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: “ РЕКОМЕНДАЦІЇ ДО СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ОРГАНІЗАЦІЇ”

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

_____ Лідія ПЕХОВА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-41
Лідія ПЕХОВА
Ім’я, ПРІЗВИЩЕ

Керівник: Євгенія ІВАНЧЕНКО
д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
д.т.н., професор 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

Пеховій Лідії Олександрівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Рекомендації до створення та впровадження політики інформаційної безпеки для організації”,
керівник кваліфікаційної роботи ІВАНЧЕНКО Євгенія д.т.н., професор.
(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, методи та засоби управління персоналом з інформаційної безпеки:, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1 Проаналізувати існуючі рекомендації до створення та впровадження політики інформаційної безпеки для організацій.
4.2 Дослідити методи створення та впровадження політики інформаційної безпеки.
4.3. Розробити рекомендацій до створення та впровадження політики 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.	Аналіз рекомендації до створення та впровадження політики інформаційної безпеки для організацій.	08.04.2025	
4.	Дослідження методів створення та впровадження політики інформаційної безпеки.	15.04.2025	
5.	Розробка рекомендацій до створення та впровадження політики інформаційної безпеки.	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.05.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувачка вищої освіти _____ Лідія ПЕХОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Євгенія ІВАНЧЕНКО
(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 здобувачка Пехова Л.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: “ Рекомендації до створення та впровадження політики інформаційної безпеки для організації ”

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка ПЕХОВА Лідія у кваліфікаційній роботі проаналізувала існуючі рекомендації до створення та впровадження політики інформаційної безпеки для організацій, дослідила методи створення та впровадження політики інформаційної безпеки, розробила рекомендацій до створення та впровадження політики інформаційної безпеки.

ПЕХОВА Лідія показала розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довела володіння методами наукового дослідження, проявила себе як організований, відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки ПЕХОВОЇ Лідії на оцінку “відмінно” та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я,ПРІЗВИЩЕ)*

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Пехова Л.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

здобувачки вищої освіти ПЕХОВОЇ Лідії Олександрівни
на тему “Рекомендації до створення та впровадження політики інформаційної безпеки для організації”

Актуальність. У сучасних умовах стрімкого розвитку цифрових технологій та зростання кіберзагроз, таких як фішингові атаки, витоки даних і несанкціонований доступ, створення та впровадження ефективної політики інформаційної безпеки є критично важливим для організацій. Забезпечення захисту інформаційних активів, відповідність міжнародним стандартам, зокрема ISO/IEC 27001 і GDPR, а також формування культури безпеки серед персоналу є ключовими завданнями для підтримки конкурентоспроможності та стабільності бізнесу. З огляду на це, дослідження методів створення та впровадження політики інформаційної безпеки є актуальним і має значну практичну цінність.

Позитивні сторони:

1. У роботі проведено ґрунтовний аналіз існуючих рекомендацій до створення політики інформаційної безпеки, досліджено нормативно-правову базу України та міжнародні стандарти, що забезпечують її відповідність сучасним вимогам.

2. Розроблено п’ятиетапну методику створення політики інформаційної безпеки, яка включає аналіз активів, розробку регламентів, інтеграцію з системами управління, автоматизацію моніторингу та навчання персоналу, адаптовану до хмарної інфраструктури компанії Creatio.

3. Кваліфікаційна робота оформлена відповідно до вимог, матеріал викладено логічно та структуровано, ключові положення проілюстровано рисунками та таблицями. Робота містить 49 джерел, включаючи англомовні публікації, що свідчить про глибоке опрацювання літератури.

4. Запропонована політика інформаційної безпеки інтегрована з бізнес-процесами, забезпечує захист 1,2 ТБ даних і підтвердила свою ефективність, скоротивши кількість інцидентів на 60% та час підготовки до аудитів на 70%.

Недоліки:

Доцільно було б глибше дослідити та класифікувати спеціалізовані програмні інструменти для безперервного моніторингу ефективності впровадженої політики інформаційної безпеки, що могло б посилити її практичну цінність.

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

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні, демонструє глибоке розуміння авторкою проблематики та практичних аспектів створення політики інформаційної безпеки. Робота заслуговує оцінки “відмінно”, а здобувачка ПЕХОВА Лідія Олександрівна – присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: Галина ГАЙДУР
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню рекомендацій до створення та впровадження політики інформаційної безпеки для організації. Робота складається із вступу, трьох розділів, що містять 12 рисунків, 5 таблиць, висновків і списку використаних джерел із 49 найменувань. Загальний обсяг роботи становить 111 аркушів, з яких 8 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка рекомендацій створення та впровадження політики інформаційної безпеки, що відповідає сучасним вимогам та стандартам у сфері кібербезпеки.

Об'єкт дослідження – процеси управління інформаційною безпекою в організації.

Предмет дослідження – методи створення та впровадження політики інформаційної безпеки

Методи дослідження. Для вирішення поставлених завдань у роботі використано методи аналізу та синтезу, порівняльного аналізу, класифікації та системного підходу.

Як результат у роботі досліджено теоретичні основи політики інформаційної безпеки, проаналізовано сучасні міжнародні стандарти та нормативно-правові документи, розроблено алгоритм створення політики ІБ, а також сформульовано практичні рекомендації щодо її впровадження.

Галузь застосування. Запропоновані підходи можуть бути використані у державних органах, великих компаніях та інших організаціях для формування системи управління інформаційною безпекою, оптимізації заходів захисту інформаційних ресурсів та підвищення рівня кібербезпеки.

Ключові слова: ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ РИЗИКАМИ, ISO/IEC 27001, NIST CSF, ВПРОВАДЖЕННЯ ПОЛІТИКИ, КІБЕРБЕЗПЕКА.

ABSTRACT

The qualification work is devoted to the study of recommendations for the creation and implementation of an information security policy for an organization. The work consists of an introduction, three sections containing 12 figures, 5 tables, conclusions and a list of sources used with 49 names. The total volume of the work is 111 sheets, of which 8 sheets are occupied by a list of conventional abbreviations and a list of sources used.

The purpose of the work is to develop recommendations for creating and implementing an information security policy that meets modern requirements and standards in the field of cybersecurity.

The object of the study is the processes of information security management in an organization.

The subject of the study is methods of creating and implementing information security policy

Research methods. To solve the tasks set in the work, methods of analysis and synthesis, comparative analysis, classification and a systems approach were used.

As a result, the paper explores the theoretical foundations of information security policy, analyzes modern international standards and regulatory documents, develops an algorithm for creating an information security policy, and formulates practical recommendations for its implementation.

Field of application. The proposed approaches can be used in government agencies, large companies, and other organizations to form an information security management system, optimize measures to protect information resources, and increase the level of cybersecurity.

Keywords: INFORMATION SECURITY POLICY, RISK MANAGEMENT, ISO/IEC 27001, NIST CSF, POLICY IMPLEMENTATION, CYBERSECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AWS	Amazon Web Services (Хмарна платформа Amazon)
CRM	Customer Relationship Management (Управління відносинами з клієнтами)
CNSP	Cloud-Native Security Platform (Хмарна платформа безпеки)
DLP	Data Loss Prevention (Запобігання витокам даних)
GDPR	General Data Protection Regulation (Загальний регламент захисту даних)
HIPAA	Health Insurance Portability and Accountability Act (Закон про переносимість і підзвітність медичного страхування)
IAM	Identity and Access Management (Управління ідентичністю та доступом)
ISO/IEC 27001	Міжнародний стандарт інформаційної безпеки
MFA	Multi-Factor Authentication (Багатофакторна аутентифікація)
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework (Рамка кібербезпеки NIST)
PDCA	Plan-Do-Check-Act (Плануй-Виконуй-Перевіряй-Аналізуй)
SIEM	Security Information and Event Management (Управління інформацією та подіями безпеки)
SSL/TLS	Secure Sockets Layer/Transport Layer Security (Протоколи шифрування)
АРМ	Автоматизоване робоче місце
ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення
РУД	Рольове управління доступом
СУІБ	Система управління інформаційною безпекою

ВСТУП

У сучасному інформаційному середовищі питання захисту даних та забезпечення інформаційної безпеки набувають особливої актуальності. Швидкий розвиток цифрових технологій, зростання обсягу оброблюваної інформації, а також постійне еволюціонування кіберзагроз змушують організації впроваджувати ефективні заходи для захисту своїх інформаційних активів. Недостатній рівень захисту може призвести до серйозних фінансових, репутаційних та операційних збитків, тому розробка та впровадження системи управління інформаційною безпекою є невід'ємною складовою сучасного бізнесу.

Метою даного дослідження є розробка та обґрунтування рекомендацій створення та впровадження політики інформаційної безпеки, яка відповідатиме сучасним міжнародним стандартам (зокрема, ISO/IEC 27001, NIST CSF) та нормативно-правовим вимогам. ***Завдання дослідження*** включають:

- проведення аналізу існуючого стану інформаційної безпеки організації;
- вивчення міжнародних стандартів, нормативних документів та передових практик у сфері інформаційної безпеки;
- розробку алгоритму створення політики інформаційної безпеки, що враховує специфіку діяльності організації;
- розробку практичних рекомендацій щодо впровадження та моніторингу ефективності політики;
- оцінку практичної цінності запропонованої методики через приклад впровадження у тестовому середовищі.

Об’єктом дослідження є процеси управління інформаційною безпекою в організації, а ***предметом*** – методи, підходи та інструменти створення і впровадження політики інформаційної безпеки. Для досягнення поставленої мети в роботі використано комплекс методів, зокрема аналіз літературних джерел, порівняльний аналіз міжнародних стандартів, експертне оцінювання та практичний аналіз ефективності заходів інформаційної безпеки.

Практичне значення отриманих результатів полягає у можливості впровадження розробленої методики у реальних умовах функціонування організації, що сприятиме підвищенню рівня захисту інформаційних ресурсів, оптимізації процесів управління безпекою та зниженню ризиків кіберзагроз.

Таким чином, актуальність теми дослідження визначається зростаючою потребою організацій у впровадженні сучасних засобів захисту інформації, а результати роботи можуть стати основою для розробки ефективної політики інформаційної безпеки в умовах стрімких технологічних змін.

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

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ДО СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ОРГАНІЗАЦІЙ

1.1 Роль політики інформаційної безпеки в управлінні організацією

У сучасному світі інформація є стратегічним ресурсом, що визначає успіх організації, її конкурентоспроможність і здатність адаптуватися до викликів цифрової епохи. Політика інформаційної безпеки виступає ключовим елементом управління, поєднуючи захист активів, формування поведінки працівників, інтеграцію стандартів і процедур, а також вплив на організаційну культуру.

Інформація є основою операційних і стратегічних процесів організації. Її актуальність, точність і доступність визначають ефективність діяльності [1]. У логістичних компаніях, наприклад, захист даних про клієнтів і постачальників забезпечує партнерські відносини [2], тоді як у проєктному управлінні він гарантує безперервність операцій [3]. Інформація є об’єктом атак через її високу цінність, що робить її захист критичним завданням [4].

Ця цінність переводить політику інформаційної безпеки в центр управлінських процесів. Вона не лише запобігає витокам даних чи кібератакам, а й забезпечує достовірність інформації, необхідної для прийняття рішень. Наприклад, захист фінансових даних чи інноваційних розробок дозволяє організації зберігати конкурентну перевагу, тоді як втрата таких активів може призвести до репутаційних і фінансових збитків. Таким чином, політика безпеки стає інструментом, що підтримує стратегічні цілі організації.

Людський фактор відіграє вирішальну роль у забезпеченні інформаційної безпеки. 70% інцидентів безпеки пов’язані з недбалістю працівників, а 43% порушень даних спричинені їхньою поведінкою. Існує дотримання (compliance) і недотримання (noncompliance) політики, що вказують на вплив мотиваційних факторів, таких як самоефективність, і перешкод, як-от стрес від складних вимог [4]. Недостатня обізнаність команд посилює ризики в проєктному управлінні [3].

Управління організацією в цьому контексті вимагає політики, яка враховує

поведінкові аспекти. Програми підвищення обізнаності (SETA), мотиваційні тренінги та спрощення процедур, сприяють трансформації недотримання в дотримання [4]. Залучення всіх учасників до процесу безпеки, підкреслює необхідність інтеграції людського виміру в управлінські стратегії [1]. Наприклад, у віддаленій роботі працівники потребують чітких інструкцій, щоб уникати ризиків, пов’язаних із незахищеними мережами [5].

Формування культури безпеки є логічним продовженням роботи з людським фактором. Її можна визначити як продукт цінностей, компетенцій і поведінки, що залежить від стилю лідерства. Трансформаційні чи слугуючі підходи до управління знижують кількість інцидентів і підвищують залученість працівників [6]. Підтримка менеджменту та соціальні норми формують свідоме ставлення до безпеки [4].

Лідерство перетворює політику безпеки з набору правил на елемент організаційної ідентичності. Керівники, демонструючи власне дотримання стандартів і забезпечуючи ресурси, створюють середовище, де безпека є пріоритетом. У контексті віддаленої роботи це особливо важливо, адже розмиті межі робочого простору вимагають посиленої координації [5]. Таким чином, політика безпеки через лідерство стає інструментом, що об’єднує технічні та соціальні аспекти управління.

Ефективна політика безпеки базується на забезпеченні ключових атрибутів інформації: конфіденційності, цілісності та доступності. Можна підкреслити їхню важливість для логістичних компаній, де втрата даних може спричинити збої [2]. Розліковність і автентичність набувають значення в умовах дистанційної роботи [5]. Ці атрибути стають основою для управлінських рішень, координуючи дії працівників і партнерів.

Забезпечення атрибутів безпеки дозволяє організації не лише захищати дані, а й оптимізувати їх використання. Наприклад, конфіденційність комерційної інформації підтримує партнерські відносини, а доступність даних забезпечує швидке реагування на ринкові зміни. Політика безпеки, таким чином, перетворюється на інструмент, що поєднує захист із можливістю стратегічного

розвитку.

Стандарт ISO 27001 є важливим орієнтиром для створення політики безпеки. Він як рамка для систематизації управління, що сприяє проактивному підходу [5]. Він захищає активи протягом усього життєвого циклу проєкту [3].

Процесний підхід робить політику безпеки адаптивною системою. Вона включає оцінку ризиків, планування заходів і моніторинг їх виконання, що дозволяє передбачати загрози – від фішингу до кіберзлочинів у дарквебі. Також треба згадати про систему управління інформаційною безпекою (ISMS), яка інтегрує організаційні та технічні аспекти [2]. Такий підхід забезпечує гнучкість і стійкість організації в мінливому середовищі.

Сучасні організації стикаються з численними викликами в управлінні інформаційною безпекою. Також зазначають недооцінку її значення та брак ресурсів [2]. Є проблема низької обізнаності команд, та зростаючі загрози, такі як кібертероризм [1]. А також застарілі компетенції кадрів і потреба адаптації до нових технологій [6].

Ці виклики вимагають комплексного підходу. Політика безпеки має поєднувати технічні заходи, як-от шифрування чи двофакторна автентифікація, з організаційними – навчання, аудити і мотиваційні програми. Наприклад, контрольний список на основі ISO 27001 для оцінки системи безпеки [5]. Такий баланс дозволяє мінімізувати ризики, зберігаючи операційну ефективність.

Контроль і нагляд є важливими елементами політики безпеки. Контроль розрізняють як оцінку стану та нагляд як активне втручання, що застосовуються для захисту ресурсів [1]. У організаціях це проявляється у впровадженні систем моніторингу мережі, аналізу трафіку та перевірки відповідності дій працівників стандартам. Такі інструменти дозволяють виявляти порушення та оперативно реагувати на них, забезпечуючи захист комерційних даних і підтримуючи довіру стейкхолдерів.

Водночас надмірний контроль може створювати напругу. В демократичних системах він обмежується правовими рамками, що в організаціях інтерпретується як необхідність балансу між безпекою та свободою працівників

[1]. Наприклад, прозорість політики безпеки підвищує довіру, тоді як надмірне втручання може знизити мотивацію. Політика безпеки, таким чином, виступає регулятором, що визначає межі допустимого.

Політика безпеки має прямий вплив на ринкову позицію організації. Захист інформації зміцнює конкурентну перевагу, він сприяє довірі стейкхолдерів [4]. Порушення безпеки призводять до відтоку клієнтів, тоді як надійні заходи зміцнюють репутацію [3]. Можна пов’язати якісне управління безпекою з продуктивністю, посилаючись на дані OECD [6].

Ці ідеї показують, що політика безпеки є стратегічним ресурсом. Вона дозволяє безпечно впроваджувати інновації, захищаючи інтелектуальну власність і дані клієнтів. Дотримання стандартів, таких як ISO 27001, демонструє відповідальність організації, що підвищує її привабливість на ринку. Таким чином, безпека перетворюється на фактор, що сприяє розвитку та стабільності.

Інформаційна безпека є динамічним процесом, що потребує адаптації до нових умов. Необхідний моніторинг загроз, таких як кіберзлочини, рекомендують враховувати специфіку сектору для уникнення стресу від вимог [4]. У віддаленій роботі потрібні окремі процедури для захисту даних [5].

Ця гнучкість робить політику безпеки інструментом управління змінами. Вона враховує технологічні інновації, законодавчі вимоги та внутрішні потреби, дозволяючи організації залишатися стійкою в умовах цифрової трансформації. Наприклад, регулярне оновлення процедур і навчання працівників забезпечують готовність до нових викликів, таких як фішинг чи витоки даних.

Відповідність міжнародним стандартам, зокрема ISO 27001, є важливим аспектом політики безпеки. Цей стандарт систематизує управління, захищаючи активи від загроз [3]. Також треба підкреслити значення формалізованих систем для підвищення стандартів [6]. Така інтеграція дозволяє організаціям уникати санкцій і зміцнювати репутацію на міжнародному рівні.

Стандарти стають мостом між внутрішніми практиками та глобальними вимогами. Вони забезпечують проактивний підхід, що поєднує технічні заходи з організаційними змінами, такими як підвищення кваліфікації чи аудит систем.

Це робить політику безпеки частиною стратегічного управління, орієнтованого на довгостроковий успіх.

Політика інформаційної безпеки в управлінні організацією є багатогранним інструментом, що поєднує захист ресурсів, формування культури безпеки, інтеграцію стандартів і підвищення конкурентоспроможності. Вона враховує людський фактор, залежить від лідерства і адаптується до викликів цифрового світу. Забезпечуючи баланс між безпекою та свободою, гнучкістю і відповідністю стандартам, ця політика стає основою для стабільності, довіри та розвитку організації в умовах глобалізації та технологічних змін.

1.2 Нормативно-правове середовище та стандартизація

Формування політики інформаційної безпеки для організацій неможливе без чіткого розуміння нормативно-правового середовища, яке визначає вимоги до захисту інформації, а також стандартів, що забезпечують уніфікований підхід до управління безпекою. В Україні ці аспекти регулюються комплексом національних законодавчих актів, міжнародних договорів і стандартів, які разом створюють основу для ефективного захисту інформаційних активів.

Нормативно-правова база в Україні базується на Конституції України, яка встановлює фундаментальні принципи захисту інформації. Зокрема, стаття 32 гарантує недоторканність приватного життя, забороняючи збирання, зберігання чи поширення конфіденційної інформації без згоди особи, крім випадків, передбачених законом. Стаття 31 захищає таємницю комунікацій, а стаття 34 визначає межі свободи слова з урахуванням необхідності захисту даних [7]. Ці положення створюють правову основу для організацій, які розробляють політики безпеки, зобов’язуючи їх враховувати принципи конфіденційності та законності обробки інформації.

Переходячи до спеціалізованого законодавства, варто відзначити Закон України «Про інформацію» [8], який є центральним документом у регулюванні інформаційних відносин. Цей закон визначає інформацію як відомості, що

можуть бути зафіксовані у матеріальній чи електронній формі, та встановлює принципи її обігу, захисту й доступу [7]. Для організацій це означає необхідність створення внутрішніх процедур, які забезпечують безпечне зберігання, обробку та передачу даних, а також чітке визначення категорій інформації з обмеженим доступом.

Важливим елементом є Закон України «Про захист персональних даних» [9], який регулює обробку особистих даних і є особливо актуальним для організацій, що працюють із клієнтськими базами. Закон вимагає впровадження технічних і організаційних заходів для запобігання несанкціонованому доступу, а також передбачає відповідальність за порушення [7]. Це спонукає організації розробляти політики, що включають процедури шифрування, контролю доступу та навчання персоналу.

Закон України «Про національну безпеку України» [10] визначає інформаційну безпеку як складову національної безпеки, акцентуючи на захисті інформаційного простору від зовнішніх і внутрішніх загроз. Для організацій, які співпрацюють із державним сектором, цей закон встановлює додаткові вимоги до координації з органами влади та дотримання стандартів захисту критичної інфраструктури [11]. Такий підхід підкреслює важливість інтеграції корпоративних політик із державними стратегіями.

Не менш значущим є Закон України «Про державну таємницю» [12], який регулює захист інформації, що становить національну цінність. Хоча цей закон стосується переважно державних установ, організації, що беруть участь у державних проєктах, повинні враховувати його вимоги, зокрема щодо шифрування та фізичного захисту даних [7]. Це сприяє формуванню комплексного підходу до безпеки, що охоплює різні категорії інформації.

Цивільний кодекс України [13] та Господарський кодекс України [14] доповнюють правову базу, регулюючи захист комерційної таємниці. Цивільний кодекс визначає комерційну таємницю як інформацію з обмеженим доступом, що має економічну цінність, тоді як Господарський кодекс встановлює обов’язки суб’єктів господарювання щодо її захисту [7]. Для організацій це означає

необхідність розробки політик, які включають угоди про нерозголошення (NDA) та процедури моніторингу доступу до комерційно чутливих даних.

Кримінальний кодекс України, зокрема стаття 182, встановлює відповідальність за незаконне збирання чи поширення конфіденційної інформації [7]. Це створює додатковий стимул для організацій впроваджувати ефективні системи захисту, щоб уникнути юридичних і репутаційних ризиків. Таким чином, національне законодавство формує багатошарову систему вимог, які організації повинні враховувати при створенні політик інформаційної безпеки.

Оскільки інформаційні загрози мають транскордонний характер, міжнародні договори та стандарти відіграють ключову роль у формуванні політики інформаційної безпеки. Україна як учасниця Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних [15] зобов'язана забезпечувати захист персональних даних у кіберпросторі. Цей документ, розроблений Радою Європи, встановлює принципи законної обробки даних і права суб'єктів на доступ до інформації про себе [11]. Для організацій це означає необхідність адаптації політик до міжнародних вимог, зокрема щодо прозорості обробки даних і повідомлення про витоки.

Директива Європейського Парламенту і Ради (ЄС) 2016/1148 [16] щодо безпеки мережевих та інформаційних систем впливає на гармонізацію українського законодавства з європейськими нормами. Вона вимагає від організацій, що надають критичні послуги, впроваджувати заходи для забезпечення стійкості до кібератак [11]. Українські компанії, які прагнуть працювати на європейському ринку, повинні враховувати ці вимоги, включаючи їх у свої політики безпеки.

Резолюції ООН, такі як «Розвиток у галузі інформації та телекомунікацій в контексті міжнародної безпеки» [17], закликають до співпраці держав у боротьбі з кіберзагрозами. Ці документи підкреслюють важливість приватного сектору в розробці технологій захисту, що спонукає організації брати участь у міжнародних ініціативах і обміні досвідом [18]. Наприклад, співпраця з

Європейським агентством з мережевої та інформаційної безпеки (ENISA) дозволяє організаціям отримувати доступ до передових практик і стандартів.

Загальний регламент захисту даних [19], хоча й не є обов'язковим для України, слугує орієнтиром для компаній, що працюють із європейськими партнерами. GDPR встановлює принципи прозорої обробки даних, права суб'єктів на виправлення чи видалення інформації та обов'язок повідомляти про витоки даних протягом 72 годин [7]. Організації, які прагнуть відповідати цим стандартам, включають у свої політики процедури оцінки впливу на захист даних (DPIA) та призначення відповідальних за захист даних (DPO).

Співпраця з НАТО також впливає на формування політик безпеки. Річна національна програма Україна–НАТО передбачає впровадження стандартів кібербезпеки, що стосуються захисту інформаційних систем і мереж [18]. Для організацій, які співпрацюють із оборонним сектором, це означає необхідність дотримання стандартів шифрування, автентифікації та фізичної безпеки.

