**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ПОЛІТИКИ ТА ПРОЦЕДУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЯХ ВІДПОВІДНО ДО МІЖНАРОДНИХ ВИМОГ”

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

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

_____ Анастасія ПЕТРЕНКО
*(підпис)* *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-42

Анастасія ПЕТРЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Діана Примаченко
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
Ім’я, ПРІЗВИЩЕ

**Київ 2025**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут кібербезпеки та захисту інформації**

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

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

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Петренко Анастасії Олександрівні
*(прізвище, ім’я, по батькові здобувача)*

1. Тема кваліфікаційної роботи “Політики та процедури інформаційної безпеки в організаціях відповідно до міжнародних вимог”,
   Керівник кваліфікаційної роботи Діана ПРИМАЧЕНКО,
   *(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)*

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

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека організацій,, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Дослідити проблеми забезпечення інформаційної безпеки в організаціях.
   4.2. Проаналізувати методи та засоби оцінки відповідності політик інформаційної безпеки міжнародним вимогам.
   4.3. Розробити рекомендації щодо вдосконалення політик та процедур інформаційної безпеки.

*5.* Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2025 р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Етапи кваліфікаційної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Визначення об’єкту, предмету, мети та завдань дослідження. | 18.03.2025 | |
| 2. | Збір та аналіз літератури. | 29.03.2025 | |
| 3. | Дослідження міжнародних вимог до політик та процедур інформаційної безпеки | 08.04.2025 | |
| 4. | Аналіз існуючих політик безпеки в організаціях | 22.04.2025 | |
| 5. | Оцінка відповідності політик міжнародним стандартам та виявлення недоліків | 08.05.2025 | |
| 6. | Формування рекомендацій щодо вдосконалення політик інформаційної безпеки | 20.05.2025 | |
| 7. | Оформлення роботи. | 22.05.2025 | |
| 8. | Оформлення презентації. | 03.06.2025 | |
| 9. | Отримання рецензії на роботу. | 03.06.2025 | |
| 10. | Захист в ЕК. | __.06.2025 | |

Здобувачка вищої освіти _____ Анастасія ПЕТРЕНКО
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Петренко А.О. до захисту кваліфікаційної роботи
*(прізвище та ініціали)*
за спеціальністю 125 Кібербезпека
*(код, найменування спеціальності)*
освітньої програми Управління інформаційною та кібернетичною безпекою
*(назва)*
на тему: "Політики та процедури інформаційної безпеки в організаціях відповідно до міжнародних вимог"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**Висновок керівника кваліфікаційної роботи**

Здобувач ПЕТРЕНКО Анастасія у кваліфікаційній роботі дослідила відповідність політик та процедур інформаційної безпеки в організаціях міжнародним стандартам, У роботі проаналізовано сучасні підходи до побудови систем інформаційної безпеки, виявлено ключові проблеми реалізації політик безпеки, серед яких – недостатня обізнаність персоналу, слабкий моніторинг інцидентів та відсутність чіткої відповідальності за дотримання вимог безпеки.

ПЕТРЕНКО Анастасія продемонструвала ґрунтовне розуміння тематики, володіння теоретичними знаннями та практичними навичками щодо оцінки відповідності політик інформаційної безпеки міжнародним вимогам, застосувала системний і науковий підхід до вирішення поставлених завдань. Результати проведеного дослідження були апробовані на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», що підтверджує актуальність і практичну значущість отриманих результатів.

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

Керівник кваліфікаційної роботи _____ Діана Примаченко
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута. Здобувач Петренко А.О. допускається до захисту даної роботи в Екзаменаційній комісії.

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

**ВІДГУК РЕЦЕНЗЕНТА**
**на кваліфікаційну бакалаврську роботу**

здобувача вищої освіти ПЕТРЕНКО Анастасія
на тему “Політики та процедури інформаційної безпеки в організаціях відповідно до міжнародних вимог”

**Актуальність.** У сучасних умовах цифрової трансформації, коли компанії активно впроваджують інформаційні технології в бізнес-процеси, питання забезпечення належного рівня інформаційної безпеки набуває особливої ваги. Одним із ключових елементів цього процесу є наявність формалізованих політик та процедур інформаційної безпеки, які відповідають міжнародним стандартам та регламентам. Недотримання таких вимог може призвести до витоку конфіденційної інформації, юридичних санкцій, зниження довіри клієнтів та партнерів. З огляду на це, дослідження проблематики оцінки відповідності політик і процедур інформаційної безпеки організацій міжнародним стандартам (ISO/IEC 27001, NIST CSF, GDPR, COBIT, PCI DSS), а також розробка рекомендацій щодо їх удосконалення є актуальним і важливим як з наукової, так і з практичної точки зору.

**Позитивні сторони.**

1. У кваліфікаційній роботі здійснено всебічний аналіз сучасних міжнародних стандартів у сфері інформаційної безпеки та оцінено їх вплив на побудову політик і процедур захисту інформації в організаціях.
2. Робота відзначається чіткою структурою, послідовністю викладу матеріалу, логічністю побудови розділів та обґрунтованістю висновків.
3. У результаті дослідження запропоновано конкретні рекомендації щодо вдосконалення політик та процедур інформаційної безпеки в організаціях, що дозволяє адаптувати міжнародні підходи до потреб українських компаній та підвищити ефективність систем управління безпекою.

**Недоліки.**

Доцільним було б провести ширшу апробацію запропонованих рекомендацій, наприклад, через впровадження кейс-стаді або експериментальну перевірку на прикладі конкретної організації. Це дозволило б наочно продемонструвати ефективність підходів у реальних умовах експлуатації та підсилити практичну цінність отриманих результатів.

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

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

Рецензент: _____ _____
*підпис* Ім’я, ПРІЗВИЩЕ

# РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню відповідності політик і процедур інформаційної безпеки в організаціях міжнародним вимогам, аналізу можливих невідповідностей та розробці рекомендацій щодо їх вдосконалення. Робота складається зі вступу, трьох розділів, що містять 7 рисунків, висновків і списку використаних джерел із 59 найменувань. Загальний обсяг роботи становить 57 аркушів, з яких 4 аркуші займають перелік умовних скорочень та список використаних джерел.

***Метою роботи*** є дослідження та оцінка відповідності політик і процедур інформаційної безпеки в організаціях міжнародним стандартам.

***Об'єктом дослідження*** є політики та процедури інформаційної безпеки, що використовуються в організаціях.

***Предмет дослідження –*** процеси та механізми впровадження політик і процедур інформаційної безпеки в організаціях.

***Методи дослідження.*** Для вирішення означеного вище наукового завдання в роботі використані методи: аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до оцінки відповідності політик і процедур інформаційної безпеки міжнародним стандартам.

Проаналізовано особливості політик і процедур інформаційної безпеки в організаціях, досліджено основні вимоги міжнародних стандартів щодо їх розробки та впровадження, оцінено рівень їхньої ефективності та розроблено практичні рекомендації щодо вдосконалення політик і процедур.

***Галузь застосування.*** Розроблені підходи можуть бути використані при оцінці відповідності політик і процедур інформаційної безпеки організацій міжнародним стандартам, а також для вдосконалення процесів управління інформаційною безпекою.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИКИ БЕЗПЕКИ, ПРОЦЕДУРИ БЕЗПЕКИ, МІЖНАРОДНІ СТАНДАРТИ, РИЗИК-МЕНЕДЖМЕНТ, АУДИТ БЕЗПЕКИ, ІНФОРМАЦІЙНІ ЗАГРОЗИ

# ABSTRACT

The qualification thesis is dedicated to the study of the compliance of information security policies and procedures in organizations with international requirements, the analysis of potential inconsistencies, and the development of recommendations for their improvement.

The work consists of an introduction, three chapters containing 7 figures, conclusions, and a list of 59 references. The total volume of the thesis is 57 pages, 4 of which are occupied by the list of abbreviations and the list of references.

**The aim of the thesis** is to study and evaluate the compliance of information security policies and procedures in organizations with international standards.

**The object of the research** is the information security policies and procedures used in organizations.

**The subject of the research** is the processes and mechanisms for implementing information security policies and procedures in organizations.

**Research methods.** To solve the outlined scientific task, the following methods were used: analysis and synthesis, comparison, classification, expert evaluation, and a systematic approach to assessing the compliance of information security policies and procedures with international standards.

The features of information security policies and procedures in organizations were analyzed, the main requirements of international standards for their development and implementation were studied, their effectiveness was assessed, and practical recommendations for improving these policies and procedures were developed.

**Field of application.** The developed approaches can be used to assess the compliance of organizational information security policies and procedures with international standards, as well as to improve information security management processes.



Keywords: INFORMATION SECURITY, SECURITY POLICIES, SECURITY PROCEDURES, INTERNATIONAL STANDARDS, RISK MANAGEMENT, SECURITY AUDIT, INFORMATION THREATS

**ЗМІСТ**

# ВСТУП

*Актуальність дослідження.* У сучасному цифровому світі інформація є важливим ресурсом для будь-якої організації. Збільшення обсягів даних, активне впровадження хмарних технологій, віддаленої роботи та автоматизованих систем управління створюють нові виклики у сфері інформаційної безпеки. Несанкціонований доступ, витік конфіденційної інформації, кібератаки та внутрішні загрози можуть призвести до значних фінансових втрат, правових наслідків та втрати довіри з боку клієнтів і партнерів.

Багато організацій запроваджують політики та процедури інформаційної безпеки, однак їх ефективність та відповідність сучасним загрозам не завжди є достатньо високими. Причинами цього можуть бути застарілі методи захисту, недостатня обізнаність персоналу, відсутність чітко регламентованих заходів безпеки або недотримання найкращих практик. Особливо це стосується підприємств малого та середнього бізнесу, де питання інформаційної безпеки часто не є пріоритетним через обмежені фінансові та технічні ресурси.

З огляду на зазначене дослідження відповідності політик і процедур інформаційної безпеки в організаціях є актуальним науковим завданням.

***Мета роботи*** полягає у дослідженні відповідності політик і процедур інформаційної безпеки в організаціях міжнародним стандартам.

***Об'єкт дослідження –*** політики та процедури інформаційної безпеки, що використовуються в організаціях.

***Предмет дослідження*** – процеси та механізми впровадження політик і процедур інформаційної безпеки в організаціях.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Проаналізувати особливості управління інформаційною безпекою в організаціях.
2. Дослідити основні вимоги міжнародних стандартів до політик і процедур інформаційної безпеки.
3. Виявити можливі невідповідності між чинними політиками та

процедурами інформаційної безпеки в організаціях і міжнародними вимогами.

4. Розробити рекомендації щодо вдосконалення політик і процедур інформаційної безпеки для забезпечення їх відповідності міжнародним стандартам.

**Методи дослідження.** Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, а також системного підходу до оцінки відповідності політик і процедур інформаційної безпеки міжнародним стандартам.

**Практичне значення одержаних результатів.** Застосування напрацювань дасть змогу організаціям здійснювати обґрунтований аналіз і вдосконалення політик та процедур інформаційної безпеки відповідно до міжнародних вимог, що сприятиме підвищенню рівня захисту інформаційних ресурсів та мінімізації ризиків порушення безпеки даних.

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

# РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЯХ

## 1.1 Визначення та основні складові інформаційної безпеки

Інформаційна безпека – це стан захищеності інформації та інфраструктури, що забезпечує її конфіденційність, цілісність і доступність. Вона спрямована на запобігання несанкціонованому доступу, використанню, розголошенню, модифікації чи знищенню інформації, а також на захист інформаційних систем від загроз, зловмисних атак, збоїв та інших ризиків.

Основні принципи інформаційної безпеки включають три ключові складові: конфіденційність, цілісність та доступність, вони відомі також під абревіатурою CIA (Confidentiality, Integrity, Availability) (рис. 3.1).

Confidentiality – забезпечує, що доступ до інформації мають лише уповноважені особи або системи. Це допомагає запобігти несанкціонованому розголошенню даних.

Integrity – забезпечує, що дані залишаються точними та не змінюються або не пошкоджуються без дозволу. Це важливо для збереження достовірності та надійності інформації.

Availability – гарантує, що інформація та ресурси доступні для використання у потрібний час уповноваженим користувачам. Вона також стосується безперервності роботи систем і швидкого відновлення після збоїв.

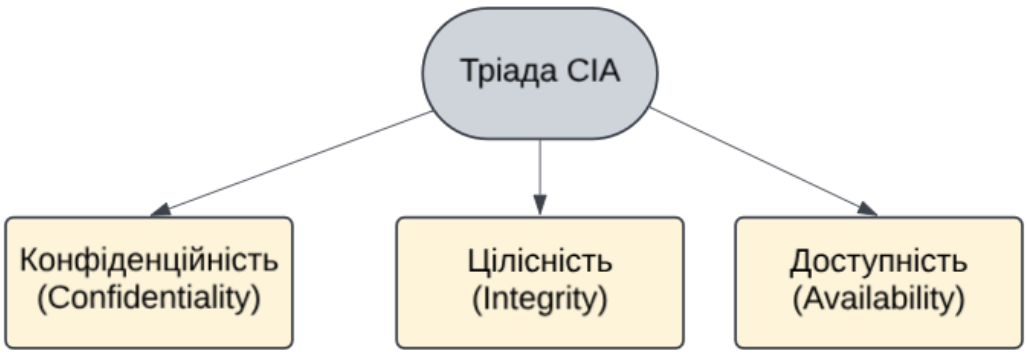


Рис. 1.1. Тріада CIA

Управління безпекою – це комплекс заходів, спрямованих на захист інформації, інфраструктури та ресурсів організації. Існує кілька основних підходів до управління безпекою, кожен з яких має свої методи та цілі.

Проактивний підхід спрямований на попередження загроз до їх виникнення. Основний принцип цього підходу – аналіз можливих ризиків і впровадження заходів, що мінімізують їхній вплив. Серед ключових методів можна виділити аудит безпеки, оцінку ризиків, розробку політик захисту, а також використання таких інструментів, як шифрування та резервне копіювання даних.

