Ф А2.2.1-32-367

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ
Фармацевтичний факультет
Кафедра менеджменту, маркетингу та забезпечення якості у фармації

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **ФОРМУВАННЯ ПІДХОДІВ ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІТЧИЗНЯНОГО ПІДПРИЄМСТВА**

Виконав:
здобувач вищої освіти
2 курсу, групи 1
спеціальності 073 Менеджмент
освітньої програми
Якість, стандартизація та сертифікація
Володимир СОЛОДКИЙ

Керівник:
доцент закладу вищої освіти
кафедри управління та забезпечення якості у фармації
канд. фармац. наук, доц.
Тетяна ЗБОРОВСЬКА

Рецензент:
професор закладу вищої освіти
кафедри фармацевтичної технології, стандартизації та сертифікації ліків
ІПКСФ НФаУ,
д. фармац. наук., професор
Вячеслав ЛЕБЕДИНЕЦЬ

Харків – 2026 рік

АНОТАЦІЯ

У кваліфікаційній роботі досліджено теоретичні, організаційні та технічні аспекти формування сучасних підходів до інформаційної безпеки на вітчизняному підприємстві. Розроблено ризик-орієнтовану методику побудови системи інформаційної безпеки із практичним застосуванням на прикладі ТОВ «СФЕРА ІТ». Особливу увагу приділено ролі системи забезпечення безперервності бізнесу (BCP/DRP) як основи кіберстійкості підприємства.

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 40 найменувань, 3 додатки, і містить 4 малюнки, 8 таблиць. Повний обсяг кваліфікаційної роботи складає 79 сторінок, з яких перелік посилань займає 5 сторінок, додатки – 13 сторінок.

Ключові слова: інформаційна безпека, ризик-орієнтований підхід, система забезпечення безперервності бізнесу, кіберзагрози, управління вразливостями, Zero Trust, ISO/IEC 27001:2022, ТОВ «СФЕРА ІТ».

ABSTRACT

The qualification work explores the theoretical, organizational and technical aspects of the formation of modern approaches to information security at a domestic enterprise. A risk-oriented methodology for building an information security system with practical application on the example of SFERA IT LLC has been developed. Particular attention is paid to the role of the business continuity plan (BCP/DRP) as the basis for the enterprise's cyber resilience.

Structure and scope of the qualification work: the qualification work consists of an introduction, three sections, general conclusions, a list of references of 40 items, 3 appendices, and contains 4 figures, 8 tables. The full volume of the qualification work is 79 pages, of which the list of references takes up 5 pages, appendices – 13 pages.

Keywords: information security, risk-oriented approach, business continuity system, cyber threats, vulnerability management, Zero Trust, ISO/IEC 27001:2022, SFERA IT LLC.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

BCP/DR – План безперервності / Відновлення після аварій

COBIT – Control Objectives for Information and Related Technologies

CSF – Cybersecurity Framework

EDR/XDR – Endpoint/Extended Detection and Response

IAM/Iga – Identity and Access Management / Identity Governance

ISMS – система управління інформаційною безпекою

KPI – ключові показники ефективності

RACI – Responsible, Accountable, Consulted, Informed

RTO/RPO – цільовий час відновлення / цільова точка відновлення

SIEM – Security Information and Event Management

ІБ – інформаційна безпека

СУЯ – система управління якістю

ВСТУП

Актуальність теми. Цифровізація бізнес-процесів, розподілені ІТ-архітектури та зростання залежності від хмарних сервісів радикально збільшили площу атаки підприємств. Перехід від точкових технічних рішень до керованих рамками моделей (NIST CSF 2.0; ISO/IEC 27001:2022; COBIT) зумовлює потребу сформувати узгоджений підхід до інформаційної безпеки (ІБ), що враховує контекст, ризик-апетит і ресурсні обмеження [20].

Інформаційна безпека (ІБ) – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, що використовується.

Згідно з міжнародним стандартом ISO/IEC 27001, теорія ІБ базується на трьох фундаментальних принципах, відомих як «Тріада CIA» [20]:

Конфіденційність (Confidentiality): Забезпечення доступу до даних лише тим особам, які мають на це право. Це захист від несанкціонованого перегляду.

Цілісність (Integrity): Підтримка точності та повноти інформації. Це гарантія того, що дані не були змінені або видалені зловмисниками чи через системні помилки.

Доступність (Availability): Забезпечення безперебійного доступу користувачів до інформації та сервісів у потрібний час.

З теоретичної та практичної точок зору, ІБ вирішує такі ключові завдання:

Мінімізація ризиків та збитків: Захист від кібератак, вірусів та фішингу запобігає фінансовим втратам і зупинкам виробництва. [5]

Захист приватності: У 2026 році захист персональних даних є критичним для запобігання крадіжці особистості та дотримання законодавства (наприклад, GDPR).

Збереження репутації: Витік корпоративних даних або клієнтських баз може назавжди знищити довіру до бренду чи організації.

Забезпечення національної стійкості: На державному рівні ІБ захищає критичну інфраструктуру (енергомережі, банківську систему, зв'язок) від кібердиверсій.

Підтримка безперервності бізнесу: Розробка стратегій резервного копіювання та відновлення дозволяє системам працювати навіть після серйозних інцидентів. [22]

Мета і завдання. Метою є розробка інтегрованої методики формування підходів до інформаційної безпеки вітчизняного підприємства на базі NIST CSF 2.0, ISO/IEC 27001:2022 та принципів ESRM з урахуванням вимірюваних метрик ефективності [20].

Завдання дослідження:

- систематизувати понятійний апарат і стандарти;
- проаналізувати сучасні підходи;
- розробити інтегровану рамку й алгоритм реалізації проєкту;
- оцінити його ефективність за ключовими показниками (KPI).

Об’єкт і предмет. Об’єкт – процеси управління ІБ. Предмет – підходи, моделі та методи формування політик, процесів і контролів ІБ.

Наукова новизна. Синтез профілів NIST CSF 2.0 з контурами ISMS (ISO/IEC 27001:2022) і процесами COBIT; матриця CSF ISO 27002 COBIT для дорожньої карти зрілості. [20]

Практичне значення. Розроблено артефакти: чек-лист аудиту, шаблони політик, методику профілювання CSF, карту контролів, модель KPI (MTTD/MTTR, виконання плану ризиків, SoA, покриття журналів). [5]

Методи дослідження: аналіз і синтез літератури, порівняльний аналіз стандартів, моделювання процесів, експертне опитування, імітаційне профілювання, побудова KPI-панелі.

Дослідження і публікації. Солодкий В.В., Крутських Т.В., Зборовська Т.В. Формування підходів до інформаційної безпеки вітчизняного підприємства. YOUTH PHARMACY SCIENCE: матеріали VI Всеукраїнської

науково-практичної конференції з міжнародною участю (10-11 грудня 2025 р., м. Харків). – Харків: НФаУ, 2025. – С.533-534 (Додаток А).

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 40 найменувань, 3 додатки, і містить 4 малюнки, 8 таблиць. Повний обсяг кваліфікаційної роботи складає 79 сторінок, з яких перелік посилань займає 5 сторінок, додатки – 13 сторінок.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття та категорії інформаційної безпеки.