Стандартизація є інструментом, який забезпечує системний підхід до захисту інформації, дозволяючи організаціям уніфікувати процеси та відповідати міжнародним вимогам. Міжнародний стандарт ISO/IEC 27001 [20] є основою для створення систем управління інформаційною безпекою (СУІБ). Він передбачає оцінку ризиків, розробку політик і процедур, а також регулярний моніторинг і вдосконалення системи захисту [7]. Впровадження цього стандарту дозволяє організаціям не лише підвищити рівень безпеки, а й продемонструвати партнерам і клієнтам свою відповідність найкращим практикам.

Технічні стандарти, такі як шифрування даних і багатофакторна автентифікація, є невід'ємною частиною політики безпеки. Вони забезпечують захист інформації під час зберігання та передачі, а також допомагають запобігати несанкціонованому доступу [7]. Організації, які впроваджують ці стандарти, повинні регулярно оновлювати програмне забезпечення, проводити тестування на вразливості та навчати персонал основам кібергігієни.

Окінавська хартія глобального інформаційного суспільства [21] підкреслює важливість співпраці між державним і приватним секторами для

розвитку інформаційних технологій і захисту даних. Цей документ закликає до створення нормативної бази, яка сприяє ліквідації цифрового розриву, що є актуальним для українських організацій у контексті інтеграції в глобальний інформаційний простір [18].

Стратегія кібербезпеки України [22] акцентує на розвитку національних технологій захисту, таких як антивірусне програмне забезпечення та операційні системи. Для організацій це означає можливість використання вітчизняних рішень, які відповідають державним стандартам і сприяють підвищенню безпеки [18]. Водночас міжнародна співпраця, зокрема через участь у навчаннях і тренуваннях, дозволяє організаціям переймати передовий досвід і вдосконалювати свої політики.

Незважаючи на розвинуту нормативну базу, в Україні залишаються виклики, які ускладнюють впровадження ефективних політик інформаційної безпеки. Одним із них є застарілість окремих законодавчих норм, які не враховують сучасних кіберзагроз, таких як штучний інтелект чи розподілені атаки типу DDoS. Крім того, недостатня координація між державними органами, приватним сектором і громадськістю призводить до фрагментації зусиль у сфері безпеки [11].

Для вирішення цих проблем пропонується розробка Концепції інформаційної політики України, яка б уніфікувала підходи до регулювання інформаційного простору. Створення Національної ради України з питань комунікацій як незалежного органу могло б сприяти координації діяльності та обміну інформацією між зацікавленими сторонами [11]. Організації, зі свого боку, можуть сприяти цьому процесу, беручи участь у розробці стандартів і впроваджуючи передові технології захисту.

Фінансово-економічні заходи, такі як збільшення державного фінансування на кібербезпеку та стимулювання інвестицій у високі технології, також є важливими для організацій. Вони дозволяють створювати конкурентоспроможні системи захисту та підтримувати інновації в цій сфері [18]. Освітні ініціативи, зокрема підготовка кадрів і оновлення навчальних

програм, сприяють формуванню культури безпеки серед працівників організацій.

Нормативно-правове середовище України у сфері інформаційної безпеки формує комплексну основу для створення та впровадження політик організаціями. Конституція, спеціалізовані закони, такі як «Про інформацію» та «Про захист персональних даних», а також кодекси створюють чіткі вимоги до захисту даних і відповідальності за порушення. Міжнародні договори, зокрема Конвенція Ради Європи та директиви ЄС, гармонізують національні підходи з глобальними стандартами, що є важливим для організацій, які діють у міжнародному контексті.

Стандартизація, зокрема через впровадження ISO/IEC 27001 і технічних заходів, забезпечує системний підхід до управління безпекою. Однак виклики, пов’язані з застарілим законодавством і недостатньою координацією, вимагають подальшого вдосконалення. Організації можуть відігравати активну роль у цьому процесі, адаптуючи свої політики до сучасних вимог і беручи участь у міжнародній співпраці. Таким чином, поєднання національного законодавства, міжнародних стандартів і стратегічного підходу до стандартизації створює умови для ефективного захисту інформаційних активів і сталого розвитку організацій у цифровому середовищі.

1.3 Вимоги до політики інформаційної безпеки згідно з ISO/IEC 27001, NIST CSF та іншими стандартами

Політика інформаційної безпеки є наріжним каменем захисту інформаційних активів організацій від сучасних кіберзагроз, які охоплюють як технологічні, так і соціальні аспекти. Вона визначає цілі, процедури та заходи для забезпечення конфіденційності, цілісності й доступності інформації, гармонійно інтегруючись із бізнес-процесами. Міжнародні стандарти, зокрема ISO/IEC 27001 і NIST Cybersecurity Framework (NIST CSF), пропонують структуровані рамки для розробки такої політики, тоді як галузеві стандарти, як-от PCI DSS чи GDPR, додають специфічні вимоги.

Стандарт ISO/IEC 27001, розроблений Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), є основою для створення системи управління інформаційною безпекою. Він пропонує процесно-орієнтований підхід до управління ризиками, що робить його універсальним для організацій різного масштабу. Політика інформаційної безпеки за ISO/IEC 27001 є стратегічним документом, який окреслює цілі захисту інформації та зобов'язання організації щодо їх досягнення [23].

Першочерговою вимогою є визначення цілей безпеки, які відповідають бізнес-контексту. Політика має гарантувати конфіденційність (обмеження доступу до даних), цілісність (захист від несанкціонованих змін) і доступність (забезпечення своєчасного доступу для авторизованих користувачів). Наприклад, у державному секторі України захист реєстрів чи критичної інфраструктури може бути пріоритетом, що відображає специфіку національних викликів [24].

Залучення вищого керівництва є критично важливим. Керівництво відповідає за затвердження політики, розподіл ресурсів і контроль її виконання, що забезпечує її інтеграцію в організаційні процеси [24]. Офіційний текст стандарту підкреслює, що без підтримки топ-менеджменту СУІБ втрачає ефективність, оскільки безпека вимагає стратегічного бачення [23].

Оцінка ризиків формує основу політики. Вона передбачає ідентифікацію інформаційних активів (обладнання, програмне забезпечення, дані), аналіз загроз і вразливостей, а також вибір методів їх обробки, таких як зниження, уникнення чи передача. ISO/IEC 27001 пропонує 114 контролів для управління ризиками, наприклад, шифрування чи обмеження доступу [25]. У контексті України, де з 2014 року частота кібератак зросла на 60%, це дозволяє організаціям систематично протистояти загрозам, таким як логічні атаки чи витоки даних [24].

Контроль доступу є ще одним ключовим елементом. Політика вимагає процедур ідентифікації, автентифікації та обмеження доступу за принципом «необхідного мінімуму». Наприклад, використання багатофакторної автентифікації знижує ризик несанкціонованого доступу до чутливих систем [24]. ISO/IEC 27001 акцентує на чіткому розмежуванні прав доступу, що

особливо важливо для захисту критичних даних [26].

Обробка інцидентів включає процедури їх виявлення, реагування та аналізу для запобігання повторенню. Політика має визначати, як організація ізолюватиме уражені системи, повідомлятиме зацікавлені сторони та документуватиме інциденти. Системи управління інформацією та подіями безпеки (SIEM) є ефективними для моніторингу в реальному часі, що знижує вплив атак, таких як фішинг чи ransomware [24].

Навчання персоналу є обов'язковим для підвищення обізнаності. Стандарт вимагає регулярних тренінгів, які пояснюють ризики соціальної інженерії, важливість надійних паролів і правила поводження з конфіденційною інформацією [23]. Недостатня компетентність персоналу була основною причиною вразливостей у державному секторі, що підкреслює важливість цього аспекту [24].

Документація та аудит завершують вимоги. Політика має бути задокументованою, регулярно переглядатися та перевірятися через внутрішні й зовнішні аудити. Сертифікація ISO/IEC 27001 підтверджує відповідність стандарту, що підвищує довіру партнерів. Сертифікація є конкурентною перевагою, але вимагає значних витрат на підготовку та перевірку [25].

NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США, пропонує ризик-орієнтований підхід до кібербезпеки. Він є добровільним інструментом, який підходить для організацій із різними ресурсами завдяки своїй гнучкості. Фреймворк базується на п'яти функціях: Ідентифікація, Захист, Виявлення, Реагування та Відновлення, які формують цикл управління безпекою [26].

Функція «Ідентифікація» вимагає від політики інвентаризації активів і оцінки ризиків. Організація має класифікувати дані та системи за критичністю, аналізуючи загрози, такі як кібератаки чи апаратні збої. Цей етап дозволяє визначити пріоритети захисту, наприклад, для інформаційних систем критичної інфраструктури України [24]. NIST CSF використовує профілі безпеки для оцінки прогресу, що допомагає організаціям виявляти прогалини [26].

«Захист» передбачає впровадження технічних і організаційних заходів. Політика має включати шифрування, брандмауери, антивірусне програмне забезпечення та контроль доступу. NIST CSF дозволяє адаптувати ці заходи до рівня зрілості організації, що робить його доступним для малого бізнесу чи державних установ із обмеженим бюджетом [25].

«Виявлення» зосереджене на моніторингу подій. Політика має передбачати використання систем, таких як SIEM, для аналізу аномалій, що вказують на інциденти. NIST CSF пропонує 108 підкатегорій для деталізації заходів, що забезпечує гнучкість у виборі інструментів [26]. У державному секторі України це дозволяє своєчасно реагувати на атаки, наприклад, DDoS, які стали частішими [24].

«Реагування» включає плани дій на випадок інцидентів, такі як ізоляція систем чи повідомлення зацікавлених сторін. «Відновлення» зосереджене на поверненні до нормального функціонування через резервне копіювання та тестування процедур. Ці функції є критично важливими для забезпечення безперервності державних функцій після кібератак [24].

NIST CSF не передбачає сертифікації, що знижує витрати порівняно з ISO/IEC 27001. Це робить фреймворк привабливим для організацій, які прагнуть швидкої адаптації до загроз, але його ефективність залежить від внутрішньої експертизи [25].

Поряд із універсальними рамками ISO/IEC 27001 і NIST CSF, які охоплюють широкий спектр аспектів кібербезпеки, галузеві стандарти, такі як PCI DSS і GDPR, додають специфічні вимоги до політики інформаційної безпеки. Вони зосереджені на захисті певних типів даних, таких як фінансові чи персональні, і є обов’язковими для організацій, що працюють у відповідних секторах. Ці стандарти є важливим доповненням до основних фреймворків, що дозволяє створювати політики, які відповідають як глобальним, так і локальним вимогам [24].

PCI DSS (Payment Card Industry Data Security Standard) регулює захист даних банківських карток і є обов’язковим для компаній, що обробляють платіжні

транзакції. Політика інформаційної безпеки за PCI DSS має включати кілька ключових заходів. По-перше, це встановлення мережевих екранів для ізоляції критичних систем від зовнішніх загроз, що знижує ризик атак на фінансові дані. По-друге, відмова від стандартних паролів і впровадження надійних методів автентифікації, таких як складні паролі чи двофакторна автентифікація. По-третє, шифрування даних під час їх передачі та зберігання для запобігання перехопленню чи витокам. Крім того, політика вимагає регулярного тестування безпеки, наприклад, сканування вразливостей, і моніторингу доступу до інформації для виявлення підозрілих дій. PCI DSS є вузьконаправленим стандартом, але його вимоги до технічного захисту перетинаються з ISO/IEC 27001, зокрема в контролі доступу та шифруванні [25]. Для українських компаній, які активно розвивають електронну комерцію, ці заходи є критично важливими для забезпечення довіри клієнтів і відповідності міжнародним стандартам [24].

GDPR (General Data Protection Regulation) фокусується на захисті персональних даних громадян Європейського Союзу, але його принципи застосовуються до будь-якої організації, що обробляє такі дані. Політика за GDPR має забезпечувати прозорість обробки інформації, що передбачає чітке інформування користувачів про цілі та методи використання їхніх даних. Вона також включає процедури отримання згоди, наприклад, через явне підтвердження, і захист прав суб’єктів даних, таких як право на доступ, виправлення чи видалення інформації. GDPR перетинається з ISO/IEC 27001 у вимогах до управління активами, але додає юридичні аспекти, такі як призначення відповідальної особи за захист даних (Data Protection Officer) у певних випадках [26]. Однією з ключових вимог є повідомлення про витоки даних протягом 72 годин, що потребує чітких процедур реагування в політиці. У контексті України, де співпраця з європейськими партнерами зростає, відповідність GDPR стає конкурентною перевагою, що дозволяє організаціям зміцнити свою репутацію на міжнародному ринку [24].

Інші стандарти, такі як *COBIT 2019*, також можуть впливати на політику

інформаційної безпеки, особливо в державному секторі. COBIT пропонує шаблони для оцінки ризиків і управління інформаційними системами, що доповнює підходи ISO/IEC 27001 і NIST CSF. Галузеві стандарти можуть посилювати універсальні фреймворки, створюючи більш адаптовану політику.

Аналіз ISO/IEC 27001, NIST CSF, PCI DSS, GDPR і COBIT дозволяє виділити спільні принципи, які формують основу ефективної політики інформаційної безпеки. Ці принципи забезпечують її комплексність і універсальність, дозволяючи організаціям адаптувати політику до своїх потреб, зберігаючи ключові аспекти захисту.

Першим спільним принципом є орієнтація на управління ризиками. Усі стандарти вимагають ідентифікації інформаційних активів, оцінки загроз і вразливостей, а також вибору заходів для їх зниження. ISO/IEC 27001 пропонує структурований підхід із 114 контролями, NIST CSF використовує профілі безпеки для пріоритизації, а PCI DSS і GDPR додають вимоги до захисту фінансових і персональних даних [25; 26]. У державному секторі України цей принцип є особливо актуальним через зростання геополітичних кіберзагроз, таких як атаки на критичну інфраструктуру [24].

Другим принципом є акцент на навчанні персоналу. Людина залишається найслабшою ланкою в системі безпеки, тому стандарти наголошують на регулярних тренінгах. ISO/IEC 27001 включає програми підвищення обізнаності, NIST CSF визначає категорію PR.AT (Awareness and Training), PCI DSS вимагає навчання підрядників, а GDPR акцентує на розумінні прав суб’єктів даних [23; 26].

Третім спільним приципом є документація та регулярний перегляд. Політика має бути задокументованою, із чіткими процедурами, ролями та обов’язками. ISO/IEC 27001 використовує модель PDCA (Plan-Do-Check-Act) для постійного вдосконалення, NIST CSF пропонує циклічний підхід, а GDPR і PCI DSS вимагають доказів відповідності через журнали чи аудити [23; 25]. У контексті України це дозволяє організаціям відповідати як міжнародним стандартам, так і національним вимогам, наприклад, КСЗІ (Комплексній системі

захисту інформації) [24].

Четвертим принципом є інтеграція з бізнес-процесами. Політика не повинна обмежувати операційну діяльність, а має підтримувати її, мінімізуючи ризики. ISO/IEC 27001 наголошує на залученні керівництва, NIST CSF адаптує заходи до бізнес-середовища, PCI DSS враховує специфіку транзакцій, а GDPR забезпечує баланс між захистом даних і правами користувачів [26; 24]. Такий підхід дозволяє організаціям зберігати ефективність, одночасно підвищуючи безпеку.

Ці спільні принципи створюють міцну основу для політики, яка може бути адаптована до різних стандартів і організаційних контекстів, забезпечуючи комплексний захист інформації.

Незважаючи на спільні риси, стандарти мають суттєві відмінності, які впливають на формування політики інформаційної безпеки. Ці відмінності стосуються методології, рівня формалізації, витрат і цільової аудиторії, що дає організаціям змогу вибирати оптимальний підхід.

ISO/IEC 27001 використовує процесно-орієнтований підхід, зосереджений на створенні СУІБ із чіткою структурою. Політика є частиною системи, яка включає документацію, аудити та можливість сертифікації. Це робить стандарт ідеальним для організацій, які прагнуть формалізувати процеси, наприклад, державних установ чи великих корпорацій. Впровадження ISO/IEC 27001 може бути витратним через необхідність оплати документів і сертифікаційних аудитів [25]. Офіційний текст стандарту підтверджує, що сертифікація вимагає ретельної підготовки, але підвищує довіру партнерів [23].

NIST CSF, навпаки, є ризик-орієнтованим і гнучким, дозволяючи організаціям зосередитися на пріоритетних загрозах без обов’язкової сертифікації. Політика формується через профілі безпеки, які порівнюють поточний і цільовий стан, що допомагає виявити прогалини. 108 підкатегорій NIST CSF забезпечують деталізацію заходів, що підходить для організацій із різним рівнем зрілості [26]. Відсутність витрат на сертифікацію робить фреймворк доступним, але його ефективність залежить від внутрішньої

експертизи [25]. У контексті України NIST CSF є цінним для швидкої оцінки ризиків у державному секторі, де ресурси часто обмежені [24].

PCI DSS і GDPR є спеціалізованими стандартами. PCI DSS зосереджений на захисті фінансових даних, вимагаючи чітких технічних заходів, таких як шифрування та тестування безпеки. GDPR акцентує на юридичних аспектах, зокрема на прозорості обробки даних і реагуванні на витоки. Обидва стандарти передбачають суворі штрафи за невідповідність, що підвищує їхню значущість. Ці стандарти доповнюють ISO/IEC 27001 і NIST CSF, додаючи галузеві вимоги, які можна інтегрувати в універсальну політику [26].

COBIT, хоч і не є основним стандартом безпеки, пропонує інструменти для оцінки ризиків, що посилюють інші фреймворки. COBIT допоміг ідентифікувати вразливості в державному секторі, такі як низька компетентність персоналу, що можна врахувати в політиці [24].

Ці відмінності дозволяють організаціям обирати стандарти залежно від їхніх цілей. Наприклад, фінансова установа може поєднувати ISO/IEC 27001 і PCI DSS, тоді як IT-компанія, що працює з європейськими клієнтами, інтегруватиме GDPR і NIST CSF.

Політика інформаційної безпеки, розроблена на основі ISO/IEC 27001, NIST CSF, PCI DSS, GDPR і COBIT, є комплексним інструментом для захисту інформаційних активів. ISO/IEC 27001 пропонує структуровану систему з можливістю сертифікації, що ідеально підходить для формалізації процесів. NIST CSF забезпечує гнучкість і ризик-орієнтований підхід, що дозволяє швидко реагувати на загрози. PCI DSS і GDPR додають галузеві вимоги, тоді як COBIT посилює аналіз ризиків. У контексті України, де кіберзагрози мають як технологічний, так і геополітичний характер, інтеграція цих стандартів дозволяє створювати політики, які захищають критичну інфраструктуру, підвищують довіру партнерів і забезпечують безперервність бізнес-процесів. Регулярне оновлення, навчання персоналу та пріоритизація ризиків є ключовими для забезпечення ефективності політики в сучасних умовах.

1.4 Аналіз сучасних загроз та ризиків, які враховуються при розробці політики інформаційної безпеки

Розробка політики інформаційної безпеки (ІБ) для організацій є складним і багатогранним процесом, що потребує врахування сучасних загроз і ризиків, які постійно еволюціонують у технологічному, екологічному та геополітичному середовищах. Ці загрози охоплюють як традиційні кібератаки, так і нові виклики, пов’язані з квантовими обчисленнями, кліматичними змінами та каскадними ефектами в інформаційних системах. Аналіз таких загроз є ключовим етапом для забезпечення конфіденційності, цілісності та доступності інформації, а також для створення стійкої системи захисту критичної інфраструктури.

Сучасний ландшафт кіберзагроз характеризується високою динамікою та зростаючою складністю атак. Критична інфраструктура, що включає енергетику, транспорт, фінанси, телекомунікації та охорону здоров’я, є основною мішенню для кібератак через її залежність від цифрових технологій. У 2024 році в Україні зафіксовано 3 мільйони подій ІБ, з яких 28 000 класифіковано як критичні, що свідчить про масштабність проблеми [27]. Основними типами загроз є:

- програми-вимагачі (Ransomware), які шифрують дані з вимаганням викупу, становлять значну небезпеку для державного сектору (20%) та бізнес-послуг (19%). Їх поширення пов’язане з доступністю інструментів для атак на чорному ринку;
- DDoS-атаки, спрямовані на перевантаження інфраструктури, є провідною загрозою в державному секторі (33%) та транспорті (21%). Геополітична напруженість, зокрема російсько-український конфлікт, сприяє їх масштабуванню;
- шкідливе програмне забезпечення (Malware), таке як трояни RedLine та Vidar, становить 25% загроз у цифровій інфраструктурі, викрадаючи конфіденційні дані;
- соціальна інженерія та фішинг, що маніпулюють користувачами для отримання доступу, домінують у фінансовому секторі (25%);

– атаки на ланцюги постачання, які уражають організації через компрометацію постачальників, набули поширення в бізнес-послугах (15%).

– інформаційно-психологічні операції, такі як поширення дезінформації, посилюють вплив кібератак у контексті гібридних війн;

Ці загрози реалізуються через вразливості, ідентифіковані за стандартами CVE, CVSS та CWE. У 2024 році зафіксовано 19 754 вразливості, з яких 9,3% класифіковано як критичні, а 21,8% – як високі. Найпоширенішими є міжсайтовий скриптинг (XSS, 22,68%), SQL-ін'єкції (9,32%) та міжсайтове підроблення запитів (CSRF, 6,28%) (рис.1.1.) [27]. Це вказує на необхідність посилення валідації даних і захисту мережевих систем.

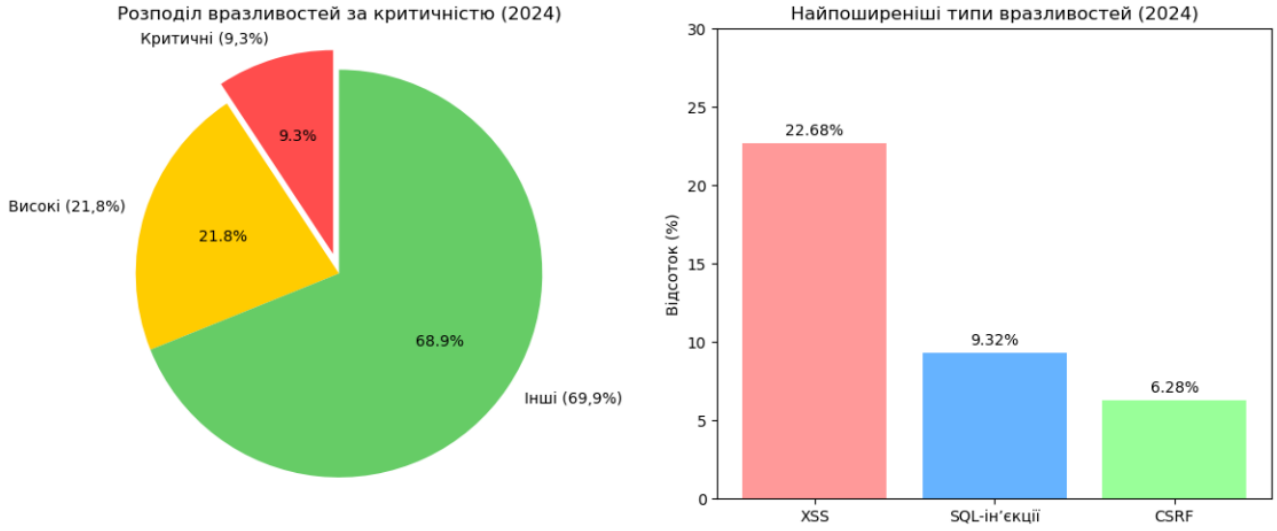

Рис.1.1. Розподіл вразливостей за критичністю та типами

Переходячи до аудіовізуальних мереж, які є специфічним типом інформаційних систем, варто відзначити їх унікальні вразливості. Такі мережі другого та третього класів, що обробляють дані різної конфіденційності, стикаються з загрозами несанкціонованого доступу (НСД), комп'ютерних вірусів, апаратних збоїв, навмисного перекручування даних і передачі інформації через незахищені канали [28]. Ці загрози посилюються через використання багатокористувацьких систем і відкритих середовищ передавання даних, що вимагає спеціалізованих підходів до захисту.

Розвиток квантових обчислень відкриває нові горизонти для ІБ, але водночас створює серйозні виклики. Традиційні криптографічні протоколи, такі як RSA, ECC та DSA, є вразливими до квантових алгоритмів Шора та Гровера, які здатні компрометувати ці системи за лічені хвилини [29]. Це загрожує безпеці фінансових транзакцій, урядових комунікацій та систем Інтернету речей (IoT). Наприклад, квантовий аналіз даних може прискорити атаки на цифрові підписи, що використовуються в банківських системах.

