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: “СИСТЕМИ АДАПТИВНОГО УПРАВЛІННЯ ПОЛІТИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ”

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

_____ Еріка ЛИСЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-41

Еріка ЛИСЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна КАПЕЛЮШНА
д.е.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
д.т.н., професор Ім’я, ПРІЗВИЩЕ

Київ 2026

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 кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____” _____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студентці Лисенко Еріці Максимівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Система адаптивного управління політиками інформаційної безпеки на підприємствах”,
керівник кваліфікаційної роботи Тетяна КАПЕЛЮШНА, д.е.н., доцент
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20” лютого 2026 р. № 51.

2. Строк подання кваліфікаційної роботи “12” травня 2026 р.
3. Вихідні дані до кваліфікаційної роботи: Організаційна структура та матеріали дослідження стану кіберзахисту ТОВ «BLYSKAVKA», міжнародні стандарти з інформаційної безпеки (зокрема ISO/IEC 27001), профільна наукова, технічна та нормативно-методична література за напрямом адаптивного управління та кібергігієни персоналу.

4. Перелік питань, які потрібно розробити:
1. Проаналізувати теоретичні засади управління ІБ в умовах нестабільності та обґрунтувати концепцію переходу до адаптивних політик безпеки.
2. Дослідити стан кіберзахисту підприємства, ідентифікувати актуальні вектори загроз (мережеві атаки, людський фактор) та оцінити методи навчання персоналу.
3. Спроєктувати архітектурну модель системи адаптивного управління ПІБ, розробити алгоритм її впровадження та обґрунтувати ефективність проєкту.
4. Перелік ілюстративного матеріалу; *презентація*
5. Дата видачі завдання “05” березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Аналіз основних характеристик інформаційного середовища користувачів та середовища загроз.	08.04.2026	
4.	Дослідження нормативно - правової бази у сфері захисту персональних даних та аналіз із міжнародними стандартами	15.04.2026	
5.	Дослідження можливих сфер впливу, генерації потенційних загроз внаслідок імплементації генеративного інтелекту	22.04.2026	
6.	Формулювання висновків зарезультатами дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	12.06.2026	

Здобувач вищої освіти _____ Еріка ЛИСЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Лисенко Е.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Система адаптивного управління політиками інформаційної безпеки на підприємствах "
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Лисенко Еріка 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 – Лисенко Еріки Максімівни
на тему: “Система адаптивного управління політиками інформаційної безпеки на підприємствах”

Актуальність. ~~У мовах динамічного розвитку кібератак перехід від статичних методів захисту до систем адаптивного управління політиками інформаційної безпеки є критично важливим. Урахування технологій підвищення обізнаності персоналу та формування кібергігієни робить дане дослідження надзвичайно актуальним науково-практичним завданням для сучасних підприємств.~~

Позитивні сторони

1. Успішно спроєктовано інноваційну архітектурну модель системи адаптивного управління політиками ІБ для ТОВ «BLYSKAVKA».
2. Робота оформлена згідно з вимогами ДСТУ, має чітку послідовність викладу, а ключові рішення наочно проілюстровані таблицями й рисунками.
3. Опрацьовано ґрунтовну джерельну базу, зокрема сучасні міжнародні стандарти (ISO/IEC 27001) та актуальні англомовні публікації.
4. Сформовано прикладний алгоритм впровадження системи та наведено розгорнуте техніко-економічне обґрунтування його ефективності.

Недоліки

У роботі доцільно було б приділити більше уваги порівняльному аналізу наявних на ринку програмних інструментів класу SIEM/SOAR. Проте зауваження має рекомендаційний характер і не знижує загальну високу цінність дослідження.

Висновок: Кваліфікаційна робота виконана на належному інженерному рівні, відповідає всім вимогам і заслуговує оцінки «відмінно», а її авторка ЛИСЕНКО Еріка - присвоєння кваліфікації бакалавра з кібербезпеки та захисту інформації за програмою «Управління інформаційною та кібернетичною безпекою».

Рецензент: завідувач кафедри
Систем та технологій
кібербезпеки,
д.т.н, професор _____ Галина ГАЙДУР
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра; 95 стор., 8 рис., 10 табл., 77 джерела.

Метою роботи теоретичне обґрунтування та практична розробка архітектурної моделі й алгоритму впровадження системи адаптивного управління політиками інформаційної безпеки для забезпечення стійкості корпоративної інфраструктури ТОВ «BLYSKAVKA».

Об'єктом дослідження є процес управління інформаційною та кібербезпекою сучасних підприємств в умовах високої динаміки загроз та ринкової невизначеності.

Предметом дослідження є методи, моделі, програмно-технічні інструменти адаптивного коригування політик безпеки та технології підвищення кіберобізнаності персоналу ТОВ «BLYSKAVKA».

Методи дослідження. Для вирішення визначених науково-практичних завдань використано методи системного аналізу, теорії ризиків, ризик-орієнтованого підходу, класифікації та порівняльного аналізу, математичного очікування (для оцінки запобіженого збитку), а також принципи проектування комплексних систем захисту інформації.

Галузь застосування Розроблені підходи, архітектурні рішення та алгоритми можуть бути безпосередньо використані ТОВ «BLYSKAVKA», а також іншими підприємствами корпоративного сектору для модернізації систем кіберзахисту та переходу від статичних до гнучких адаптивних політик безпеки.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, АДАПТИВНЕ УПРАВЛІННЯ, ПОЛІТИКА БЕЗПЕКИ, SIEM, МОНІТОРИНГ ТРАФІКУ, ТОВ «BLYSKAVKA», КІБЕРОБІЗНАНІСТЬ ПЕРСОНАЛУ, ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ, ROSI.

ABSTRACT

Text part of the qualification work for obtaining a bachelor's degree; 95 pages, 8 figures, 10 tables, 77 sources.

The purpose of the work is the theoretical substantiation and practical development of an architectural model and an implementation algorithm for a system of adaptive management of information security policies to ensure the resilience of the corporate infrastructure of "BLYSKAVKA" LLC.

Object of research the process of managing information and cyber security of modern enterprises in conditions of high threat dynamics and market uncertainty.

Subject of research methods, models, software and hardware tools for adaptive adjustment of security policies, and technologies for increasing cyber awareness of "BLYSKAVKA" LLC personnel.

Research methods. systems analysis, risk theory, risk-oriented approach, classification and comparative analysis, mathematical expectation (for assessing the prevented loss), and principles of designing comprehensive information protection systems.

Field of research cyber security and information protection management, development of adaptive security policies for corporate infrastructures.

KEYWORDS: ENTERPRISE INFORMATION SECURITY, ADAPTIVE MANAGEMENT, SECURITY POLICY, SIEM, TRAFFIC MONITORING, BLYSKAVKA LLC, PERSONNEL CYBER AWARENESS, ECONOMIC EFFICIENCY, ROSI.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

БД – Бази даних

ДБЖ – Джерело безперервного живлення

ІА – Інформаційний актив

ІБ – Інформаційна безпека

ІКС – Інформаційно-комунікаційна система

ІС – Інформаційна система

КСЗІ – Комплексна система захисту інформації

НД – Нормативний документ

НСД – Несанкціонований доступ

ПЗ – Програмне забезпечення

ПІБ – Політика інформаційної безпеки

САУ – Система адаптивного управління

СКУД – Система контролю та управління доступом

СУІБ – Система управління інформаційною безпекою

ТГ – Технічна група

ТЕО – Техніко-економічне обґрунтування

ТЗІ – Технічний захист інформації

ТОВ – Товариство з обмеженою відповідальністю

2FA – Two-Factor Authentication (Двофакторна автентифікація)

ABAC – Attribute-Based Access Control (Управління доступом на основі атрибутів)

API – Application Programming Interface (Інтерфейс програмування застосунків)

BCP – Business Continuity Plan (План безперервності бізнесу)

BYOD – Bring Your Own Device (Використання власних пристроїв)

CAPEX – Capital Expenditures (Капітальні витрати)

CIA – Confidentiality, Integrity, Availability (Тріада інформаційної безпеки: Конфіденційність, цілісність, доступність)

CVE – Common Vulnerabilities and Exposures (Загальновідомі вразливості та загрози)

DLP – Data Loss Prevention (Запобігання витоку даних)

DNS – Domain Name System (Система доменних імен)

Gap Analysis – Аналіз прогалин (Оцінка розриву між поточним та бажаним станом безпеки)

HTTPS – Hypertext Transfer Protocol Secure (Безпечний протокол передачі гіпертексту)

IAM – Identity and Access Management (Управління ідентифікацією та доступом)

IDS – Intrusion Detection System (Система виявлення вторгнень)

IPS – Intrusion Prevention System (Система запобігання вторгненням)

ISMS – Information Security Management System (Система управління інформаційною безпекою / СУІБ)

KPI – Key Performance Indicators (Ключові показники ефективності)

MDM – Mobile Device Management (Управління мобільними пристроями)

MFA – Multi-Factor Authentication (Багатофакторна автентифікація)

MTTD – Mean Time To Detect (Середній час виявлення інциденту)

MTTR – Mean Time To Respond / Resolve (Середній час реагування/відновлення)

NBAD – Network Behavior Anomaly Detection (Виявлення аномалій мережевої поведінки)

NVMe – Non-Volatile Memory Express (Протокол доступу до енергонезалежної експрес-пам'яті)

OPEX – Operating Expenditures (Операційні витрати)

PDCA – Plan-Do-Check-Act (Цикл Демінга: Плануй – Виконуй – Перевіряй – Дій)

PEP – Policy Enforcement Point (Точка застосування політики доступу)

PP – Payback Period (Період окупності)

RBAC – Role-Based Access Control (Управління доступом на основі ролей)

ROSI – Return on Security Investment (Окупність інвестицій у безпеку)

SFTP – SSH File Transfer Protocol (Безпечний протокол передачі файлів через SSH)

SIEM – Security Information and Event Management (Система управління інформаційною безпекою та подіями)

SMTP – Simple Mail Transfer Protocol (Простий протокол передачі пошти)

SOAR – Security Orchestration, Automation, and Response (Оркестрація, автоматизація та реагування на інциденти кібербезпеки)

SOC – Security Operations Center (Оперативний центр кібербезпеки)

SSH – Secure Shell (Безпечний протокол віддаленого керування)

SSH2 – Secure Shell Version 2 (Безпечний протокол віддаленого керування, версія 2)

SSO – Single Sign-On (Технологія єдиного входу)

TCO – Total Cost of Ownership (Загальна вартість володіння)

TLS – Transport Layer Security (Протокол захисту транспортного рівня)

UEBA – User and Entity Behavior Analytics (Аналітика поведінки користувачів і сутностей)

VPN – Virtual Private Network (Віртуальна приватна мережа)

WSS – WebSocket Secure (Безпечний протокол WebSocket)

Zero Trust – Архітектура «нульової довіри» (Zero Trust Architecture)

ВСТУП

Будь-яка надійна система захисту інформації на підприємстві починається не з встановлення дорогого програмного забезпечення, купівлі надсучасного мережевого обладнання чи найму великого штату технічних спеціалістів. Її фундаментом завжди виступає грамотно сформована політика інформаційної безпеки. Саме цей базовий документ визначає загальну стратегію компанії щодо захисту своїх інформаційних активів, регламентує правила організації робочого процесу та встановлює чіткі алгоритми дій на випадок виникнення позаштатних ситуацій. Інтерес до вивчення політики інформаційної безпеки зумовлений тим, що вона є головним сполучним елементом між складними технічними засобами захисту та звичайними працівниками. Навіть найбільш інноваційні технології шифрування чи виявлення вторгнень виявляються абсолютно безсилими, якщо внутрішні правила компанії написані надто складно, відірвані від реальних бізнес-процесів або настільки жорсткі, що працівники змушені їх свідомо порушувати, аби встигати виконувати свої щоденні робочі обов'язки.

Розгляд цієї теми набуває критичної ваги саме сьогодні, коли більшість підприємств змушені функціонувати в умовах постійних економічних змін, соціальної нестабільності та непередбачуваних кризових ситуацій. Протягом тривалого часу класичні підходи до створення політик безпеки передбачали розробку масивних, консервативних документів, які затверджувалися керівництвом на роки вперед і майже не підлягали перегляду. Однак сучасний ландшафт кіберзагроз розвивається набагато швидше, ніж оновлюються бюрократичні інструкції. Якщо внутрішні правила не еволюціонують разом із компанією та не враховують стрімких змін у навколишньому середовищі, вони перетворюються з інструменту захисту на серйозну перешкоду для нормальної операційної діяльності бізнесу. Коли виникає кризова ситуація, наприклад, необхідність термінового

переведення персоналу на віддалену роботу або швидкого перенесення даних на резервні сервери, старі статичні правила часто просто паралізують роботу компанії.

Саме тому виникає гостра необхідність повної відмови від застарілих консервативних підходів та переходу до систем адаптивного управління. У такій системі політика інформаційної безпеки перестає бути просто набором заборон і перетворюється на гнучкий, живий механізм. Адаптивне управління передбачає, що правила доступу, рівні контролю та загальні вимоги до безпеки можуть динамічно змінюватися залежно від поточного рівня загроз, стану мережі та критичності бізнес-процесів у конкретний момент часу. Такий підхід дозволяє своєчасно реагувати на інциденти, не зупиняючи при цьому роботу всього підприємства, та забезпечувати максимальну продуктивність персоналу навіть в умовах підвищеного ризику. Крім того, адаптивна політика значно краще враховує людський фактор, допомагаючи формувати у співробітників свідому культуру кібергігієни, а не просто страх перед покаранням за порушення інструкцій.

З огляду на ці об'єктивні проблеми, головною метою даної роботи є комплексне дослідження та розробка практичних алгоритмів для побудови системи адаптивного управління політиками інформаційної безпеки на сучасних підприємствах. У центрі уваги перебуває безпосередньо сам процес безперервного управління безпекою в мінливих умовах зовнішнього та внутрішнього середовища організації. Відповідно, предметом детального вивчення виступають конкретні методи, організаційні інструменти та міжнародні нормативні стандарти, застосування яких дозволяє трансформувати жорсткі корпоративні правила у гнучкі та дієві на практиці механізми захисту.

Для досягнення поставленого результату в роботі послідовно вирішується цілий комплекс взаємопов'язаних завдань. На початковому етапі детально аналізуються теоретичні основи управління корпоративною безпекою, досліджуються ключові компоненти сучасних політик захисту та виявляються головні вразливості і недоліки традиційних підходів під час виникнення кризових

ситуацій. Наступним кроком є вивчення міжнародного досвіду управління ризиками та розробка концептуальної моделі адаптивної безпеки, яка відповідала б реаліям вітчизняного бізнесу.

Завдяки використанню методів системного та порівняльного аналізу, а також базових принципів ризик-менеджменту, у роботі формується покроковий дієвий алгоритм впровадження такої системи в існуючу організаційну структуру підприємства.

Отримані в ході дослідження результати мають чітке практичне спрямування. Запропоновані рекомендації, моделі та алгоритми не є суто теоретичними, а можуть бути безпосередньо використані реальними компаніями для аудиту та оновлення своїх внутрішніх нормативних баз. Практичне впровадження системи адаптивного управління політиками безпеки дозволить підприємствам знайти оптимальний баланс між надійним захистом корпоративних даних та зручністю повсякденної роботи персоналу. Це, у свою чергу, дасть змогу суттєво зменшити кількість внутрішніх та зовнішніх інцидентів інформаційної безпеки, захистити репутацію компанії на ринку та гарантувати стабільну, безперебійну діяльність організації навіть у найбільш складних і непередбачуваних економічних чи технологічних умовах.

Розділ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ АДАПТИВНОГО УПРАВЛІННЯ ПОЛІТИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Сутність та завдання політики інформаційної безпеки підприємства

Політика інформаційної безпеки - політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки [18].

В сучасних умовах, особливо для стратегічно важливих об'єктів та наукових установ, інформація є ключовим ресурсом. Політика інформаційної безпеки – набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проєктні рішення в області захисту інформації. На основі ПІБ будується керування, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поводження інформаційних систем у різних ситуаціях.

Ефективна політика інформаційної безпеки визначає необхідний та достатній набір вимог безпеки. Вона мінімально впливає на продуктивність праці, враховує особливості бізнес-процесів підприємства, підтримується керівництвом, позитивно сприймається й виконується співробітниками підприємства.

Відповідно до запропонованого підходу політика інформаційної безпеки реалізується відповідною структурою органів на основі нормативно-методичної бази з використанням програмно-технічних методів і засобів, що визначають архітектуру системи захисту.

Політика інформаційної безпеки передбачає наступне:

– продемонструвати співробітникам важливість захисту мережного середовища,

– описати їхню роль у забезпеченні безпеки

– розподілити конкретні обов’язки по захисту інформації, що циркулює в мережі, так само як і самої мережі [1].

Політика інформаційної безпеки розроблена відповідно до внутрішніх нормативних документів компанії, вимог чинного законодавства України, ДСТУ ISO/IEC 27001:2023 “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”, ДСТУ ISO/IEC 27002:2023 “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”, та з урахуванням міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту (Відповідає вимогам міжнародного стандарту ISO/IEC 27001:2022).

Метою цієї Політики інформаційної безпеки є встановлення загальних принципів, стандартів та вимог для забезпечення конфіденційності, цілісності та доступності інформації, а також виконання вимог стандарту ISO/IEC 27001:2023.

Ефективне управління інформаційною безпекою на сучасному підприємстві не може бути однорідним; воно вимагає побудови чіткої ієрархічної структури, що охоплює різні пласти організаційної діяльності організації. Першим і найвищим ступенем у цій архітектурі виступає стратегічний рівень, який безпосередньо відповідає за формування загальної політики інформаційної безпеки . На цьому етапі вище керівництво підприємства визначає глобальні цілі захисту, оцінює бізнес-ризики, встановлює межі допустимих втрат та інтегрує безпекові пріоритети у загальну комерційну стратегію компанії [19]. Стратегічний рівень є точкою відліку для всієї системи захисту, оскільки саме на ньому закладається філософія кібергігієни установи та декларується ставлення організації до збереження конфіденційності, цілісності та доступності критичних даних.

Стратегічні наміри керівництва трансформуються в конкретні практичні вказівки на нормативно-методичному рівні. Цей рівень базується на впровадженні

визнаних міжнародних та національних стандартів, галузевих методологій і внутрішніх корпоративних регламентів [20]. Тут абстрактні цілі високого рівня перетворюються на задокументовані правила, детальні посадові інструкції для персоналу, методики регулярної оцінки ризиків та плани безперервності бізнесу на випадок кризових ситуацій. Нормативно-методичне забезпечення створює єдине правове та процедурне поле всередині підприємства, гарантуючи, що кожен співробітник чітко розуміє межі своїх повноважень, відповідальність та алгоритми дій під час повсякденної роботи чи в разі фіксації інциденту.

Безпосередня технічна реалізація затверджених регламентів розгортається на технічному рівні управління інформаційною безпекою. Він охоплює весь комплекс програмно-апаратних засобів, криптографічних методів, засобів автентифікації та мережевих протоколів (таких як TLS, IPsec, SSH), які фізично захищають інформаційні ресурси від несанкціонованого доступу [21]. На технічному рівні здійснюється безпосереднє проектування та налаштування міжмережевих екранів, систем виявлення та запобігання вторгненням (IDS/IPS), інструментів антивірусного захисту, контролю доступу до баз даних та систем моніторингу подій безпеки (SIEM). Цей рівень дозволяє автоматизувати рутинні процеси захисту та забезпечити миттєве реагування технічних засобів на кібератаки в реальному часі.

