Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: «Методика впровадження міжнародних стандартів з кібербезпеки на об'єкті інформаційної діяльності»

Виконавець: студенка IV курсу, групи КБ-41

_____ **Оксана ХРИСТУНОВА**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Микола БРАІЛОВСЬКИЙ
Нормоконтроль		Олександр ЛУКАШОВ

Київ 2025

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедрою
кібербезпеки та захисту інформації
_____Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека та захист інформації
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** (група) **Христуновій Оксані Олександрівні** (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Методика впровадження міжнародних стандартів з кібербезпеки на об'єкті інформаційної діяльності

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від «28».11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Міжнародні стандарти у сфері ІБ, науково-методична література, нормативно-правова база України, існуючі практики та підходи до впровадження СУІБ

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Роль стандартизації у забезпеченні кібербезпеки, СУІБ: сутність та ключові фактори успішної реалізації, детальний аналіз міжнародного стандарту ISO/IEC 27001:2022, процедура сертифікації СУІБ за стандартом ISO/IEC 27001:2022, взаємозв'язок ISO/IEC 27001 та ISO/IEC 27002, етапи та підходи до впровадження СУІБ, розробка методики впровадження міжнародних стандартів на основі циклу PDCA, фаза планування (Plan), фаза впровадження (Do), фаза моніторингу та перегляду (Check), фаза постійного вдосконалення (Act), висновки.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Підвищення доступності та ефективності реалізації СУІБ на основі міжнародних стандартів для об’єктів інформаційної діяльності.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: «29» листопада 2024 року

Завдання видав	_____	Микола БРАІЛОВСЬКИЙ
	(підпис)	(ім’я, прізвище)
Завдання прийняла до виконання	_____	Оксана ХРИСТУНОВА
	(підпис)	(ім’я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 27.01.2025	*виконано*
2	Аналіз літератури та міжнародної нормативно-правової бази в сфері кібербезпеки	28.01.2025 – 10.02.2025	*виконано*
3	Дослідження ролі стандартизації та принципів функціонування СУІБ	11.02.2025 – 21.02.2025	*виконано*
4	Вивчення стандарту ISO/IEC 27001:2022 та процедури сертифікації	22.02.2025 – 07.03.2025	*виконано*
5	Аналіз заходів контролю згідно з ISO/IEC 27002	08.03.2025 – 18.03.2025	*виконано*
6	Вивчення підходів до управління ризиками за ISO 31000 та ISO/IEC 27005	19.03.2025 – 05.04.2025	*виконано*
7	Дослідження підходів впровадження СУІБ	06.04.2025 – 15.04.2025	*виконано*
8	Розробка методики впровадження СУІБ, що підвищить доступність та ефективність реалізації СУІБ на основі міжнародних стандартів для організацій	16.04.2025 – 21.05.2025	*виконано*
9	Узагальнення результатів, формування висновків	21.05.2025 – 03.06.2025	*виконано*
10	Оформлення пояснювальної записки	03.06.2025 – 08.06.2025	*виконано*
11	Підготовка до захисту	09.06.2025 – 13.06.2025	*виконано*

Завдання видав _____ Микола БРАЇЛОВСЬКИЙ
(підпис) (ім’я, прізвище)

Завдання прийняла до виконання _____ Оксана ХРИСТУНОВА
(підпис) (ім’я, прізвище)

Термін подання кваліфікаційної роботи до ЕК «13» червня 2024 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та двох додатків. Основний текст займає 96 сторінок, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. У пояснювальній записці кваліфікаційної роботи міститься 6 рисунків і 23 таблиці.

Метою роботи є розробка методики поетапного впровадження СУІБ на основі міжнародних стандартів.

Для досягнення зазначеної мети поставлено наступні завдання:

- проаналізувати роль та значення міжнародних стандартів у забезпеченні інформаційної безпеки
- здійснити поглиблений аналіз міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002 та ISO 31000
- дослідити існуючі підходи впровадження СУІБ згідно з вимогами серії стандартів ISO 27000
- розробити методику впровадження СУІБ, що підвищить доступність та ефективність реалізації СУІБ на основі міжнародних стандартів для організацій.

Об’єктом дослідження є процес впровадження та функціонування системи управління інформаційною безпекою в організаціях.

Предметом дослідження є методика впровадження СУІБ, що відповідає вимогам міжнародних стандартів, для об’єкту інформаційної діяльності.

Практичною цінністю отриманих результатів є те, що розроблена методика надає організаціям чіткий, поетапний посібник для впровадження міжнародних стандартів інформаційної безпеки, значно спрощуючи та прискорюючи процес побудови ефективної СУІБ. Вона дозволяє системно управляти ризиками, впроваджувати необхідні заходи контролю та

забезпечувати безперервне вдосконалення, що є критично важливим для підвищення рівня кібербезпеки та стійкості бізнесу в умовах постійних загроз.

Ключові слова: інформаційна безпека, міжнародні стандарти, ISO/IEC 27001, управління ризиками, СУІБ, ISO/IEC 27002, ISO/IEC 27005, ISO 31000, методика впровадження, захист інформаційних активів.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ − Інформаційна безпека;

СУІБ − Система управління інформаційною безпекою

НБУ − Національний банк України

НПА − Нормативно-правовий акт

ПД − Персональні дані

ПЗ − Програмне забезпечення

ІС − Інформаційна система

ІТ − Інформаційні технології

ЦОД − Центр обробки даних

СЕДО − Система електронного документообігу

СКУД − Система контролю та управління доступом

ЗУ − Закон України

API − Application Programming Interface – інтерфейс програмування додатків

BSI − British Standards Institution – Британський інститут стандартів

CERT-UA − Government Computer Emergency Response Team of Ukraine – Урядова команда реагування на комп’ютерні надзвичайні події України

CIA − Confidentiality, Integrity, Availability – Конфіденційність, цілісність, доступність

CMMC − Cybersecurity Maturity Model Certification – Модель сертифікації зрілості кібербезпеки

CSF − Cybersecurity Framework – Фреймворк кібербезпеки

DDoS − Distributed Denial of Service – Розподілена атака типу "відмова в обслуговуванні"

DLP − Data Loss Prevention – Запобігання витоку даних

ENISA − European Union Agency for Cybersecurity – Агентство Європейського Союзу з кібербезпеки

FISMA − Federal Information Security Management Act – Закон про управління інформаційною безпекою у федеральних установах США

GDPR − General Data Protection Regulation – Загальний регламент про захист даних

HIPAA − Health Insurance Portability and Accountability Act – Закон США про переносимість і підзвітність медичного страхування

IAF − International Accreditation Forum – Міжнародний форум з акредитації

IoT − Internet of Things – Інтернет речей

ISO − International Organization for Standardization – Міжнародна організація зі стандартизації

KPIs − Key Performance Indicators – Ключові показники ефективності

MTTR − Mean Time To Respond – Середній час на реагування

NDA − Non-Disclosure Agreement – Угода про нерозголошення

NIST − National Institute of Standards and Technology – Національний інститут стандартів і технологій США

PCI DSS − Payment Card Industry Data Security Standard – Стандарт безпеки даних індустрії платіжних карток

PDCA − Plan-Do-Check-Act – Плануй-Виконуй-Перевіряй-Дій

PESTEL − Political, Economic, Social, Technological, Environmental, Legal – Політичні, Економічні, Соціальні, Технологічні, Екологічні, Правові фактори

PII − Personally Identifiable Information – Персонально ідентифікована інформація

PwC − PricewaterhouseCoopers (міжнародна аудиторська та консалтингова компанія)

RACI − Responsible, Accountable, Consulted, Informed – Відповідальний, Підзвітний, Консультує, Інформований

ROI − Return on Investment – Рентабельність інвестицій

SIEM − Security Information and Event Management – Управління інформацією та подіями безпеки

SMART − Specific, Measurable, Achievable, Relevant, Time-bound – Конкретні, Вимірювані, Досяжні, Релевантні, Обмежені в часі

SoA − Statement of Applicability – Заява про застосовність

SOC − System and Organization Controls – Звітність за системою контролю організацій

SOX − Sarbanes-Oxley Act – Закон Сарбейнса–Окслі

SWOT − Strengths, Weaknesses, Opportunities, Threats – Сильні сторони, Слабкі сторони, Можливості, Загрози

TÜV SÜD − Technischer Überwachungsverein Süd (Технічний наглядовий союз Південний) – Міжнародний сертифікаційний орган

ВСТУП

Актуальність. У сучасному світі, де інформація є ключовим активом, а цифровізація охоплює всі сфери діяльності, питання інформаційної безпеки набувають критичного значення. Зростаюча кількість та витонченість кіберзагроз − від цілеспрямованих кібератак та витоків конфіденційних даних до програм-вимагачів та інсайдерських загроз − постійно еволюціонують, несучи значні фінансові, репутаційні та операційні ризики для організацій будь-якого масштабу.

У цьому контексті, впровадження ефективної Системи управління інформаційною безпекою на основі міжнародних стандартів, зокрема серії ISO/IEC 27000, є не просто рекомендацією, а життєвою необхідністю. Ці стандарти пропонують визнану світову методологію для системного та комплексного управління ІБ. Вони дозволяють організаціям не тільки захищати свої інформаційні активи, а й демонструвати довіру своїм партнерам та клієнтам, забезпечувати відповідність зростаючим регуляторним вимогам (наприклад, GDPR, національне законодавство про кібербезпеку) та підвищувати свою конкурентоспроможність на ринку.

Незважаючи на очевидні переваги стандартизованого підходу, процес впровадження міжнародних стандартів інформаційної безпеки часто стикається зі значними викликами. Це може бути пов'язано з відсутністю чіткої, практично орієнтованої дорожньої карти, складністю адаптації загальних вимог стандартів до унікальних операційних умов конкретної організації, а також труднощами з інтеграцією нових процесів ІБ у вже існуючу корпоративну культуру та операційну діяльність.

Саме тому розробка уніфікованої, структурованої методики поетапного впровадження міжнародних стандартів інформаційної безпеки, заснованої на принципах циклу PDCA (Plan-Do-Check-Act), набуває особливої актуальності. Така методика надасть організаціям чіткий, послідовний та деталізований посібник, що спростить процес побудови та вдосконалення СУІБ. Вона

забезпечить системний підхід до управління ризиками, ефективне впровадження необхідних контролів, безперервний моніторинг ефективності та постійну адаптацію до мінливого ландшафту кіберзагроз, що є запорукою довгострокової стійкості та безпеки інформаційних активів.

Розроблена методика спрямована не лише оптимізувати та спростити процес відповідності міжнародним вимогам, а й суттєво сприяти підвищенню загального рівня інформаційної безпеки, зниженню операційних ризиків та зміцненню позицій організації на ринку в умовах постійних та зростаючих кіберзагроз.

Метою кваліфікаційної роботи є розробка методики поетапного впровадження СУІБ на основі міжнародних стандартів, що зробить цей процес більш доступним та підвищить ефективність управління інформаційною безпекою на організаційному рівні.

Досягнення мети потребує розв’язання таких *задач*:

- аналіз ролі та значення міжнародних стандартів у забезпеченні інформаційної безпеки;
- поглиблений аналіз міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002 та ISO 31000;
- дослідження існуючих підходів впровадження СУІБ згідно з вимогами серії стандартів ISO 27000;
- розробка методику впровадження СУІБ, що підвищить доступність та ефективність реалізації СУІБ на основі міжнародних стандартів для організацій.

Об'єкт дослідження: процес впровадження та функціонування системи управління інформаційною безпекою в організаціях.

Предмет дослідження: Методика впровадження СУІБ, що відповідає вимогам міжнародних стандартів, для об’єкту інформаційної діяльності.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. Українські науковці та експерти активно досліджують проблеми інформаційної безпеки, що відображено у значній кількості публікацій. Основна увага приділяється:

- Зростанню кіберзагроз: Вітчизняні джерела підкреслюють постійне збільшення кількості та складності кібератак на державні установи та приватний сектор України, особливо в умовах повномасштабної війни (за даними Держспецзв'язку України, звіт за 2023 рік). Аналізуються вектори атак, такі як фішинг, шкідливе програмне забезпечення, DDoS-атаки, а також їхні наслідки для критичної інфраструктури та бізнесу (згідно з публікаціями НБУ, звіт про кібербезпеку, 2023).
- Правовому та нормативному регулюванню: Значна частина робіт присвячена аналізу українського законодавства у сфері кібербезпеки та захисту інформації (наприклад, дослідження Калініченко, 2022; Закон України «Про основні засади забезпечення кібербезпеки України»). Обговорюються питання його імплементації, відповідності міжнародним стандартам та необхідності подальшого гармонізації з європейським законодавством (згідно з аналітичними матеріалами Національного інституту стратегічних досліджень, 2023).
- Побудові систем управління інформаційною безпекою: Вітчизняні автори часто звертають увагу на теоретичні аспекти та практичні рекомендації щодо створення СУІБ (наприклад, роботи О.В. Хорошка, 2018; Л.М. Безкоровайної, 2021). Проте, як свідчить аналіз цих праць, бракує уніфікованих, деталізованих методик поетапного впровадження міжнародних стандартів, адаптованих до українських реалій, що робить цей процес складним для багатьох організацій.
- Особливостям кібербезпеки в умовах гібридної війни: Окремий блок досліджень стосується унікального досвіду України у протидії

кіберагресії, аналізу кібератак на енергетичний сектор, фінансові установи та державні реєстри (за даними CERT-UA, 2022-2024 роки).

В цілому, вітчизняна література підтверджує критичну важливість проблеми ІБ та наявність законодавчої бази, але висвітлює потребу у більш практичних інструментах та методиках для ефективного впровадження міжнародних стандартів.

Зарубіжні джерела демонструють більш глибокий та різноманітний підхід до проблематики інформаційної безпеки, що зумовлено ширшим досвідом впровадження міжнародних стандартів та більшими інвестиціями у дослідження та розвиток ІБ (згідно з Gartner Hype Cycle for Cyber Security, 2023). Тут виділяються такі ключові аспекти:

- Комплексність загроз та управління ризиками: Зарубіжні експерти наголошують на ескалації глобальних кіберзагроз, що вимагають впровадження проактивних та адаптивних стратегій управління ризиками (наприклад, дослідження ENISA, 2023; Ponemon Institute, Cost of a Data Breach Report, 2024). Значна увага приділяється інтеграції управління ризиками ІБ у загальну систему управління ризиками підприємства (Enterprise Risk Management). Стандарти, як ISO 31000 та ISO/IEC 27005, є основою для цих підходів (відповідно до ISO/IEC, Guidance on Information Security Risk Management).
- Роль міжнародних стандартів (ISO 27000-серія): Переважна більшість публікацій визнає ISO/IEC 27001 як золотий стандарт для побудови СУІБ (згідно з працями John T. Case, 2020; British Standards Institution, 2023). Детально розглядаються його вимоги, а також роль ISO/IEC 27002 як кодексу практик, що надає конкретні заходи контролю. Обговорюються переваги сертифікації за ISO 27001 для підвищення довіри, зниження витрат на аудит та забезпечення відповідності (за даними ISO Survey, 2022; BSI Group, 2024).
- Практики впровадження та виклики: Зарубіжна література рясніє описами практичних кейсів впровадження СУІБ, аналізом успішних стратегій

та розбором типових перешкод (наприклад, публікації ISACA, 2023; NIST, Cybersecurity Framework, 2022). Часто підкреслюється важливість підходу PDCA (Plan-Do-Check-Act) як універсального циклу для безперервного вдосконалення СУІБ (згідно з працями W. Edwards Deming, 1993; ISO, Introduction to Management System Standards). Виклики включають нестачу кваліфікованого персоналу, опір змінам, складність інтеграції СУІБ з існуючими бізнес-процесами та необхідність безперервного моніторингу ефективності (за даними (ISC), Cybersecurity Workforce Study, 2023).

Аналіз вітчизняної та зарубіжної літератури виявляє, що проблема забезпечення інформаційної безпеки є однією з ключових та найбільш динамічних викликів для сучасних організацій. Незалежно від географічного розташування чи сектору економіки, компанії стикаються зі зростаючими загрозами, що вимагають системного та безперервного підходу до захисту інформаційних активів.

Галузь застосування. Процеси впровадження та функціонування СУІБ у організаціях, що прагнуть створити або вдосконалити свою СУІБ на основі загальновизнаних світових стандартів

Практична цінність полягає у тому, що розроблена методика надає організаціям чіткий, поетапний посібник для впровадження міжнародних стандартів інформаційної безпеки, значно спрощуючи та прискорюючи процес побудови ефективної СУІБ. Вона дозволяє системно управляти ризиками, впроваджувати необхідні заходи контролю та забезпечувати безперервне вдосконалення, що є критично важливим для підвищення рівня кібербезпеки та стійкості бізнесу в умовах постійних загроз.

РОЗДІЛ 1. МІЖНАРОДНІ СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ОСНОВИ ТА НЕОБХІДНІСТЬ

1.1. Роль та значення стандартизації у забезпеченні кібербезпеки

Інформаційна безпека стосується процедур, розроблених для захисту даних від несанкціонованого доступу або змін, навіть коли дані перебувають у стані спокою або передаються. Вона охоплює широкий спектр питань, включаючи захист цифрових активів, де зберігаються конфіденційні дані.

Інформаційна безпека ґрунтується на трьох основних принципах, відомих як тріада CIA: конфіденційність, цілісність і доступність:

- Конфіденційність − надання доступу лише уповноваженим особам, які потребують доступу;
- Цілісність − збереження точності та повноти інформації;
- Доступність − забезпечення доступності інформації для уповноважених користувачів у момент, коли вона їм потрібна.

Що означає кожен із принципів тріади для інформаційної безпеки:

1. *Конфіденційність*. Коли організація вживає заходів для збереження своєї інформації у таємниці або конфіденційності, це називається конфіденційністю. У реальному житті це означає обмеження доступу до даних для запобігання небажаному розголошенню. Несанкціоноване розголошення інформації або несанкціонований доступ до інформаційних систем може бути попереджено шляхом впровадження заходів конфіденційності. Для ефективного дотримання принципу конфіденційності необхідно захищати конфіденційну інформацію, надаючи доступ лише тим особам, яким він необхідний для виконання службових обов’язків. Конфіденційність потрібна для запобігання витоку конфіденційної інформації стороннім особам. Дані користувачів можна

захистити, використовуючи механізми автентифікації, зокрема паролі, а також шифрування даних під час передавання або зберігання.

2. *Цілісність*. Цілісність означає здатність особи або об’єкта зберігати самостійність і стабільність. У сфері інформаційної безпеки це передбачає захист даних від неконтрольованого або несанкціонованого додавання, видалення чи модифікації. Цілісність ґрунтується на ідеї, що даним можна довіряти як точним і незміненим належним чином. Поняття незаперечності, тобто неможливості заперечити факт події або дії, тісно пов’язане з цілісністю. Цей принцип забезпечує незаперечність інформації та сервісів, а також простежуваність дій, здійснених з ними. Точність і узгодженість даних мають зберігатися завжди. Особливо в юридичних ситуаціях необхідно підтвердити збереження достовірності документів. Для забезпечення цілісності даних часто використовують хешування, цифрові підписи та цифрові сертифікати.

3. *Доступність*. Якщо бізнес володіє цінними системами, застосунками чи даними, які неможливо оперативно використовувати, це втрачає будь-який сенс. Доступність означає, що всі системи і застосунки функціонують належним чином, а ресурси є доступними для авторизованих користувачів своєчасно і надійно. Метою забезпечення доступності є гарантування того, що дані та сервіси доступні, коли необхідно приймати рішення. Доступність системи й послуг для авторизованих користувачів є критично важливою, оскільки вона повинна бути забезпечена в будь-який момент, коли виникає потреба. Резервування критичних систем, стійкість до відмов апаратного забезпечення, регулярне створення резервних копій, масштабні плани аварійного відновлення тощо − усе це є способами забезпечення доступності.

Кібербезпека − це сукупність процесів, технологій і практик, спрямованих на захист цифрової особистості, інфраструктури та даних, доступних через кіберпростір, від атак, пошкоджень і несанкціонованого доступу.

Технології завжди залишаються вразливими, оскільки наші суспільства дедалі більше залежать від цифрової інфраструктури. Широкий спектр кіберризиків, включаючи кібершахрайство, крадіжки інтелектуальної власності

та персонально ідентифікованої інформації, перебої в роботі сервісів, пошкодження або знищення майна, а також шпигунство за допомогою шкідливого ПЗ, постійно змінюється і створює загрозу для інфраструктури ІКТ. Побоювання щодо безпеки використання ІКТ підривають довіру громадськості та держав до їхнього революційного потенціалу як рушія економічного та соціального прогресу.

Незалежно від того, чи є компанія великою чи малою, вона повинна мати стратегію впровадження та підтримки кібербезпеки. Ряд організацій і груп визначили стандарти та процедури, яких слід дотримуватися при створенні ІТ-інфраструктури або забезпеченні хоча б базового рівня її захисту. Ці зібрання правил називаються фреймворками і стандартами.

Фреймворк за визначенням − це структура, що лежить в основі або поза межами певної системи. Фреймворк не визначає, яким чином реалізується система; він лише її описує. Як наслідок, компанія може заявляти про дотримання будь-якого фреймворку, за умови виконання всіх його вимог. Структура фреймворку може бути розширена додатковими компонентами, однак його базова основа залишається незмінною.

Стандарт, згідно з самим терміном, описує етапи та процедури виконання певної роботи, що й обумовлює його значущість. Прийняття міжнародного стандарту забезпечує уніфікований підхід до виконання завдання в будь-якій точці світу. Організація може розробити власні правила, адаптовані до внутрішнього контексту, або дотримуватись загальновизнаних міжнародних норм, правил і стандартів.

Останніми роками багато організацій працюють над стандартизацією базової інфраструктури безпеки підприємств, що оперують персонально ідентифікованою інформацією (PII) або фінансовими даними, з метою ускладнення доступу до них для несанкціонованих осіб. Це дозволяє компаніям бути впевненими, що їхні дані захищені від хакерів і, навіть у разі успішного злому, втрати інформації будуть мінімальними.

Важливою складовою IT-управління є формування та впровадження правил кібербезпеки. Політики кібербезпеки компанії мають бути тісно пов’язані з відповідними стандартами, формуючи засади ефективного управління ризиками. Типову структуру IT-управління наведено на рисунку 1.1. Стандарти кібербезпеки виступають критичною ланкою між принципами, що визначають політику, і реаліями щоденної експлуатації. Вони є основою для подальших впроваджувальних заходів, включаючи створення функціональних і технічних вимог, розробку архітектури та дизайну, операційні інструкції й процедури. Ієрархію IT-управління наведено на рис. 1.1.