Реактивний підхід – передбачає виявлення та ліквідацію загроз після їхнього виникнення. Він зосереджений на швидкому реагуванні на інциденти та мінімізації їхніх наслідків. Основні методи включають системи моніторингу, виявлення вторгнень, аналіз логів, оновлення програмного забезпечення та використання антивірусного захисту.

Регуляторний підхід базується на дотриманні законодавчих норм, міжнародних стандартів та внутрішніх політик безпеки. Це включає відповідність таким стандартам, як ISO/IEC 27001, GDPR, NIST, а також створення внутрішніх нормативних документів, що регулюють безпеку даних і контроль за їх дотриманням.

Технічний підхід фокусується на впровадженні сучасних технологій для захисту інформаційних систем. Це включає використання брандмауерів, систем багатофакторної автентифікації, управління правами доступу, мережевої сегментації, а також технологій шифрування та резервного копіювання.

Організаційний підхід спрямований на управління людським фактором та організацію ефективної системи безпеки в компанії. Він передбачає навчання персоналу, контроль за дотриманням правил безпеки, розмежування прав доступу до ресурсів, а також розробку планів дій у разі виникнення надзвичайних ситуацій.

Ефективне управління безпекою базується на поєднанні всіх зазначених підходів. Проактивні заходи дозволяють запобігти ризикам, реактивні – швидко

реагувати на загрози, регуляторний підхід забезпечує відповідність стандартам, технічні методи захищають системи, а організаційні заходи допомагають мінімізувати людський фактор. Разом ці підходи формують комплексну систему безпеки, яка забезпечує надійний захист інформації та інфраструктури.

## 1.2 Міжнародні стандарти та нормативно-правові акти у сфері інформаційної безпеки

Захист інформації в сучасних організаціях неможливий без системного підходу, що включає дотримання міжнародних стандартів, нормативно-правових вимог і внутрішньої регламентації. В умовах глобалізації, швидкого розвитку інформаційних технологій та зростання кіберзагроз усе більшої актуальності набуває правова та стандартизаційна основа інформаційної безпеки.

Міжнародні стандарти інформаційної безпеки — це офіційно затверджені документи, розроблені авторитетними міжнародними організаціями (наприклад, ISO, NIST, IETF), які встановлюють загальні вимоги, принципи та підходи до захисту інформації, управління ризиками та забезпечення стійкості інформаційних систем. Їхнє головне призначення — уніфікувати правила захисту даних у різних країнах і галузях, сприяти юридичній відповідності, підтримувати надійність та взаємодію в глобальному цифровому середовищі.

Запровадження міжнародних стандартів дозволяє:

– підвищити загальний рівень кібербезпеки;

– забезпечити правову та регуляторну відповідність;

– спростити аудит і сертифікацію безпеки;

– формувати довіру між організаціями, особливо у сфері електронної комерції, фінансів, медицини та державного управління.

У більшості випадків саме ці стандарти стають базою для розробки внутрішніх політик інформаційної безпеки, адаптованих до конкретних умов і потреб організації.

Окрім стандартів, важливим фактором є юридичні норми, які регулюють обробку, зберігання та передачу інформації. Законодавство в галузі інформаційної безпеки часто вимагає дотримання певних процедур і встановлює відповідальність за порушення. Йдеться як про міжнародні регламенти (наприклад, у ЄС чи США), так і про національні закони, які передбачають захист персональних даних, обов'язкове повідомлення про інциденти, аудит безпеки тощо.

Організації, що ігнорують ці вимоги, можуть зазнати фінансових санкцій, втрат репутації або юридичної відповідальності. Саме тому дотримання правових вимог – не лише питання формальності, а ключовий елемент управління ризиками.

Політики інформаційної безпеки – це внутрішні документи, які формалізують підходи до захисту даних, встановлюють правила поведінки працівників, визначають процедури доступу, моніторингу, реагування на інциденти тощо. Вони базуються на вимогах міжнародних стандартів і правових норм, але при цьому враховують специфіку кожної організації.

Основні функції політик:

– регламентування доступу – хто, коли і до чого має право доступу.

– захист даних – способи збереження цілісності, конфіденційності, доступності.

– моніторинг та аудит – контроль за виконанням заходів безпеки.

– реагування на інциденти – визначення чітких алгоритмів дій.

– навчання персоналу – інструктажі, тестування, підвищення обізнаності.

Політики мають бути чітко структуровані, затверджені керівництвом, регулярно оновлювані та доведені до всіх працівників. Наявність таких документів дозволяє зробити систему безпеки прозорою та керованою.

Політики інформаційної безпеки сприяють захисту даних та інформаційних систем організації, встановлюючи правила та регламентуючи заходи, які допомагають забезпечити конфіденційність, цілісність і доступність

інформації. Вони дозволяють зменшити ризики витоку даних, запобігти кібератакам і забезпечити відповідність стандартам безпеки.

Один із напрямів, який охоплюють політики – конфіденційність інформації. Вони визначають рівні доступу до даних, регулюють автентифікацію користувачів і передбачають використання шифрування. Це обмежує доступ до інформації лише для уповноважених осіб і зменшує ймовірність її потрапляння до сторонніх осіб.

Політики також допомагають підтримувати цілісність даних, тобто запобігати несанкціонованим змінам або пошкодженню інформації. Для цього передбачаються механізми контролю змін, цифрові підписи та хешування. Такі заходи застосовуються, наприклад, у фінансових та державних установах, де необхідно зберігати точність інформації.

Ще один аспект політик – доступність інформації. Вони регулюють резервне копіювання, використання систем захисту від атак, що можуть перешкоджати доступу до даних, а також відмовостійкі рішення. Це зменшує ризики втрати інформації через технічні збої або зловмисні дії.

Окрім цього, політики визначають правила використання інформаційних ресурсів працівниками. Вони встановлюють порядок роботи з корпоративними даними, визначають обмеження щодо доступу до них, а також передбачають навчання персоналу. Це допомагає уникати порушень безпеки через людські помилки або несанкціоновані дії.

Також політики можуть бути пов’язані з виконанням вимог законодавства. У багатьох сферах існують стандарти та нормативні акти, які регулюють зберігання та обробку даних, наприклад, ISO/IEC 27001 або GDPR. Дотримання встановлених правил допомагає організаціям уникати штрафів та юридичних ризиків.

Загалом, політики безпеки формують систему заходів, що дозволяє впорядкувати захист інформації. Вони встановлюють чіткі правила доступу, використання й обробки даних, що знижує ризики загроз та забезпечує стабільну роботу інформаційних систем.

Політики інформаційної безпеки охоплюють різні аспекти захисту даних і регулюють правила використання інформаційних ресурсів. Вони допомагають організаціям мінімізувати ризики, запобігати загрозам і забезпечувати стабільність роботи інформаційних систем (рис. 1.2).

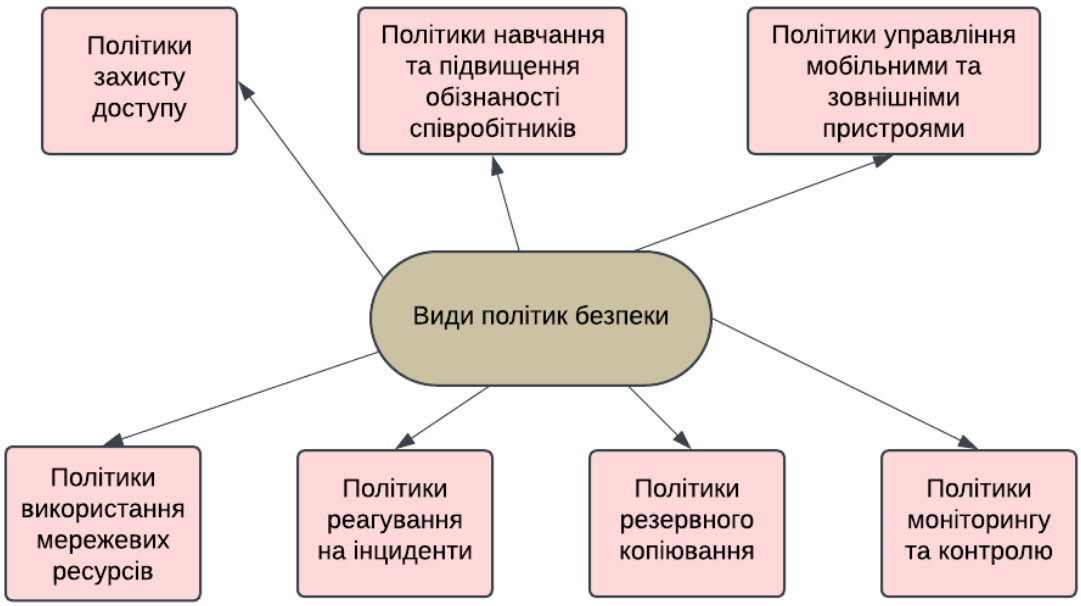


Рис. 1.2. Основні види політик безпеки.

Впровадження комплексних політик безпеки дозволяє організаціям мінімізувати ризики, пов’язані із загрозами в інформаційному середовищі. Вони регулюють управління доступом, моніторинг активності, використання мереж та мобільних пристроїв, а також резервне копіювання й реагування на інциденти. Дотримання цих політик сприяє стабільності роботи інформаційних систем та підвищенню загального рівня кібербезпеки.

## 1.3 Роль політик і процедур в забезпеченні інформаційної безпеки організацій

Сучасні організації стикаються з численними загрозами інформаційної безпеки, які можуть призвести до фінансових втрат, витоку конфіденційних даних, зупинки бізнес-процесів та репутаційних ризиків. Найпоширеніші кібератаки показані на рисунку 1.3.

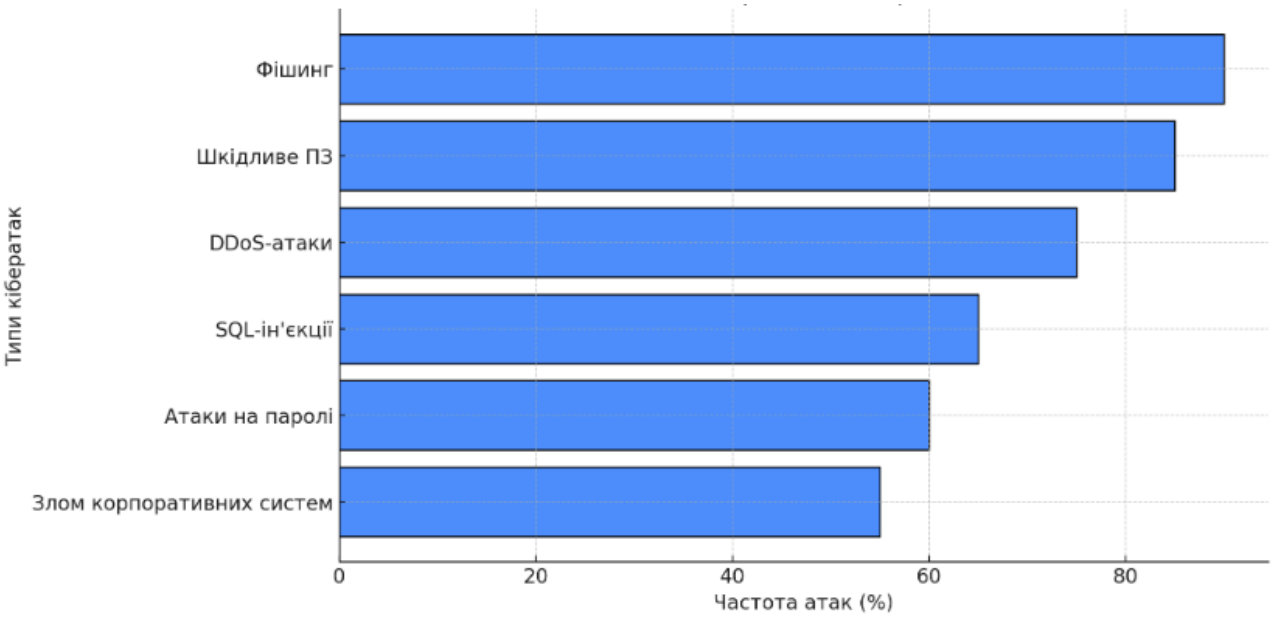


Рис. 1.3. Найпоширеніші кібератаки

Інформаційна безпека в організації не може ґрунтуватися виключно на технічних засобах. Вона потребує системного управління, в основі якого лежать формалізовані політики та процедури. Саме вони визначають правила, відповідальність і порядок дій усіх учасників інформаційного середовища.

Однією з функцій політик є запобігання загрозам до їх реалізації. Наприклад, чітко прописані вимоги до автентифікації та мінімізації доступу значно знижують ризик внутрішнього витоку даних або несанкціонованого проникнення в систему. Політика резервного копіювання дозволяє оперативно відновити інформацію після збоїв або атак програм-вимагачів. Таким чином, політики не лише регулюють поведінку користувачів, а й забезпечують стійкість організації до інцидентів.

Політики задають загальні правила, а процедури деталізують їх виконання. Наприклад, якщо політика вимагає реагування на інциденти, то процедура визначає, хто саме, в які строки, за яким алгоритмом має діяти. Це дозволяє:

– уникати паніки в критичних ситуаціях;
– пришвидшити локалізацію інцидентів;
– мінімізувати втрати.

Недостатнє або відсутність забезпечення ІБ для будь-якої організації, можуть призвести до серйозних фінансових, юридичних та репутаційних втрат.

У табл. 1.1 наведено основні слабкі місця в системах безпеки організацій та можливі наслідки їхньої експлуатації зловмисниками.

Таблиця 1.1.