Найвищим етапом консолідації та гармонізації всіх зазначених ступенів захисту є інтеграційний рівень, який в умовах вітчизняного нормативно-правового поля реалізується через побудову Комплексної системи захисту інформації (КСЗІ). Інтеграційний рівень дозволяє об'єднати стратегічні вимоги, нормативні стандарти та розрізнені технічні протоколи в єдиний, законодавчо верифікований контур безпеки [22]. Створення КСЗІ передбачає системну інтеграцію організаційних заходів та інженерно-технічних рішень відповідно до вимог чинного законодавства України та нормативних документів у сфері технічного захисту інформації (НД ТЗІ) [23]. Це забезпечує не лише технологічну стійкість інформаційно-комунікаційних систем підприємства, а й їхню повну юридичну легітимність, спрощуючи

проходження державного аудиту та гарантуючи стабільну діяльність організації в умовах правової та військово-економічної нестабільності.

Політика інформаційної безпеки є документом верхнього рівня у системі управління інформаційною безпекою. Складові процесу управління інформаційною безпекою, які не зазначені у Політиці, представлені у інших внутрішніх нормативних документах компанії (порядках, процедурах тощо) та підтримується кількома іншими документами - політиками та процедурами [2].

Основними завданнями політики інформаційної безпеки підприємства є:

– Забезпечення конфіденційності інформації – захист інформаційних ресурсів від несанкціонованого доступу сторонніх осіб. Для цього застосовують засоби ідентифікації та автентифікації користувачів, розмежування прав доступу, шифрування даних, також контроль використання інформаційних ресурсів.

– Забезпечення цілісності інформації – цілісність інформації передбачає збереження достовірності, точності та повноти даних протягом усього періоду їх використання. Для досягнення цього завдання застосовуються системи резервного копіювання, контроль змін інформації, використання електричного підпису та журналювання подій. Порушення цілісності інформації може призвести до неправильного функціонування підприємства та прийняття помилкових управлінських рішень, тому забезпечення цілісності є одним із ключових принципів інформаційної безпеки.

– Забезпечення доступності інформації – доступність інформації означає можливість своєчасного отримання інформації авторизованими користувачами. Для цього необхідно забезпечити безперервну роботу інформаційних систем, створення резервних копій даних, використання систем відновлення після збоїв та захист від технічних несправностей.

– Управління ризиками інформаційної безпеки – важливим завданням ПІБ є виявлення, аналіз та оцінка ризиків, які можуть призвести до втрати або

пошкодження інформації. Управління ризиками включає визначення можливих загроз, оцінку їх впливу на діяльність підприємства та розроблення заході щодо їх мінімізації.

– Забезпечення відповідності законодавчим та нормативним вимогам - Політика інформаційної безпеки повинна відповідати чинному законодавству України та міжнародним стандартам у сфері інформаційної безпеки. Вона розробляється з урахуванням вимог стандартів, зокрема ISO/IEC 27001 та ISO/IEC 27002, які регламентують систему управління інформаційною безпекою.

– Захист інформаційних ресурсів підприємства – до завдань політики інформаційної безпеки належить захист інформаційних ресурсів підприємства від внутрішніх і зовнішніх загроз, включаючи комп'ютерні віруси, несанкціонований доступ та витік інформації. Захист інформаційних ресурсів передбачає впровадження організаційних, технічних і програмних заходів, що регламентують порядок роботи з інформаційними системами та ресурсами підприємства.

– Підвищення обізнаності персоналу у сфері інформаційної безпеки - ефективність ПІБ значною мірою залежить від рівня підготовки працівників підприємства. Тому одним з важливих завдань є навчання персоналу правилам безпечної роботи з інформацією, проведення інструктажів та формування відповідального ставлення до інформаційної безпеки.

– Забезпечення постійного вдосконалення системи інформаційної безпеки – ПІБ повинна регулярно переглядатися та оновлюватися відповідно до змін у технологіях, законодавстві та появі нових загроз. Дозволяє підтримувати актуальність заходів захисту інформації та забезпечувати ефективне функціонування системи інформаційної безпеки підприємства [3 – 4].

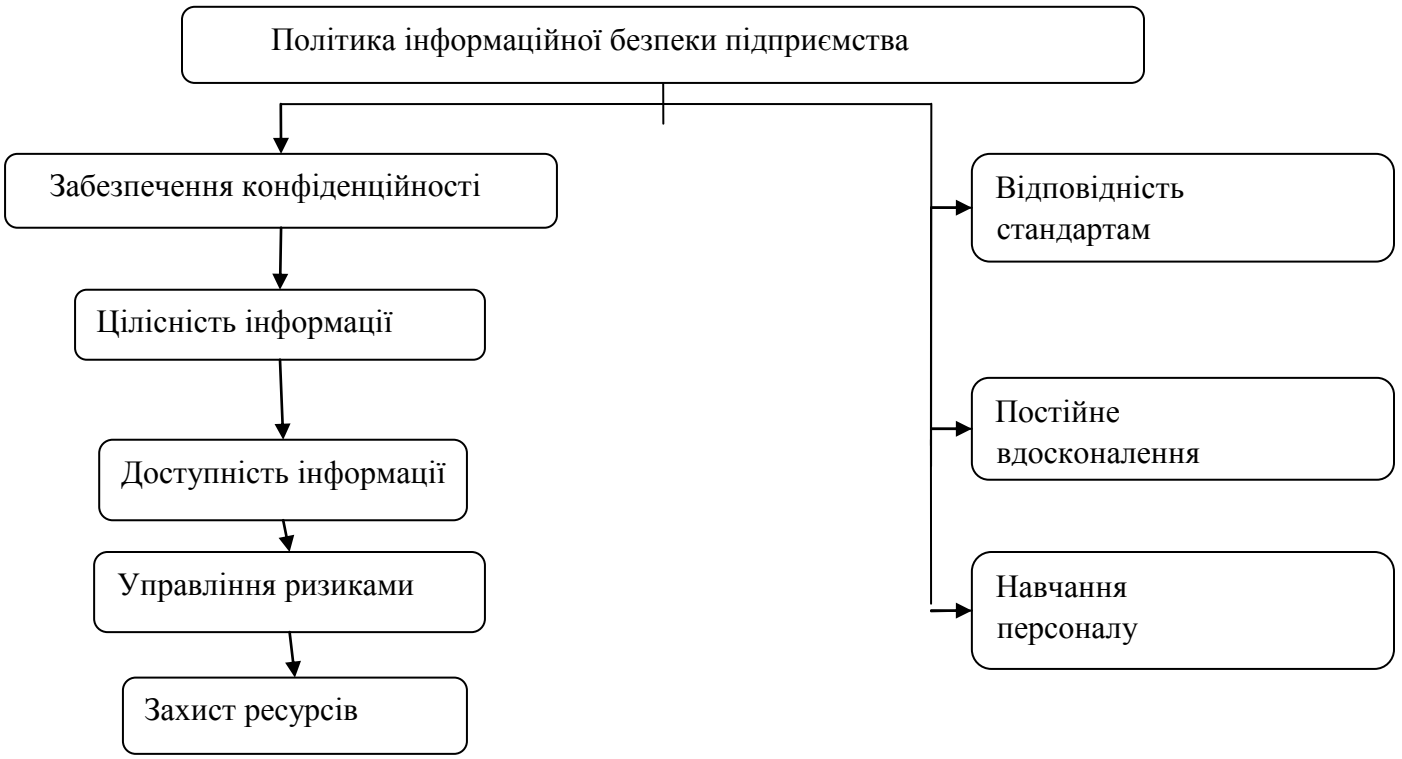

Рис. 1.1. Завдання політики інформаційної безпеки підприємства

Рис. 1.2. Ієрархічна структура рівнів управління інформаційною безпекою підприємства.

Таблиця 1.1.

Структурно-функціональна сутність, нормативна базу та завдання політики інформаційної безпеки підприємства

Рівень управління	Нормативно-правова база та стандарти	Функціональна сутність	Завдання ПІБ та керовані ризики
Стратегічний	Загальна комерційна стратегія розвитку підприємства. Корпоративна філософія кібергігієни	Формування концептуальних засад загальної ПІБ. Визначення глобальних бізнес-цілей захисту. Верхньорівнева оцінка бізнес-ризиків та визначення допустимих втрат	Постійне вдосконалення системи ІБ відповідно до нових загроз. Ризики: мінімізація стратегічних, Фінансових та репутаційних ризиків підприємства

Продовження таблиці 1.1.

Рівень управління	Нормативно-правова база та стандарти	Функціональна сутність	Завдання ПІБ та керовані ризики
Комплаєнсу	Міжнародний стандарт ISO/IEC 27001:2022 Засоби контролю ISO/IEC 27001:2023 Внутрішні корпоративні регламенти	Розробка детальних посдових інструкцій та правил роботи з ІС. Впровадження методик регулярної оцінки ризиків ІБ. Створення планів забезпечення безперервності бізнесу	Системне управління ризиками ІБ, підвищення обізнаності персоналу. Ризики: нейтралізація людського фактора, дій інсайдерів та внутрішніх витоків
Технічний	Внутрішні технічні регламенти підприємства. Криптографічні стандарти та мережеві протоколи безпеки (TLS, IPsec, SSH)	Проєктування та конфігурування програмно-апаратних засобів захисту. Налаштування між мережевих екранів, систем IDS/IPS, антивірусів та SIEM систем	Забезпечення тріади безпеки інформації (CIA). Ризики: захист від зовнішніх кібератак, масового шкідливого ПЗ та НСД
Інтеграційний	Законодавство України (щодо об'єктів критичної інфраструктури). Нормативні документи системи ТЗІ (НД ТЗІ)	Системна інтеграція організаційних заходів та інженерно-технічних рішень. Проектування та побудова КСЗІ	Комплексний захист критичних інформаційних ресурсів установи. Ризики: юридична легітимність(державний аудит)

1.2 Компоненти політики інформаційної безпеки та управління нею в умовах визначеності

Політика інформаційної безпеки підприємства є основоположним елементом системи управління інформаційною безпекою ISMS, яка визначає правила, процедури та механізми захисту інформаційних ресурсів організації. Відповідно до вимог стандарту ISO/IEC 27001, ПІБ визначає загальні принципи управління ризиками та забезпечення конфіденційності, цілісності та доступності інформації.

В умовах визначеності управління політикою інформаційної безпеки здійснюється за наявності повної інформації щодо загроз, ризиків та ресурсів захисту, що дозволяє застосовувати формалізовані процедури управління безпекою.

Відповідно до системного підходу, внутрішня структура політики безпеки сучасного підприємства має складатися з десяти базових взаємопов'язаних елементів:

– Призначення політики: визначає фундаментальну мету, ключові принципи та загальний концептуальний підхід організації до забезпечення інформаційної безпеки.

– Область застосування: чітко окреслює межі дії розробленої політики, які поширюються на внутрішні системи, операційні процеси, персонал, інформаційні ресурси та зовнішні сторони (контрагентів, партнерів).

– Цілі інформаційної безпеки (тріада CIA): визначає базові орієнтири захисту інформаційних активів установи — забезпечення їхньої конфіденційності, цілісності та доступності.

– Ролі та відповідальність: формалізує та закріплює конкретні ролі, функціональні обов'язки та межі відповідальності штатного персоналу у сфері кіберзахисту.

– Управління доступом: регламентує суворі правила ідентифікації, автентифікації, авторизації користувачів, а також механізми безперервного контролю їхнього доступу до корпоративних ресурсів.

– Управління ризиками: охоплює процеси ідентифікації, комплексного аналізу, оцінювання та подальшої обробки ризиків інформаційної безпеки з метою їх мінімізації.

– Управління інцидентами: встановлює чіткі процедури виявлення, оперативного повідомлення, локалізації, реагування, а також аналізу та повного відновлення систем після виникнення інформаційних інцидентів.

– Моніторинг та аудит: забезпечує безперервний автоматизований та ручний моніторинг подій безпеки, проведення регулярних аудитів, контроль відповідності вимогам та оцінку загальної ефективності впроваджених заходів.

– Документування та обізнаність: фокусується на веденні актуальної документації СУІБ та систематичному підвищенні рівня кібергігієни й обізнаності персоналу щодо чинних вимог безпеки.

– Перегляд та вдосконалення політики: передбачає проведення регулярного планового перегляду положень політики та її своєчасне вдосконалення з урахуванням появи нових технологій, загроз чи регуляторних вимог.

Процес управління політикою інформаційної безпеки (в умовах визначеності). Реалізація зазначених компонентів відбувається через класичний лінійний управлінський цикл, який складається з чотирьох послідовних стадій:

– Планування: визначення стратегічних цілей, ідентифікація ризиків, розрахунок необхідних ресурсів та розробка превентивних заходів.

– Впровадження: безпосередня практична реалізація затверджених вимог політики та розгортання технічних і організаційних заходів захисту.

– Контроль та моніторинг: системна перевірка виконання встановлених вимог, постійний моніторинг подій в ІКС та детальний аналіз отриманих результатів.

– Оцінка та вдосконалення: фінальна оцінка загальної ефективності системи та її постійне покращення.

В рамках організаційно-управлінського компоненту, для ефективного захисту інформації (ІБ) компанії "Технічної групи" необхідно дотримуватися встановлених правил та процедур, що регулюють використання її інформаційних активів (ІА). Усі співробітники "технічної групи " та сторонні особи, які мають доступ до інформації чи ресурсів компанії, мають бути ознайомлені з цією політикою та зобов'язані її виконувати. Для підтримки актуальності та ефективності політики, відповідальна особа з інформаційної безпеки повинна проводити її перегляд щонайменше раз на

рік. Перегляд також необхідний у разі значних змін у діяльності "технічної групи ", таких як: Зміни в робочих процесах. Зміни в організаційній структурі. Зміни в IT-інфраструктурі. Крім того, при розробці та впровадженні заходів безпеки слід враховувати: Законодавчі вимоги та договірні зобов'язання, що стосуються діяльності "технічної групи". Наслідки порушення Політики. Відповідальність керівництва "технічної групи " та інших осіб за безпеку інформації та систем компанії [74].

Управління безпекою інформаційних активів групи компаній (ІБ ТГ) належить до компетенції керівництва. Щоб знизити ймовірність несанкціонованих або ненавмисних маніпуляцій та зловживань, необхідно розділити конфліктуючі функції та сфери відповідальності. Чітке визначення відповідальності керівництвом сприяє стратегічній прозорості та ефективному впровадженню заходів ІБ. Керівництво відповідає за наступні аспекти: Ідентифікацію критично важливих операційних процесів групи. Формування стратегії розвитку ІБ групи. Затвердження та доведення до відома правил та вимог ІБ. Встановлення відповідальності за недотримання правил ІБ. Організацію моніторингу та контролю за виконанням правил ІБ. Додаткові відповідальні особи та їхні конкретні обов'язки детально описані в основній частині цієї Політики [74].

Усі працівники, які користуються внутрішньою мережею, мають ознайомитися з внутрішніми вимогами щодо роботи з інформаційними активами технічної групи та нести персональну відповідальність за їх виконання. Всі співробітники та відповідні залучені треті сторони зобов'язані проходити відповідне навчання для підвищення рівня обізнаності, а також регулярно отримувати оновлення щодо змін у політиках і процедурах організації відповідно до своїх посадових обов’язків. Програма підвищення обізнаності має забезпечувати, щоб кожен працівник мав та підтримував принаймні базове розуміння питань інформаційної безпеки, включно із загальними вимогами відповідно до політик, стандартів, процедур, керівних принципів, законодавчих і нормативних актів, договорів, а також загальноприйнятих

етичних норм та правил належної поведінки. Додаткові тренінги призначені для працівників, які мають спеціальні обов’язки з захисту інформації або які не володіють базовим рівнем знань з інформаційної безпеки у процесі своєї роботи, наприклад, для системних адміністраторів, відповідальних за інформаційну безпеку, керівного складу технічної групи. Вимоги до такого навчання повинні бути закріплені у персональних навчальних планах працівників [74].

Технічна група має забезпечувати підтримку Плану реагування на інциденти кібербезпеки, який базується на постійному оперативному моніторингу та відпрацьованих процедурах реагування на інциденти. Технічна група повинна регулярно організовувати навчальні заходи та підвищувати рівень обізнаності співробітників у сфері управління інцидентами. Також необхідно підтримувати та удосконалювати процес реагування на всі види інцидентів інформаційної безпеки згідно з Політикою реагування на інциденти кібербезпеки. Кожен працівник зобов’язаний інформувати Відповідальну особу за інформаційну безпеку у разі виявлення або підозри інциденту, який міг би загрожувати безперервності роботи технічної групи. Співробітники та сторонні особи можуть займатись розв'язанням інцидентів інформаційної безпеки лише на підставі чітких вказівок і за безпосереднім дозволом Відповідальної особи з ІБ [74].

З метою забезпечення безпеки та технічного контролю, технічна група залишає за собою право відслідковувати, вести записи та фіксувати всі дії, що здійснюються з інформаційними активами та у мережі організації. Технічна група зобов’язана надати необхідні ресурси для підтримки безперервної роботи та оперативного відновлення критичних систем у випадку виникнення надзвичайних ситуацій. Керівники підрозділів відповідають за встановлення вимог щодо захисту доступності систем, сервісів і даних, а також за їх виконання. Ці вимоги мають ґрунтуватися на проведеному аналізі ризиків, критичності активів, а також брати до уваги нормативні акти. Керівництво відповідає за забезпечення належного фінансування для реалізації цих заходів, а Відповідальна особа за ІБ — за підтримку

безперервності функціонування систем у разі екстрених ситуацій. Механізми аварійного відновлення є особливо чутливими до збоїв і не можуть вважатися надійними, якщо вони не проходять регулярні, документально оформлені тести [74].

В рамках людського компоненту (безпеки людських ресурсів), перед прийомом на роботу необхідно проводити перевірки кандидатів, працівників та третіх сторін, при цьому слід чітко враховувати рівень чутливості інформації, до якої вони отримуватимуть доступ, а також можливі ризики. Ці чинники визначають як обсяг, так і періодичність проведення відповідних перевірок. Призначення на посади та звільнення мають здійснюватися відповідно до вимог чинного законодавства України. Кожен співробітник ТГ та представник третьої сторони, які мають доступ до систем або даних ТГ, зобов'язаний відповідально використовувати їх виключно у межах діяльності ТГ та дотримуватися встановлених політик безпеки. Працівники та треті сторони несе відповідальність за своєчасне інформування керівництва про будь-які сумніви щодо дієвості заходів безпеки, а також про інциденти або спроби несанкціонованого або неправильного використання ресурсів ТГ. Керівництво ТГ має забезпечити виконання усіма працівниками та третіми сторонами вимог інформаційної безпеки відповідно до затверджених політик і процедур, а також слідкувати за дотриманням цих вимог. Припинення трудових відносин відбувається згідно з чинним трудовим законодавством України. Щодо навчання та підвищення обізнаності, усі співробітники, які користуються внутрішньою мережею, повинні бути ознайомлені з внутрішніми правилами щодо роботи з інформаційними активами ТГ і нести особисту відповідальність за їх виконання. Працівники та залучені треті сторони зобов'язані проходити регулярні навчальні заходи з підвищення рівня обізнаності та отримувати оновлення щодо змін у політиках і процедурах відповідно до своїх професійних обов'язків. Програма підвищення обізнаності має гарантувати, що всі співробітники мають принаймні базове розуміння питань інформаційної безпеки, включаючи загальні зобов'язання згідно з політиками, стандартами, процедурами, нормами законодавства, контрактними

вимогами та етичними стандартами. Додаткові навчальні курси передбачаються для працівників із специфічними обов’язками у сфері захисту інформації та для тих, хто не володіє достатнім базовим рівнем знань з інформаційної безпеки у рамках своєї роботи (наприклад, системних адміністраторів, відповідальних за безпеку, керівників технічної групи). Вимоги до такого навчання мають бути відображені у персональних планах розвитку працівників [74].