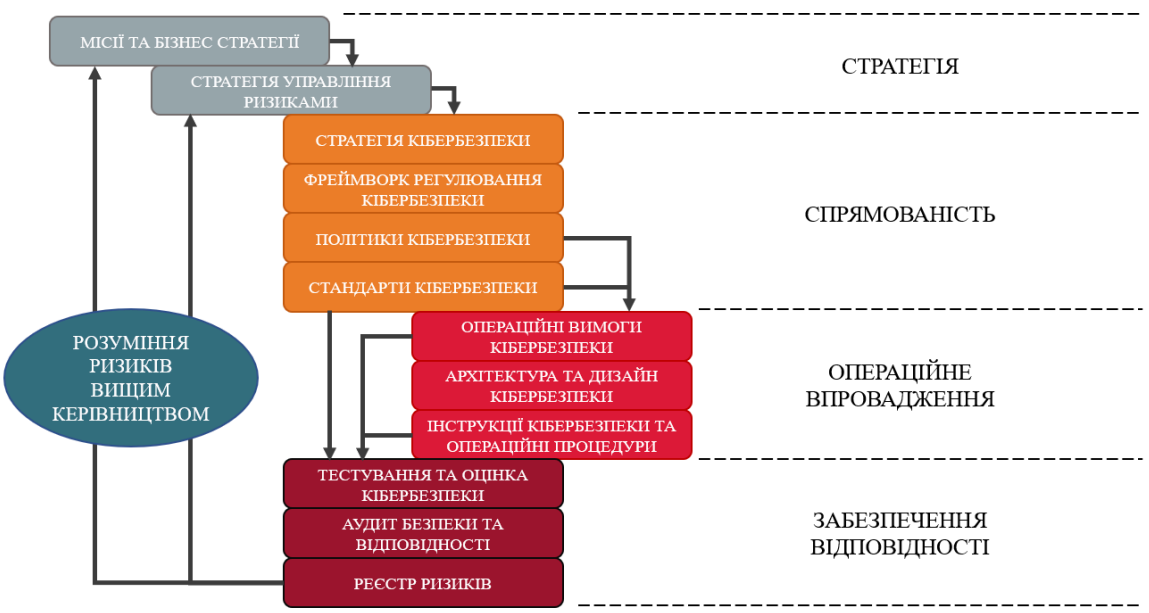

Рисунок 1.1. Ієрархія IT-управління

Пряма простежуваність є критичною на кожному рівні процесу IT-управління для забезпечення відповідності вимогам та ефективного управління IT-ресурсами, а також їхнього аудиту. Політики компанії та зовнішні регуляторні зобов’язання повинні бути відображені в її стандартах кібербезпеки (наприклад, зовнішніх стандартах і контрольних процедурах, таких як регулювання у сфері фінансів або конфіденційності даних).

Стандарти надають спільну систему орієнтирів, яка дозволяє оцінити, чи має організація процеси, процедури та інші контролі, що відповідають погодженому мінімальному рівню вимог. Залежно від потреб бізнесу або зацікавлених сторін, організація може створити та підтримувати власні процедури відповідно до принципів інформаційної безпеки. Якщо компанія відповідає вимогам певного стандарту, це надає третім сторонам − таким як клієнти, постачальники та партнери − впевненість у її здатності діяти згідно з визначеним рівнем якості.

Дотримання стандарту також може стати частиною маркетингової стратегії, що дозволяє компанії отримати конкурентну перевагу над іншими організаціями. Наприклад, при виборі між продуктами або послугами клієнт може віддати перевагу компанії, яка відповідає вимогам безпекового стандарту, над тією, яка такого відповідності не має.

З іншого боку, деякі нормативні та законодавчі вимоги прямо визначають обов’язковість дотримання певних стандартів у відповідних випадках. Наприклад, якщо компанія зберігає, обробляє або передає дані власників платіжних карток, вона зобов’язана відповідати Стандарту безпеки даних індустрії платіжних карток (PCI DSS). Даний стандарт поширюється на всі організації, що приймають кредитні та дебетові картки. Ведучі платіжні системи, зокрема Visa та Mastercard, визначили PCI DSS як галузевий еталон. Невиконання цих вимог може призвести до штрафних санкцій, підвищення вартості обробки транзакцій або навіть відмови у співпраці з окремими платіжними компаніями.

Крім того, якщо організація повинна була відповідати стандарту, але не зробила цього, і зазнала порушення безпеки, вона може бути притягнута до відповідальності в судовому порядку з боку споживачів, які постраждали внаслідок інциденту.

Стандарти також сприяють організаціям у дотриманні нормативно-правових актів, таких як Закон про захист даних (Data Protection Act), Закон Сарбейнса–Окслі (SOX), Закон про переносимість і підзвітність

медичного страхування (HIPAA) та інші подібні законодавчі акти. Використання стандартів як основи для управління та захисту інформаційних систем полегшує дотримання чинних і майбутніх нормативних вимог у порівнянні з організаціями, які ігнорують стандартизований підхід.

1. Сімейство стандартів інформаційної безпеки ISO/IEC 27000. Сімейство стандартів ISO 27000 з управління інформаційною безпекою − це сукупність стандартів, що становлять основу найкращих практик у сфері менеджменту інформаційної безпеки. Центральним елементом цієї серії є стандарт ISO 27001, який встановлює вимоги до СУІБ. ISO 27001 є міжнародним стандартом, що визначає критерії для побудови СУІБ. Його структура розроблена таким чином, щоб допомогти організаціям централізовано, узгоджено й економічно ефективно управляти процедурами безпеки.

2. Стандарт безпеки даних платіжних карток (PCI DSS). Рада зі стандартів безпеки індустрії платіжних карток (PCI SSC) − це незалежна організація, заснована компаніями Visa, MasterCard, American Express, Discover і JCB для адміністрування та нагляду за стандартом PCI DSS. Згідно з цим регламентом, компанії, фінансові установи та торговельні організації зобов’язані дотримуватись визначених вимог безпеки під час роботи з даними власників платіжних карток. Для цього необхідно підтримувати безпечне середовище для прийому, обробки, зберігання та передачі даних платіжних карт.

3. Закон про управління інформаційною безпекою у федеральних установах США (FISMA). Federal Information Security Management Act (FISMA) − це набір принципів забезпечення безпеки даних, обов’язкових для виконання федеральними агентствами США з метою захисту й збереження даних. Приватні підприємства, які мають контрактні зобов’язання з урядом, також підпадають під дію цього законодавства. FISMA спрямований на захист урядових даних та інформації, а також на забезпечення контрольованості витрат на безпеку. Закон встановлює набір вимог і стандартів, яких повинні дотримуватись державні установи для досягнення цілей захисту даних.

4. Закон США про переносимість і підзвітність медичного страхування (HIPAA). З метою захисту конфіденційності й недоторканності персональної медичної інформації Закон про переносимість і підзвітність медичного страхування (HIPAA), ухвалений у 1996 році (відомий також як Закон Кеннеді–Кассебаума), запровадив національні стандарти. HIPAA поширюється на всі форми захищеної медичної інформації (PHI), яка може бути використана для ідентифікації конкретної особи. Усі суб'єкти, що підпадають під дію закону − медичні установи, страхові плани, центри обробки медичних даних − зобов'язані дотримуватися вимог HIPAA. Завдяки впровадженим стандартам безпеки пацієнти можуть бути впевнені, що їхні ключові медичні дані залишаються конфіденційними.

5. Фреймворк кібербезпеки Національного інституту стандартів і технологій США (NIST CSF). Фреймворк кібербезпеки NIST є ефективним інструментом для структурування та вдосконалення програми кіберзахисту. Його було створено для підтримки організацій у формуванні та покращенні їхньої кіберстійкості. Програма кібербезпеки, побудована на основі NIST CSF, широко визнається галузевим стандартом. Він надає рекомендації щодо управління та зниження кіберризиків, ґрунтуючись на чинних стандартах, настановах та практиках. Хоча фреймворк NIST CSF спочатку призначався для захисту критичної інфраструктури США, його можуть використовувати організації будь-де у світі.

6. Звітність за системою контролю організацій (SOC). SOC (System and Organization Controls) − це звіти про внутрішній контроль, розроблені Американським інститутом дипломованих бухгалтерів (AICPA) для обслуговуючих організацій. Завдяки звітам SOC постачальники послуг можуть підвищити довіру клієнтів до наданих сервісів та продемонструвати ефективність власних внутрішніх контролів. Існує три типи звітів SOC: SOC 1, SOC 2 та SOC 3, вибір яких залежить від вимог до обліку, безпеки, конфіденційності чи доступності.

7. Модель сертифікації зрілості кібербезпеки (CMMC). CMMC (Cybersecurity Maturity Model Certification) − це фреймворк, який використовує Міністерство оборони США для оцінювання безпеки, компетентності та кіберстійкості своїх підрядників і субпідрядників. Його мета − забезпечити захищеність ланцюга постачання через усунення вразливостей. Фреймворк CMMC охоплює практики контролю, домени безпеки, процедури та функціональні можливості. Він має п’ять рівнів зрілості: від рівня 1 (найнижчого) до рівня 5 (найвищого). Очікується, що підрядники забезпечуватимуть відповідний рівень захисту залежно від обсягу даних, які обробляються в межах контракту. Отримання кожного рівня сертифікації вимагає відповідності визначеним вимогам і координації з елементами кібербезпеки.

Інформаційні стандарти безпеки допомагають підтвердити, що організація відповідає визначеним рівням захисту даних і дотримується вимог. Їх ефективне впровадження й управління є основною функцією СУІБ.

1.2. **СУІБ: Сутність та ключові фактори успішної реалізації**

Інформаційні активи набувають особливого значення в умовах зростаючої взаємозалежності бізнес-середовища. Унаслідок цієї зростаючої взаємопов’язаності інформація піддається дедалі більшій кількості та різноманітності загроз і вразливостей. Інформаційна безпека − це захист інформації від цього широкого спектра загроз з метою забезпечення безперервності бізнесу, зменшення втрат та підвищення рентабельності інвестицій.

Для досягнення інформаційної безпеки необхідно впровадити відповідний набір політик, процесів, процедур, організаційних структур, а також програмних і апаратних функцій, які мають бути створені, реалізовані, відслідковувані, переглянуті та вдосконалені, аби забезпечити досягнення визначених цілей у сфері безпеки та бізнесу.

СУІБ є фреймворком для створення, моніторингу, перегляду, підтримки та вдосконалення відповідності організації вимогам інформаційної безпеки з метою досягнення бізнесових і регуляторних цілей. Вона призначена для ефективної ідентифікації, зменшення та управління ризиками шляхом проведення оцінки ризиків з урахуванням ризик-апетиту організації. Аналіз вимог до захисту інформаційних активів і впровадження відповідних контролів для їх захисту сприяє ефективному функціонуванню СУІБ.

СУІБ охоплює політики, процеси, настанови, виділені ресурси та супутні дії, які організація координує з метою захисту своїх інформаційних активів.

Інформація − це впорядковані й оброблені дані, що мають змістовне значення в контексті для отримувача. Як і інші ключові бізнес-активи, інформація є критично важливою для функціонування організації й, відповідно, має бути належним чином захищеною. Цифрова інформація може зберігатися на електронних або оптичних носіях (наприклад, файли даних), паперова − у документах, а також у вигляді неформалізованих знань серед персоналу. Передача інформації можлива через кур'єра, електронну пошту, усне спілкування тощо − і вона має бути захищеною незалежно від способу передавання. У багатьох організаціях інформація залежить від інформаційно-комунікаційних технологій та інфраструктури. Ці технології часто є критичними компонентами організації, які підтримують створення, обробку, зберігання, передавання, захист і знищення інформації.

Конфіденційність, доступність і цілісність становлять три основні виміри інформаційної безпеки. Реалізація та управління належними заходами захисту в межах СУІБ, яка враховує широкий спектр можливих ризиків, сприяє зниженню наслідків інцидентів у сфері інформаційної безпеки та, таким чином, забезпечує довгостроковий успіх і безперервність діяльності організації.

Контролі впроваджуються відповідно до процесу управління ризиками та адмініструються за допомогою СУІБ для захисту визначених інформаційних активів у процесі досягнення цілей інформаційної безпеки. Ці контролі включають політики й процеси, а також процедури та організаційні структури.

З метою досягнення конкретних цілей організації в сфері інформаційної безпеки та бізнесу контрольні заходи мають бути визначені, впроваджені, оцінені, переглянуті та, за необхідності, оновлені. Під час реалізації заходів інформаційної безпеки слід враховувати характер і особливості бізнес-діяльності компанії. СУІБ гарантує, що заходи безпеки продовжують відповідати необхідним процесам та законодавчим вимогам. У цьому контексті впровадження СУІБ має розглядатися як стратегічне рішення для підприємства, оскільки її проєктування та реалізація залежать від потреб і цілей організації, вимог безпеки, застосовуваних процесів, а також її розміру та структури.

Управління охоплює дії, спрямовані на керування, контроль та постійне вдосконалення організації в межах належних організаційних структур. Діяльність у сфері управління включає дії, стилі або практики організації, керування, спрямування, контролю та регулювання ресурсів. У малих підприємствах управлінська структура може бути пласкою й складатися лише з однієї особи, тоді як у великих корпораціях вона може мати ієрархічну будову з десятками або навіть сотнями працівників.

З точки зору СУІБ, управління включає нагляд, підтримку та прийняття рішень, необхідних для досягнення бізнесових цілей і виконання регуляторних вимог шляхом забезпечення захисту інформаційних активів організації. Управління інформаційною безпекою проявляється у розробці та впровадженні необхідних політик, процесів і настанов, які надалі реалізуються в межах організації.

Система управління використовує фреймворк для допомоги організації у досягненні її цілей. Впровадження системи управління передбачає врахування структури організації, політик, планування діяльності, а також ролей і обов’язків.

СУІБ допомагає організації досягати таких результатів:

- виконання вимог усіх зацікавлених сторін у сфері інформаційної безпеки;

- більш ефективне проєктування та реалізація організаційних завдань;
- досягнення поставлених цілей у сфері інформаційної безпеки;
- дотримання чинного законодавства, нормативних вимог і галузевих найкращих практик;
- забезпечення системного управління інформаційними активами.

СУІБ відображає ставлення організації до захисту даних. Впровадження СУІБ може мати особливе значення для організації в контексті захисту як власних даних, так і даних клієнтів.

СУІБ має ключове значення, оскільки забезпечує структурований підхід до захисту найбільш конфіденційних даних і активів компанії. Вона допомагає організаціям виявляти загрози для їхніх даних і активів та розробляти стратегії протидії.

Згідно з останнім дослідженням PwC, кожна четверта компанія у світі за останні три роки зазнала витоку даних, що спричинив втрати від 1 до 20 мільйонів доларів США і більше. За результатами дослідження IBM і Ponemon за 2022 рік, середня вартість витоку даних у 2022 році становила 4,35 мільйона доларів. У 2021 році середня вартість становила 4,24 мільйона доларів, а у 2020 році − 3,86 мільйона, що свідчить про зростання на 12,7%. Дослідження Британського інституту стандартів (BSI) засвідчило, що 51,6% організацій, які мають сертифіковану СУІБ, повідомили про зменшення кількості інцидентів безпеки.

СУІБ допомагає організації системно розробляти план обробки конфіденційної інформації, зокрема персональних даних і комерційно чутливої інформації. Це знижує ймовірність витоку даних, а також пов’язаних із ним фінансових збитків і репутаційних ризиків.

Необхідно належним чином реагувати на ризики, пов’язані з інформаційними активами організації. Кожен з таких активів супроводжується

відповідним ризиком, який слід враховувати й управляти ним за допомогою процесів управління ризиками. Інформаційна безпека потребує управління ризиками, що охоплює фізичні, людські та технологічні загрози для всіх типів інформації, яка зберігається або використовується компанією.

Це стратегічне рішення повинно бути безперервно інтегрованим, масштабованим і оновлюваним відповідно до потреб організації при розробці СУІБ.

Проєктування та впровадження СУІБ залежить від низки чинників, включно з цілями організації, вимогами безпеки, бізнес-процесами, а також її розміром і структурою. Під час розробки та функціонування СУІБ необхідно враховувати інтереси всіх зацікавлених сторін, зокрема споживачів, постачальників, ділових партнерів, акціонерів та інших ключових третіх осіб.

Важливість СУІБ важко переоцінити. Вона є ключовим інструментом ініціатив з управління ризиками в будь-якій галузі. Через взаємозв’язок публічних і приватних мереж, а також поширення обміну інформаційними активами, управління доступом до даних і їх обробкою стає дедалі складнішим. Окрім того, масове використання мобільних носіїв інформації створює потенційну загрозу ефективності чинних заходів контролю.

Підприємства, які дотримуються стандартів сімейства СУІБ, демонструють свою здатність впроваджувати послідовні та загальновизнані принципи інформаційної безпеки для своїх клієнтів і партнерів. При цьому проєктування та розробка інформаційних систем не завжди враховують вимоги інформаційної безпеки. Рівень відповідності вимогам безпеки, якого можна досягти виключно за допомогою технологічних засобів, є обмеженим. Такий підхід може виявитися неефективним, якщо його не доповнено належним управлінським механізмом та політиками/процедурами в межах СУІБ.

Інтеграція заходів безпеки в повнофункціональну інформаційну систему може бути складною й витратною. СУІБ потребує ретельного планування та уваги до деталей, оскільки передбачає визначення наявних контролів. Наприклад, для забезпечення належного дозволу на доступ та його обмеження

до інформаційних активів або приміщень необхідно спроєктувати та впровадити відповідні засоби контролю доступу. Такі контролі можуть бути технологічними, фізичними, адміністративними або комбінованими, залежно від специфіки діяльності компанії та її потреб у сфері безпеки.

Завдяки ефективному впровадженню СУІБ компанії можуть з більшою впевненістю захищати свої інформаційні активи, оскільки система сприяє виявленню та аналізу ризиків, впровадженню відповідних заходів контролю та дотриманню регуляторних вимог.

Існує низка чинників, які сприяють ефективному впровадженню СУІБ і допомагають компанії досягати своїх бізнес-цілей. До найважливіших критеріїв успіху належать:

- документована інформація щодо цілей, політик, процедур та реалізації заходів з інформаційної безпеки, яка доступна і узгоджена з бізнес-цілями організації;
- архітектура, впровадження, відстеження, підтримка та вдосконалення фреймворку інформаційної безпеки відповідно до культури та цінностей організації;
- підтримка і залученість усіх рівнів управління, особливо вищого керівництва. Впровадження має розпочинатися з ініціативи топменеджменту, щоб забезпечити формування належної культури на всіх етапах реалізації СУІБ. Такий підхід відомий як top-down;
- чітке розуміння потреб у сфері управління ризиками та інформаційної безпеки;
- успішне впровадження програм підвищення обізнаності, навчання та освіти у сфері інформаційної безпеки, які інформують усі зацікавлені сторони,

включаючи працівників, про визначені обов’язки організації в галузі інформаційної безпеки та мотивують їх дотримуватися встановлених вимог;

- ефективне управління інцидентами інформаційної безпеки;
- ефективна стратегія та процеси забезпечення безперервності бізнесу;
- адекватна система для оцінювання ефективності функціонування фреймворку інформаційної безпеки;
- постійне вдосконалення роботи системи управління шляхом виявлення та усунення невідповідностей у міру їх виникнення.

СУІБ підвищує ймовірність того, що організація регулярно досягатиме ключових критеріїв успіху, необхідних для захисту її інформаційних активів.

Серія стандартів ISO 27000 охоплює всі вимоги, включно з галузевими, для впровадження надійної та сталої СУІБ. Організація самостійно обирає, які саме елементи впроваджувати, виходячи з бізнес-вимог.

1.3. **Детальний аналіз міжнародного стандарту ISO/IEC 27001:2022**

Фреймворк ISO − це набір політик і процесів, які можуть бути використані організаціями. Стандарт ISO 27001 встановлює фреймворк, що допомагає організаціям будь-якого розміру та галузі системно й економічно ефективно захищати інформацію шляхом впровадження СУІБ. Він є конкурентною перевагою для бізнесу й демонструє іншим організаціям, що вашій компанії можна довірити обробку цінних інформаційних активів/даних і об’єктів інтелектуальної власності третіх сторін. Це відкриває низку нових можливостей і водночас знижує ризики для компанії.

Компанії можуть пройти сертифікацію за стандартом ISO 27001 і підтвердити своїм клієнтам і партнерам, що забезпечують захист даних, а також отримати необхідні знання та практики, передбачені стандартом. Окрім того,

фізичні особи можуть отримати сертифікацію як Lead Auditor або Lead Implementer стандарту ISO 27001. Цей стандарт має глобальне визнання як міжнародний.

ISO 27001 є міжнародним стандартом, що походить від управлінського стандарту BS 7799. Цей стандарт складався з двох частин:

- Частина 1: Кодекс практик, що стосується контролів та забезпечує формалізоване управління інформаційною безпекою. У грудні 2000 року він був прийнятий як ISO 17799: Інформаційні технології − Кодекс практик з управління інформаційною безпекою;
- Частина 2: Специфікація щодо впровадження СУІБ. Вперше була опублікована Британським інститутом стандартів (BSI) у 1999 році як СУІБ − Специфікація з настановами щодо використання. У 2002 році документ було оновлено з урахуванням моделі забезпечення якості PDCA (Plan-Do-Check-Act).

Стандарт BS 7799 був розроблений за підтримки Департаменту торгівлі та промисловості Великобританії (DTI) як керівництво для створення та впровадження СУІБ. BSI опублікував BS 7799 у 1995 році.

Основною метою BS 7799 було надати впевненості керівництву організації в ефективності заходів і підходів до інформаційної безпеки, навіть у випадках використання власних технологій. На момент свого створення стандарт мав на меті забезпечення безпеки корпоративної інформації за трьома основними напрямами: доступністю, конфіденційністю та цілісністю.

Важливо зазначити, що BS 7799 не охоплює захист від усіх можливих загроз − лише від тих, які організація вважає суттєвими, і лише в тому обсязі, в якому це економічно доцільно з погляду результатів оцінки ризиків.