Вразливості організацій та їхні наслідки

| Вразливості організацій | Наслідки недостатньої інформаційної безпеки |
|---|---|
| Слабкі паролі та відсутність багатофакторної автентифікації | Компрометація облікових записів та витік паролів |
| Недостатнє навчання персоналу з питань кібербезпеки | Фінансові втрати через кібератаки та шахрайство |
| Використання застарілого програмного забезпечення | Збої у роботі інформаційних систем через шкідливе ПЗ |
| Недостатній контроль доступу до критичних даних | Несанкціонований доступ до конфіденційних даних |
| Відсутність регулярного аудиту безпеки | Юридична відповідальність за порушення регламентів (GDPR, ISO 27001) |
| Наявність уразливостей у веб-додатках та мережевій інфраструктурі | Втрати репутації та довіри клієнтів |
| Відсутність ефективної політики резервного копіювання | Недоступність критичних систем через DDoS-атаки |
| Низький рівень моніторингу та виявлення загроз | Компрометація корпоративних даних та промислове шпигунство |
| Використання незахищених хмарних сервісів | Втрата або знищення важливої інформації через відсутність бекапів |

Продовження таблиці 1.1.

| | |
|---|---|
| Соціальна інженерія та відсутність захисту від фішингу | Використання корпоративної інфраструктури для проведення атак |
| Ненадійні постачальники IT-послуг та відсутність контролю | Порушення безперервності бізнес-процесів та зупинка роботи |
| Відсутність плану реагування на інциденти | Витік персональних даних клієнтів та можливі штрафи |
| Недостатній захист мобільних пристроїв та BYOD-політики | Використання корпоративних серверів для розповсюдження вірусів |
| Використання неліцензійного програмного забезпечення | Маніпуляція або підміна фінансових транзакцій |
| Недостатній захист IoT-пристроїв у корпоративній мережі | Втрата конкурентних переваг через витік конфіденційної інформації |
| Наявність занадто великої кількості привілеїв у співробітників | Можливість внутрішнього саботажу та шкідливих дій співробітників |
| Недостатня сегментація мережі та слабкі міжмережеві екрани | Втрата критичних бізнес-даних через атаки програм-вимагачів |
| Відсутність політики оновлення програмного забезпечення | Ризик юридичних наслідків через недостатній захист клієнтських даних |
| Відсутність шифрування конфіденційних даних | Масові фішингові атаки на співробітників компанії |
| Погано налаштовані права доступу до файлових серверів | Зниження ефективності роботи через численні інциденти безпеки |

**Висновки до розділу 1**

Розглянуто основні теоретичні аспекти інформаційної безпеки в організаціях, які є ключовими для забезпечення захисту інформаційних ресурсів.

Розгляд основних понять та принципів інформаційної безпеки показав, що безпека даних ґрунтується на тріаді конфіденційність, цілісність і доступність (CIA). Ці принципи визначають основні вимоги до захисту інформації та є фундаментальними для будь-якої системи кібербезпеки.

Аналіз політик та процедур інформаційної безпеки продемонстрував, що

ефективне управління безпекою в організації неможливе без чітко визначених правил і процедур. Політики безпеки регулюють доступ до ресурсів, методи шифрування, правила автентифікації користувачів, а також порядок моніторингу і реагування на інциденти. Структуровані та впроваджені відповідно до міжнародних стандартів (наприклад, ISO/IEC 27001), вони дозволяють значно знизити рівень загроз.

У рамках дослідження ризиків та загроз інформаційної безпеки було виявлено, що сучасні організації стикаються як із зовнішніми, так і внутрішніми загрозами. Основними викликами є кібератаки (фішинг, шкідливе ПЗ, DDoS-атаки, злом паролів, SQL-ін'єкції), витоки даних (ненавмисні та зловмисні) та внутрішні загрози (недотримання політик, соціальна інженерія, зловживання доступом). Виявлено, що зниження цих ризиків можливе лише за умови комплексного підходу, який поєднує технічні, організаційні та адміністративні заходи.

Таким чином, результати цього розділу підтвердили важливість системного підходу до забезпечення інформаційної безпеки. Використання міжнародних стандартів, ефективних політик безпеки, сучасних технологій захисту та підвищення обізнаності персоналу є ключовими факторами для створення надійної системи кібербезпеки в організації.

# РОЗДІЛ 2 АНАЛІЗ СУЧАСНИХ МІЖНАРОДНИХ ВИМОГ ДО ПОЛІТИК ТА ПРОЦЕДУР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1 Огляд основних міжнародних стандартів (ISO/IEC 27001, NIST, COBIT та ін.)

Міжнародні стандарти інформаційної безпеки встановлюють вимоги до захисту даних, управління ризиками та розробки ефективних заходів безпеки в організаціях. Вони допомагають структурувати політики та процедури безпеки відповідно до кращих світових практик, що мінімізує потенційні загрози та забезпечує відповідність правовим нормам (табл. 2.1).

ISO/IEC 27001 – міжнародний стандарт для системи управління інформаційною безпекою (СУІБ), розроблений Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Він визначає вимоги до встановлення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою.

Основні вимоги

– контекст організації – визначення внутрішніх та зовнішніх факторів, що впливають на безпеку інформації;

– лідерство – керівництво повинно бути залучене у процес управління інформаційною безпекою;

– планування – виявлення ризиків та можливостей, встановлення цілей;

– підтримка – забезпечення ресурсами, кваліфікацією персоналу, комунікацією та документуванням;

– операційна діяльність – реалізація політики безпеки, управління ризиками, впровадження контролів безпеки;

– оцінка ефективності – моніторинг, вимірювання, аналіз та аудит безпеки;

– постійне покращення – впровадження коригувальних дій і підвищення ефективності СУІБ.

National Institute of Standards and Technology (NIST) – це набір стандартів та рекомендацій, розроблених Національним інститутом стандартів і технологій США для кібербезпеки. Найвідоміший документ – NIST Cybersecurity Framework (CSF).

Основні вимоги:

– Identify (Ідентифікація) – визначення активів, ризиків, загроз та нормативних вимог;

– Protect (Захист) – впровадження засобів контролю для обмеження або зменшення впливу кіберзагроз;

– Detect (Виявлення) – моніторинг системи для виявлення атак або аномальної поведінки;

– Respond (Реагування) – заходи реагування на інциденти, включаючи аналіз та повідомлення про порушення;

– Recover (Відновлення) – процеси для відновлення операцій після інциденту.

General Data Protection Regulation (GDPR) – загальний регламент захисту даних ЄС, який встановлює суворі правила обробки персональних даних громадян Європейського Союзу.

Основні вимоги

– законність обробки – дані можуть оброблятися лише на законних підставах (згода, договір, законні інтереси);

– принципи захисту даних – мінімізація даних, обмеження цілей, прозорість, точність, конфіденційність;

– права суб'єктів даних – право на доступ, виправлення, видалення, обмеження обробки та перенесення даних;

– безпека обробки – впровадження технічних і організаційних заходів для захисту даних;

– оповіщення про витік даних – компанії повинні повідомляти органи нагляду про порушення протягом 72 годин;

– офіцер із захисту даних (DPO) – необхідний для організацій, які широко обробляють персональні дані.

Control Objectives for Information and Related Technologies (COBIT) – це фреймворк управління IT-безпекою, який допомагає організаціям відповідати регуляторним вимогам.

Основні вимоги

– управління IT-процесами для підтримки стратегічних цілей;

– оцінка ризиків та відповідність нормативним вимогам;

– контроль доступу до IT-систем;

– забезпечення ефективного управління IT-ресурсами.

Таблиця 2.1.

Порівняльна характеристика міжнародних стандартів щодо політик і процедур інформаційної безпеки

| **Стандарт** | **Основний фокус стандарту** | **Вимоги до політик ІБ** | **Особливості для організацій** | **Рекомендовано для** |
|---|---|---|---|---|
| ISO/IEC 27001 | Система управління інформаційною безпекою (СУІБ) | Формалізація політик ІБ, управління ризиками, безперервне вдосконалення процесів | Вимагає чіткої структури документів: політика доступу, резервного копіювання, реагування на інциденти | Організації всіх розмірів, особливо середній та великий бізнес |
| NIST CSF | Рамкова модель кібербезпеки | Описує необхідність політик на етапах Identify, Protect, Detect, Respond, Recover | Гнучкий фреймворк для адаптації під потреби бізнесу США та міжнародного ринку | Критична інфраструктура, великі компанії, державний сектор США |

Продовження таблиці 2.1

| | | | | |
|---|---|---|---|---|
| COBIT 2019 | Управління IT-процесами | Фокус на політиках контролю доступу, відповідальності, моніторингу й аудиту | Підкреслює відповідальність керівництва та управління ризиками в IT | IT-компанії, фінансовий сектор, великі корпорації |
| GDPR | Захист персональних даних громадян ЄС | Визначає політики щодо згоди на обробку даних, права суб'єктів, оповіщення про витік | Особлива увага до персональних даних і процедур обробки | Організації, які обробляють персональні дані громадян ЄС |
| PCI DSS | Захист платіжних карткових даних | Політики автентифікації, шифрування, контроль доступу до систем із платіжними даними | Жорсткі вимоги до захисту карткових систем, регулярний аудит | Банки, фінансові установи, e-commerce |

## 2.2 Адаптація міжнародних вимог до національних та корпоративних стандартів

Оцінка відповідності політик інформаційної безпеки встановленим стандартам, таким як ISO/IEC 27001, NIST, GDPR, PCI DSS, здійснюється через декілька ключових методів. Насамперед використовується аудит інформаційної безпеки, який може бути внутрішнім або зовнішнім. Внутрішній аудит проводиться співробітниками організації або залученими експертами для перевірки відповідності політик та процесів внутрішнім вимогам та стандартам. Зовнішній аудит виконується незалежними сертифікаційними органами для офіційного підтвердження відповідності.

Оцінка ризиків, передбачає аналіз активів, вразливостей та потенційних загроз, що можуть вплинути на безпеку організації. Це дозволяє визначити пріоритетні заходи для мінімізації ризиків. Додатково застосовується геп-аналіз (Gap Analysis), який допомагає виявити невідповідності між поточним станом інформаційної безпеки та вимогами стандартів, а також окреслити шляхи для їх

усунення.

Тестування та моніторинг, які включають регулярне сканування вразливостей, проведення етичного хакінгу (penetration testing), а також моніторинг систем з метою виявлення підозрілої активності. Крім того, для відповідності стандартам проводиться оцінка відповідності законодавчим нормам, наприклад, перевірка виконання вимог щодо захисту персональних даних у відповідності до GDPR або вимог до фінансових операцій згідно з PCI DSS.

Приклади реальних політик безпеки та їх відповідність стандартам:

*Приклад 1.* Політика управління доступом (Access Control Policy), визначає правила контролю доступу до інформаційних систем та ресурсів організації.

Основні положення:

- використання принципу мінімальних привілеїв (Least Privilege);
- використання мультифакторної аутентифікації (MFA);
- регулярний перегляд та оновлення списків доступу;
- впровадження ролей користувачів (RBAC).

Аналіз відповідності політики представлений в табл. 2.2.

Таблиця 2.2.

Аналіз відповідності Access Control Policy

| Стандарт | Відповідність |
|---|---|
| ISO/IEC 27001 | Відповідає вимогам контролю доступу (A.9.1 – A.9.4). |
| NIST CSF | Відповідає категорії Protect (PR.AC). |
| GDPR | Частково відповідає, якщо політика враховує принципи конфіденційності (ст. 25 GDPR). |
| PCI DSS | Відповідає вимогам PCI DSS 8.1–8.8 (аутентифікація та контроль доступу). |

Якщо організація використовує лише парольний захист без MFA, вона може не відповідати вимогам PCI DSS та NIST CSF. Також потрібно впроваджувати аудит доступу для відповідності ISO/IEC 27001.

*Приклад 2.* Політика резервного копіювання (Backup Policy), визначає правила збереження та відновлення даних організації для запобігання втраті критичної інформації.

Основні положення:

– регулярне автоматизоване резервне копіювання;

– зберігання резервних копій у захищених локаціях;

– шифрування резервних копій;

– регулярне тестування відновлення даних.

Аналіз відповідності політики представлений в табл. 2.3.

Таблиця 2.3.

Аналіз відповідності Backup Policy

| Стандарт | Відповідність |
|---|---|
| ISO/IEC 27001 | Відповідає вимогам A.12.3 (управління резервними копіями). |
| NIST CSF | Відповідає категорії Recover (RC.RP). |
| GDPR | Відповідає ст. 32 (безпека обробки персональних даних). |
| PCI DSS | Частково відповідає, необхідно забезпечити безпеку резервних копій карткових даних. |

Якщо резервні копії не шифруються або не тестується їх відновлення, організація не відповідатиме ISO/IEC 27001 та NIST CSF. Для відповідності PCI DSS необхідно застосувати спеціальні заходи захисту карткових даних.

*Приклад 3.* Політика інцидент-менеджменту (Incident Response Policy), визначає процедури виявлення, реагування та усунення загроз інформаційної безпеки в організації.

Основні положення:

– визначення та класифікація інцидентів безпеки;

– процедура реагування на інциденти та повідомлення про них;

– навчання персоналу щодо кіберзагроз;

– проведення форензичного аналізу після інциденту.

Аналіз відповідності політики представлений в табл. 2.3.

Таблиця 2.3.

Аналіз відповідності Incident Response Policy

| Стандарт | Відповідність |
|---|---|
| ISO/IEC 27001 | Відповідає вимогам A.16 (управління інцидентами). |

Продовження таблиці 2.3.

| | |
|---|---|
| NIST CSF | Відповідає категорії Respond (RS.RP, RS.CO, RS.AN). |
| GDPR | Відповідає ст. 33 (повідомлення про витік даних у 72 години). |
| PCI DSS | Відповідає вимогам 12.10 (план реагування на інциденти). |

Якщо в організації відсутня формальна процедура реагування на інциденти або немає плану навчання персоналу, вона не відповідатиме жодному з перерахованих стандартів.

Оцінка відповідності політик інформаційної безпеки міжнародним стандартам є важливим процесом для забезпечення належного рівня захисту інформаційних активів організації. Використання таких методів, як аудит безпеки, аналіз ризиків, геп-аналіз та моніторинг загроз, дозволяє виявити слабкі місця та визначити шляхи їх усунення.

На прикладі політик управління доступом, резервного копіювання та інцидент-менеджменту було продемонстровано, що відповідність вимогам таких стандартів, як ISO/IEC 27001, NIST CSF, GDPR та PCI DSS, вимагає комплексного підходу. Недостатнє впровадження заходів безпеки, таких як мультифакторна аутентифікація, шифрування резервних копій чи формалізоване управління інцидентами, може призвести до невідповідності вимогам регуляторів та підвищеного рівня ризику для організації.