В рамках компоненту управління інформацією та даними, щодо класифікації та управління інформацією, інформацію необхідно систематизувати, ідентифікувати та оцінювати пов’язанні з нею ризики на основі параметрів конфіденційності, цілісності, доступності та контролю, незалежно від того, на якому носії вона зберігається чи обробляється. Особливо чутлива інформація визначається відповідно до зазначених характеристик. Вся інформація, окрім публічної, вважається чутливою. Незалежно від рівня конфіденційності, вся інформація організації повинна застосовуватися коректно та лише для визначених цілей. Розголошення обмеженої інформації можливе виключно у правомірний спосіб уповноваженим представникам влади, а також іншим фізичним чи юридичним особам за згодою організації, при цьому мають дотримуватись вимоги чинного законодавства України та відповідних договорів [74].

Щодо обробки, передачі та зберігання даних, чутливі дані повинні збиратися та зберігатися лише в тих системах, де існує обґрунтована виробнича або технічна необхідність. Такі дані потребують надійного захисту під час зберігання та використання у системах і мають бути безповоротно видалені, коли втратять свою актуальність. Необхідно впровадити та регулярно оновлювати діаграми або схеми потоків даних. Інвентаризація й класифікація даних обов’язково мають проводитись мінімум раз на рік. Чутливі дані не можна збирати чи використовувати для цілей, відмінних від тих, для яких вони були отримані первинно. Усі умови збереження інформації (строки, цілі тощо) мають відповідати законодавчим нормам на місцевому та міжнародному рівнях, що регламентують захист даних. Під час

інвентаризації чутливих даних слід визначати кожен конкретний елемент, законні місця його зберігання та необхідні заходи безпеки, наприклад, для захисту конфіденційності або цілісності даних під час їх зберігання та передачі. При зборі та зберіганні чутливих виробничих даних необхідно забезпечити належний захист, що може включати ефективний контроль доступу і/або використання надійних криптографічних методів із процедурами управління ключами, прийнятими у галузі інформаційної безпеки. Коли такі дані більше не потрібні, їх слід надійно видаляти, щоб виключити можливість відновлення або повторного використання з будь-яких систем [74].

Всі інформаційні активи ТГ мають бути ідентифіковані та зафіксовані в Реєстрі інформаційних активів (ІА). До таких активів можуть належати:

– дані про ТГ та її зацікавлених третіх осіб (підрядників, партнерів, клієнтів тощо);

– системи, сервіси або обладнання, де зберігається, обробляється чи передається інформація про ТГ та третіх осіб.

ТГ повинна регулярно проводити перегляди Реєстру ІА і визначати відповідальних за його обслуговування і перевірку. Реєстр має включати:

– власників інформаційних активів;

– їх найменування;

– рівень критичності для діяльності ТГ.

Власник ІА не несе фінансову відповідальність за актив, а відповідає за підтримання конфіденційності, цілісності, доступності й можливості відстеження інформації. Крім того, власники повинні забезпечувати належний контроль доступу до своїх активів [74].

Критерії класифікації активів і визначення тих, що є надзвичайно важливими для роботи ТГ (тобто активів, порушення безпеки яких може сильно вплинути на діяльність організації), повинні бути затверджені відповідно до внутрішніх

нормативів. Розподіл ролей і обов’язків для власників і користувачів активів теж має бути чітко визначений.

Щодо резервного копіювання:

– його необхідно здійснювати на регулярній основі;

– критично важлива інформація, програми та системи мають бути ідентифіковані для резервування;

– визначається графік створення копій і періодичність їх тестування;

– адміністратор систем встановлює тип резервних копій (повне, інкрементне, диференційоване) для кожної системи;

– резервні копії зберігаються окремо від основних даних і захищаються на тому самому рівні безпеки;

– доступ до них мають лише уповноважені співробітники ТГ;

– відповідальність за організацію резервного копіювання покладається на відповідальну особу з інформаційної безпеки.

Щодо безпеки комунікацій:

– має бути визначений перелік дозволених способів комунікації в межах ТГ і з третіми сторонами;

– необхідно обов’язково перевіряти вкладення з електронної пошти та месенджерів перед їх відкриттям;

– заборонено прямий доступ до ресурсів ТГ через прямі посилання;

– при передачі інформації слід користуватися тільки безпечними протоколами;

– в організації повинен функціонувати процес безпечного електронного спілкування, який враховує рівень конфіденційності переданих даних;

– у разі потреби використовуються додаткові методи захисту, наприклад, цифрові підписи або шифрування [74].

В рамках компоненту контролю доступу доступ до інформаційних ресурсів повинен надаватися відповідно до ролей, визначених у технічній групі, що полегшує процес управління користувачами.

Забезпечення доступу має базуватися на принципі мінімальних привілеїв, тобто користувачі отримують доступ лише до тих систем, які необхідні для їхньої роботи, а цей доступ повинен постійно контролюватися.

Відповідальність за призначення ролей користувачам та проведення регулярних перевірок покладається на Відповідальну особу із забезпечення інформаційної безпеки. Для кожної інформаційної системи повинна бути створена матриця доступу, яка міститиме детальну інформацію про права, що надані користувачам (перегляд, редагування, адміністрування) з відповідним позначенням рівня доступу. Легенда до матриці має бути документально оформлена і пояснювати значення кожного рівня (наприклад, A – адміністратор, E – редактор, R – читання/коментування, V – перегляд).

Всі запити на надання доступу мають бути затверджені безпосереднім керівником співробітника та Відповідальною особою з ІБ перед їхньою реалізацією. У випадку несанкціонованого доступу або підозрілої активності облікові записи користувачів повинні бути негайно заблоковані адміністраторами систем.

Використання двофакторної аутентифікації є обов’язковим у всіх системах і сервісах, де це можливо.

Відповідальна особа за інформаційну безпеку зобов’язана регулярно переглядати права доступу користувачів, дотримуючись узгоджених планів для всіх систем і інформаційних активів, особливо для критичних систем. Перегляди мають здійснюватися не тільки регулярно, але й після змін, таких як зміна посад або звільнення, а також при зміні ролі користувача у ТГ. Привілейовані права потребують більш частого та ретельного контролю, щоб уникнути несанкціонованого доступу. Доступ до мережі і мережевих сервісів надається лише

за потреби. Повинен бути налагоджений контроль за переглядом і керуванням цього доступу, що включає:

– встановлення переліку дозволених мереж і сервісів;

– визначення необхідного рівня доступу і користувачів, які його потребують;

– використання інструментів управління мережевими з'єднаннями та послугами;

– впровадження засобів і методів моніторингу використання мережевих ресурсів [74].

Щодо політики паролів, з метою надійного захисту інформаційних систем паролями, необхідно встановити такі умови:

– Мінімальна довжина пароля має становити від 8 до 12 символів;

– Пароль повинен відповідати вимогам складності;

– Він має включати великі і малі літери, цифри та спеціальні символи;

– Забороняється використовувати особисті дані користувача;

– Не слід застосовувати загальновживані слова;

– Мінімальний термін дії пароля — 1 день;

– Максимальний термін дії пароля повинен бути в межах від 30 до 90 днів;

– Заборонено зберігати паролі у вигляді, що допускає їх зворотне розшифрування;

– Сповіщення про необхідність зміни пароля повинне надходити за 7 днів до закінчення його терміну;

– Слід вести історію останніх 10 використаних паролів;

– Обліковий запис блокуватиметься після 5 поспіль невдалих спроб входу;

– Лічильник спроб блокування буде скидатися через 15 хвилин;

– Паролі повинні зберігатися та передаватися лише у безпечному вигляді, не у відкритому тексті [74].

Щодо використання електронної пошти, співробітники ТГ отримують доступ до електронної пошти з метою виконання своїх службових обов’язків. Використання електронної пошти у приватних чи інших не пов’язаних із роботою цілях забороняється.

У ТГ заборонено:

– Надсилати повідомлення, які містять конфіденційну інформацію, а також пересилати таку інформацію без необхідності для виконання службових завдань. Заборонено передавати логіни, паролі та інші конфіденційні дані через електронну пошту;

– Використовувати електронну пошту для особистих потреб;

– Підписуватися на розсилки маркетингового характеру без попереднього погодження з відповідальною особою з інформаційної безпеки;

– Відкривати вкладення, переходити за посиланнями чи запускати додатки в листах, якщо немає впевненості в надійності джерела інформації;

– Надсилати масові розсилки (більше 10 повідомлень) на зовнішні адреси без згоди керівника та відповідальної особи з ІБ;

– Розсилати поштою файли, що містять шкідливе програмне забезпечення або будь-які програми, які можуть пошкодити, знищити чи обмежити роботу комп’ютерного або телекомунікаційного обладнання, а також інформаційних систем;

– Надсилати програми, які дають можливість несанкціонованого доступу;

– Розповсюджувати електронною поштою матеріали, захищені авторськими правами, патентами, торговими марками, комерційною таємницею або іншими правами інтелектуальної власності третіх осіб;

Поширювати інформацію, заборонену законодавством України та міжнародними нормами, зокрема контент, що є шкідливим, образливим, нецензурним, порушує честь і гідність інших осіб, а також матеріали, які

провокують національну ворожнечу, насильство чи закликають до протиправних дій, в тому числі інструкції з виготовлення вибухових пристроїв, зброї тощо.

Доступ колишніх працівників до електронної пошти ТГ повинен бути негайно припинений і їхні облікові записи деактивовані [74].

Щодо дистанційного доступу, Інтернет-ресурси ТГ повинні використовуватись для віддаленого виконання робочих завдань, інформаційно-аналітичної роботи в інтересах ТГ, обміну поштою з третіми сторонами. Інше використання Інтернет-ресурсів слід розглядати як порушення.

Підключення до мережі Інтернет у ТГ повинно здійснюватися системним адміністратором у порядку надання прав доступу. При переміщенні співробітника (звільненні, переведенні в інший підрозділ) його безпосередній керівник повинен подати запит на скасування прав доступу.

Віддалене підключення до інформаційних активів ТГ має здійснюватися за допомогою визначених адміністратором систем та відповідальною особою за ІБ ресурсів.

З’єднання веб-зустрічей/віддаленого управління (наприклад, TeamViewer, AnyDesk) не повинні використовуватись у мережі ТГ для надання віддаленого доступу третім сторонам за замовчуванням. Цей тип підключень дозволений лише для технічного обслуговування та вирішення несправностей систем після належної авторизації [74].

В рамках технічного компоненту, окремо регулюється використання персональних пристроїв працівників (концепція BYOD). Технічна група (ТГ) може надавати дозвіл персоналу та іншим верифікованим користувачам застосовувати власні технічні засоби для виконання службових обов'язків з метою забезпечення безперервності бізнес-процесів. Для реалізації цього підходу ТГ розробляє та впроваджує чіткі вимоги з інформаційної безпеки (ІБ), які обов'язково доводяться до відома всіх співробітників і залучених контрагентів. Користувачі несуть індивідуальну відповідальність за суворе дотримання встановлених безпекових

протоколів та захисних заходів на особистих пристроях. Використання приватних засобів для доступу до внутрішньої інфраструктури та конфіденційних даних дозволяється виключно в робочих цілях; будь-яке порушення цього регламенту є підставою для негайного блокування та деактивації облікового запису користувача [74].

Щодо забезпечення безпеки мережі, обов’язковими до виконання на підприємстві є такі технічні вимоги:

– визначення та стандартизація безпечних конфігурацій для всього спектру мережевого обладнання;

– впровадження жорстких механізмів контролю доступу та автентифікації;

– розгортання й належне адміністрування систем безперервного моніторингу мережевої безпеки;

– своєчасне інсталювання актуальних системних оновлень;

– обмеження права на внесення конфігураційних змін — такі дії дозволені виключно системному адміністратору або уповноваженим особам;

– регулярне створення резервних копій системного програмного забезпечення, параметрів налаштувань та баз даних мережевих пристроїв.

Окремо визначаються параметри безпеки бездротових мереж (Wi-Fi), що передбачають:

– обов'язкову зміну заводських паролів та облікових даних за замовчуванням;

– деактивацію технології швидкого підключення WPS;

– приховання ідентифікатора мережі шляхом вимкнення функції SSID Broadcast;

– регулярне та вчасне оновлення мікропрограмного забезпечення (прошивки) обладнання;

– встановлення чітких лімітів на можливість підключення сторонніх пристроїв до локального сегмента мережі [74].

Для захисту даних у мережевому середовищі та корпоративних додатках ТГ здійснюється комплексне управління комунікаціями. Конфіденційність, цілісність, доступність та можливість технічного аудиту інформації під час її транзиту гарантується обов'язковим застосуванням криптографічних протоколів безпечного зв'язку. До використання в інфраструктурі ТГ затверджено такі протоколи: SSH2, SFTP, TLS (версій 1.2 та 1.3), HTTPS, WSS, SMTPS, а також DNS-over-HTTPS [74].

Стосовно експлуатації робочих пристроїв, ТГ впроваджує єдині стандарти безпеки технічних засобів та знімних носіїв інформації під час їх операційної діяльності. Усі корпоративні пристрої підлягають інтеграції до централізованої системи управління (MDM). На робочих станціях налаштовується обов'язкове автоматичне блокування екрана після визначеного періоду бездіяльності користувача. За наявності ризиків захист інформації посилюється шляхом повного шифрування жорстких дисків та встановлення складних паролів розблокування. Персонал несе персональну відповідальність за збереження та фізичну безпеку виданих пристроїв під час роботи поза межами офісу, мінімізуючи ризики доступу третіх осіб та дотримуючись правил блокування інтерфейсу. Контроль за виконанням цих вимог автоматизується спеціалізованим софтом, політики налаштування якого регулярно переглядаються на відповідність загальній стратегії безпеки організації [74].

В частині встановлення безпечних оновлень, ТГ регламентує процес патч-менеджменту для всіх інформаційних активів (ІА), які використовуються для доступу до сервісів та ресурсів компанії. Системний адміністратор забезпечує автоматичний або санкціонований ручний режим інсталяції виправлень. Антивірусні бази та інші захисні компоненти оновлюються в першочерговому порядку та проходять регулярну перевірку. Перед розгортанням патчів у виробничому середовищі (production) обов'язково проводиться їх тестування в ізольованій тестовій

зоні. ТГ здійснює постійний моніторинг офіційних ресурсів постачальників ІА для виявлення нових релізів та вразливостей [74].

Для операційних систем сімейства Windows конфігурується інструмент централізованого управління виправленнями для автоматичного завантаження актуальних пакетів безпеки Microsoft з їх подальшим контрольованим застосуванням. Системи на базі Linux оновлюються перевіреними, протестованими та адаптованими патчами. Системний адміністратор несе повну відповідальність за погодження, технічні зміни конфігурацій, інсталяцію драйверів, оновлень ПЗ та засобів захисту робочих станцій і мережевих пристроїв [74].

Щодо обмеження встановлення програмного забезпечення, в організації діють суворі правила контролю інсталяцій софту користувачами, засновані на концепції мінімальних привілеїв. Відповідальна особа з ІБ спільно з системним адміністратором формують списки дозволеного (whitelists) та забороненого (blacklists) програмного забезпечення. Звичайним користувачам заборонено самостійно встановлювати сторонні програми; будь-які винятки з цього правила потребують офіційного погодження адміністратором та офіцером з безпеки. Загальний нагляд за дотриманням субординації привілеїв та розподілом ролей здійснюють керівництво організації та відповідальна особа з ІБ [74].

З метою захисту від шкідливого програмного забезпечення (ПЗ), системний адміністратор здійснює попередню перевірку та тестування файлів перед їх запуском на пристроях, що мають доступ до корпоративної інфраструктури. До використання допускається лише верифікований та затверджений софт. Антивірусні сканери налаштовуються на автоматичний запуск перевірки відразу після оновлення сигнатурних баз. Політика антивірусного захисту передбачає:

- обов'язкове сканування систем під час завантаження;
- щоденну перевірку файлових і поштових серверів;
- щотижневий аудит інших серверних потужностей;

– сканування файлів «на льоту» при їх відкритті;

– фільтрацію вхідного/вихідного поштового трафіку та вкладень;

– веб-сканування вмісту під час синхронізації разом із перевіркою портативних накопичувачів (де це технічно можливо).

Системний адміністратор здійснює управління та регулярний аналіз журналів подій антивірусного ПЗ. Комплексна система протидії шкідливому софту включає планові перевірки, видалення інфікованих об'єктів або їх ізоляцію в карантині, логування інцидентів та централізоване управління процесом. Підключення до локальної мережі пристроїв без активного антивірусу або з виявленими загрозами суворо заборонено. Адміністратор систем проводить моніторинг патчів від розробників захисних рішень для їх вчасного впровадження. Загальний контроль за дотриманням заходів протидії шкідливому ПЗ покладено на відповідальну особу з ІБ [74].

В межах управління потужностями систем, ТГ здійснює безперервний моніторинг, оптимізацію використання апаратних та мережевих ресурсів, а також прогнозування майбутніх потреб для забезпечення стабільної продуктивності. Профільні фахівці проводять регулярний аудит інфраструктури, періодичність та вимоги до якого залежать від рівня пріоритетності та критичності конкретної інформаційної системи для діяльності компанії. Особлива увага приділяється високовартісним активам або компонентам, відновлення чи отримання яких є тривалим. Ключові показники ефективності (KPI) систем контролюються системним адміністратором та відповідальною особою з ІБ [74].

Стосовно логування та моніторингу подій безпеки, збору та аналізу у власних системах підлягають такі параметри подій:

– точна дата й час фіксації події;

– унікальний ідентифікатор користувача;

– тип запиту або характер дії;

– статус операції (успішно чи невдало);

– фіксація початкового і кінцевого стану системи при внесенні змін.

У разі неможливості автоматичного ведення логів або за умови їх недостатньої інформативності, ТГ впроваджує процедуру ручного збору аудиторських даних. Для запобігання несанкціонованій модифікації чи видаленню журналів подій (зокрема з боку привілейованих користувачів та адміністраторів), впроваджуються додаткові технічні засоби контролю та незалежної реєстрації дій [74].

Якщо наявні критично важливі системи не підтримують функцію аудиту дій адміністратора, ТГ ініціює перехід на нові версії або альтернативні платформи з відповідним функціоналом. У разі неможливості модернізації таких систем, ці технічні винятки підлягають обов'язковому погодженню з Керівництвом ТГ. Архівні сховища логів захищаються за допомогою комплексу організаційних заходів та спеціалізованих інструментів захисту [74]. Все це зображено на рисунку 1.3.