Спочатку BS 7799 існував як єдиний стандарт і розглядався як кодекс поведінки. Його було створено не як специфікацію, яка могла б слугувати основою для зовнішньої перевірки третьою стороною та сертифікації, а радше як директиву для компаній. Проте, у міру того як підприємства почали

усвідомлювати масштаби, серйозність та взаємозв’язок ризиків інформаційної безпеки, а також на тлі зростання кількості законів і нормативних актів у сфері захисту даних та конфіденційності, виникла потреба в сертифікаційній опції, пов’язаній зі стандартом.

Унаслідок цього було створено другу частину стандарту − BS 7799-2, яка вже мала формат специфікації (частина 2).

Стандарти ISO 17799 та BS 7799-1 було віднесено до кодексу практик, що стосується контролів, а не систем управління інформаційною безпекою (частина 1). Крім того, було встановлено зв’язок між кодексом практик і стандартом, відповідно до якого ISO 27001 вимагав використання ISO 17799 як джерела рекомендацій щодо вибору та впровадження контролів.

У листопаді 2005 року Міжнародна організація зі стандартизації (ISO) прийняла BS 7799-2 як стандарт ISO/IEC 27001, і ISO 27001 став єдиним сертифікованим стандартом для систем управління інформаційною безпекою .

Стандарт ISO 27001 визначає критерії для створення, впровадження та підтримки СУІБ в організації. Повна назва останньої редакції стандарту, опублікованої у 2022 році, звучить як:

Інформаційна безпека, кібербезпека та захист конфіденційності − Системи управління інформаційною безпекою − Вимоги

(Information security, cybersecurity and privacy protection − Information security management systems − Requirements).

Стандарт складається з двох основних частин:

- Основна частина: містить 11 пунктів (Clause), пронумерованих від 0 до 10. Клаузи 0–3 описують сам стандарт, тоді як клаузи 4–10 встановлюють вимоги, яким має відповідати компанія для дотримання стандарту.
- Додаток A (Annex A): включає 93 контрольні заходи, які необхідно врахувати під час впровадження СУІБ.

Згідно з циклом PDCA (Plan-Do-Check-Act), розробленим В. Едвардсом Демінгом, бізнес-процеси слід розглядати як такі, що перебувають у постійному циклі зворотного зв'язку, аби управлінський персонал міг виявляти й коригувати ті частини процесу, які потребують удосконалення. Цикл PDCA наведено на рис. 1.2.

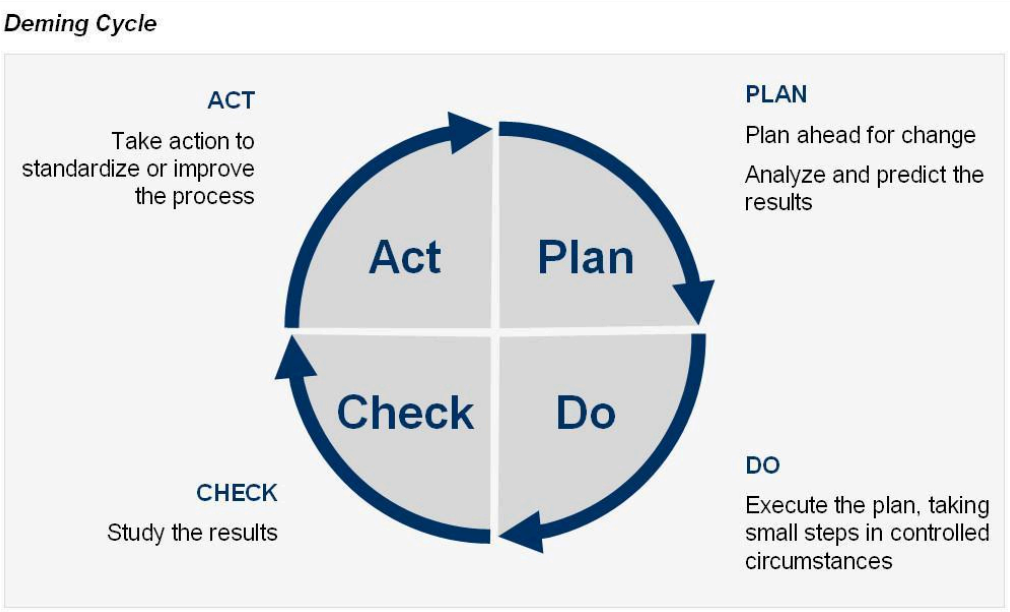

Рисунок 1.2. Цикл PDCA

Першим етапом має бути планування, за яким слідують впровадження та вимірювання ефективності. Результати вимірювань слід порівнювати з початково визначеними параметрами, щоб виявити будь-які відхилення або потенційні напрями для покращення. Отримані дані мають бути представлені керівництву для ухвалення рішення щодо подальших дій.

Передумовою для впровадження ISO 27001 є використання циклу PDCA, що бере свій початок у сфері забезпечення якості. Виконання PDCA є необхідним до моменту розуміння процесів, передбачених вимогами ISO 27001. Аналіз стандарту через призму PDCA дозволяє чіткіше уявити, як реалізується управління (governance) та як досягається узгодження із покращеними бізнес-цілями.

Детальніше розглянуто розділи стандарту ISO 27001 та їх відповідність фазам PDCA.

Розділи 0–3 є допоміжними та надають загальну інформацію про стандарт.

Розділ 0: Вступ − містить загальний огляд стандарту, пояснює його призначення та сумісність з іншими стандартами ISO;

Розділ 1: Сфера застосування − визначає обсяг дії стандарту й наголошує, що він застосовний до організацій будь-якого типу;

Розділ 2: Нормативні посилання − містить перелік джерел, що є обов'язковими для розуміння й впровадження сертифікаційного стандарту (у даному випадку ISO 27001). Ці посилання надають додаткові рекомендації, вимоги або практики, які слід враховувати при впровадженні СУІБ;

Розділ 3: Терміни та визначення − містить термінологію з ISO 27000, яка застосовується і в контексті ISO 27001.

Розділи 2 та 3 безпосередньо відсилають до стандарту ISO 27000, де наводяться необхідні терміни й визначення.

Фаза Plan (Планування) охоплює Розділи 4–7. Вона допомагає виявити можливості та спланувати зміни.

Розділ 4: Контекст організації − розуміння контексту організації є передумовою для успішного впровадження СУІБ (де і як функціонує організація). Це досягається шляхом аналізу зовнішніх і внутрішніх факторів, які впливають на інформаційну безпеку організації. До зовнішніх факторів належать законодавчі та нормативні вимоги, економічне та політичне середовище, соціальні й культурні норми, у межах яких діє компанія. Для розуміння внутрішніх факторів необхідно враховувати організаційну структуру, культуру, цінності компанії. Далі слід визначити сторони, зацікавлені в інформаційній безпеці організації, залежно від характеру її діяльності. До них можуть належати клієнти, партнери, постачальники, працівники, місцева влада тощо. Після ідентифікації таких сторін необхідно визначити їхні вимоги до інформаційної безпеки. Враховуючи різноманітність зацікавлених сторін,

вимоги також будуть відрізнятися. Наприклад, деякі клієнти можуть передавати конфіденційну або персональну інформацію, яка підпадає під дію законодавства, тому вони вимагатимуть належного її захисту. Наступним кроком є планування та погодження вимог, які буде реалізовано в межах СУІБ, що впроваджується.

Лише за умови ґрунтовного розуміння зазначених факторів можливо ефективно впровадити СУІБ в будь-якій організації.

Розділ 5: Лідерство − ключовими компонентами цього розділу є зобов'язання керівництва, політика інформаційної безпеки, а також організаційні ролі та обов'язки. Залучення вищого керівництва є обов'язковою умовою для ефективного функціонування системи управління. Воно є основою для формування політики та цілей у сфері інформаційної безпеки. Серед інших обов'язків, які мають бути виконані, − забезпечення ресурсами для підтримки СУІБ, включно з виділенням персоналу, часу та фінансів. Політика інформаційної безпеки повинна бути належним чином задокументована і доведена до відома всіх відповідних сторін − як усередині організації, так і за її межами. СУІБ має бути інтегрована в організаційні процеси й застосовуватись у повсякденній діяльності. Це формує позитивний приклад для працівників, завдяки чому СУІБ сприйматиметься не як окрема структура, а як частина загальної операційної діяльності компанії. Після впровадження СУІБ мають бути визначені й реалізовані кроки з її постійного вдосконалення. Керівництво може надати працівникам можливість надавати зворотний зв'язок і пропонувати покращення. Без належної підтримки керівництва впровадження СУІБ в організації, ймовірно, буде невдалим.

Політика інформаційної безпеки повинна відображати наміри компанії щодо захисту інформації та чітко засвідчувати зобов'язання керівництва щодо дотримання вимог безпеки та постійного вдосконалення СУІБ. Вона також має створювати передумови для встановлення цілей у сфері інформаційної безпеки. Політика інформаційної безпеки є основою СУІБ в будь-якій організації й

визначає її стратегічний вектор. Як документ найвищого рівня, вона не містить детальних описів засобів контролю безпеки.

Розділ 5 також стосується процесу чіткого визначення та розподілу конкретних ролей і відповідальності в межах організації. Призначення відповідальних осіб за питання інформаційної безпеки та донесення цих обов'язків до всіх співробітників дозволяє працівникам чітко розуміти, що від них очікується, як вони впливають на захист інформації та яким чином можуть зробити свій внесок. Вищим керівництвом призначаються два типи відповідальності: відповідальність за повноцінне впровадження СУІБ та відповідальність за моніторинг ефективності СУІБ і звітування перед керівництвом.

Розділ 6: Планування − у процесі планування в межах СУІБ слід постійно враховувати ризики та можливості. Ризики − це небажані події, які можуть мати негативні наслідки для компанії. Можливості − це дії, які організація може реалізувати для підвищення рівня інформаційної безпеки. Ідентифікація, документування та управління ризиками і можливостями є критично важливими для ефективного функціонування СУІБ, оскільки дозволяють організації зрозуміти сильні та слабкі сторони своєї операційної діяльності та використати їх для побудови ефективної системи захисту. Оцінка ризиків організації повинна враховуватися під час визначення цілей інформаційної безпеки. Також має бути чітко окреслено, що саме вважається прийнятним ризиком для компанії. За результатами оцінки формується план обробки ризиків. Усі оновлення СУІБ повинні проводитися планово.

Розділ 7: Підтримка − для забезпечення сталого функціонування СУІБ необхідно мати належну кількість компетентних ресурсів, відповідні знання, ефективну комунікацію та контроль за обробкою документованої інформації. Без належних ресурсів − як фінансових, так і людських − впровадження СУІБ неможливе. Це зона відповідальності керівництва. Організація повинна визначити, які навички є необхідними для виконання завдань у сфері інформаційної безпеки, і забезпечити наявність у персоналу відповідної

підготовки та досвіду. Підвищення кваліфікації може здійснюватися як за допомогою внутрішніх програм навчання, так і через зовнішнє навчання або наставництво. Навіть за умови наявності якісної документації та контролів, без належного розуміння персоналом способу їх реалізації ефективний захист неможливий. Працівники повинні знати, що саме робити і чому це важливо. Для цього можуть використовуватись електронна пошта, інформаційні розсилки, дискусійні групи, онлайн-курси. Ці інструменти сприяють кращому розумінню співробітниками цілей організації у сфері безпеки.

Комунікація інформації є сутністю розуміння, а усвідомлення того, що відбувається з безпекою, є ключовим чинником успіху СУІБ. У цьому контексті слід визначити, яку інформацію необхідно передавати як усередині компанії, так і за її межами, а також хто має право чи несе відповідальність за цю комунікацію. Правила комунікації формуються на основі цілей інформаційної безпеки організації.

Інформація повинна бути задокументована, розроблена, оновлена та контрольована відповідно до вимог стандарту ISO 27001. Вона може охоплювати як настанови щодо виконання процесів (політики, процедури тощо), так і підтвердження виконаних дій (записи). Важливо, щоб така інформація була захищеною і доступною у необхідний момент у придатному для використання вигляді. Також інформація має супроводжуватися чіткими ідентифікаторами, зокрема реєстраційним номером, назвою, датою створення та автором.

Розділ 8 − фаза Do (Виконання). Вона має на меті перевірку впроваджених змін.

Розділ 8: Функціонування − СУІБ повинна функціонувати на щоденній основі. Компанія впроваджує численні заходи контролю, процеси та дії з інформаційної безпеки для реагування на ризики й можливості та забезпечує, щоб усі дотримувалися встановлених вимог. Впровадження включає визначення критеріїв для процесів і реалізацію необхідних заходів контролю згідно з цими критеріями. Політики та процедури з інформаційної безпеки мають регулярно

переглядатися, щоб враховувати й адаптуватися до змін в організації. Такі зміни можуть бути як навмисними, так і ненавмисними. Для кожного процесу має бути визначений відповідальний власник. Зовнішні (аутсорсингові) операції організації повинні бути ідентифіковані та належним чином контрольовані з точки зору інформаційної безпеки.

Оцінка ризиків у сфері інформаційної безпеки також повинна проводитись регулярно та у заплановані інтервали. Перша оцінка ризиків може здатися значно складнішою, ніж наступні перегляди. Після оцінювання виконується стратегічно важливіше й дорожче завдання − обробка ризиків.

Докладна SoA разом із комплексною методикою оцінки й обробки ризиків становить основу для ухвалення рішень щодо подальших дій у сфері інформаційної безпеки.

Розділ 9 − фаза Check (Перевірка). Вона передбачає аналіз результатів перевірки, оцінювання ефективності та виявлення отриманих уроків.

Розділ 9: Оцінювання результативності − стандарт ISO 27001 вимагає, щоб функціонування СУІБ підлягало моніторингу, вимірюванню, аналізу та оцінюванню. Компанія самостійно визначає, що саме підлягає вимірюванню, і закріплює це у політиках, цілях та процедурній документації. Передусім оцінюється результативність заходів контролю та процесів інформаційної безпеки, зокрема у порівнянні з установленими політиками, цілями та процедурами. Методи, що використовуються для вимірювання та аналізу, мають бути чітко визначені для забезпечення достовірних результатів. Отримані результати подаються на розгляд вищому керівництву. Менеджмент повинен проводити перегляд СУІБ у встановлені терміни, з урахуванням статусу завдань з попередніх переглядів, інформації з внутрішнього й зовнішнього контексту, позицій зацікавлених сторін, результатів оцінки ризиків тощо. За результатами аналізу керівництво може прийняти рішення про вдосконалення, зокрема щодо автоматизації процесів.

Розділ 10 − фаза Act (Дія). Вона передбачає вжиття заходів на основі висновків, отриманих під час фази перевірки.

Розділ 10: Поліпшення − якщо якась вимога не була виконана, це вважається невідповідністю. Такі невідповідності повинні бути усунені шляхом вжиття коригувальних дій у найкоротший термін. Стандарт ISO 27001 вимагає, щоб організація зберігала записи, які підтверджують суть невідповідності, вжиті заходи, результати реалізованих коригувальних дій. Також компанія повинна впевнитися, що усунула саме першопричину невідповідності. Процедура коригувальних дій має бути задокументована та реалізована як елемент належної практики.

Крім того, постійне вдосконалення є невід'ємною частиною ISO 27001. СУІБ повинна ставати все більш придатною, адекватною та ефективною для досягнення своїх цілей.

Політика вдосконалення СУІБ може включати такі положення:

- визначення відповідальних осіб за планування, управління та координацію заходів щодо вдосконалення;
- комунікацію того, що всі працівники можуть робити внесок у процес постійного вдосконалення;
- визначення способів фіксації всієї релевантної інформації, пов'язаної з вдосконаленнями;
- впровадження вдосконалень шляхом документування змін, обґрунтування їх доцільності, очікуваних результатів та оцінювання ефективності здійснених змін.
- вдосконалення є безперервним процесом, у межах якого постійно визначається, що працює найкраще.

Друга частина стандарту ISO 27001, Додаток А (Annex A), містить 93 контрольні заходи, згруповані в чотири категорії. Документ SoA визначає, які саме заходи з Додатку А є застосовними для конкретної організації з

урахуванням таких чинників, як характер діяльності, чинне законодавство та нормативні вимоги. Визначення SoA є ключовим етапом впровадження фреймворку СУІБ. Це обов'язковий документ, що становить основу реалізації системи управління інформаційною безпекою.

Разом з тим, варто враховувати, що впровадження стандарту ISO 27001 в організації має і свої недоліки. Аналіз сильних і слабких сторін, можливостей та загроз (SWOT) дозволяє отримати реалістичне, об'єктивне та базоване на даних уявлення про результати впровадження.

У стратегічному плануванні аналіз SWOT використовується для оцінювання конкурентної позиції компанії та виявлення можливостей і загроз. SWOT-аналіз враховує як внутрішні, так і зовнішні чинники, а також поточні та майбутні можливості. SWOT-аналіз наведено на рис. 1.3.

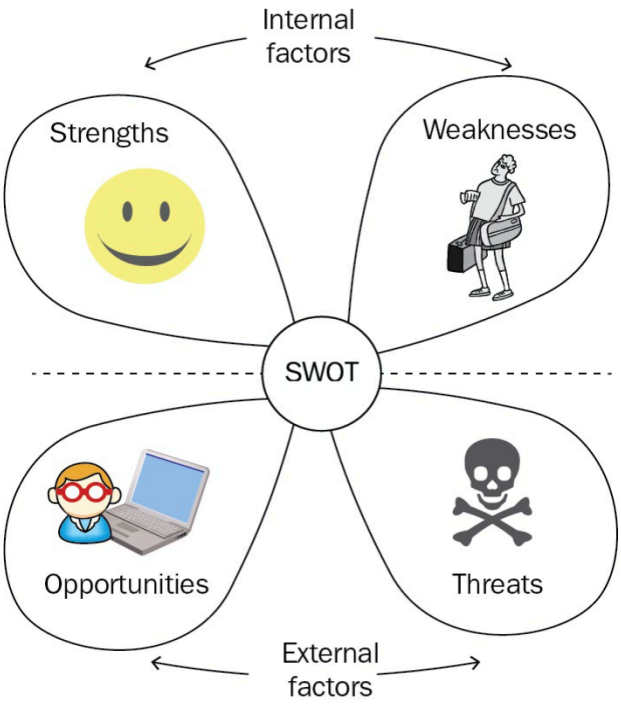

Рисунок 1.3. SWOT-аналіз

Впровадження СУІБ вимагає від організації витрат ресурсів і є стратегічним рішенням. Проведення SWOT-аналізу щодо впровадження СУІБ

може допомогти у визначенні контексту організації та зацікавлених сторін, а також забезпечити ефективність реалізації системи.

Такий аналіз є корисним для формування кращого розуміння середовища безпеки та підтримки бізнесу шляхом надання уявлення про активи, ризики, проблеми та виклики в галузі безпеки, з якими стикається ІТ-відділ, а отже, і бізнес у цілому.

Сильними сторонами впровадження СУІБ є:

- підвищення загального рівня безпеки в організації;
- краща демонстрація відповідності різним нормативам щодо захисту даних, що забезпечує підвищення рентабельності інвестицій;
- виділення бізнесу серед конкурентів в умовах зростаючої конкуренції;
- підвищення довіри та репутації компанії;
- чітко визначений життєвий цикл для усунення слабких місць;
- кращий захист інформації, особливо конфіденційної;
- впровадження найкращих практик управління безпекою;
- зниження витрат, пов’язаних із інцидентами інформаційної безпеки.

У деяких випадках впровадження СУІБ може виявитися слабким місцем для організації. Для прийняття ефективних рішень необхідно проаналізувати розрив між фактичними результатами та очікуваним ефектом. Основні слабкі сторони можуть включати:

- значні витрати часових, фінансових і людських ресурсів на впровадження;

- адаптація до нових процесів і процедур;
- складність і витрати, пов’язані з СУІБ, особливо якщо вона неправильно спроєктована або реалізована.

Впровадження СУІБ може відкрити нові можливості для бізнесу, зокрема:

- маркетингова перевага для компанії;
- виявлення можливостей для вдосконалення під час аудиту;
- покращення ринкової позиції, що сприяє залученню нових перспектив і партнерств.

Певні загрози, пов’язані з політикою безпеки та практиками, можуть виникати внаслідок впровадження СУІБ, зокрема:

- ризик розголошення інформації третім сторонам;
- високе навантаження на ресурси організації;
- надмірна впевненість у здатності СУІБ забезпечити повний захист усієї інформації.

У SWOT-аналізі сильні та слабкі сторони компанії, ініціативи або галузі розглядаються об’єктивно, з опорою на факти та статистичні дані. Аналіз не повинен містити упереджених припущень або “сірих зон”, а має бути зосередженим на реальних ситуаціях. Водночас його слід розглядати як рекомендаційний інструмент, а не як припис до обов’язкового виконання.

Попри те, що переваги впровадження переважають недоліки, проведення SWOT-аналізу до впровадження стандарту ISO 27001 забезпечує керівництво більшою ясністю щодо аспектів, на яких слід зосередити увагу. Після впровадження фреймворку СУІБ організація не лише підвищує свою репутацію,

а й бере на себе більшу відповідальність за дотримання правових і регуляторних вимог.

1.4. Процедура сертифікації СУІБ за стандартом ISO/IEC 27001:2022

У динамічному світі законодавчі та нормативні акти змінюються залежно від низки факторів, зокрема галузі, країни та типу інформації. У деяких сферах компанії добре обізнані з відповідними вимогами, тоді як в інших − тільки починають їх опановувати. Через зростання кількості та важливості інцидентів, пов’язаних із безпекою, уряди в усьому світі усвідомили необхідність захисту громадян і бізнесу від зловживання конфіденційною інформацією. Це постійно еволюційна сфера, оскільки розвиток технологій зумовлює появу нових законів і нормативних актів.

Без належних заходів безпеки компанія стає вразливою до кібернападів, значних штрафів і санкцій з боку регуляторних органів, судових позовів через недбалість, а також до небажаної уваги з боку ЗМІ, яка може підірвати її репутацію, бренд і загальну вартість. Необхідно чітко визначити та задокументувати всі законодавчі, нормативні, договірні вимоги, а також вимоги до безпеки систем.

Дотримання правових і регуляторних вимог не є виключною відповідальністю ІТ-відділу чи команди з інформаційної безпеки. Критично важливим є залучення інших ключових функцій, зокрема юридичного відділу, відділу кадрів і фінансів.