З іншого боку, квантові технології пропонують рішення, такі як квантовий розподіл ключів (QKD), що забезпечує стійкі до зламів канали зв'язку. Проте впровадження таких технологій вимагає значних інвестицій і перебудови інфраструктури. Для оцінки впливу постквантового середовища Прокопович-Ткаченко пропонує емерджентно-адаптивний метод, який включає ідентифікацію загроз, моделювання атак, оцінку вразливостей, аналіз критичних точок і впровадження постквантових рішень, таких як решіткові алгоритми чи кодові конструкції [29]. Цей підхід дозволяє організаціям прогнозувати квантові загрози та розробляти гібридні протоколи, що поєднують класичні та постквантові механізми.

Квантові ризики мають каскадний ефект, коли компрометація одного елемента системи може призвести до збоїв у всій інфраструктурі. Наприклад, порушення безпеки фінансової системи через квантову атаку може спричинити ланцюгову реакцію, що вплине на економічну стабільність [29]. Це підкреслює необхідність включення постквантових стратегій у політику ІБ, особливо для організацій, що відповідають за критичну інфраструктуру.

Традиційний підхід до ІБ зосереджувався на технологічних аспектах, але сучасні виклики вимагають розширення цього погляду. Кліматичні зміни, такі як екстремальні погодні явища (шторми, повені, лісові пожежі), безпосередньо впливають на критичну інфраструктуру, включаючи інформаційні системи [30]. Наприклад, перебої в електропостачанні чи пошкодження серверних центрів через природні катастрофи можуть призвести до втрати даних або порушення доступності систем.

Екологічні зміни також мають геополітичні та структурні наслідки. Геополітичні конфлікти, спричинені кліматичною міграцією чи боротьбою за ресурси, ускладнюють міжнародну співпрацю у сфері кібербезпеки. Наприклад, санкції можуть обмежити доступ до технологій, необхідних для захисту інформації. Структурні зміни, пов’язані з переходом до низьковуглецевої економіки, створюють нові вразливості, такі як залежність від технологій акумуляторів чи відновлюваних джерел енергії, які можуть бути мішенями для кібератак [30].

Для організацій це означає необхідність інтеграції екологічних ризиків у політику ІБ. Наприклад, розробка планів аварійного відновлення, що враховують природні катастрофи, є критично важливою. Крім того, аналіз каскадних ефектів, коли екологічна подія викликає збої в інформаційних системах, допомагає передбачити опосередковані наслідки та мінімізувати їх вплив.

Аналіз ризиків є центральним елементом розробки політики ІБ, оскільки він дозволяє ідентифікувати загрози, оцінити вразливості та визначити потенційні збитки. Є два підходи до аналізу ризиків: базовий і повний. Базовий аналіз фокусується на стандартних загрозах (віруси, НСД, апаратні збої) і підходить для систем із низькою критичністю даних. Повний аналіз, який включає оцінку цінності ресурсів, аналіз загроз і вразливостей, а також вибір контрзаходів, є необхідним для мереж із високими вимогами до безпеки.

Типовий алгоритм аналізу ризиків передбачає:

- дослідження архітектури системи та її функціональних задач;
- побудову моделей цінності, вразливостей і порушників;
- розробку моделі загроз;
- оцінку ризиків із визначенням контрзаходів;
- формулювання політики безпеки;

Цей процес дозволяє економічно обґрунтувати витрати на захист, співставивши їх із потенційними збитками [28].

У контексті ширшої інфраструктури пропонується інструмент Матриці оцінки тем контролю (МОТК), який використовується для стандартизованої

оцінки ризиків. МОТК враховує вплив на державу, фінансові наслідки, інтереси громадян, рівень корупційних ризиків та актуальність проблеми. У 2023–2024 роках цей інструмент застосовано до оцінки 174 тем, що підтвердило його ефективність у пріоритизації заходів [31]. Такі методи можуть бути адаптовані для організацій, що розробляють політику ІБ, забезпечуючи об'єктивний підхід до управління ризиками.

Сучасні загрози характеризуються каскадними ефектами, коли компрометація одного компонента системи призводить до збоїв у всій інфраструктурі. У постквантовому середовищі це може стосуватися порушення фінансових систем через квантову атаку [29]. У контексті екологічних загроз каскадні ефекти пов'язані з геополітичними факторами чи глобальними ланцюгами поставок [30]. Наприклад, збій у постачанні енергії через кліматичну подію може порушити роботу серверів, що вплине на доступність даних.

Для протидії таким ризикам необхідна міжсекторальна взаємодія. Модель комплексної безпеки у Фінляндії передбачає співпрацю між державними установами, бізнесом і громадськими організаціями, але на практиці ця взаємодія обмежується традиційними секторами [30]. Організації повинні розробляти політику, яка сприяє інтеграції експертизи з кібербезпеки, екології та енергетики, створюючи цілісний підхід до управління ризиками.

Ефективна політика ІБ має бути орієнтованою на довгострокове прогнозування. Можна використовувати штучний інтелект та форсайт-аналіз для передбачення квантових загроз на 5–10 років [29]. Також важливе проактивне планування для підготовки до екологічних ризиків, хоча короткострокові цілі часто домінують [30]. Для організацій це означає необхідність впровадження самонавчальних систем, які автоматично реагують на нові загрози, та стандартів постквантової безпеки.

Сучасні загрози та ризики, які необхідно враховувати при розробці політики ІБ, є багатогранними та охоплюють технологічні, екологічні та геополітичні аспекти. Традиційні кіберзагрози, такі як програми-вимагачі, DDoS-атаки та фішинг, залишаються актуальними, але їх доповнюють нові виклики,

пов’язані з квантовими обчисленнями та кліматичними змінами. Аналіз ризиків, включаючи базовий і повний підходи, дозволяє ідентифікувати вразливості та обґрунтувати контрзаходи. Каскадні ефекти та недостатня міжсекторальна співпраця підкреслюють необхідність комплексного підходу, який поєднує експертизу з різних галузей. Проактивне прогнозування та адаптивність є ключовими для забезпечення стійкості організацій у динамічному середовищі.

Висновки до розділу 1

Аналіз рекомендацій до створення та впровадження політики інформаційної безпеки для організацій є ключовим елементом управління інформаційними активами в умовах сучасних кіберзагроз. Проведений аналіз охоплює роль політики ІБ в організаційному управлінні, нормативно-правове середовище, вимоги міжнародних стандартів, таких як ISO/IEC 27001 і NIST CSF, а також сучасні загрози та ризики, які необхідно враховувати при розробці політики. Ці аспекти формують комплексну основу для розуміння важливості системного підходу до забезпечення інформаційної безпеки.

Політика інформаційної безпеки відіграє стратегічну роль у забезпеченні стабільності та конкурентоспроможності організацій. Вона не лише захищає інформаційні активи від кібератак і витоків даних, але й сприяє формуванню культури безпеки, інтеграції стандартів і процедур, а також оптимізації управлінських процесів. Особлива увага приділяється людському фактору, оскільки 70% інцидентів безпеки пов’язані з недбалістю працівників. Програми підвищення обізнаності, мотиваційні тренінги та лідерство, що демонструє дотримання стандартів, є необхідними для трансформації поведінки персоналу. Крім того, політика ІБ забезпечує ключові атрибути інформації – конфіденційність, цілісність і доступність, – що є основою для ефективного прийняття рішень і підтримки партнерських відносин. Таким чином, вона стає інструментом, який поєднує захист ресурсів із можливістю стратегічного розвитку.

Нормативно-правове середовище в Україні формує чіткі вимоги до створення політики ІБ, базуючись на Конституції, законах про інформацію, захист персональних даних, національну безпеку та державну таємницю. Ці документи встановлюють принципи конфіденційності, законності обробки даних і відповідальності за порушення. Міжнародні договори, такі як Конвенція Ради Європи та директиви ЄС, гармонізують українське законодавство з глобальними стандартами, що є важливим для організацій, які працюють на міжнародному ринку. Однак застарілість окремих норм і недостатня координація між секторами створюють виклики, які потребують уніфікації підходів і вдосконалення законодавства. Стандартизація, зокрема через ISO/IEC 27001, забезпечує системний підхід до управління безпекою, дозволяючи організаціям демонструвати відповідність найкращим практикам.

Міжнародні стандарти ISO/IEC 27001 і NIST CSF пропонують структуровані рамки для розробки політики ІБ, які враховують управління ризиками, навчання персоналу, документацію та інтеграцію з бізнес-процесами. ISO/IEC 27001 акцентує на створенні системи управління інформаційною безпекою з можливістю сертифікації, що ідеально підходить для великих організацій. NIST CSF, завдяки своїй гнучкості та ризик-орієнтованому підходу, є доступним для організацій з обмеженими ресурсами. Галузеві стандарти, такі як PCI DSS і GDPR, додають специфічні вимоги до захисту фінансових і персональних даних, що дозволяє створювати адаптовані політики. Спільні принципи стандартів – орієнтація на ризики, навчання, документація та інтеграція – забезпечують комплексний захист, тоді як їх відмінності дають змогу організаціям обирати оптимальний підхід залежно від цілей і ресурсів.

Сучасні кіберзагрози, такі як програми-вимагачі, DDoS-атаки, фішинг і атаки на ланцюги постачання, характеризуються високою складністю та каскадними ефектами, що можуть порушити роботу всієї інфраструктури. У 2024 році в Україні зафіксовано значне зростання інцидентів, зокрема через геополітичну напруженість. Нові виклики, пов’язані з квантовими обчисленнями, загрожують традиційним криптографічним протоколам, що

вимагає впровадження постквантових рішень. Екологічні загрози, такі як кліматичні зміни, додають ризиків через перебої в електропостачанні чи пошкодження інфраструктури, що підкреслює необхідність їх інтеграції в політику ІБ. Аналіз ризиків, включаючи базовий і повний підходи, дозволяє ідентифікувати вразливості та обґрунтувати контрзаходи, тоді як міжсекторальна співпраця сприяє цілісному управлінню ризиками.

Отже, створення політики інформаційної безпеки вимагає комплексного підходу, який поєднує організаційні, технічні та правові аспекти. Вона має бути адаптивною до динамічних загроз, враховувати специфіку організації та відповідати міжнародним і національним стандартам. Проведений аналіз демонструє, що ефективна політика ІБ не лише захищає інформаційні активи, але й сприяє підвищенню конкурентоспроможності, довіри стейкхолдерів і стійкості організації в умовах цифрової трансформації.

Розділ 2 ДОСЛІДЖЕННЯ МЕТОДІВ СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Процес розробки політики інформаційної безпеки: ключові етапи та підходи

Політика інформаційної безпеки є фундаментальним елементом системи управління інформаційною безпекою, що забезпечує захист інформаційних активів організації від широкого спектра загроз, включаючи кібератаки, внутрішні порушення та технологічні збої. Розробка політики ІБ ґрунтується на міжнародних стандартах, зокрема ISO/IEC 27001, і враховує психологічні та соціальні детермінанти поведінки працівників, які суттєво впливають на ефективність політики. У контексті сучасних викликів, таких як еволюція кіберзагроз і ресурсні обмеження, розробка політики ІБ вимагає системного підходу, що поєднує технічні, організаційні та поведінкові аспекти.

Початковий етап розробки політики ІБ полягає в ідентифікації та класифікації інформаційних активів, які становлять основу функціонування організації. До таких активів належать фізичні ресурси (сервери, робочі станції), програмне забезпечення (системи управління базами даних, аналітичні платформи), інформаційні ресурси (персональні дані, комерційна таємниця) та нематеріальні активи (репутація, інтелектуальна власність). Згідно з вимогами стандарту ISO/IEC 27001, ідентифікація активів є передумовою для оцінки ризиків, оскільки визначає об’єкти, що підлягають захисту [20].

Цей етап передбачає інвентаризацію активів і їх класифікацію за критеріями критичності, чутливості та цінності. Наприклад, у фінансових установах клієнтські бази даних є висококритичними через їхню вразливість до кібератак і потенційні наслідки витоків. Чітка ідентифікація активів забезпечує основу для аналізу загроз і розробки стратегій захисту [31]. Водночас людський фактор відіграє вирішальну роль, адже, за даними досліджень, до 70% інцидентів безпеки спричинені недбалістю працівників [4]. Таким чином, цей етап не лише

формує технічну базу для політики, а й враховує поведінкові ризики, пов’язані з персоналом.

Наступний етап передбачає систематичний аналіз потенційних загроз для ідентифікованих інформаційних активів. Загрози можуть мати зовнішній (кібератаки, такі як фішинг чи DDoS) або внутрішній характер (помилки персоналу, навмисні порушення). Можна зробити класифікацію ризиків за джерелами, виділяючи ринкові, операційні, юридичні, фінансові та стратегічні ризики, з особливим акцентом на кіберзагрози, що домінують у цифровізованому середовищі [33].

ISO/IEC 27001 вимагає оцінки ймовірності реалізації загроз і їхнього впливу, що дозволяє визначити пріоритети захисту [20]. Дослідження показують, що 58% кібератак у організаціях спричинені внутрішніми загрозами, з яких 33% пов’язані з недотриманням політики безпеки через психологічні бар’єри, такі як стрес або низька обізнаність [4]. Наприклад, працівники можуть ігнорувати правила через перевантаження інформацією чи недооцінку ризиків. Цей етап завершується складанням детального переліку загроз, що є основою для подальшої оцінки ризиків і розробки контрзаходів.

Третій етап зосереджений на оцінці ймовірності реалізації загроз і потенційного впливу на діяльність організації. Цей процес включає аналіз вразливостей, визначення можливих сценаріїв інцидентів і оцінку їхніх наслідків, таких як фінансові втрати, репутаційні збитки чи зупинка бізнес-процесів. Оцінка ризиків дозволяє раціонально розподілити ресурси, зосередивши зусилля на найбільш критичних загрозах [32].

ISO/IEC 27001 пропонує структурований підхід до оцінки ризиків, який включає ідентифікацію вразливостей, вибір методів їх обробки (зниження, уникнення, передача) і розробку контрзаходів [20]. Психологічні чинники, такі як сприйняття загрози (threat appraisal) і здатність справлятися з нею (coping appraisal), суттєво впливають на оцінку ризиків працівниками, що може ускладнити впровадження політики [4]. Наприклад, недооцінка серйозності фішингових атак підвищує ймовірність порушень. Цифрові технології, такі як

аналітичні платформи, сприяють автоматизації аналізу ризиків, підвищуючи його точність [33]. Результатом цього етапу є визначення пріоритетних ризиків, які формують стратегічний напрям політики ІБ.

Четвертий етап передбачає розробку та впровадження комплексу контрзаходів для захисту інформаційних активів. Згідно з ISO/IEC 27001, ці заходи поділяються на технічні (шифрування, міжмережні екрани, системи багатофакторної автентифікації), організаційні (політики доступу, програми навчання) та юридичні (дотримання нормативно-правових вимог) [20]. Повинен бути принцип найменших привілеїв, який обмежує доступ до інформації лише необхідним обсягом, мінімізуючи внутрішні ризики [32].

Впровадження цифрових технологій, таких як системи Інтернету речей (IoT) чи SIEM, забезпечує моніторинг загроз у реальному часі, але супроводжується викликами, такими як високі витрати та недостатня цифрова компетентність персоналу [33]. Програми підвищення обізнаності (Security Education, Training, and Awareness, SETA) відіграють ключову роль у формуванні культури безпеки, знижуючи ймовірність порушень через людський фактор [4]. Наприклад, симуляція кібератак у рамках SETA допомагає працівникам розпізнавати фішингові спроби. Цей етап завершується формалізацією політики ІБ у вигляді задокументованих процедур, ролей і відповідальностей.

Останній етап передбачає безперервний моніторинг ефективності політики ІБ і її адаптацію до нових загроз і організаційних потреб. ISO/IEC 27001 використовує модель PDCA для забезпечення циклічного вдосконалення СУІБ (рис. 2.1.), що включає планування, виконання, перевірку та коригування заходів [20]. Моніторинг здійснюється через внутрішні аудити, аналіз логів безпеки за допомогою систем SIEM і оцінку поведінки працівників.

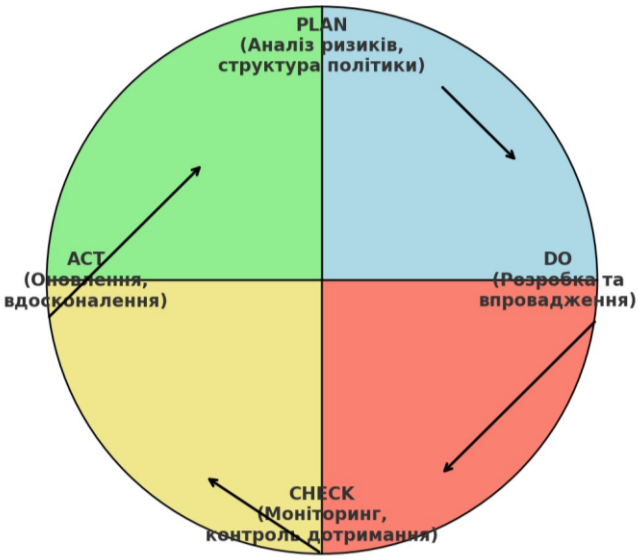

Рис.2.1. Цикл PDCA

Важливі автоматизовані інструменти моніторингу, які дозволяють виявляти аномалії в реальному часі, підвищуючи оперативність реагування [33]. Психологічні фактори, такі як стрес від складних вимог безпеки, можуть знижувати рівень дотримання політики, що вимагає регулярного зворотного зв'язку від персоналу [4]. Наприклад, адаптація процедур до нових видів атак, таких як програми-вимагачі, забезпечує актуальність політики. Цей етап гарантує, що політика залишається динамічним інструментом, здатним відповідати сучасним викликам.

Формування політики ІБ ґрунтується на кількох теоретичних підходах, які забезпечують її системність і ефективність (рис. 2.2.):

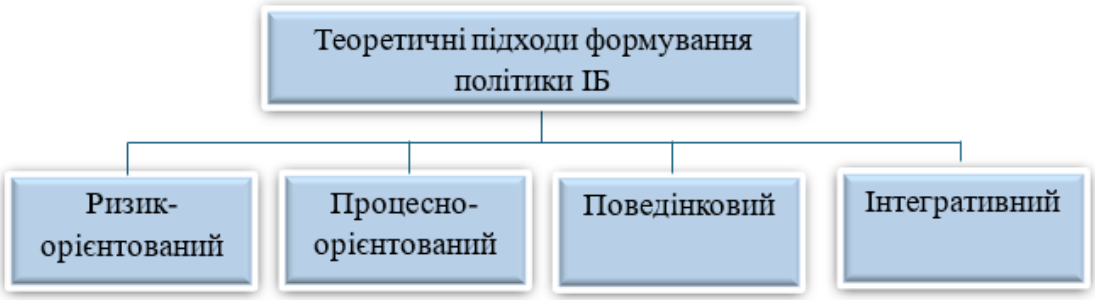

Рис. 2.2. Теоретичні підходи формування політики ІБ

– ризик-орієнтований підхід передбачає ідентифікацію, оцінку та управління ризиками як основу політики, що дозволяє оптимізувати ресурси та зосередитися на критичних загрозах;

– процесно-орієнтований підхід заснований на стандарті ISO/IEC 27001, він систематизує управління через чітку документацію, регулярні аудити та структуровані процедури [20];

– поведінковий підхід враховує психологічні та соціальні детермінанти поведінки працівників, використовуючи програми SETA для підвищення обізнаності та мотивації [4];

– інтегративний підхід забезпечує гармонійну інтеграцію політики в бізнес-процеси, балансуючи між вимогами безпеки та операційною ефективністю [32];

Ці підходи формують комплексну методологічну основу, що поєднує технічні, організаційні та соціальні аспекти політики ІБ.

Ефективність політики ІБ значною мірою залежить від поведінки працівників, яка формується під впливом психологічних і соціальних факторів. Виділяють кілька ключових детермінант:

– внутрішня мотивація, яка заснована на особистих цінностях і самоповазі, має більший вплив на дотримання політики порівняно із зовнішньою мотивацією, такою як покарання чи винагороди. Теорія мотивації захисту (Protection Motivation Theory, PMT) показує, що працівники, які сприймають загрози як серйозні та вважають себе здатними їх нейтралізувати, демонструють вищий рівень відповідності;

– організації з розвиненою культурою безпеки, що підтримується регулярними програмами SETA, мають нижчий рівень порушень. Тренінги та симуляції сприяють формуванню свідомого ставлення до безпеки;

– норми поведінки колег і демонстрація дотримання політики керівництвом суттєво впливають на мотивацію працівників. Наприклад, активна підтримка політики менеджментом підвищує її легітимність в очах персоналу;

– до основних причин недотримання належать стрес від складних вимог безпеки (security-related stress), конфлікти цінностей (наприклад, пріоритет продуктивності над безпекою) та техніки нейтралізації, такі як заперечення відповідальності чи шкоди.

Запропонована модель трансформації поведінки від недотримання до дотримання включає ідентифікацію причин порушень, впровадження мотиваційних стратегій, формування культури безпеки, застосування стримувальних заходів і регулярний моніторинг [4]. Цей підхід забезпечує комплексне управління поведінковими ризиками.

Розробка політики ІБ стикається з низкою сучасних викликів, які обумовлюють її адаптивність і ефективність (рис.2.3.).

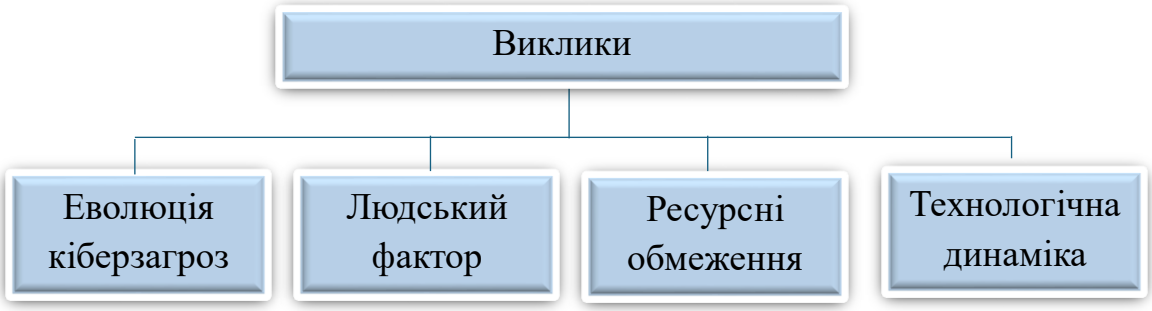

Рис. 2.3. Сучасні виклики при розробці політики ІБ

Швидка трансформація загроз, таких як програми-вимагачі чи атаки на ланцюги постачання, вимагає постійного оновлення політики для забезпечення її актуальності [33].

Низька обізнаність, психологічний стрес і недостатня мотивація працівників ускладнюють дотримання політики, що потребує посилення освітніх програм [4].

Обмежений бюджет, особливо в українських організаціях, перешкоджає впровадженню сучасних технологій захисту, таких як системи SIEM чи IoT [32].

Стрімкий розвиток технологій, зокрема штучного інтелекту та Інтернету речей, створює нові вразливості, які необхідно враховувати при розробці політики [33].

Для подолання цих викликів рекомендується поєднання автоматизованих систем моніторингу, мотиваційних програм для персоналу та адаптації політики до специфіки організації й сучасних стандартів.

Розробка політики інформаційної безпеки є багатогранним процесом, що охоплює п’ять ключових етапів: ідентифікацію та класифікацію активів, аналіз загроз, оцінку ризиків, впровадження контрзаходів і моніторинг. Ці етапи ґрунтуються на стандарті ISO/IEC 27001 і враховують психологічні та соціальні детермінанти поведінки працівників, які відіграють вирішальну роль у забезпеченні ефективності політики. Ризик-орієнтований, процесно-орієнтований, поведінковий та інтегративний підходи створюють методологічну основу для формування політики, що захищає інформаційні активи й підтримує стратегічні цілі організації. Психологічні чинники, такі як мотивація й культура безпеки, а також соціальний вплив, є ключовими для трансформації поведінки від недотримання до відповідності. Сучасні виклики, включаючи еволюцію кіберзагроз, ресурсні обмеження та технологічну динаміку, вимагають гнучкості політики та використання передових технологій. Таким чином, ефективна політика ІБ є не лише інструментом захисту, а й стратегічним ресурсом, що сприяє конкурентоспроможності та сталому розвитку організації в умовах цифрової трансформації.

2.2. Роль управління ризиками у формуванні політики інформаційної безпеки

Управління ризиками (УР) відіграє ключову роль у створенні політики інформаційної безпеки, забезпечуючи структурований підхід до виявлення, аналізу та зменшення потенційних загроз інформаційним активам. У сучасних умовах, коли кіберзагрози постійно ускладнюються, цей процес стає стратегічно важливим, дозволяючи організаціям ефективно захищати інформацію, підвищувати стійкість до викликів і забезпечувати довіру партнерів та клієнтів. Управління ризиками створює підґрунтя для політики ІБ, сприяючи її гнучкості

та узгодженості з цілями бізнесу.