Формування науково обґрунтованих підходів до забезпечення інформаційної безпеки підприємства потребує чіткого визначення ключових понять, категорій та термінології. Понятійно-категоріальний апарат забезпечує однозначність трактування основних термінів, створює спільну методологічну основу для аналізу, оцінювання ризиків, побудови політик безпеки та розроблення практичних заходів. У межах інформаційної безпеки використовуються як технічні, так і організаційно-правові категорії, що відображають багатовимірність цього явища. [5]

Інформація у контексті безпеки розглядається як будь-які дані, які мають цінність для підприємства, незалежно від форми подання – електронної, паперової, усної чи мультимедійної.

Інформаційний актив – це ресурс підприємства, що містить інформацію або забезпечує її обробку, передачу, зберігання чи використання. До інформаційних активів належать:

- дані (службові, персональні, технічні, фінансові, комерційні);
- інформаційні системи (ERP, CRM, SCADA, бухгалтерські системи);
- обладнання та інфраструктура (сервери, мережеве обладнання, робочі станції);
- програмне забезпечення;
- доступи, облікові записи та облікові дані;
- персонал, що має знання, компетенції та доступи.

Таким чином, інформаційні активи охоплюють як матеріальні, так і нематеріальні елементи.

Інформаційна безпека – це стан захищеності інформаційних активів підприємства від випадкових або навмисних впливів, унаслідок яких може бути порушено їхню конфіденційність, цілісність чи доступність.

Традиційно ІБ базується на трикутнику CIA:

- Конфіденційність (Confidentiality) – забезпечення доступу до інформації лише уповноваженим особам.
- Цілісність (Integrity) – гарантування точності, повноти та незмінності даних.
- Доступність (Availability) – забезпечення можливості отримати інформацію у потрібний час.

Сучасні моделі доповнюють CIA ще трьома компонентами:

- Відстежуваність / аудит (Accountability/Traceability)
- Автентичність (Authenticity)
- Відмовостійкість / стійкість (Resilience)

Ці три поняття складають основу будь-якої системи управління безпекою.

Загроза: подія або дія, яка здатна завдати шкоди інформаційним активам, порушити їх конфіденційність, цілісність або доступність. Приклади загроз:

- кібератаки (фішинг, DDoS, шкідливе ПЗ);
- внутрішні порушення;
- технічні відмови;
- помилки персоналу;
- фізичні інциденти (пожежа, крадіжка, стихійні лиха). [22]

Вразливість: слабке місце системи безпеки, яке може бути використане загрозою. Приклади:

- відсутність оновлень;
- помилки конфігурації;
- слабкі паролі;

- недостатній контроль доступу;
- відсутність шифрування.

Ризик: ймовірність реалізації загрози з урахуванням існуючих вразливостей та очікуваних наслідків. У простій формі ризик описують як:[5]

Ризик = Ймовірність × Наслідки

У ширшому контексті ризик розглядається у взаємозв'язку з критичністю активів та дієвістю поточних заходів безпеки. [5]

Інцидент ІБ – це подія, яка:

- вже спричинила; або
- може потенційно спричинити

порушення одного або кількох принципів CIA.

Інциденти поділяють на:

- події (events) – технічні або організаційні аномалії;
- порушення (breaches) – доведена компрометація активів;
- критичні інциденти – ті, що впливають на бізнес-процеси, викликають зупинку сервісів, витік даних, фінансові втрати. [22]

Контроль безпеки (security control) – це захід (технічний, організаційний або фізичний), що зменшує ризики. Контролі поділяються на:

- Превентивні (MFA, шифрування, політики доступу);
- Детективні (SIEM, IDS/IPS, логування);
- Коригувальні (бекапи, патч-менеджмент);
- Компенсуючі (додаткові заходи, що покривають недоліки основних). [5]

У сучасних системах ІБ контролі будуються відповідно до стандартів ISO/IEC 27002, NIST SP 800-53, CIS Controls. [7]

Управління ІБ потребує чіткої ієрархії документів:

- Політика – високорівневий документ, що визначає принципи безпеки.
- Стандарт – деталізує мінімальні вимоги до реалізації політики.

- Процедура – описує конкретну послідовність дій для виконання вимог.

Наприклад: Політика управління доступом переходить у формування Стандартів для паролів та Процедури видачі доступу.

Зрілість ІБ визначає здатність підприємства:

- системно управляти ризиками; [5]
- мінімізувати вплив інцидентів; [22]
- забезпечувати відповідність стандартам;
- інтегрувати ІБ у бізнес-процеси.

У сучасних умовах інформаційна безпека є:

- елементом корпоративного управління (governance);
- частиною стратегічного планування;
- засобом забезпечення конкурентоспроможності;
- механізмом підтримки операційної стійкості бізнесу.

Таким чином, ІБ не обмежується технічними засобами – вона інтегрується у всі бізнес-процеси та забезпечує виконання нормативних, договірних і регуляторних вимог.

1.2 Стандарти та рамки: ISO/IEC 27001:2022, ISO/IEC 27002, NIST CSF 2.0, COBIT

Забезпечення інформаційної безпеки підприємства неможливе без застосування формалізованих міжнародних стандартів та рамкових моделей. Вони встановлюють вимоги, принципи, кращі практики та механізми впровадження системи управління інформаційною безпекою (СУІБ), а також сприяють уніфікації процесів, забезпечують відповідність нормативним вимогам та підвищують рівень кіберстійкості. До найбільш поширених на рівні підприємств належать: ISO/IEC 27001:2022, ISO/IEC 27002, NIST Cybersecurity Framework (CSF) 2.0 та COBIT. [20]

ISO/IEC 27001:2022 – стандарт вимог до системи управління інформаційною безпекою [20]

ISO/IEC 27001:2022 є ключовим міжнародним стандартом, що визначає вимоги до побудови, впровадження, підтримки та вдосконалення СУІБ. Його основні характеристики: [20]

Структура та підхід:

- ґрунтується на моделі PDCA (Plan–Do–Check–Act);
- інтегрується з іншими системами менеджменту (ISO 9001, ISO 22301 тощо);
- передбачає включення управління ризиками як центрального елемента. [5]

Ключові елементи ISO 27001

- Контекст організації: аналіз зацікавлених сторін, області застосування.
- Лідерство та політики безпеки.
- Планування управління ризиками ІБ. [5]
- Підтримка: ресурси, компетентності, документація.
- Операційний контроль безпеки.
- Оцінювання ефективності (KPIs, аудит, моніторинг).
- Постійне вдосконалення.

Додаток А ISO/IEC 27001:2022 містить перелік контрольних заходів, структурованих за 4 доменами: [20]

- Організаційні (Organizational).
- Людські (People).
- Фізичні (Physical).
- Технологічні (Technological).

Контролі Додатку А повністю відповідають контрольним практикам ISO/IEC 27002.

ISO/IEC 27002 – каталог контрольних заходів безпеки

ISO/IEC 27002 є деталізованим керівництвом, що описує як саме повинні виконуватися контролі, зазначені в ISO 27001. Стандарт не встановлює вимог – він надає практичні рекомендації.

Структура та зміст ISO 27002

У виданні 2022 року контролі згруповані за темами:

5 – Організаційні контролі

6 – Людські контролі

7 – Фізична безпека

8 – Технологічні контролі

Серед ключових груп контролів:

- політики та структура управління;
- сегментація мережі;
- криптографія;
- журналювання, моніторинг та SIEM;
- управління конфігураціями;
- управління вразливостями;
- резервування та відновлення;
- захист від шкідливого ПЗ;
- DevSecOps та безпечна розробка.

Значення ISO/IEC 27002

- забезпечує уніфікований підхід до контролів;
- дає можливість аудиту та побудови SoA;
- дозволяє формувати політики ІБ на єдиній базі;
- є мостом між вимогами (ISO 27001) і їх реалізацією.