Таким чином, для забезпечення ефективної ІБ компанії необхідно регулярно переглядати політики безпеки, адаптувати їх до сучасних загроз, навчати персонал та проводити аудити відповідності. При умові використання комплексного та системного підхіду до управління безпекою дозволить організації відповідати міжнародним стандартам та забезпечити захист критично важливої інформації.

## 2.3 Порівняння підходів до управління інформаційною безпекою в різних країнах

Під час аналізу відповідності політик інформаційної безпеки міжнародним стандартам було виявлено ряд критичних недоліків, які суттєво впливають на рівень захищеності корпоративних даних. Основні проблеми можна розділити на організаційні, технічні та нормативно-правові аспекти.

Головних організаційна проблема у сфері інформаційної безпеки є недостатня обізнаність персоналу [29]. Низький рівень знань працівників щодо питань кібербезпеки, відсутність регулярного навчання та інструктажу сприяють несвідомому порушенню правил, що може призвести до витоку або компрометації конфіденційної інформації. Зокрема, поширеними проблемами є недостатня обізнаність про методи соціальної інженерії, ігнорування правил безпечного використання паролів та автентифікації, а також застосування персональних пристроїв для доступу до корпоративних ресурсів.

У багатьох організаціях політики безпеки визначають загальні принципи та правила, однак не закріплюють конкретну відповідальність співробітників. Це ускладнює контроль за виконанням заходів безпеки та створює труднощі в оперативному реагуванні на можливі інциденти [30]. Відсутність чітко визначених обов’язків, спеціальних посадових осіб, які б контролювали виконання політик, а також брак мотиваційних механізмів щодо дотримання вимог безпеки посилюють ризики.

Низький рівень інтеграції інформаційної безпеки у бізнес-процеси. Часто безпека розглядається як окремий процес, що існує поза межами основної операційної діяльності компанії. Це призводить до того, що безпекові вимоги не враховуються під час розробки нових продуктів та послуг, а заходи захисту сприймаються як перешкода, а не як стратегічно важливий елемент.

Відсутність періодичного перегляду та оновлення політик безпеки – багато компаній використовують застарілі нормативні документи, які не враховують сучасні загрози та новітні технології. Оскільки кіберзагрози постійно еволюціонують, необхідно регулярно оновлювати вимоги та адаптувати політики відповідно до нових реалій, щоб забезпечити ефективний рівень захисту інформаційних активів [31].

У багатьох організаціях відсутній чіткий механізм розподілу доступу до інформаційних активів, що створює значні ризики. Зокрема, проблема полягає у відсутності рольової моделі доступу, яка б чітко регламентувала, хто і за яких умов може отримувати доступ до критичних даних [32]. Крім того, часто використовуються загальні облікові записи, що ускладнює аудит дій користувачів і створює можливості для несанкціонованих змін у системах. Ще одним слабким місцем є відсутність періодичної перевірки прав доступу, через що співробітники можуть зберігати доступ до конфіденційної інформації навіть після зміни їхніх посадових обов'язків або звільнення.

Проблеми з управлінням доступом напряму пов'язані з недостатнім рівнем захисту критичних даних. У багатьох організаціях не застосовуються сучасні методи шифрування та криптографічного захисту, що робить інформацію вразливою до витоків і атак. Відсутність політики обов'язкового шифрування критичної інформації означає, що дані можуть зберігатися у відкритому вигляді, що значно полегшує їхнє перехоплення у разі компрометації системи [33]. Крім того, нерідко ігнорується використання цифрового підпису, що ускладнює перевірку автентичності даних і підвищує ризик підробки документів. Додатково загрозу становить незахищене зберігання резервних копій, оскільки їхній витік може призвести до значних репутаційних і фінансових втрат.

Технічною проблемою є недостатній рівень моніторингу та виявлення загроз, організації не завжди використовують сучасні системи моніторингу інформаційної безпеки, що ускладнює своєчасне виявлення аномальної активності та потенційних атак [34]. Відсутність автоматизованих механізмів виявлення загроз, таких як SIEM або UEBA, призводить до того, що можливі інциденти залишаються непоміченими до моменту, коли завдано значної шкоди. Крім того, бракує ефективної системи сповіщень про атаки в режимі реального часу, що ускладнює швидке реагування. Додатково організації недостатньо використовують аналітику поведінки користувачів, яка дозволяє виявляти підозрілі дії та запобігати витокам інформації ще до того, як вони призведуть до серйозних наслідків [35].

У багатьох організаціях не впроваджено централізовану систему моніторингу та усунення вразливостей, що значно ускладнює процес виявлення та реагування на потенційні загрози. Це призводить до того, що інформаційні системи не проходять регулярний аналіз на наявність слабких місць, а оновлення програмного забезпечення та впровадження патчів не відбувається своєчасно. Використання застарілих версій програмного забезпечення, які містять відомі вразливості, створює додаткові ризики для інформаційної безпеки організації [36].

Організації також стикаються з нормативно-правовими проблемами, які можуть ускладнювати їхню діяльність. Однією з основних є недостатня відповідність міжнародним стандартам безпеки. Багато компаній не адаптують свої політики інформаційної безпеки до вимог таких стандартів, як ISO/IEC 27001, GDPR, NIST, що може створювати бар’єри для інтеграції в міжнародні ринки та ускладнювати взаємодію з партнерами. Відсутність відповідності цим нормативам може також призвести до штрафів або обмежень з боку регуляторів. У багатьох компаніях ці документи є закритими, що обмежує доступ до них не лише для співробітників, але й для партнерів та клієнтів. Це може спричинити ненавмисні порушення вимог безпеки, оскільки користувачі просто не обізнані про необхідні регламенти та правила поведінки з інформаційними ресурсами [37]. Нестача відкритих інструкцій і політик знижує загальну обізнаність і підвищує ймовірність інцидентів, пов’язаних із порушенням норм кібербезпеки.

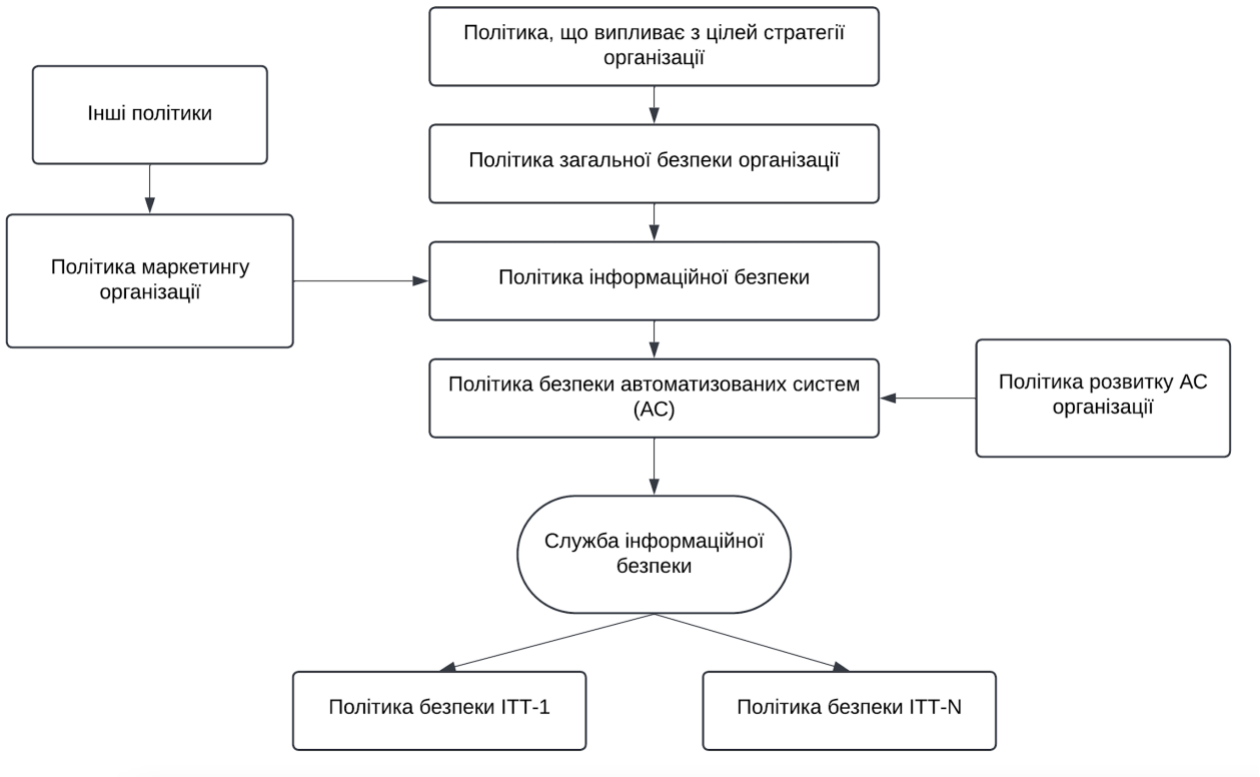


Рис. 2.1. Структура реалізації політик інформаційної безпеки в організації

## Висновки до розділу 2

Проаналізовано відповідність політик та процедур інформаційної безпеки міжнародним стандартам, таким як ISO/IEC 27001, 27002, 27005, а також нормативним вимогам щодо захисту інформаційних активів. Визначено ключові аспекти, що регламентують впровадження заходів безпеки, включаючи контроль доступу, управління ризиками, захист персональних даних та відповідальність користувачів за дотримання політик безпеки.

Розглянуто практики оцінки відповідності політик безпеки організацій встановленим міжнародним вимогам. Визначено методики аналізу інформаційної безпеки, зокрема аудит відповідності, моніторинг ризиків та перевірку ефективності впроваджених заходів. Виявлено, що багато організацій стикаються з труднощами в адаптації своїх політик до сучасних вимог через недостатню інтеграцію стандартів ІБ у бізнес-процеси.

Виокремлено основні проблеми реалізації політик інформаційної безпеки, серед яких недостатня обізнаність персоналу, відсутність чіткої відповідальності за дотримання безпеки, слабкий моніторинг інцидентів та використання застарілих підходів до управління доступом. Запропоновано заходи для усунення виявлених недоліків, що сприятиме підвищенню рівня захисту інформаційних активів та відповідності організацій міжнародним стандартам інформаційної безпеки.

# РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПОЛІТИК ТА ПРОЦЕДУР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 3.1 Рекомендації щодо впровадження міжнародних вимог у корпоративні політики безпеки

Одним із прикладів організації, яка активно працює над питаннями ІБ, є компанія ДТЕК – найбільший приватний енергетичний холдинг України, що здійснює свою діяльність у сферах генерації, дистрибуції та продажу електроенергії, а також у галузі відновлюваної енергетики та газовидобутку. ДТЕК має складну корпоративну структуру, що об’єднує кілька автономних підприємств, які підпорядковуються загальному керівництву.

*Основні виклики в сфері інформаційної безпеки.*

Оскільки ДТЕК обробляє великі обсяги конфіденційної інформації, зокрема персональні дані користувачів, комерційну таємницю, фінансову та податкову інформацію, забезпечення її захисту є ключовим завданням компанії.

Основні виклики, з якими стикається організація у сфері ІБ, включають [37]:

- Необхідність відповідності державним та міжнародним стандартам ІБ (ISO/IEC 27001, NIST, GDPR).
- Захист критичної інфраструктури від кібератак (енергетична галузь є однією з головних цілей хакерських угрупувань).
- Організація ефективного управління ризиками, включаючи розробку планів реагування на інциденти.
- Забезпечення контролю доступу та автентифікації, особливо в умовах дистанційної роботи та використання хмарних сервісів.
- Фізичний захист серверних приміщень та обладнання від несанкціонованого доступу та форс-мажорних ситуацій.

*Рекомендації щодо вдосконалення ІБ*

Для забезпечення належного рівня інформаційної безпеки в організаціях,

подібних до ДТЕК, необхідно реалізувати комплекс заходів [37]:

1. Розробка та оновлення політики інформаційної безпеки.

- Визначення основних принципів і стандартів ІБ з урахуванням міжнародних та національних норм.
- Регулярний перегляд та оновлення політики відповідно до змін у законодавстві та загрозах.
- Розробка внутрішніх регламентів, положень та процедур, що деталізують аспекти захисту інформації.

2. Посилення контролю доступу та автентифікації.

- Використання багатофакторної автентифікації (MFA) для входу в корпоративні системи.
- Впровадження рольової моделі доступу (RBAC), яка обмежує права користувачів відповідно до їх посадових обов'язків.
- Регулярне оновлення паролів та моніторинг активності користувачів.

3. Захист мережевої інфраструктури.

- Використання міжмережевих екранів (Firewall) та систем виявлення загроз (IDS/IPS).
- Організація розмежованих мереж для співробітників, гостей та критичних систем.
- Моніторинг трафіку та виявлення аномальної активності за допомогою систем SIEM.

4. Захист даних та резервне копіювання.

- Шифрування конфіденційних даних як у стані спокою, так і під час передавання.
- Регулярне створення резервних копій (backup) зберігання їх у захищених локаціях. Впровадження політики мінімізації зберігання критичної інформації.

5. Розвиток культури інформаційної безпеки серед персоналу [37].

- Регулярне навчання співробітників щодо основ кібербезпеки та

захисту даних.

- Проведення тестових кібератак та фішингових кампаній для оцінки рівня підготовки персоналу.
- Впровадження механізму звітності про підозрілі дії та інциденти.

6. Проведення аудиту та тестування безпеки.