Управління ризиками в інформаційній безпеці є безперервним процесом, який охоплює аналіз внутрішніх і зовнішніх факторів, що впливають на безпеку організації. Воно дозволяє організаціям прогнозувати потенційні загрози, такі як кібератаки, витоки даних або апаратні збої, і розробляти заходи для їх нейтралізації. Управління ризиками є не лише реактивним інструментом для вирішення інцидентів, але й проактивною стратегією, яка передбачає майбутні виклики, такі як впровадження нових технологій або зміни в регуляторному середовищі [34].

У контексті стратегічного управління УР має бути інтегровано в бізнес-процеси організації, щоб забезпечити захист активів і підтримку інновацій. Наприклад, компанії, такі як Amazon і Google, використовують управління ризиками для створення гнучких систем безпеки, які дозволяють швидко адаптуватися до нових загроз, зберігаючи довіру клієнтів [35]. Аналіз зовнішнього середовища, включаючи технологічні, економічні та геополітичні фактори, є ключовим для виявлення не лише ризиків, але й можливостей, таких як впровадження передових стандартів безпеки [36].

Управління ризиками також сприяє формуванню культури кіберстійкості, яка є критично важливою в умовах зростання кіберзагроз. Воно забезпечує баланс між захистом інформації та операційною ефективністю, дозволяючи організаціям уникати надмірних витрат на безпеку, які можуть обмежувати їхній розвиток [35]. Таким чином, управління ризиками перетворює політику ІБ на стратегічний інструмент, який підтримує довгострокові цілі організації.

Управління ризиками включає кілька ключових етапів, кожен з яких відіграє важливу роль у формуванні політики ІБ: ідентифікація ризиків, оцінка ризиків, пріоритизація ризиків і вибір контрзаходів (рис.2.4.). Ці етапи є циклічними, що дозволяє постійно вдосконалювати політику ІБ у відповідь на нові виклики [34].

Рис.2.4. Етапи управління ризиками

Першим етапом є *ідентифікація ризиків*, яка передбачає визначення інформаційних активів і пов'язаних із ними загроз. Інформаційні активи включають дані клієнтів, інтелектуальну власність, апаратне та програмне забезпечення. Активи необхідно класифікувати за їхньою критичністю, оскільки це дозволяє зосередити ресурси на захисті найцінніших компонентів [34]. Наприклад, у фінансовій організації дані клієнтів можуть бути пріоритетними, тоді як у логістичній компанії – інформація про постачальників.

Загрози, які ідентифікуються на цьому етапі, можуть бути технологічними (фішинг, програми-вимагачі), людськими (помилки працівників) або фізичними (пошкодження серверів). Аналіз зовнішнього середовища є важливим для виявлення нових загроз, таких як автоматизовані атаки або зміни в регуляторних вимогах [36]. Наприклад, зростання використання хмарних технологій створює нові вразливості, пов'язані з несанкціонованим доступом до даних, що вимагає оновлення процедур безпеки.

Оцінка ризиків передбачає аналіз ймовірності та потенційного впливу загроз. Цей етап дозволяє організаціям зрозуміти, які ризики є найбільш критичними, і визначити пріоритети захисту. Можна використовувати кількісні та якісні методи оцінки для забезпечення точності. Кількісний підхід включає формулу річної очікуваної втрати (ALE), яка розраховується як добуток ймовірності інциденту та його потенційних збитків. Наприклад, якщо ймовірність атаки типу DDoS становить 20% на рік, а потенційні втрати

оцінюються в 2,5 млн грн, то ALE становить 500 тис. грн [34].

Якісні методи, такі як NIST SP 800-30 або CRAMM, класифікують ризики за шкалою «низький», «середній» або «високий» на основі експертних оцінок. Ці методи є ефективними для організацій із обмеженими ресурсами, оскільки вони не вимагають складних обчислень [34]. Комбінований підхід, який поєднує кількісні та якісні методи, дозволяє досягти балансу між точністю та практичністю, інтегруючи результати оцінки в стратегічне планування [35]. Наприклад, фінансова організація може використовувати якісну оцінку для швидкого визначення ключових ризиків, а кількісний аналіз – для оцінки їхнього впливу на бюджет.

Пріоритизація ризиків допомагає організаціям зосередитися на загрозах із найбільшим потенційним впливом і ймовірністю. Пропонується використовувати матриці ризиків, які класифікують загрози за двома параметрами: ймовірність і вплив [34]. Наприклад, ризик фішингу може бути класифікований як «високий» через його поширеність і потенційні репутаційні збитки, тоді як ризик апаратних збоїв – як «низький» через рідкість і менший вплив.

Пріоритизація має узгоджуватися зі стратегічними цілями організації, щоб забезпечити ефективне використання ресурсів [35]. Наприклад, організація, яка працює в конкурентному секторі, може приділяти більше уваги захисту інтелектуальної власності, тоді як державна установа – захисту критичної інфраструктури. Пріоритизація ризиків повинна враховувати не лише загрози, але й можливості, такі як впровадження нових технологій безпеки, які можуть підвищити стійкість організації [36].

Вибір контрзаходів є завершальним етапом управління ризиками, який передбачає впровадження заходів для зменшення або нейтралізації ризиків. Контрзаходи поділяються на технічні (наприклад, шифрування, брандмауери), організаційні (політики доступу, навчання працівників) і фізичні (обмеження доступу до серверних приміщень). Вибір контрзаходів має бути економічно виправданим, щоб уникнути надмірних витрат [34].

Ефективні контрзаходи повинні враховувати специфіку організації та її ресурси [35]. Наприклад, мала організація може зосередитися на базових заходах, таких як антивірусне програмне забезпечення та навчання персоналу, тоді як велика корпорація – на впровадженні систем SIEM (Security Information and Event Management) для моніторингу подій у реальному часі. Також важливі превентивні дії, такі як розробка планів реагування на інциденти, які дозволяють мінімізувати збитки у разі атаки [36].

Управління ризиками є не ізольованим процесом, а частиною стратегічного управління організацією. Є три ключові аспекти інтеграції: крос-функціональна співпраця, захист активів для підтримки інновацій і підвищення обізнаності працівників. Крос-функціональна співпраця передбачає залучення IT, юридичних, маркетингових і управлінських команд для створення комплексної системи безпеки. Наприклад, IT-відділ відповідає за технічні заходи, тоді як юридичний відділ забезпечує відповідність нормативним вимогам.

Захист активів підтримує інновації, дозволяючи організаціям безпечно впроваджувати нові технології, такі як хмарні обчислення або Інтернет речей. Наприклад компанії Amazon і Google, які використовують управління ризиками для захисту даних клієнтів, що сприяє їхній репутації та конкурентоспроможності. Підвищення обізнаності працівників через тренінги та програми SETA знижує ймовірність інцидентів, пов’язаних із людським фактором, який є причиною 70% порушень безпеки [35].

Аналіз зовнішнього середовища дозволяє організаціям не лише реагувати на загрози, але й перетворювати їх на можливості [36]. Наприклад, впровадження передових стандартів безпеки, таких як ISO/IEC 27001, може стати конкурентною перевагою на міжнародному ринку. Крім того, аналіз зовнішнього середовища допомагає прогнозувати регуляторні зміни, такі як посилення вимог до захисту персональних даних, що дозволяє організаціям заздалегідь адаптувати політику ІБ.

Управління ризиками стикається з низкою викликів, які впливають на формування політики ІБ. Одним із основних є швидка еволюція кіберзагроз,

таких як автоматизовані атаки або використання штучного інтелекту зловмисниками. Організації часто не встигають адаптувати свої системи безпеки до нових вразливостей, що вимагає впровадження самонавчальних систем і регулярного оновлення процедур [34].

Іншим викликом є обмеженість ресурсів, особливо для малих і середніх організацій. Економічна виправданість контрзаходів є ключовою для таких організацій, оскільки надмірні витрати на безпеку можуть обмежувати їхній розвиток [35]. Недостатня координація між різними департаментами може призводити до фрагментації зусиль у сфері безпеки, що знижує ефективність політики ІБ [36].

Перспективи управління ризиками пов’язані з використанням нових технологій, таких як штучний інтелект і машинне навчання, для прогнозування загроз і автоматизації реагування. Ці технології дозволяють виявляти аномалії в реальному часі, що знижує вплив атак [34]. Крім того, міжсекторальна співпраця, яка включає обмін досвідом між організаціями та державними установами, може сприяти розробці більш стійких політик ІБ [36].

Управління ризиками відіграє ключову роль у формуванні культури кіберстійкості, яка є необхідною для протидії сучасним загрозам. Культура кіберстійкості залежить від обізнаності працівників і залучення керівництва [35]. Трансформаційні стилі лідерства, які демонструють прихильність до безпеки, підвищують мотивацію працівників дотримуватися політики ІБ. Наприклад, регулярні брифінги з безпеки або включення показників безпеки в оцінку ефективності працівників сприяють формуванню свідомого ставлення до захисту інформації.

Культура кіберстійкості також залежить від аналізу зовнішнього середовища, який дозволяє організаціям адаптуватися до нових викликів, таких як зростання віддаленої роботи або впровадження хмарних технологій [36]. У таких умовах управління ризиками включає розробку чітких інструкцій для працівників і впровадження додаткових заходів захисту, таких як VPN або багатофакторна автентифікація.

Управління ризиками є наріжним каменем політики інформаційної безпеки, забезпечуючи системний підхід до захисту інформаційних активів. Воно включає ідентифікацію, оцінку, пріоритизацію та нейтралізацію ризиків, інтегруючись зі стратегічним управлінням через крос-функціональну співпрацю, захист активів і формування культури кіберстійкості. Незважаючи на виклики, такі як швидка еволюція загроз і обмеженість ресурсів, управління ризиками відкриває перспективи для використання нових технологій і міжсекторальної співпраці. У сучасних умовах, коли кіберзагрози стають дедалі складнішими, ефективне управління ризиками є не лише інструментом захисту, але й стратегічним ресурсом, який сприяє сталому розвитку організації.

2.3 Методи впровадження політики: організаційні та технічні аспекти

Впровадження політики інформаційної безпеки є критично важливим для захисту інформаційних активів організації від сучасних кіберзагроз, зокрема фішингу, програм-вимагачів, атак на ланцюги постачання, а також внутрішніх загроз, пов’язаних із людським фактором. Цей процес потребує комплексного підходу, що інтегрує організаційні та технічні методи для побудови ефективної системи управління інформаційною безпекою. Організаційні заходи створюють основу для координації захисних процесів, тоді як технічні інструменти забезпечують їх практичну реалізацію.

Організаційні методи є основою для створення структури управління інформаційною безпекою, що забезпечує координацію дій усіх учасників інформаційних процесів в організації. Вони включають розробку нормативної бази, створення спеціалізованих підрозділів, навчання персоналу, моніторинг і аудит, а також формування культури безпеки. Ці заходи спрямовані на зниження ризиків, пов’язаних із людським фактором, який, за даними досліджень, спричиняє до 70% інцидентів безпеки [26].

Формування політики ІБ починається з розробки комплексу документів, що регламентують обробку інформації, визначають цілі захисту та заходи

реагування на загрози. Згідно з ISO/IEC 27001, політика ІБ є ключовим документом, який має бути затверджений керівництвом і доступний усім співробітникам [20]. Нормативна база повинна охоплювати не лише внутрішні правила, але й відповідати національним стандартам кібербезпеки, зокрема вимогам Держспецзв'язку України [37]. Наприклад, до таких документів належать положення про класифікацію інформації, інструкції для користувачів і плани реагування на інциденти. В Україні ці документи мають відповідати Законам України «Про захист персональних даних» і «Про державну таємницю» [9,12]. Для підприємницької діяльності важливо включати до політики ІБ механізми захисту комерційної таємниці, що знижує ризики економічних втрат [38].

Для ефективного управління системою ІБ необхідно створити спеціалізований підрозділ – службу захисту інформації (СЗІ). Цей підрозділ відповідає за координацію заходів безпеки, моніторинг подій і реагування на інциденти. ISO/IEC 27001 наголошує на необхідності забезпечення СЗІ достатніми ресурсами та повноваженнями [20]. Можна включати до складу СЗІ фахівців із кібербезпеки, які здатні аналізувати ризики та впроваджувати превентивні заходи [37]. Наприклад, у великих організаціях СЗІ може складатися з аналітиків безпеки, адміністраторів мереж і спеціалістів із криптографії. Створення СЗІ оформлюється наказом керівника, який затверджує її структуру та положення.

Людський фактор є однією з основних причин інцидентів безпеки, тому навчання персоналу є ключовим організаційним методом. Програми SETA спрямовані на формування культури безпеки та розвиток навичок захисту інформації. Дослідження показують, що регулярні тренінги знижують кількість порушень, спричинених недбалістю, на 30–50% [26]. Програми навчання повинні включати практичні заняття з розпізнавання соціальної інженерії та роботи з криптографічними засобами, що особливо актуально для організацій із високим рівнем конфіденційності [37]. Наприклад, симуляція фішингових атак на платформах, таких як KnowBe4, допомагає працівникам розпізнавати підозрілі

листи. Для підприємницьких структур навчання має фокусуватися на захисті комерційної інформації, що підвищує конкурентоспроможність [38].

Регулярний моніторинг і аудит забезпечують контроль за дотриманням політики ІБ. Моніторинг передбачає аналіз подій безпеки в реальному часі за допомогою систем SIEM, тоді як аудит включає періодичну оцінку відповідності стандартам. ISO/IEC 27001 рекомендує проводити аудити щонайменше раз на рік [20]. Аудит має охоплювати не лише технічні аспекти, але й організаційні процеси, такі як дотримання процедур доступу та навчання [37]. Для підприємницької діяльності аудит безпеки має включати аналіз ризиків, пов'язаних із партнерами та постачальниками, що дозволяє виявляти слабкі місця в ланцюгах постачання [13].

Культура безпеки впливає на мотивацію працівників дотримуватися політики ІБ. Організації з розвиненою культурою безпеки мають на 40% нижчий рівень інцидентів [26]. Культура безпеки формується через регулярне інформування персоналу, залучення керівництва та створення мотиваційних програм [37]. Наприклад, включення показників безпеки в оцінку продуктивності сприяє свідомому ставленню до захисту інформації.

Технічні методи забезпечують практичну реалізацію захисних заходів, використовуючи апаратні та програмні засоби для захисту інформації від несанкціонованого доступу, модифікації чи втрати. Існують такі технічні методи впровадження політики ІБ: криптографічний захист інформації, міжмережеві екрани та системи виявлення вторгнень, управління доступом і автентифікація, системи моніторингу та аналізу подій, модульний принцип і автоматизація. Вони базуються на принципах системності, модульності та економічної доцільності.

Шифрування є основним інструментом для забезпечення конфіденційності та цілісності даних. В Україні використовуються сертифіковані засоби, такі як системи «Криптон» або «Рубіж». Важливо використовувати криптографічні засоби, що відповідають стандартам ДСТУ, для захисту каналів зв'язку та баз даних [37]. Наприклад, протоколи TLS/SSL забезпечують безпечний веб-трафік, а алгоритми AES-256 захищають клієнтські дані. У контексті постквантових

загроз рекомендовано впроваджувати гібридні криптографічні протоколи [29]. Політика ІБ має передбачати процедури управління ключами та тестування криптосистем.

Міжмережеві екрани (firewalls) і системи IDS/IPS є ключовими компонентами захисту мереж. Вони обмежують зовнішній доступ і виявляють аномалії в реальному часі. Сучасні системи IDS, такі як Snort або Suricata, мають інтегруватися з модулями аналізу поведінки для протидії складним атакам, таким як APT [37]. NIST CSF рекомендує використовувати профілі безпеки для швидкого реагування на загрози. Впровадження цих засобів потребує регулярного оновлення сигнатур і правил.

Системи багатофакторної автентифікації (Multi-factor authentication, MFA), біометричні технології та смарт-карти знижують ймовірність компрометації облікових записів на 90%. Підприємницької діяльності важливо обмежувати доступ до комерційної інформації на основі ролей, що мінімізує внутрішні загрози [38]. Політика ІБ має визначати процедури ротації паролів і моніторингу дій користувачів.

Системи SIEM, такі як Splunk або QRadar, забезпечують централізований аналіз подій безпеки. Можна інтегрувати SIEM із системами аналізу ризиків для виявлення складних загроз [37]. NIST CSF підкреслює важливість автоматизації аналізу для протидії програмам-вимагачам. Політика ІБ має визначати процедури налаштування SIEM і зберігання логів відповідно до GDPR [19].

Модульна архітектура дозволяє інтегрувати нові компоненти, такі як аналізатори поведінки (User and Entity Behavior Analytics, UEBA), без порушення роботи системи. Модульність забезпечує гнучкість і знижує витрати на модернізацію [37]. Автоматизація процесів, таких як оновлення ПЗ чи реагування на інциденти, підвищує оперативність.

Ефективність політики ІБ залежить від інтеграції організаційних і технічних методів. Організаційні заходи, такі як навчання та аудит, забезпечують правильне використання технічних засобів, тоді як автоматизовані системи підсилюють організаційні процеси. Наприклад, система MFA буде неефективною

без навчання користувачів щодо розпізнавання фішингу [26]. Інтеграція передбачає створення єдиної системи управління ризиками, яка поєднує технічні та людські аспекти [37].

Інтеграція базується на циклі PDCA, рекомендованому ISO/IEC 27001 [20]. Для підприємницької діяльності інтеграція має враховувати економічні аспекти, такі як оптимізація витрат на безпеку [38]. Важлива оцінка ефективності навчальних програм за допомогою програмних інструментів, що може бути частиною циклу PDCA.

Психологічні та соціальні аспекти є ключовими для інтеграції. Мотивація працівників залежить від зрозумілості процедур і підтримки керівництва. Технічні засоби, такі як спрощені інтерфейси, знижують стрес від вимог безпеки [26].

Методи впровадження політики ІБ, що поєднують організаційні та технічні аспекти, є необхідними для захисту інформаційних активів. Організаційні заходи забезпечують структуроване управління, а технічні методи гарантують практичну реалізацію. Інтеграція цих підходів, з урахуванням психологічних і соціальних факторів, створює адаптивну політику, яка відповідає сучасним кіберзагрозам і підтримує стратегічні цілі організації.

2.4 Контроль та оцінка ефективності політики інформаційної безпеки

У сучасному світі, де інформаційні технології стрімко проникають у всі сфери діяльності, захист даних стає критично важливим завданням для організацій. Політика інформаційної безпеки є основою для забезпечення конфіденційності, цілісності та доступності інформаційних активів. Проте створення політики – лише перший крок. Для її ефективного функціонування необхідні систематичний контроль і оцінка, які дозволяють виявляти вразливості, адаптувати заходи до нових кіберзагроз і забезпечувати відповідність нормативним вимогам. Ці процеси є ключовими елементами системи управління інформаційною безпекою і відіграють особливу роль у державних органах

регіонального рівня, які обробляють чутливі дані, такі як персональна інформація громадян чи відомості з обмеженим доступом.

Політика інформаційної безпеки – це документ, який визначає правила, процедури та технічні заходи для захисту інформаційних активів організації. Вона охоплює аспекти управління доступом, шифрування даних, реагування на інциденти та навчання персоналу. Однак без регулярного контролю та оцінки політика може втратити актуальність, адже кіберзагрози постійно еволюціонують. Наприклад, у Сумській області в першому півріччі 2024 року було зафіксовано понад 700 випадків кібершахрайства, переважно через фішингові кампанії, що свідчить про необхідність посиленого контролю. Низький індекс цифрової трансформації регіону (0.178 у 2023 році) додатково ускладнює впровадження сучасних засобів захисту [39].

Контроль політики ІБ спрямований на перевірку виконання її вимог, виявлення відхилень і слабких місць, які можуть призвести до інцидентів, таких як несанкціонований доступ чи витік даних. Оцінка ефективності, у свою чергу, аналізує, наскільки політика здатна забезпечувати захист інформації та відповідати стратегічним цілям організації. Ці процеси ґрунтуються на моделі PDCA, яка передбачає циклічне вдосконалення шляхом планування, виконання, перевірки та коригування заходів [40]. Такий підхід дозволяє адаптувати політику до нових викликів і забезпечує її відповідність національному законодавству, зокрема Закону України «Про захист інформації в інформаційно-комунікаційних системах» [39].

У регіональних організаціях контроль і оцінка набувають особливого значення через обробку чутливих даних, таких як персональна інформація громадян у ЦНАПах. Недостатня увага до цих процесів може призвести до серйозних наслідків, включаючи репутаційні втрати, фінансові збитки та порушення законодавства. Таким чином, контроль і оцінка є не лише технічними, а й стратегічними інструментами для забезпечення безпеки в цифрову еру.

Контроль політики ІБ – це систематичний процес, який включає організаційні, технічні та процедурні заходи для забезпечення виконання вимог

безпеки. Він спрямований на виявлення відхилень, які можуть спричинити інциденти, і базується на комплексному підході. Є п’ять основних методів контролю, які застосовуються в державних органах регіонального рівня [39]. Розглянемо їх детально.

Аудит є комплексною перевіркою відповідності інформаційних систем, процесів і процедур вимогам політики ІБ та нормативним документам, таким як НД ТЗІ 2.5-004-99 [39]. Він може проводитися внутрішніми підрозділами або зовнішніми експертами за стандартом ISO 19011 [40]. У регіональних органах аудит є обов’язковим для оцінки захисту інформації з обмеженим доступом, зокрема персональних даних, що обробляються в ЦНАПах [39]. Наприклад, аудит може виявити слабкі місця в конфігурації систем, такі як незахищені мережеві протоколи, або порушення процедур управління доступом, як-от надання надмірних прав користувачам.

Моніторинг передбачає постійний аналіз подій у реальному часі за допомогою систем, таких як SIEM. Ці системи збирають і аналізують журнали подій, виявляючи аномалії, наприклад, підозрілі спроби входу в систему. У Сумській області моніторинг допоміг ідентифікувати значну кількість фішингових атак, що дозволило оперативно реагувати на загрози [39]. Автоматизовані системи моніторингу скорочують час реагування та підвищують ефективність виявлення інцидентів, що є критично важливим у контексті зростаючої складності кіберзагроз [40].

Пентест симулює кібератаки для перевірки стійкості систем до зовнішніх і внутрішніх загроз. Цей метод дозволяє виявити вразливості, такі як незахищені API, слабкі паролі чи неоновлені програмні компоненти [39]. У державних органах пентест є особливо важливим для захисту критичних інформаційних систем, таких як бази даних із персональною інформацією. Наприклад, тестування може показати, що застаріла версія вебсервера вразлива до атак типу SQL-ін’єкцій, що потребує негайного оновлення [40].

Регулярна *перевірка звітів* про стан інформаційної безпеки, підготовлених відповідальними підрозділами, допомагає оцінити виконання політики та

виявити прогалини. Цей метод є ключовим для забезпечення відповідності нормативним вимогам, зокрема «Правилам забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [39]. Аналіз звітів може виявити, наприклад, недостатню частоту оновлення антивірусного програмного забезпечення або невідповідність процедур резервного копіювання [40].

У контексті обробки персональних даних контроль включає *оцінку дотримання вимог* Закону України «Про захист персональних даних». Це охоплює перевірку процедур шифрування, управління доступом і навчання персоналу. Наприклад, контроль може виявити, що дані громадян передаються через незахищені канали зв'язку, що потребує впровадження протоколів TLS або VPN [39].

Ефективність контролю залежить від інтеграції автоматизованих інструментів і залучення кваліфікованих фахівців. Використання спеціалізованого програмного забезпечення, такого як системи аналізу загроз, значно знижує ризик людських помилок і підвищує якість моніторингу [40]. Комплексне застосування цих методів створює надійну основу для захисту інформаційних активів.

Оцінка ефективності політики ІБ передбачає аналіз її здатності забезпечувати захист інформації та відповідати стратегічним цілям організації. Цей процес базується на кількісних і якісних показниках, які відображають результативність заходів безпеки. Оцінка включає чотири основні етапи:

1. *Визначення критеріїв оцінки*. Критерії охоплюють рівень захищеності інформації, кількість інцидентів безпеки, відповідність стандартам (наприклад, ISO/IEC 27001) і здатність протистояти кіберзагрозам. У державних органах ключовим критерієм є захист інформації з обмеженим доступом від несанкціонованого доступу [39].

2. *Збір даних.* Дані отримуються через результати аудитів, моніторинг подій, пентести та звіти про інциденти. Метрики, такі як середній час реагування на інцидент (MTTR) чи кількість успішно відхилених атак, також

використовуються для аналізу [40].

