпеки: досвід вітчизняних компаній . Вісник Київського національного університету технологій та дизайну. 2022. № 6. С. 89–94.

47. Літвиненко П. В. Побудова ISMS на державних підприємствах: кроки до впровадження ISO/IEC 27001 . Збірник наукових праць «Інформаційні технології і безпека». 2022. № 1(17). С. 66–73.

48. Черняк В. Я. Методологічні аспекти впровадження стандарту ISO/IEC 27001 в умовах гібридних загроз . Актуальні проблеми інформаційної безпеки. 2023. № 3. С. 15–22.

49. Яворський І. Р. Роль міжнародних стандартів в оцінюванні кіберризиків малого та середнього бізнесу . Бізнес Інформ. 2023. № 8. С. 172–178.

50. Андрушко М. Ю. Нормативне забезпечення інформаційної безпеки в Україні: аналіз відповідності стандартам ISO/IEC 27001 . Публічне управління і адміністрування в Україні. 2022. № 20. С. 99–104.

51. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. URL : https:.zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 26.04.2025)

52. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. URL: https:.zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 26.04.2025)

53. Міністерство цифрової трансформації України. Національна стратегія з кібербезпеки України на 2021–2025 роки. Київ, 2021. URL: https:.cip.gov.ua/ua/news/strategiya-kyberbezpeky (дата звернення: 26.04.2025)

54. European Union Agency for Cybersecurity (ENISA). ISO 27001 Implementation Guide. Brussels: ENISA Publications, 2022. URL: https:.www.enisa.europa.eu/publications (дата звернення: 26.04.2025)

55. World Economic Forum. Global Cybersecurity Outlook 2023. Geneva: WEF, 2023. URL: https:.www.weforum.org/reports/globalcybersecurity-outlook-2023 (дата звернення: 26.04.2025)

56. Gartner Research. Key Steps for a Successful ISO/IEC 27001 Certification Journey. Stamford, 2022. URL: https:.www.gartner.com/en/documents/27001-certification (дата звернення: 26.04.2025)

57. Національний координаційний центр кібербезпеки при РНБО. Огляд стану кіберзахисту в Україні 2023. Київ, 2023. URL: https:.ncscc.gov.ua (дата звернення: 27.04.2025)

58. Information Security Forum. The Standard of Good Practice for Information Security 2022. London: ISF, 2022. URL: https:.www.securityforum.org (дата звернення: 27.04.2025)

59. Deloitte Ukraine. Управління інформаційною безпекою в Україні: виклики, тренди, рішення. Аналітичний звіт. Київ: Deloitte, 2021. URL: https:.www2.deloitte.com/ua/uk/pages/risk/articles/cybersecurity.html (дата звернення: 05.05.2025)

60. EY Ukraine. Інформаційна безпека 2021: стратегія або необхідність? Київ: Ernst & Young, 2021. URL: https:.www.ey.com/uk_ua/cybersecurity (дата звернення: 05.05.2025)

61. The CyberPeace Institute. Mapping ISO/IEC 27001 Implementation Globally. Geneva, 2023. URL: https:.cyberpeaceinstitute.org/reports/iso-map (дата звернення: 05.05.2025)

62. IT Ukraine Association. Cybersecurity Guide для бізнесу. Київ: IT Ukraine, 2023. 34 с. URL: https:.itukraine.org.ua (дата звернення: 05.05.2025)

Додаток А

Зразок документа аудиту відповідності ISO/IEC 27001

Назва документа:
`Внутрішній аудит СУІБ: Звіт про відповідність вимогам ISO/IEC 27001:2022`

1. Загальні відомості

Дата аудиту: 05.05.2025
Аудитори: Прізвище, ім’я
Підрозділи, що перевірялись: [ІТ-відділ, бухгалтерія тощо]
Об’єкт аудиту: Відповідність СУІБ вимогам ISO/IEC 27001:2022
Стандарт: ISO/IEC 27001:2022
Ціль аудиту: Перевірити ефективність впровадження та функціонування СУІБ

2. Підсумки аудиту

Розділ стандарту	Стан відповідності	Коментарі / Виявлені невідповідності
Розділ 4: Контекст організації	Відповідає	Контекст чітко визначено, визначено зовнішні та внутрішні чинники
Розділ 6: Планування	Частково відповідає	Відсутній формалізований реєстр ризиків
Annex A: A.9 Контроль доступу	Відповідає	Наявна матриця доступів, політика управління доступом

3. Виявлені невідповідності

№	Опис	Критичність (H/M/L)	Рекомендація	Відповідальний	Строк усунення
1	Відсутній журнал інцидентів ІБ	Середня	Впровадити систему реєстрації інцидентів	ІТ-служба	20.05.2025

4. Висновок

Впровадження СУІБ здійснено на 85%. Виявлені недоліки не є критичними, але потребують усунення до проходження зовнішнього сертифікаційного аудиту.

5. Додатки

Копії політик, процедур
Матриця відповідності Додаток А
Фото/скани реєстрів або журналів
Протоколи інтерв’ю з персоналом

Додаток Б

Шаблон матриці відповідності Додатку А (ISO/IEC 27001:2022)

№	Контроль з Annex A (ISO/IEC 27001:2022)	Назва контролю	Застосовується (Так/Ні)	Причина незастосування (якщо «Ні»)	Документ, що підтверджує виконання	Відповідальний
A.5.1	Policies for information security	Політики ІБ	Так	–	Політика ІБ, Наказ №1	Керівник ІБ
A.5.13	Information security in project management	Безпека у проєктах	Ні	В організації немає ІТ-проєктів	–	–
A.6.1	Organizational roles, responsibilities and authorities	Ролі та обов’язки	Так	–	Посадові інструкції, Наказ №2	HR + Керівник ІБ
A.8.9	Disposal of media	Знищення носіїв	Так	–	Інструкція з утилізації, Акт списання	ІТ-служба