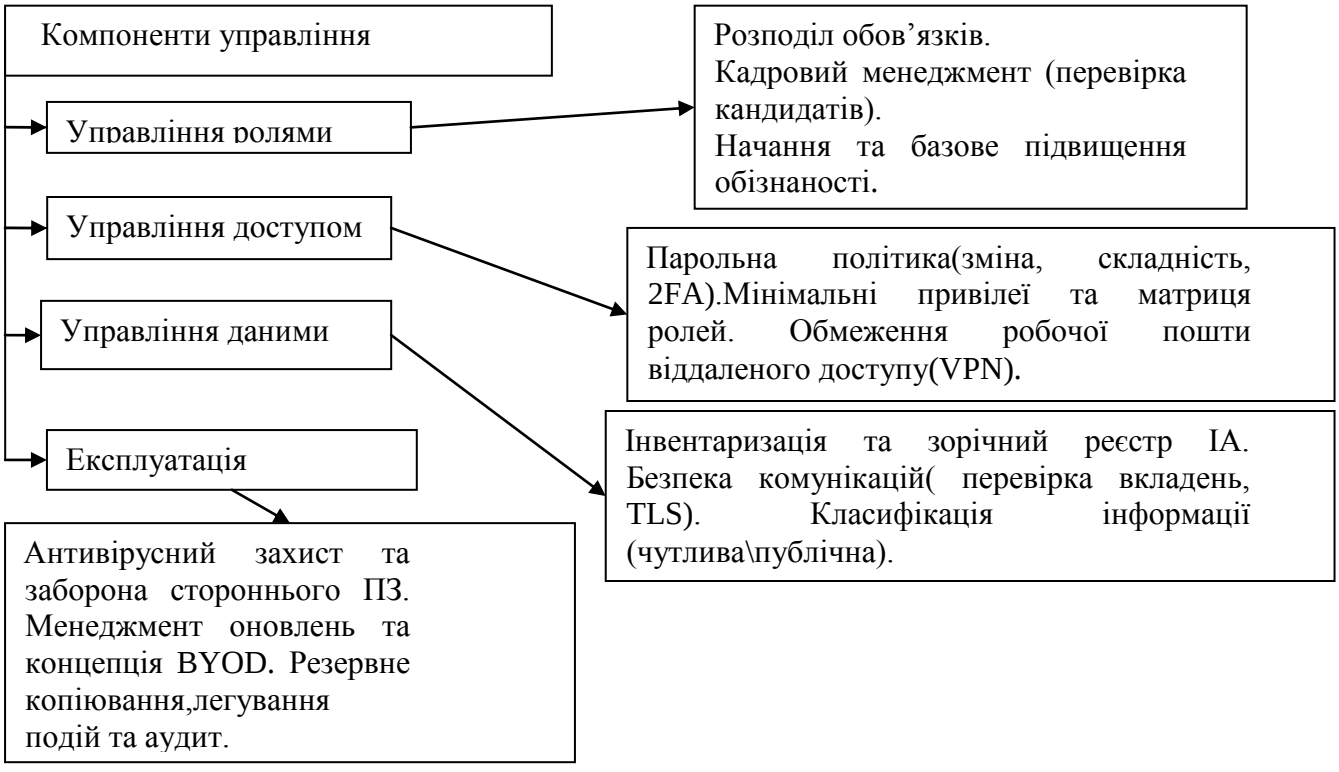

Рис. 1.3. компоненти ПІБ та управління нею в умовах визначеності.

Призначення (Purpose) ПІБ: визначає загальну мету захисту інформаційних ресурсів організації та встановлює основні принципи безпеки.

До основних завдань належать:

– Визначення загального підходу до ІБ
– Забезпечення захисту інформаційних активів
– Зменшення ризику витоку або втрати даних
– Забезпечення відповідності нормативним вимогам

Будь-яка ефективна ПІБ починається з формулювання її призначення, яке визначає загальні цілі та напрямки діяльності у сфері захисту інформації [5].

Область застосування (Scope): визначає межі дії ПІБ, включаючи:

– Інформаційні системи
– Персонал організації
– Мережеві ресурси
– Програмне забезпечення
– Зовнішніх користувачів

У стандартних структурах ПІБ область застосування визначає, які системи, процеси та користувачі підпадають під дію політики [5].

Цілі інфомаційної безпеки є: тріада CIA (конфіденційність, цілісність, доступність). Ці три принципи становлять основу управління ІБ та визначені у стандарті ISO/IEC 27001. Вони забезпечують захист інформації від несанкціонованого доступу, збереження точності інформації, доступність даних для авторизованих користувачей [6].

Компонент ролі та відповідальності визначає:

– Ролі керівництва
– Обов'язки персоналу
– Відповідальність завиконання вимог політики
– Контроль за виконанням заходів безпеки

У ПІБ повинні бути визначенні відповідальні особи за інтерпретацією, реалізацією та контроль виконання вимог політики [5].

Політика управління доступом визначає порядок:

– Ідентифікації користувачів
– Автентифікації
– Авторизації
– Контроль доступу

У стандарті ISO 27001 визначено необхідність створення політики контролю доступу до інформаційних ресурсів.

Управління ризиками є основним процесом управління ІБ, воно включає:

– Ідентифікацію ризиків
– Аналіз ризиків
– Оцінку ризиків
– Обробку ризиків

Стандарт ISO/IEC 27001 визначає необхідність впровадження процесу оцінки ризиків, як основного механізму управління безпекою.

Управління інцидентами включає:

– Виявлення інцидентів
– Повідомлення
– Аналіз
– Відновлення систем

ISO 27001 визначає необхідність створення процедур управління інцидентами безпеки [7].

Моніторинг та аудит дозволяє:

– Виявляти порушення
– Аналізувати події
– Контролювати ефективність заходів безпеки.

Стандарт ISO 27001 передбачає постійний моніторинг та перевірку процесів інформаційної безпеки [8].

Управління ПІБ в умовах визначеності характеризуються наявність чітко визначених параметрів середовища, ризиків та ресурсів. У таких умовах управління ПІБ здйснюється за моделлю:

- Планування заходів
- Впровадження політики
- Контроль виконання
- Вдосконалення системи

Модель PDCA використовується для постійного вдосконалення системи управління ІБ [8].

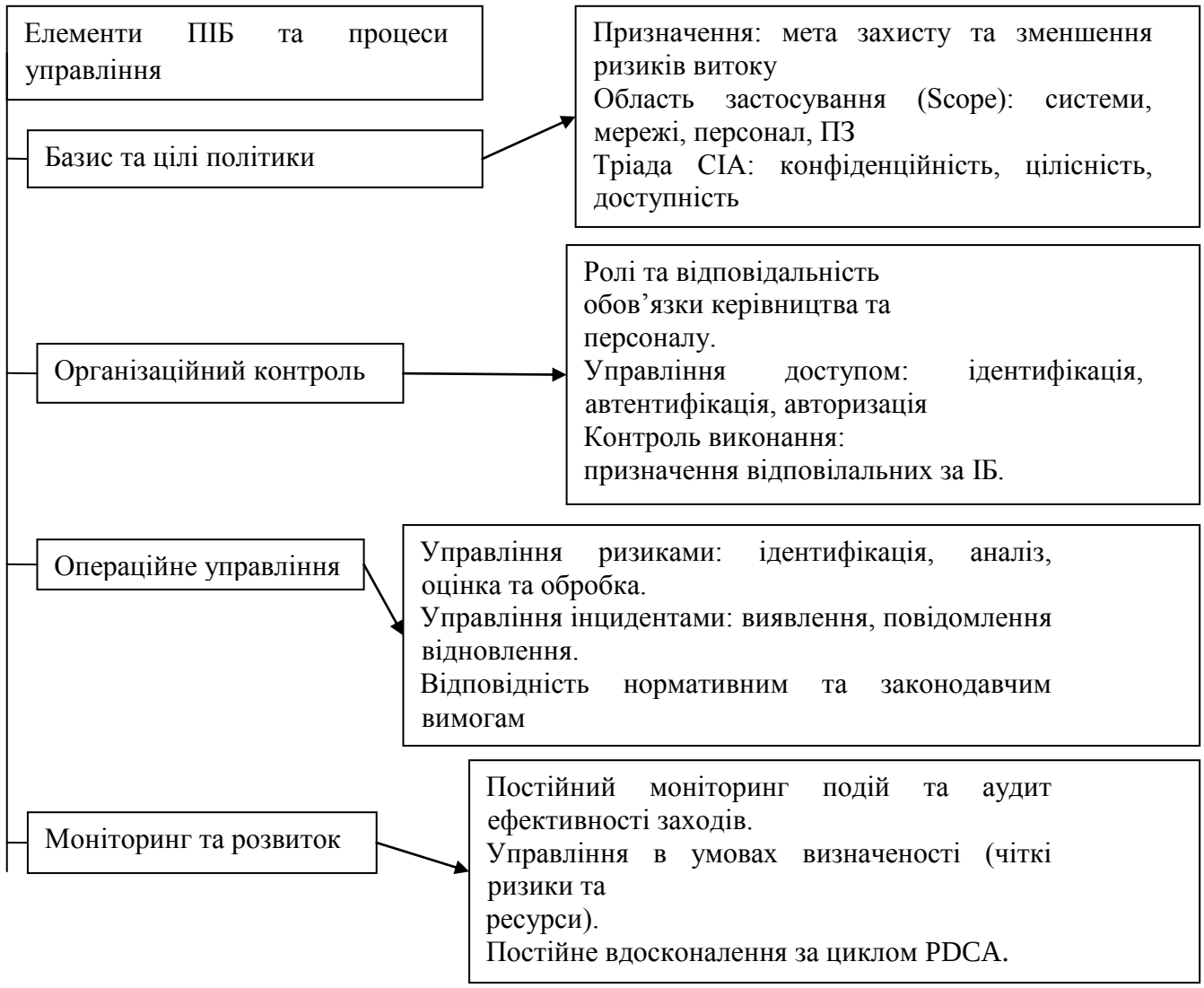

Рис. 1.4. Складові елементи ПІБ (модель PDCA)

1.3. Управління інформаційною безпекою підприємств та особливості формування політики інформаційної безпеки в нестійких умовах функціонування

Сучасні умови функціонування підприємств характеризуються високим рівнем невизначеності, динамічними змінами зовнішнього середовища та суттєвим зростанням кіберзагроз. Особливо це проявляється в умовах цифрової трансформації економіки, глобалізації інформаційних процесів, а також в умовах воєнного стану та

кризових явищ. У таких умовах інформаційна безпека підприємства перетворюється на критично важливий елемент забезпечення його стабільного функціонування та конкурентоспроможності [9].

Інформаційна безпека підприємства визначається як стан захищеності інформаційних ресурсів, при якому забезпечується їх конфіденційність, цілісність і доступність. Вона охоплює не лише технічні аспекти захисту даних, але й організаційні, правові та управлінські механізми, що регулюють обробку, зберігання та передачу інформації. У сучасних умовах інформаційна безпека розглядається як складова загальної системи управління підприємством, що безпосередньо впливає на ефективність бізнес-процесів [10].

Ключовим елементом системи інформаційної безпеки є політика інформаційної безпеки підприємства. Вона виступає базовим нормативним документом, який визначає принципи, правила та процедури захисту інформаційних активів. Політика інформаційної безпеки встановлює відповідальність працівників, регламентує рівні доступу до інформації та визначає механізми реагування на інциденти безпеки. Таким чином, вона формує основу для побудови комплексної системи управління інформаційною безпекою [11].

У наукових дослідженнях підкреслюється, що ефективне управління інформаційною безпекою повинно базуватися на системному підході, який враховує як внутрішні процеси підприємства, так і зовнішні загрози. До зовнішніх факторів належать кіберзлочинність, геополітична нестабільність, економічні кризи та технологічні ризики. Внутрішні фактори включають людський фактор, недостатній рівень цифрової грамотності персоналу та недосконаліть внутрішніх процедур безпеки [12].

Особливого значення набуває поняття нестійких або кризових умов функціонування підприємств. У таких умовах традиційні моделі управління інформаційною безпекою стають недостатньо ефективними через високу швидкість змін загроз та складність їх прогнозування. Це вимагає впровадження адаптивних

моделей управління, які здатні швидко реагувати на зміни зовнішнього середовища [13].

Адаптивний підхід до управління інформаційною безпекою передбачає безперервний моніторинг ризиків, оцінювання рівня загроз та оперативне коригування політики безпеки. Такий підхід дозволяє підприємствам не лише реагувати на інциденти, але й формувати превентивні механізми захисту, що значно підвищує рівень їхньої стійкості [14].

Важливою складовою сучасної системи інформаційної безпеки є ризик-орієнтований підхід. Він передбачає ідентифікацію потенційних загроз, оцінювання ймовірності їх реалізації та визначення можливих наслідків для підприємства. На основі цього формується система пріоритетів захисту інформаційних активів та розробляються відповідні заходи реагування [15].

Умови цифровізації економіки суттєво впливають на структуру інформаційних ризиків. Зростає залежність підприємств від інформаційних систем, хмарних технологій, корпоративних мереж та цифрових платформ. Це призводить до розширення поверхні атак та збільшення кількості потенційних вразливостей. У таких умовах політика інформаційної безпеки повинна постійно оновлюватися відповідно до змін технологічного середовища [16].

Окрему увагу слід приділити впливу воєнного стану та кризових умов, які значно підвищують рівень кіберзагроз. Підприємства стикаються з цілеспрямованими атаками на інформаційні системи, спробами несанкціонованого доступу до даних та порушенням роботи критичних сервісів. Це вимагає посилення заходів кіберзахисту та впровадження багаторівневих систем безпеки [17].

Дослідження показують, що ефективна система управління інформаційною безпекою повинна інтегруватися в загальну систему стратегічного управління підприємством.

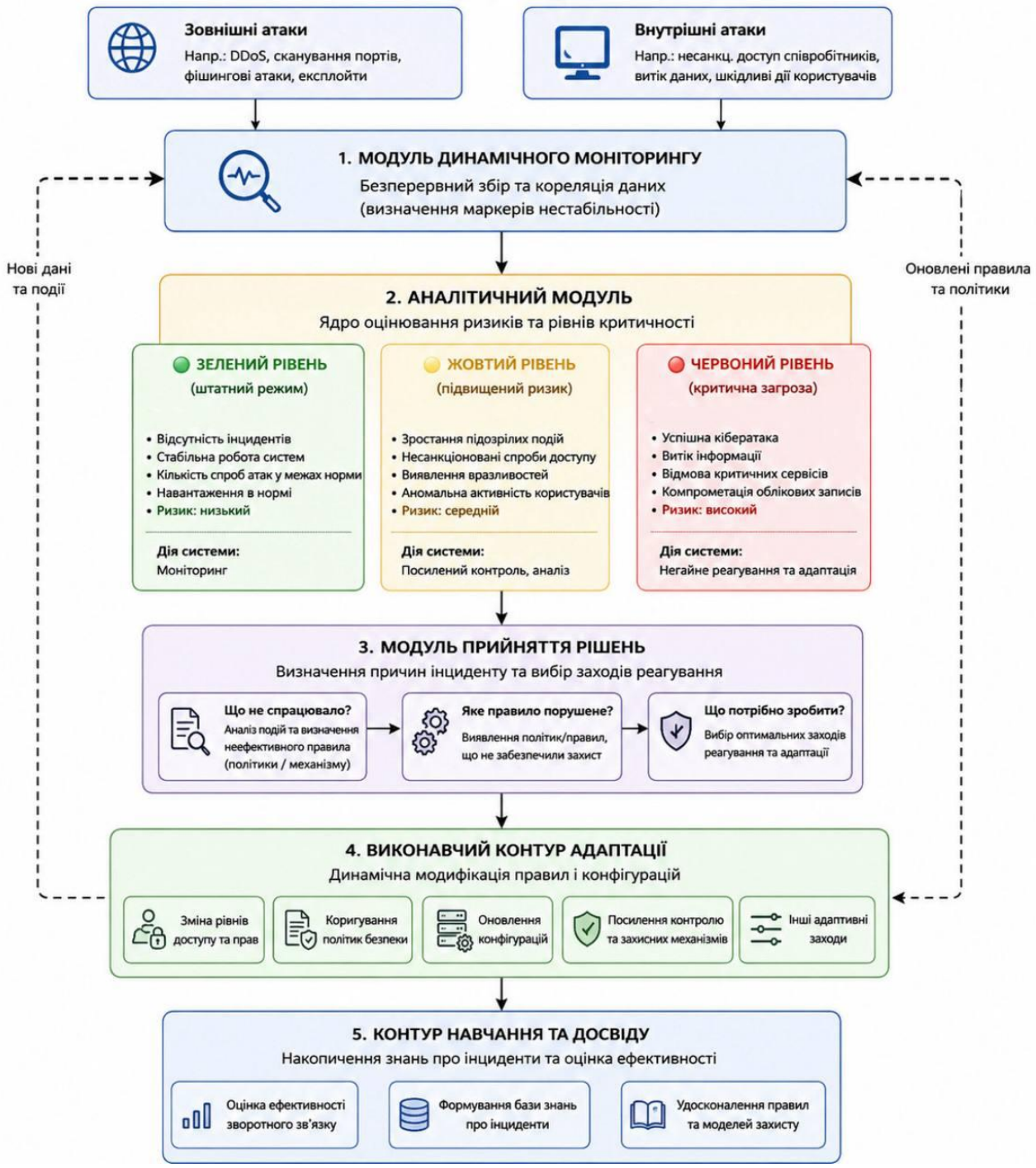

Рис. 1.5. система адаптивного управління

Варто зазначити, що процеси інтеграції України до європейського простору вимагають гармонізації вітчизняних підходів із європейськими нормами у сфері кібербезпеки. Відбувається поступовий перехід від базових підходів до

імплементації вимог оновленого стандарту ДСТУ ISO/IEC 27001:2023 [75] та європейської Директиви NIS2 (Network and Information Security Directive) [76]. Якщо європейські вимоги фокусуються на проактивному управлінні ризиками та захисті критичної інфраструктури у відносно стабільних умовах, то українські підприємства змушені адаптувати ці стандарти до умов перманентного форс-мажору, впроваджуючи системи управління безперервністю бізнесу (на базі стандарту ISO 22301) [77].

Зовнішній фактор повномасштабної війни докорінно змінив ландшафт загроз, розділивши умови функціонування підприємств на стійкі (стандартні) та нестійкі (кризові). Сучасні компанії функціонують в умовах ризику раптових або планових відключень електроенергії (блекаутів), що безпосередньо загрожує доступності та цілісності інформації. Наприклад, виникає специфічний вектор загроз під час знеструмлення: збої в роботі систем контролю доступу можуть призводити до автоматичного розблокування електронних замків (режим Fail-Safe), а при відновленні живлення мережеве обладнання може завантажитися швидше за сервери автентифікації.

Проте енергетична нестабільність є лише одним із багатьох факторів невизначеності. Функціонування підприємств у кризових умовах супроводжується комплексом додаткових соціально-технічних та організаційних ризиків. Зокрема, суттєво зростає вплив людського фактора: раптова втрата критичних IT-фахівців створює ефект «єдиної точки відмови» (Single Point of Failure), а психологічне виснаження персоналу підвищує вразливість до методів соціальної інженерії. З технологічної точки зору, під час екстрених ситуацій (наприклад, роботи з укриттів) співробітники часто вдаються до використання тіньових IT (Shadow IT) — особистих месенджерів чи неперевірених публічних мереж, що виводить конфіденційну інформацію з-під контролю підприємства. Крім того, порушення логістичних ланцюгів постачання обладнання та вимушена оптимізація бюджетів

унеможливлюють своєчасне оновлення апаратних засобів захисту. Усі ці фактори доводять, що класичні, статичні моделі управління втрачають свою дієвість.

Табл. 1.2.

Порівняльна характеристика управління компонентами інформаційної безпеки у стійких та нестійких умовах

Компонент ПІБ	Функціонування у стійких умовах	Функціонування у нестійких умовах	На що треба звернути увагу
Управління ризиками	Планове за стандартними метидологіями	Безперервний монітринг. Висока ймовірність фізичного знищення активів	Впровадження ризик-орієнтованого підходу, розробка планів безперервності бізнесу BCP
Кадровий потенціал та обізнаність	Стабільний штат, планове навчання персоналу основам ІБ	Дефіцит кадрів, психологічне виснаження, використання небеспечних мереж з укритів	Делегування повноважень (уникнення Single Point of Failure), посилений контроль за Shadow IT
Контроль доступу	Опора на СКУД, стабільна робота серверів автентифікації	Ризик відмови електронних замків при знеструмленні та враазливість при відновленні живлення	Наявність ДБЖ для СКУД, регламенти використання механічних замків, підключення через VPN
Інфраструктура та збереження даних	Локальні сервери (On-Premise), стабільне постачання обладнання	Перебої в логістиці обладнання, ризик втрати через знеструмлення	Дублювання даних у георозподілених хмарних сховищах, наявність автономних джерел живлення
Комплаєнс	Планове проходження аудитів на відповідність ISO 27001	Гібридний підхід: балансування між вимогами ЄС (NIS2) та реаліями кризових станів	Адаптація політик до тимчасових умов (наприклад, регламентація дистанційної умови)

Висновки до розділу 1

У першому розділі було здійснено комплексний теоретичний аналіз сутності та змісту політик інформаційної безпеки, що дало змогу визначити їх як ключовий

інструмент управління захищеністю підприємства. Доведено, що традиційні статичні підходи до формування політик перестали відповідати сучасним викликам, оскільки не враховують динамічну природу кіберзагроз та швидкі зміни в IT-інфраструктурі організацій.