- Виконання регулярних тестів на проникнення (пентестів) для виявлення вразливостей.
- Проведення зовнішніх та внутрішніх аудитів для оцінки ефективності заходів ІБ.
- Впровадження плану реагування на інциденти та швидке усунення виявлених загроз [37-38].

| | | | |
|---|---|---|---|
| ЧАО "ДТЭК ПАВЛОГРАДУГОЛЬ" | ЧАО "ДТЭК ДОБРОТВОРСКАЯ ТЭС-2" | АО "ДТЭК ДОНЕЦКИЕ ЭЛЕКТРОСЕТИ"" | ООО "ПРИМОРСКАЯ ВЕТРОЭЛЕКТРОСТАНЦИЯ" |
| ЧАО "ДТЭК ШАХТА КОМСОМОЛЕЦ ДОНБАССА" | ООО «СОЛАР ФАРМ - 1» | АО "ДТЭК ДНЕПРОВСКИЕ ЭЛЕКТРОСЕТИ" | ООО "НЕФТЕГАЗРАЗРАБОТКА" |
| ПАО "ДТЭК ДОБРОПОЛЬСКАЯ ЦОФ" | ООО «ТРИФАНОВКА ЭНЕРЖИ» | ЧАО "ДТЭК ПЭС-ЭНЕРГОУГОЛЬ" | ООО "НЕФТЕГАЗСИСТЕМЫ" |
| ПАО «ДТЭК ОКТЯБРЬСКАЯ ЦОФ" | ЧАО «КИЕВОБЛЭНЕРГО » | АО "ДТЭК КРЫМЭНЕРГО" | ООО "ИНВЕСТЭКОГАЗ" |
| ООО "ДТЭК ДОБРОПОЛЬЕУГОЛЬ" | АО «ОДЕССАОБЛЭНЕРГО» | АО "К.ЭНЕРГО" | ООО "ДТЕК НЕФТЕГАЗ" |
| АО "ДТЭК ЗАПАДЭНЕРГО" | АО «СВЕТ ШАХТЕРА» | ООО "ВИНД ПАУЕР" | ООО "НЕФТЕГАЗЭКСПЛУАТАЦИЯ" |
| АО "ДТЭК ДНЕПРОЭНЕРГО" | ОДО «ШАХТА «БЕЛОЗЕРСКАЯ» | ЧАО "НЕФТЕГАЗДОБЫЧА" | ООО "НЕФТЕГАЗГЕОРАЗВЕДКА" |
| | ООО "НЕФТЕГАЗЭНЕРГИЯ" | ЧАО "ДТЭК КИЕВСКИЕ ЭЛЕКТРОСЕТИ" | ООО "КОСУЛ" |

Рис. 3.1. Структура підприємств ДТЕК [37]

Забезпечення стабільності функціонування організації як бізнес-структури та об’єкта державного значення потребує впровадження ефективної системи інформаційної безпеки (ІБ), яка відповідатиме міжнародним та національним стандартам. Враховуючи критичність оброблюваних даних і масштаб діяльності, інформаційна безпека повинна базуватися на комплексному підході, що охоплює як технологічні, так і організаційні аспекти [37].

Компанія реалізує свій підхід до менеджменту ризиків, зосереджуючи увагу на наступних ключових аспектах:

1. Своєчасна ідентифікація, оцінка та управління ризиками і можливостями – організація впроваджує методики аналізу загроз, що дозволяють оперативно реагувати на потенційні небезпеки та зменшувати ймовірність інцидентів.

2. Прийняття рішень, що відповідають рівню ризику та можливостям – забезпечується інтеграція управління ризиками у всі ключові бізнес-процеси компанії, що сприяє підвищенню ефективності стратегічного планування.

3. Формування системи управління безперервності бізнесу – розробляються заходи для підтримки роботи організації в умовах надзвичайних ситуацій та мінімізації можливих переривань діяльності.

4. Створення ефективної системи страхового захисту – реалізуються механізми фінансового захисту організації на випадок втрат, пов’язаних із порушенням інформаційної безпеки.

Для детального аналізу системи інформаційної безпеки було обрано підрозділ ДТЕК КЕМ (Київські електромережі), який відповідає за надання електроенергетичних послуг у Києві. В ході дослідження доступної документації щодо забезпечення ІБ у компанії було виявлено низку специфічних особливостей:

- Політика інформаційної безпеки (ПІБ) організації офіційно затверджена у 2015 році та є основним документом, що регулює заходи щодо забезпечення безпеки даних.
- Велика кількість регламентуючих документів – організація використовує широкий перелік нормативних актів, які окреслюють різні аспекти забезпечення ІБ, серед яких:
  - Регламент інформаційної безпеки
  - Інструкція з видалення електронної пошти на ПК
  - Правила чистого столу та чистого екрану
  - Процедура управління доступом до конфіденційної інформації

- Розвинена система управління ризиками – компанія використовує "Карту вразливостей" та "Реєстр ризиків ІБ", що дозволяють системно оцінювати потенційні загрози та реалізовувати заходи для їх мінімізації.
- Обмежений доступ до документів – політика інформаційної безпеки та супутні документи доступні лише певним категоріям співробітників, що зменшує ризик витоку конфіденційної інформації. Доступ регламентується посадовими обов’язками, державними вимогами та необхідністю для виконання робочих завдань.
- Відсутність загального ознайомлення з регламентами – нові працівники проходять інструктаж з основних аспектів інформаційної безпеки, однак доступ до деяких положень можливий лише за окремим запитом. Наприклад, Регламент захисту інформації не є доступним для всіх співробітників без відповідного запиту.
- Закритість ПІБ для клієнтів – на відміну від фінансових установ, які відкрито публікують свої політики ІБ для підвищення довіри клієнтів, компанія застосовує більш закритий підхід. Це має як позитивні, так і негативні наслідки:
- Позитивний аспект – підвищена захищеність критичної інформації, що мінімізує ймовірність її витоку.
- Негативний аспект – відсутність відкритої політики може знижувати рівень довіри серед споживачів послуг, оскільки прозорість заходів безпеки часто сприймається як гарантія захисту даних.

Документ політики інформаційної безпеки організації містить 17 сторінок і структурований у 6 підрозділів, кожен з яких детально регламентує окремі аспекти функціонування Системи забезпечення інформаційної безпеки (СЗІБ).

Процес створення та розробки політики інформаційної безпеки в компанії включає такі етапи:

1. Визначення концепції ПІБ – формування базових принципів та напрямів забезпечення інформаційної безпеки.
2. Схематичне формулювання ПІБ – створення структури документа, визначення його ключових розділів та методів реалізації.

3. Розробка та впровадження – безпосереднє створення документу, його затвердження та контроль виконання положень.

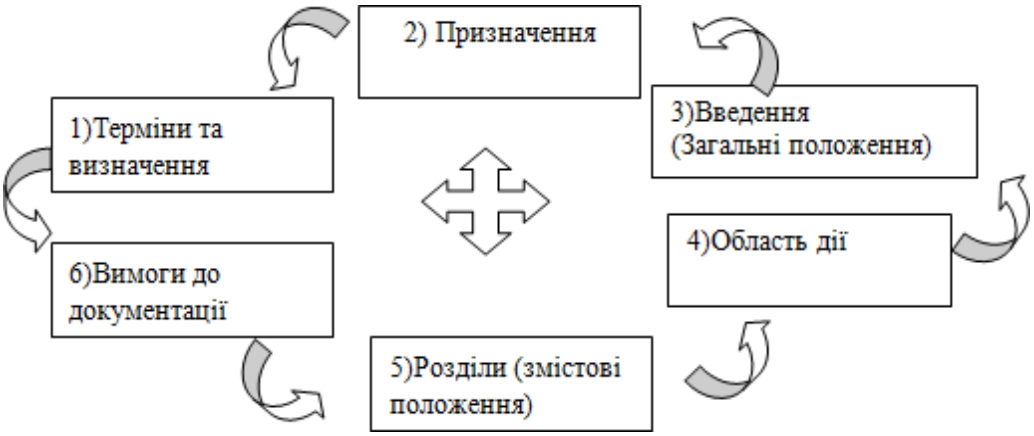


Рис. 3.2. Схема організаційної структури політики інформаційної безпеки в ДТЕК КЕМ [37]

Таким чином, можна зробити висновок, що політика інформаційної безпеки (ПІБ) організації є комплексним документом, що охоплює різні аспекти захисту інформаційних активів. Вона враховує взаємозв'язок між усіма структурними елементами, забезпечуючи узгоджене управління інформаційною безпекою. Водночас, аналіз показав, що документ не містить окремих підрозділів, які деталізують **процедури аудиту ПІБ, розподіл ролей та відповідальності користувачів**, а також регламентацію використання інформаційних активів третіми сторонами.

Якщо для невеликих компаній відсутність таких підрозділів може не мати критичного значення, то для великої організації, як **ДТЕК КЕМ**, що працює з численними партнерами, клієнтами та державними структурами, ці питання є пріоритетними. Чітке визначення повноважень співробітників і партнерів дозволяє зменшити ризик порушень у сфері інформаційної безпеки [37].

Ключові аспекти побудови політики інформаційної безпеки

1. ***Терміни та визначення*** *Політика інформаційної безпеки містить пояснення ключових термінів, що використовуються в сфері ІБ. Зокрема*:

- **Інформаційна безпека** – стан захищеності інформаційних активів організації від реальних або потенційних загроз у технологічних, інформаційних та бізнес-процесах.

- **Інформаційний ресурс** – будь-яка інформація, а також технічні засоби, що використовуються для її збереження, обробки та передачі.
- **Інцидент інформаційної безпеки** – подія, що призводить до порушення конфіденційності, цілісності або доступності інформації.
- **Критична інформація** – дані, порушення яких може спричинити значні фінансові та репутаційні втрати для організації.

Використання чітко визначених термінів у політиці забезпечує розуміння стандартів ІБ серед усіх співробітників.

2. ***Призначення політики інформаційної безпеки*** *Документ визначає загальні принципи та підходи організації до забезпечення ІБ. Він включає як технологічні, так і організаційні заходи, спрямовані на зменшення ризиків витоку, втрати або несанкціонованого використання даних*.

Основні цілі політики:

- Захист конфіденційної інформації від несанкціонованого доступу або розголошення.
- Забезпечення цілісності та доступності критичних інформаційних активів.
- Визначення механізмів моніторингу, управління ризиками та реагування на кіберінциденти.

Водночас, виявлено певний недолік документа: він не містить окремого розділу щодо **системи управління інформаційною безпекою (СУІБ)**, яка є ключовим компонентом сучасних підходів до ІБ. Ця інформація міститься в інших внутрішніх документах компанії, проте їхнє посилання в ПІБ відсутнє.

3. ***Загальні положення*** *Політика визначає сферу дії, об'єкти захисту та відповідальних осіб. Основні положення базуються на міжнародних стандартах безпеки, зокрема*:

- **ISO/IEC 27001** – стандарт з управління інформаційною безпекою.
- **CobiT** – методологія управління інформаційними технологіями та контролю ризиків.

Організація визначає, що перегляд політики здійснюється **раз на рік**, однак наразі чинний документ затверджений ще у **2015 році**, що свідчить про його **застарілість**. Сучасні стандарти інформаційної безпеки вимагають регулярного оновлення політики відповідно до змін у законодавстві, технологіях та загрозах.

4. ***Конфіденційність і правові вимоги*** *Компанія працює з різними категоріями конфіденційної інформації, серед яких*:

- **Персональні дані клієнтів та співробітників.**
- **Фінансова та комерційна інформація, податкові звіти.**
- **Відомості про інфраструктуру електромереж.**

Відповідно до **Закону України «Про інформацію»**, ці дані належать до конфіденційної категорії, а їхнє розголошення може призвести до значних ризиків для компанії та її клієнтів.

5. ***Наслідки порушення інформаційної безпеки*** *Політика чітко визначає, що* ***порушення безпеки інформації може призвести до серйозних наслідків****, серед яких*:

- Фінансові втрати, пов’язані з відшкодуванням збитків.
- Репутаційні ризики через втрату довіри клієнтів і партнерів.
- Втрати конкурентних переваг через витік комерційної інформації.
- Потенційні юридичні наслідки, включаючи штрафи та санкції.

Серед ключових ***об’єктів захисту*** в межах забезпечення інформаційної безпеки організація визначає наступні категорії [38]:

1) ***Конфіденційні інформаційні активи*** – це критично важливі дані, доступ до яких має бути обмежений. До них належать корпоративні відомості, комерційна таємниця, фінансова документація, а також будь-які інші дані, розголошення яких може завдати шкоди компанії. Крім того, сюди входять електронні та паперові документи, бази даних, звітність та будь-яка структурована або неструктурована інформація, незалежно від форми її збереження.

2) ***Бізнес-процеси та операції з обробки даних*** – захисту підлягають усі дії, що стосуються інформаційних потоків в організації, зокрема алгоритми обробки даних, політики доступу, застосовані технологічні рішення, регламенти управління інформацією, а також рольова модель взаємодії між співробітниками. Окрему увагу приділено контролю за діями персоналу, який обробляє, аналізує та передає корпоративні дані.

3) ***Цифрова та фізична інфраструктура*** – комплекс апаратних та програмних засобів, що використовуються для зберігання, аналізу та передавання інформації. До цієї категорії належать серверні потужності, комп'ютерні мережі, канали комунікації, телекомунікаційне обладнання, захисні системи, а також фізичні об'єкти, які забезпечують безпечне функціонування інформаційних систем.

Відповідно до вимог міжнародних та національних стандартів інформаційної безпеки, положення **Політики інформаційної безпеки** є обов'язковими для виконання всіма структурними підрозділами організації, її співробітниками, а також сторонніми особами, які мають доступ до інформаційних активів компанії. До цієї категорії належать:

- ***Штатні співробітники*** (незалежно від рівня доступу до інформаційних ресурсів).
- ***Тимчасово залучений персонал*** (контрактні працівники, стажери).
- ***Партнерські організації*** (компанії, що надають послуги або співпрацюють в рамках укладених угод).
- ***Зовнішні користувачі*** (аудитори, клієнти, підрядники, обслуговуючий персонал).

Усі ці особи повинні дотримуватися вимог безпеки, зокрема правил обробки даних, використання корпоративних інформаційних систем, а також забезпечення конфіденційності інформації, що стала їм доступною в процесі взаємодії з організацією.