NIST Cybersecurity Framework (CSF) 2.0. NIST CSF – це рамкова модель кібербезпеки, розроблена для підприємств різних галузей. Версія 2.0 розширює можливості моделі, мінімізує складність та включає сучасні вимоги. Структура NIST CSF 2.0 містить 6 основних функцій: [7]

- Identify (Ідентифікація)

- Protect (Захист)
- Detect (Виявлення)
- Respond (Реагування)
- Recover (Відновлення)
- Govern (Управління) – нова функція 2.0

Суть CSF дає підприємству можливість оцінити рівень зрілості із безпеки; містить outcomes (цільові результати), які можна мапувати на ISO чи COBIT; підтримує різні рівні впровадження (Implementation Tiers); дозволяє будувати профілі безпеки (Current / Target Profile). [16]

Переваги: гнучкість у впровадженні; орієнтація на ризики; проста інтеграція у корпоративні системи управління. [5]

NIST CSF часто використовується як операційний фреймворк, тоді як ISO 27001 – як формальний. [7]

COBIT – корпоративна модель управління IT та безпекою [16]

COBIT (Control Objectives for Information and Related Technologies) – це рамка корпоративного IT-управління, що охоплює як інформаційну безпеку, так і загальне управління інформаційними ресурсами. [16]

Особливості COBIT[16]

- охоплює всі аспекти IT Governance;
- містить набір процесів, цілей контролю, метрик і практик;
- дозволяє підприємству узгоджувати ІБ із загальною стратегією та цілями бізнесу;
- має інтеграцію з ISO 27001 та ITIL.

Структура COBIT: Governance Objectives (EDM) та Management Objectives (APO, BAI, DSS, MEA). [16]

Серед них багато процесів напряму стосуються ІБ: APO12 – Управління ризиками; DSS05 – Забезпечення безпеки; DSS02 – Керування інцидентами; MEA03 – Оцінювання відповідності. [5]

COBIT є важливим елементом для підприємств, що прагнуть інтегрувати ІБ у корпоративну модель управління. [16]

Хоча ISO 27001, NIST CSF та COBIT виконують різні функції, вони не суперечать, а доповнюють один одного: [7]

- ISO/IEC 27001 – система управління (менеджмент). [20]
- ISO/IEC 27002 – контрольні заходи (як робити).
- NIST CSF – операційна рамка, орієнтована на ризики та зрілість.
- COBIT – корпоративне IT-управління та відповідність стратегії.

Таким чином, підприємство може одночасно використовувати: ISO 27001 для аудитів; ISO 27002 для контролів; NIST CSF для оцінювання зрілості; COBIT для узгодження із бізнес-цілями та говернансом. [7]

1.3. Управління ризиками: ERM/ESRM і ISO 27005

Ефективне управління ризиками є ключовим елементом формування підходів до інформаційної безпеки підприємства. У сучасних умовах кіберзагроз традиційне технічне розуміння безпеки є недостатнім, тому актуальним стає інтеграційний підхід, спрямований на узгодження інформаційної безпеки з бізнес-цілями та загальною системою корпоративного управління ризиками (Enterprise Risk Management, ERM). У межах цього підходу особливе місце займає концепція Enterprise Security Risk Management (ESRM), яка розглядає безпеку як бізнес-функцію, що має підтримувати створення, збереження і розвиток цінності підприємства.

Одночасно із цим міжнародний стандарт ISO/IEC 27005 визначає структуровану методологію управління ризиками інформаційної безпеки. Використання ISO/IEC 27005 забезпечує формалізований процес виявлення, аналізу та обробки ризиків, що дозволяє узгодити технічні, організаційні та управлінські заходи із системними рамками ERM та ESRM.

ERM спрямований на встановлення єдиного підходу до ідентифікації, оцінювання та управління ризиками на всіх рівнях функціонування підприємства. У цьому контексті ризики інформаційної безпеки розглядаються не відокремлено, а в рамках загальної карти корпоративних ризиків. Основні принципи ERM включають:

- системність і взаємозв’язок ризиків;
- інтеграцію процесу управління ризиками у стратегічне та операційне управління;
- орієнтацію на захист вартості (value protection) та можливість її підвищення (value creation);
- прозорість, документованість та обґрунтованість рішень.

В рамках ERM ризики ІБ оцінюються так само, як і фінансові, операційні, правові чи стратегічні ризики, що забезпечує їхню коректну пріоритизацію. [5]

Підхід ESRM розширює традиційне управління інформаційною безпекою, роблячи акцент на:

- зв’язку між активами та цінністю бізнесу;
- повній участі керівництва у визначенні критичних активів та прийнятного рівня ризику;
- інтеграції безпеки у всі ключові бізнес-процеси;
- фокусі на управлінні ризиками, а не на окремих технологіях;
- орієнтації на підтримку бізнес-цілей, а не виключно на технічний контроль.

ESRM передбачає, що служба безпеки виступає партнером для бізнес-підрозділів, а не окремою структурою. Завдяки цьому ризики інформаційної безпеки розглядаються у контексті загальних бізнес-ризиків, а рішення щодо впровадження захисних заходів стають більш збалансованими і економічно обґрунтованими. [5]

ISO/IEC 27005 задає чітку послідовність дій у процесі управління ризиками, що включає: [3]

1. Встановлення контексту дає визначення меж оцінювання ризиків, класифікує інформаційні активи, встановлює критерії прийнятності ризику та описує бізнес-процеси, які підтримують ці активи. [5]

2. Ідентифікація ризиків: визначення загроз і вразливостей; встановлення потенційних шляхів реалізації атак; аналіз залежностей між активами та процесами.

3. Аналіз ризиків: оцінювання ймовірностей реалізації загроз; визначення потенційних збитків; аналіз чинників, які впливають на рівень ризику.

4. Оцінювання ризиків: порівняння отриманих значень з критеріями прийнятності та визначення пріоритетів щодо обробки ризиків.

5. Обробка ризиків включає вибір одного або комбінованих варіантів: уникнення; зменшення; передання (наприклад, через страхування або аутсорсинг); прийняття.

6. Моніторинг і перегляд це регулярне оновлення оцінки ризиків; аудит ефективності заходів; відстеження нових загроз і змін у процесах.

7. Комунікація і консультації передбачає взаємодію між керівництвом, ІТ-підрозділом, службою безпеки та власниками активів для забезпечення спільного розуміння ризиків.

Поєднання зазначених підходів дає підприємству можливість вибудувати цілісну модель управління ризиками інформаційної безпеки, де: ISO 27005 забезпечує методологічну основу; ESRM створює модель взаємодії бізнесу та безпеки; ERM задає корпоративний контекст і стратегічні орієнтири. У підсумку підприємство отримує: [5]

- прозору та керовану систему оцінювання ризиків;
- можливість приймати рішення щодо безпеки на основі бізнес-пріоритетів;
- оптимізацію витрат і підвищення відповідності стандартам;
- підвищення стійкості до інцидентів та відмов; [22]
- чітку взаємодію між технічними та управлінськими рівнями.

1.4. ISO/IEC 27002:2022 – структура контролів і атрибути

ISO/IEC 27002:2022 є методичним стандартом, який визначає детальні практики реалізації контрольних заходів інформаційної безпеки, зазначених у Додатку A ISO/IEC 27001:2022. На відміну від ISO 27001, що встановлює вимоги, ISO 27002 надає розгорнуті рекомендації, приклади та контекст застосування контролів. Видання 2022 року зазнало значної модернізації та було адаптоване до сучасних кіберзагроз, хмарних технологій, DevSecOps та Zero Trust. [20]

У стандарті вперше введено атрибутивну модель, яка дозволяє підприємствам гнучко класифікувати, групувати та адаптувати контролі відповідно до своїх потреб.