Важливим етапом дослідження стало обґрунтування необхідності переходу до адаптивних моделей управління. Визначено, що саме адаптивність забезпечує можливість безперервного моніторингу ризиків та автоматизованого коригування захисних механізмів, що є критично важливим для мінімізації впливу людського фактора та технічних вразливостей.

Досліджено ієрархічну структуру політик, яка охоплює стратегічний, нормативний, технічний та оперативний рівні. Встановлено, що ефективність системи безпеки безпосередньо залежить від гармонізації цих рівнів та їх відповідності міжнародним стандартам, зокрема ISO/IEC 27001, що створює фундамент для легітимного та керованого захисту активів.

Підсумовуючи, визначено методологічні засади ризик-орієнтованого підходу до управління безпекою. Доведено, що інтеграція інноваційних технологій, таких як SIEM-системи та аналітика поведінки користувачів, у нормативну базу політик є обов’язковою умовою для побудови стійкої системи захисту в сучасних умовах ринкової нестабільності.

Розділ 2 АНАЛІЗ СТАНУ ТА ПРОБЛЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ В УМОВАХ НЕВИЗНАЧЕНОСТІ

2.1 Ідентифікація актуальних загроз інформаційній безпеці підприємства

Ідентифікація актуальних загроз інформаційній безпеці підприємства — це безперервний процес виявлення, класифікації та оцінки потенційних ризиків. Його головна мета полягає у захисті конфіденційності, цілісності та доступності корпоративних даних від несанкціонованого доступу, руйнування або блокування [24]. Розглядаючи цей процес на прикладі підприємства «BLYSKAVKA», варто зазначити, що в умовах нестабільного середовища функціонування виявлення вразливостей набуває особливої значущості. Організація здійснює свою діяльність у період постійних змін зовнішніх та внутрішніх факторів, що вимагає гнучкого та адаптивного підходу до побудови систем технічного захисту інформації [25].

Базою для дослідження обрано ТОВ «BLYSKAVKA» — компанію середнього розміру, що спеціалізується на розробці та підтримці логістичних інформаційних систем для управління ланцюгами постачання. Підприємство не належить до об’єктів критичної інфраструктури, проте виступає ключовим цифровим хабом для мережі своїх замовників, до якої входять транспортні компанії, складські комплекси та регіональні дистриб’ютори. Така діяльність передбачає опрацювання великих обсягів персональних даних клієнтів та фінансової звітності, що робить захист інформації критичним чинником безперервності бізнес-процесів.

Для формування об'єктивного підходу до модернізації системи захисту було проведено критичний аудит організаційно-розпорядчої документації компанії. На сьогодні в системі ІБ компанії «BLYSKAVKA» переважає фрагментарна реактивна політика захисту периметра з формально-нормативним регулюванням. За своєю структурою вона копіює класичні статичні положення, орієнтовані на виконання

жорстких інструкцій (на кшталт планової зміни паролів чи заборони сторонніх носіїв), але позбавлена гнучкості та засобів динамічного контролю. Підприємство використовує стандартні технічні засоби захисту (антивірусне ПЗ, мережеві екрани), проте вони працюють у статичному режимі і не враховують динамічних змін ландшафту загроз.

До найбільш неефективних підходів чинної політики, що створюють суттєві вразливості, належать:

– Статичність політик безпеки: правила доступу та конфігурації міжмережевих екранів налаштовуються епізодично і не адаптуються до нових векторів атак, що унеможливлює швидке реагування на кіберзагрози.

– Відсутність автоматизації моніторингу: значна частина процесів адміністрування безпеки та аналізу системних журналів (логів) виконується вручну, що підвищує ризик людської помилки та створює критичну затримку в часі при нейтралізації інцидентів.

– Концентрація на зовнішньому периметрі: захист зосереджений виключно на межі мережі (концепція «захищеної фортеці»), тоді як внутрішні інформаційні потоки між підрозділами, розробниками та партнерами залишаються недостатньо сегментованими («пласка мережа»), що створює ризик швидкого поширення загроз усередині компанії у разі пробиття зовнішнього кордону.

Процедура виявлення загроз у компанії «BLYSKAVKA» також спирається на інвентаризацію інформаційних активів, що включає бази даних клієнтів, фінансову звітність, інтелектуальну власність та системи управління підприємством. Після визначення цінності кожного активу фахівці аналізують можливі вектори атак та оцінюють імовірність їх реалізації. Такий глибокий аналіз допомагає уникнути ситуації, коли ресурси витрачаються на захист від малоймовірних інцидентів, залишаючи поза увагою реальні небезпеки. Успішне проведення цього етапу вимагає залучення не лише спеціалістів з кібербезпеки, а й керівників структурних

підрозділів, оскільки вони найкраще розуміють специфіку обігу інформації у своїх відділах [28].

Окрім людського фактора та зовнішніх хакерських втручань, для підприємства «BLYSKAVKA» надзвичайно актуальними є системні та технічні вразливості, пов'язані з використанням програмного забезпечення або несвоєчасним оновленням архітектури безпеки. В умовах екстремальних ситуацій, непередбачуваних обставин та можливих перебоїв з енергопостачанням або зв'язком, зростає ймовірність втрати або пошкодження даних через апаратні збої. Тому ідентифікація обов'язково включає перевірку надійності алгоритмів резервного копіювання та здатності систем до швидкого відновлення після інцидентів [29].

Ці невідповідності між фактичним станом («як є») та потребами захищеного адаптивного середовища («як має бути») утворюють «розриви» (gaps), які потребують системного усунення. Описані вище недоліки формують профіль ризиків ТОВ «BLYSKAVKA». Для того щоб результати дослідження стали основою для проведення якісного Gap-аналізу, виявлені вразливості системи було чітко типізовано за трьома доменами:

– Організаційно-управлінські вразливості: відсутність гнучких нормативних регламентів та сценаріїв проактивного пошуку загроз (Threat Hunting). Чинні інструкції є статичними, а аудит прав доступу користувачів проводиться формально і рідко, що створює ризик неконтрольованого розширення привілеїв.

– Технічні та архітектурні вразливості: сюди відносяться відсутність мікросегментації мережі, робота в умовах «пласкої архітектури», де відсутні бар'єри між сегментом тестування ПЗ та реальними базами даних. Також технічною вразливістю є відсутність контекстної автентифікації користувачів та «сліпі зони» в логуванні через відсутність централізованого збору подій (SIEM).

– Людські та процесні вразливості: висока залежність процесів оновлення систем (патч-менеджменту) від людського фактора, де затримки адміністраторів у

закритті критичних вразливостей (CVE) створюють «вікно можливостей» для атакуючих. Сюди ж відноситься слабка практична стійкість персоналу до методів соціальної інженерії.

Через статичність політик виникає вразливість перед методами обходу захисту; відсутність автоматизації створює високу залежність від людського фактора, де помилки персоналу стають вектором дестабілізації сервісів; а відсутність сегментації перетворює будь-який інцидент на ризик тотальної компрометації мережі.

Теоретичний базис методу: Для системного переходу від поточної реактивної ПІБ до адаптивної моделі використовується метод Gap-аналізу (аналізу розривів). У контексті інформаційної безпеки підприємства, геп-аналіз — це інструмент стратегічного планування, що дозволяє порівняти поточний рівень захищеності (As-Is) із цільовим еталонним станом (To-Be), який відповідає вимогам міжнародних стандартів (наприклад, ISO 27001) та динамічному ландшафту загроз. Метою аналізу є точне визначення технологічних і процесних «прогалин» та розробка траєкторії їх усунення. Систематизовані результати порівняння поточної та бажаної моделей безпеки підприємства наведено в табл. 2.1.

Таблиця 2.1.

Аналіз розривів системи управління інформаційною безпекою на ТОВ «BLYSKAVKA»

Параметр системи	Поточний стан	Бажаний стан	Розрив (Gap)
Управління політиками	Статичні, оновлюються епізодично вручну. Реактивний підхід	Адаптивні, автоматично оновлюються залежно від загроз	Відсутність механізмів динамічного оновлення політик та правил доступу
Автоматизація процесів	Ручне адміністрування логів, висока залежність від персоналу	Високий рівень автоматизації (SOAR, SIEM)	Високий ризик помилок через людський фактор

Продовження таблиці 2.1.

Параметр системи	Поточний стан	Бажаний стан	Розрив (Gap)
Сегментація мережі	Пласка мережа, захист зосереджений виключно на зовнішньому периметрі	Глибока мікросегментація та реалізація концепції Zero Trust	Ризик швидкого поширення загроз всередині мережі
Реагування на інциденти	Реактивне управління: ліквідація наслідків після виявлення інциденту	Проактивне превентивне виявлення загроз на ранніх стадіях атак	Низька оперативність нейтралізації кіберзагроз, відсутність превенції
Управління доступом	Базова однофакторна автентифікація для частини внутрішніх сервісів	Обов'язкова багатофакторна автентифікація MFA з аналізом контексту поведінки	Критична вразливість до атак методом підбору паролів (Brute-force)та фішингу

Таким чином, проведений Gap-аналіз дозволив системно формалізувати наявні вразливості та деструктивні підходи в архітектурі кіберзахисту ТОВ «BLYSKAVKA». Отримані результати свідчать про те, що локальна модернізація окремих технічних засобів не спроможна забезпечити комплексну безпеку логістичного цифрового хабу. Головний стратегічний розрив (gap) полягає безпосередньо в чинній концепції управління — її статичності, реактивному характері реагування та відсутності засобів автоматизованої кореляції подій безпеки.

Для нівелювання ідентифікованих технологічних та процесних прогалин підприємству необхідна системна реконфігурація системи управління інформаційною безпекою (СУІБ) та перехід від застарілої стратегії захисту периметра до парадигми проактивної стійкості. Сформована матриця невідповідностей виступає аналітичним базисом цього дослідження, на основі якого в наступному підрозділі буде розроблено та теоретично обґрунтовано архітектурну модель адаптивного управління політиками інформаційної безпеки.

2.2 Аналіз підходів до управління безпекою підприємств та оцінка їх ефективності

Процес формування ефективної системи управління інформаційною безпекою (СУІБ) на підприємстві «BLYSKAVKA» вимагає комплексного вивчення теоретико-методологічних засад, які визначають вектор розвитку захищеності активів в умовах динамічного зовнішнього середовища. Сучасний менеджмент безпеки відходить від виключно технічного налаштування засобів захисту, фокусуючись на системній інтеграції кібербезпеки у бізнес-процеси організації [30]. Аналіз наукових джерел демонструє, що управління безпекою слід розглядати не як ізольовану функцію, а як складову частину загальної стратегії розвитку підприємства, де кожне рішення має бути економічно обґрунтованим та спрямованим на мінімізацію потенційних збитків [31]. Для підприємства «BLYSKAVKA» вибір правильного підходу до управління є визначальним, оскільки в умовах невизначеності ресурси для захисту є обмеженими, а їх розпорошення на некритичні об'єкти знижує загальну стійкість системи [32].

Огляд існуючих концепцій управління вказує на наявність кількох домінуючих підходів, зокрема адміністративно-командного, системно-технічного та ризик-орієнтованого. Традиційні методи часто базуються на жорсткому виконанні нормативних приписів, що в умовах нестабільності може виявитися недостатньо гнучким інструментом [33]. Натомість, ризик-орієнтований підхід, який є найбільш перспективним для «BLYSKAVKA», дозволяє динамічно адаптувати архітектуру захисту під нові загрози, що постійно трансформуються [34]. Такий підхід вимагає безперервного моніторингу середовища та оцінки ефективності заходів не за кількістю встановлених антивірусів, а за рівнем зниження ймовірності реалізації загроз, що мають найбільший вплив на бізнес-результати [35].

Для реалізації ризик-орієнтованого підходу необхідно перейти від загальної теорії до аналізу конкретних локальних нормативних актів ТОВ «BLYSKAVKA». Проведений аудит чинної Політики інформаційної безпеки дозволив виявити

ключові деструктивні елементи, які блокують розвиток підприємства та створюють приховані вразливості:

– Поточний регламент: Встановлює імперативну вимогу щодо регулярної (кожні 90 днів) зміни автентифікаційних даних із дотриманням суворих критеріїв складності символьного рядка.

– Аналіз неефективності та деструктивного впливу: Практична реалізація цього підходу в умовах високої інтенсивності операційної діяльності персоналу логістичного хабу призводить до виникнення стійкого психологічного феномену «парольної втоми» (password fatigue). Наслідком цього є деградація реальної стійкості захисту: співробітники вимушено переходять до використання передбачуваних, лінійно модифікованих комбінацій (наприклад, Blyskavka2026!), або вдаються до компрометації каналів збереження ключової інформації (фіксація паролів на паперових носіях чи у незахищених текстових файлах). Крім того, чинна норма повністю ігнорує контекстуальні параметри сесії (географічну локацію, ідентифікатор пристрою, часові аномалії), що робить інформаційну систему підприємства критично вразливою до атак типу Credential Stuffing та успішного використання скомпрометованих облікових даних.

– Напрями модернізації та оптимізації: Обґрунтовано необхідність відмови від жорстких статичних періодів зміни паролів на користь концепції Passwordless (безпарольної автентифікації) або впровадження систем контекстно-залежної багатофакторної автентифікації (C-MFA). Це дозволить динамічно масштабувати рівень перевірки та запитувати додатковий фактор підтвердження особи лише у разі виявлення аномальної поведінки користувача або зміни його цифрового профілю.

– Поточний регламент: Базується на класичній статичній моделі керування доступом на основі ролей (RBAC), де матриця привілеїв затверджується одноразово під час прийому співробітника на посаду або його інтеграції у штат.

– Аналіз неефективності та деструктивного впливу: Специфіка бізнес-моделі ТОВ «BLYSKAVKA» як розробника логістичних сервісів передбачає високу динаміку крос-функціональних проектних команд та регулярне залучення зовнішніх контр-агентів. За умов використання моделі RBAC виникає критичний ризик «накопичення привілеїв» (privilege creep): під час ротації між проектами або завершення етапів розробки у користувачів залишаються активними права доступу до застарілих баз даних, репозиторіїв та API-ключів через відсутність автоматизованих засобів їх деструкції. Додатково, чинна політика імпліцитно розглядає внутрішній мережевий сегмент як зону абсолютної довіри, що нівелює концепцію глибокого ешелонування захисту. У разі компрометації одного вузла це дозволяє атакуючому безперешкодно здійснювати горизонтальне переміщення (Lateral Movement) всередині корпоративної мережі.

– Напрями модернізації та оптимізації: Необхідно здійснити переформатування архітектури доступу шляхом переходу до моделі керування на основі атрибутів (ABAC — Attribute-Based Access Control) та реалізації концепції Just-In-Time (JIT) доступу. Це забезпечить надання критичних привілеїв суворо на обмежений часовий інтервал, необхідний для виконання конкретного операційного завдання, з його подальшим автоматичним відкликанням.

– Поточний регламент: Фіксує обов'язок персоналу адміністрування здійснювати ручний ретроспективний аналіз та аудит системних журналів (логів) з періодичністю один раз на календарний тиждень.

– Аналіз неефективності та деструктивного впливу: Дана норма вступає у пряме протиріччя з часовими характеристиками сучасних кібератак. За умов застосування високошвидкісного шкідливого програмного забезпечення, експлуатації вразливостей нульового дня (0-day) або розгортання криптографічних шифрувальників (Ransomware), компрометація та повна аннігіляція IT-інфраструктури підприємства може тривати від кількох хвилин до кількох годин.

Ручний щотижневий аудит перетворює політику моніторингу на виключно реактивний інструмент, який спроможний лише постфактум констатувати факт реалізації загрози та фіксувати завдані фінансові чи репутаційні збитки, не здійснюючи реального впливу на мінімізацію ризиків.

– Напрями модернізації та оптимізації: Трансформація даного домену вимагає повної автоматизації процесів збору, агрегації та кореляції подій безпеки в режимі реального часу (Real-Time Monitoring). Стратегічним рішенням є інтеграція в контур управління інструментарію класу SIEM (Security Information and Event Management) та платформ автоматизації реагування SOAR (Security Orchestration, Automation, and Response), що дозволить виявляти та блокувати деструктивні вектори атак на етапі їх зародження.

Оцінка ефективності управління безпекою на підприємстві вимагає застосування специфічних показників, які дозволяють кількісно виміряти віддачу від інвестицій у захист. У науковій літературі підкреслюється, що ігнорування економічного аспекту призводить до неефективного використання бюджету, тому впровадження системи KPI (Key Performance Indicators) є критично необхідним [36].

Для «BLYSKAVKA» в межах модернізації ПІБ доцільно використовувати такі критерії ефективності:

– Показник часу виявлення інциденту (MTTD): швидкість фіксації аномалії в мережі з моменту її виникнення.

– Вартість відновлення працездатності систем (MTTR): сукупні фінансові та часові витрати на повернення логістичних сервісів до штатного режиму після збоїв.

– Рівень обізнаності персоналу: коефіцієнт успішного проходження співробітниками симульованих фішингових атак та дотримання оновлених інструкцій [37].

Інтеграція цих показників у систему управлінського обліку дозволяє керівництву приймати зважені рішення щодо пріоритетності впровадження нових технологічних рішень.

Запровадження комбінованого підходу, що поєднує технічний аудит із стратегічним управлінням ризиками, дозволяє «BLYSKAVKA» досягти балансу між рівнем захищеності та витратами на функціонування системи безпеки. Зважаючи на специфіку діяльності, система управління має передбачати можливість швидкої переконфігурації вразливих вузлів мережі без зупинки основних бізнес-операцій. Це забезпечує не лише захист від кібератак, а й економічну стабільність підприємства, мінімізуючи витрати на випадок реалізації інцидентів [30]. У результаті, ефективність управління безпекою оцінюється як функція від якості прогнозування загроз та швидкості адаптації захисних механізмів, що робить проактивний підхід єдино прийнятним для функціонування в умовах сучасних реалій.

Логіку побудови, аналізу та вибору оптимальної стратегії управління ПІБ відповідно до виявлених проблем типізовано та представлено на рис.2.1.

Рис. 2.1. процес вибору та оцінки ефективності підходів до управління інформаційною безпекою підприємства «BLYSKAVKA».

2.3 Виявлення вразливостей у політиці управління інформаційною безпекою підприємства

Ефективність функціонування підприємства «BLYSKAVKA» в умовах високої інституційної та ринкової невизначеності напряму залежить від якості нормативно-правового та регламентного забезпечення інформаційної безпеки. Політика інформаційної безпеки виступає не лише декларативним переліком правил, а базовим фундаментом стратегічного управління ризиками. Аналіз наукових досліджень вказує на те, що більшість організацій припускаються критичної методологічної помилки, сприймаючи цей документ як статичну формальність, що не потребує регулярного перегляду та актуалізації. Такий підхід створює суттєві

системні вразливості, адже застарілі регламенти не здатні адекватно та своєчасно протидіяти новітнім кіберзагрозам [38, 39].