Проблематика забезпечення ІБ для зовнішніх користувачів

Попри формальне закріплення обов'язковості дотримання заходів інформаційної безпеки всіма задіяними сторонами, існує **проблема обмеженого доступу зовнішніх осіб до політики ІБ**. Організація практикує **закритий підхід до розповсюдження нормативних документів**, що обмежує можливість третіх осіб ознайомитися з вимогами безпеки [38-39].

Це призводить до **низки ризиків**:

- **Низька обізнаність клієнтів і партнерів щодо вимог безпеки** – вони можуть несвідомо порушувати регламенти, що створює потенційні загрози.
- **Відсутність доступу до актуальних інструкцій** – сторонні користувачі не мають чітких алгоритмів дій у разі виникнення інцидентів, що ускладнює реагування на можливі загрози.
- **Проблеми з контролем дотримання заходів ІБ** – організація не може ефективно оцінити, чи сторонні особи дотримуються політики безпеки, оскільки вона не є для них відкритою.

5. Управління інформаційною безпекою.

Цей розділ є одним із найбільш масштабних, оскільки містить детальний опис процесів забезпечення інформаційної безпеки (ІБ) в організації. Всі його складові тісно взаємопов'язані, оскільки організація прагне підтримувати стандартизований підхід до захисту даних, який охоплює всі напрямки діяльності. Кожен підрозділ політики проходить узгодження на відповідність загальним положенням інформаційної безпеки, що забезпечує цілісність системи управління ризиками та мінімізує потенційні загрози.

5.1. Стратегічне управління інформаційною безпекою

Основою політики інформаційної безпеки є **розробка та впровадження стратегічного підходу** до її підтримки. Відповідальність за визначення загальних принципів безпеки, контроль виконання заходів та їхнє поширення серед співробітників покладається на керівний склад компанії [39].

Документальна база організації з інформаційної безпеки включає широкий спектр інструкцій, положень та правил. Їхня розробка та затвердження покладається на керівників відповідних департаментів:

- **ІТ-відділ** забезпечує впровадження технологічних рішень та підтримку інформаційних систем.
- **Служба безпеки** контролює фізичну та мережеву безпеку, доступ до об’єктів та захист критичних активів.
- **Відділ управління персоналом** займається підвищенням обізнаності співробітників у сфері інформаційної безпеки.

Всі документи, які розробляються в межах політики інформаційної безпеки, проходять обов’язкове узгодження з відповідальними особами, щоб виключити суперечності та забезпечити відповідність єдиній корпоративній стратегії захисту даних.

5.2. Організаційні заходи та ресурси

Організація використовує комплексний підхід до забезпечення ІБ, поєднуючи **технічні засоби, кадрові ресурси та спеціалізоване програмне забезпечення**. Основна увага приділяється централізованому управлінню інформаційною безпекою, що включає підтримку всіх корпоративних інформаційних систем у захищеному середовищі.

5.3. Політика взаємодії із зовнішніми користувачами

Забезпечення захисту інформації в межах співпраці з партнерами та зовнішніми користувачами здійснюється через **систему обмеженого доступу**. Доступ до корпоративних інформаційних ресурсів, таких як фінансові документи, бази даних, технічна документація, може надаватися виключно після підписання **Договору про нерозголошення (NDA) [40]**.

Окрім цього, всі зовнішні користувачі, які отримують доступ до корпоративної інформації, повинні використовувати її виключно у **виробничих цілях**, без можливості передачі третім особам. У разі потреби додаткових прав доступу рішення ухвалюється керівництвом або власником інформаційного активу.

Для фізичного захисту інформації застосовуються **інженерні та організаційні заходи**:

- Впровадження обмеженого доступу до об’єктів організації (пропускна система, охорона, відеоспостереження).
- Фізичний контроль за інформаційною інфраструктурою (закрита серверна зона, захищені архіви, контроль переміщення носіїв інформації).

Усі договори з партнерами містять пункти щодо:

- **Дотримання вимог внутрішньої політики інформаційної безпеки організації.**
- **Відповідальності за підтримку заходів безпеки та запобігання витоку даних.**
- **Обмеження доступу до критичних активів для сторонніх користувачів.**

5.4. Класифікація інформаційних активів

Одним із важливих напрямів управління інформаційною безпекою є **класифікація активів**, що дозволяє ефективно визначати рівень їхньої критичності та рівень доступу до них. Відповідальність за безпеку активів закріплена за відповідальними особами, які контролюють правильне використання та захист даних.

5.5. Управління безпекою персоналу

Організація забезпечує інформаційну безпеку через **інтеграцію вимог ІБ у кадрову політику**. Вимоги щодо безпечної роботи з корпоративними ресурсами включені в **трудові договори та посадові інструкції**.

При прийомі на роботу всі співробітники проходять **обов’язкове ознайомлення** з політикою безпеки. Контроль за виконанням заходів ІБ здійснюється протягом усього періоду роботи співробітника.

Особливий акцент зроблено на **відповідальності персоналу за порушення заходів ІБ**. У посадових інструкціях містяться положення щодо [40-42]:

- **Юридичних наслідків** у разі порушення вимог безпеки.
- **Санкцій за порушення** правил використання інформаційних ресурсів.

- **Контролю дій працівників** під час роботи з конфіденційною інформацією.

Навчання користувачів інформаційної безпеки проводиться регулярно та включає:

- Ознайомлення з політикою інформаційної безпеки.
- Пояснення юридичної відповідальності за порушення вимог.
- Практичне навчання роботі з корпоративними даними.

На практиці навчання проходить через **інструктаж при прийомі на роботу** та **тестування працівників** раз на півроку. Проте, основний акцент робиться на **знаннях посадових обов'язків**, а не на глибокому вивченні політики ІБ, що є певним недоліком.

Додаткові аспекти інформаційної безпеки

Окрім основних заходів, політика ІБ організації також регламентує такі напрямки [42]:

- **Фізична безпека** (контроль доступу до обладнання, зонування територій).
- **Захист інформаційних систем** (впровадження механізмів резервного копіювання, управління оновленнями, захист від шкідливого ПЗ).
- **Політика контролю доступу** (авторизація, ідентифікація користувачів, управління привілеями).
- **Забезпечення безперервності бізнес-процесів** (стратегії мінімізації ризиків та швидкого відновлення роботи у разі інцидентів).
- **Аналіз ризиків та аудит** (регулярна оцінка ризиків та відповідність законодавчим вимогам).

Останній пункт є **обов'язковим елементом управління інформаційною безпекою**, оскільки дозволяє **формувати ефективні стратегії захисту**. Відповідальність за процес оцінки ризиків покладена на **Комітет з управління ризиками**, який здійснює моніторинг загроз та впроваджує заходи щодо їх усунення.

Регулярний аудит інформаційної безпеки дозволяє **виявляти слабкі місця** та коригувати стратегію безпеки відповідно до сучасних викликів [43-44].

6. Вимоги до інформаційної безпеки

Останній розділ політики інформаційної безпеки регламентує перелік нормативних документів, які використовуються для впровадження, підтримки та розвитку Системи управління інформаційною безпекою (СУІБ). Основною метою є встановлення стандартів, правил, процедур та обов'язкових вимог для всіх підрозділів організації з метою ефективного регулювання заходів інформаційної безпеки.

ДТЕК КЕМ використовує **класичну модель регламентації документів** у сфері інформаційної безпеки, поділяючи їх на три основні рівні: **верхній рівень (стратегічні документи), середній рівень (процедури) та нижній рівень (інструкції та правила)**. Такий підхід забезпечує систематизацію всіх нормативних документів, їхню узгодженість між собою та відповідність загальній політиці організації у сфері безпеки.

Політика інформаційної безпеки визначена як основний документ, що описує **цілі, призначення, ключові принципи функціонування СУІБ**. Вона встановлює загальні напрями діяльності у сфері інформаційної безпеки, окреслює базові вимоги до процесів захисту інформації та визначає відповідальність різних підрозділів у межах єдиної корпоративної системи управління ризиками.

Підпорядкованість усіх нормативних документів у сфері інформаційної безпеки представлена у вигляді **структурної моделі**, що відображає їхній взаємозв'язок. Ця схема забезпечує узгоджене функціонування всіх заходів із підтримки безпеки інформаційних активів та їхньої інтеграції у загальну систему управління організацією [44].

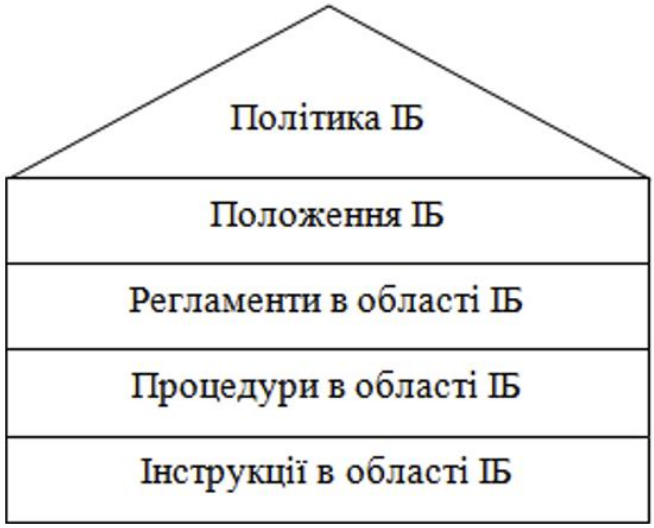


Рис. 3.3. Структура документального регулювання інформаційної безпеки [44]

## 3.2 Перспективи розвитку політик інформаційної безпеки в умовах цифрової трансформації

Проведений аналіз політики інформаційної безпеки **ДТЕК КЕМ** дозволив визначити основні підходи компанії до формування ***Системи управління*** **інформаційною безпекою (СУІБ)** та її ключові завдання щодо **захисту інформаційних ресурсів**. Головний акцент зроблено на **ризик-орієнтованому підході,** що передбачає **систематичне оцінювання загроз, управління ризиками та усунення вразливостей.**

Політика інформаційної безпеки в компанії є ***функціональною та дієвою***, оскільки містить всі необхідні структурні елементи:

- Чітке визначення ***базових принципів та концепції безпеки***.
- Опис ***цілей і завдань*** системи інформаційної безпеки.
- Визначення ***відповідальності структурних підрозділів*** за підтримку заходів ІБ.
- Регламентацію ***процедур контролю доступу*** для працівників, партнерів та сторонніх осіб.
- Окреслення ***механізмів підвищення обізнаності персоналу*** щодо ІБ.

Однак, у процесі аналізу були виявлені **недоліки,** які потребують доопрацювання, що буде розглянуто у наступному підрозділі **(див. підрозділ 3.2)**. Визначені проблемні аспекти дозволяють сформулювати **рекомендації** щодо вдосконалення політики ІБ та оптимізації процесів її реалізації [45].

Важливо відзначити, що розробка політики інформаційної безпеки **не може бути універсальною** для всіх компаній. Попри наявність загальнодоступних шаблонів та прикладів політик інших організацій, кожне підприємство має **індивідуалізувати процес створення та впровадження ПІБ**. Відповідальність за її розробку повинна лежати на керівництві організації спільно з фахівцями у сфері інформаційної безпеки, які володіють глибоким розумінням **структури бізнес-процесів та інформаційної інфраструктури**.

Мінімальний набір розділів для базової ПІБ

На початковому етапі розробки політики ІБ доцільно використовувати **базову структуру**, що включає такі основні розділи:

- **Опис організаційної структури інформаційної безпеки** – деталізує об’єкти захисту, суб’єктів контролю, відповідальних осіб, рівень доступу та загальні принципи управління інформаційною безпекою.
- **Контроль доступу та управління привілеями** – визначає механізми надання, обмеження та перевірки доступу користувачів до інформаційних активів [45].
- **Процедури змін у системі захисту** – регламентують перехід між рівнями безпеки, адаптацію політики до нових викликів та впровадження оновлень.
- **Моніторинг, аудит та аналіз ефективності заходів ІБ** – визначає регулярність перевірок, методи оцінки ефективності політики безпеки та заходи щодо вдосконалення системи захисту.

На основі аналізу політики інформаційної безпеки **ДТЕК КЕМ** було розроблено **власну схему побудови ПІБ**, яка детально описує **ключові етапи її розробки та реалізації**.

Основні етапи створення ПІБ

1. Аналіз та формування концепції

На першому етапі визначаються **ключові нормативні документи та стандарти**, які будуть використані в основі політики інформаційної безпеки. До них належать [46]:

- ***Міжнародні стандарти*** (ISO/IEC 27001, NIST, GDPR).
- ***Національні регламенти та законодавчі вимоги***.
- ***Внутрішні корпоративні стандарти*** щодо інформаційної безпеки.

На основі цих документів формуються **основні вимоги та положення ПІБ**, які включають:

- Регламент управління доступом до інформаційних систем, механізми ідентифікації та захисту інформаційних ресурсів.
- Вимоги щодо резервного копіювання даних.
- Політику щодо оновлення та модернізації програмного забезпечення.
- Регламент управління інцидентами та звітності про порушення інформаційної безпеки.

2. Визначення рівня захищеності інформаційної системи

На цьому етапі проводиться **оцінка ризиків та визначення рівня захисту**, який необхідний для забезпечення безпеки критичних даних. Залежно від типу та важливості інформаційних активів встановлюються рівні безпеки [47]:

- ***Базовий рівень*** – мінімальні заходи захисту для неконфіденційних даних.
- ***Підвищений рівень*** – посилений контроль для критичної корпоративної інформації.
- ***Повний рівень захисту*** – максимальний контроль над даними, що є комерційною або державною таємницею.

Вибір рівня безпеки визначає **методи аналізу ризиків та підходи до управління загрозами**, які будуть використовуватися в організації.

3. Розробка заходів із протидії загрозам

Політика інформаційної безпеки повинна передбачати комплексні заходи захисту, які поділяються на чотири основні категорії [48-50]:

- ***Нормативно-правові*** – відповідність законодавчим нормам, регулювання внутрішньої документації.
- ***Організаційні*** – правила роботи з даними, відповідальність співробітників, навчання персоналу.
- ***Технологічні*** – засоби захисту інформаційних активів, системи моніторингу та управління ризиками.
- ***Програмно-апаратні*** – використання антивірусного захисту, фаєрволів, системи двофакторної автентифікації та шифрування даних.