Структура контролів ISO/IEC 27002:2022

Стандарт містить 93 контролі, об’єднані в 4 тематичні домени, що відповідають чотирьом типам заходів безпеки:

5 – Організаційні контролі (Organizational Controls).

6 – Людські контролі (People Controls).

7 – Фізичні контролі (Physical Controls).

8 – Технологічні контролі (Technological Controls).

Таке групування полегшує побудову політик, проведення аудиту, складання SOA (Statement of Applicability) та інтеграцію з іншими фреймворками.

Організаційні контролі (розділ 5). Цей розділ охоплює стратегічні, процедурні та адміністративні механізми управління безпекою, включаючи:

- політики інформаційної безпеки;
- ролі та відповідальність;
- сегментацію мереж;
- захист від шкідливих дій персоналу;
- безпеку постачальників;
- управління ризиками;

- планування безперервності;
- моніторинг та аудит.

Організаційні контролі формують основу СУІБ та забезпечують відповідність вимогам ISO 27001.

Людські контролі (розділ 6). Спрямовані на забезпечення безпечної поведінки персоналу:

- перевірки перед наймом;
- навчання та обізнаність;
- обов’язки персоналу щодо поводження з інформацією;
- реагування на порушення дисципліни;
- управління ризиками, пов’язаними з людським чинником.

Підкреслюється, що персонал – ключовий елемент кіберзахисту, а людський фактор є одним з головних джерел ризиків. [5]

Фізичні контролі (розділ 7) включають вимоги до:

- фізичного зонування;
- контролю доступу до приміщень;
- захисту обладнання;
- безпеки робочих місць;
- середовищних ризиків (пожежа, затоплення, кліматичні впливи).

Контролі забезпечують захист матеріальних активів підприємства.

Технологічні контролі (розділ 8) охоплюють технічні аспекти:

- управління ідентифікацією і доступом (IAM);
- автентифікація, MFA, RBAC;
- ведення журналів та моніторинг;
- захист від шкідливого ПЗ;
- криптографія;
- резервування;
- DevSecOps та безпечна розробка;
- управління конфігураціями;

- вразливості та патч-менеджмент.

Технологічні контролі – основа технічної кіберстійкості підприємства.

Ключовою інновацією оновленого стандарту ISO/IEC 27002:2022є введення атрибутів контролів, які дозволяють: класифікувати контролі за різними характеристиками; будувати власні профілі безпеки; узгоджувати контролі з NIST CSF, COBIT, CIS Controls; оптимізувати позиціювання контролів у політиках; автоматизувати управління ризиками та Audits-as-Code. [7]

Атрибути не змінюють зміст контролів – вони є метаданими, що дозволяють гнучко групувати їх залежно від контексту підприємства.

Стандарт визначає п’ять груп атрибутів, кожна має підкатегорії:

1. Control Type (Тип контролю): превентивний, детективний, коригувальний. Це допомагає будувати архітектуру Defense-in-Depth.

2. Cybersecurity Concepts (Кіберконцепти) відповідають функціям NIST (Identify, Protect, Detect, Respond, Recover): ідентифікація (Identify), захист (Protect), виявлення (Detect), реагування (Respond), відновлення (Recover). Завдяки цьому легко мапувати ISO 27002 на CSF. [7]

3. Information Security Properties (Властивості ІБ) відповідають CIA+: конфіденційність, цілісність, доступність, автентичність, відстежуваність, відмовостійкість. Це дозволяє визначити, на яку властивість активів спрямований контроль.

4. Operational Capabilities (Операційні можливості) підкреслюють функціональні категорії безпеки: управління доступом, захист від загроз, керування активами, оцінювання безпеки, реагування на інциденти, безперервність, розробка та інженерія безпеки. Цей атрибут найчастіше використовується для побудови Security Operations Playbooks. [22]

5. Security Domains (Домен захисту): управління ризиками, захист від технічних загроз, фізична безпека, захист у ланцюгу постачання, керування інформацією/даними. Це дозволяє інтегрувати ISO 27002 з бізнес-моделями (ERM/ESRM). [5]

Використання атрибутів дає змогу будувати власні “профілі безпеки” залежно від галузі, швидко адаптувати СУІБ до нових загроз, автоматизувати аудит і SoA (особливо у SIEM/GRC системах), виконувати мапування на інші фреймворки, будувати комплексну карту контролів, забезпечити зворотну трасування від загроз до контролів.

Підприємство може використовувати стандарт для:

- розроблення політик;
- побудови каталогів контролів;
- формування чіткої архітектури безпеки;
- управління ризиками; [5]
- документування SoA;
- оцінювання зрілості;
- підготовки до сертифікації ISO 27001.

Оновлена атрибутивна модель дозволяє створювати гнучкі, кастомізовані, масштабовані програми ІБ, адаптовані до реальних потреб бізнесу.

1.5. NIST CSF 2.0 – функції, категорії та outcomes

NIST Cybersecurity Framework (CSF) – один із найвідоміших міжнародних фреймворків кібербезпеки, який застосовується підприємствами для побудови системи управління ризиками, оцінки зрілості процесів та планування заходів захисту. Версія 2.0, представлена у 2024 році, стала значним оновленням, яке розширило рамку, спростило її структуру та адаптувало її до сучасних кіберзагроз, хмарних моделей та вимог до говернансу. [7]

NIST CSF 2.0 відрізняється від ISO/IEC 27001 тим, що не є стандартом відповідності – це операційний фреймворк, спрямований на практичне впровадження та оцінювання кіберзахисту через вимірювані результати (outcomes). [20]

Структура NIST CSF 2.0. Framework складається з трирівневої структури: [7]

Функції (Functions) – найвищий рівень, описує великі домени діяльності.

Категорії (Categories) – деталізують напрями роботи в межах кожної функції.

Outcomes – опис результатів, яких має досягти організація (конкретні наведені цілі).

Це дозволяє підприємству будувати власні профілі (Current/Target Profile) та порівнювати ступінь реалізації контролів.

Основні функції NIST CSF 2.0. Версія 2.0 містить шість функцій, що охоплюють повний життєвий цикл управління ризиками. [7]

1. Govern (Управління) – нова функція CSF 2.0

Включає стратегічні аспекти: роль керівництва; політики та процедури; структура відповідальності; управління ризиками; контроль постачальників; вимоги відповідності (compliance).

Сутність Govern – у поєднанні ІБ із бізнес-цілями та корпоративним управлінням. Категорії Govern (приклади): GV.PO – політики, GV.RR – ролі та відповідальність, GV.RM – управління ризиками, GV.SC – безпека ланцюга постачання, GV.OV – нагляд та аудит.