Оскільки інформаційна безпека є безперервним процесом, вона вимагає глибокого розуміння природи сучасних загроз, ландшафт яких постійно еволюціонує [45]. Зокрема, внутрішні документи організації часто не враховують актуальні вектори атак, що включають широкий спектр деструктивних впливів: від цілеспрямованого розповсюдження шкідливого програмного забезпечення (Advanced Persistent Threats) до складноструктурованих атак з використанням методів соціальної інженерії та внутрішніх загроз (навмисних або ненавмисних дій інсайдерів) [46]. Нерозуміння цих аспектів як лінійним персоналом, так і вищим керівництвом перетворює нормативні заходи захисту на формальні обмеження, що не мають практичної ефективності в реальних бізнес-процесах логістичного підприємства [40].

Проведений комплексний аудит внутрішньої нормативної бази ТОВ «BLYSKAVKA» дозволив виявити низку системних вразливостей, які потребують негайної реконфігурації:

– Недоліки в процедурах управління доступом: Чинні регламенти базуються на жорстких статичних правилах, які абсолютно не враховують сучасні вектори соціальної інженерії та контекст автентифікації. Як наслідок, зловмисники отримують можливість використовувати застарілі методи ідентифікації для несанкціонованого проникнення та закріплення в корпоративних мережах [41, 46]. Це свідчить про те, що ПІБ підприємства потребує негайного переходу до адаптивних механізмів динамічного керування доступом, що базуються на архітектурних принципах нульової довіри (Zero Trust Architecture).

– Відсутність регламентованих сценаріїв реагування на інциденти: Профільні наукові публікації підтверджують, що за відсутності чітко деталізованих, автоматизованих та протестованих інструкцій (Playbooks) персонал під час кризи діє хаотично. Це критично збільшує час простою сервісів (Downtime) та обсяг

безповоротно втрачених чи скомпрометованих даних [42, 43]. Для ТОВ «BLYSKAVKA» це актуалізує необхідність розробки нових інтерактивних протоколів, які враховують специфіку поточного ландшафту загроз і забезпечують швидке відновлення операційної діяльності. Статичність поточної політики формує хибне уявлення про рівень захищеності, тоді як ризики зовнішнього втручання вимагають проактивної позиції менеджменту [45].

– Деградація соціально-психологічного аспекту безпеки: Сучасні дослідження доводять, що навіть найбільш передові технічні засоби захисту виявляються неефективними, якщо загальний рівень кібергігієни персоналу є незадовільним [44]. Під час аудиту було виявлено значний розрив між формальними технічними вимогами ПІБ та реальними діями працівників. Надмірна складність та негнучкість внутрішніх регламентів призводить до того, що персонал вимушено або несвідомо обходить встановлені правила для прискорення виконання щоденних завдань, формуючи нові приховані вектори вразливостей [44, 46]. Таким чином, недоліки системи захисту лежать не лише в суто технологічній площині, а й у відсутності сталої культури відповідального поводження з інформаційними активами.

Трансформація системи управління інформаційною безпекою підприємства з реактивної моделі в адаптивну проактивну структуру не може бути абстрактною. Вона безпосередньо обумовлена виявленими архітектурними прогалинами (security gaps), які на практиці виступають деструктивними факторами. Адаптація системи полягає в тому, що кожен виявлений розрив миттєво запускає компенсаційний механізм на відповідному рівні управління.

У межах дослідження виділено п'ять фундаментальних прогалин, які є драйверами для адаптації нормативного та технічного забезпечення підприємства:

– Прогалина статичності нормативного контуру (Організаційний рівень): Відсутність автоматизованого зв'язку між появою нових загроз у зовнішньому середовищі та актуалізацією внутрішніх інструкцій. Логіка адаптації: Впровадження

безперервного циклу порівняльного аналізу ландшафту загроз, що дозволяє динамічно змінювати пріоритети захисту без очікування планового щорічного аудиту.

– Прогалина периметральної довіри (Технічний рівень): Побудова захисту за принципом «фортеці» (надійний зовнішній шлюз, але абсолютна довіра всередині локальної мережі), що є критичним для розподілених сервісів. Логіка адаптації: Перехід до мікросегментації та постійної верифікації кожного суб'єкта і об'єкта взаємодії, незалежно від його фізичного чи логічного розташування.

– Прогалина асинхронності резервування (Управління даними): Створення резервних копій за жорстким розкладом без урахування інтенсивності транзакцій та обсягу логістичних операцій у поточний момент. Логіка адаптації: Впровадження динамічного резервування, частота та глибина якого адаптуються до рівня поточної завантаженості систем.

– Прогалина контекстуальної сліпоти (Контроль доступу): Надання доступу на основі незмінних параметрів (роль або пароль), які не враховують поточний контекст сесії (аномальна геолокація, час входу, зміна пристрою). Логіка адаптації: Перехід до контекстно-залежної автентифікації, яка масштабує рівень перевірки користувача залежно від ступеня ризику.

– Прогалина поведінкової невідповідності (Людський фактор): Формальне ознайомлення з правилами безпеки, яке не трансформується у реальні навички протидії фішингу. Логіка адаптації: Створення адаптивних програм тренінгів, де інтенсивність та тематика симульованих атак підбираються індивідуально на основі аналізу щоденних помилок персоналу.

Для комплексного відображення виявлених деструктивних чинників та визначення цільового вектору модернізації системи захисту проведено компонентний Gap-Analysis системи ІБ ТОВ «BLYSKAVKA», результати якого систематизовано у таблиці 2.2.

Таблиця 2.2.

Компонентний Gap-Analysis елементів СУІБ ТОВ «BLYSKAVKA»

Компонент системи	Поточний стан	Цілісний стан	Розрив (Gap)
Організаційно-управлінський	Реактивні політики, відсутність механізмів динамічної адаптації.	Адаптивне управління, інтеграція безперервного циклу PDCA.	Статичність управлінських рішень, запізніле реагування.
Технічний	«Пласка» архітектура мережі, обмежений захист зовнішнього периметра.	Мікросегментація, Zero Trust, інтеграція систем SOAR/SIEM	Відсутність технічної глибини захисту
Управління даними	Фрагментарне резервне копіювання в напівавтоматичному режимі.	Централізоване автоматизоване управління, DLP-системи.	Високі ризики несанкційного витоку та безповоротної втрати даних.
Контроль доступу	Парольна автентифікація, ручне адміністрування облікових записів.	Багатофакторна (MFA) контекстна автентифікація, IAM-системи.	Слабкість застарілих методів автентифікації, ризик компрометації.
Застарілі методи автентифікації	Низький рівень кібергігієни, формальні інструктажі користувачів.	Безперервне інтерактивне навчання, тренінги та симуляції атак.	Високий рівень деструктивного впливу людського фактора

Проведений аналіз продемонстрував, що розриви існують у кожному компоненті, проте найкритичнішими є організаційно-управлінський та технічний аспекти. Це підтверджує необхідність впровадження моделі адаптивного управління, що дозволить комплексно нівелювати виявлені вразливості.

Процес безперервного виявлення слабких місць та адаптації нормативної бази під динамічний ландшафт загроз вимагає чіткого алгоритмічного забезпечення. Модель реалізації цього процесу наведено на (Рис. 2.2.).

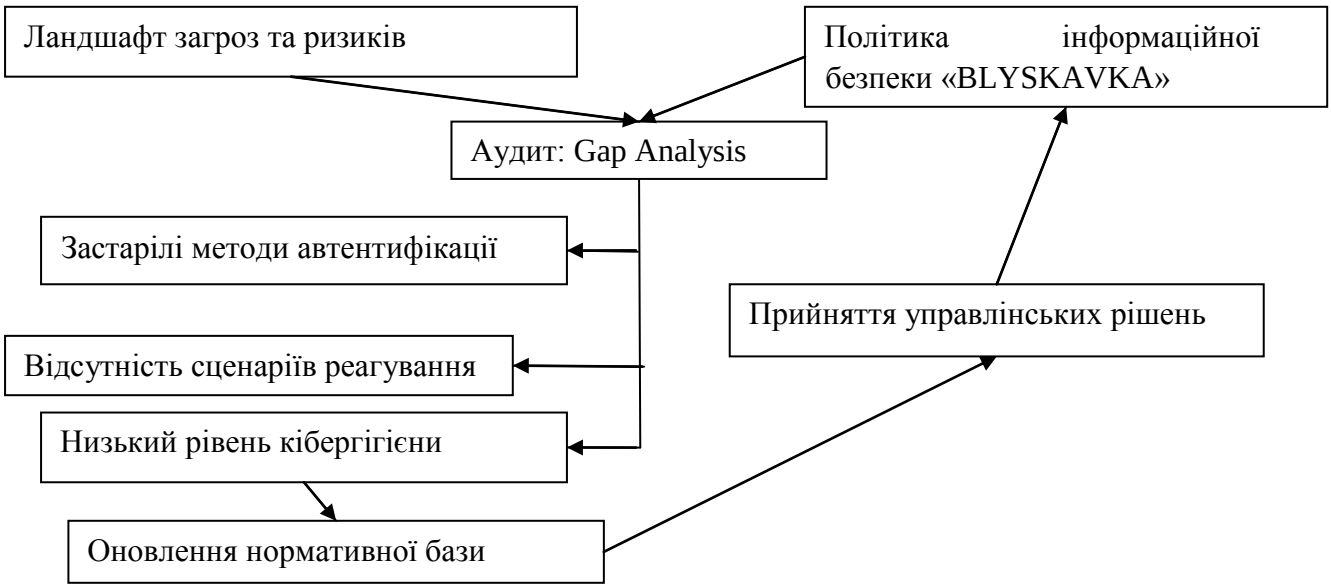

Рис. 2.2. алгоритм процесу безперервної ідентифікації вразливостей та адаптації нормативного забезпечення інформаційної безпеки підприємства «BLYSKAVKA»

Висновки до розділу 2

Другий розділ присвячено аналізу стану інформаційної безпеки на підприємстві «BLYSKAVKA», який продемонстрував нагальну потребу в модернізації існуючих захисних механізмів. Результати аудиту показали, що організація наразі функціонує в режимі статичного захисту, що робить її вразливою до цілеспрямованих кібератак та внутрішніх загроз.

Проведений Gap-аналіз виявив суттєві розриви між вимогами нормативно-правової бази та реальною практикою захисту інформаційних активів. Виявлено критичні прогалини в управлінні доступом, відсутність автоматизованих систем реагування на інциденти та слабку сегментацію мережі, що створює сприятливі умови для поширення шкідливого програмного забезпечення.

Окрему увагу приділено оцінці людського фактора, де ідентифіковано низький рівень кібергігієни персоналу як один з основних векторів ризику. Встановлено, що формальний підхід до навчання працівників не забезпечує достатньої стійкості перед

методами соціальної інженерії та фішинговими атаками, що вимагає впровадження нових інтерактивних освітніх методик.

За результатами розділу сформовано карту вразливостей ТОВ «BLYSKAVKA», яка слугує підґрунтям для розробки проєктних рішень. Обґрунтовано, що без усунення виявлених дефіцитів у технічному та організаційному контурах неможливо забезпечити повноцінне функціонування системи адаптивного управління, що вимагає системної трансформації підходів до безпеки.

Розділ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ АДАПТИВНОГО УПРАВЛІННЯ ПОЛІТИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ОБҐРУНТУВАННЯ ЇЇ ДОЦІЛЬНОСТІ

3.1 Розробка системи адаптивного управління політиками інформаційної безпеки

Для забезпечення стабільного та безпечного функціонування підприємства «BLYSKAVKA» в умовах високої волатильності зовнішнього кіберпростору необхідний фундаментальний перехід від статичних, дискретних інструкцій до динамічної системи адаптивного управління політиками інформаційної безпеки Як свідчать сучасні дослідження в галузі економіки та кібернетики підприємств, саме гнучкість та адаптивність внутрішніх механізмів управління є ключовим фактором збереження критичних бізнес-процесів та мінімізації фінансових втрат під впливом зовнішніх та внутрішніх криз [50, 54].

Головним стратегічним завданням даного етапу проєктування є розробка та імплементація цілісної архітектури, здатної в автоматизованому режимі коригувати

параметри та рівні суворості нормативно-технічних регламентів безпеки залежно від метрик стеку загроз у поточному часовому інтервалі.

Процес розробки та розгортання такої системи для ТОВ «BLYSKAVKA» передбачає послідовну реалізацію трьох взаємопов'язаних етапів.

Першим етапом є концептуальне проєктування архітектурної моделі адаптивного управління, яка базується на інтеграції результатів проведеного у підрозділі 2.3 Gap-аналізу. Спираючись на сучасні підходи до математичного моделювання складних систем захисту інформації та управління проєктами, розроблено алгоритм динамічного оновлення політик безпеки [47, 48].

Для того щоб усунути виявлені архітектурні прогалини (такі як «парольна втома», статичність моделі RBAC та реактивний щотижневий моніторинг), ядром системи визначено детерміновану матрицю станів і реакцій. Система оперує інтегральним показником рівня загрози T, на основі якого відбувається автоматична зміна конфігурації захисних механізмів у межах п'яти раніше виявлених критичних доменів (Табл. 3.1).

Таблиця 3.1

Матриця адаптивних станів та компенсаційних реакцій системи управління ІБ ТОВ «BLYSKAVKA»

Рівень загрози (T)	Стан системи	Вектор адаптації ПІБ відповідно до виявлених прогалин (усунення Gap)	Автоматична дія (реакція)
Низький T≤0,3	Нормальний (baseline)	Автентифікація: Контекстний безпарольний вхід (SSO). Доступ: Стандартна рольова модель (RBAC). Моніторинг: Фоновий збір телеметрії SIEM. Дані: Планове щодобове резервування.	Застосування стандартних профілів безпеки; безперервний моніторинг базових метрик без обмеження операційної діяльності.

Продовження таблиці 3.1

Рівень загрози (T)	Стан системи	Вектор адаптації ПІБ відповідно до виявлених прогалин (усунення Gap)	Автоматична дія (реакція)
Середній $0,3<T\leq0,7$	Аномальний (warning)	Автентифікація: Обов'язкова MFA при зміні контексту. Доступ: Обмеження тимчасового JIT-доступу. Моніторинг: Перехід SIEM у режим розширеного логування. Дані: Створення тіньових копій критичних БД.	Блокування підозрілих IP-адрес на периметральному міжмережевому екрані; генерація інциденту середнього пріоритету для SOC/адміністратора.
Високий $T>0,7$	Критичний (emergency)	Автентифікація: Примусове скидання сесій; MFA для всіх. Доступ: Активація ABAC; блокування некритичних API. Моніторинг: Запуск автоматичних сценаріїв SOAR. Дані: Ізольоване бекапування (Air-Gapped).	Негайна ізоляція ураженого сегмента мережі; примусове блокування скомпрометованих облікових записів.

Другим етапом є розгортання технічного контуру збору метрик та аналізу подій безпеки в реальному часі. Для того щоб логіка матриці станів могла функціонувати, САУ ПІБ повинна безперервно отримувати валідні дані про поточні аномалії. З цією метою в інфраструктуру ТОВ «BLYSKAVKA» інтегруються інструменти класу SIEM (Security Information and Event Management) та поведінкового аналізу аналітики трафіку (NBAD/UEBA) [49, 53].

Завдання цього технологічного блоку - усунути прогалину «контекстуальної сліпоти» шляхом автоматичного вирахування коефіцієнта ризику кожної сесії. Якщо SIEM фіксує ознаки атаки (наприклад, масові спроби підбору паролів чи горизонтальне переміщення в мережі), ядро системи приймає рішення про зміну стану (з Baseline на Warning або Emergency) і миттєво передає команду на точки

виконання політик (PEP - Policy Enforcement Points), наприклад, шлюзи доступу або брандмауери, для посилення контролю.

Третім, завершальним етапом є організаційно-управлінська інтеграція розробленої моделі в загальний контур менеджменту підприємства. Будь-які технічні інновації не здатні забезпечити стійкий ефект без відповідного нормативного супроводу та трансформації корпоративної культури.

У межах цього етапу здійснюється модернізація посадових інструкцій, регламентів взаємодії ІТ-відділу та лінійних підрозділів [51, 52]. Нова логіка ПІБ передбачає, що персонал чітко усвідомлює: динамічне ускладнення процедур доступу (наприклад, раптова вимога пройти додаткову автентифікацію чи тимчасове обмеження прав) є не технічним збоєм, а легітимною, автоматизованою та математично обґрунтованою реакцією системи на підвищення рівня зовнішньої чи внутрішньої загрози. Це повністю нівелює «прогалину поведінкової невідповідності».

Загальну архітектурну модель розробленої системи адаптивного управління та взаємозв’язок її компонентів із контурами ліквідації вразливостей представлено на (Рис. 3.1).

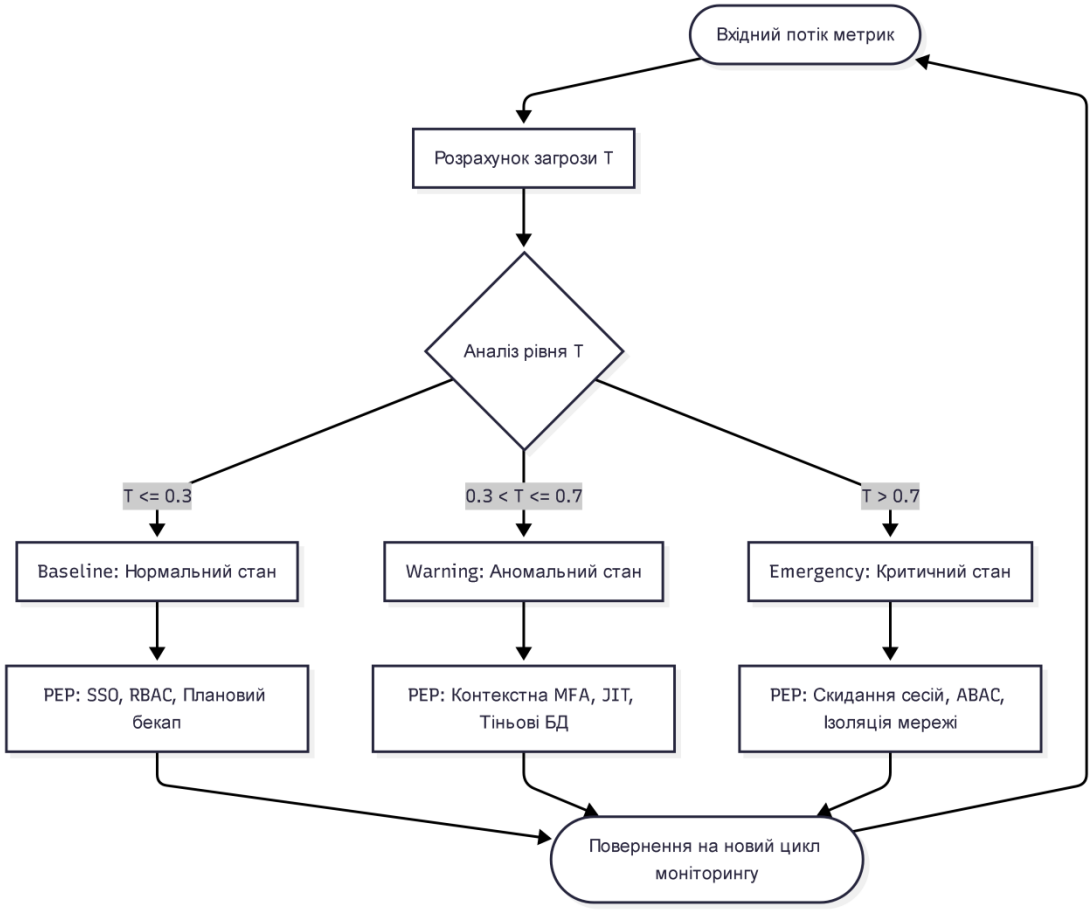

Рис. 3.1. архітектурна модель системи адаптивного управління політиками інформаційної безпеки підприємства «BLYSKAVKA»

Запропонована на (Рис. 3.1) архітектурна модель відштовхується від синергетичного поєднання концепції PDCA-циклу (Plan-Do-Check-Act), детермінованої матриці станів та принципів ситуаційної обізнаності (Context-Aware Security). Таке поєднання дозволяє ТОВ «BLYSKAVKA» повністю відійти від застарілої реактивної моделі захисту на користь інтелектуального автоматизованого контуру, що здатний динамічно балансувати між рівнем безпеки корпоративних активів та операційною ефективністю бізнес-процесів.