4. Регламент сертифікації та перевірки відповідності

Для підтвердження ефективності політики безпеки необхідно впроваджувати **процедуру сертифікації та аудиту**. Це включає:

- Періодичне оновлення політики відповідно до змін у законодавстві та технологіях.
- Розклад **перегляду заходів безпеки** та внесення змін до регламентуючих документів.
- Контроль ефективності механізмів захисту інформації.

5. Навчання персоналу та роз’яснення вимог політики ІБ

Важливим етапом є **підготовка співробітників**, які працюють з інформаційними активами. Політика безпеки повинна передбачати:

- Проведення регулярних тренінгів.
- Ознайомлення всіх працівників із ключовими вимогами політики безпеки.
- Контроль за дотриманням правил та проведення тестування знань у сфері ІБ.

6. Визначення меж застосування ПІБ та її оновлення

Завершальний етап передбачає **визначення меж політики ІБ**, її інтеграцію в загальну систему управління підприємством та встановлення механізмів контролю за її дотриманням [50].

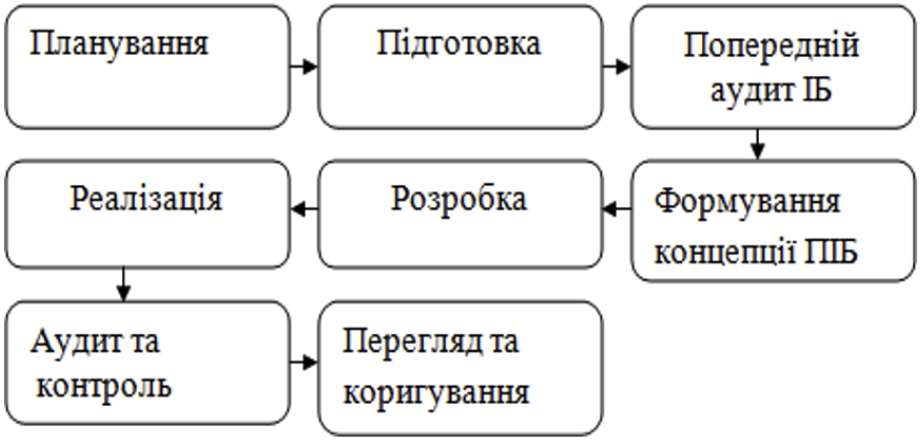


Рис. 3.4. Алгоритм формування політики інформаційної безпеки

1) ***Планування*** – визначення необхідності впровадження ПІБ, обговорення з керівництвом, встановлення цілей та завдань, повідомлення відповідальних осіб та підрозділів.

2) ***Підготовка*** – призначення команди розробників ПІБ, розподіл обов'язків, вивчення законодавчих та нормативних вимог, аналіз методик створення політики.

3) ***Попередній аудит ІБ*** – оцінка поточного стану інформаційної безпеки, ідентифікація ризиків, вразливостей, класифікація активів, визначення критичних точок бізнес-процесів.

4) ***Формування концепції ПІБ*** – розробка загальної структури документа, вибір стандартів та методології, погодження ключових принципів та напрямів.

5) ***Розробка*** – деталізація заходів, формулювання правил доступу, процедур моніторингу та реагування, складання документації, перевірка на узгодженість.

6) ***Реалізація*** – офіційне впровадження політики, доведення до персоналу, навчання співробітників, адаптація до корпоративних процесів.

7) ***Аудит та контроль*** – регулярне тестування ефективності політики, моніторинг дотримання вимог, перегляд та внесення коригувань у разі необхідності [51].

Таблиця 3.1.

Структура політики інформаційної безпеки (адаптований варіант)

| Розділ | Опис |
|---|---|
| Вступ | Політика інформаційної безпеки (ПІБ) є основним документом, що регламентує правила, вимоги та принципи захисту інформаційних ресурсів організації. Містить основні терміни та визначення відповідно до міжнародних стандартів (ISO/IEC 27000:2016) та законодавчих норм. Описує мету та значення впровадження ПІБ для компанії. |
| Загальні положення | Визначає основні принципи інформаційної безпеки організації, цілі та завдання політики, механізми забезпечення безпеки даних, права та обов'язки відповідальних осіб. |
| Нормативна база | Включає нормативно-правові акти, що регулюють ІБ, зокрема, закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», а також міжнародні стандарти ISO/IEC 27001, 27002, 27005. |
| Цілі політики | Окреслює основні цілі ПІБ, серед яких: забезпечення конфіденційності, цілісності та доступності інформації, захист інформаційних активів, зменшення ризиків, дотримання вимог законодавства та стандартів ІБ. |
| Основні завдання | Реалізація заходів щодо захисту інформації, впровадження надійної системи контролю доступу, запобігання загрозам, забезпечення безперервності функціонування ІТ-інфраструктури, визначення відповідальності за порушення. |

Продовження таблиці 3.1

| | |
|---|---|
| Розподіл ролей та відповідальності | Описує повноваження відповідальних осіб та підрозділів (служба ІБ, ІТ-департамент, служба безпеки, управління персоналом), визначає відповідальність за дотримання політики та регламентує процеси контролю. |
| Контроль доступу до інформаційних систем | Регламентує правила надання доступу до інформаційних ресурсів підприємства, контроль прав користувачів, обмеження доступу для сторонніх осіб, управління привілеями та облік дій користувачів. |
| Захист обладнання та інформаційної інфраструктури | Встановлює вимоги до використання апаратного та програмного забезпечення, регламентує правила роботи з матеріальними носіями інформації, описує заходи захисту обладнання та мережевої інфраструктури. |
| Управління ризиками, загрозами та інцидентами | Включає процедури ідентифікації ризиків, класифікації загроз, оцінки вразливостей, впровадження заходів протидії, а також механізми реагування на інциденти та дії персоналу у разі їх виявлення. |
| Відповідальність за дотримання ПІБ | Визначає осіб, відповідальних за виконання вимог політики, регламентує персональну відповідальність за роботу з інформаційними активами, встановлює санкції за порушення політики. |
| Криптографічний захист та програмні засоби | Регламентує використання криптографічних методів захисту, управління цифровими підписами, політику шифрування даних, принципи безпечного використання програмного забезпечення та засобів контролю безпеки. |
| Супутня документація | Включає додаткові документи, що регулюють питання ІБ (регламенти, інструкції, положення), зокрема правила доступу, політику безпечного використання інформаційних ресурсів, протоколи захисту інформації. |

Продовження таблиці 3.1

| | |
|---|---|
| Аудит та контроль виконання ПІБ | Визначає процедури планового та позапланового аудиту інформаційної безпеки, періодичність перевірок, відповідальних осіб та критерії оцінки ефективності реалізованих заходів. |
| Обмін інформацією та взаємодія з партнерами | Визначає вимоги до обміну інформацією між структурними підрозділами, регламентує правила надання даних стороннім особам та партнерам, встановлює обмеження щодо розголошення корпоративної інформації. |
| Загальні рекомендації | Включає спеціалізовані політики, такі як політика парольного захисту, політика використання електронної пошти, вимоги до захисту мереж та управління мобільними пристроями. |

## 3.3 Рекомендації для покращення ефективності процедур інформаційної безпеки в організаціях

Розробка та реалізація стратегії інформаційної безпеки для критично важливих об’єктів потребує комплексного підходу, що поєднує оцінку поточного стану безпеки, управління ризиками та впровадження сучасних технологічних рішень. Основним завданням є не лише аналіз рівня інформаційної безпеки та визначення вразливостей, а й розробка практичного підходу, який дозволить узгодити міжнародні стандарти безпеки із реальними процесами впровадження захисних рішень в організації.

З метою структурного відображення послідовності впровадження технічних заходів було розроблено дорожню карту, яка демонструє взаємозв’язок між впровадженням технологій захисту та їх відповідністю до стандартів інформаційної безпеки. Дорожня карта є інструментом стратегічного планування, що дозволяє візуалізувати ключові етапи реалізації заходів безпеки та оцінити їхній вплив на організацію.

Основні функції дорожньої карти [52-54]:

1. Структуроване відображення критичних етапів безпеки – карта дозволяє побачити основні завдання та порядок їх виконання, що спрощує управління процесами інформаційної безпеки.

2. Інструмент комунікації – спрощує обговорення заходів безпеки між керівництвом та технічними фахівцями, дозволяючи узгоджувати стратегічні рішення.

3. Контроль прогресу – забезпечує можливість моніторингу реалізації кожного етапу та оцінки його ефективності.

Для розробки дорожньої карти використано діаграму Ганта – інструмент планування, який дозволяє графічно відобразити взаємозв'язки між завданнями, визначити строки реалізації та оцінити вплив впроваджених заходів на загальну систему безпеки [54].

Етапи впровадження технологічних рішень для посилення безпеки

Відповідно до розробленої стратегії інформаційної безпеки, послідовність реалізації технічних заходів включає наступні етапи [55]:

- WAF – впровадження Web Application Firewall для захисту веб-додатків від атак.
- BDS – інтеграція Breach Detection System для виявлення загроз та вторгнень.
- IAM – впровадження Identity & Access Management System для контролю та управління доступом користувачів.
- PAM – інтеграція Privileged Access Management System для захисту привілейованих акаунтів.
- CASB – застосування Cloud Access Security Broker для моніторингу та безпечного доступу до хмарних ресурсів.
- NAC – впровадження Network Access Control для управління доступом до корпоративної мережі.
- ICS – розгортання Industrial Cybersecurity System для захисту промислових систем та SCADA.

- UEBA – використання User & Entity Behavior Analytics System для виявлення аномальної активності користувачів.
- DBS – реалізація Database Security Solution для захисту баз даних.
- INV – проведення інвентаризації активів та оцінка критичних точок безпеки.
- STCN – сегрегація корпоративної та технологічної мереж для підвищення рівня захисту.
- STNE – сегментація внутрішніх мереж підприємства для зниження ризиків поширення атак.

Контрольні заходи та відповідність стандартам безпеки

З метою забезпечення відповідності міжнародним стандартам інформаційної безпеки (ISO/IEC 27001, NIST, GDPR), паралельно з впровадженням технічних засобів необхідно реалізувати контрольні заходи, які визначають регламент і правила керування ризиками [56-59].

Основні контрольні заходи:

- 1.1 – систематизація та актуалізація нормативної документації з ІБ.
- 2.1 – розробка методики оцінки ризиків інформаційної безпеки.
- 3.1 – впровадження програми підвищення обізнаності персоналу щодо кібербезпеки.
- 4.1 – впровадження рольової моделі доступу до корпоративних ресурсів.
- 4.2 – реалізація процесу періодичного перегляду прав доступу.
- 5.1 – формалізація вимог ІБ в проектному управлінні.
- 6.1 – створення процедури управління криптографічним захистом інформації.
- 7.1 – розробка політики управління мобільними пристроями.
- 7.2 – регламент використання переносних носіїв даних.
- 8.1 – впровадження безпечного цикл розробки програмного забезпечення (SDLC).
- 9.1 – розробка та впровадження процесу управління інцидентами в

ІБ.

- 10.1 – реалізація процесу управління вразливостями інформаційних систем.
- 11.1 – стандартизація контролю постачальників послуг для забезпечення ІБ.
- 12.1 – створення вимог до налаштування безпечної конфігурації обладнання.
- 13.1 – оцінка ефективності функціонування системи інформаційної безпеки [60].

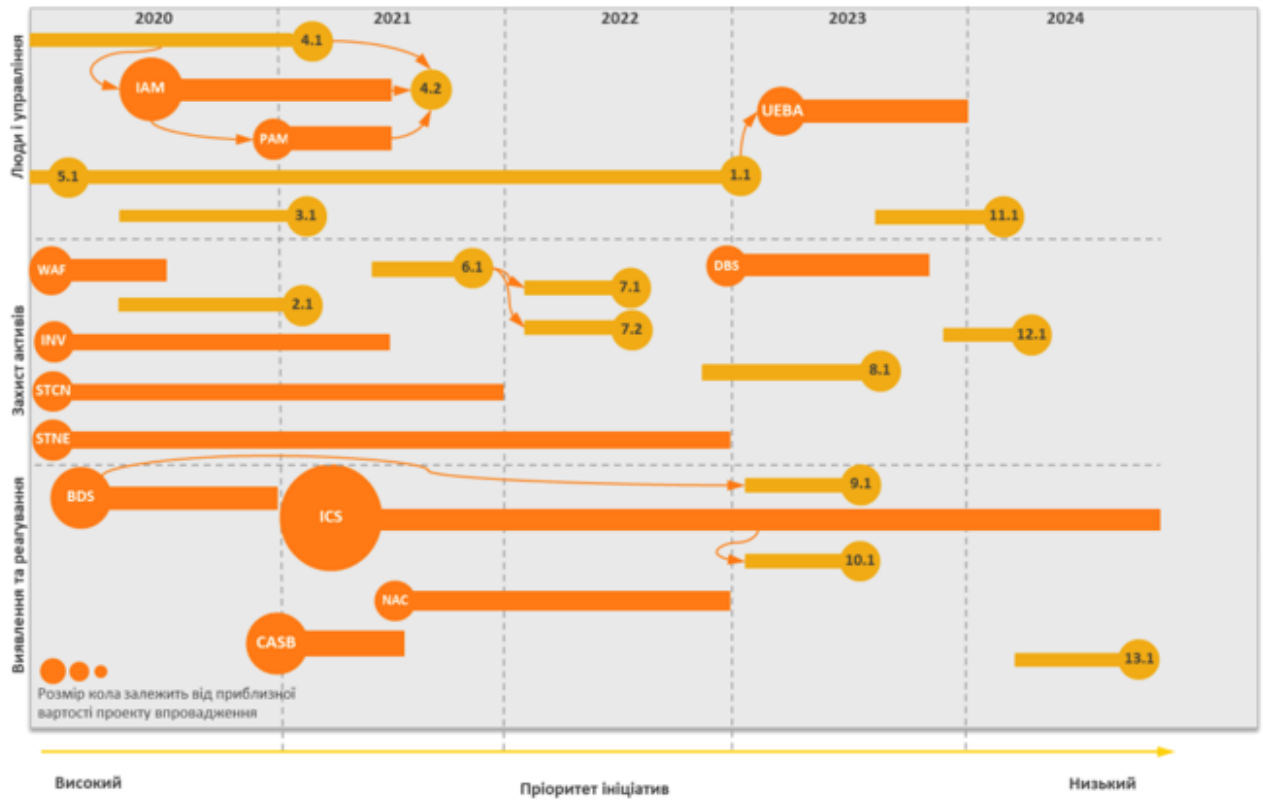


Рис 3.3. Дорожня карта реалізації технічних та методологічних заходів інформаційної безпеки

## Висновки до розділу 3

Розглянуто основні підходи до вдосконалення політик та процедур інформаційної безпеки в організаціях, визначено критичні аспекти управління ризиками та захисту інформаційних активів. Проведено аналіз поточного стану ІБ, визначено основні проблеми та сформульовано рекомендації щодо оптимізації існуючих заходів безпеки, включаючи контроль доступу, управління інцидентами, політику зберігання та обміну інформації.