2. Identify (Ідентифікація) містить категорії, що забезпечують розуміння бізнес-контексту та активів: інвентаризація активів; класифікація даних; оцінювання ризиків; модель загроз; залежності від постачальників. Outcomes Identify потрібні для створення карти активів та ризиків. [5]

3. Protect (Захист) охоплює превентивні заходи: доступи (IAM, RBAC, MFA); шифрування; сегментація мережі; налаштування; захист кінцевих точок; обізнаність персоналу. Protect відповідає за мінімізацію ймовірності інцидентів. [22]

4. Detect (Виявлення) включає: моніторинг подій (SIEM, SOC); кореляція журналів; аналіз аномалій; виявлення поведінкових ризиків. Detect відповідає за раннє виявлення аномалій та потенційних атак. [5]

5. Respond (Реагування) охоплює процес реагування: аналіз інцидентів;

оперативне рішення; ескалація; інформування керівництва; взаємодія з зовнішніми структурами. Respond забезпечує мінімізацію шкоди. [22]

6. Recover (Відновлення) містить:плани відновлення (DRP); резервування; відновлення сервісів; оцінку післяінцидентних заходів (lessons learned). Recover підвищує стійкість та відмовостійкість бізнесу. [22]

Категорії NIST CSF 2.0. Кожна функція містить підкатегорії (Categories), які деталізують: [7]

- що саме потрібно робити;
- в який спосіб;
- на якому рівні зрілості.

У NIST CSF 2.0 сформовано понад 100 категорій, згрупованих за: управління (Govern); ідентифікацією активів; контрзаходами Protect; SIEM/SOC; IR/DR; тестуванням безпеки; DevSecOps; Zero Trust. [7]

Outcomes – ключовий елемент CSF 2.0. Outcomes – це очікувані результати, а не процеси чи вимоги. Саме outcomes роблять CSF практичним, операційним та вимірюваним.

Приклади outcomes:

“Ідентифіковано всі інформаційні активи підприємства”

“Впроваджено багатофакторну автентифікацію для всіх критичних систем”

“Журнали подій збираються централізовано та корелюються у SIEM”

“Інциденти реагування документуються і аналізуються”

“Відновлення сервісів виконується у межах визначених RTO/RPO”

Це дозволяє: формувати вимірювані KPI; мапувати ISO та COBIT; визначати прогалини (GAP); будувати dashboard-и; масштабувати програму ІБ. [16]

Рівні впровадження (Implementation Tiers). NIST CSF 2.0 визначає 4 рівні зрілості: [7]

Partial – реактивний, без формалізації.

Risk-Informed – ризик-орієнтований, частково системний.

Repeatable – стандартизований, контрольований.

Adaptive – прогнозуючий, з аналітикою та автоматизацією.

Tiers допомагають підприємству визначити поточний і цільовий стан.

Взаємозв'язок NIST CSF 2.0 з ISO/IEC 27001 і COBIT. NIST CSF 2.0 ідеально інтегрується з іншими рамками: ISO 27001 – вимоги, ISO 27002 – контролі, CSF – результати діяльності, COBIT – процеси управління. [20]

Саме тому CSF часто застосовується як операційна надбудова над ISO 27001.

Впровадження CSF 2.0 дає організації: чітку, вимірювану модель кіберзахисту; узгодженість між бізнес-цілями та ІБ; інструменти для побудови roadmap-ів; зручний механізм оцінювання зрілості; можливість інтеграції з DevSecOps і Zero Trust; гнучкість та масштабованість. [19]

1.6. Метрики ефективності та узгодження CSF і взаємозв'язок з ISO/IEC 27002

Оцінювання ефективності системи інформаційної безпеки потребує застосування кількісних та якісних метрик, які дозволяють вимірювати стан захищеності, динаміку покращень та рівень відповідності вимогам стандартів. У межах запропонованого підходу ключовим завданням є встановлення зв'язку між функціями Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) та конкретними практиками і контролями стандарту ISO/IEC 27002. Це дозволяє сформувати інтегровану модель оцінювання, яка одночасно підтримує процес управління ризиками, аудит відповідності та оперативний моніторинг показників безпеки. [5]

Для кожної функції CSF визначаються релевантні ключові показники ефективності (KPI), які охоплюють технічні, процесні та організаційні аспекти. Функція Identify:

1. Відсоток ідентифікованих інформаційних активів від фактичної кількості.

2. Частота оновлення реєстру активів.

3. Рівень охоплення аналізом ризиків (coverage ratio). [5]

4. Відсоток актуалізованих політик та процедур.

Функція Protect:

1. Покриття багатофакторною автентифікацією (MFA Coverage Rate).

2. Частка критичних систем, інтегрованих з SSO.

3. Відсоток застосованих оновлень і патчів у встановлені строки (Patch Compliance).

4. Кількість порушень політик доступу.

5. Повнота журналювання дій (Logging Coverage).

Функція Detect:

1. MTTD (Mean Time to Detect) – середній час виявлення інциденту.

2. Охоплення моніторингом (SIEM Coverage).

3. Відсоток корельованих подій у порівнянні з необробленими логами.

4. Доля інцидентів, виявлених автоматизовано vs вручну. [22]

Функція Respond:

1. MTTR (Mean Time to Respond) – середній час реакції.

2. Відсоток інцидентів, для яких є документовані SOP (Standard Operating Procedures).

3. Тривалість ескалації.

4. Кількість відхилень від плану реагування.

5. Частота тестування планів реагування (Response Plan Testing Rate). [22]

Функція Recover:

1. Середній час відновлення сервісів (Mean Time to Recovery).

2. Відсоток систем, для яких існують актуальні резервні копії.

3. Успішність відновлення даних під час тестів (Backup Restore Success Rate).

4. Час повного відновлення після інциденту (Full Recovery Time).[22]

ISO/IEC 27002 визначає практики безпеки та контрольні заходи, але не задає конкретних метрик. Тому у процесі узгодження здійснюється мапування KPI CSF на відповідні контролі ISO/IEC 27002 (табл. 2.1.). Це дозволяє:

- забезпечити прозорість вимірювання ефективності;
- спростити аудит та самооцінку;
- створити єдине середовище моніторингу для технічного та управлінського рівнів;
- визначити критерії відповідності у документі Statement of Applicability (SoA).

Узгодження виконується шляхом:

1. Виділення outcome-функцій CSF – наприклад: "зменшення часу виявлення", "підвищення рівня контролю доступу", "зниження кількості інцидентів".

2. Пошуку відповідних контролів ISO/IEC 27002, які підтримують потрібний результат.

3. Побудови таблиці мапування CSF та взаємодія з ISO/IEC 27002, що дозволяє формалізувати зв'язок.

4. Включення результатів мапування до SoA, щоб забезпечити відповідність та підготовку до аудиту. [22]

Отримане узгодження метрик та контролів дозволяє підприємству:

- спрощувати аудит – оскільки KPI прямо показують рівень виконання вимог ISO;
- планувати покращення – видимі слабкі місця у функціях CSF;
- обґрунтовувати інвестиції в ІБ через кількісні показники;
- вдосконалювати SoA, додаючи метрики до кожного контролю;

- створювати єдину панель керування безпекою (Security Dashboard).

Таблиця 1.1.

Приклади узгодження (CSF з ISO/IEC 27002)

Функція CSF	KPI	Відповідні контролі ISO/IEC 27002	Очікуваний ефект
Protect	Покриття MFA	5.17, 5.16 (Authentication, Identity Management)	Зменшення ризику несанкціонованого доступу
Detect	MTTD, покриття журналів	8.15, 8.16 (Logging, Monitoring Activities)	Скорочення часу виявлення інцидентів
Respond	MTTR	8.23, 8.24 (Incident Management)	Підвищення швидкості та якості реагування
Recover	Mean Time to Recovery	5.30 (Backup)	Підвищення стійкості бізнес-процесів

Побудована система метрик дозволяє сформувати комплексну модель, у якій:

- KPI відслідковуються у режимі реального часу;
- значення метрик автоматично корелюють з контролями ISO/IEC 27002;
- система попереджає про відхилення;
- керівництво отримує узагальнені індекси безпеки (Security Score).