Залежно від моделі ведення бізнесу, компанії часто підпадають під дію кількох законодавств, у тому числі законів різних країн, деякі з яких можуть мати суперечливі вимоги. Оптимальною практикою є створення зведеної схеми всіх нормативно-правових і договірних зобов’язань у співпраці з юридичним відділом (або зовнішнім експертом). Щоб визначити, чи є чинні заходи безпеки достатніми для забезпечення відповідності, або чи потрібно вжити додаткових

заходів, слід виявити вимоги, які можуть вплинути на компанію, і обговорити результати з командою безпеки.

Консультації щодо застосовного законодавства та нормативів також можна отримати в професійних юридичних служб. Хоча відповідність нормативам суттєво впливає на інформаційну безпеку, надання повноважень юридичному відділу для аналізу відповідного законодавства або залучення зовнішніх спеціалістів дає змогу зекономити час і зусилля. Такі дії сприятимуть удосконаленню процедур безпеки та підвищенню комерційної цінності компанії в довгостроковій перспективі.

Орган сертифікації перевіряє дотримання нормативних вимог організацією, зокрема шляхом оцінювання того, чи впроваджено всі необхідні заходи контролю та чи вживаються відповідні дії у випадках невідповідності.

Отримання сертифіката ISO 27001 свідчить про відданість компанії постійному вдосконаленню, розвитку та захисту інформаційних активів і конфіденційних даних шляхом впровадження належної оцінки ризиків, прийнятних політик і відповідних засобів контролю.

Якщо організація отримує сертифікацію за стандартом ISO 27001, це означає, що її СУІБ було перевірено та підтверджено на відповідність стандарту іншою стороною − так званим сертифікаційним органом.

Організації, які мають сертифікат ISO 27001, публічно заявляють про те, що є надійними, впровадили СУІБ відповідно до вимог стандарту та пройшли офіційне підтвердження відповідності від сертифікаційного органу ISO. Сертифікація демонструє партнерам, зацікавленим сторонам і клієнтам, що компанія серйозно ставиться до управління інформаційною безпекою.

Головним органом, який здійснює нагляд за всією системою акредитації відповідності, є Міжнародний форум з акредитації (International Accreditation Forum, IAF). Це глобальна організація, до якої входять сертифікаційні органи з різних країн. Вона відповідає за розробку, зміну та проєктування ключових міжнародних стандартів.

Членство в IAF відкрите для акредитаційних органів, які проводять та адмініструють програми акредитації органів валідації/верифікації, а також органів, що здійснюють акредитацію у сфері систем управління, продуктів, процесів, послуг, персоналу тощо. IAF є асоціацією акредитаційних органів. Акредитаційні органи, у свою чергу, обирають і акредитують сертифікаційні органи, які після проведення аудиту СУІБ видають сертифікат організації. Прикладами сертифікаційних органів є: BSI, TÜV SÜD, Intertek.

Процес сертифікаційного аудиту зазвичай складається з двох етапів:

1. *Eman 1* − Огляд документації (Stage 1: Documentation Review): на цьому етапі аудитор переглядає процеси та політики організації, щоб перевірити їх відповідність вимогам стандарту ISO.

2. *Eman 2* − Сертифікаційний аудит (Stage 2: Certification Audit): на цьому етапі аудитор оцінює відповідність організації стандарту ISO 27001. Зокрема, перевіряється ефективність впровадження контрольних заходів, зазначених у SoA.

В Україні сертифікацію СУІБ за стандартом ISO/IEC 27001 здійснюють органи з сертифікації, які мають відповідну акредитацію. Проте сам стандарт ISO 27001 не є частиною національного законодавства, а сертифікація за ним не є обов’язковою, якщо інше не передбачено вимогами замовника, контрактами або галузевими нормативами.

В Україні сертифікацію за ISO/IEC 27001 можуть надавати:

- міжнародні органи з сертифікації, які працюють в Україні (наприклад, BSI, TÜV SÜD, SGS, DQS, Intertek тощо);
- українські органи з сертифікації, акредитовані Національним агентством з акредитації України (НААУ).

Національне агентство з акредитації України (НААУ) діє відповідно до:

- Закону України «Про акредитацію органів з оцінки відповідності» №2407-IV від 20.01.2005 року;

− міжнародних норм, зокрема вимог ISO/IEC 17021-1, що регламентують діяльність органів з сертифікації систем управління.

НААУ не проводить сертифікацію самостійно, а акредитує органи, які мають право проводити аудит та видавати сертифікати відповідності систем управління інформаційною безпекою вимогам стандарту ISO/IEC 27001.

1.5. **Висновки до розділу 1**

Для впровадження системи управління інформаційною безпекою в ІТ-підприємстві необхідно провести оцінку поточного стану інформаційної безпеки з метою визначення вимог до захисту. Цей первинний аналіз не лише дозволяє зафіксувати існуючий рівень безпеки, але й формує основу для вибору відповідної моделі впровадження.

Стандарт ISO/IEC 27001, що еволюціонував з британського стандарту BS 7799, здобув міжнародне визнання. Він складається з двох основних частин: перша включає 11 розділів, а друга − Додаток А − містить 93 контролі. Структура стандарту базується на циклі PDCA (Plan – Do – Check – Act), що забезпечує поетапне впровадження. Рішення щодо впровадження СУІБ може бути краще обґрунтоване за допомогою інструменту SWOT-аналізу. Після впровадження першочерговим завданням стає дотримання вимог чинного законодавства та нормативно-правових актів.

Проведений аналіз інформаційної безпеки надає вищому керівництву вихідну точку для прийняття обґрунтованих рішень щодо впровадження СУІБ, а також забезпечує чітке розуміння поточних умов і ресурсів організації для формалізації параметрів впровадження. Процеси акредитації та сертифікації є завершальними етапами на шляху до отримання сертифіката відповідності.

РОЗДІЛ 2. КЛЮЧОВІ АСПЕКТИ ТА ЕТАПИ ВПРОВАДЖЕННЯ СУІБ ЗА МІЖНАРОДНИМИ СТАНДАРТАМИ

1.1. Заходи контролю інформаційної безпеки: Взаємозв'язок ISO/IEC 27001 та ISO/IEC 27002

Стандарт ISO 27001 рекомендує застосовувати ризик-орієнтований підхід до інформаційної безпеки. Відповідно, організації мають виявляти загрози інформаційній безпеці та реагувати на них шляхом встановлення контрольних заходів.

Такі заходи описані в Додатку А стандарту. У Додатку А до ISO 27001 міститься 93 контрольні заходи, згруповані у 4 категорії − від А.5 до А.8. Впровадження всіх 93 контролів не є обов’язковим, і лише деякі з них мають бути зафіксовані документально. Організація самостійно визначає, які з них впроваджувати, спираючись на власну методологію управління ризиками.

Такий підхід надає компаніям гнучкість: вони можуть зосередитися на найбільш критичних для себе контролях і не витрачати ресурси на ті, що не є релевантними. Застосовні контролі визначаються в SoA.

У Додатку А до ISO 27001 кожен контроль описується в одному реченні − це дозволяє зрозуміти його мету, але не надає конкретних інструкцій щодо впровадження. Докладні пояснення містяться у стандарті ISO 27002.

Нижче подано узагальнений огляд того, на що спрямовані категорії контролів:

- А.5 − організаційні контролі;
- А.6 − контролі для персоналу;
- А.7 − фізичні контролі;

- A.8 − технологічні контролі.

ISO/IEC 27002 надає рекомендації щодо впровадження заходів безпеки, наведених у Додатку А стандарту ISO 27001, який є міжнародним стандартом для СУІБ. Серія стандартів ISO 27000 − це сукупність документів, що стосуються різних аспектів управління інформаційною безпекою. У цій серії ISO 27001 є базовим фреймворком, який містить обов'язкові вимоги до впровадження СУІБ. По суті, це перелік усього, що потрібно реалізувати для забезпечення відповідності стандарту.

Натомість, ISO 27002 є більш детальним і комплексним стандартом, однак сертифікація за ISO 27002 неможлива, оскільки він не є управлінським стандартом. Це збірник вимог, які допомагають організаціям налаштовувати свої політики та процеси з метою досягнення певних результатів. Тобто, він фактично встановлює правила експлуатації системи. У випадку з ISO 27001 ідеться про СУІБ, тож саме ISO 27001 підлягає сертифікації.

Інформаційна безпека в рамках цієї системи має бути спроєктована, реалізована, моніторингована, переглянута та вдосконалена. Це означає, що вище керівництво організації має виконувати конкретний набір завдань, зокрема встановлювати цілі, проводити вимірювання ефективності й організовувати внутрішні аудити. Усі ці аспекти визначені в ISO 27001, але не охоплюються ISO 27002.

Крім того, ISO 27002 не розрізняє, які контролі є релевантними для конкретної організації, а які − ні. Натомість ISO 27001 вимагає проведення оцінки ризиків, щоб визначити доцільність і обсяг впровадження кожного контрольного заходу.

Отже, чому ці два стандарти не поєднані в один? Тому що лише в роздільному вигляді вони є зручними у використанні. Якби це був один об'єднаний стандарт, він був би надто громіздким і складним, що ускладнило б його практичне застосування.

ISO 27001 призначений для закладення основ і створення фреймворку інформаційної безпеки в організації; ISO 27002 − для впровадження контрольних заходів; ISO 27005 − для проведення оцінки ризиків і управління ризиками.

Кожен стандарт серії ISO 27000 виконує окрему функцію в галузі інформаційної безпеки. ISO 27001 неможливо ефективно впровадити без ISO 27002, так само як ISO 27002 без управлінського каркасу, що його забезпечує ISO 27001, залишиться лише ініціативою кількох ентузіастів з інформаційної безпеки, не справивши жодного реального впливу на безпеку організації.

Організаційні контролі A.5 охоплюють систему управління та структуру корпоративного врядування, які підтримують і спрямовують впровадження та функціонування інформаційної безпеки в межах організації. Ця структура включає ролі, обов’язки, політики та процедури, що формують організаційний фундамент для досягнення цілей компанії у сфері захисту інформації.

Основною метою таких контролів є встановлення стандартів, оцінювання результативності, порівняння фактичних показників зі стандартами та вжиття необхідних коригувальних дій, щоб гарантувати відповідність стану інформаційної безпеки цілям і політикам організації. У межах цієї категорії наголошується на важливості лідерства, стратегічного планування та організаційної структури для забезпечення всебічної інформаційної безпеки.

Інтеграція організаційних контролів у версію ISO 27002:2022 є важливим кроком, що підкреслює значущість управління та корпоративного врядування в системі інформаційної безпеки. У центрі уваги − необхідність міцного організаційного фундаменту, який складається з чітко визначених ролей, обов’язків, політик і процедур, узгоджених із цілями компанії у сфері захисту інформації. Завдяки цим контролям можливо встановлювати стандарти, вимірювати та порівнювати показники ефективності, вживати коригувальні дії в разі потреби.

Формуючи культуру безпеки через стратегічне планування та лідерство, організаційні контролі сприяють створенню стійкої системи безпеки, здатної

проактивно управляти ризиками та зменшувати їхній вплив. Ця категорія доводить, що надійна система інформаційної безпеки виходить за межі суто технологічного підходу і потребує комплексних, скоординованих організаційних зусиль.

Оскільки людська помилка або зловмисні дії часто є найслабшою ланкою в системі безпеки, контролі для персоналу (people controls) спрямовані на формування свідомої поведінки та практик у сфері безпеки на всіх рівнях організації.

Контролі A.6 охоплюють перевірку нових співробітників (background checks), визначення обов'язків у сфері безпеки в трудових контрактах, проведення постійного навчання з питань інформаційної безпеки, створення процедур для повідомлення про інциденти безпеки.

Крім того, такі заходи враховують сучасні виклики, зокрема дистанційну роботу, що підкреслює їхню актуальність і здатність адаптуватися до змін у робочому середовищі.

Інтегруючи ці контролі, організації здатні краще захищати свої інформаційні активи, забезпечувати безперервність бізнесу, зберігати довіру клієнтів та відповідати нормативним вимогам.

Контролі для персоналу в стандарті ISO 27001 підкреслюють ключову роль людського фактора в управлінні інформаційною безпекою. Ці контролі охоплюють вісім основних напрямів:

- проведення перевірки нових працівників (screening);
- визначення відповідальності працівників і організації за інформаційну безпеку в трудових контрактах (умови працевлаштування);
- регулярне підвищення обізнаності, навчання й інформування щодо інформаційної безпеки;

- впровадження формалізованого дисциплінарного процесу за порушення політик;
- визначення обов’язків після звільнення або зміни посади;
- укладання угод про конфіденційність або нерозголошення;
- встановлення заходів безпеки для віддаленої роботи;
- створення системи повідомлення про інциденти інформаційної безпеки.

Ці заходи спрямовані на зміцнення конфіденційності, цілісності та доступності інформації шляхом керування ризиками, пов’язаними з людським фактором.

Фізичні контролі A7 − це матеріальні та інфраструктурні заходи, спрямовані на захист активів і ресурсів організації, включно з даними. Такі заходи охоплюють як створення фізичних бар’єрів (стіни, двері, замки), так і організацію контрольованих зон з обмеженням доступу.

Крім того, вони передбачають проєктування приміщень таким чином, щоб гарантувати безпеку працівників і фізичних систем, які зберігають, обробляють або передають інформацію. Основна мета фізичних контролів − запобігти несанкціонованому доступу, пошкодженню, крадіжці або втручанню у ресурси організації.

Ці заходи є критично важливою частиною комплексної програми безпеки, оскільки забезпечують першу лінію захисту від потенційних загроз, які можуть поставити під загрозу цілісність, доступність та конфіденційність інформації.

Впровадження фізичних контролів відповідно до стандарту ISO 27001 здатне суттєво підвищити рівень загальної безпеки організації.

Фізичні контролі охоплюють не лише заходи з обмеження фізичного доступу до захищених зон, а й визначають протоколи безпечного поводження з

обладнанням, захисту від зовнішніх загроз та підтримання безпечних умов праці.

Регулюючи такі аспекти, як забезпечення інженерних комунікацій або утилізація обладнання, фізичні контролі створюють всебічний бар’єр від потенційних фізичних загроз, забезпечуючи тим самим цілісність, конфіденційність і доступність інформаційних активів організації.

Крім того, ці заходи зміцнюють стійкість організації, дозволяючи їй ефективно реагувати на фізичні інциденти та відновлюватися після непередбачених переривань у роботі.

Технологічні контролі А.8 забезпечують структуровану та комплексну систему управління й захисту цифрової інфраструктури організації. Вони охоплюють різні аспекти інформаційних технологій, зокрема кінцеві пристрої користувачів, обмеження доступу до даних, управління потужностями, захист від шкідливого програмного забезпечення та безпечну розробку програмного забезпечення.

У сучасну цифрову епоху, коли інформація дедалі частіше обробляється, зберігається та передається в електронному вигляді, важливість технологічних контролів неможливо переоцінити. Заходи, передбачені в межах цих контролів, мають на меті не лише захист від кіберзагроз, а й оптимальне використання ресурсів, безпечне управління даними та збереження цілісності систем.

Впровадження таких контролів дозволяє організаціям зменшити ризики, пов’язані з технічними вразливостями, запобігати витокам даних, а також забезпечити конфіденційність, цілісність і доступність своїх інформаційних активів.

Технологічні контролі мають на меті забезпечити безпечну роботу цифрових систем організації, захистити інформацію від несанкціонованого доступу та зберегти цілісність систем. Їхній широкий і комплексний характер відображає складність та багатовимірність сучасної інформаційної безпеки в цифрову епоху.

Ці контролі виходять за межі простої охорони даних, охоплюючи також керування доступом, оптимізацію ресурсів, оцінку вразливостей та інші критично важливі компоненти. Впровадження таких заходів допомагає організаціям безпечно й ефективно орієнтуватися в сучасному цифровому середовищі, забезпечуючи надійні механізми захисту від кіберзагроз та безперервність діяльності.

Постійний моніторинг, перегляд і оновлення технологічних контролів є необхідною умовою для адаптації до змінного ландшафту загроз інформаційної безпеки.

Підводячи підсумок, ISO 27002 є зводом практичних рекомендацій щодо контролів СУІБ і містить набагато детальніші описи, ніж контрольні заходи, наведені в Додатку А стандарту ISO 27001. Перелік із 93 контрольних заходів, згрупованих у чотири набори контролів, розкривається в розділах А.5–А.8 стандарту ISO 27002:2022.

Хоча ISO 27002 сам по собі не є сертифікаційним стандартом, дотримання його принципів управління інформаційною безпекою допомагає компанії відповідати вимогам сертифікації за ISO 27001. У цьому документі пояснюється, як дотримуватись стандарту ISO 27001 і як його впроваджувати на практиці.

Оскільки універсального рішення в сфері інформаційної безпеки не існує, відповідні контрольні заходи слід обирати на основі оцінки ризиків і релевантності цих заходів до виявлених загроз. У цьому контексті для визначення цілей інформаційної безпеки можна застосовувати тріаду CIA − конфіденційність (Confidentiality), цілісність (Integrity), доступність (Availability).

1.2. **Загальні етапи та підходи до впровадження СУІБ**

СУІБ охоплює політики, стандарти, процедури, практики, поведінкові моделі та заплановані дії, які організація впроваджує для захисту своїх

(важливих) інформаційних активів. Вона забезпечує як самій організації, так і її зовнішнім сторонам чітке уявлення про цілі та контекст інформаційної безпеки.

Проєктування та реалізація СУІБ залежить від потреб і цілей організації. Також слід враховувати її розміри та структуру, ринок або регіон діяльності, а також чутливість інформації, якою вона володіє чи управляє від імені інших осіб. Метою СУІБ є ідентифікація, оцінка (за потреби) та управління загрозами інформаційній безпеці задля захисту цифрових активів організації. Цей процес не є одноразовою подією, а являє собою безперервний цикл управління ризиками. СУІБ сприяє вимірюванню та звітуванню щодо ефективності контролів. Успішне впровадження СУІБ створює як реалістичну, так і практичну основу для виявлення та управління ризиками у сфері інформаційної безпеки.

У межах СУІБ враховуються керівництво, працівники, постачальники та регуляторні органи, що є критичними ресурсами. Впровадження СУІБ − це стратегічне бізнес-рішення. З огляду на це, критично важливо забезпечити залучення та підтримку вищого керівництва як необхідну передумову для успішної реалізації СУІБ.

Важливо, щоб усі компоненти СУІБ не лише створювалися, а й запроваджувалися у використання, а не відкладалися до реалізації за принципом «все й одразу». При цьому досконалість не повинна бути головною метою − СУІБ має механізми самокорекції та постійного вдосконалення.

Немає обов’язкової вимоги базувати СУІБ саме на стандарті ISO 27001, однак цей стандарт забезпечує глобально визнану і зрозумілу структуру. Саме вона відкриває можливість отримання сертифікації СУІБ, яку визнають у всьому світі. СУІБ, побудована на основі ISO 27001, передбачає комплексний, ієрархічний та інтегрований підхід до виявлення та усунення ризиків інформаційної безпеки. Це включає врахування питань політик і процедур, використаних технологій і засобів, а найголовніше − людей і їх поведінки.

1. Підтримка керівництва

Переконати керівництво у необхідності впровадження СУІБ може здаватися складним завданням. Адже найважливішим пріоритетом для керівництва є прибутковість компанії, а отже, рішення здебільшого ухвалюються, спираючись на показник рентабельності інвестицій (ROI − Return on Investment).

Одним з ключових аспектів переконання є правильне подання інформації у формі, яку керівництво зрозуміє і зможе підтримати.

Очевидно, що керівництво шукатиме конкретні переваги запропонованого впровадження СУІБ. Нижче наведено чотири найважливіші з них:

- Відповідність вимогам (Compliance): Стандарт ISO 27001 надає методологію, яка дозволяє компанії ефективно і економічно дотримуватись численних вимог щодо захисту даних, конфіденційності та IT-управління (особливо якщо це організація у фінансовій, медичній або державній сфері).
- Маркетингова перевага: На ринку з високим рівнем конкуренції наявність сертифікату ISO 27001 може стати чинником, що вирізняє компанію серед інших, особливо якщо потенційні клієнти вимагають відповідального поводження з їхніми даними.
- Зменшення витрат: Інформаційна безпека зазвичай сприймається як витрата без очевидної фінансової віддачі. Однак потенціал економії виникає завдяки зниженню витрат, пов’язаних з інцидентами безпеки. Часто трапляються простої сервісів або втрата даних. Хоч наразі не існує точного інструменту або технології для підрахунку можливої економії, уникнення таких випадків зазвичай викликає позитивну реакцію з боку керівництва.
- Упорядкування бізнесу: Якщо компанія активно зростала впродовж останніх років, можливо, виникали труднощі з визначенням відповідальних осіб за інформаційні активи або з контролем доступу до інформаційних систем. Впровадження ISO 27001 змусить чітко визначити ролі та зони

відповідальності, що покращить внутрішню структуру компанії й допоможе вирішити подібні організаційні проблеми.

На завершення, стандарт ISO 27001 − це більше, ніж просто сертифікат на стіні. У більшості випадків керівництво звертає увагу, якщо ці переваги представлено стисло, чітко й аргументовано.

2. Реалізація проєкту

Впровадження СУІБ, що базується на стандарті ISO 27001, є складним завданням, яке охоплює значну кількість учасників і широкий спектр заходів. Такий процес може тривати від кількох місяців (для невеликих компаній) до понад року (для великих корпорацій).

Ключем до успішного впровадження є чітке визначення того, що саме потрібно зробити, хто відповідальний за виконання та в які строки це має бути реалізовано, тобто застосування принципів управління проєктами.

3. Визначення сфери застосування

Основною метою визначення сфери застосування СУІБ є встановлення типів інформації, що підлягає захисту. При цьому не має значення, де саме зберігається ця інформація − на території компанії чи в хмарному середовищі, або як до неї здійснюється доступ − локально чи віддалено. Найважливіше − це усвідомлення відповідальності організації за захист інформації незалежно від способу, місця чи засобу доступу.

Наприклад, якщо співробітники отримують доступ до внутрішньої мережі та чутливих даних з особистих пристроїв, ці пристрої мають бути враховані у сфері застосування. Сфера повинна охоплювати зацікавлені сторони, логічні та фізичні межі, а також можливі виключення. Вона визначає межі, в яких функціонує система управління.