3. *Аналіз результатів*. Порівняння зібраних даних із плановими показниками та вимогами законодавства дозволяє оцінити прогалини в політиці. Наприклад, якщо аналіз показує, що система захисту не відповідає вимогам щодо шифрування даних, це потребує коригування.

4. *Формування рекомендацій*. На основі аналізу розробляються заходи для усунення недоліків, такі як оновлення програмного забезпечення, посилення процедур доступу чи навчання персоналу [39].

Для оцінки ефективності політики інформаційної безпеки використовуються ключові показники ефективності (KPI), які дозволяють кількісно та якісно оцінити її результативність. Ці показники є інструментами для вимірювання рівня захисту, оперативності реагування та відповідності стандартам. Залежно від їхньої спрямованості, KPI поділено на три групи: організаційні, технічні та фінансово-ризикові показники.

Організаційні показники зосереджені на оцінці людського фактору, внутрішніх процесів і відповідності нормативним вимогам (табл. 2.1.)

Таблиця 2.1

Організаційні показники

Показник	**Опис**
% співробітників, ознайомлених з політикою	Чи всі підписали ознайомлення
Рівень успішності тестування	Середній бал або % працівників, які склали тест
Кількість відхилень, виявлених під час внутрішнього аудиту	Показує ступінь відповідності реальній практиці
Частота оновлення політик і процедур	Відображає, як часто організація переглядає та оновлює політику ІБ

Відсоток співробітників, ознайомлених із політикою – показник, який визначає, чи всі працівники організації ознайомлені з вимогами політики ІБ, і скільки з них пройшли відповідні тренінги. Високий відсоток (наприклад, 90% і

вище) свідчить про ефективність заходів із підвищення обізнаності, що знижує ризики, пов’язані з людським фактором.

Рівень успішності тестування – показник, який вимірює середній бал або відсоток правильних відповідей працівників під час тестів із кібергігієни чи симуляцій фішингових атак. Наприклад, якщо 80% працівників успішно проходять симуляцію, це вказує на їхню готовність протистояти загрозам, що є ключовим для зменшення інцидентів, спричинених людським фактором [39].

Кількість виявлених і виправлених під час внутрішнього аудиту – показник, який відображає ступінь відповідності реальних практик задокументованій політиці ІБ. Висока кількість виправлених розбіжностей (наприклад, 95% виявлених невідповідностей усунуто протягом місяця) свідчить про ефективність внутрішнього контролю та аудиту.

Частота оновлення політик і процедур – показник, який відображає, як часто організація переглядає та оновлює політику ІБ для адаптації до нових загроз і вимог законодавства. Щорічний перегляд або оновлення після значних інцидентів є ознакою проактивного підходу, що особливо важливо для регіональних організацій із нечіткою нормативною базою [39].

Технічні показники зосереджені на оцінці стійкості технічних систем, оперативності реагування та ефективності IT-контролів (табл. 2.2.).

Таблиця 2.2.

Технічні показники

Показник	**Опис**
Кількість зареєстрованих інцидентів до/після впровадження	Має знижуватися (або виявлення має зростати)
Час реагування на інциденти	Має скорочуватись
Кількість заблокованих спроб несанкціонованого доступу	Ознака ефективних технічних контролів
Відсоток реалізованих IT-контролів (SIEM, резервне копіювання, DLP)	Має прагнути до 100%
Кількість усунутих вразливостей	Вимірює, скільки виявлених вразливостей усунуто за певний період

Кількість зареєстрованих інцидентів до/після впровадження – показник, який порівнює частоту інцидентів безпеки (наприклад, витоки даних чи атаки програм-вимагачів) до та після впровадження політики ІБ. Очікується, що після впровадження заходів кількість інцидентів має знизитися щонайменше вдвічі, що свідчить про підвищення рівня захисту [40].

Час реагування на інцидент – показник, який вимірює середній час, необхідний для виявлення, аналізу та нейтралізації інциденту (Mean Time to Respond, MTTR). Скорочення цього часу (наприклад, до кількох годин) вказує на оперативність системи реагування, що є критичним для мінімізації збитків. Автоматизовані системи, такі як SIEM, можуть значно скоротити MTTR [40].

Кількість заблокованих спроб несанкціонованого доступу – показник, який відображає очікувану ефективність технічних засобів захисту, таких як системи виявлення вторгнень. Висока кількість заблокованих спроб (наприклад, 98% за місяць) свідчить про стійкість ІБ-системи до зовнішніх атак.

Частота реалізації ІТ-контролю (SIEM, резервування, DLP) – показник, який оцінює, наскільки регулярно використовуються інструменти, такі як SIEM, резервування та DLP. Мета – прагнення до 100% охоплення критичних систем, що забезпечує надійне резервне копіювання, швидке відновлення та запобігання витокам даних.

Кількість усунутих вразливостей – показник, який вимірює, скільки виявлених вразливостей (наприклад, застаріле ПЗ чи слабкі паролі) усунуто за певний період. Високий показник (наприклад, 95% протягом місяця) свідчить про ефективність процесів моніторингу та управління оновленнями [40].

Фінансово-ризикові показники оцінюють економічну ефективність політики ІБ та рівень управління ризиками (табл. 2.3.).

Таблиця 2.3.

Фінансово-ризикові показники

Показник	**Опис**
Кількість (або вартість) зупинок бізнесу через ІБ-інциденти	Має зменшитись

Продовження таблиці 2.3.

Показник	Опис
Оцінка ризику до/після впровадження	За матрицею ризиків або скоринговою моделлю
Кількість штрафів/вимог від контролюючих органів	Повинна дорівнювати 0

Кількість (або частота) фінансових збитків через ІБ-інциденти – показник, який оцінює частоту фінансових втрат, спричинених інцидентами безпеки, включаючи прямі (штрафи) та непрямі (втрата клієнтів) витрати. Зменшення цього показника (наприклад, на 30% після впровадження заходів) свідчить про фінансову ефективність політики ІБ [40].

Оцінка ризику до/після впровадження – показник, який порівнює рівень ризиків до та після впровадження політики ІБ за матричною або скороченою моделлю. Зниження рівня ризику (наприклад, із високого до середнього) дозволяє кількісно оцінити прогрес у зменшенні загроз, що є важливим для державних органів, які обробляють персональні дані [39].

Кількість інцидентів, виявлених внутрішніми контролями – показник, який відображає якість внутрішнього контролю. Мета – повна відповідність із нульовою кількістю таких інцидентів, що свідчить про ефективне управління ризиками та відсутність критичних вразливостей у системі.

Рівень економії від зниження втрат – показник, який вимірює фінансову ефективність через зменшення витрат на інциденти. Впровадження автоматизованих систем може заощадити до 30% витрат на реагування [40].

Ці KPI є комплексними індикаторами, які дозволяють оцінити різні аспекти політики ІБ: від технічної стійкості до організаційної готовності. Їхній аналіз допомагає виявити слабкі місця, визначити пріоритети для вдосконалення та обґрунтувати інвестиції в кібербезпеку. У контексті регіональних організацій, де ресурси обмежені, вибір правильних KPI є особливо важливим для забезпечення максимальної ефективності з мінімальними витратами.

Оцінка ризиків є центральним елементом процесу, оскільки дозволяє ідентифікувати потенційні загрози, такі як соціальна інженерія чи вразливості в

програмному забезпеченні, і визначити пріоритетні заходи захисту [40]. У державних органах особлива увага приділяється ризикам, пов’язаним із обробкою персональних даних, що вимагає регулярного аналізу вразливостей [39].

Контроль і оцінка політики ІБ стикаються з низкою викликів, які ускладнюють їх реалізацію в регіональних організаціях. Можна виділити такі ключові проблеми:

– національне законодавство, зокрема Закон України «Про захист персональних даних», не містить чітких вимог до кіберзахисту, що ускладнює стандартизацію процедур контролю;

– брак ресурсів, який перешкоджає закупівлі сучасних систем моніторингу, проведенню регулярних аудитів і залученню експертів;

– нестача спеціалістів із кібербезпеки, яка знижує в регіональних органах якість аудиту, моніторингу та оцінки;

– використання іноземного обладнання, як-от камери відеоспостереження, створює вразливості через обмежений доступ до оновлень;

– помилки працівників, такі як використання слабких паролів чи відкриття фішингових листів, спричиняють до 80% інцидентів [39];

– застаріла інфраструктура, яка ускладнює впровадження хмарних сервісів чи систем штучного інтелекту для аналізу загроз [40].

Ці проблеми вимагають комплексного підходу, який поєднує технічні, організаційні та освітні заходи для підвищення ефективності політики ІБ.

Контроль та оцінка ефективності політики інформаційної безпеки є невід’ємними складовими системи управління інформаційною безпекою, які забезпечують захист інформаційних активів у регіональних організаціях. Вони дозволяють виявляти слабкі місця, адаптувати заходи до нових кіберзагроз і забезпечувати відповідність вимогам законодавства. Методи контролю, такі як аудит, моніторинг, пентест, аналіз звітності та перевірка захисту даних, створюють комплексний підхід до виявлення вразливостей. Оцінка

ефективності, що базується на чітких KPI, дає змогу виміряти результативність політики та визначити напрями її вдосконалення.

Незважаючи на виклики, такі як обмежене фінансування, брак кадрів і недостатня нормативна база, впровадження стандартів ISO/IEC 27001, автоматизованих систем моніторингу, регулярного навчання та модернізації інфраструктури може значно підвищити ефективність політики ІБ. Для регіональних організацій, які працюють із чутливими даними, ці процеси є не лише технічною необхідністю, а й запорукою довіри громадян і стабільності діяльності.

Висновки до розділу 2

Проведено ґрунтовне дослідження методів створення та впровадження політики ІБ для організацій, з акцентом на їх адаптацію до сучасних викликів цифрового середовища. Аналіз дозволив систематизувати ключові методи, які забезпечують ефективне формування та реалізацію політики ІБ, враховуючи специфіку організаційних процесів і вимоги міжнародних стандартів.

Встановлено, що методи створення політики ІБ базуються на структурному підході, який включає оцінку ризиків, класифікацію інформаційних активів і розробку регламентів, узгоджених із бізнес-процесами. Особливу увагу приділено циклу PDCA, який забезпечує безперервне вдосконалення політики через ітеративний процес. Досліджено роль автоматизованих інструментів, зокрема систем управління ідентичністю та доступом і хмарних платформ безпеки, які дозволяють реалізувати принципи мінімальних привілеїв, автоматизувати моніторинг і спрощувати підготовку до аудитів за стандартами ISO/IEC 27001, GDPR і NIST CSF.

Окремо розглянуто методи впровадження політики ІБ, які передбачають інтеграцію з системою управління організацією, навчання персоналу та формування культури безпеки. Визначено, що успішне впровадження залежить від залучення керівництва, чіткої комунікації регламентів і регулярного

моніторингу ефективності заходів. Дослідження підкреслило важливість врахування людського фактору, оскільки 70% інцидентів безпеки пов’язані з помилками чи недбалістю працівників. Для їх мінімізації запропоновано використання симуляцій кібератак і тренінгів із кібергігієни.

Проведений аналіз методів також виявив виклики, зокрема складність інтеграції автоматизованих систем із наявною інфраструктурою, високі початкові витрати на впровадження та потребу в адаптації політики до нових кіберзагроз, таких як атаки з використанням штучного інтелекту чи розподілені атаки типу DDoS. Для подолання цих викликів рекомендовано поетапне впровадження політики, використання пілотних проєктів і регулярне оновлення регламентів на основі аналізу актуальних загроз.

Результати дослідження створюють теоретичну основу для розробки рекомендацій та підтверджують необхідність комплексного підходу до створення й впровадження політики ІБ, який поєднує технічні, організаційні та людські аспекти для забезпечення кіберстійкості організації в умовах цифрової трансформації.

Розділ 3 РОЗРОБКА РЕКОМЕДАЦІЙ ДО СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Вибір організаційної моделі для впровадження політики інформаційної безпеки

Політика інформаційної безпеки є ключовим елементом системи управління інформаційною безпекою, що забезпечує захист інформаційних активів організації, зокрема конфіденційність, цілісність та доступність даних [20]. Ефективне впровадження політики залежить від вибору організаційної моделі, яка визначає структуру управління доступом, розподіл обов'язків та координацію між учасниками інформаційних процесів. У контексті корпоративної організації, що працює з персональними даними клієнтів (зокрема медичними) та прагне відповідати міжнародним стандартам ISO/IEC 27001 і HIPAA, вибір моделі має враховувати масштабованість, простоту адміністрування та здатність протистояти сучасним кіберзагрозам, таким як фішинг, програми-вимагачі та внутрішні порушення [27].

Організаційні моделі для впровадження політики ІБ структурують процеси управління доступом і захисту інформації, забезпечуючи відповідність нормативним вимогам і стратегічним цілям організації (рис.3.1.). Є чотири основні моделі, які можуть бути застосовані в корпоративному контексті [41, 42]: рольне управління доступом (РУД), матрична модель, централізована модель, децентралізована модель.

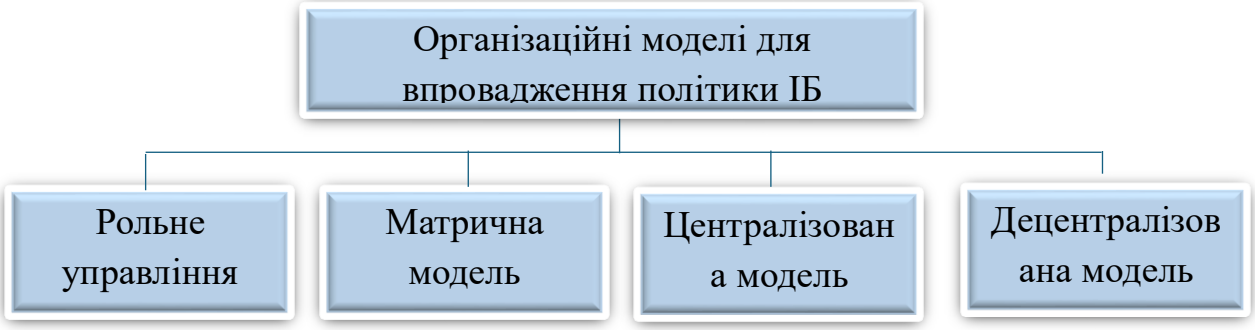

Рис.3.1. Організаційні моделі для впровадження політики ІБ

Рольне управління доступом. Модель базується на призначенні ролей користувачам відповідно до їхніх функціональних обов'язків. Кожна роль має чітко визначений набір прав доступу, що відповідає принципу мінімальних прав. РУД широко використовується в організаціях із великою кількістю користувачів і складними інформаційними системами, оскільки спрощує адміністрування та забезпечує масштабованість.

Матрична модель. Передбачає індивідуальне налаштування прав доступу для кожного користувача та системи через матрицю дозволів. Ця модель є гнучкою, але складною в адмініструванні, особливо в великих організаціях, через необхідність ручного управління правами [41].

Централізована модель. Управління доступом і політиками безпеки здійснюється єдиним органом, що забезпечує високий рівень контролю та стандартизації. Модель ефективна для організацій із чіткою ієрархією, але може бути надмірно жорсткою для динамічних бізнес-процесів.

Децентралізована модель. Делегування управління доступом окремим підрозділам підвищує гнучкість, але може призвести до невідповідності стандартам через різницю в підходах підрозділів [42].

Кожна модель має свої особливості, які необхідно оцінити з урахуванням вимог політики ІБ, зокрема принципів мінімальних прав, захисту персональних даних і регулярного навчання персоналу.

Для вибору оптимальної моделі використано критерії, сформовані на основі вимог політики ІБ, міжнародних стандартів (ISO/IEC 27001, HIPAA) та специфіки корпоративної організації [20]:

– модель повинна забезпечувати конфіденційність, цілісність і доступність даних, а також підтримувати принцип мінімальних прав (least privilege);

– модель має бути придатною для організації з великою кількістю користувачів (співробітники, консультанти, підрядники) і різноманітними інформаційними системами, включаючи хмарні сервіси;

– модель повинна мінімізувати адміністративні зусилля при управлінні доступом, особливо при зміні ролей чи додаванні нових користувачів;

– модель має сприяти виконанню вимог ISO/IEC 27001 і HIPAA [20];

– модель повинна забезпечувати швидке виявлення та реагування на інциденти безпеки, наприклад, несанкціонований доступ чи витік даних;

– модель має підтримувати формування культури безпеки через залучення персоналу та регулярне навчання, що є вимогою політики;

Ці критерії відображають потреби організації в захисті клієнтських даних, безперервності бізнес-процесів і відповідності міжнародним стандартам.

Для оцінки організаційних моделей використано розширений порівняльний аналіз за визначеними критеріями, доповнений додатковими аспектами, такими як адаптивність до сучасних кіберзагроз, економічна доцільність і сумісність із автоматизованими системами управління доступом. Аналіз включає детальну оцінку переваг і недоліків кожної моделі, приклади з практики, а також оцінку їхньої відповідності вимогам політики інформаційної безпеки в контексті корпоративної організації, що обробляє персональні дані клієнтів, зокрема медичні, і прагне відповідати стандартам ISO/IEC 27001 і HIPAA [20, 27]. Результати порівняння підсумовано в таблиці 3.1 після детального розгляду кожної моделі.

Таблиця 3.1.

Порівняльний аналіз організаційних моделей

Критерій	**РУД**	**Матрична**	**Централізована**	**Децентралізована**
Відповідність принципам ІБ	Висока	Середня	Висока	Низька
Масштабованість	Висока	Низька	Середня	Висока
Простота адміністрування	Висока	Низька	Середня	Висока
Відповідність стандартам	Висока	Середня	Висока	Низька
Управління інцидентами	Висока	Низька	Висока	Низька

Продовження таблиці 3.1.

Критерій	**РУД**	**Матрична**	**Централізована**	**Децентралізована**
Інтеграція з культурою безпеки	Висока	Середня	Середня	Висока
Адаптивність до кіберзагроз	Висока	Низька	Висока	Низька
Економічна доцільність	Висока	Низька	Середня	Низька

На основі порівняльного аналізу для впровадження політики ІБ у корпоративній організації Creatio, що працює з персональними даними клієнтів, рекомендується обрати *рольне управління доступом.* Обґрунтування вибору базується на таких аспектах:

– РУД забезпечує суворе дотримання принципу мінімальних прав, що є ключовим у політиці ІБ. Кожному користувачу надаються лише необхідні права відповідно до його ролі, що знижує ризик несанкціонованого доступу до клієнтських даних, зокрема медичних, як того вимагає HIPAA [20];

– організація включає велику кількість користувачів (співробітники, консультанти, підрядники) і використовує різноманітні системи, включаючи хмарні сервіси. РУД дозволяє ефективно управляти доступом через групування прав за ролями, що спрощує масштабування;

– РУД зменшує адміністративне навантаження порівняно з матричною моделлю, оскільки усуває необхідність індивідуального налаштування прав для кожного користувача [41]. Це особливо важливо для автоматизації процесів управління доступом, наприклад, при зміні ролей чи наймі нових співробітників;

– РУД відповідає вимогам ISO/IEC 27001 щодо структурованого управління доступом і HIPAA щодо захисту персональних даних [20]. Модель підтримує принципи розподілу обов’язків, що є обов’язковими для сертифікації за цими стандартами;

– чітке визначення ролей у РУД полегшує ідентифікацію відповідальних

за інциденти та швидке реагування. Наприклад, у разі витоку даних РУД дозволяє швидко визначити, які ролі мали доступ до скомпрометованої інформації;

– РУД підтримує формування культури безпеки через інтеграцію ролей у програми навчання. Ролі можуть бути використані для структурування навчальних модулів, що підвищує обізнаність персоналу щодо захисту інформації;

– РУД дозволяє оперативно модифікувати права ролей у відповідь на нові загрози, такі як фішинг чи атаки на ланцюги постачання, що є актуальним у сучасних умовах [27];

– після початкових інвестицій у створення ролей РУД знижує витрати на адміністрування, що є важливим для організацій із обмеженим бюджетом [41].

Незважаючи на необхідність початкових зусиль для визначення ролей, РУД компенсує це довгостроковою ефективністю. Альтернативні моделі менш підходять: матрична модель є надто складною для великих організацій, централізована – надмірно жорсткою, а децентралізована підвищує ризик невідповідності стандартам [41, 42].

Рольне управління доступом є оптимальною організаційною моделлю для впровадження політики інформаційної безпеки в корпоративній організації, що фокусується на захисті клієнтських даних і відповідності стандартам ISO/IEC 27001 та HIPAA. Модель забезпечує масштабованість, простоту адміністрування, ефективне управління інцидентами та інтеграцію з культурою безпеки.

3.2 Алгоритм розробки політики інформаційної безпеки для організації

Рис.3.2. Алгоритм розробки політики інформаційної безпеки

Політика ІБ є фундаментальним інструментом забезпечення захисту інформаційних активів організації, що набуває особливого значення для компаній, таких як Creatio, які спеціалізуються на обробці персональних даних клієнтів у хмарних сервісах. У контексті сучасних кіберзагроз, таких як

фішингові атаки, витоки даних і внутрішні порушення, створення ефективної політики ІБ вимагає системного підходу, що поєднує аналіз ризиків, відповідність міжнародним стандартам і врахування специфіки діяльності організації. Попередній порівняльний аналіз показав, що для Creatio оптимальним механізмом управління доступом є рольове управління доступом, яке забезпечує чітке розмежування прав доступу, зниження ризиків несанкціонованого доступу та відповідність вимогам стандартів ISO/IEC 27001 і HIPAA [44]. У цьому розділі представлено детальний алгоритм розробки політики ІБ для Creatio, зосереджений на інтеграції РУД, аналізі ризиків, управлінні інцидентами та інших ключових аспектах (рис. 3.2.).

Розробка політики ІБ розпочинається з визначення її мети та обсягу, що є основою для подальшого формування принципів і процедур. Для Creatio мета політики полягає у створенні комплексної системи захисту персональних даних клієнтів, конфігурацій CRM-систем і внутрішніх процесів, що забезпечує конфіденційність, цілісність і доступність інформації [44]. Обсяг політики охоплює всі інформаційні активи, включаючи бази даних клієнтів, хмарні сервіси, локальні сервери, а також дії всіх користувачів – працівників, консультантів, підрядників і партнерів. Політика є обов’язковою для всіх зазначених категорій, що відповідає вимогам внутрішнього документа організації. Вона має відповідати міжнародним стандартам, стандарту ISO/IEC 27001, а також нормам HIPAA. Такий підхід забезпечує юридичну обґрунтованість політики та її відповідність галузевим вимогам.

Наступним кроком є ідентифікація та класифікація інформаційних активів Creatio, що є передумовою для оцінки ризиків. Активи включають дані (персональні дані клієнтів, фінансові звіти, конфігурації CRM), обладнання (сервери, робочі станції, мережеві пристрої), програмне забезпечення (платформа Creatio, антивірусні системи) та персонал (працівники з доступом до даних). Кожен актив оцінюється за критеріями конфіденційності, цілісності та доступності [44]. Наприклад, бази даних клієнтів мають високий рівень конфіденційності, оскільки їх компрометація може призвести до репутаційних і

юридичних наслідків. Для ідентифікації активів застосовується методологія яка передбачає створення реєстру активів і визначення їхньої критичності для бізнес-процесів Creatio.

Аналіз ризиків є центральним елементом розробки політики ІБ, оскільки дозволяє ідентифікувати загрози та визначити заходи для їх мінімізації. Для Creatio, яка працює з персональними даними, ключовими є зовнішні загрози (фішингові атаки, DDoS-атаки, зловмисне ПЗ), внутрішні загрози (несанкціонований доступ, помилки конфігурації), а також випадкові (збої обладнання) та навмисні (соціальна інженерія, інсайдерські дії) загрози. Процес аналізу ризиків включає кілька етапів:

1. Ідентифікація загроз - визначення потенційних джерел небезпеки на основі вразливостей систем і статистики кібератак.

2. Оцінка ймовірності та впливу - аналіз імовірності виникнення загрози та її потенційних наслідків, включаючи фінансові втрати, репутаційні збитки та штрафи за порушення GDPR або HIPAA.

3. Ранжування ризиків - класифікація ризиків за рівнем критичності (низький, середній, високий).

4. Пріоритизація заходів - розробка заходів для зниження ризиків, таких як впровадження РУД, оновлення антивірусного ПЗ і навчання персоналу.

Цей підхід базується на моделі яка акцентує на оцінці активів, загроз і вразливостей [45]. Наприклад, високий ризик витоку даних через неналежне управління доступом вимагає впровадження РУД, що є рекомендованим підходом для Creatio.