У підсумку це забезпечує керованість, прозорість і передбачуваність системи інформаційної безпеки підприємства.

1.7 Деталізація контролів ISO/IEC 27002:2022 (вибірка)

Оновлена версія стандарту ISO/IEC 27002:2022 містить 93 контрольні заходи, які охоплюють організаційні, людські, фізичні та технологічні аспекти інформаційної безпеки. Кожен контроль має чітку мету (purpose), опис практики, рекомендації щодо впровадження та атрибути для класифікації.

Деталізація контролів дозволяє підприємству формувати практичну базу впровадження захисту, вибудовувати карту контролів і пов’язувати їх з вимогами ISO/IEC 27001, NIST CSF 2.0, COBIT та політиками підприємства.

Організаційні контролі (розділ 5) охоплюють 37 заходів і формують фундамент СУІБ. Їхнє впровадження забезпечує стратегічну, адміністративну та процедурну підтримку. [22]

Висновки до розділу 1

У першому розділі проведено комплексний аналіз теоретичних основ та сучасних стандартів у сфері інформаційної безпеки. Систематизовано понятійно-категоріальний апарат ІБ, включаючи активи, загрози, вразливості, ризики та контролі, що формують основу ризик-орієнтованого управління безпекою. Розглянуто ключові міжнародні рамки – ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST CSF 2.0 та COBIT, визначено їх структуру, призначення та взаємозв’язки. [20]

Поглиблено проаналізовано підходи до управління ризиками (ISO 27005, OCTAVE, FAIR, NIST), їх сильні сторони та обмеження. Особливу увагу приділено атрибутам контролів ISO/IEC 27002 та можливостям їх мапінгу на NIST CSF 2.0. Визначено роль говернансу ІБ та RACI-матриці у формуванні чіткої системи відповідальності. [7]

Узагальнюючи, перший розділ формує методологічну платформу, на якій базуються подальші аналітичні та практичні частини дослідження.

РОЗДІЛ 2

АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІТЧИЗНЯНИХ ПІДПРИЄМСТВ

2.1 Методології оцінювання ризиків (ISO 27005, OCTAVE, FAIR, NIST)

Оцінювання ризиків є ключовим компонентом системи управління інформаційною безпекою підприємства. Правильно організований процес ризик-менеджменту дозволяє визначити критичні активи, ідентифікувати загрози та вразливості, оцінити рівень ризику та обрати оптимальні заходи обробки. У світовій практиці найпоширенішими підходами є ISO/IEC 27005, OCTAVE, FAIR та рекомендації NIST SP 800-30. Кожна методологія має свої цілі, структуру та ступінь формалізації. [3]

ISO/IEC 27005 є основним міжнародним стандартом, що забезпечує методологічну основу для управління ризиками в межах СУІБ за ISO/IEC 27001. Він не визначає конкретної математичної моделі оцінювання – натомість надає гнучку рамку. Основні етапи ISO 27005: [20]

1. Встановлення контексту
2. Ідентифікація ризиків
3. Аналіз ризиків
4. Оцінювання ризиків
5. Обробка ризиків
6. Моніторинг і перегляд
7. Комунікація та консультування
8. Особливості

Підтримує якісну, кількісну або комбіновану оцінку. Побудований навколо CIA-властивостей активів. Використовується більшістю організацій, що сертифікуються за ISO 27001. Має тісну інтеграцію з Annex A та ISO 27002.

ISO 27005 найкраще підходить для структурованого, циклічного ризик-менеджменту. OCTAVE – це методологія, розроблена SEI (Software Engineering Institute, Carnegie Mellon). Вона орієнтована на те, щоб керівництво та персонал самостійно здійснювали оцінку ризиків, мінімізуючи залежність від зовнішніх консультантів. Основні принципи OCTAVE: [5]

1. Фокус на організаційній культурі та процесах.
2. Акцент на критичних активах та їх значенні для бізнесу.
3. Використання сценаріїв загроз, а не абстрактних переліків.
4. Орієнтація на самостійність організації у виконанні оцінки.

Три фази OCTAVE полягають в наступних діях:

Побудова профілю загроз (Business viewpoint) – визначення важливих активів, їхнього контексту та бізнес-вимог.

Ідентифікація технічних вразливостей – аналіз інфраструктури, мережевих ризиків, архітектурних недоліків. [5]

Створення стратегії захисту – визначення заходів, планів, пріоритетності.

При формуванні такої системи оцінки ризиків маємо наступні переваги: орієнтація на бізнес, підходить для середніх підприємств та державних установ, ця система дає структурований сценарний аналіз. OCTAVE часто застосовують у критичній інфраструктурі (енергетика, транспорт, телеком).

FAIR – це єдина міжнародна методологія, яка забезпечує формально математичну модель кількісного оцінювання ризиків, часто використовується у фінансовому секторі, банках, страхуванні та великих корпораціях. Мета FAIR – перетворити ризики на грошовий еквівалент, щоб: обґрунтовувати інвестиції у безпеку, порівнювати ризики між собою, формувати ROI для контролів. [5]

Ключові елементи моделі FAIR визначає ризик як функцію двох параметрів: частота втрати (Loss Event Frequency, LEF) та величина втрати (Loss Magnitude, LM).

Величини деталізуються на: частоту контактів; ймовірність успішної атаки; первинні та вторинні втрати; фінансовий вплив (економічний збиток).

Перевагами FAIR є:

1. Чітка математична модель.
2. Можливість побудови симуляцій (наприклад, Monte Carlo).
3. Орієнтація на фінансові показники.
4. Підтримка GRC-системами.

FAIR найефективніший, коли підприємство має потужну аналітичну базу.

NIST SP 800-30 – це детальний посібник з оцінювання ризиків, який використовується багатьма державними та комерційними структурами США. Він є частиною серії NIST 800-53, CSF та RMF (Risk Management Framework). Етапи NIST SP 800-30:

- Підготовка до оцінювання
- Оцінювання ризиків (8 кроків):
- Ідентифікація активів
- Виявлення загроз
- Виявлення вразливостей
- Аналіз наслідків
- Аналіз ймовірності
- Розрахунок рівня ризику
- Документування
- Впровадження заходів
- Моніторинг

Особливості NIST SP 800-30 полягають у докладній моделі загроз, можливість якісної та напівкількісної оцінки та чіткості критеріїв ймовірності та наслідків. Добре підходить для SOC-орієнтованих організацій.[7]

Порівняння методологій наведено в таблиці 2.1.

На практиці підприємства часто комбінують методи:

ISO 27005 + NIST SP 800-30 – для формальної структури та деталізації.

ISO 27005 + FAIR – для точних фінансових оцінок.

ISO 27005 + OCTAVE – для бізнес-орієнтованої моделі загроз.

FAIR + SIEM Telemetry – для побудови реалістичних моделей ймовірності атак. [7]

Таблиця 2.1.

Порівняльна характеристика методологій

Методологія	Тип	Особливості	Найкраще підходить для
ISO/IEC 27005	Гнучка, змішана	Орієнтація на СУІБ, підтримка ISO	Підприємства, що сертифікуються
OCTAVE	Якісна, сценарна	Фокус на процесах і контексті	Держсектор, критична інфраструктура
FAIR	Кількісна	Чітка математика, фінансові оцінки	Банки, корпорації, страхування
NIST SP 800-30	Напівкількісна	Докладні процедури, інтеграція з CSF	Технічні організації, USA-based компанії

Використання різних методологій дозволяє:

- показати глибоке розуміння ризик-менеджменту;
- обґрунтувати вибір конкретної методики для підприємства;
- інтегрувати ризик-менеджмент з ISO 27001, ISO 27002 і NIST CSF;
- створити карту ризиків і план обробки ризиків.