Зазвичай, сфера застосування охоплює всю організацію разом із її процесами, продуктами та послугами. Для її коректного визначення необхідно врахувати бюджет, нормативні вимоги, положення стандарту, наміри керівництва, поточний стан організації тощо. Проведення gap-аналізу може допомогти виявити відсутні елементи системи управління та оцінити, наскільки

поточний стан відповідає вимогам стандарту. Це також дозволяє ефективно управляти наявними ресурсами.

Сфера застосування буде основою для визначення об’єктів оцінки ризиків, що в свою чергу вплине на інші компоненти СУІБ. Не завжди є потреба впроваджувати однаковий рівень безпеки по всій організації − невдало сформульована сфера може стати однією з причин провалу впровадження. Тому необхідно формалізувати сферу застосування документально, незалежно від її обсягу.

При формуванні сфери СУІБ слід врахувати такі аспекти:

- місія компанії;
- цілі СУІБ;
- види діяльності організації;
- що є критичним і підлягає захисту (наприклад, інтелектуальна власність, дані клієнтів);
- фізичні межі проєкту;
- чи охоплює СУІБ усі підрозділи компанії;
- участь постачальників послуг;
- наявність виключень.

Якщо організація не має достатніх повноважень для управління певними ділянками, це може бути підставою для їх виключення зі сфери, що ускладнює управління відповідними ризиками.

Відповідно до ISO 27001, під час визначення сфери застосування СУІБ необхідно враховувати такі аспекти як внутрішній та зовнішній контекст

організації, потреби та очікування зацікавлених сторін, а також залежності та інтерфейси між СУІБ і зовнішнім середовищем.

Внутрішній контекст охоплює фактори, що перебувають під контролем компанії (наприклад, організаційна структура, ресурси, внутрішні процеси, корпоративна культура). Зовнішній контекст включає фактори, на які організація не має прямого впливу, однак мусить на них реагувати або до них адаптуватись − зокрема, це політична, економічна, технологічна, правова та соціальна ситуація.

Під зацікавленими сторонами розуміють усіх, хто має інтерес до функціонування СУІБ, зокрема:

- співробітники − тому що виконують процедури згідно СУІБ;
- клієнти − довіряють організації свої персональні або конфіденційні дані;
- партнери, підрядники, акціонери, регулятори тощо.

Залежності − це зовнішні сервіси або функції, що підтримують функціонування СУІБ, але не входять до її сфери (наприклад, юридичне супроводження, хостинг). Інтерфейси визначають межі СУІБ та демонструють, яка інформація обробляється, передається або отримується за межами цієї системи.

Для невеликих компаній зазвичай доцільно включити в сферу всю організацію − це спрощує реалізацію СУІБ. Великі компанії можуть обмежити сферу лише певними підрозділами або бізнес-напрямами, зокрема, пов’язаними з обробкою чутливої інформації. У будь-якому випадку, ISO 27001 вимагає формального документального оформлення сфери застосування СУІБ. Такий опис може бути частиною іншого документа (наприклад, політики інформаційної безпеки) або оформлюватися окремо.

4. Політика ІБ

Політика інформаційної безпеки є найвищим рівнем документу в системі управління інформаційною безпекою , і вона не повинна бути надмірно деталізованою. Її завдання − окреслити основні вимоги до інформаційної безпеки, продемонструвати стратегічне бачення керівництва та визначити загальні принципи досягнення цілей у сфері захисту інформації. Вона задає напрямок, якого мають дотримуватись усі внутрішні процедури, включно з політиками прийнятного використання, фізичної безпеки, використання електронної пошти тощо.

Під час формування політики інформаційної безпеки слід враховувати такі аспекти:

- Адаптація до контексту організації: політика має відповідати масштабам, галузі та операційним реаліям підприємства. Наприклад, політика великої виробничої компанії буде істотно відрізнятися від політики IT-компанії малого або середнього бізнесу.
- Формування цілей. У політиці мають бути визначені механізми постановки, затвердження та перегляду цілей СУІБ, які створюють основу для розробки всієї системи безпеки.
- Підтвердження зобов’язань керівництва: політика має чітко відображати зобов’язання вищого керівництва щодо задоволення потреб зацікавлених сторін та постійного вдосконалення СУІБ.
- Призначення відповідальної особи: доцільно визначити уповноважену особу для регулярного внутрішнього та зовнішнього інформування про політику (наприклад, для клієнтів або постачальників).
- Регулярний перегляд: політика має переглядатися на регулярній основі (наприклад, щорічно), із зазначенням відповідальної особи, яка контролює її актуальність.

Відповідно до пункту 5.2 стандарту ISO 27001, вищий менеджмент має забезпечити, щоб цілі СУІБ були узгоджені зі стратегічними напрямами розвитку компанії. У цьому контексті політика інформаційної безпеки виконує роль ключового зв'язку між керівництвом і заходами інформаційної безпеки. Щоб бути дієвою, політика повинна бути короткою, лаконічною і зрозумілою для осіб, що приймають рішення.

5. Методика оцінювання ризиків

Оцінювання ризиків є одним із найскладніших етапів у реалізації проєкту з впровадження ISO 27001, адже потребує чіткого визначення правил виявлення ризиків та встановлення допустимого рівня ризику. На цьому етапі необхідно вирішити, який підхід буде застосовано − якісний чи кількісний, які шкали будуть використовуватись для вимірювання ймовірності та наслідків, яким буде поріг прийнятного ризику тощо.

Оцінку рівня ризику (його наслідків і ймовірності) має здійснювати власник ризику, тобто особа, відповідальна за актив, що піддається ризику. У разі використання кількісного підходу можна детальніше дослідити профіль ризиків організації та застосовувати стандартизовану шкалу для оцінки рівня зрілості безпекових контролів, що впроваджені.

Роботу з оцінки та обробки ризиків може здійснювати керівник проєкту або фахівець з інформаційної безпеки як самостійно, так і за участі зовнішніх консультантів. У великих організаціях процес оцінювання ризиків зазвичай виконується тією ж командою, що відповідає за впровадження ISO 27001. Менші компанії можуть виконати цю процедуру самостійно, за умови використання відповідної документації та інструментів, без залучення сторонніх експертів.

6. Оцінка та управління ризиками

Процес оцінювання ризиків може тривати кілька днів для малого бізнесу або декілька місяців − для великих організацій, тому на цьому етапі важливо ретельно спланувати всі дії. Основна мета − отримати повну картину загроз для даних організації як з внутрішніх, так і з зовнішніх джерел.

Відповідно до стандарту ISO 27001, процедура оцінювання ризиків включає п’ять основних кроків:

1. Ідентифікація ризиків − перелік активів, загроз і вразливостей. Для зручності можна використовувати цифрові таблиці, в яких зазначаються ідентифікатор ризику, власники ризику, рівень впливу та ймовірність настання події.

2. Призначення власників ризику − визначаються відповідальні особи на основі їх обізнаності щодо активу або повноважень впливати на нього.

3. Аналіз ризику − оцінюється потенційний вплив події та ймовірність її виникнення.

4. Обчислення ризику − визначення рівня ризику шляхом додавання або множення значень впливу і ймовірності. Наприклад, при впливі 4 та ймовірності 2 отримаємо рівень ризику 8 (4×2) або 6 (4+2), залежно від прийнятого в організації методу. Важливо використовувати однаковий підхід до розрахунків у всіх випадках.

5. Оцінка ризику − порівняння отриманого значення ризику з прийнятним порогом, визначеним у методології. Якщо, наприклад, отримане значення дорівнює 8, а прийнятний рівень − 5, такий ризик вважається неприйнятним.

Для зменшення неприйнятних ризиків застосовується етап обробки ризиків, на якому розробляється план впровадження відповідних контролів з Додатку A (Annex A), щоб знизити ймовірність або вплив ризиків. На кожному етапі оцінювання та обробки ризиків необхідно вести документацію, зокрема звіт про оцінку ризиків. Також важливо отримати затвердження наявних залишкових ризиків.

7. SoA

SoA − це обов’язковий документ згідно з ISO 27001, що фіксує підхід організації до визначення релевантних контролів, пояснює, чому деякі з них не застосовуються, та описує стан впровадження актуальних заходів.

SoA документує середовище контролів у межах СУІБ та базується на результатах оцінки ризиків і заходах їх обробки. Шаблоном для складання SoA виступає Додаток А до стандарту.

Відповідно до пункту 6.1.3(d) ISO 27001, SoA має включати такі ключові елементи:

- перелік контролів, які будуть застосовані з-поміж запропонованих у Додатку А;
- обґрунтування вибору контролів, що є релевантними у поточному контексті організації;
- стан реалізації кожного застосовного контролю (чи впроваджено його, чи ні);
- пояснення щодо виключення контролів, які не є релевантними.

Таким чином, SoA надає всебічну картину поточного стану інформаційної безпеки в організації. Вона також слугує ключовим документом для представлення СУІБ керівництву та є основним джерелом інформації для зовнішніх аудиторів.

Після формування SoA наступним кроком є створення практичного та чіткого плану обробки ризиків.

8. План обробки ризиків

План обробки ризиків складається після завершення розробки Декларації застосовності. RTP є ключовим документом, що деталізує реалізацію вибраних контролів із SoA. Він виконує роль практичного плану дій, спрямованого на зменшення прийнятих ризиків до прийнятного рівня.

У RTP має бути чітко зазначено:

- які саме заходи безпеки (контролі) будуть впроваджуватись;

- хто відповідальний за впровадження кожного з них;
- терміни реалізації заходів;
- які ресурси (фінансові, людські тощо) будуть необхідні для реалізації;
- як оцінити ефективність реалізації та чи досягнуто очікуваного результату.

Таким чином, хоча SoA і процедура оцінювання/обробки ризиків формують основу, план обробки ризиків − це етап, де починається фактичне впровадження. Він забезпечує послідовність дій і відповідальність, необхідні для ефективного функціонування СУІБ.

У наступному етапі відбувається реалізація запланованих контролів, що покращує процеси інформаційної безпеки в організації.

9. Впровадження засобів захисту

На цьому етапі розпочинається безпосереднє втілення усіх передбачених контролів і політик, а також впровадження відповідної документації та технологічних рішень, що трансформують підходи організації до управління інформаційною безпекою.

Нижче наведено орієнтовний перелік необхідних документів, передбачених стандартом ISO 27001:

- Документ із визначенням сфери застосування СУІБ (пункт 4.3)
- Політика інформаційної безпеки та цілі СУІБ (пункти 5.2 і 6.2)
- Методологія оцінки та обробки ризиків (пункт 6.1.2)
- Заява про застосовність (SoA) (пункт 6.1.3 d)

- План обробки ризиків (пункти 6.1.3 e, 6.2, 8.3)
- Звіт з оцінки ризиків (пункти 8.2 і 8.3)
- Розподіл ролей і відповідальності (контролі A.6.2, A.6.6)
- Інвентар активів (контроль A.5.9)
- Політика прийнятного використання активів (A.5.10)
- Політика контролю доступу (A.5.15)
- Документовані операційні процедури (A.5.37)
- Принципи безпечної інженерії систем (A.8.27)
- Політика безпеки постачальників (A.5.19)
- Процедури реагування на інциденти (A.5.26)
- Процедури забезпечення безперервності бізнесу (A.5.30)
- Вимоги законодавчого, нормативного та договірного характеру (A.5.31)

Обов’язкові записи (згідно ISO 27001):

- Документи про навчання, кваліфікації, досвід (пункт 7.2)
- Результати моніторингу й вимірювання (пункт 9.1)
- Програма внутрішнього аудиту (пункт 9.2)
- Результати внутрішнього аудиту (пункт 9.2)

- Документи про проведення аналізу з боку керівництва (пункт 9.3)
- Результати коригувальних дій (пункт 10.1)
- Журнали дій користувачів, виключень, подій безпеки (A.12.4.1, A.12.4.3)

Окрім обов’язкових, також можуть бути розроблені додаткові документи: політика BYOD, процедури внутрішнього аудиту, політика класифікації інформації, політика використання мобільних пристроїв і роботи з дому, процедури коригувальних дій тощо.

Найбільшою складністю є впровадження нових політик та процедур у повсякденну діяльність персоналу. Щоб подолати опір змінам, необхідно проводити регулярні навчання, інформувати про переваги СУІБ і залучати співробітників до процесу.

10. Реалізація програм навчання та підвищення обізнаності

Пояснення причин запровадження нових політик і процедур, а також надання відповідного навчання є необхідними умовами для їх ефективного дотримання персоналом. Однією з найпоширеніших причин невдачі впровадження ISO 27001 є недостатній рівень навчання та обізнаності працівників.

Усі співробітники повинні володіти необхідними знаннями та навичками для виконання своїх функцій у межах СУІБ. Виявлені прогалини в компетенціях мають бути усунені. Окремі групи отримують цільове навчання, орієнтоване на конкретні обов’язки в межах системи.

Під час розроблення навчального плану необхідно враховувати:

- цільову аудиторію;
- зміст навчальних матеріалів;

- формат подачі навчання;
- час і періодичність проведення;
- відповідальних осіб за організацію, оновлення змісту й реалізацію навчання;
- потребу в оцінюванні ефективності або тестуванні знань.
- Навчальна програма формується після аналізу зібраних даних.

Впровадження СУІБ також вимагає ефективної системи внутрішніх комунікацій. Завдяки продуманим комунікаційним заходам інформаційна безпека інтегрується в операційну діяльність підприємства. Систематичне використання інформаційних панелей, оперативних повідомлень та інструктажів сприяє підтриманню обізнаності працівників щодо актуальних загроз і політик.

Для організації належного інформаційного супроводу необхідно визначити цільову аудиторію, засоби передачі інформації (використовувані або нові), зміст повідомлень і частоту комунікації. За умови залучення спеціалізованого підрозділу корпоративних комунікацій ефективність реалізації значно підвищується.\

11. Операціалізація СУІБ

На цьому етапі стандарт ISO 27001 має бути інтегрований у повсякденну діяльність організації. У розділах 4–10 містяться посилання на обов’язкову документацію, яка включає як документи, так і записи. Записи слугують доказами виконання конкретних дій у певний момент часу.

Записи створюються (вручну або автоматично) під час виконання певних дій і фіксують факт їх здійснення. Наприклад, система резервного копіювання створює журнали під час автоматичного створення резервних копій. Журнали

подій або книга обліку відвідувачів також є прикладами записів. Таким чином, записи забезпечують підтвердження виконання дій.

Документи, на відміну від записів, підлягають періодичному перегляду та оновленню. Зазвичай вони мають версії. Документація є важливим елементом для забезпечення виконання процесів відповідно до цілей системи управління. Вона відображає план дій і слугує підтвердженням виконання зобов'язань.

Стандарт ISO 27001 не визначає точного обсягу документації − він залежить від низки чинників: розміру та основних функцій організації, складності й взаємозалежності бізнес-процесів, характеру контрольного середовища, рівня кваліфікації персоналу, а також юридичних або регуляторних вимог. Під час розробки документації слід ураховувати цільову аудиторію − вона має бути корисною та зрозумілою для користувачів.

Перехід від етапу впровадження СУІБ до її повноцінного функціонування не повинен бути різким. Ефективним підходом є використання створених артефактів і процесів одразу після їх появи. Така стратегія забезпечує низку переваг: по-перше, організація не сприймає впровадження СУІБ як «революційний» проєкт. Раннє використання нових або змінених процесів сприяє зростанню підтримки системи, а також дозволяє на ранньому етапі збирати дані та докази для подальшого вдосконалення.

Важливо забезпечити доступність нових і оновлених процесів для операційних підрозділів. СУІБ має стати складовою звичайної операційної діяльності організації.

У багатьох організаціях трансформаційні процеси стикаються з низкою внутрішніх бар'єрів. Ефективному впровадженню СУІБ можуть заважати такі чинники, як культура спротиву змінам, велика організаційна структура зі сповільненими процесами прийняття рішень, вимога до уникнення ризиків у специфічних галузях, відчуття нестачі ресурсів та перевантаження працівників тощо. Це особливо актуально, коли впровадження зумовлене виключно вимогами нормативного комплаєнсу.

Для подолання цих бар'єрів необхідно використовувати ефективні та послідовні методи комунікації, які наголошують на перевагах СУІБ і пояснюють працівникам, яку цінність система приносить саме їм. Додатковим чинником подолання складнощів може бути прагнення до максимальної простоти в реалізації СУІБ.

Корисним інструментом у процесі впровадження та експлуатації системи є календар безпеки. Хоча стандарт ISO 27001 не вимагає обов'язкового створення такого календаря, він може відігравати важливу роль у плануванні виконання регулярних або запланованих дій, пов'язаних як із вимогами розділів 4–10 стандарту, так і з заходами контролю, передбаченими в Заяві про застосовність (SoA).

Календар заходів з інформаційної безпеки може стати частиною ширшого календаря відповідності (compliance calendar). До заходів, які доцільно планувати та відстежувати за допомогою такого інструменту, належать внутрішні аудити СУІБ, періодичні перевірки привілейованих користувачів, управлінські огляди, ревізії реєстрів ризиків, а також щорічні тренінги з підвищення обізнаності з питань інформаційної безпеки.

12. Моніторинг та вимірювання ефективності СУІБ

Як відомо, управляти можна лише тим, що піддається вимірюванню. Моніторинг функціонування СУІБ може здійснюватися різними способами, проте одним із ключових інструментів для оцінки її ефективності та впровадження змін є вимірювання результативності окремих її компонентів. Організація самостійно визначає, які саме показники є релевантними, яким чином вони будуть вимірюватися та публікуватися.

Наприклад, у випадку із резервним копіюванням компанія може встановити ціль втрати даних не більше ніж за останні п'ять годин. Такий показник відповідає критеріям SMART і дозволяє перевірити, чи справді відновлення даних відповідає заданому допуску.

Процес сертифікації СУІБ і сам сертифікат завжди прив'язані до конкретної версії SoA. У разі внесення змін до кількості або змісту контрольних

заходів організація має оновити SoA та, за потреби, звернутись до органу сертифікації для перегляду сертифіката (це може потребувати додаткової оплати, якщо не входить у стандартний цикл ресертифікації). Оскільки SoA є похідним результатом процесу оцінки та обробки ризиків, вона часто безпосередньо пов’язана з реєстром ризиків.

SoA є також ключовим документом під час підготовки до аудиту − вона слугує основою для побудови плану аудиту та визначення відповідних ресурсів. СУІБ, побудована відповідно до ISO 27001, має відповідати положенням розділів 4–10 стандарту. SoA містить обґрунтовану добірку релевантних для організації контрольних заходів із 93, передбачених у Додатку А ISO 27001.

Зазначимо, що досвідчені системи менеджменту, як правило, оперують більшою кількістю метрик. Чим критичнішим або складнішим є напрямок контролю, тим більше уваги має бути приділено формуванню надійних індикаторів для моніторингу. Поширеним підходом є добір показників ефективності на основі рівня ризиків, які вони знижують. Ті контролі, що зменшують більшу кількість суттєвих ризиків, заслуговують на пріоритетну увагу при оцінюванні.

Незалежно від того, як саме буде організовано процес моніторингу ефективності заходів, важливо чітко визначити методику загальної оцінки ефективності СУІБ і кожного конкретного елемента системи.

13. Внутрішній аудит

Внутрішній аудит СУІБ має два основні завдання відповідно до пункту 9.2 стандарту ISO 27001. Перше − перевірка відповідності СУІБ вимогам стандарту, внутрішнім політикам і процедурам організації, а також чинному законодавчому та регуляторному середовищу. Результатом такого аудиту є звіт, у якому зазначаються як відповідності (conformities), так і невідповідності (non-conformities) встановленим критеріям.

Друге завдання внутрішнього аудиту − виявлення шляхів для вдосконалення функціонування СУІБ. Програма аудиту СУІБ є організаційною рамкою, в межах якої проводяться внутрішні аудити. Зазвичай вона розрахована

на кілька років і охоплює графік та обсяг кожного з планованих аудитів. Аудити мають проводитися з визначеною періодичністю та охоплювати всі обов’язкові розділи стандарту, а також контрольні заходи, визначені в SoA.

Кожен окремий аудит СУІБ може охоплювати лише певні сфери контролю або розділи стандарту. Аудитор не має права виходити за межі визначеного обсягу без відповідного дозволу. При проведенні внутрішнього аудиту фокус ставиться не на діях конкретних осіб, а на ефективності системи в цілому. Якщо виявляються недоліки у роботі персоналу, вони мають розглядатися як ознаки слабкості самої системи − наприклад, недостатнє розуміння працівником своїх обов’язків, відсутність компетентності або неякісна політика та процедури підтримки.

Важливо розуміти, що аудит СУІБ − це не лише оцінка впроваджених контролів, а насамперед оцінка ефективності всієї системи управління. У більшості випадків відмова контролю вказує на несправність або відсутність одного з ключових елементів СУІБ. Усунення першопричини здебільшого призводить до усунення і самих проблем із контролями.

Аудитори СУІБ, як і всі інші ролі в межах системи, мають володіти необхідними знаннями та компетенціями. Загальний IT-аудитор може мати достатньо знань для перевірки контролів, однак без глибокого розуміння принципів роботи СУІБ він не зможе провести повноцінний аудит.

Отже, внутрішній аудит дозволяє виявити потенційно критичні невідповідності, що можуть зашкодити організації, і забезпечує фундамент для їх оперативного усунення.

14. Огляд з боку керівництва

Метою огляду з боку керівництва є оцінка ефективності функціонування СУІБ з урахуванням ряду факторів та прийняття необхідних рішень щодо її коригування (відповідно до пункту 9.3 ISO 27001). Огляд проводиться вищим керівництвом організації на регулярній основі в заздалегідь визначені моменти часу. Це є стандартною практикою в межах управління СУІБ.

Згідно з вимогами стандарту ISO 27001, під час огляду керівництвом мають бути враховані наступні вхідні дані:

- інформація про виконання рішень, прийнятих за результатами попереднього огляду;
- зміни у зовнішніх та внутрішніх аспектах, що мають вплив на СУІБ;
- результати моніторингу та вимірювання, результати аудитів, досягнення цілей у сфері інформаційної безпеки, а також зворотний зв'язок щодо ефективності функціонування СУІБ;
- відгуки зацікавлених сторін;
- результати оцінювання ризиків та стан виконання плану обробки ризиків;
- можливості для постійного вдосконалення.
- За результатами огляду керівництвом мають бути ухвалені рішення щодо вдосконалення СУІБ та її коригування. Ці рішення мають бути задокументовані − зазвичай у протоколі зустрічі з огляду СУІБ.