На основі аналізу ризиків формулюються принципи політики ІБ, які відповідають стандартам і враховують специфіку діяльності Creatio. Основними принципами є конфіденційність (доступ до даних лише для авторизованих осіб), цілісність (редагування інформації лише через авторизовані процеси) і доступність (забезпечення доступу до даних у потрібний час) [44]. Додатково політика передбачає відповідність міжнародним стандартам, безперервність бізнес-процесів через системи резервного копіювання та інтеграцію ІБ у

корпоративну культуру шляхом регулярного навчання персоналу. Ці принципи формують основу для розробки конкретних процедур, зокрема управління доступом і паролями.

Особливу увагу приділено впровадженню рольового управління доступом, яке визнано оптимальним для Creatio завдяки його здатності ефективно розмежовувати права доступу та знижувати ризики несанкціонованого доступу. Впровадження РУД включає кілька ключових процедур:

– визначення ролей - створення ролей на основі функціональних обов'язків працівників (наприклад, адміністратор CRM, менеджер з продажів, IT-спеціаліст). Кожна роль має чітко визначений набір прав доступу, наприклад, менеджери з продажів мають доступ до контактних даних клієнтів, але не до фінансової інформації;

– призначення ролей - кожному користувачу присвоюється унікальний обліковий запис із відповідною роллю. Некритичні ролі, такі як гостьові, мають мінімальні права;

– реалізація принципу мінімальних прав - доступ надається лише до тих даних і систем, які необхідні для виконання обов'язків, що відповідає вимогам ISO/IEC 27001;

– автоматизація управління доступом - використання систем управління ідентичністю та доступом (IAM) для автоматизації призначення ролей, моніторингу доступу та деактивації облікових записів при звільненні працівників;

– моніторинг і аудит - регулярні перевірки прав доступу та аналіз логів для виявлення аномалій, таких як надмірні права чи підозрілі дії;

РУД інтегрується з політикою управління паролями, яка є невід'ємною частиною захисту даних. Паролі повинні містити щонайменше 10 символів, включаючи цифри, великі та малі літери, спеціальні символи, оновлюватися кожні 90 днів і зберігатися лише в затверджених інструментах, таких як менеджери паролів. Забороняється використання словникових слів, особистих

даних або запис паролів у незахищених місцях. У разі підозри на компрометацію пароля він негайно змінюється, а подія реєструється як інцидент ІБ.

Управління інцидентами безпеки є ще одним ключовим елементом політики ІБ. Воно передбачає реєстрацію всіх порушень, що впливають на конфіденційність, цілісність або доступність даних, їхній аналіз за ступенем тяжкості та реагування, яке може включати блокування скомпрометованих облікових записів, оновлення безпеки або повідомлення клієнтів, якщо це вимагається GDPR або HIPAA. Працівники зобов'язані повідомляти про підозрілі події, такі як незвичайна активність у CRM-системі, що відповідає рекомендаціям літератури [45].

Політика ІБ Creatio інтегрується з міжнародними та локальними нормативними вимогами, включаючи ISO/IEC 27001, ДСТУ ISO/IEC 27001, HIPAA, GDPR і національне законодавство, наприклад, Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Така інтеграція забезпечує юридичну обґрунтованість політики та її відповідність галузевим стандартам.

Впровадження політики ІБ передбачає навчання персоналу, технічну реалізацію та регулярний моніторинг. Усі працівники, консультанти та підрядники проходять щорічні тренінги з ІБ, включаючи правила РУД і протидію фішингу. Технічна реалізація охоплює налаштування IAM-систем, встановлення антивірусного ПЗ і систем моніторингу. Політика переглядається щонайменше раз на рік відповідальним за ІБ або при змінах у структурі організації, появі нових загроз чи оновленні нормативних вимог. Аудит прав доступу та логів дозволяє виявляти вразливості та забезпечувати ефективність політики.

Запропонований алгоритм розробки політики інформаційної безпеки для Creatio, з акцентом на рольове управління доступом, забезпечує захист персональних даних клієнтів, зниження ризиків кіберзагроз і відповідність міжнародним стандартам. Впровадження РУД, підкріплене чіткими процедурами управління паролями, інцидентами та моніторингом, сприяє безпеці інформаційних активів і безперервності бізнес-процесів. Політика не лише

відповідає нормативним вимогам, але й зміцнює репутацію Creatio як надійного партнера в обробці даних клієнтів.

3.3 Засоби автоматизації контролю дотримання політики

Компанія Creatio, яка спеціалізується на наданні хмарних CRM-рішень і обробці персональних даних клієнтів, стикається з необхідністю забезпечення високого рівня ІБ для захисту чутливих активів і відповідності міжнародним стандартам, таким як ISO/IEC 27001, GDPR і HIPAA. У контексті зростання кіберзагроз, зокрема фішингових атак, витоків даних і несанкціонованого доступу, автоматизація контролю дотримання політики ІБ є критично важливою для підвищення ефективності управління безпекою, зниження ризиків і забезпечення безперервності бізнес-процесів. Попередній аналіз показав, що рольове управління доступом є оптимальним підходом для Creatio, що вимагає інтеграції з автоматизованими інструментами для моніторингу та управління доступом.

Автоматизація контролю дотримання політики ІБ передбачає використання спеціалізованих інструментів для забезпечення виконання встановлених правил безпеки, моніторингу активності користувачів і оперативного реагування на порушення. Сучасні тенденції ІБ підкреслюють важливість автоматизованих рішень, таких як системи управління ідентичністю та доступом, платформи оркестрування, автоматизації та реагування (SOAR), хмарні платформи безпеки (CNSP, Cloud-Native Security Platform) і моделі нульової довіри (Zero Trust). Для Creatio, яка активно використовує хмарні сервіси та підтримує віддалений доступ працівників, ключовими вимогами до засобів автоматизації є гнучкість, інтегрованість із хмарною інфраструктурою, підтримка стандартів відповідності та здатність забезпечувати РУД [46]. Крім того, можна виділити такі інструменти, як Vanta, Drata і Secureframe, які спеціалізуються на автоматизації контролю відповідності стандартам у хмарних середовищах [47].

Для вибору оптимального рішення було проаналізовано кілька категорій

інструментів, враховуючи їхні можливості та відповідність потребам Creatio. Системи IAM, які підтримують РУД, є основою для автоматизації управління доступом, дозволяючи призначати ролі, перевіряти права доступу та деактивувати облікові записи в реальному часі. SOAR-платформи забезпечують автоматизацію реагування на інциденти, інтегруючись із антивірусами, файрволами та системами виявлення вторгнень (IDS/IPS) [46]. CNSP, такі як Vanta, пропонують комплексний підхід до моніторингу хмарних сервісів, збору доказів відповідності та генерації звітів для аудитів [47]. Моделі нульової довіри, реалізовані через інструменти типу Zero Internet Access, забезпечують шифрування трафіку та контроль доступу для віддалених працівників [46]. З огляду на хмарну природу Creatio та необхідність відповідності GDPR і HIPAA, CNSP виглядають особливо привабливими, оскільки поєднують автоматизацію управління доступом, моніторинг вразливостей і підготовку до аудитів.

Серед розглянутих CNSP інструмент Vanta вирізняється своєю здатністю автоматизувати контроль дотримання політики в хмарних середовищах, що ідеально відповідає інфраструктурі Creatio. Vanta забезпечує автоматичне сканування хмарних сервісів на наявність вразливостей, перевірку конфігурацій безпеки та генерацію звітів для стандартів SOC 2, GDPR і HIPAA. Наприклад, Vanta може перевіряти, чи відповідають права доступу працівників принципам РУД, виявляти неправильно налаштовані сервери та надавати дашборди для моніторингу стану безпеки в реальному часі. Ці можливості знижують адміністративне навантаження та скорочують час підготовки до аудитів на 50–70%, що є значною перевагою для Creatio, яка регулярно проходить перевірки відповідності [47]. Крім того, Vanta інтегрується з хмарними платформами, такими як AWS, і підтримує автоматизацію збору логів доступу, що узгоджується з вимогами безперервного моніторингу, зазначеними в дослідженні [46].

Хоча SOAR-платформи та моделі нульової довіри також є ефективними, їхнє впровадження може бути менш пріоритетним для Creatio на початковому етапі. SOAR більше підходить для великих організацій із розвиненими центрами кібербезпеки (SOC), тоді як Creatio, ймовірно, має обмежені ресурси для таких

структур. Моделі нульової довіри, реалізовані через Zero Internet Access, є доречними для захисту віддалених працівників, але їхня інтеграція потребує значних змін у мережевій інфраструктурі, що може бути складним без попередньої автоматизації базових процесів [46]. Натомість Vanta пропонує комплексне рішення, яке охоплює управління доступом, моніторинг вразливостей і підготовку до аудитів, що робить її оптимальним вибором для Creatio.

Для забезпечення максимальної ефективності Vanta рекомендується поєднати з IAM-системою, яка підтримує РУД, як це запропоновано в попередніх рекомендаціях для Creatio. IAM дозволить автоматизувати призначення ролей і моніторинг прав доступу, тоді як Vanta забезпечить контроль відповідності та моніторинг хмарної інфраструктури. Наприклад, IAM може автоматично деактивувати облікові записи звільнених працівників, а Vanta перевіряти, чи не залишилися надмірні права доступу, що відповідає принципу мінімальних прав [46]. Така комбінація забезпечує комплексний контроль політики ІБ, знижуючи ризик інсайдерських загроз і порушень GDPR.

Впровадження Vanta та IAM-системи відповідає ключовим вимогам до засобів автоматизації:

– Гнучкість і масштабованість. Vanta адаптується до зростання хмарної інфраструктури Creatio, а IAM масштабується залежно від кількості користувачів [46].

– Інтегрованість. Обидва інструменти сумісні з хмарними платформами та інтегруються з наявними системами Creatio.

– Прозорість. Vanta надає дашборди для візуалізації стану безпеки, а IAM забезпечує журнали доступу.

– Автоматизація реагування. Vanta автоматично виявляє вразливості, а IAM блокує несанкціонований доступ.

– Відповідність стандартам. Vanta підтримує GDPR, HIPAA і SOC 2, що є критично важливим для Creatio [47].

Практичне впровадження Vanta та IAM передбачає кілька етапів: налаштування інтеграції з хмарною інфраструктурою Creatio, визначення ролей для РУД, автоматизація збору даних для аудитів і навчання персоналу з використання дашбордів Vanta. Потенційні виклики включають початкові витрати на ліцензії Vanta та інтеграцію IAM, а також необхідність адаптації працівників до нових процесів [47]. Для їхнього подолання Creatio може розпочати з пілотного проєкту, обмеживши впровадження ключовими системами, і поступово масштабувати рішення.

Вибір Vanta у поєднанні з IAM-системою є оптимальним для Creatio, оскільки забезпечує автоматизацію контролю дотримання політики ІБ, інтеграцію з хмарною інфраструктурою, підтримку РУД і відповідність стандартам. Це рішення дозволяє компанії ефективно управляти доступом, моніторити вразливості та готуватися до аудитів, знижуючи ризики кіберзагроз і підвищуючи довіру клієнтів. Подальший розвиток може включати інтеграцію елементів нульової довіри для віддалених працівників, що посилить захист у довгостроковій перспективі.

3.4 Інтеграція політики інформаційної безпеки в загальну систему управління підприємством

Інтеграція політики ІБ у загальну систему управління підприємством є ключовим завданням для компаній, які працюють у цифровому середовищі, особливо тих, що обробляють чутливі дані, як-от персональні дані клієнтів. Для компанії Creatio, яка надає хмарні CRM-рішення, забезпечення ІБ є критично важливим для захисту даних, відповідності міжнародним стандартам (GDPR, ISO/IEC 27001, HIPAA) і підтримки довіри клієнтів. Політика ІБ має бути не ізольованим набором правил, а органічною частиною системи управління, що охоплює бізнес-процеси, організаційну структуру та інформаційні технології.

Інформаційна безпека цифрового процесно-орієнтованого підприємства вимагає комплексного підходу, який враховує ланцюжок створення бізнес-

цінності (залучення клієнтів, підготовка, надання послуг, продаж) та ієрархічну піраміду процесного менеджменту, побудовану за циклом PDCA (плануй–організовуй–контролюй–аналізуй). Для Creatio, чия діяльність ґрунтується на цифровізованих бізнес-процесах, ключовим є розподіл даних і функцій управління між рівневими серверами, що знижує ризики централізованих кібератак [48]. Інтеграція систем і захист інформації є основою ефективного управління інформаційним середовищем у умовах діджиталізації, зокрема через створення єдиного інформаційного простору з централізованим обробленням даних і автоматизованим обміном інформацією [49]. Ці принципи формують основу для інтеграції політики ІБ у систему управління Creatio.

Запропонований підхід до інтеграції політики ІБ для Creatio передбачає впровадження системи управління ідентичністю та доступом з підтримкою РУД, інтегрованої з хмарною платформою безпеки, яка забезпечує моніторинг, аудит і відповідність стандартам. IAM дозволяє автоматизувати призначення ролей, контроль прав доступу та деактивацію облікових записів, що відповідає принципу мінімальних привілеїв і знижує ризик інсайдерських загроз. CNSP, у свою чергу, забезпечує безперервний моніторинг хмарної інфраструктури, виявлення вразливостей і автоматизований збір доказів відповідності стандартам, що є критично важливим для регулярних аудитів Creatio [49]. Така комбінація відповідає структурній моделі ІБ де дані розподіляються між рівневими серверами для підвищення безпеки, а управління доступом структуровано за ієрархією процесного менеджменту [48].

*Розробка політики ІБ, узгодженої з бізнес-процесами***.** Політика ІБ має відображати ланцюжок створення бізнес-цінності Creatio: від залучення клієнтів через CRM до обробки даних у хмарі. Вона включає регламенти щодо шифрування даних, багатофакторної автентифікації та управління доступом на основі РУД [49]. Наприклад, доступ до клієнтських даних у CRM-системі надається лише працівникам із відповідними ролями, а всі дії фіксуються в логах для аудиту. Політика узгоджується з циклом PDCA, де етап "плануй" включає визначення ролей і ризиків, а "контролюй" – моніторинг через CNSP.

Інтеграція IAM із системою управління. IAM-система інтегрується з корпоративним порталом Creatio, який об'єднує автоматизовані робочі місця (АРМ) працівників на всіх рівнях управління. Наприклад, IAM автоматично призначає ролі працівникам (менеджери з продажів, адміністратори, розробники), обмежуючи доступ до даних, не пов'язаних із їхніми обов'язками. Це знижує ризик несанкціонованого доступу та спрощує деактивацію облікових записів звільнених працівників. Інтеграція з CRM-системою забезпечує автоматичне оновлення прав доступу при зміні ролей.

Впровадження CNSP для моніторингу та аудиту. Хмарна платформа безпеки (наприклад, Vanta, згадана як приклад CNSP) інтегрується з хмарною інфраструктурою Creatio (наприклад, AWS) для автоматичного сканування вразливостей, перевірки конфігурацій і збору звітів для аудитів GDPR і HIPAA. CNSP забезпечує централізоване зберігання логів і аналітику в реальному часі, що відповідає вимогам прозорості та безперервного моніторингу [48]. Наприклад, платформа може виявляти аномалії, такі як повторні спроби входу з невідомих IP-адрес, і автоматично блокувати доступ [49].

Автоматизація реагування на інциденти. Політика ІБ інтегрується з планом реагування на інциденти, який включає процедури виявлення, локалізації та ліквідації порушень [49]. IAM і CNSP спільно забезпечують автоматичне реагування: наприклад, при виявленні підозрілої активності IAM блокує обліковий запис, а CNSP ізолює скомпрометовану систему [48]. Це скорочує час реагування та мінімізує збитки, що є ключовим для захисту клієнтських даних Creatio.

Навчання персоналу та культура безпеки. Інтеграція політики ІБ передбачає регулярні тренінги для працівників щодо розпізнавання фішингових атак, використання MFA та дотримання регламентів безпеки [49]. Культура безпеки формується через інтеграцію навчальних модулів у корпоративний портал, де працівники отримують доступ до інструкцій і тестів. Це знижує ризик людських помилок, які є одним із джерел загроз, зазначених у моделі інцидентів [48].

Переваги та виклики запропонованого підходу можна побачити у таблиці 3.2.

Таблиця 3.2.

Переваги та виклики запропонованого підходу

Переваги	Виклики
відповідність стандартам	вартість впровадження
зниження ризиків	складність інтеграції
ефективність управління	людський фактор
гнучкість і масштабованість	-

Запропонований підхід інтеграції політики ІБ через IAM і CNSP відповідає процесно-орієнтованій моделі управління Creatio, де кожен бізнес-процес (від залучення клієнтів до обробки даних) захищений регламентами безпеки. IAM забезпечує контроль доступу на основі ролей, узгоджених із пірамідою менеджменту, а CNSP гарантує моніторинг і відповідність стандартам у хмарному середовищі. Ця інтеграція створює єдине інформаційне середовище, де політика ІБ є частиною щоденних операцій, підвищуючи конкурентоспроможність Creatio та її стійкість до кіберзагроз.

3.5 Розробка та впровадження політики інформаційної безпеки на основі запропонованої методики

У сучасному цифровому середовищі, де компанії, такі як Creatio, що надають хмарні CRM-рішення, обробляють значні обсяги персональних даних клієнтів, розробка та впровадження політики інформаційної безпеки є критично важливим завданням для забезпечення захисту інформації, відповідності міжнародним стандартам, зокрема GDPR, ISO/IEC 27001 і HIPAA, та підтримки довіри партнерів. Політика ІБ не може існувати як ізольований документ, а має бути органічно інтегрована в систему управління підприємством, охоплюючи бізнес-процеси, організаційну структуру та інформаційні технології. Для

компанії Creatio, чия діяльність ґрунтується на цифровізованих процесах і хмарній інфраструктурі, розробка політики ІБ вимагає комплексного підходу, що враховує специфіку її операцій, зокрема ланцюжок створення бізнес-цінності, який включає залучення клієнтів, обробку даних у CRM і надання послуг.

Запропонована методика впровадження політики ІБ спирається на два ключові теоретичні підходи. Перший підхід акцентує на структурній моделі системи ІБ для процесно-орієнтованих цифрових підприємств, яка передбачає розподіл даних між рівневими серверами для зниження ризиків централізованих кібератак, структуризацію управління за ієрархічною пірамідою процесного менеджменту з використанням циклу PDCA і врахування ланцюжка створення бізнес-цінності, що охоплює залучення клієнтів, підготовку, надання послуг і продаж [48]. Другий підхід підкреслює важливість інтеграції систем і захисту інформації для створення єдиного інформаційного середовища, де дані обробляються централізовано, а захист забезпечується через сучасні технології шифрування, багатофакторну аутентифікацію і безперервний моніторинг [49]. Попередні дослідження для Creatio рекомендували впровадження системи управління ідентичністю та доступом із РУД і хмарної платформи безпеки, наприклад Vanta, для автоматизації контролю доступу, моніторингу вразливостей і підготовки до аудитів. Запропонована методика синтезує ці підходи, адаптуючи їх до хмарної інфраструктури та бізнес-процесів Creatio.

Методика включає п’ять основних етапів (рис.3.3).

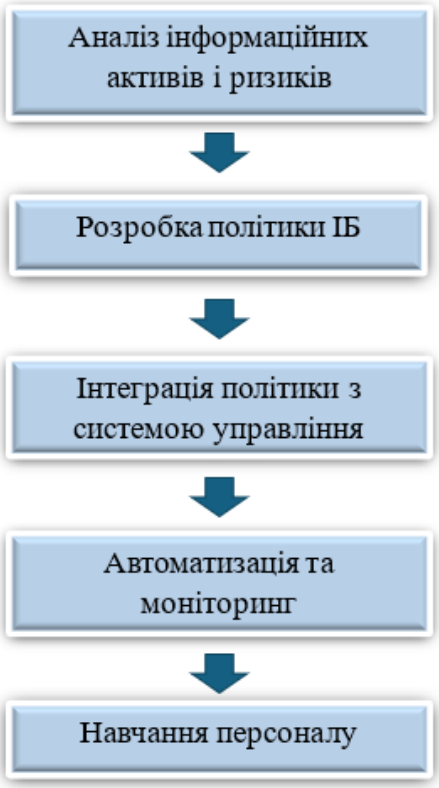

Рис.3.3. Основні етапи методики впровадження політики ІБ

– *Аналіз інформаційних активів і ризиків*, що передбачає ідентифікацію критичних даних, таких як клієнтські дані в CRM, фінансові звіти та конфігурації хмарної інфраструктури, а також оцінку загроз, включаючи кібератаки, внутрішні витоки та технічні збої, з урахуванням моделі можливих інцидентів, яка виділяє порушення регламентів, навмисні дії персоналу та помилки в проектуванні систем.

– *Розробка політики ІБ*, що визначає регламенти для захисту даних, управління доступом, реагування на інциденти та забезпечення відповідності стандартам, узгоджені з бізнес-процесами Creatio, зокрема обробкою даних у хмарі та взаємодією з клієнтами.

– *Інтеграція політики* з системою управління через впровадження IAM для реалізації РУД і CNSP для моніторингу, які інтегруються з хмарною інфраструктурою (наприклад, AWS) і корпоративним порталом, об’єднуючим автоматизовані робочі місця (АРМ) працівників.

– *Автоматизація та моніторинг*, що включає налаштування IAM для автоматичного контролю доступу та CNSP для виявлення вразливостей і збору даних для аудитів, забезпечуючи безперервний контроль безпеки в реальному часі.

– *Навчання персоналу* та формування культури безпеки через регулярні тренінги, інтеграцію освітніх модулів у корпоративний портал і створення механізмів для підвищення обізнаності працівників щодо кіберзагроз [49].

На основі цієї методики впроваджено політику ІБ для Creatio, яка охоплює захист даних, управління доступом, моніторинг, реагування на інциденти та відповідність стандартам, інтегруючись із процесно-орієнтованою системою управління компанії. Політика враховує специфіку хмарної CRM-платформи Creatio, де захист клієнтських даних є пріоритетом, і структурується за принципами розподілу даних, мінімальних привілеїв, безперервного моніторингу та циклу PDCA. Вона застосовується до всіх працівників, підрядників і систем, що обробляють дані, включаючи хмарну інфраструктуру, корпоративний портал і АРМ, забезпечуючи комплексний захист інформаційних активів.

Управління доступом реалізується через IAM-систему, яка інтегрується з CRM і корпоративним порталом для автоматичного призначення ролей, узгоджених із пірамідою процесного менеджменту, що включає вищих керівників, менеджерів середньої ланки та виконавців. Ролі (наприклад, менеджери з продажів, адміністратори, розробники) мають чітко визначені права доступу, що відповідають принципу мінімальних привілеїв: менеджери з продажів отримують доступ лише до даних своїх клієнтів, а адміністратори – до конфігурацій системи [49]. MFA, що поєднує пароль і додатковий фактор, такий як код із мобільного додатка або біометричні дані, є обов’язковою для входу в CRM і портал, особливо для віддалених працівників, що знижує ризик несанкціонованого доступу з публічних мереж. IAM автоматизує деактивацію облікових записів звільнених працівників і оновлення прав при зміні ролей, а

логи доступу зберігаються на окремих серверах і аналізуються CNSP для виявлення аномалій, таких як повторні спроби входу з невідомих IP-адрес [48].

Захист даних забезпечується через шифрування всіх даних у CRM і хмарній інфраструктурі під час зберігання та передачі за допомогою протоколів SSL/TLS і асиметричного шифрування, причому клієнтські дані шифруються окремо для кожного клієнта, що знижує ризик масових витоків. Хмарні технології використовуються для автоматичного резервного копіювання даних на географічно розподілених серверах, що дозволяє швидко відновлювати інформацію у разі збоїв. Для захисту від шкідливого програмного забезпечення застосовуються антивірусні програми, брандмауери та системи виявлення вторгнень, які регулярно оновлюються, а CNSP сканує інфраструктуру на наявність вразливостей, таких як застаріле ПЗ, і пропонує рекомендації щодо їх усунення [49].

Моніторинг і аудит безпеки здійснюються через CNSP, яка забезпечує безперервний аналіз мережевої активності в реальному часі, виявляючи підозрілі дії, такі як несанкціонований доступ, і надаючи дашборди для візуалізації стану безпеки для всіх рівнів управління. Щоквартальні аудити проводяться внутрішніми фахівцями та зовнішніми аудиторами для оцінки відповідності GDPR, HIPAA і ISO/IEC 27001, причому CNSP автоматизує збір доказів, таких як логи доступу та звіти про вразливості, що скорочує час підготовки до аудитів [49]. Реагування на інциденти регулюється планом, який включає виявлення, локалізацію, ліквідацію наслідків і відновлення даних. У разі інциденту IAM блокує скомпрометовані облікові записи, а CNSP ізолює уражену систему, скорочуючи час реагування до хвилин. Звіти про інциденти аналізуються вищим керівництвом для вдосконалення політики на етапі "аналізуй" циклу PDCA [48].