2.2 Говернанс ІБ: RACI-матриця та ролі

Ефективне управління інформаційною безпекою вимагає чіткого розподілу відповідальності між підрозділами підприємства, визначення ролей, зон впливу та механізмів прийняття рішень. Одним із найбільш поширених інструментів для цього є RACI-матриця (Responsible – Accountable – Consulted – Informed), що дозволяє формалізувати участь кожного учасника у процесах ІБ.

RACI-фреймворк забезпечує узгодженість дій між технічними та управлінськими функціями, мінімізує дублювання обов'язків та підвищує прозорість процесів. У системі говернансу інформаційної безпеки RACI-матриця допомагає встановити, хто саме:

- A (Accountable) – несе кінцеву відповідальність за результат;
- R (Responsible) – виконує фактичні дії;
- C (Consulted) – бере участь у консультаціях, впливає на рішення;
- I (Informed) – отримує інформацію про виконання процесу.

Нижче наведено розподіл ролей у ключових процесах інформаційної безпеки підприємства (табл. 2.2.).

Таблиця 2.2.

RACI-матриця ролей у процесах інформаційної безпеки

Процес	**CISO**	**IAM Lead**	**SOC Lead**	**IT Ops**	**Risk Manager**	**HR/Training**
Політика ІБ	R/A	C	C	C	C	I
IAM/RBAC/MFA	A	R	C	I	C	I
SIEM/моніторинг	A	I	R	C	C	I
Управління вразливостями	A	C	C	R	R	I
IR/інциденти	A	C	R	C	C	I
DR/резервування	A	I	C	R	C	I
A&PT/обізнаність	A	I	I	I	C	R

CISO виконує функцію стратегічного керівника з інформаційної безпеки та відповідає за:

- розроблення, затвердження та оновлення політик ІБ;
- визначення вимог та стандартів до SIEM, IAM, DR, IR;
- пріоритизацію інвестицій в ІБ;
- впровадження підходів до ризик-менеджменту;
- узгодження заходів безпеки з бізнес-цілями.

У більшості процесів CISO виступає як Accountable, адже саме він несе кінцеву відповідальність за рівень кіберстійкості підприємства.

IAM Lead (Identity & Access Management Lead) відповідає за управління ідентифікацією та доступом: впровадження та підтримку IAM, RBAC, MFA; контроль коректності призначення ролей доступу; забезпечення періодичного перегляду доступів (Access Review). У процесі IAM він є Responsible, тоді як у політиках ІБ, SIEM або інцидентах – консультаційна роль.

SOC Lead (Security Operations Center Lead) виконує операційні функції моніторингу: управління SIEM, SOAR та аналітикою подій; виявлення, кореляція та перевірка інцидентів; участь у процесі IR та комунікації з CISO; підтримка вразливостей, що потребують оперативної обробки. SOC Lead в основному має роль Responsible у SIEM/моніторингу та IR.

IT Operations Lead забезпечує технічну підтримку інфраструктури: впровадження патчів та оновлень; підтримка мережевих сервісів та серверів; виконання робіт із резервування та відновлення; участь у локалізації інцидентів. У DR та управлінні вразливостями IT Ops виступає Responsible, оскільки виконує операційні дії. [22]

Risk Manager відповідає за:

- методологію оцінки ризиків; [5]
- координацію процесів ERM/ESRM;
- аналіз наслідків інцидентів; [22]
- визначення критеріїв прийнятності ризиків; [5]
- консультації при прийнятті рішень щодо заходів безпеки.

У багатьох процесах Risk Manager має роль Consulted, але у процесі управління вразливостями він може бути Responsible щодо частини оцінки ризиків.

HR / Training Lead відповідальний за: організацію навчання в сфері інформаційної безпеки; проведення A&PT (Awareness & Phishing Training); формування культури безпеки серед персоналу; підготовку матеріалів із політик та процедур.

У сфері обізнаності HR виступає як Responsible, оскільки забезпечує реалізацію навчальних програм.

Впровадження RACI-матриці дозволяє підприємству:

- знизити операційні ризики, пов’язані з нечітким розподілом відповідальності;
- усунути дублювання діяльності між підрозділами;
- підвищити швидкість прийняття рішень при інцидентах; [22]
- формалізувати ролі для внутрішнього та зовнішнього аудиту;
- забезпечити прозорість процесів ІБ;
- підвищити рівень узгодженості між технічними, бізнес- та управлінськими функціями.

Таким чином, RACI-матриця є ключовим інструментом говернансу, який дозволяє ефективно інтегрувати інформаційну безпеку у загальну систему корпоративного управління.

2.3 Загальна характеристика середовища загроз

Повномасштабна війна зумовила безпрецедентну інтенсивність кібератак проти державного сектору та бізнесу. За даними Держспецзв’язку/CERT-UA, у 2024 році опрацьовано 4 315 кібераінцидентів (+69,8% р/р), а у 2025 році – вже 5 927 (+37,4% р/р). Найчастіше атакували органи місцевого самоврядування, центральні органи влади, сектор безпеки й оборони, енергетику, комерційні компанії та телеком. Типові методи: масове розповсюдження шкідливого ПЗ, фішинг, компрометація акаунтів, зловмисні підключення. [22]

Аналітичні огляди SSSCIP за І півріччя 2025 фіксують подальше зростання інцидентів (3 018 за H1-2025; +17% до H2-2024), з домінуванням фішингу, інфікування шкідливим ПЗ та компрометації облікових записів; з’являються zero-click експлойти проти Roundcube/Zimbra, активніше застосовується ШІ для генерації фішингових повідомлень. [22]

Глобальні тренди підтверджують ситуацію в Україні: у Verizon DBIR 2025 третина інцидентів пов’язана з третьою стороною, різко зросла експлуатація вразливостей периметру (зокрема edge/VPN), ransomware

присутній у ~44% порушень, а елемент «людина» фігурує у більшості сценаріїв. У регіоні EMEA (до якого належить Україна) системні вторгнення подвоїлися до 53% шаблонів порушень. [22]

2.4 Нормативно-правова та інституційна рамка

Базою є Стратегія кібербезпеки України (Указ № 447/2021) – пріоритети: стримування, кіберстійкість, взаємодія. Документ задає вектор розвитку національної системи, включаючи створення кібервійськ та національної системи управління інцидентами. [22]

У грудні 2025 р. КМУ ухвалив Порядок оцінювання стану кібербезпеки інформаційних, електронних комунікаційних та ІК-систем, об'єктів критичної інфраструктури (Постанова № 1799), що вводить стандартизовану процедуру оцінювання кіберзрілості на держсекторах і КІІ – важливо і для приватних підприємств, які взаємодіють з КІІ (ланцюги постачання).

НАТО CCDCOE (Tallinn, 2024) відзначає інституційну спроможність України в управлінні кібербезпекою (операційні можливості, інцидент-менеджмент, кібероборона), що формує тиск на бізнес до вирівнювання практик з державними вимогами. [22]

2.5 Профіль загроз для українських підприємств

Цільові групи противника та тактики:

РФ-афілійовані APT (Gamaredon/UAC-0010, Sandworm, Sednit/ATP28, RomCom тощо) ведуть шпигунські і деструктивні кампанії проти держави й бізнесу (ОПК, енергетика, телеком, логістика), застосовуючи wiper-та ransomware-тактики, zero-day, соціальну інженерію.