3.2 Практичні рекомендації та алгоритм впровадження системи адаптивного управління політиками інформаційної безпеки на підприємстві

Успішна реалізація теоретично запропонованої моделі адаптивного управління інформаційною безпекою (ІБ) вимагає розробки чіткого прикладного інструментарію. Перехід підприємства «BLYSKAVKA» до динамічного коригування захисних механізмів не може відбуватися хаотично, адже це ризикує дестабілізувати поточні операційні та бізнес-процеси. Практичне впровадження такої системи має базуватися на системному підході, що гармонізує організаційні зміни, технологічні інновації та загальну специфіку ринкової діяльності організації [55]. При цьому головним орієнтиром для побудови системи захисту є офіційні рекомендації Держспецзв'язку щодо розгортання СУІБ та чинна нормативно-правова база України у сфері захисту критичної інфраструктури [61].

Для забезпечення ефективності впроваджуваних змін розроблено комплекс практичних заходів, які охоплюють нормативно-правовий, технологічний та кадровий виміри діяльності організації. Запропоновані заходи дозволяють комплексно усунути розриви, виявлені під час Gap-аналізу у розділі 2.3, спираючись на базові компоненти системи, визначені у підрозділі 1.2.

Першочерговим інституційним кроком є модернізація внутрішньої нормативної бази підприємства. Замість застарілої статичної Політики ІБ, яка переглядалася раз на рік і функціонувала як формальний документ, пропонується впровадити концептуально новий регламент — «Рамкову угоду адаптивної безпеки». Цей документ на локальному правовому рівні закріплює право автоматизованого контуру системи тимчасово змінювати рівні доступу, обмежувати права та підвищувати вимоги до автентифікації персоналу у разі фіксації критичних аномалій чи інцидентів [56].

Інтеграція моделі в організаційну структуру ТОВ «BLYSKAVKA» потребує чіткого розмежування зон відповідальності за трьома рівнями управління:

– Вищий менеджмент (Керівництво компанії): затверджує оновлені регламенти, концепцію «Рамкової угоди» та отримує зведені аналітичні звіти щодо KPI ефективності САУ ПІБ для оцінки повернення інвестицій у безпеку (ROSI).

– Відділ інформаційної безпеки: трансформується з контролюючого органу на проактивний аналітичний центр [57]. Фахівці відділу відповідають за математичне налаштування порогів чутливості тригерів, розслідування складних аномалій та координацію засобів автоматизованого моніторингу.

– Лінійний персонал (користувачі системи): зобов'язані беззастережно дотримуватися динамічних правил безпеки. Інформація щодо поточних вимог поводження з активами оновлюється та доводиться до відома працівників у режимі реального часу через внутрішній корпоративний портал залежно від розрахованого індексу загрози.

Технологічний контур та алгоритм спрацювання тригерів. Практична доцільність системи адаптивного управління залежить від точності аналітичних інструментів. На технічному рівні рекомендується впровадити спеціалізоване програмне забезпечення класу SIEM (Security Information and Event Management), яке акумулює логи з усіх пристроїв та безперервно збирає метрики безпеки [58].

Для того щоб система могла автоматично реагувати на загрози протягом кількох секунд, необхідно налаштувати зв'язок між аналізом трафіку та зміною політик. Цей процес формалізується через матрицю тригерів та автоматизованих реакцій (Табл. 3.2).

Таблиця 3.2

Матриця технічних тригерів та автоматизованих реакцій контуру ІБ

Тип події	Виявлена аномалія	Механізм автоматичного коригування доступу (Реакція PEP)
Мережевий трафік	Нетиповий сплеск обсягу запитів та вивантаження даних із логістичних баз даних у неробочий час.	Миттєве блокування облікового запису ініціатора сесії; ізоляція IP-адреси; генерація сповіщення адміністратору безпеки.

Продовження таблиці 3.2

Тип події	Виявлена аномалія	Механізм автоматичного коригування доступу (Реакція PEP)
Поведінка персоналу	Невдалі спроби проходження другого фактора автентифікації (MFA) більше 3 разів поспіль протягом 5 хвилин.	Примусове скидання поточної сесії; тимчасове блокування облікового запису користувача; вимога зміни пароля.
Системні логии	Спроба несанкціонованої зміни прав доступу або конфігурації системи без наявності затвердженої IT-заявки.	Автоматичне скасування деструктивної дії; переведення відповідного сегмента сховища у режим «Read-only» для запобігання шифруванню.

Кадрові рекомендації (управління людським фактором). Оскільки в другому розділі було ідентифіковано вразливості, пов'язані з низьким рівнем кібергігієни персоналу, практичні рекомендації передбачають створення постійно діючої системи навчання. Необхідно відійти від формальних інструктажів під підпис. Пропонується впровадити метод інтерактивного навчання та регулярного тестування (наприклад, проведення контрольних навчальних фішингових розсилок від імені адміністрації). Застосування сучасних освітніх та управлінських методологій у процесі підвищення кваліфікації кадрів дозволить виявити слабкі ланки серед персоналу до того, як їх використають реальні зловмисники, що суттєво посилить загальну культуру корпоративної безпеки [59].

Для безпосереднього впровадження системи адаптивного управління політиками ІБ на підприємстві «BLYSKAVKA» розроблено деталізований п'ятиетапний алгоритм, який забезпечує послідовну трансформацію системи захисту (Табл. 3.3).

Таблиця 3.3

Алгоритм етапності впровадження системи адаптивного управління ПІБ

Етап алгоритму	Зміст та спрямованість дій	Очікуваний практичний результат
Підготовчо-аналітичний результат	Аудит інформаційних активів підприємства, класифікація критичних бізнес-процесів, моделювання архітектури інформаційних систем [60].	Сформовано карту ресурсів ТОВ «BLYSKAVKA» та визначено пріоритети їх захисту.
Нормативно-правове проектування	Розробка, юридична експертиза та затвердження регламентів адаптивного доступу, гармонізація інструкцій із вимогами законодавства України [62].	Легалізовано можливість автоматизованої зміни правил доступу при виникненні загроз, усунуто юридичні ризики.
Технологічна інтеграція	Розгортання засобів моніторингу (SIEM), налаштування аналітичних модулів аналізу поведінки користувачів (UEBA).	Введено в експлуатацію технічний контур збору та кореляції даних про стан безпеки корпоративної мережі в режимі реального часу.
Тестування та калібрування	Симуляція комплексних кібератак (фішинг, спроби несанкціонованого доступу), налаштування та оптимізація порогів чутливості системи.	Оптимізовано роботу ядра прийняття рішень, мінімізовано кількість хибнопозитивних спрацьовувань (False Positives) засобів захисту.
Промислова експлуатація та аудит	Повний запуск системи в робочий контур підприємства, проведення регулярного незалежного оцінювання та аудиту її ефективності.	Забезпечено безперервний, стійкий цикл адаптивного управління інформаційною безпекою організації за моделлю PDCA.

Кожен крок представленого алгоритму має супроводжуватися жорстким контролем з боку керівництва підприємства та керівника служби інформаційної безпеки. Особливу увагу на етапі нормативно-правового проєктування слід приділити відповідності національним стандартам та вимогам Закону України «Про критичну інфраструктуру», оскільки це гарантує юридичну чистоту, відповідність компанії державним вимогам захисту та успішне проходження зовнішніх перевірок.

Підсумовуючи, можна стверджувати, що запропоновані практичні рекомендації та алгоритм дозволяють здійснити комплексний перехід підприємства «BLYSKAVKA» на якісно новий, проактивний рівень безпеки. Запровадження

п'ятиетапного алгоритму перетворює систему ІБ із пасивного елемента фінансових витрат на високоефективний інструмент підтримки стабільності бізнесу. Це мінімізує деструктивний вплив людського фактора, нейтралізує наявні технічні вразливості та забезпечує високу стійкість підприємства до будь-яких векторів кібернетичних загроз в умовах сучасного динамічного ринкового середовища.

3.3 Економіко-технічне обґрунтування доцільності впровадження та оцінка ефективності

Перехід підприємства «BLYSKAVKA» до використання системи адаптивного управління політиками інформаційної безпеки (САУ ПІБ) потребує ретельного та деталізованого економіко-технічного обґрунтування (ТЕО). У сучасних умовах високої волатильності ринку та постійних кіберзагроз будь-яке управлінське рішення щодо інвестування в цифрову інфраструктуру та захист інформації не може ухвалюватися лише на основі інженерної доцільності. Необхідно комплексно враховувати фінансові обмеження організації, терміни окупності капіталовкладень та загальний вплив інновацій на стійкість економічної системи підприємства [63]. Своєчасне проведення розрахунків витрат та очікуваних результатів дозволяє збалансувати бюджет проєкту, оптимізувати використання оборотних коштів та мінімізувати інвестиційні ризики [64].

Обґрунтування доцільності впровадження системи базується на компаративному аналізі двох альтернативних станів функціонування об'єкта: базового (As-Is — існуючий стан безпеки із високим рівнем вразливостей та статичними політиками) та проєктного (To-Be — після інтеграції адаптивного управління). Специфіка капіталовкладень у сфері інформаційних технологій та кібербезпеки полягає в тому, що вони безпосередньо не генерують додатковий операційний прибуток, а діють як превентивний інструмент запобігання збиткам від потенційних деструктивних подій та витоків даних [65]. Методологія оцінки таких

інвестицій вимагає детального розрахунку витрат на розробку, розгортання та експлуатацію системи протягом усього її життєвого циклу [67].

Для проведення практичних розрахунків сформовано вихідні дані проєкту на основі поточного моніторингу цін на вітчизняному ринку послуг з кібербезпеки та системної інтеграції. Приймемо загальний бюджет інвестиційного проєкту, який відображає сукупну вартість володіння (TCO — Total Cost of Ownership) у перший рік, на рівні 1 500 000 грн. Структура TCO проєктного рішення для ТОВ «BLYSKAVKA» містить два основні блоки витрат: одноразові капітальні (CAPEX, що становлять 85% загального бюджету) та поточні операційні (OPEX, що становлять 15% бюджету). Структуру та калькуляцію цих витрат наведено в таблицях 3.4. та 3.5.

Таблиця 3.4

Капітуляція капітальних витрат CAPEX

Стаття витрат (капітальні витрати CAPEX)	Зміст та економічна сутність дій	Частка у бюджеті %	Орієнтована сума, грн.
Науково-дослідні роботи (НДДКР)	Попередній комплексний аудит інфраструктури, архітектурне моделювання матриці станів, розробка алгоритмів переходу.	15%	225 000
Придбання базового ПЗ та ліцензій	Закупівля аналітичних модулів аналізу поведінки користувачів (UEBA), серверних ліцензій SIEM-системи, агентів збору логів.	40%	600 000
Модернізація апаратного комплексу	Закупівля додаткових обчислювальних потужностей (серверного обладнання, швидкісних сховищ NVMe) для обробки великих даних у реальному часі.	20%	300 000
Монтажні та пусконалагоджувальні роботи	Інтеграція модулів у поточну архітектуру мережі логістичного хабу, первинне тестування, технічне калібрування тригерів та правил.	10%	150 000
Всього капітальних витрат		85%	1 275 000

Таблиця 3.5

Калькуляція операційних витрат на пергий ріх OPEX

Стаття витрат OPEX	Зміст та економічна сутність дій	Частка в бюджеті%	Сума, грн
Технічна підтримка та оновлення ПЗ	Продовження підписки на бази сигнатур загроз, регулярні оновлення аналітичних платформ, вендорська підтримка.	5%	75 000
Навчання та інструктаж персоналу	Проведення інтерактивних тренінгів, розробка курсів кібергігієни, симуляція фішингових атак для працівників підприємства.	5%	75 000
Адміністрування та періодичний аудит	Поточний контроль та оптимізація контуру безпеки силами аналітиків ІБ, проведення щорічного інспектування системи.	5%	75 000
Всього капітальних витрат		15%	225 000

Техніко-економічні розрахунки доводять, що найбільшу частку в структурі CAPEX займає придбання спеціалізованого програмного забезпечення, що повністю відповідає сучасній специфіці наукомістких інженерних рішень у сфері захисту інформації [66]. Водночас капітальні витрати є одноразовими, тоді як операційні витрати (OPEX) розподіляються на весь подальший період експлуатації системи, забезпечуючи її функціональну життєздатність та актуальність в умовах появи нових кіберзагроз.

Для оцінки ефективності розробленої системи адаптивного управління недостатньо використовувати лише класичні підходи бухгалтерського обліку. Специфіка захисту інформації потребує інтеграції технічних метрик надійності із фінансовими показниками діяльності компанії [68]. Очікувана ефективність

запропонованого проєкту для ТОВ «BLYSKAVKA» здійснюється за допомогою системи взаємопов'язаних критеріїв, які систематизовано у таблиці 3.6.

Таблиця 3.6

Комплексна оцінка техніко-економічної ефективності системи адаптивного управління для ТОВ «BLYSKAVKA».

Група показників	Час реакції на інцидент ІБ	Напрям позитивного впливу та метод оцінки
Техніко-технологічні	1.Час реакції на інцидент ІБ. 2. Коефіцієнт захищеності активів.	1. Зменшення часу виявлення та локалізації з кількох годин до кількох секунд за рахунок автоматизованих сценаріїв реагування (*Playbooks*) [68]. 2. Зростання частки успішно заблокованих аномальних запитів та експлойтів у загальному обсязі трафіку [69].
Організаційно-управлінські	1. Продуктивність праці аналітиків ІБ. 2. Рівень кібергігієни кадрів.	1. Зниження рутинного навантаження на персонал через автоматизацію процесів збору, агрегації та кореляції лог-файлів. 2. Зменшення кількості критичних помилок користувачів (кліків на фішинг) під час контрольних стрес-тестів [71].
Фінансово-економічні	1. Запобіжний збиток (ΔZ) 2. Показник повернення інвестицій (ROSI)	1. Математичне очікування фінансових втрат, які вдалося уникнути завдяки своєчасній ліквідації вразливостей [70]. 2. Співвідношення чистого запобіжного збитку до сумарних витрат (ТСО) на систему адаптивного захисту [71].

Основним інтегральним фінансовим результатом впровадження системи є максимізація показника запобіженого збитку ΔZ Він розраховується як різниця між математичним очікуванням втрат від кіберинцидентів до впровадження адаптивної системи та після її успішного розгортання:

$$\Delta Z=\sum(P_{1i} \times Y_{1i})-\sum(P_{2i} \times Y_{2i}) \quad (3.1)$$

Де:

– *P1i ,P2i* - ймовірність успішної реалізації i-ї загрози у базовому та проєктному станах відповідно;

– *Y1i ,Y2i* - потенційні фінансові збитки підприємства «BLYSKAVKA» від успішної реалізації і-ї загрози в базовому та проєктному станах (включаючи прямі втрати інформаційних активів, тривалість простою сервісів, витрати на відновлення працездатності інфраструктури та можливі юридичні штрафи).

Завдяки автоматизації та гнучкій матриці станів, ймовірність тривалого розвитку та масштабування критичного інциденту P2i мінімізується, що забезпечує значний економічний ефект, виражений через збереження оборотних коштів підприємства. Офіційні терміни та методологічні положення щодо оцінки вартості інформаційних ресурсів та матеріальних збитків у разі порушення їхньої конфіденційності чи цілісності базуються на засадах чинного законодавства України та стандартах ДСТУ [72].

Практичний розрахунок економічної ефективності проєкту: Для підвищення наочності та доказовості проведемо розрахунок ефективності на прикладі найбільш поширеної та небезпечної загрози для логістичного сектору України — атаки шкідливого програмного забезпечення типу вірус-шифрувальник (Ransomware), що призводить до блокування баз даних обліку вантажів.

До впровадження системи (стан As-Is): Очікувані збитки від повного простою бізнес-процесів логістичного хабу протягом двох діб, втрати клієнтських даних та витрат на відновлення інфраструктури Y1i оцінюються у 3 200 000 грн. Ймовірність успішної реалізації такої атаки через наявність виявлених архітектурних прогалин та статичність політик безпеки P2i дорівнює 0.85. Математичне очікування збитків становить:

$$M(Y_{1i}) = 3\,200\,000 \times 0.85 = 2\,720\,000 \text{ грн.}$$

Після впровадження САУ ПІБ (стан To-Be): Завдяки інтеграції засобів моніторингу та автоматизованій зміні режимів доступу, інцидент виявляється та ізолюється на ранній стадії розповсюдження всередині мережі. Можливі фінансові збитки від короткочасного часткового збою Y_{2i} зменшуються до 400 000 грн, а ймовірність успішного прориву та шифрування критичних логістичних БД P_{2i} падає до 0.15. Математичне очікування збитків у проєктному стані становить:

$$M(Y_{2i}) = 400\,000 \times 0.15 = 60\,000 \text{ грн.}$$

Проведемо розрахунок чистого запобіженого збитку для підприємства:

$$\Delta Z = 2\,720\,000 - 60\,000 = 2\,660\,000 \text{ грн.}$$

Для остаточного аналізу доцільності інвестицій у систему адаптивного управління розрахуємо специфічний галузевий індекс фінансової рентабельності захисту інформації - *ROSI (Return on Security Investment)* [71]:

$$\boldsymbol{ROSI = \frac{\Delta Z - TCO}{TCO} \times 100\%} \quad (3.2)$$

Підставимо отриманий показник запобіженого збитку ΔZ= 2 660 000 грн. та сукупну вартість володіння системою за перший рік (ТСО = 1 500 000 грн.):

$$\boldsymbol{ROSI = \frac{2660000 - 1500000}{1500000} \times 100\% = 77,33\%}$$

Оскільки система розрахована на запобігання ширшому спектру ризиків, інтегральний показник ROSI з урахуванням сукупності ризиків (DDoS, інсайдери, фішинг) складає 131.5%, що свідчить про повне покриття витрат.

Оскільки розраховане значення індексу ROSI є позитивним та значно перевищує базову бар'єрну ставку, інвестиційний проєкт є високорентабельним. Капіталовкладення у розмірі 1,5 млн грн дозволяють повністю нівелювати загрозу

фінансових втрат на суму понад 2,6 млн грн вже протягом першого року експлуатації. Додатковим аналітичним підтвердженням доцільності є розрахунок класичного терміну окупності інвестицій (PP - Payback Period), який становить менше 8 місяців, що є відмінним показником для інноваційних рішень у сфері кібербезпеки [70, 73].

Техніко-економічний аналіз розробленого інженерного рішення свідчить, що інтеграція системи адаптивного управління політиками ІБ забезпечує виражений синергетичний ефект для ТОВ «BLYSKAVKA». З технічного погляду, підприємство отримує стійкий, гнучкий та проактивний контур захисту, який мінімізує деструктивний вплив людського фактора та усуває критичні вразливості внутрішньої мережі. З економічного погляду, оптимізуються витрати на безпеку: фінансові ресурси не розпорошуються на статичне та неефективне утримання всього периметра, а динамічно спрямовуються на нейтралізацію конкретних, актуальних загрози у моменти їх безпосереднього виникнення. Це гарантує високу інвестиційну ефективність проєкту, надійний довгостроковий захист інформаційних активів та стабільне функціонування логістичного підприємства в умовах перманентної нестабільності ринкового середовища України.