Варто зазначити, що внутрішній аудит СУІБ повинен передувати огляду керівництвом, оскільки його результати є ключовим джерелом інформації для ухвалення рішень у межах такого огляду.

15. Корекція, коригувальні дії та вдосконалення

Метою функціонування системи управління є усунення або, бажано, попередження невідповідностей. Відповідно, стандарт ISO 27001 вимагає, щоб корекційні дії (corrections) та коригувальні дії (Corrective Actions, CA) здійснювалися системно, тобто з обов'язковим виявленням, усуненням і підтвердженням усунення першопричини невідповідності. Також стандарт

зобов’язує організації постійно вдосконалювати свою СУІБ, і СА є одним з основних інструментів цього процесу.

Необхідність у СА може виникнути в результаті внутрішніх або зовнішніх аудитів, перегляду з боку керівництва, інцидентів інформаційної безпеки, результатів тестування або перевірок безпеки.

За процесом СА зазвичай наглядає власник ризику, який також перевіряє відповідність заходів до реєстру ризиків.

Корекція − це негайна дія, спрямована на усунення виявленої невідповідності.

Коригувальна дія (СА) − це дії, спрямовані на усунення корінної (первинної) причини невідповідності та недопущення її повторної появи в майбутньому.

Наприклад, у випадку, якщо зловмисник проник у будівлю компанії, обійшовши систему контролю доступу, перевірка виявляє, що пристрій контролю не працював. Корекція: негайне розміщення охоронця для перевірки допуску працівників. Коригувальна дія: діагностика та ремонт пристрою контролю доступу, запровадження перевірки його працездатності за графіком.

СА фіксується у встановленій процедурі, яка включає аналіз кореневої причини та визначення заходів для запобігання повторенню інциденту. У разі виявлення невідповідностей під час сертифікаційних або наглядових аудитів СА має бути впроваджена в межах установлених термінів.

Вдосконалення передбачає, що організації, які вже мають функціонуючу СУІБ, зобов’язані постійно працювати над її покращенням. Це є обов’язковим елементом усіх систем управління, і СУІБ не є винятком.

Джерелами вдосконалення можуть бути внутрішні аудити, зовнішні аудити, перегляди з боку керівництва, інциденти інформаційної безпеки, перевірки безпеки, результати тестування, пропозиції зацікавлених сторін.

Хоча запропоновані вдосконалення не обов’язково мають бути впроваджені, вони повинні бути розглянуті. Організація самостійно приймає рішення щодо тих вдосконалень, які, на її думку, принесуть користь СУІБ.

Пропозиції як внутрішніх, так і зовнішніх аудиторів варто враховувати, однак їх реалізація не є обов'язковою. Організація встановлює строки реалізації погоджених вдосконалень.

16. Сертифікація СУІБ

Перед тим як СУІБ може бути повністю сертифікована, незалежна та авторитетна третя сторона має оцінити її відповідність стандарту ISO 27001, внутрішнім політикам і процесам організації, а також правовому та регуляторному контексту, в якому працює бізнес.

Мета сертифікаційного аудиту полягає у наступному:

- підтвердження відповідності вимогам ISO 27001 для клієнтів та інших зацікавлених сторін;
- мінімізація ризиків інформаційної безпеки для клієнтів і постачальників;
- формування довіри до інформаційної безпеки організації з боку споживачів, постачальників, регуляторів та інших зацікавлених осіб.

Більшість акредитованих органів з сертифікації (СВ) пропонують аналіз розривів (gap analysis) або попередній аудит перед офіційним початком процедури сертифікації. Процес сертифікації поділяється на два етапи − Етап 1 та Етап 2. Подача заявки − організація звертається до обраного органу з сертифікації. Аудит Етапу 1 − попередня оцінка готовності та відповідності документів і політик. Аудит Етапу 2 − детальна перевірка імплементації системи, процесів та контролів на практиці.

Якщо після другого етапу аудиту не виявлено значних невідповідностей, орган сертифікації рекомендує видачу сертифікату відповідності ISO/IEC 27001.

Впровадження СУІБ може займати від кількох місяців у малих підприємствах до року і більше − у великих компаніях. Успішне й ефективне впровадження може покращити операційні показники, такі як ефективність,

результативність, економія коштів, а також зменшити частоту виникнення інцидентів.

У малих компаніях менеджер проєкту часто виконує також функції фахівця з безпеки, тоді як у великих підприємствах ці ролі зазвичай розділені. Професійний менеджер проєкту відповідає за загальне керування проєктом, тоді як спеціаліст з інформаційної безпеки здійснює контроль за безпекою та бере участь у впровадженні СУІБ.

Хоча стандарт ISO 27001 не вимагає формування окремої команди проєкту, така практика є доцільною для організацій із чисельністю понад 200 співробітників. Для малих підприємств достатньо менеджера проєкту, який координуватиме впровадження разом з іншими залученими учасниками.

Незалежно від розміру організації, доцільно залучати співробітників до таких видів діяльності, як оцінка ризиків, обробка ризиків, перегляд політик і процедур з метою узгодження документів безпеки з поточними бізнес-процесами, а також участь у затвердженні цілей безпеки й політик, щоб забезпечити підтримку та відповідність загальній бізнес-стратегії.

1.3.**Висновки до розділу 2**

Процес впровадження СУІБ може здаватися складним, однак насправді є достатньо зрозумілим. У його основі лежить формалізоване виявлення та управління загрозами для інформації організації. Щойно межі системи чітко окреслено, можна переходити безпосередньо до етапу впровадження. Як і у випадку з будь-яким масштабним проєктом, успіх залежить від ретельно продуманого планування. Важливо забезпечити, щоб документація відповідала своєму призначенню та була адаптована до потреб цільової аудиторії. Слід пам’ятати, що положення 4–10 стандарту є обов’язковими до виконання − вони містять вимоги, які необхідно враховувати під час створення та функціонування СУІБ.

РОЗДІЛ 3. РОЗРОБКА МЕТОДИКИ ВПРОВАДЖЕННЯ МІЖНАРОДНИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Підхід до розробки методики: Обґрунтування вибору циклу PDCA

Вибір циклу PDCA (Plan-Do-Check-Act) як основи для розробки методики впровадження міжнародних стандартів інформаційної безпеки – це стратегічне рішення, що ґрунтується на кількох ключових перевагах.

PDCA, розроблений У. Едвардсом Демінгом, є глобально визнаною моделлю для будь-якої системи менеджменту, зокрема й для СУІБ. Його універсальність полягає у здатності адаптуватися до різних контекстів та масштабів організації. Це означає, що розроблена методика не буде жорстко прив'язана до однієї компанії, а зможе бути застосована в широкому спектрі організацій, від малих підприємств до великих корпорацій.

Однією з найважливіших особливостей PDCA є його здатність забезпечувати безперервне вдосконалення. У динамічному світі кібербезпеки, де загрози постійно еволюціонують, а технології швидко змінюються, СУІБ не може бути статичною. Фаза «Check» (моніторинг та перегляд) і «Act» (постійне вдосконалення) у циклі PDCA дозволяють організації постійно оцінювати ефективність своїх заходів безпеки, виявляти недоліки та оперативно вносити корективи. Це гарантує, що СУІБ залишається актуальною, ефективною та адаптивною до нових викликів.

Крім того, цикл PDCA пропонує системний та структурований підхід, що є критично важливим для впровадження таких комплексних стандартів, як ISO/IEC 27001. Він розбиває складний процес на послідовні, керовані етапи: планування, реалізація, перевірка та коригування. Ця структура не лише спрощує процес впровадження, але й забезпечує послідовність дій, чіткий розподіл відповідальності та ефективне використання ресурсів. Кожен етап має

чітко визначені цілі та результати, що мінімізує невизначеність і дозволяє ефективно контролювати прогрес.

Отже, можна виділити наступні переваги методу PDCA:

1. *Універсальність та визнання у міжнародних стандартах*: Цикл PDCA, розроблений У. Едвардсом Демінгом, є наріжним каменем для багатьох систем управління, включаючи стандарти ISO. Самі стандарти, такі як ISO 27001, побудовані на цій моделі. Це означає, що використання PDCA забезпечує природну сумісність та гармонізацію з вимогами, які потрібно впровадити.

2. *Забезпечення безперервного вдосконалення*: Ключова перевага PDCA полягає в його здатності забезпечувати постійне вдосконалення. Інформаційна безпека – це не статичний стан, а безперервний процес адаптації до нових загроз та технологій. Кожна фаза циклу (планування, впровадження, моніторинг, коригування) створює основу для наступної, дозволяючи організації постійно підвищувати ефективність своєї СУІБ.

3. *Системний та структурований підхід*: PDCA пропонує чітку, логічну структуру, що розбиває складний процес впровадження СУІБ на керовані, послідовні етапи. Це дозволяє уникнути хаотичного підходу, забезпечити послідовність дій, ефективне розподілення ресурсів та контроль за виконанням. Кожна фаза має свою мету, результати та дії, що робить методику зрозумілою та застосовною.

4. *Фокус на результативності та ефективності*: Цикл PDCA вимагає моніторингу та аналізу результатів (фаза Check) для оцінки ефективності впроваджених заходів. Це дозволяє не просто виконувати вимоги, а й переконатися, що вони дійсно працюють, і, за потреби, внести коригувальні дії (фаза Act). Такий підхід гарантує, що СУІБ буде не лише відповідати стандарту, а й ефективно захищати інформаційні активи.

Розроблена методика є практичним, уніфікованим та структурованим посібником, створеним для допомоги організаціям у ефективному впровадженні та підтримці СУІБ згідно з міжнародними стандартами, зокрема ISO/IEC 27001. Її головна мета – демістифікувати складний процес стандартизації кібербезпеки,

роблячи його зрозумілим, керованим та досяжним для будь-якої компанії, незалежно від її розміру, галузі чи поточного рівня зрілості в питаннях ІБ.

Методика побудована таким чином, щоб забезпечити всебічний підхід до інформаційної безпеки, охоплюючи не лише технічні аспекти захисту, а й організаційні, процесні та людські фактори. Вона визнає, що ефективна СУІБ – це не одноразова дія, а безперервний цикл вдосконалення, який має інтегруватися в повсякденну діяльність організації.

Структурно методика розбита на чотири основні фази, які логічно відображають послідовність дій, необхідних для створення та підтримки функціонуючої СУІБ. Кожна фаза об'єднує в собі декілька деталізованих етапів, загальна кількість яких складає 13. Ці етапи є конкретними кроками, які необхідно виконати. Для кожного етапу методика надає:

- Чіткі дії: Що саме потрібно зробити.
- Практичні рекомендації: Як найкраще виконати ці дії, спираючись на передовий досвід та уникнення типових помилок. Ці рекомендації можуть включати використання певних інструментів, підходів або посилатися на необхідність розробки конкретних документів (шаблони яких можуть бути надані в прикладних матеріалах).
- Очікувані результати/документи: Конкретні deliverables, які мають бути отримані після завершення етапу. Це можуть бути політики, процедури, реєстри, протоколи чи інші записи, що підтверджують виконання вимог.

Така деталізація та покроковий формат роблять методику надзвичайно практичною та зручною для використання. Вона слугує як дорожня карта для керівництва, так і робочим інструментом для команд, відповідальних за впровадження ІБ. Це дозволяє організаціям не тільки досягти відповідності вимогам міжнародних стандартів для можливої сертифікації, але й побудувати справді міцну, адаптивну та ефективну систему захисту інформації, що є фундаментом для сталого розвитку в цифровому світі.

Філософія розробленої методики полягає в перетворенні процесу впровадження складних міжнародних стандартів інформаційної безпеки з потенційно хаотичного та ресурсоємного завдання на керований, передбачуваний та ефективний шлях. Вона ґрунтується на принципі, що інформаційна безпека є не просто набором технічних заходів, а невід'ємною частиною стратегічного управління організацією, що потребує системного підходу та постійного вдосконалення. Методика прагне демократизувати доступ до високих стандартів ІБ, роблячи їх реалізованими для ширшого кола організацій, незалежно від їхнього розміру чи галузі.

Структуру методики впровадження СУІБ наведено в Таблиці А.1 Додатку А.

2.2. **Фаза 1: Планування (Plan)**

Фаза: «Plan»

Номер Emany: Етап 1

Назва Emany: Ініціювання проєкту СУІБ та визначення контексту організації

Дії:

1. Призначення керівника проєкту СУІБ.

2. Формування проєктної команди СУІБ.

3. Аналіз внутрішніх факторів, що впливають на ІБ (організаційна структура, культура, ресурси, технології).

4. Аналіз зовнішніх факторів, що впливають на ІБ (законодавство, ринок, конкуренція, технологічні тренди).

5. Визначення зацікавлених сторін (внутрішніх та зовнішніх) та їхніх вимог до ІБ.

Результати:

- Статут проєкту СУІБ.

- Протокол засідання ініціативної групи.

- Документ «Контекст організації та зовнішні/внутрішні фактори».

Рекомендації:

1. Залучіть ключових стейкхолдерів на початковому етапі.

2. Проведіть SWOT-аналіз або PESTEL-аналіз для розуміння зовнішнього та внутрішнього середовища.

Прикладні матеріали:

Приклад внутрішніх та зовнішніх факторів наведено в таблиці Б.1 Додатку Б.

Приклад зацікавлених сторін та їхніх вимог наведено в таблиці Б.2 Додатку Б.

Верхньорівневу структуру документу «Контекст організації та зовнішні/внутрішні фактори» наведено в таблиці Б.3 Додатку Б.

Фаза: «Plan»

Номер Etapy: Етап 2

Назва Etapy: Визначення області застосування (Scope) СУІБ

Дії:

1. Визначення меж СУІБ: Чітко окресліть фізичні (локації), організаційні (підрозділи), технологічні (системи, ПЗ) та інформаційні (типи даних) кордони, в яких функціонуватиме СУІБ.

2. Ідентифікація інформаційних активів: Створіть перелік усіх активів, що знаходяться в межах визначеної області та підлягають захисту.

3. Обґрунтування виключень: Якщо якісь елементи не включаються до області застосування, чітко обґрунтуйте причини та оцініть потенційні ризики.

4. Документування області застосування: Оформіть всі визначені межі та включені активи в офіційний документ.

Результати:

- Документ «Область застосування СУІБ» (СУІБ Scope Document).

- Графічна схема меж СУІБ (за потреби).

Рекомендації:

1. Будьте реалістичними: Визначте область, яку організація дійсно здатна контролювати та захищати. Краще почати з меншої, керованої області та розширювати її з часом.

2. Врахуйте всі критичні бізнес-процеси: Переконайтеся, що всі ключові процеси, пов'язані з обробкою конфіденційної інформації, включені до області застосування.

3. Отримайте затвердження керівництва: Область застосування має бути офіційно затверджена вищим керівництвом.

Прикладні матеріали:

Приклад внутрішніх та зовнішніх факторів наведено в таблиці Б.4 Додатку Б.

Приклад графічної схеми меж СУІБ (табличний формат) наведено в таблиці Б.5 Додатку Б.

Фаза: «Plan»

Номер Етапу: Етап 3

Назва Етапу: Ідентифікація вимог зацікавлених сторін та правових/регуляторних зобов'язань

Дії:

1. Визначення конкретних вимог зацікавлених сторін: Проведення опитувань, інтерв'ю та аналіз договорів для виявлення їхніх очікувань до ІБ (наприклад, вимоги клієнтів до конфіденційності даних, очікування співробітників щодо захисту їхніх персональних даних).

2. Ідентифікація застосовних правових та регуляторних актів: Вивчення національного законодавства (наприклад, Закони України «Про захист

персональних даних», «Про основні засади забезпечення кібербезпеки України»), міжнародних норм (якщо застосовно, наприклад, GDPR, PCI DSS) та галузевих стандартів.

3. Визначення договірних зобов'язань: Аналіз угод з партнерами, клієнтами, постачальниками щодо вимог до ІБ, які організація повинна виконувати.

4. Документування та категоризація вимог: Систематизація всіх виявлених вимог та зобов'язань, їхнє оформлення у відповідні реєстри.

Результати:

- Реєстр вимог зацікавлених сторін.
- Реєстр правових та регуляторних зобов'язань.

Рекомендації:

1. Залучайте юридичний відділ для точної інтерпретації правових та регуляторних вимог.

2. Використовуйте матриці відповідності для ефективного відстеження та управління вимогами.

3. Регулярно оновлюйте реєстри, оскільки законодавство та вимоги можуть змінюватися.

Прикладні матеріали:

Приклад фрагменту реєстру вимог зацікавлених сторін наведено в таблиці Б.6 Додатку Б.

Приклад фрагменту реєстру вимог зацікавлених сторін наведено в таблиці Б.7 Додатку Б.

Фаза: «Plan»

Номер Etapy: Етап 4

Назва Etapy: Розробка Політики інформаційної безпеки та розподіл ролей/відповідальності

Дії:

1. Формулювання Політики інформаційної безпеки: Створіть офіційний документ, який декларує зобов'язання вищого керівництва щодо управління ІБ, визначає цілі ІБ та загальні принципи.

2. Затвердження Політики ІБ: Отримайте офіційне підтвердження та підпис Політики від вищого керівництва.

3. Визначення ключових ролей у СУІБ: Опишіть основні позиції, відповідальні за різні аспекти ІБ (наприклад, Власник інформації, Адміністратор ІБ, Керівник СУІБ, Власники процесів).

4. Деталізація відповідальності та повноважень: Чітко визначте обов'язки та повноваження для кожної ролі, пов'язаної з інформаційною безпекою.

5. Комунікація Політики та розподілу ролей: Забезпечте, щоб Політика ІБ та інформація про ролі були доведені до відома всіх співробітників та зацікавлених сторін.

Результати:

- Затверджена Політика інформаційної безпеки.

- Матриця ролей та відповідальності СУІБ.

Рекомендації:

1. Політика має бути зрозумілою, чіткою та лаконічною, без надмірної технічної термінології.

2. Переконайтеся, що політика відображає бізнес-цілі та підтримує основну діяльність організації.

3. Обов'язки та повноваження повинні бути документально закріплені та доведені до відома співробітників.

Прикладні матеріали:

Приклад структури Політики інформаційної безпеки наведено в таблиці Б.8 Додатку Б.

Приклад фрагменту Матриці ролей та відповідальності (RACI) для СУІБ наведено в таблиці Б.9 Додатку Б.

Фаза: «Plan»

Номер Etapy: Етап 5

Назва Etapy: Управління ризиками ІБ

Дії:

1. Ідентифікація активів: Створіть повний перелік інформаційних активів (дані, ПЗ, обладнання, послуги, персонал) в межах області застосування СУІБ.

2. Ідентифікація загроз та вразливостей: Виявіть потенційні загрози (кібератаки, збої, природні катастрофи) та вразливості (неоновлене ПЗ, слабкі паролі) для цих активів.

3. Оцінка ризиків: Проаналізуйте ймовірність реалізації загроз та потенційний вплив на бізнес. Використовуйте якісні або кількісні методи оцінки.

4. Визначення критеріїв прийнятності ризиків: Встановіть рівень ризиків, які організація готова прийняти.

5. Обробка ризиків: Розробіть план дій для зниження, уникнення, передачі або прийняття ризиків.

6. Розробка Заяви про застосовність (Statement of Applicability - SoA): Задокументуйте обрані заходи контролю (з ISO/IEC 27002), обґрунтуйте їхній вибір та поясніть виключені контролі.

Результати:

- Реєстр інформаційних активів.
- Реєстр ризиків інформаційної безпеки.
- План обробки ризиків (Risk Treatment Plan).
- Заява про застосовність (SoA).

Рекомендації:

1. Використовуйте уніфіковані методології оцінки ризиків (наприклад, ISO/IEC 27005 або власну адаптовану), що забезпечить послідовність та об'єктивність.

2. Залучайте експертів з різних підрозділів, оскільки вони є власниками активів та процесів і найкраще розуміють пов'язані з ними ризики.

3. Періодично переглядайте ризики, адже ландшафт загроз та вразливостей постійно змінюється.

Прикладні матеріали:

Приклад фрагменту Реєстру інформаційних активів наведено в таблиці Б.10 Додатку Б.

Приклад фрагменту Реєстру ризиків інформаційної безпеки наведено в таблиці Б.11 Додатку Б.

2.3. **Фаза 2: Впровадження (Do)**

Фаза: «Do»

Номер Етапу: Етап 6

Назва Етапу: Розробка та впровадження контролів безпеки

Дії:

1. Деталізація заходів контролю: Розробіть детальні вимоги та специфікації для кожного заходу контролю, обраного в Плані обробки ризиків та SoA.

2. Розробка внутрішніх процедур та інструкцій: Створіть покрокові документи, що описують, як мають бути виконані технічні, організаційні та фізичні контролі (наприклад, процедура управління доступом, інструкція з резервного копіювання).

3. Впровадження технічних засобів захисту: Реалізуйте обрані технологічні рішення (наприклад, встановлення та налаштування міжмережевих екранів, антивірусного ПЗ, систем SIEM, шифрування).

4. Впровадження організаційних та фізичних контролів: Запровадьте відповідні організаційні заходи (наприклад, розмежування обов'язків, політики «чистого столу») та заходи фізичної безпеки (контроль доступу до приміщень, відеоспостереження).

5. Тестування та валідація контролів: Проведіть перевірку впроваджених контролів для підтвердження їхньої ефективності та відповідності вимогам.

6. Документування впровадження: Зафіксуйте всі виконані дії, конфігурації систем та результати тестування.

Результати:

- Розроблені та затверджені процедури, інструкції та регламенти з безпеки.
- Впроваджені технічні засоби захисту (брандмауери, антивіруси, SIEM тощо).
- Реалізовані організаційні та фізичні заходи контролю.
- Звіти про результати тестування контролів.

Рекомендації:

1. Дотримуйтеся пріоритетів, визначених Планом обробки ризиків.

2. Забезпечте належне документування всіх впроваджених контролів та їхніх конфігурацій.

3. Використовуйте ISO/IEC 27002 як посібник для деталізації та реалізації контролів.

4. Забезпечте інтеграцію впроваджених контролів з існуючими бізнес-процесами.