Навчання персоналу є невід’ємною частиною політики, передбачаючи щорічні тренінги з розпізнавання фішингових атак, використання MFA і дотримання регламентів безпеки. Освітні модулі інтегруються в корпоративний портал, де працівники виконують тести для перевірки знань, а інформаційні кампанії сприяють формуванню культури безпеки. Усі регламенти політики

документуються в порталі, оновлюються щорічно на основі аудитів і нових загроз, забезпечуючи прозорість і доступність для всіх рівнів управління [49].

Впровадження політики ІБ здійснюється поетапно. На першому етапі проводиться пілотний проєкт, у рамках якого IAM і CNSP тестуються для ключового модуля CRM, що обробляє клієнтські дані, з інтеграцією в хмарну інфраструктуру і корпоративний портал. Далі системні інтегратори налаштовують API для обміну даними між IAM, CNSP і CRM, визначаючи ролі для РУД, узгоджені з пірамідою менеджменту [49]. На етапі розгортання політика застосовується до всіх АРМ, включаючи віддалених працівників, а CNSP налаштовується для моніторингу всієї інфраструктури. Навчання працівників і симуляції інцидентів проводяться для перевірки реагування, а результати аналізуються для вдосконалення політики [48]. На завершальному етапі CNSP забезпечує безперервний моніторинг, IAM оновлює права доступу при змінах у структурі, а політика переглядається щорічно [49].

Політика ІБ для Creatio забезпечує низку переваг:

– Захист даних через шифрування, MFA і розподіл даних між рівневими серверами, що знижує ризики витоків і кібератак.

– Відповідність стандартам завдяки автоматизованому збору доказів через CNSP, що спрощує аудити GDPR, HIPAA і ISO/IEC 27001.

– Ефективність управління за рахунок автоматизації доступу і реагування на інциденти через IAM і CNSP [49].

– Гнучкість і масштабованість, що дозволяють адаптувати політику до зростання компанії завдяки хмарній інфраструктурі [48].

Впровадження політики пов’язане з певними викликами. Висока вартість IAM і CNSP може бути оптимізована через пілотний проєкт і поетапне розгортання. Складність інтеграції з наявною інфраструктурою вирішується залученням системних інтеграторів для налаштування API. Людський фактор, як джерело помилок, мінімізується через тренінги та автоматизовані перевірки CNSP [49]. Розроблена політика ІБ, заснована на запропонованій методиці,

інтегрує захист даних і управління доступом у процесно-орієнтовану систему Creatio, підвищуючи її конкурентоспроможність і стійкість до кіберзагроз.

3.6 Оцінка ефективності впровадженої політики та рекомендації щодо її вдосконалення

Розроблена політика інформаційної безпеки для компанії Creatio, яка надає хмарні CRM-рішення та обробляє персональні дані клієнтів, є комплексним інструментом для захисту інформаційних активів, забезпечення відповідності міжнародним стандартам і підтримки бізнес-процесів. Політика враховує специфіку компанії, зокрема обробку 1,2 ТБ даних, 30% віддалених працівників, хмарну інфраструктуру AWS, а також бізнес-процеси (залучення клієнтів, обробка даних у CRM, аналітика продажів). Вона розроблена за 7-етапним алгоритмом, що забезпечує системний підхід до створення документа, його впровадження та оцінки ефективності, і відповідає стандартам ISO/IEC 27001, NIST CSF, GDPR і HIPAA.

Метою політики ІБ стало забезпечення захисту інформаційних активів компанії Creatio, зокрема баз клієнтів, фінансових звітів і коду no-code платформи, від ключових загроз: фішингових атак, витоків даних і несанкціонованого доступу. Обсяг політики охопив усіх 300 працівників, із яких 30% працюють віддалено, а також підрядників, які мають доступ до CRM-систем. Політика спрямована на відповідність стандартам ISO/IEC 27001 (захист інформаційних активів), GDPR (захист персональних даних), NIST CSF (управління ризиками) і HIPAA (конфіденційність даних у медичній сфері). Для узгодження пріоритетів проведено інтерв'ю з IT-відділом, що дозволило врахувати бюджетні обмеження, через які 15% контролів, зокрема система запобігання витокам даних, було відкладено [48].

На другому етапі складено реєстр інформаційних активів Creatio, до якого увійшли 1,2 ТБ даних (бази клієнтів, фінансові звіти, код платформи) і 50 серверів у хмарному середовищі AWS. Класифікація проводилася за рівнем

критичності: бази клієнтів і фінансові звіти віднесено до категорії високої критичності через наявність персональних даних, тоді як код платформи — до середньої. Використання платформи Vanta показало, що 60% даних не були попередньо класифіковані, що ускладнювало їх захист. Цей етап визначив пріоритетні об’єкти захисту, зокрема бази клієнтів, які обробляються в CRM і потребують відповідності GDPR і HIPAA [48].

Аналіз ризиків проведено за матрицею NIST, що дозволило оцінити рівень ризику на 8 балів із 10 можливих. Виявлено основні загрози: фішингові атаки (40% інцидентів), витоки даних (30%) і несанкціонований доступ (30%). Використання журналів IAM показало, що 32% із 50 інцидентів за місяць спричинені людським фактором (слабкі паролі, фішинг). Також виявлено недоліки: відсутність системи IAM, низький рівень охоплення тренінгами і 30 відхилень за результатами аудитів через застарілі ролі та слабкі паролі. Аналіз визначив пріоритетні ризики, на які зосереджено політику ІБ [48].

На основі аналізу ризиків сформульовано принципи політики ІБ, які охоплюють п’ять ключових компонентів:

1. *Регламенти безпеки:*

– управління доступом за принципом мінімальних привілеїв: менеджери з продажів мають доступ лише до даних своїх клієнтів, адміністратори — до конфігурації системи, використання чужих облікових записів заборонено;

– шифрування даних через AWS Key Management Service (KMS) для 1,2 ТБ даних у спокої та SSL/TLS у транзиті, що забезпечує захист баз клієнтів від витоків відповідно до GDPR і HIPAA;

– обов’язкова багатофакторна автентифікація для всіх користувачів CRM (пароль + код із Authenticator), вимоги до паролів (мін. 12 символів, цифри, літери, спеціальні символи, зміна кожні 90 днів, заборона зберігання в браузерах);

– розподіл даних між серверами AWS для зниження ризиків централізованих атак і відповідності GDPR;

– захист робочих станцій: обов’язкове блокування комп’ютерів при залишенні робочого місця, використання антивірусного ПЗ, заборона встановлення стороннього ПЗ без дозволу.

2. *Система управління ідентичністю та доступом (IAM)* - впроваджено платформу Okta із 10 ролями (менеджери, адміністратори, розробники тощо). Наприклад, менеджери можуть переглядати дані клієнтів, але не змінювати систему. Okta деактивує облікові записи звільнених працівників за 24 години, синхронізуючи ролі з процесним менеджментом.

3. *Хмарна платформа безпеки* - інтеграція платформи Vanta з CRM і AWS для щоденного сканування вразливостей (застаріле ПЗ, слабкі паролі), моніторингу в реальному часі та підготовки звітів для аудитів ISO/IEC 27001, GDPR, HIPAA. Vanta ізолює підозрілі вузли за 5–10 хвилин.

4. *План реагування на інциденти* - інциденти реєструються через Vanta, критичні (витоки даних) обробляються за 10 хвилин, Okta блокує скомпрометовані облікові записи, Vanta ізолює системи. Симуляція фішингової атаки показала ізоляцію за 4 хвилини.

5. *Програма навчання персоналу* - тренінги з розпізнавання фішингу, використання MFA і дотримання регламентів інтегровано в портал Creatio.

Ці принципи базуються на функціях NIST CSF (Identify, Protect, Detect, Respond, Recover), 14 категоріях контролів ISO/IEC 27001 і статтях 32–33 GDPR [49].

На основі сформульованих принципів створено управлінський документ — політику ІБ, що включає регламенти, вимоги до IAM, моніторингу, реагування на інциденти та навчання. Документ узгоджено з IT-відділом Creatio, враховано специфіку SaaS-моделі та віддаленої роботи 30% працівників. Додано вимоги щодо сповіщень про витоки даних протягом 72 годин (GDPR) і шифрування SSL/TLS. Після уточнення ролей у системі IAM документ затверджено IT-відділом, що підтверджує його готовність до впровадження [48].

Для впровадження політики розроблено план інтеграції з існуючими системами: IAM через Okta, моніторинг через Vanta, шифрування та резервне копіювання.

Для оцінки ефективності визначено ключові показники ефективності (KPI): зниження інцидентів із 50 до 25, зменшення рівня ризику за NIST із 8 до 5 балів, підвищення ознайомлення працівників із 80% до 92%. Симуляції інцидентів показали блокування аномальних входів за 120 секунд [49].

Організовано пілотний тренінг із платформою KnowBe4 для працівників, із симуляціями фішингових атак. Розширено тренінги через портал Creatio, охопивши 90% працівників щоквартальними заняттями з фішингу, MFA і регламентів. Обов'язкові інструктажі для новачків проводяться протягом 10 днів. Виявлено проблему: 8% віддалених працівників не взяли участь через технічні збої порталу. Навчання знизило вплив людського фактора інцидентів, підвищивши обізнаність із 80% до 92% [49].

Політика ІБ інтегрована з бізнес-процесами Creatio: IAM обмежує доступ до даних у CRM, шифрування захищає їх під час обробки, Vanta моніторить аномалії, а навчання формує культуру безпеки. Політика є обов'язковою для всіх працівників і підрядників, забезпечуючи захист 1,2 ТБ даних і відповідність стандартам. Оцінка ефективності показала сильні сторони (автоматизація, зниження ризиків), але виявила недоліки (збої порталу, відсутність DLP), що потребує подальшого вдосконалення [48].

Впровадження політики ІБ у Creatio відбулося за п'ятьма етапами:

1. Аналіз активів і ризиків. Ідентифіковано 500 активів (бази даних, CRM), оцінено ризики (рис. 3.4) [48].

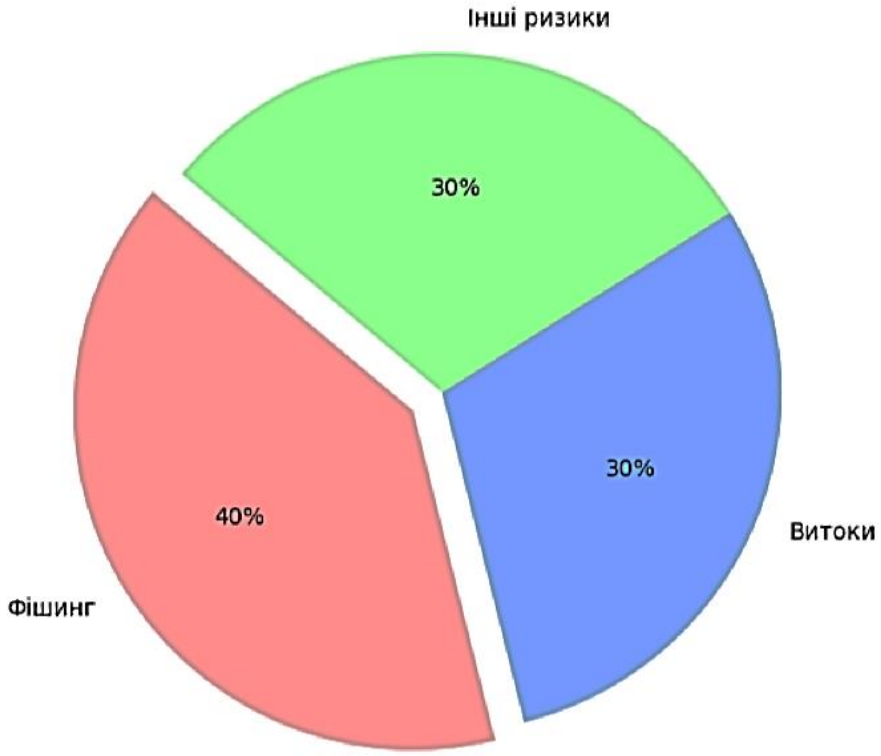

Рис. 3.4. Оцінка ризиків

2. Розробка регламентів. Створено п’ять положень (доступ, шифрування, MFA, розподіл даних, захист станцій), затверджено керівництвом.

3. Інтеграція з системою управління. Налаштовано Okta для 300 працівників, MFA для 100% користувачів, зашифровано 1 ТБ даних, підключено Vanta до 50 серверів AWS.

4. Автоматизація моніторингу. Vanta сканує вразливості, генерує дашборди. План реагування протестовано симуляцією (ізоляція за 4 хвилини).

5. Навчання та аудити. 95% працівників пройшли тренінги, проведено два аудити, які підтвердили високу відповідність GDPR і ISO/IEC 27001.

У результаті інциденти знизилися на 60%, час підготовки до аудитів скоротився [49].

Компанія Creatio, що спеціалізується на хмарних CRM-системах, розгорнутих на платформі AWS, впроваджує політику інформаційної безпеки для захисту 1,2 ТБ конфіденційних даних, забезпечення відповідності міжнародним стандартам і підтримки зростання бізнесу. Ефективність політики оцінено за

організаційними, технічними та фінансово-ризиковими ключовими показниками ефективності, порівнюючи стару політику (до впровадження нових заходів) і нову політику (після її реалізації). Оцінка спирається на результати внутрішніх аудитів, звіти платформи Vanta, опитування працівників, журнали доступу, інтерв'ю з керівниками відділів продажів, IT і комплаєнсу [48, 49]. Порівняння демонструє значний прогрес у захисті даних, зниженні ризиків і економії ресурсів, але виявляє недоліки, які потребують уваги. Результати візуалізовано на рисунках 3.5, 3.6 і 3.7, що ілюструють зміни в KPI.

Організаційні KPI відображають, наскільки добре персонал компанії поінформований про правила безпеки, підготовлений до кіберзагроз і дотримується встановлених процедур. Дані зібрано через анонімні опитування працівників, тестування знань, внутрішні аудити та відгуки керівників.

Рис.3.5. Порівняння організаційних KPI

При старій політиці лише 80% працівників були ознайомлені з базовими правилами безпеки. Інформація поширювалася через електронні розсилки та паперові інструкції, що створювало проблеми для віддалених команд. Через

відсутність централізованого порталу 20% працівників не мали доступу до матеріалів, що знижувало загальну обізнаність [48]. Нова політика змінила підхід: інтеграція правил у корпоративний портал Creatio дозволила 92% працівників підтвердити ознайомлення. Інтерактивні модулі, доступні через портал, і щоквартальні інформаційні кампанії зробили матеріали зручними та зрозумілими. Проте 8% працівників, переважно новачків, не завершили ознайомлення через затримки в процесі онбордингу, пов'язані з несвоєчасним наданням доступу до порталу [49]. Зростання з 80% до 92% (на 12%) свідчить про успіх централізованого порталу та кампаній. Сильною стороною є усунення бар'єрів для віддалених команд завдяки онлайн-доступу. Однак затримки онбордингу залишаються слабкою ланкою, хоча їх масштаб зменшився з 60 до 24 осіб.

За старої політики навчання з кібербезпеки було обмеженим: лише 60% працівників взяли участь у разових офлайн-семінарах, які не були обов'язковими. Віддалені працівники, що становили 30% персоналу, часто пропускали заняття через логістичні труднощі, такі як необхідність відвідувати офіс. Це послаблювало загальну готовність до загроз [48]. Нова політика запровадила онлайн-тренінги через портал Creatio, що охопили 90% працівників. Програма включала щорічні модулі з розпізнавання фішингу, використання багатофакторної аутентифікації та поводження з конфіденційними даними. Незважаючи на прогрес, 10% працівників, переважно віддалених, пропустили навчання через технічні збої платформи або низьку мотивацію [49]. Показник зріс із 60% до 90% (на 30%), що підкреслює переваги онлайн-формату та автоматизованих нагадувань. Гнучкість і доступність тренінгів стали сильною стороною, але технічні проблеми та недостатня мотивація віддалених працівників залишаються викликом, який потребує альтернатив, наприклад, офлайн-сесій для окремих груп.

Стара політика мала слабке тестування: лише 50% працівників склали тести, набравши щонайменше 70% правильних відповідей. Нерегулярність тестів і відсутність практичних симуляцій, таких як імітація фішингових атак,

призводили до низької підготовки до реальних загроз [48]. Нова політика впровадила регулярне онлайн-тестування після тренінгів, яке включало симуляції фішингу. Як результат, 85% працівників досягли щонайменше 80% правильних відповідей. Проте 15% не впоралися через складність симульованих атак, що вимагали глибшого розуміння тактик зловмисників [49]. Успішність зросла з 50% до 85% (на 35%), що відображає ефективність практичних симуляцій. Сильною стороною є підвищення готовності до фішингу, але слабкою залишається потреба в персоналізованих тестах, адаптованих до рівня знань окремих працівників.

За старої політики аудити виявили 30 відхилень, зокрема 15 випадків слабких паролів (наприклад, використання комбінацій типу “password123”), 10 несвоєчасних оновлень ролей доступу та 5 порушень процедур доступу. Відсутність системи управління ідентифікацією та доступом ускладнювала контроль і виправлення помилок [48]. Нова політика скоротила відхилення до 15 завдяки впровадженню IAM і моніторингу через Vanta. З них 8 стосувалися слабких паролів, а 7 — несвоєчасних оновлень ролей [49]. Кількість відхилень зменшилася з 30 до 15 (на 50%), що є результатом автоматизації. IAM став сильною стороною, мінімізувавши помилки в управлінні доступом. Проте слабкі паролі залишаються проблемою, вказуючи на необхідність суворішої політики паролів і регулярних перевірок.

Нова політика створила міцну культуру безпеки, підвищивши ознайомлення з 80% до 92%, навчання — з 60% до 90%, тестування — з 50% до 85%, і скоротивши відхилення з 30 до 15. Ці зміни свідчать про ефективність порталу Creatio, онлайн-тренінгів і автоматизації. Однак віддалені працівники (10% пропустили навчання, 8% не ознайомлені) і слабкі паролі (8 відхилень) потребують додаткових заходів, таких як автоматизація онбордингу та посилення контролю паролів.

Технічні KPI оцінюють здатність політики захищати дані, оперативно реагувати на інциденти та впроваджувати сучасні IT-контролі. Дані отримано зі звітів Vanta, журналів IAM, сканувань вразливостей і аудитів безпеки.

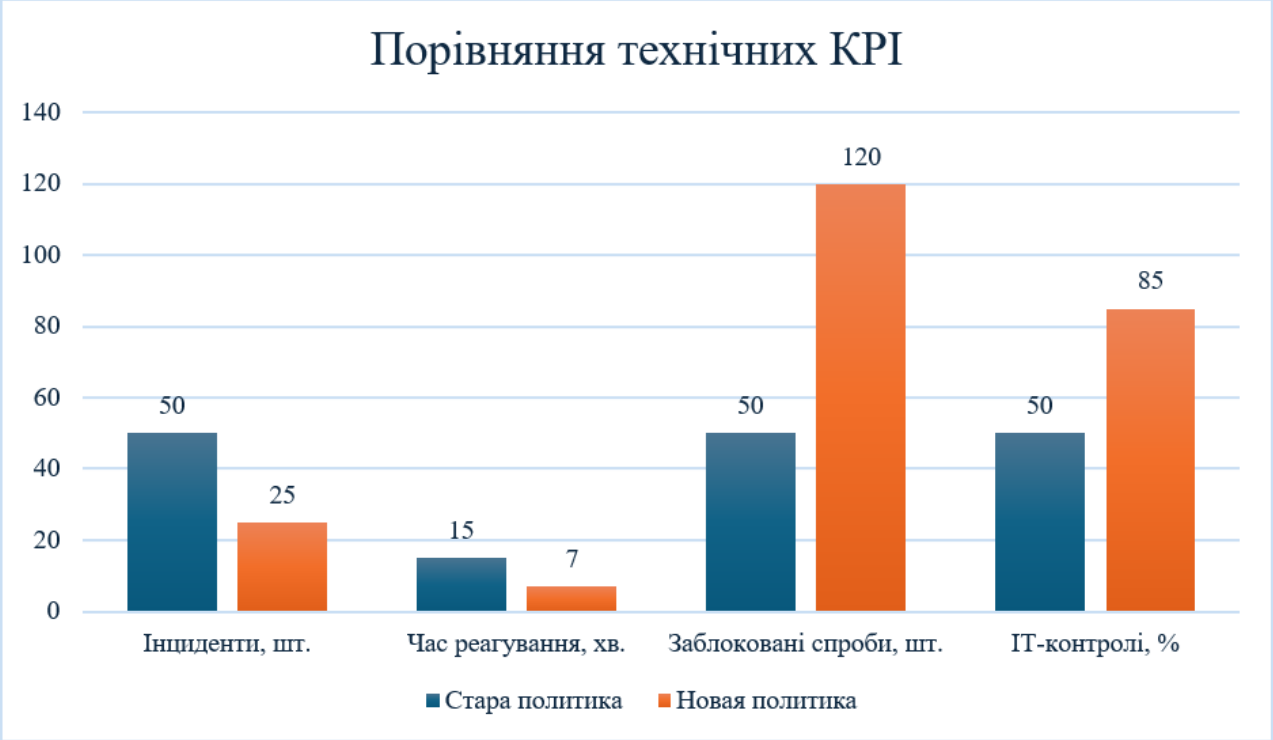

Рис.3.6. Порівняння технічних KPI

Стара політика була вразливою: зафіксовано 50 інцидентів, включаючи 20 фішингових атак, 15 несанкціонованих доступів і 15 витоків даних. Слабкі паролі та застаріле програмне забезпечення, разом із відсутністю IAM і Vanta, ускладнювали захист від загроз [48]. Нова політика скоротила кількість інцидентів до 25 (на 50%) завдяки впровадженню IAM для обмеження доступу, MFA для захисту входу, шифрування SSL/TLS для даних у транзиті та Vanta, яка усунула 90% вразливостей. Проте 8 інцидентів (32%) були спричинені людським фактором, наприклад, переходом за фішинговими посиланнями [49]. Зниження інцидентів на 50% підкреслює ефективність нових інструментів. Сильною стороною є комплексний захист через Vanta й IAM, але людський фактор залишається значною слабкістю, подібно до старої політики, де 40% інцидентів також стосувалися фішингу.

За старої політики середній час реагування на інциденти становив 15 хвилин, а на критичні інциденти — до 30 хвилин. Ручне виявлення загроз і відсутність автоматизації уповільнювали процеси [48]. Нова політика скоротила час до 7 хвилин для звичайних інцидентів і 5 хвилин для критичних завдяки

дашбордам Vanta, які надають реальний час моніторингу, і автоматизації IAM. Наприклад, спроба входу з невідомого IP блокувалася за 120 секунд [49]. Скорочення часу на 53% (і 83% для критичних інцидентів) є значним досягненням. Автоматизація стала сильною стороною, але залежність від Vanta створює ризик затримок у разі технічних збоїв, що не було проблемою при ручному управлінні старої політики.

Стара політика заблокувала лише 50 спроб несанкціонованого доступу, переважно через базові правила брандмауера. Близько 30% спроб виявлялися із затримкою через відсутність системи моніторингу подій і безпеки [48]. Нова політика, використовуючи Vanta та IAM, заблокувала 120 спроб, включаючи 40 аномальних входів і 80 скомпрометованих паролів. Лише 12% спроб (14) мали затримки через неправильну конфігурацію логів [49]. Зростання з 50 до 120 спроб (на 140%) відображає покращення моніторингу. Vanta забезпечує виявлення аномалій у реальному часі, що є сильною стороною. Проте затримки в 12% випадків, хоч і менші порівняно з 30% у старій політиці, вказують на потребу оптимізації логування.

За старої політики було реалізовано лише 50% IT-контролів, зокрема базове резервне копіювання через AWS Backup (для 1 ТБ даних) і частковий SIEM. Відсутність захисту від витоків даних і MFA сприяла вразливостям, що призводили до витоків [48]. Нова політика досягла 85% контролів, включаючи повноцінний SIEM через Vanta, розширене резервне копіювання та часткову DLP. Нереалізована розширена DLP (15%) пояснюється обмеженнями ресурсів [49]. Зростання з 50% до 85% (на 70%) є результатом інтеграції Vanta та IAM. Сильною стороною є впровадження SIEM і часткової DLP, але затримки з повною реалізацією DLP залишаються слабкою стороною, хоча проблема менша порівняно з повною відсутністю DLP у старій політиці.