Розроблено комплексний підхід до впровадження сучасних методів і технологій для посилення рівня безпеки, що передбачає інтеграцію новітніх рішень, таких як Web Application Firewall (WAF), Identity & Access Management (IAM), Privileged Access Management (PAM) та інших технологій для захисту корпоративних мереж та інформаційних систем.

Продемонстровано ефективність поетапного підходу до розробки та реалізації політики інформаційної безпеки, що включає аудит існуючих процесів, впровадження нових методик контролю ризиків та підвищення обізнаності персоналу. Визначено ключові напрями розвитку інформаційної безпеки, що дозволяють організаціям забезпечити стабільність бізнес-процесів, захист даних і відповідність міжнародним стандартам кібербезпеки.

# ВИСНОВКИ

Розглянуто основні теоретичні аспекти інформаційної безпеки в організаціях, які є ключовими для забезпечення захисту інформаційних ресурсів.

Розгляд основних понять та принципів інформаційної безпеки показав, що безпека даних ґрунтується на тріаді конфіденційність, цілісність і доступність (CIA). Ці принципи визначають основні вимоги до захисту інформації та є фундаментальними для будь-якої системи кібербезпеки.

Аналіз політик та процедур інформаційної безпеки продемонстрував, що ефективне управління безпекою в організації неможливе без чітко визначених правил і процедур. Політики безпеки регулюють доступ до ресурсів, методи шифрування, правила автентифікації користувачів, а також порядок моніторингу і реагування на інциденти. Структуровані та впроваджені відповідно до міжнародних стандартів (наприклад, ISO/IEC 27001), вони дозволяють значно знизити рівень загроз.

У рамках дослідження ризиків та загроз інформаційної безпеки було виявлено, що сучасні організації стикаються як із зовнішніми, так і внутрішніми загрозами. Основними викликами є кібератаки (фішинг, шкідливе ПЗ, DDoS-атаки, злом паролів, SQL-ін'єкції), витоки даних (ненавмисні та зловмисні) та внутрішні загрози (недотримання політик, соціальна інженерія, зловживання доступом). Виявлено, що зниження цих ризиків можливе лише за умови комплексного підходу, який поєднує технічні, організаційні та адміністративні заходи.

Таким чином, результати цього розділу підтвердили важливість системного підходу до забезпечення інформаційної безпеки. Використання міжнародних стандартів, ефективних політик безпеки, сучасних технологій захисту та підвищення обізнаності персоналу є ключовими факторами для створення надійної системи кібербезпеки в організації.

Проаналізовано відповідність політик та процедур інформаційної безпеки міжнародним стандартам, таким як ISO/IEC 27001, 27002, 27005, а також

нормативним вимогам щодо захисту інформаційних активів. Визначено ключові аспекти, що регламентують впровадження заходів безпеки, включаючи контроль доступу, управління ризиками, захист персональних даних та відповідальність користувачів за дотримання політик безпеки.

Виокремлено основні проблеми реалізації політик інформаційної безпеки, серед яких недостатня обізнаність персоналу, відсутність чіткої відповідальності за дотримання безпеки, слабкий моніторинг інцидентів та використання застарілих підходів до управління доступом. Запропоновано заходи для усунення виявлених недоліків, що сприятиме підвищенню рівня захисту інформаційних активів та відповідності організацій міжнародним стандартам інформаційної безпеки.

Розглянуто основні підходи до вдосконалення політик та процедур інформаційної безпеки в організаціях, визначено критичні аспекти управління ризиками та захисту інформаційних активів. Проведено аналіз поточного стану ІБ, визначено основні проблеми та сформульовано рекомендації щодо оптимізації існуючих заходів безпеки, включаючи контроль доступу, управління інцидентами, політику зберігання та обміну інформації.

Розроблено комплексний підхід до впровадження сучасних методів і технологій для посилення рівня безпеки, що передбачає інтеграцію новітніх рішень, таких як Web Application Firewall (WAF), Identity & Access Management (IAM), Privileged Access Management (PAM) та інших технологій для захисту корпоративних мереж та інформаційних систем.

Продемонстровано ефективність поетапного підходу до розробки та реалізації політики інформаційної безпеки, що включає аудит існуючих процесів, впровадження нових методик контролю ризиків та підвищення обізнаності персоналу. Визначено ключові напрями розвитку інформаційної безпеки, що дозволяють організаціям забезпечити стабільність бізнес-процесів, захист даних і відповідність міжнародним стандартам кібербезпеки.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Деркач А. А. Управління інформаційною безпекою: навч. посіб. Харків: ХНЕУ, 2019. 256 с.

2. Коваленко О. П. Кібербезпека: сучасні виклики та загрози. Львів: ЛНУ імені Івана Франка, 2020. 290 с.

3. Морозов М. М. Основи інформаційної безпеки: підручник. Одеса: ОНПУ, 2017. 310 с.

4. Петров В. В. Захист інформації в комп'ютерних системах. Київ: КНУ імені Тараса Шевченка, 2016. 275 с.

5. Сидоренко С. М. Інформаційна безпека держави: стратегічні аспекти. Дніпро: ДНУ, 2019. 340 с.

6. Іванченко О. Г. Аналіз загроз інформаційній безпеці в Україні Інформаційна безпека. 2020. № 2. С. 15–22.

7. Кравченко П. С. Міжнародні стандарти інформаційної безпеки та їх впровадження в Україні Кібербезпека: освіта, наука, техніка. 2019. № 1. С. 45–53.

8. Литвиненко Д. М. Роль держави у забезпеченні інформаційної безпеки Стратегічні пріоритети. 2018. № 3. С. 28–35.

9. Мельник І. В. Управління ризиками в системах інформаційної безпеки Вісник НТУУ «КПІ». 2021. № 4. С. 67–74.

10. ISO/IEC 27007:2011. Information technology – Security techniques – Guidelines for information security management systems auditing.

11. Назаренко О. О. Захист персональних даних в умовах цифрової трансформації Право України. 2020. № 5. С. 112–119.

12. Олійник Т. В. Кіберзагрози та методи їх нейтралізації Інформаційні технології та безпека. 2019. № 6. С. 53–60.

13. Павленко Ю. С. Аудит інформаційної безпеки: методологічні аспекти Економіка та держава. 2021. № 7. С. 53–59.

14. Цвілій О. О. Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою Телекомунікаційні та інформаційні технології. 2014. № 2. С. 73–79.

15. Цвілій О. О. Системи управління інформаційною безпекою: гармонізація з міжнародними стандартами, правилами та процедурами Перспективні напрями захисту інформації: зб. тез І Всеукр. наук.-практ. конф. 2015. С. 107–111.

16. Про ліцензування певних видів господарської діяльності: Закон України. URL: http:zakon1.rada.gov.ua/laws/show/1775-14 (дата звернення: 26.04.2025).

17. Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню: Постанова Кабінету Міністрів України від 25.05.2011 № 543. URL: http:zakon2.rada.gov.ua/laws/show/543-2011-%D0%BF (дата звернення: 10.03.2025).

18. ISO/IEC 17799:2005. Information technology – Security techniques – Code of practice for information security management.

19. ISO/IEC 27001:2005. Information Security Management – Specification with Guidance for Use.

20. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних: підручник. Київ: Вид-во ТОВ «НВП» Інтерсервіс, 2009. 716 с.

21. Коваленко О. П. Кібербезпека: сучасні виклики та загрози. Львів: ЛНУ імені Івана Франка, 2020. 290 с.

22. Морозов М. М. Основи інформаційної безпеки: підручник. Одеса: ОНПУ, 2017. 310 с.

23. Захист інформації в автоматизованих системах управління: навч. посіб. / уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

24. Shang K., Hossen Z. Applying fuzzy logic to risk assessment and decision making Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries. November 2013.

25. Pokoradi L. Fuzzy logic-based risk assessment . URL: http:www.zmka.hu/docs/Volume1/Issue1/pdf/04poko.pdf (дата звернення: 26.04.2025).

26. The Security Risk Management Guide. Microsoft Corporation, 2006 . URL: http:www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default (дата звернення: 26.04.2025).

27. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. URL: http:www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id=38836 (дата звернення: 20.03.2025).

28. Про криптографічний та технічний захист інформації: Закон України. URL: https:ips.ligazakon.net/document/NT1819 (дата звернення: 26.04.2025).

29. Fisher T. Free and Public DNS Servers. Lifewire, 2018 . URL: https:www.lifewire.com/free-and-public-dnsservers-2626062 (дата звернення: 26.04.2025).

30. Захист конфіденційної інформації – персональних даних . URL: https:cutt.ly/iuggGRH (дата звернення: 26.04.2025).

31. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України № 80/94-ВР від 05.07.1994 р. URL: https:zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 26.04.2025).

32. Global Cybersecurity Index (GCI) 2018 . URL: https:www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (дата звернення: 26.04.2025).

33. Рибальченко Л. В., Косиченко О. О. Проблеми безпеки персональних даних в Україні Регіональна економіка. Запоріжжя, 2019. С. 57–62.

34. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик . URL: http:www.justinian.com.ua/article.php?id=3222 (дата звернення: 15.04.2025).

35. Гнатюк С. А. Кібербезпека та захист інформації: навч. посіб. Київ: КНЕУ, 2021. 284 с.

36. Горбенко В. П., Коваленко В. О. Управління ризиками в інформаційній безпеці. Харків: ХНУРЕ, 2019. 312 с.

37. Scherer M., Gorski P. Information Security Management Handbook. CRC Press, 2017. 540 p.

38. HP ArcSight – ефективний інструмент для моніторингу подій інформаційної безпеки . URL: http:itsec.ru/articles2/Oborandteh/hp-arcsight--effektivnyyinstrument-dlya-monitoringa-sobytiy-ib (дата звернення: 26.04.2025).

39. Актуальні питання безпеки інформації . URL: https:www.science-education.ru/ru/article/view?id=17991 (дата звернення: 26.04.2025).

40. Kavanagh K., Bussa T., Sadowski G. Magic Quadrant for Security Information and Event Management. Gartner, 3 December 2018.

41. CLUSIF. MEHARI 2010 Overview . URL: http:www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-verview.pdf (дата звернення: 16.04.2025).

42. CLUSIF. MEHARI 2010 Fundamental concepts and functional specifications . URL: http:www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf (дата звернення: 26.04.2025).

43. Alberts C. J., Behrens S. G., Pethia R. D., Wilson W. R. CCTA Risk Analysis and Management Method. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation. 1999. P. 84–100.

44. Boiko A., Shendryk V. System Integration and Security of Information Systems. 2017 . URL:

https:www.researchgate.net/publication/313483965_System_Integration_and_Security_of_Information_Systems (дата звернення: 18.04.2025).

45. Політика інформаційної безпеки. Затверджено наказом АТ «УКРТРАНСНАФТА» від 28.08.2019 р. № 413 . URL: http:www.ukrtransnafta.com/politika-informatziynoi-bezpeky/ (дата звернення: 26.04.2025).

46. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) . URL: https:eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (дата звернення: 18.04.2025).

47. SANS. Security Policy Template . URL: https:www.sans.org/informationsecurity-policy/ (дата звернення: 26.04.2025).

48. ДТЕК Київські електромережі . URL: https:dtek.com/ru/sustainable_development/governance/ (дата звернення: 19.04.2025).

49. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Основні положення Кабінет Міністрів України. 1996. URL: https:tzi.com.ua/downloads/DSTU%203396.1-96.pdf (дата звернення: 26.04.2025).

50. CLUSIF. MEHARI 2010 Risk analysis and treatment guide . URL: http:www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-RiskAnalysis-and-Treatment-Guide.pdf (дата звернення: 26.04.2025).

51. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності Юридичний вісник. 2019. № 3. URL: https:lexinform.com.ua/dumka-eksperta/doktrynalni-polozhennya-informatsijnoyi-bezpeky-ukrayiny-v-umovah-suchasnosti (дата звернення: 26.04.2025).

52. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів Резонанс. 2017. № 18. С. 3–14. URL: http:nbuviap.gov.ua/images/rezonans/2017/rez18.pdf (дата звернення: 26.04.2025).

53. Промислові комунікаційні мережі. Захищеність (кібербезпека) мереж і систем. Частина 2-1 ISO/IEC. 2015 . URL: https:pdf.standartgost.ru/catalog/Data2/1/4293762/4293762664.pdf (дата звернення: 26.04.2025).

54. Гузенко В. В. Становлення та розвиток світових стандартів інформаційної безпеки Наукові записки Національного педагогічного університету імені М. П. Драгоманова. Серія 18: Економіка і право. 2018. Вип. 28. С. 154–160.

55. Міжнародні стандарти інформаційної безпеки: компаративне дослідження Публічне управління та адміністрування в Україні. 2019. Вип. 2. С. 123–130.

56. Calder A., Watkins S. IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page Publishers, 2015. 368 p.

57. Humphreys E. Implementing the ISO/IEC 27001 Information Security Management System Standard. Artech House, 2007. 286 p.