Прикладні матеріали:

Приклади контролів безпеки та їхньої реалізації наведено в таблиці Б.12 Додатку Б.

Загальний процес впровадження контролю наведено на рис. Б.1 Додатку Б.

Фаза: «Do»

Номер Emany: Етап 7

Назва Emany: Управління документацією СУІБ

Дії:

1. Розробка та впровадження регламенту управління документацією СУІБ: Створіть внутрішній документ, який детально описує всі процедури, пов'язані з життєвим циклом документів СУІБ. Це включає створення, перегляд, затвердження, розповсюдження, зберігання, ідентифікацію версій та контроль доступу.

2. Створення та ведення реєстру документів СУІБ: Сформуйте централізований перелік усіх документів, що належать до СУІБ, із зазначенням назви, унікального ідентифікатора, версії, дати затвердження, відповідальних осіб та місця зберігання.

3. Забезпечення контрольованого створення та перегляду документів: Встановіть процедури для розробки нових документів та регулярного перегляду існуючих, включаючи процес погодження та затвердження.

4. Впровадження системи версіонування документів: Забезпечте чіткий ідентифікатор версії для кожного документа, що дозволяє відстежувати зміни та використовувати лише актуальні версії.

5. Організація розповсюдження та доведення документів до відома: Розробіть механізми для своєчасного донесення актуальних документів до відповідних співробітників та зацікавлених сторін.

6. Забезпечення контрольованого зберігання документів: Визначте місця зберігання (електронні та фізичні), умови зберігання, резервного копіювання та захисту від несанкціонованого доступу.

7. Встановлення правил вилучення застарілих документів: Розробіть процедуру архівації або знищення застарілих версій документів, зберігаючи необхідні історичні записи.

Результати:

- Регламент управління документацією СУІБ: Затверджений внутрішній документ, що описує процедури роботи з усією документацією СУІБ.
- Реєстр документів СУІБ: Актуальний, централізований перелік усіх документів, що входять до Системи управління інформаційною безпекою.
- Затверджені версії всіх документів СУІБ: Вся необхідна документація розроблена, затверджена та доступна у контрольованих версіях.
- Впроваджена система версіонування та архівування документів: Чіткий механізм для відстеження змін у документах та зберігання їхньої історії.

Рекомендації:

1. Використовуйте Системи електронного документообігу (СЕДО): Це значно спрощує процеси створення, погодження, зберігання, версіонування та розповсюдження документів, автоматизуючи багато ручних операцій.

2. Впровадьте єдину систему нумерації та версіонування документів: Це допоможе швидко знаходити потрібні документи та відстежувати їхній статус, наприклад: «ІБ-ПОЛ-001 v1.0».

3. Розробіть шаблони документів: Створення уніфікованих шаблонів для різних типів документів (політик, процедур, інструкцій, реєстрів, форм) забезпечить єдність стилю та прискорить розробку.

4. Забезпечте доступність документів: Переконайтеся, що співробітники мають легкий доступ до необхідних документів відповідно до їхніх ролей та обов'язків.

5. Проводьте періодичний перегляд документів: Встановіть регулярний графік перегляду (наприклад, щорічно) для забезпечення актуальності та відповідності змінам.

Прикладні матеріали:

Ієрархію документації СУІБ наведено в таблиці Б.13 Додатку Б.

Приклад структури типового документа СУІБ наведено в таблиці Б.14 Додатку Б.

Фаза: «Do»

Номер Етапу: Етап 8

Назва Етапу: Проведення програм навчання та підвищення обізнаності персоналу

Дії:

1. Визначення потреб у навчанні: Оцініть, які знання та навички з ІБ потрібні різним категоріям персоналу, виходячи з їхніх ролей та обов'язків.

2. Розробка навчальних матеріалів: Створіть змістовні та зрозумілі матеріали (презентації, пам'ятки, відео, інструкції, тести) для різних програм навчання.

3. Проведення навчальних заходів: Організуйте та проведіть тренінги, семінари, вебінари, онлайн-курси для підвищення обізнаності співробітників.

4. Регулярне інформування: Забезпечте постійне розповсюдження актуальної інформації про загрози та правила ІБ через внутрішні канали комунікації (наприклад, корпоративний портал, електронні розсилки).

5. Оцінка рівня обізнаності: Проводьте тестування знань або симуляції (наприклад, фішингових атак) для перевірки ефективності навчання та обізнаності персоналу.

6. Аналіз результатів та коригувальні дії: На основі оцінки виявляйте прогалини в знаннях та коригуйте навчальні програми.

Результати:

- План навчання та підвищення обізнаності з питань ІБ.
- Розроблені навчальні матеріали.
- Записи про проведені навчання та тренінги (списки учасників, дати).
- Результати тестування рівня обізнаності персоналу.

Рекомендації:

1. Адаптуйте матеріали до рівня та ролей співробітників, використовуючи зрозумілу мову та релевантні приклади.

2. Використовуйте інтерактивні формати (відео, квізи, ігрові симуляції) для кращого засвоєння інформації.

3. Проводьте регулярні симуляції фішингових атак та інших соціальних інженерних загроз для підвищення пильності та формування практичних навичок.

4. Заохочуйте відкриту комунікацію та ставтеся до помилок як до можливості для навчання, а не покарання.

Прикладні матеріали:

Приклади програм навчання з інформаційної безпеки за ролями наведено в таблиці Б.15 Додатку Б.

2.4. **Фаза 3: Моніторинг та перегляд (Check)**

Фаза: «Check»

Номер Етапу: Етап 9

Назва Етапу: Моніторинг, вимірювання, аналіз та оцінка ефективності СУІБ

Дії:

1. Визначення ключових показників ефективності (KPIs) для моніторингу СУІБ (наприклад, кількість інцидентів, час реагування, відсоток вразливостей).

2. Збір даних щодо визначених KPIs з різних джерел (журнали систем, звіти з інструментів безпеки, результати сканувань).

3. Аналіз зібраних даних для виявлення тенденцій, аномалій та оцінки виконання цілей ІБ.

4. Оцінка ефективності впроваджених контролів безпеки та процесів СУІБ.

5. Підготовка звітів про результати моніторингу та оцінки ефективності.

Результати:

- Перелік визначених KPIs для СУІБ.
- Звіти про результати моніторингу KPIs та подій ІБ.
- Звіти про оцінку ефективності контролів безпеки.

Рекомендації:

1. Автоматизуйте збір даних для моніторингу, де це можливо (наприклад, за допомогою SIEM-систем).

2. Використовуйте інструменти візуалізації даних (дашборди) для швидкого та наочного відображення стану безпеки.

3. Регулярно переглядайте та оновлюйте KPIs, щоб вони залишалися релевантними до поточних загроз та цілей організації.

Прикладні матеріали:

Приклади KPIs для моніторингу СУІБ наведено в таблиці Б.16 Додатку Б.

Приклад дашборду моніторингу СУІБ наведено на рис. Б.2 Додатку Б.

Фаза: «Check»

Номер Етапу: Етап 10

Назва Етапу: Проведення внутрішніх аудитів СУІБ

Дії:

1. Розробка програми внутрішнього аудиту: Створіть план аудитів, що включає їхній обсяг, частоту, методи та критерії (вимоги ISO/IEC 27001, внутрішні політики, процедури).

2. Формування команди внутрішніх аудиторів: Призначте кваліфікованих та незалежних аудиторів, які не несуть безпосередньої відповідальності за процес, що аудитується.

3. Проведення аудитів: Виконайте заплановані аудити, збираючи об'єктивні докази (документи, записи, інтерв'ю, спостереження).

4. Підготовка звітів про аудит: Сформуйте звіти, що містять виявлені невідповідності (відхилення від вимог стандарту чи внутрішніх документів), спостереження та рекомендації.

5. Доведення результатів аудиту: Ознайомте з результатами аудиту відповідальних осіб та керівництво.

Результати:

- Програма внутрішнього аудиту СУІБ.
- Звіти про проведення внутрішніх аудитів.
- Реєстр виявлених невідповідностей та спостережень.

Рекомендації:

1. Забезпечте незалежність та об'єктивність внутрішніх аудиторів для достовірності результатів.

2. Використовуйте чіткі чек-листи аудиту, розроблені на основі вимог стандарту та внутрішніх документів.

3. Забезпечте відкриту та конструктивну комунікацію між аудиторами та аудитованими підрозділами.

Прикладні матеріали:

Приклад структури Програми внутрішнього аудиту СУІБ наведено в таблиці Б.17 Додатку Б.

Приклад фрагменту Звіту про внутрішній аудит наведено в таблиці Б.18 Додатку Б.

Фаза: «Check»

Номер Етапу: Етап 11

Назва Етапу: Аналіз СУІБ з боку керівництва

Дії:

1. Підготовка вхідних даних для аналізу: Зберіть та узагальніть всю необхідну інформацію про функціонування СУІБ. Це включає результати попередніх аудитів, показники моніторингу (KPIs), звітність про інциденти ІБ, зворотний зв'язок від зацікавлених сторін, статус коригувальних дій та зміни у зовнішньому/внутрішньому контексті організації.

2. Проведення засідання керівництва: Організуйте та проведіть зустріч вищого керівництва, на якій буде представлений звіт та обговорений поточний стан СУІБ.

3. Оцінка ефективності СУІБ: Керівництво оцінює, наскільки СУІБ відповідає встановленим цілям, вимогам стандарту ISO/IEC 27001, а також її загальну придатність та адекватність для потреб організації.

4. Прийняття рішень: За результатами аналізу керівництво приймає рішення щодо подальших кроків, таких як необхідність зміни політик, виділення додаткових ресурсів, впровадження нових контролів, перегляд цілей або зміни в області застосування СУІБ.

5. Документування результатів аналізу: Зафіксуйте всі обговорення, прийняті рішення та призначені відповідальності у протоколі засідання.

Результати:

- Звіт для аналізу СУІБ з боку керівництва (Management Review Report).
- Протокол засідання керівництва щодо аналізу СУІБ.

- Рішення та розпорядження керівництва щодо подальших кроків у розвитку СУІБ.

Рекомендації:

1. Забезпечте активну участь вищого керівництва в процесі аналізу, оскільки їхня прихильність та підтримка є критично важливими.

2. Сформуйте чіткий порядок денний засідання, щоб забезпечити структуроване та продуктивне обговорення.

3. Фокусуйтеся на прийнятті конкретних, вимірюваних рішень та чіткому визначенні відповідальних за їх виконання.

Прикладні матеріали:

Приклад вхідних даних для аналізу СУІБ з боку керівництва наведено в таблиці Б.19 Додатку Б.

Приклад фрагменту Протоколу засідання керівництва щодо аналізу СУІБ наведено в таблиці Б.20 Додатку Б.

2.5. **Фаза 4: Постійне вдосконалення (Act)**

Фаза: «Act»

Номер Emany: Етап 12

Назва Emany: Управління невідповідностями та коригувальні дії

Дії:

1. Ідентифікація та документування невідповідностей: Зафіксуйте будь-які відхилення від вимог стандарту ISO/IEC 27001, внутрішніх політик, процедур або запланованих результатів. Невідповідності можуть бути виявлені під час аудитів, моніторингу, аналізу інцидентів або зворотного зв'язку.

2. Аналіз першопричин: Для кожної невідповідності проведіть глибокий аналіз, щоб виявити її справжні причини, а не лише симптоми. Це може бути відсутність процедури, недостатнє навчання, збій обладнання тощо.

3. Розробка планів коригувальних дій: Сформулюйте конкретні, вимірювані, досяжні, релевантні та обмежені в часі (SMART) дії, спрямовані на усунення виявлених невідповідностей та запобігання їх повторенню.

4. Впровадження коригувальних дій: Реалізуйте заплановані дії. Це може включати оновлення документів, проведення додаткового навчання, налаштування систем або зміну процесів.

5. Перевірка ефективності коригувальних дій: Оцініть, наскільки успішно впроваджені дії усунули невідповідність та її першопричину, а також чи не спричинили вони нових проблем.

6. Документування процесу: Ведіть записи про весь цикл управління невідповідностями та коригувальними діями.

Результати:

- Реєстр невідповідностей: Документ, що містить інформацію про всі виявлені невідповідності.
- Плани коригувальних дій: Детальні плани усунення невідповідностей та їхніх першопричин.
- Звіти про впровадження та ефективність коригувальних дій: Документальні підтвердження виконання планів та досягнутих результатів.

Рекомендації:

1. Застосовуйте системний підхід до усунення кореневих причин, а не лише симптомів проблеми. Використовуйте техніки, як «5 чому» або «діаграма риб'ячої кістки».

2. Забезпечте оперативне реагування на виявлені невідповідності, щоб мінімізувати потенційний збиток.

3. Відстежуйте прогрес виконання коригувальних дій та їхню ефективність.

Прикладні матеріали:

Приклад фрагменту Реєстру невідповідностей наведено в таблиці Б.21 Додатку Б.

Діаграму "5 чому" (приклад аналізу першопричин) наведено на рис. Б.3 Додатку Б.

Фаза: «Act»

Номер Emany: Етап 13

Назва Emany: Постійне вдосконалення СУІБ

Дії:

1. Аналіз даних для виявлення можливостей покращення: Здійсніть комплексний аналіз усіх зібраних даних з попередніх фаз (результати моніторингу, аудити, аналіз керівництва, інциденти, невідповідності, зворотний зв'язок від зацікавлених сторін).

2. Формування пропозицій щодо покращення: На основі проведеного аналізу ініціюйте конкретні пропозиції, спрямовані на підвищення загальної ефективності, придатності та адекватності СУІБ. Це може включати оптимізацію існуючих процесів, впровадження нових технологій чи контролів.

3. Планування та впровадження покращень: Розробіть детальні плани для реалізації вибраних покращень, визначте відповідальних осіб та терміни.

4. Оцінка ефективності впроваджених покращень: Після реалізації змін перевірте, чи досягнуті очікувані результати та чи підвищилася ефективність СУІБ.

5. Оновлення документації СУІБ: Актуалізуйте відповідну документацію (політики, процедури, реєстри) відповідно до внесених змін та покращень.

6. Ініціювання нового циклу PDCA: Результати цього етапу стають вхідними даними для нового циклу Планування, забезпечуючи безперервний процес вдосконалення.

Результати:

- Плани постійного вдосконалення СУІБ.

- Реалізовані зміни та покращення у СУІБ.
- Оновлені версії документів СУІБ.
- Підвищення загальної ефективності та зрілості СУІБ.

Рекомендації:

1. Створіть культуру постійного вдосконалення в організації, заохочуючи всіх співробітників до виявлення та подання пропозицій.

2. Регулярно переглядайте нові міжнародні стандарти, кращі практики та тенденції у сфері кібербезпеки для виявлення потенційних покращень.

3. Використовуйте методології управління проєктами для ефективного планування та впровадження масштабних покращень СУІБ.

Прикладні матеріали:

Приклад Плану постійного вдосконалення СУІБ наведено в таблиці Б.22 Додатку Б.

2.6. **Висновки до Розділу 3**

Розроблена методика є практичним та уніфікованим інструментом, що дозволяє організаціям поетапно впроваджувати міжнародні стандарти інформаційної безпеки, зокрема ISO/IEC 27001. Її структура, заснована на циклі PDCA, забезпечує системний підхід до управління СУІБ, охоплюючи планування, реалізацію, моніторинг та постійне вдосконалення. Завдяки детальній розбивці на 13 етапів, з чітко визначеними діями, рекомендаціями та очікуваними результатами, методика значно підвищує доступність та ефективність процесу побудови та підтримки СУІБ, сприяючи підвищенню рівня інформаційної безпеки та стійкості організацій до сучасних кіберзагроз.

ВИСНОВКИ

У кваліфікаційній роботі було досягнуто поставленої мети — розроблено методику поетапного впровадження Системи управління інформаційною безпекою (СУІБ) на основі міжнародних стандартів, що робить цей процес більш доступним та підвищує ефективність управління ІБ на організаційному рівні.

Під час виконання роботи було:

1. Проаналізовано роль та значення міжнародних стандартів у забезпеченні сучасної інформаційної безпеки. Визначено, що в умовах зростаючих кіберзагроз та складності інформаційних систем, міжнародні стандарти є невід'ємним інструментом для системного управління ІБ, підвищення довіри та відповідності регуляторним вимогам.

2. Здійснено поглиблений аналіз ключових міжнародних стандартів: ISO/IEC 27001, ISO/IEC 27002 та ISO 31000. Детальне вивчення їхніх вимог, принципів та взаємозв'язків дозволило сформувати комплексне розуміння архітектури СУІБ та необхідних контролів.

3. Досліджено існуючі підходи та практики впровадження СУІБ згідно з вимогами серії стандартів ISO 27000. Виявлення сильних сторін та типових викликів цих підходів дозволило інтегрувати найкращі практики та уникнути поширених помилок у власній розробці. Зокрема, аналіз вітчизняної та зарубіжної літератури висвітлив пробіл у деталізованих, практично орієнтованих методиках поетапного впровадження СУІБ, адаптованих до українських реалій.

4. На основі проведеного аналізу та досліджень, розроблено власну методику впровадження міжнародних стандартів інформаційної безпеки. Ця методика базується на принципах циклу PDCA (Plan-Do-Check-Act), що забезпечує її циклічність та безперервне вдосконалення. Методика деталізована на 13 послідовних етапів, кожен з яких містить чітко визначені дії, рекомендації

та очікувані результати/документи, роблячи її чітким та практичним посібником для організацій.

Запропонована методика дозволить організаціям системно та поетапно впроваджувати вимоги міжнародних стандартів ІБ, оптимізувати процеси управління ризиками, підвищити обізнаність персоналу та забезпечити постійний моніторинг та покращення СУІБ. Це сприятиме не лише досягненню відповідності вимогам стандартів, а й підвищенню загального рівня інформаційної безпеки, зниженню операційних ризиків та зміцненню позицій організації на ринку в умовах зростаючих кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27000:2018. Information security management systems – Overview and vocabulary. – Geneva: ISO, 2018.

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

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

4. ISO 31000:2018. Risk management – Guidelines. – Geneva: ISO, 2018.

5. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. – Geneva: ISO, 2022.

6. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI (зі змінами). – К. : Верховна Рада України, 2010.

7. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII (зі змінами). – К. : Верховна Рада України, 2017.

8. Goodwin, R. Information Security Management: The Essential ISO 27001 Guide / R. Goodwin. – Kogan Page, 2020. – 288 p.

9. Ramesh, R. Cybersecurity Management in the Digital Age: Best Practices and Emerging Trends / R. Ramesh, S. Kumar. – CRC Press, 2023. – 350 p.

10. Верба, І. В. Інформаційна безпека в умовах гібридної війни: український досвід / І. В. Верба, О. П. Савич // Збірник наукових праць Військової академії. – 2023. – № 1. – С. 123-130.

11. Калініченко, В. А. Актуальні питання імплементації європейського законодавства у сфері кібербезпеки в Україні / В. А. Калініченко // Правове життя сучасної України : матеріали конф. – 2022. – Т. 2. – С. 150-153.

12. Хорошко, О. В. Системи управління інформаційною безпекою: принципи побудови та функціонування / О. В. Хорошко // Вісник Київського

національного університету імені Тараса Шевченка. Фізико-математичні науки. – 2018. – № 2. – С. 87-95.

13. Безкоровайна, Л. М. Практичні аспекти впровадження ISO 27001 на підприємствах України / Л. М. Безкоровайна // Науковий вісник Ужгородського національного університету. Серія: Економіка. – 2021. – Вип. 2 (59). – С. 101-106.

14. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape Report 2023. – Luxembourg: Publications Office of the European Union, 2024.

15. Ponemon Institute. Cost of a Data Breach Report 2024 / IBM Security. – 2024.

16. World Economic Forum. The Global Cybersecurity Outlook 2024. – Geneva: World Economic Forum, 2024.

17. Gartner, Inc. Hype Cycle for Cyber Security 2023. – Stamford: Gartner, 2023.

18. Case, J. T. ISO 27001: A Pocket Guide / J. T. Case. – IT Governance Publishing, 2020. – 148 p.

19. British Standards Institution (BSI). The ISO 27001 standard: What it is and why it matters. – 2023.

20. ISO. The ISO Survey of Management System Standard Certifications 2022. – Geneva: ISO, 2023.

21. ISACA. State of Cybersecurity 2023. – Schaumburg: ISACA, 2023.

22. National Institute of Standards and Technology (NIST). Cybersecurity Framework Version 1.1. – Gaithersburg: NIST, 2018.

23. Deming, W. E. The New Economics for Industry, Government, Education / W. E. Deming. – 2nd ed. – Cambridge: MIT Press, 1993. – 264 p.

24. ISO. Introduction to Management System Standards. – Geneva: ISO, 2023.

25. (ISC)². Cybersecurity Workforce Study 2023. – Clearwater: (ISC)², 2023.

26. PwC. Global Economic Crime and Fraud Survey 2022. – London: PwC, 2022.

27. European Parliament and Council. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). – Brussels: European Parliament, 2016.

28. Payment Card Industry Security Standards Council (PCI SSC). Payment Card Industry Data Security Standard (PCI DSS) v.4.0. – Wakefield: PCI SSC, 2022.

29. U.S. National Archives and Records Administration (NARA). Federal Information Security Management Act of 2014 (FISMA). – Washington, D.C.: NARA, 2014.

30. U.S. Congress. Health Insurance Portability and Accountability Act of 1996 (HIPAA). – Washington, D.C.: U.S. G.P.O., 1996.

31. American Institute of Certified Public Accountants (AICPA). SOC for Service Organizations. – Durham: AICPA, 2023.

32. U.S. Department of Defense. Cybersecurity Maturity Model Certification (CMMC) Program. – Washington, D.C.: DoD, 2023.

33. Sarbanes-Oxley Act of 2002. Public Law 107-204. – Washington, D.C.: U.S. G.P.O., 2002.

34. Forrester Research. Predictions 2024: Cybersecurity. – Cambridge: Forrester, 2023.

35. Cybersecurity Ventures. Cybercrime Report 2024. – Menlo Park: Cybersecurity Ventures, 2024.

36. CERT-UA. Звіти про кібератаки та кіберінциденти за 2022-2024 роки. – Київ: CERT-UA, 2022-2024.

37. Національний інститут стратегічних досліджень. Аналітичний звіт "Кібербезпека України: виклики та шляхи розвитку". – Київ: НІСД, 2023. – 80 с.