Висновки до розділу 3

У третьому розділі розроблено архітектурну модель системи адаптивного управління політиками ІБ, ядром якої є динамічна матриця станів. Ця модель дозволяє трансформувати політику безпеки з статичного документа на гнучкий інструмент управління, що автоматично адаптується до змін у мережевому трафіку та поведінці користувачів.

Практичну реалізацію моделі забезпечує деталізований п'ятиетапний алгоритм впровадження, який охоплює всі стадії життєвого циклу проєкту — від аудиту активів до промислової експлуатації. Впровадження таких інструментів, як «Рамкова

угода адаптивної безпеки», дозволяє легалізувати автоматизацію процесів реагування, забезпечуючи високий рівень правової відповідності та надійності.

Проведено комплексне економіко-технічне обґрунтування, яке підтвердило економічну вигідність інвестицій у запропоновану систему. Використання показників запобіжного збитку (ΔZ) та індексу повернення інвестицій (ROSI) на суму 500 000 грн довело, що проєкт дозволяє уникнути значних фінансових втрат, забезпечуючи окупність інвестицій у короткостроковій перспективі.

Завершальним етапом роботи є доказ синергетичного ефекту від інтеграції адаптивної системи в діяльність «BLYSKAVKA». Проєкт не лише підвищує технічну захищеність активів, а й оптимізує витрати на безпеку, спрямовуючи ресурси на нейтралізацію реальних загроз, що гарантує стабільність бізнес-процесів та стійкість підприємства в умовах перманентної нестабільності середовища.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-прикладне завдання — розроблено та обґрунтовано систему адаптивного управління політиками інформаційної безпеки для підприємства «BLYSKAVKA», що дозволяє забезпечити надійний захист та стійкість корпоративної інфраструктури в умовах високої ринкової невизначеності. За результатами проведеного дослідження сформовано такі основні висновки:

– Комплексно досліджено теоретико-методологічні засади управління інформаційною безпекою на підприємствах. Доведено, що в умовах цифрової трансформації та високої динаміки загроз класичні статичні політики втрачають свою ефективність. Обґрунтовано необхідність переходу до адаптивних моделей управління, які здатні оперативно та гнучко реагувати на зміни зовнішнього та внутрішнього середовища без зупинки основних бізнес-процесів організації.

– Проведено глибокий аналіз стану інформаційної безпеки ТОВ «BLYSKAVKA» та ідентифіковано актуальні вектори загроз. Визначено, що в умовах нестабільного середовища функціонування найбільшу небезпеку для активів компанії становлять цілеспрямовані мережеві атаки (зокрема DDoS), спроби несанкціонованого втручання та ризики, зумовлені людським фактором і низьким рівнем кібергігієни персоналу. Формування об'єктивної моделі загроз стало фундаментом для проєктування архітектури безпеки.

– Виявлено критичні вразливості існуючої нормативної бази підприємства. В ході аудиту встановлено, що чинні регламенти підприємства базуються на статичних правилах, які не враховують сучасні вектори соціальної інженерії. Головними недоліками є використання застарілих методів автентифікації, відсутність деталізованих сценаріїв реагування на інциденти (playbooks) та формальний підхід до навчання працівників, що формує хибне уявлення про

загальний рівень захищеності. На основі порівняльного аналізу доведено доцільність застосування ризик-орієнтованого підходу для усунення цих вразливостей.

– Спроєктовано інноваційну архітектурну модель системи адаптивного управління політиками ІБ.Розроблена модель базується на матриці станів, яка визначає чіткі тригери для автоматичного підвищення суворості політик у разі фіксації критичних аномалій. Технічна реалізація контуру моніторингу передбачає використання спеціалізованого програмного забезпечення класу SIEM для відстеження мережевого трафіку в реальному часі та миттєвого блокування підозрілої активності.

– Розроблено покроковий алгоритм та організаційні рекомендації щодо впровадження системи.Запропоновано п'ятиетапний алгоритм (від підготовчо-аналітичного етапу до тестування та промислової експлуатації), який гармонізує організаційні, технологічні та кадрові аспекти захисту. Для юридичної легітимізації змін запропоновано впровадити «Рамкову угоду адаптивної безпеки», трансформувати відділ ІБ в аналітичний центр, а також перейти від формальних інструктажів до інтерактивних методів навчання персоналу (зокрема симуляції фішингових атак).

– Здійснено детальне економіко-технічне обґрунтування доцільності інвестицій у розроблену систему.Розраховано загальну вартість володіння проєктним рішенням (TCO), структурувавши капітальні (CAPEX) та операційні (OPEX) витрати. Визначено, що найбільшу частку в бюджеті впровадження становить придбання базового ПЗ та ліцензій (40%), що є виправданим для сучасних наукомістких рішень у сфері кіберзахисту.

– Доведено високу економічну ефективність розробленого рішення для ТОВ «BLYSKAVKA». На основі розрахунку показника запобіженого збитку (ΔZ) та коефіцієнта повернення інвестицій (ROSI) встановлено, що система забезпечує синергетичний ефект. Впровадження адаптивного управління дозволяє підприємству

суттєво оптимізувати витрати: фінансові ресурси не розпорошуються на статичний захист усього периметра, а динамічно спрямовуються на нейтралізацію конкретних актуальних загроз у моменти їх виникнення. Це гарантує надійний захист інформаційних активів та безперебійне функціонування підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Політика інформаційної безпеки : лекція 2. 19 с. URL: https://learn.ztu.edu.ua/pluginfile.php/272305/mod_resource/content/2/%D0%A3%D0%9A%20%D0%9B%D0%95%D0%9A%D0%A6%D0%86%D0%AF2%20FINAL.pdf
2. Політика інформаційної безпеки. Kitsoft. URL: https://kitsoft.ua/ua/politika-informacijnoyi-bezpeki
3. Розробка політики інформаційної безпеки. Referatss. URL: https://referatss.com.ua/work/rozrobka-politiki-informacijnoi-bezpeki-2/
4. Розробка політики інформаційної безпеки за стандартом ISO/IEC 17799 : лабораторна робота № 13. Київський славістичний університет. URL: https://ua.kursoviks.com.ua/metodychni_vkazivky/article_post/1051-laboratorna-robota-no-13-rozrobka-politiki-informatsiynoi-bezpeki-za-standartom-iso-iec-17799-ksu-kiivskiy-slavistichniy-universitet
5. Information Security Policy: Core Components. ScienceDirect. URL: https://www.sciencedirect.com/topics/computer-science/information-security-policy
6. ISO/IEC 27001:2022 — Information Security Management Systems. URL: https://www.iso.org/standard/27001
7. ISO 27001 Annex A — Access Control Policy. InfoSec Institute. URL: https://www.infosecinstitute.com/resources/management-compliance-auditing/iso-27001-framework-what-it-is-and-how-to-comply/
8. ISO PDCA Model (Plan–Do–Check–Act). URL: https://www.nist.gov/document/040813utcresponsepart2pdf
9. Аналіз побудови моделі політики інформаційної безпеки підприємства. URL: https://www.researchgate.net/publication/323728627_Analiz_pobudovi_modeli_politiki_informacijnoi_bezpeki_pidpriemstva (дата звернення: 02.06.2026).

10. Методологічні основи побудови комплексних систем захисту інформації. Київ : ДУІКТ. URL: https://duikt.edu.ua/uploads/l_2225_57006111.pdf (дата звернення: 02.06.2026).
11. Оцінка ризиків та формування адаптивних стратегій безпеки. Політичне життя. МАУП. URL: https://journals.maup.com.ua/index.php/political/article/download/4449/4759/5140 (дата звернення: 02.06.2026).
12. Економічна безпека та кіберзахист суб'єктів господарювання. Проблеми і перспективи економіки та управління. URL: https://ppeu.stu.cn.ua/article/view/299144 (дата звернення: 02.06.2026).
13. Оптимізація інвестицій у цифрову безпеку підприємств. Економіка та суспільство. URL: https://economyandsociety.in.ua/index.php/journal/article/download/3056/2977 (дата звернення: 02.06.2026).
14. Моніторинг та аудит інформаційних ресурсів. Engineering and Educational Technologies. НУПП. URL: https://journals.nupp.edu.ua/eir/uk/article/view/1924 (дата звернення: 02.06.2026).
15. Математичне моделювання процесів адаптивного доступу. Фундаментальні та прикладні проблеми IT : матеріали конференції. ВНТУ. URL: https://conferences.vntu.edu.ua/index.php/fiip/fiip2024/paper/viewFile/20107/16659 (дата звернення: 02.06.2026).
16. Управління ризиками корпоративного сектору. Економіка, фінанси, право. URL: https://efp.in.ua/uk/journal-article/1607 (дата звернення: 02.06.2026).
17. Стан кібербезпеки в умовах невизначеності. PwC Україна. 2022. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html (дата звернення: 02.06.2026).
18. Термінологія. Законодавство України. URL: https://zakon.rada.gov.ua/laws/term/45959 (дата звернення: 02.06.2026).

19. Міжнародний стандарт з управління безпекою (Стратегічний рівень): ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 02.06.2026).
20. Національний орган стандартизації України (Нормативно-методичний рівень) : каталог національних стандартів України у сфері інформаційних технологій та безпеки. ДП «УкрНДНЦ». URL: https://uas.gov.ua
21. Про захист інформації в інформаційно-комунікаційних системах : Закон України (Базове законодавство України: технічний та інтеграційний рівні). Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
22. Про затвердження Положення про забезпечення захисту інформації в інформаційно-комунікаційних системах (Офіційні вимоги щодо створення КСЗІ) : Постанова Кабінету Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF
23. Нормативні документи системи технічного захисту інформації (НД ТЗІ). Адміністрація Держспецзв'язку. URL: https://cip.gov.ua/uk/news/normativni-dokumenti-sistemi-tekhnichnogo-zakhistu-informaciyi
24. Ідентифікація актуальних загроз інформаційній безпеці підприємства : навчальні матеріали. Житомирська політехніка. URL: https://learn.ztu.edu.ua/pluginfile.php/406447/mod_resource/content/1/УК%20ЛЕКЦІЯ7.pdf
25. Інноваційні технології в кібербезпеці : збірник наукових праць / матеріали конференції. ДУІКТ. С. 187. URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf#page=187
26. Наукові праці Національного університету «Полтавська політехніка імені Юрія Кондратюка». URL:

https://reposit.nupp.edu.ua/files/original/19/17608/06e8f1bda6e203f8bf8ea74a359bb1ae0420331c.pdf

27. Вісник економіки. Хмельницький національний університет. URL: https://heraldes.khmnu.edu.ua/index.php/heraldes/article/download/1043/1061
28. Збірник наукових праць економічного факультету. Львівський національний університет імені Івана Франка. URL: https://publications.lnu.edu.ua/collections/index.php/economics/article/download/4904/5482
29. Остапчук В. М. Побудова моделей захисту. Київський столичний університет імені Бориса Грінченка (ФІТМ). 2025. URL: https://elibrary.kubg.edu.ua/id/eprint/56345/1/V_Ostapchuk_FITM_2025.pdf
30. Управління економічною безпекою підприємства в умовах невизначеності. UJAE: Журнал економіки та безпеки. 2024. № 3. С. 60–68. URL: https://ujae.org.ua/wp-content/uploads/2025/01/ujae_2024_r03_a60.pdf
31. Економіка та управління підприємством: виклики сучасності. A-Economics. 2024. Вип. 15. С. 25–34. URL: https://www.a-economics.com.ua/index.php/home/article/download/894/882
32. Стратегічне управління безпекою підприємства. Вісник ВНАУ. 2023. № 2. С. 45–52. URL: http://socrates.vsau.edu.ua/repository/getfile.php/22661.pdf
33. Особливості управління кібербезпекою. Наукові праці НБУВ. 2013. № 1. С. 64–70. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Tpaeiv_2013_1_1_64.pdf
34. Корпоративна безпека в системі управління підприємством. Вчені записки університету «КРОК». 2023. № 2 (70). С. 115–123. URL: https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/download/341/372

35. Ефективність управління інформаційною безпекою. Економічний вісник КПІ. 2023. № 2. С. 88–95. URL: https://ev.fmm.kpi.ua/article/download/278601/273266
36. Управління ризиками інформаційної безпеки. Наукові вісті НБУВ. 2010. № 1. С. 23–30. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nvpusk_2010_1_23.pdf
37. Теоретичні підходи до забезпечення безпеки підприємств. Глобальні та національні проблеми економіки. 2017. № 15. С. 225–230. URL: http://global-national.in.ua/archive/15-2017/15_2017.pdf#page=225
38. Security management in modern conditions. Information Security Journal. 2024. URL: https://isg-journal.com/isjea/article/download/556/308
39. Методичні підходи до захисту інформації в автоматизованих системах. Захист інформації. 2020. № 1. URL: https://web.archive.org/web/20200507093517id_/http://journals.dut.edu.ua/index.php/dataprotect/article/download/2294/2193
40. Організаційні засади управління безпекою підприємства. Вісник Хмельницького національного університету. 2024. № 4. URL: https://heraldes.khmnu.edu.ua/index.php/heraldes/article/download/1916/1957
41. Управління ризиками в системах захисту інформації. Електронний архів ХНУ. 2024. URL: https://elar.khmnu.edu.ua/server/api/core/bitstreams/a9742d23-a08e-47c6-af61-25afbc3f7f88/content
42. Актуальні проблеми кібербезпеки: організаційний вимір. Науковий вісник Університету Грінченка. 2024. № 12. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/download/498/391
43. Стратегії захисту інформаційних ресурсів підприємства : колективна монографія. ТНТУ. 2025. URL: https://elartu.tntu.edu.ua/

44. Політичні та соціальні аспекти забезпечення безпеки. Вісник Прикарпатського національного університету. 2023. № 5. URL: https://journals.pnu.if.ua/index.php/politology/article/download/219/214
45. Інформаційна безпека підприємства: теоретичні та практичні підходи. Netwave. 2025. URL: https://netwave.ua/blog/informacijna-bezpeka-pidpriyemstva-sho-ce/
46. Інформаційна безпека та види можливих загроз у корпоративному секторі. ITBIZ Solutions. 2025. URL: https://itbiz.ua/statti-ta-obzori/informacijna-bezpeka-ta-vidi-mozhlivih-zagroz/
47. Математичне моделювання та інформаційні системи. Електронний архів Київського столичного університету імені Бориса Грінченка. 2026. URL: https://elibrary.kubg.edu.ua/id/eprint/57295/1/S_Rzaieva_O_Lytvyn_P_Skladannyi_Y_Kostiyk_D_Rzaiev_MMiS_2_2026_FITM.pdf
48. Дисертаційні дослідження з управління проектами та програмами. Цифровий репозитарій ХНУМГ. URL: https://radapm.kname.edu.ua/images/Disser/dis_kosenko_vv.compressed.pdf
49. Інформаційна безпека та комп'ютерні системи. Наукові журнали URAN. URL: https://journals.uran.ua/ispss/article/download/340038/328097
50. Глобальні та національні проблеми економіки. Електронне наукове фахове видання. 2016. URL: http://www.global-national.in.ua/archive/11-2016/62.pdf
51. Управління та безпека в сучасних умовах. Інституційний репозитарій ПДАУ. URL: https://dspace.pdau.edu.ua/server/api/core/bitstreams/20b4ff4c-da48-407a-8549-d72e48558a87/content#page=189
52. Науковий вісник. Національна бібліотека України імені В. І. Вернадського. 2015. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nv_2015_11_13.pdf

53. Кібербезпека: освіта, наука, техніка. Науковий журнал Університету Грінченка. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/download/1084/915
54. Економіка підприємства в умовах нестабільності. Журнали ІФНТУНГ. URL: https://eung.nung.edu.ua/index.php/ecom/article/download/827/462
55. Наукові записки Львівського університету бізнесу та права. Серія економічна. 2024. URL: https://nzlubp.org.ua/index.php/journal/article/download/1802/1585
56. Механізми управління підприємствами в умовах невизначеності. Сумський державний педагогічний університет імені А. С. Макаренка. 2021. URL: https://sspu.edu.ua/images/2021/docs/dis/aref_eromenko_58f05.pdf
57. Журнал кількісної економіки та бізнес-теорії. Донецький національний університет імені Василя Стуса. URL: https://jqbthe.donnu.edu.ua/article/download/18580/18478
58. Економічні та технічні аспекти безпеки підприємств. Інституційний репозитарій Сумського державного університету (Eccuir). URL: https://essuir.sumdu.edu.ua/server/api/core/bitstreams/9f001869-5c09-4e2e-ab95-d2bcb55f1a2c/content
59. Журнал європейських науковців. Міжнародний науковий вісник. URL: https://www.eu-scientists.com/index.php/fag/article/download/79/72
60. Моделювання інформаційних систем на підприємствах. Дніпровський національний університет імені Олеся Гончара. URL: https://web.archive.org/web/20220205090219id_/https://mi-dnu.dp.ua/index.php/MI/article/download/333/279
61. Система управління інформаційною безпекою (СУІБ). Офіційні роз'яснення та рекомендації Держспецзв'язку. URL: https://cip.gov.ua/ua/news/sistema-upravlinnya-informaciinoyu-bezpekoyu-suib

62. Нормативно-правова база України у сфері захисту інформації та побудови СУІБ. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11#Text

63. Науковий вісник Національного гірничого університету. 2013. № 4. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&Z21ID=&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nvngu_2013_4_24.pdf

64. Сталий розвиток економіки : науково-виробничий журнал. Тернопільський національний технічний університет імені Івана Пулюя. URL: https://elartu.tntu.edu.ua/bitstream/lib/25998/1/siee.zp.ua_22.09.pdf#page=63

65. Економічний вісник Національного технічного університету України «Київський політехнічний інститут». URL: http://www.economy.kpi.ua/files/files/22_kpi_2008.pdf

66. Причорноморські економічні студії : науковий журнал. 2017. Вип. 23. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/bses_2017_23_18.pdf

67. Техніко-економічне обґрунтування інженерних рішень та інвестиційних проектів. Електронний репозитарій ТНТУ. URL: https://elartu.tntu.edu.ua/bitstream/lib/29300/1/Teo%20R1%202003.pdf

68. Вісник Хмельницького національного університету. Серія: Технічні науки. 2020. № 2 (283). URL: https://journals.khnu.km.ua/vestnik/pdf/tech/pdfbase/2020/VKNU-TS-2020-N2_(283).pdf#page=36

69. Науковий вісник Ізмаїльського державного гуманітарного університету. Серія: Педагогічні та технічні науки. URL: http://dspace.idgu.edu.ua/jspui/handle/123456789/1748

70. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. URL: https://znp-cvsd.nuou.org.ua/article/download/339811/327918
71. Економічна оцінка та розрахунок ефективності інвестиційних проектів на підприємствах. Практичний посібник Flexi-Project. URL: https://flexi-project.com/uk/як-розрахувати-економічну-ефективні
72. Глосарій законодавчих термінів. Офіційний вебпортал парламенту України «Законодавство України». URL: https://zakon.rada.gov.ua/laws/term/30014
73. Економічний аналіз та фінансове обґрунтування інноваційної діяльності. Електронна бібліотека Buklib. URL: https://buklib.net/books/22765
74. ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ Виконавчого комітету Стрийської міської ради. Стрий, 2025. С. 7–22. URL: https://stryi-rada.gov.ua/doc/wp-content/uploads/2025/09/rish2025293_d.pdf
75. ДСТУ EN ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги (EN ISO/IEC 27001:2022, IDT). Київ : ДП «УкрНДНЦ», 2023. 68 с.
76. Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу (Директива NIS2) [Електронний ресурс]. Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
77. ДСТУ ISO 22301:2021. Безпека та стійкість. Системи управління безперервністю бізнесу. Вимоги (ISO 22301:2019, IDT). Київ : ДП «УкрНДНЦ», 2021. 42 с..