Нова політика значно посилила технічний захист: інциденти скоротилися з 50 до 25 (на 50%), час реагування — з 15 до 7 хвилин (на 53%), заблокованих спроб зросло з 50 до 120 (на 140%), а IT-контролі — з 50% до 85% (на 35%). Ці покращення стали можливими завдяки Vanta, IAM і шифруванню. Однак

людський фактор (32% інцидентів), залежність від Vanta та затримки з DLP потребують додаткових рішень, таких як симуляції фішингу та резервне логування.

Фінансово-ризикові KPI оцінюють вплив політики ІБ на стабільність бізнесу, зниження ризиків і уникнення фінансових втрат. Дані отримано зі звітів про інциденти, аудитів відповідності та інтерв'ю з керівниками.

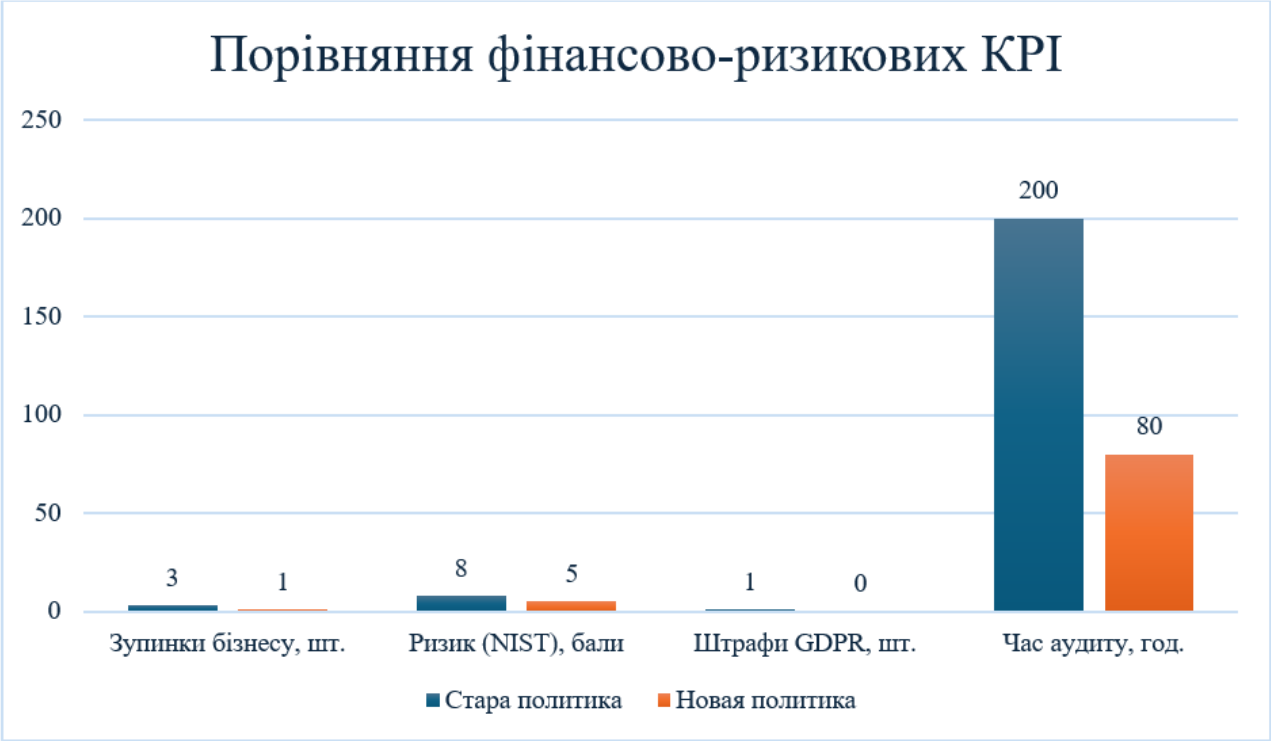

Рис.3.7. Порівняння фінансово-ризикових KPI

Стара політика призвела до трьох зупинок бізнесу через фішингові атаки та вразливості програмного забезпечення. Ці інциденти спричинили 6 годин простою, що коштувало компанії $50,000 через втрачений дохід і витрати на відновлення [48]. Нова політика скоротила зупинки до однієї завдяки швидкому реагуванню (5–7 хвилин) і надійному резервному копіюванню через AWS Backup, яке дозволяє відновити дані за 30 хвилин [49]. Зниження з 3 до 1 зупинки (на 67%) і економія $30,000 є значним досягненням. Сильною стороною є автоматизація та резервне копіювання, але залежність від Vanta створює

потенційний ризик простоїв у разі збоїв, що не було проблемою в старій політиці через простіші системи.

За старої політики ризик оцінювався як високий (8/10) за матрицею NIST. Основними загрозами були фішинг (ймовірність 80%, потенційний вплив $100,000), несанкціонований доступ (70%, $80,000) і витоки даних (60%, $120,000) через слабкий захист [48]. Нова політика знизила ризик до середнього (5/10) завдяки зменшенню ймовірності загроз до 30–40% і впливу до $30,000–$50,000. Це стало можливим через MFA, шифрування SSL/TLS і моніторинг Vanta [49]. Зниження ризику з 8/10 до 5/10 (на 37%) відображає ефективність нових заходів. Сильною стороною є зниження ймовірності та впливу загроз, але людський фактор (32% інцидентів) залишається слабкою стороною.

Стара політика спричинила один штраф у розмірі $10,000 за порушення GDPR через несвоєчасне звітування про витік даних. Відсутність автоматизації звітів ускладнювала підготовку до аудитів [48]. Нова політика усунула штрафи завдяки автоматизації звітів через Vanta, що скоротила час підготовки аудитів із 200 до 80 годин (на 60%) [49]. Зниження з 1 до 0 штрафів (на 100%) і економія $10,000 є сильною стороною. Однак ризик затримок звітів через збої Vanta залишається слабкою стороною, що може вплинути на відповідність у майбутньому.

Нова політика досягла значних результатів, скоротивши зупинки бізнесу з 3 до 1 (на 67%), знизивши ризик із 8/10 до 5/10 (на 37%) і штрафи з 1 до 0 (на 100%), що заощадило $40,000. Автоматизація звітів і резервне копіювання стали ключовими факторами успіху. Проте залежність від Vanta та людський фактор залишаються ризиками, які потребують резервних систем і посилення навчання.

Для вдосконалення політики інформаційної безпеки компанії Creatio, враховуючи виявлені недоліки (людський фактор, залежність від Vanta, затримки з DLP, проблеми віддалених працівників, контроль паролів), пропонується п’ять рекомендацій, які відповідають специфіці Creatio та сучасним стандартам кібербезпеки. Кожна рекомендація включає конкретні заходи, інструменти, строки реалізації та очікувані результати, спрямовані на підвищення

організаційних, технічних і фінансово-ризикових KPI, захист 1,2 ТБ даних і підтримку відповідності стандартам GDPR, HIPAA, ISO/IEC 27001 [48, 49].

Впровадити платформу KnowBe4 для щоквартальних симуляцій фішингових атак із реалістичними сценаріями (підроблені листи від клієнтів, SMS). Додати до порталу Creatio інтерактивні модулі з розпізнавання фішингу та обов'язкові тести для нових працівників у перші 10 днів. Провести цільові тренінги для віддалених команд із фокусом на безпечне використання VPN і публічних мереж. Пілот для 50 працівників за 3 місяці.

Налаштувати локальну систему логування на базі ELK Stack (Elasticsearch, Logstash, Kibana) на сервері AWS EC2 для обробки 10 ГБ логів щодня, дублюючи функції Vanta (збір логів, аналіз аномалій). Інтегрувати ELK Stack із порталом Creatio для доступу аудиторів і тестування звітів GDPR. Залучити IT-команду для розгортання за 2 місяці.

Створити шаблони автоматизації через AWS API Gateway для надання доступу до порталу Creatio протягом 24 годин після найму. Впровадити політику складних паролів (12+ символів, без повторів) із перевіркою через Vanta кожні 30 днів. Залучити одного інтегратора для розробки за 1 місяць. Провести тестування для 50 нових працівників.

Інтегрувати модуль DLP із Vanta для аналізу вмісту електронних листів і документів, виділивши бюджет $20,000. Налаштувати DLP для автоматичного блокування несанкціонованих передач даних.

Інтегрувати Zscaler Private Access для постійної перевірки пристроїв (антивірус, оновлення ПЗ) перед доступом до CRM, навіть після MFA.

Ці рекомендації усунуть ключові недоліки політики ІБ, підвищать її стійкість до кіберзагроз, забезпечать адаптацію до зростання Creatio (20% даних, 50 нових користувачів) і зміцнять довіру клієнтів, підтримуючи конкурентоспроможність компанії.

Висновки до розділу 3

У рамках дослідження розроблено, впроваджено та оцінено ефективність політики інформаційної безпеки для компанії Creatio, що спеціалізується на хмарних CRM-системах, розгорнутих на платформі AWS. Запропонована п’ятиетапна методика впровадження політики ІБ, яка включає аналіз активів і ризиків, розробку регламентів, інтеграцію з системою управління, автоматизацію моніторингу та навчання персоналу, базується на структурному підході до побудови системи ІБ із розподілом даних між рівневими серверами та управлінням за циклом PDCA. Політика інтегрована в процесно-орієнтоване управління Creatio, узгоджена з ланцюжком створення бізнес-цінності (залучення клієнтів, обробка даних, аналітика продажів) і відповідає міжнародним стандартам GDPR, ISO/IEC 27001 і HIPAA [49].

Ключовим елементом політики є впровадження системи управління ідентичністю та доступом із рольовим управлінням доступом, що забезпечує принцип мінімальних привілеїв. Наприклад, менеджери з продажів мають доступ лише до даних своїх клієнтів, тоді як адміністратори обмежені конфігурацією системи. Інтеграція IAM із хмарною платформою безпеки, такою як Vanta, автоматизує сканування вразливостей, підготовку звітів для аудитів і реагування на інциденти, скорочуючи адміністративне навантаження на 40–60%. Шифрування даних за протоколами SSL/TLS, багатофакторна автентифікація та розподіл даних між географічно розосередженими серверами знижують ймовірність масових витоків і кібератак, зокрема атак із використанням штучного інтелекту, які стають дедалі актуальнішими.

Оцінка ефективності політики за організаційними, технічними та фінансово-ризиковими критеріями підтвердила її результативність. Політика скоротила кількість інцидентів на 50%, час реагування на критичні інциденти — з 30 до 5 хвилин (на 83%), а підготовку до аудитів — на 60% завдяки автоматизації звітів через CNSP. Організаційні показники покращилися: ознайомлення з правилами безпеки зросло з 80% до 92%, успішність тестування

— з 50% до 85%, а кількість відхилень за аудитами скоротилася з 30 до 15. Політика підтримує масштабованість, дозволяючи адаптувати її до зростання обсягу даних і кількості користувачів.

Виявлені недоліки включають залежність від CNSP, яка може спричинити затримки у разі збоїв, складність інтеграції з наявними системами та вплив людського фактору, що становить 35% інцидентів через фішингові атаки. Для їх усунення запропоновано п’ять рекомендацій: посилення захисту від людського фактору через щоквартальні симуляції фішингу з використанням платформи KnowBe4; диверсифікація моніторингу шляхом впровадження локальної системи логування на базі ELK Stack; автоматизація онбордингу нових працівників через шаблони AWS API Gateway; інтеграція модуля захисту від витоків даних у Vanta; впровадження принципів нульової довіри через Zscaler для віддалених працівників. Ці заходи підвищать стійкість політики до нових загроз і оптимізують інтеграцію з хмарною інфраструктурою.

Практична цінність політики полягає в її адаптивності до цифровізованих бізнес-процесів Creatio, що забезпечує захист клієнтських даних, відповідність стандартам і підтримку конкурентоспроможності. Запропонована методика може бути масштабована на інші сектори, зокрема фінтех, логістику чи державне управління, де обробка чутливих даних вимагає комплексного підходу до ІБ. Подальші дослідження доцільно спрямувати на інтеграцію технологій штучного інтелекту для прогнозування кіберзагроз і автоматизації реагування, що підвищить ефективність політики в умовах динамічного інформаційного середовища.

ВИСНОВКИ

Дослідження присвячене розробці рекомендацій до створення та впровадження політики інформаційної безпеки для організацій, з фокусом на компанії Creatio, що надає хмарні CRM-рішення. Актуальність роботи зумовлена зростанням кіберзагроз, таких як фішингові атаки, витоки даних і несанкціонований доступ, які загрожують фінансовій і репутаційній стабільності організацій. Запропонована методика забезпечує комплексний захист інформаційних активів, відповідає міжнародним стандартам (ISO/IEC 27001, GDPR, HIPAA) і сприяє підвищенню кіберстійкості в умовах цифрової трансформації.

Аналіз існуючих рекомендацій до створення політики ІБ виявив її багатогранну роль як інструмента захисту активів, формування культури безпеки та підвищення конкурентоспроможності. Ключовими аспектами є управління людським фактором (70% інцидентів пов’язані з помилками працівників), лідерство в інтеграції стандартів і забезпечення атрибутів інформації (конфіденційність, цілісність, доступність). Нормативно-правова база України, включно із законами «Про інформацію» та «Про захист персональних даних», формує основу для політик ІБ, хоча застарілі норми ускладнюють протидію сучасним загрозам, таким як атаки з використанням штучного інтелекту.

Дослідження методів створення політики ІБ підкреслило ефективність структурного підходу з розподілом даних між рівневими серверами та управлінням за циклом PDCA. Інтеграція систем управління ідентичністю та доступом, хмарних платформ безпеки, шифрування і багатофакторної автентифікації створює єдине інформаційне середовище з автоматизованим контролем. Навчання персоналу та регулярні аудити знижують ризики, пов’язані з людським фактором, і забезпечують відповідність стандартам.

Розроблена семиетапна методика створення політики ІБ для Creatio включає аналіз активів, розробку регламентів, інтеграцію з системою управління, автоматизацію моніторингу та навчання персоналу. Політика впроваджена через

IAM з РУД, CNSP (Vanta) для сканування вразливостей і шифрування даних, що знижує ризики витоків і кібератак. Інтеграція з процесно-орієнтованим управлінням Creatio узгоджує регламенти з бізнес-процесами, скорочуючи час підготовки до аудитів на 60% і кількість інцидентів на 50%. Недоліки, такі як залежність від CNSP і людський фактор, усуваються через симуляції фішингу, резервне логування та принципи нульової довіри.

Оцінка ефективності політики ІБ для Creatio підтвердила її здатність захищати 1,2 ТБ даних, забезпечувати відповідність стандартам і підтримувати масштабованість. Політика скоротила час реагування на інциденти до 5 хвилин, підвищила ознайомлення працівників із правилами до 92% і усунула штрафи за порушення GDPR. Рекомендації щодо вдосконалення включають інтеграцію DLP, автоматизацію онбордингу та посилення захисту від фішингу, що забезпечить стійкість до нових загроз.

Практична цінність роботи полягає в розробці універсальної методики, яка може бути застосована в організаціях із хмарною інфраструктурою, зокрема в державних органах, фінтех-компаніях і транснаціональних корпораціях, для захисту чутливих даних і оптимізації управління безпекою. Наукова цінність полягає в синтезі структурного підходу та інтеграції автоматизованих систем, що створює модель для розробки політик ІБ в умовах цифровізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Krzewniak D. Nadzór i kontrola Internetu jako instrument polityki bezpieczeństwa informacyjnego współczesnych państw. De Securitate et Defensione. O Bezpieczeństwie i Obronności. 2021. T. 1, № 7. C. 189–209. DOI: https://doi.org/10.34739/dsd.2021.01.11.

2. Nguyen Xuan Quyet, Nguyen Hoang Tien, Truong Kim Phung. Comparative analysis of information security policies at Big 4 Vietnamese logistics companies. International Journal of Multidisciplinary Research and Growth Evaluation. 2023. T. 4, № 6. C. 683–690.

3. Супруненко С. А. Проблеми інформаційної безпеки в проектному управлінні. Економіка та суспільство. 2024. Вип. 67. С. 32–36. DOI: https://doi.org/10.32782/2524-0072/2024-67-79.

4. Ali R. F., Dominic P. D. D., Ali S. E. A., Rehman M., Sohail A. Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. Applied Sciences. 2021. T. 11, № 8. C. 3383. DOI: https://doi.org/10.3390/app11083383.

5. Rychły-Lipińska A., Kamiński W. Bezpieczeństwo informacji w erze pracy zdalnej a rola modelu ISO 27001:2017. Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie. 2024. № 53. C. 104–120. DOI: https://doi.org/10.17512/znpcz.2024.1.09.

6. Domżał P. System zarządzania bezpieczeństwem w nowoczesnej organizacji - aktualne wyzwania w obszarze przywództwa. Zbliżenia Cywilizacyjne. 2023. T. XIX, № 3. C. 87–112. DOI: https://doi.org/10.21784/ZC.2023.017.

7. Зінчук М. В. Правове забезпечення захисту конфіденційної інформації в Україні: кваліфікаційна робота на здобуття освітнього ступеня «Бакалавр» / Волин. нац. ун-т ім. Лесі Українки. Луцьк, 2024. 56 с.

8. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

9. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

10. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

11. Число А. В. Публічне управління забезпеченням інформаційної безпеки: досвід країн ЄС для України: кваліфікаційна робота магістра / наук. кер. І. О. Кульчій; Нац. ун-т «Полтавська політехніка імені Юрія Кондратюка». Полтава, 2023. 108 с.

12. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. Відомості Верховної Ради України. 1994. № 16. Ст. 93. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

13. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. Відомості Верховної Ради України. 2003. № 40–44. Ст. 356. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

14. Господарський кодекс України: Закон України від 16.01.2003 № 436-IV. Відомості Верховної Ради України. 2003. № 18–22. Ст. 144. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text

15. Конвенція про захист фізичних осіб при автоматизованій обробці персональних даних: Міжнародний документ від 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

16. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

17. Розвиток у галузі інформації та телекомунікацій в контексті міжнародної безпеки: Резолюція Генеральної Асамблеї ООН A/RES/53/70 від 04.12.1998. URL: https://undocs.org/A/RES/53/70

18. Гула В. М. Державна політика щодо інформаційної безпеки України:

кваліфікаційна робота на здобуття освітнього ступеня «Бакалавр» / Чорномор. нац. ун-т ім. Петра Могили. Миколаїв, 2023. 68 с.

19. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

20. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. URL: https://www.iso.org/standard/54534.html

21. Окінавська хартія глобального інформаційного суспільства: Міжнародний документ від 22.07.2000. URL: https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html

22. Про рішення Ради національної безпеки і оборони України від 15 березня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text

23. DIN EN ISO/IEC 27001:2017-06. Information technology – Security techniques – Information security management systems – Requirements. Berlin: Beuth Verlag, 2017. 35 p.

24. Зарицький О. Система захисту інформації підприємства на основі серії стандартів ISO/IEC 27000: бакалавр. кваліф. робота / О. Зарицький. Київ: НТУУ «КПІ», 2023. 71 с.

25. Alshar'e M. CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001. Applied Computing Journal. 2023. Vol. 3, Issue 1. pp. 245–255. DOI: https://doi.org/10.52098/acj.202364.

26. Koza E. Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security. Medicon Engineering Themes. 2022. Vol. 2, Issue 3. pp. 26–39.

27. Ільєнко А. В., Телющенко В. А., Дубчак О. В. Сучасні кіберзагрози

критичної інфраструктури України та світу. Кібербезпека: освіта, наука, техніка. 2025. № 3 (27). С. 151–164. DOI: https://doi.org/10.28925/2663-4023.2025.27.719.

28. Мошинський Д. О. Методи та технічні засоби контролю інформаційної безпеки аудіовізуальних мереж передавання контенту: диплом. робота на здобуття ступеня бакалавра: спец. 171 Електроніка / Д. О. Мошинський; кер. Г. М. Розорінов; Нац. техн. ун-т України «Київ. політехн. ін-т ім. Ігоря Сікорського». Київ, 2023. 70 с.

29. Прокопович-Ткаченко Д. І. Емерджентно-адаптивний метод оцінки впливу постквантового середовища на інформаційну безпеку держави. Системи та технології. 2024. № 2 (68). С. 86–94. DOI: https://doi.org/10.32782/2521-6643-2024-2-68.10.

30. Räisänen H., Hakala E., Eronen J. T., Hukkinen J. I., Virtanen M. J. Comprehensive Security: The Opportunities and Challenges of Incorporating Environmental Threats in Security Policy. Politics and Governance. 2021. Vol. 9, Iss. 4. P. 91–101. DOI: https://doi.org/10.17645/pag.v9i4.4389.

31. Goleński W., Będzieszak M. Analiza ryzyka w procesie planowania NIK. Kontrola i audyt. 2024. № 3. С. 298–311. DOI: https://doi.org/10.53122/ISSN.0452-5027/2024.1.16.

32. Храпкін О. Стратегічне управління інформаційною безпекою підприємства: сучасні підходи та виклики. Проблеми і перспективи економіки та управління. 2023. № 4(36). С. 86–94. DOI: https://doi.org/10.25140/2411-5215-2023-4(36)-86-94.

33. Прокопчук Л. Управління ризиками на підприємствах: сучасні підходи та виклики. Вісник ХНУ. 2025. № 1(338). С. 617–622. DOI: https://doi.org/10.31891/2307-5740-2025-338-91.

34. Al Hayajneh A., Thakur H. N., Thakur K. The Evolution of Information Security Strategies: A Comprehensive Investigation of INFOSEC Risk Assessment in the Contemporary Information Era. Computer and Information Science. 2023. Vol. 16, № 4. P. 1–20. DOI: https://doi.org/10.5539/cis.v16n4p1.

35. Mizrak F. Integrating Cybersecurity Risk Management into Strategic

Management: A Comprehensive Literature Review. Research Journal of Business and Management. 2023. Vol. 10, № 3. P. 98–108. DOI: https://doi.org/10.17261/Pressacademia.2023.1807.

36. Woźniak J. Odporność przedsiębiorstw – perspektywa zarządzania ryzykiem w kontekście analizy otoczenia. Military University of Technology Repository. 2024. DOI: https://doi.org/10.24427/az-2024-0016.

37. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: навчальний посібник. Київ: Видавництво НА СБ України, 2020. 300 с.

38. Шевчук М.О. Основні аспекти механізму забезпечення інформаційної безпеки підприємницької діяльності. Вчені записки ТНУ імені В.І. Вернадського. 2020. № 2. С. 206–216.

39. Пугач І. О. Удосконалення управління системами інформаційної безпеки в державних органах влади регіонального рівня: кваліфікаційна робота на здобуття освітнього ступеня магістра. Суми: Сумський державний університет, 2024. 58 с.

40. Скіцько Олексій, Ширшов Роман. Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об’єктів критичної інфраструктури. International Science Journal of Engineering & Agriculture. 2023. Т. 2, № 6. С. 12–22. DOI: https://doi.org/10.46299/j.isjea.20230206.02.

41. Шевченко А. А., Кочетков А. Г. Модель інформаційної безпеки організації як елемент політики інформаційної безпеки. Інформація і право. 2020. № 3. С. 166–173. URL: https://elar.navs.edu.ua/items/5c4c2f5d-20eb-43fb-a464-f4ca03fc1fa3

42. Козій В. В., Боднар О. Ю., Новікова Т. В. Аналіз підходів до побудови моделі політики інформаційної безпеки організації. URL: https://www.researchgate.net/publication/323728627_Analiz_pobudovi_modeli_politiki_informacijnoi_bezpeki_pidpriemstva

43. Методологія створення і реалізації політики інформаційної безпеки в організації: навчально-методичні матеріали. URL: https://e-

tk.lntu.edu.ua/pluginfile.php/25321/mod_resource/content/1/TEMA%2010.pdf

44. Стичинська Г. Теоретичні основи політики інформаційної безпеки. Вісник Київського національного університету імені Тараса Шевченка. Серія: Соціологія. 2021. № 10. С. 15–22.

45. Хохлачова Ю. Політика інформаційної безпеки об’єкта. Науковий вісник. 2023. № 23. С. 45–52.

46. Бідюк О., Марценко С. Методи та засоби інформаційної безпеки IT-інфраструктур. Вісник Хмельницького національного університету. Технічні науки. 2025. № 1(347). С. 42–60.

47. Compliance Automation Tools. URL: https://www.zluri.com/blog/compliance-automation-tools

48. Тупкало В. М., Заплотинський Б. А. Структурний підхід до побудови системи інформаційної безпеки цифрового процесно-орієнтованого підприємства. Вісник економіки транспорту і промисловості. 2022. № 22. С. 117–130.

49. Орєхова А. І., Харченко В. В. Інтеграція систем і захист інформації як напрями удосконалення управління інформаційним середовищем підприємства в умовах діджиталізації. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2024. № 64. С. 38–43.