38. Bank for International Settlements (BIS). Cyber Resilience in the Financial Sector. – Basel: BIS, 2021.

39. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»" від 26.08.2021 № 447/2021. – К. : Президент України, 2021.

ДОДАТКИ

Додаток А

Таблиця А.1

Структура методики впровадження СУІБ

Фаза PDCA	Етап №	Назва Етапу
P (Plan)	1	Ініціювання проєкту СУІБ та визначення контексту організації
P (Plan)	2	Визначення області застосування (Scope) СУІБ
P (Plan)	3	Ідентифікація вимог зацікавлених сторін та правових/регуляторних зобов'язань
P (Plan)	4	Розробка Політики інформаційної безпеки та розподіл ролей/відповідальності
P (Plan)	5	Управління ризиками ІБ
D (Do)	6	Розробка та впровадження контролів безпеки
D (Do)	7	Управління документацією СУІБ
D (Do)	8	Проведення програм навчання та підвищення обізнаності персоналу
C (Check)	9	Моніторинг, вимірювання, аналіз та оцінка ефективності СУІБ
C (Check)	10	Проведення внутрішніх аудитів СУІБ
C (Check)	11	Аналіз СУІБ з боку керівництва
A (Act)	12	Управління невідповідностями та коригувальні дії
A (Act)	13	Постійне вдосконалення СУІБ

Додаток Б

Таблиця Б.1

Приклад внутрішніх та зовнішніх факторів

Внутрішні фактори	**Зовнішні фактори**
Організаційна структура	Законодавство у сфері ІБ
Культура інформаційної безпеки	Конкуренція на ринку
Наявні ресурси (фінансові, кадрові)	Технологічні тренди (нові загрози)
ІТ-інфраструктура та технології	Вимоги клієнтів та партнерів
Бізнес-процеси організації	Стандарти та регуляторні вимоги галузі

Таблиця Б.2

Приклад зацікавлених сторін та їхніх вимог

Зацікавлена сторона	**Вимоги до ІБ**
Керівництво	Захист репутації, мінімізація фінансових втрат
Співробітники	Захист персональних даних
Клієнти	Конфіденційність їхньої інформації
Регулятори	Відповідність законодавству

Таблиця Б.3

Верхньорівнева структура документу «Контекст організації та зовнішні/внутрішні фактори»

Розділ документу	**Зміст**
1. Вступ та мета	Опис мети документу, його роль у СУІБ.
2. Внутрішній контекст	Детальний опис організації (структура, цінності, стратегія, можливості).
3. Зовнішній контекст	Аналіз ринкових, правових, технологічних, соціальних факторів.

Продовження Таблиці Б.3

1	2
4. Зацікавлені сторони та їхні вимоги	Перелік сторін, їхні потреби, очікування та вплив на ІБ.
5. Висновки та вплив на СУІБ	Узагальнення виявлених факторів, їхній вплив на цілі СУІБ.

Таблиця Б.4

Приклад внутрішніх та зовнішніх факторів

Категорія	**Опис / Приклад**
Інформація	Конфіденційні дані клієнтів, фінансова звітність, комерційна таємниця
Системи	CRM-система, бухгалтерська програма, файловий сервер, корпоративна мережа
Бізнес-процеси	Обробка замовлень клієнтів, фінансовий облік, управління персоналом, розробка ПЗ
Підрозділи	Відділ продажів, Фінансовий відділ, ІТ-відділ, Департамент маркетингу
Фізичні локації	Центральний офіс (Київ, вул. Хрещатик, 10), віддалений ЦОД (вул. Київська, 5)

Таблиця Б.5

Приклад графічної схеми меж СУІБ (табличний формат)

Елемент організації	**Статус включення в Область Застосування СУІБ**	**Коментар**
Департаменти		
Відділ продажів	Включено	Обробляє конфіденційні дані клієнтів.
Фінансовий відділ	Включено	Працює з фінансовою звітністю.
ІТ-відділ	Включено	Відповідає за підтримку всіх ІС.
Відділ кадрів	Включено	Обробляє персональні дані співробітників.
Відділ маркетингу	Виключено (частково)	Тільки публічні активності; внутрішні дані маркетингу включені через ІТ.
Інформаційні Системи		
CRM-система	Включено	Містить критичні дані клієнтів.
Бухгалтерська програма	Включено	Обробляє всі фінансові операції.
Корпоративний веб-сайт	Включено (адміністрування)	Контроль за публічною інформацією та безпекою платформи.

Продовження Таблиці Б.5

1	2	3
Застарілі системи (Legacy Systems)	Виключено	Вимагають окремого аудиту та плану міграції/виведення.
Фізичні Локації		
Головний офіс (м. Київ)	Включено	Усі робочі місця та серверні приміщення.
Віддалений склад	Виключено	Не обробляє конфіденційну інформацію, має мінімальний доступ.

Таблиця Б.6

Приклад фрагменту реєстру вимог зацікавлених сторін

Зацікавлена сторона	**Тип вимоги**	**Опис вимоги**	**Джерело вимоги**
Клієнт (Фіз. особа)	Регуляторна	Захист персональних даних згідно ЗУ «Про захист ПД»	Закон України
Постачальник «Х»	Договірна	Дотримання умов NDA щодо комерційної таємниці	Договір про співпрацю
НБУ	Регуляторна	Виконання вимог Постанови НБУ №95 (для фін. установ)	Постанова НБУ
Співробітники	Внутрішня	Захист особистих даних, безпечне робоче середовище	Кодекс етики

Таблиця Б.7

Приклад фрагменту реєстру вимог зацікавлених сторін

Нормативний акт / Стандарт	**Стаття/Пункт**	**Зміст вимоги**	**Застосовність**
ЗУ «Про захист персональних даних»	Ст. 24	Обов'язок повідомляти про витік персональних даних.	Усі ПД
GDPR (General Data Protection Reg.)	Art. 32	Вимоги до технічних та організаційних заходів безпеки (для обробників даних ЄС).	Якщо обробляються дані резидентів ЄС
PCI DSS v.3.2.1	Req. 3.4	Захист збережених даних власників карток.	Для обробників платіжних карт

Таблиця Б.8

Приклад структури Політики інформаційної безпеки

Розділ	**Короткий опис**
1. Мета та сфера застосування	Чому політика створена, на що поширюється.
2. Зобов'язання керівництва	Заява вищого керівництва щодо підтримки ІБ.
3. Основні принципи ІБ	Фундаментальні правила (конфіденційність, цілісність, доступність).
4. Організаційна структура ІБ	Опис ролей та відповідальності (наприклад, Власник інформації, Керівник СУІБ).
5. Порядок перегляду та оновлення	Як часто політика переглядається, хто відповідальний.

Продовження додатку Б

Таблиця Б.9

Приклад фрагменту Матриці ролей та відповідальності (RACI) для СУІБ

Процес / Активність	**Керівник СУІБ**	**Власник інформації**	**Адміністратор ІБ**	**Користувач**
Розробка політик ІБ	R, A	C	I	I
Оцінка ризиків ІБ	A	R	C	I
Надання прав доступу	I	A	R	C
Реагування на інциденти ІБ	A	I	R, C	R
Пояснення: R - Відповідальний (Responsible), A - Підзвітний (Accountable), C - Консультує (Consulted), I - Інформований (Informed).				

Таблиця Б.10

Приклад фрагменту Реєстру інформаційних активів

Назва активу	**Тип активу**	**Власник активу**	**Класифікація (Конфіденційність/Цілісність/Доступність)**
База даних клієнтів	Дані	Відділ продажів	Висока/Висока/Висока
Корпоративний веб-сервер	Обладнання	ІТ-відділ	Висока/Висока/Висока
Політика ІБ	Документ	Керівник СУІБ	Висока/Висока/Висока

Продовження додатку Б

Таблиця Б.11

Приклад фрагменту Реєстру ризиків інформаційної безпеки

Ідентифікатор ризику	**Загроза**	**Вразливість**	**Рівень ризику (до обробки)**	**Стратегія обробки ризику**	**Обрані заходи контролю (з SoA)**
R-005	Фішингова атака	Низька обізнаність персоналу, відсутність спам-фільтрів	Високий	Зниження	A.7.2.2 (Обізнаність), A.8.2.1 (Захист від шкідливого ПЗ)
R-012	Несанкціонований доступ до системи	Слабкі паролі, відсутність 2FA	Високий	Зниження	A.9.2.1 (Контроль доступу), A.9.2.2 (Парольна політика)
R-018	Втрата даних через відмову обладнання	Відсутність резервного копіювання	Середній	Зниження	A.12.3.1 (Резервне копіювання)

Продовження додатку Б

Таблиця Б.12

Приклади контролів безпеки та їхньої реалізації

Категорія контролю	**Приклад контролю (ISO 27002)**	**Опис впровадження**
Організаційний	А.6.2 Розподіл обов'язків	Впроваджено процедуру розмежування обов'язків для критичних процесів
Технічний	А.8.2.1 Захист від шкідливого ПЗ	Встановлено та налаштовано корпоративний антивірус на всіх робочих станціях
Фізичний	А.11.1.2 Контроль доступу	Впроваджено систему контролю та управління доступом (СКУД) до серверної кімнати
Процедурний	А.12.1.1 Процедури операційної діяльності	Розроблено процедуру щоденного резервного копіювання баз даних

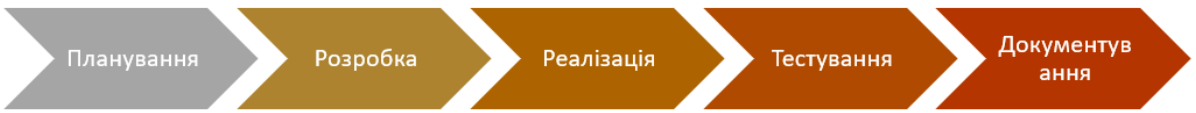

Рисунок Б.1. Загальний процес впровадження контролю

Таблиця Б.13

Ієрархія документації СУІБ

Рівень документа	**Призначення**	**Приклад**
Стратегічні документи	Визначають підходи та методи управління ІБ, її структуру та корпоративне управління.	Стратегія ІБ
Політики	Регулюють предметні області ІБ, визначають цілі та завдання процесів.	Політика управління доступом
Процедури	Описують етапи процесів ІБ.	Процедура надання, зміни та блокування доступу
Вимоги та правила	Звід правил / вимог до організації діяльності.	Рольова матриця доступу
Шаблонні документи (звіти)	Шаблони результатів виконання конкретних процедур ІБ.	Звіт щорічного перегляду прав доступу співробітників в ІС

Таблиця Б.14

Приклад структури типового документа СУІБ

Секція документа	**Короткий опис**
Заголовок документа	Назва, тип, актуальна версія, дата останнього перегляду, автор.
Короткий опис	Важливість для об'єкта інформаційної діяльності, перелік ролей та відповідальностей.

Продовження додатку Б

Продовження Таблиці Б.14

1	2
Посилання між документами	Зв'язок з іншою документацією.
Основний зміст	Загальні положення, поняття, вимоги, детальний опис.
Закінчення	Прикінцеві положення, правила використання, історія перегляду та оновлення.

Таблиця Б.15

Приклади програм навчання з інформаційної безпеки за ролями

Категорія персоналу	**Основні теми навчання**	**Метод навчання**
Всі співробітники	Основи ІБ, політика «чистого столу/екрану», розпізнавання фішингу, безпечна робота з поштою та інтернетом.	Онлайн-курс, періодичні розсилки, симуляції фішингу
Нові співробітники	Вступний курс з ІБ, ключові політики безпеки компанії, правила користування ресурсами.	Обов'язковий інструктаж, внутрішній портал
ІТ-спеціалісти	Безпечна розробка/налаштування систем, управління вразливостями, реагування на інциденти, криптографія.	Спеціалізовані тренінги, вебінари
Керівний склад	Роль керівництва в СУІБ, управління ризиками ІБ, забезпечення відповідності.	Семінари, аналітичні матеріали

Продовження додатку Б

Таблиця Б.16

Приклади KPIs для моніторингу СУІБ

KPI	**Одиниця виміру**	**Цільове значення**	**Джерело даних**
Кількість критичних інцидентів ІБ	Кількість	≤ 1 на місяць	Система управління інцидентами
Середній час на виявлення інциденту (MTTD)	Години	≤ 2 години	SIEM-система
Відсоток виявлених вразливостей високого ризику	%	≤ 5%	Звіт сканування вразливостей
Кількість несанкціонованих спроб доступу	Кількість	≤ 50 на день	Журнали аутентифікації

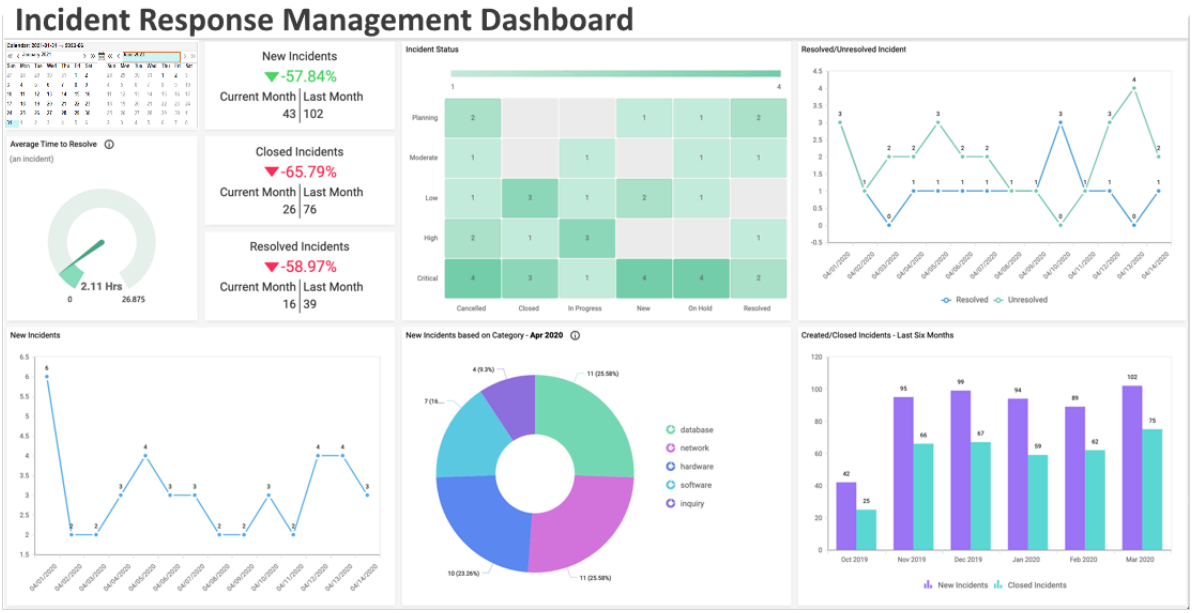

Рисунок Б.2. Приклад дашборду моніторингу СУІБ

Продовження додатку Б

Таблиця Б.17

Приклад структури Програми внутрішнього аудиту СУІБ

Розділ програми аудиту	**Опис**
Мета аудиту	Перевірка відповідності СУІБ вимогам ISO/IEC 27001 та внутрішнім політикам/процедурам.
Обсяг аудиту	Перелік процесів, підрозділів, систем, які будуть перевірятися.
Критерії аудиту	Застосовні вимоги стандарту (ISO/IEC 27001), внутрішні політики, процедури, законодавство.
Графік аудиту	Дати проведення аудитів, тривалість, розподіл за об'єктами перевірки (річний/квартальний план).
Команда аудиту	Склад команди внутрішніх аудиторів, їхня кваліфікація та відповідальність.

Таблиця Б.18

Приклад фрагменту Звіту про внутрішній аудит

Дата аудиту	**Об'єкт аудиту**	**Виявлена невідповідність**	**Посилання на вимогу**	**Рекомендація аудитора**
15.05.2025	Відділ розробки	Відсутня документована процедура керування змінами ПЗ.	ISO 27001:2022, 8.1	Розробити та впровадити процедуру керування змінами.

Продовження додатку Б

Продовження Таблиці Б.18

1	2	3	4	5
20.05.2025	IT-інфраструктура	Журнали доступу до критичних серверів не переглядаються регулярно.	Внутрішня Процедура моніторингу	Встановити регулярний графік перегляду журналів та відповідальних.

Таблиця Б.19

Приклад вхідних даних для аналізу СУІБ з боку керівництва

Категорія вхідних даних	**Приклад інформації**
Результати попередніх аналізів	Статус виконання рішень з минулих засідань.
Зміни у зовнішніх та внутрішніх факторах	Нові регуляторні вимоги, зміни в організаційній структурі.
Показники ефективності СУІБ (KPIs)	Динаміка кількості інцидентів, час реагування на інциденти.
Результати аудитів	Звіти внутрішніх та зовнішніх аудитів, виявлені невідповідності.
Зворотний зв'язок від зацікавлених сторін	Скани від клієнтів, пропозиції співробітників щодо ІБ.
Статус коригувальних дій	Прогрес усунення невідповідностей та їхня ефективність.
Можливості для постійного вдосконалення	Нові технології, покращення процесів.

Таблиця Б.20

Приклад фрагменту Протоколу засідання керівництва щодо аналізу СУІБ

Дата засідання	**Присутні (Ключові ролі)**	**Обговорені питання**	**Прийняті рішення**	**Відповідальний**	**Термін**
05.06.2025	Генеральний директор, Керівник СУІБ, Директор з ІТ	Результати внутрішнього аудиту (недоліки в управлінні доступом).	Затвердити план коригувальних дій для усунення невідповідностей.	Керівник СУІБ	30.06.2025
		Зростання кількості фішингових атак.	Ініціювати поглиблений тренінг з обізнаності для всіх співробітників.	HR-відділ	15.07.2025
		Необхідність перегляду політики використання хмарних сервісів.	Доручити Керівнику СУІБ розробити пропозиції щодо нової політики.	Керівник СУІБ	31.07.2025

Продовження додатку Б

Таблиця Б.21

Приклад фрагменту Реєстру невідповідностей

Ідентифікатор	**Дата виявлення**	**Джерело виявлення**	**Опис невідповідності**	**Першопричина**	**Заплановані коригувальні дії**	**Відповідальний**	**Термін**	**Статус**
НВ-001	15.05.2025	Внутрішній аудит	Відсутність актуальної політики використання мобільних пристроїв.	Політика не переглядалася після зміни законодавства (2024).	Оновити політику, довести до відома співробітників, провести навчання.	Керівник СУІБ	30.06.2025	В процесі
НВ-002	20.05.2025	Інцидент ІБ	Співробітник передав конфіденційну інформацію через незахищений канал.	Недостатня обізнаність щодо правил поводження з конфіденційною інформацією.	Провести обов'язковий додатковий тренінг для всіх співробітників з конфіденційності.	HR-відділ	15.07.2025	Відкрито

Продовження додатку Б

Продовження Таблиці Б.21

1	2	3	4	5	6	7	8	9
НВ-003	25.05.2025	Моніторингсистем	Антивірусне ПЗ на кількох робочих станціях не оновлюється.	Неналаштована автоматична функція оновлення.	Налаштувати автоматичне оновлення антивірусного ПЗ, провести перевірку.	ІТ-відділ	10.06.2025	Виконано

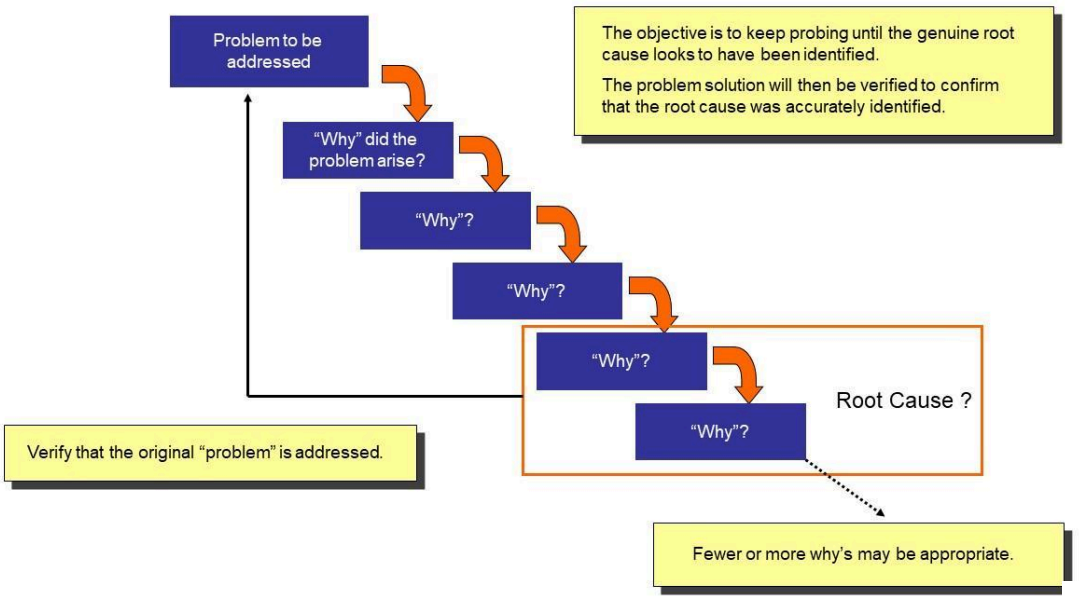

Рисунок Б.3. Діаграма "5 чому" (приклад аналізу першопричин)

Продовження додатку Б

Таблиця Б.22

Приклад Плану постійного вдосконалення СУІБ

Ідентифікатор покращення	**Джерело пропозиції**	**Опис покращення**	**Очікуваний результат**	**Відповідальний**	**Термін**	**Статус**
PI-001	Аналіз керівництва	Впровадження системи централізованого управління паролями.	Зниження ризику витоків через слабкі/спільні паролі.	IT-відділ	30.09.2025	Заплановано
PI-002	Звіт аудиту	Перегляд та оптимізація процесу реагування на інциденти ІБ.	Скорочення часу реагування (MTTR) на 20%.	Керівник СУІБ	31.10.2025	В процесі
PI-003	Зворотний зв'язок (HR)	Додати інтерактивні модулі до програми навчання з обізнаності.	Збільшення рівня обізнаності персоналу на 15%.	HR-відділ	31.01.2026	Відкрито
PI-004	Нові технології	Дослідження та пілотне впровадження системи DLP (Data Loss Prevention).	Запобігання несанкціонованому витоку конфіденційних даних.	Керівник СУІБ	30.06.2026	Заплановано