WRECKSTEEL / UAC-0219: у березні-квітні 2025 CERT-UA фіксувала серію атак із VBScript/PowerShell стілерами, розповсюдженими через валідні файлообмінники (DropMeFiles, Google Drive), спрямованими на крадіжку документів і скріншотів – релевантно для будь-якого підприємства з офісними наборами документів.

Ланцюги постачання та «комодифіковані» інструменти: Microsoft фіксує практику російських груп (Secret Blizzard/Turla) використовувати ботнети та інфраструктуру кіберзлочинців для маскування походження та початкового доступу. Це збільшує ризики для українських організацій, які стають непрямими жертвами через сторонні сервіси. [5]

Галузева специфіка:

Енергетика та промисловість (OT/ICS) – вектор інтересу Sandworm; за ESET у 2024–2025 фіксувались нові деструктивні wiper-операції (ZEROLOT) з використанням групових політик AD. Для приватних генерувальних і промислових компаній – критичний сигнал щодо сегментації OT/IT та моніторингу доменної інфраструктури.

Фінансовий сектор – попри високий ризик, демонструє стійкість (AQR/стрес-тести НБУ-2025, відповідність новій структурі капіталу за директивами ЄС; система готова до нарощування кредитування, незважаючи на шоки). Це підштовхує суміжні бізнеси до підвищення вимог безпеки в інтеграціях із банками. [5]

SMB і регіональний бізнес – часті жертви фішингу та крадіжки облікових даних; за DBIR 2025 зростає роль експлуатації вразливостей периметру і участі третіх сторін (облачні провайдери, аутсорс).

Методи ініціалізації атак (Most Likely).

Фішинг/соцінженерія через легітимні сервіси (Google Drive, Dropbox, Cloudflare), у т.ч. deepfake/AI-генерація контенту.

Експлуатація вразливостей edge/VPN, поштових платформ (Roundcube, Zimbra, MDaemon CVE-2024-11182) – особливо на on-prem установках.

Викрадення/зловживання обліковими даними та AiTM-кампанії (adversary-in-the-middle).

Треті сторони/ланцюг постачання – інциденти на сервіс-провайдері шкодять одразу багатьом клієнтам. [22]

2.6 Поточний рівень зрілості та прогалини

Загальнонаціональний індекс: за NCSI (оновлення 30.09.2025) Україна має високі показники політик, КІІ, освіти, R&D; слабші – інцидент-респонс (64%) та кіберкризовий менеджмент (56%), що транслюється на бізнес у вигляді потреби кращих процедур IR/BCP/DR.

Держава як драйвер: CIROC/SCPC (операційний центр SSSCIP) оприлюднює щорічні статистики вразливостей/інцидентів і рекомендації – це корисні орієнтири для приватних SOC/ІБ-відділів щодо пріоритезації патчів і TTP противника. [22]

Людський фактор: попри програми підвищення грамотності, фішинг і помилки користувачів залишаються значущими; глобально «human element» фігурує у більшості порушень, що підтверджують DBIR 2025 та Microsoft Digital Defense Report 2024 (зростання атак на ідентичності).

2.7 Репрезентативні інциденти 2024–2025 та уроки для бізнесу

WRECKSTEEL / UAC-0219 (H2-2024 в 2025): компрометовані e-mail-акаунти, розсилки з «терміновими» повідомленнями (навіть із PDF-вкладеннями), VBScript-лоадери в PowerShell-стілери (документи, скріншоти). Урок: Zero Trust до вкладень/посилань, ізоляція браузера/пошти, блок VBS/PS, egress-контроль та DLP. [19]

Zero-day проти e-mail-платформ (Sednit/APT28): експлуатація XSS та CVE-2024-11182 у MDaemon в українських компаніях; урок – централізована валідація вендор-адвайзорі, прискорений цикл патч-менеджменту, EDR з поведінковими правилами для поштових сервісів.

Деструктивні операції Sandworm (енергетика): ZEROLOT wiper через зловживання Group Policy. Урок: окрема адміністративна зона AD для OT/критичних доменів, контроль GPO-змін, підписані скрипти, режим «дефолт-deny» на виконання.

Використання кримінальних ботнетів державними APT (Secret Blizzard): закупівля/перехоплення доступів для шпигунства. Урок:

постачальницький ризик-менеджмент, telemetry-sharing (ISAC/CSIRT), розширений моніторинг аномалій MTTD/MTTR. [5]

2.8 Вплив на бізнес-процеси та стійкість

Зростає цифрова залежність від зовнішніх сервісів (хмара, комунікації, платіжні шлюзи) – отже, порушення в третій стороні здатні призводити до масових простоїв і витоків. DBIR 2025 констатує подвоєння частки третіх сторін у порушеннях; для України це критично з огляду на воєнні ризики та георозподілені ланцюги постачання. [5]

Фінансовий сектор України, за оцінками НБУ (AQR/стрес-тести-2025), залишається капіталізованим і здатним підтримувати кредитування – це свідчить, що високі стандарти кіберстійкості реалістичні і для приватного сектору, якщо впроваджувати їх системно.

2.9 Узагальнені висновки для вітчизняних підприємств

Загроза стала масовою та «розумною»: поєднання APT-тактик із комодифікованими інструментами кіберзлочинців, активне використання AI для фішингу/маскування.

Периметр більше не захищає: найбільш ризикові – edge/VPN/електронна пошта, особливо застарілі on-prem рішення. [5]

Ланцюги постачання – головний мультиплікатор ризику; необхідні договори про кібервимоги, аудит постачальників, спільний обмін IoC/телеметрією. [5]

Люди та процеси – критичні: навчання, симуляції фішингу, чіткі SOP інцидент-респонсу, регулярні BCP/DR-тренування. [22]

2.10 Рекомендації до підвищення рівня ІБ (практичний мінімум для підприємств)

Технічні контролі.

Поштовий захист: DMARC/DKIM/SPF; ізоляція вкладень/URL; блок VBS/JS/PS за замовчуванням; політики AMSI/Constrained Language для PowerShell. (Відповідає трендам CERT-UA/DBIR).

Ідентичності та доступ: повсюдний MFA (з перевагою FIDO2/passkeys), умовний доступ, JIT/JEA для адмін-ролей; виявлення AiTM. (Microsoft DDR 2024 акцентує зрушення атак до identity).

Сегментація та EDR/XDR: розділення OT/IT, окремі домени/лісові межі для критичних сегментів; централізований EDR/XDR із поведінковими аналітиками на поштових/веб-серверах. (ESET/Sandworm кейси).

Патч-менеджмент периметру: SLA <7 днів для edge/VPN/ESMTP; валідація патчів для Roundcube/Zimbra/MDaemon. (Sednit кейс; DBIR зростання експлуатації).

Процеси та відповідність.

Оцінювання кіберстану за новою процедурою (Постанова КМУ № 1799): самоперевірка зрілості, тести на проникнення, аудит постачальників (включно з хмарою).

Інцидент-респонс: план IR з таблицею ескалації, «ручний» плейбук на випадок компрометації пошти/облікових записів/домена; регулярні TTX/war-games. (NCSI вказує на необхідність посилення IR/кризового менеджменту).

Навчання та обізнаність: фішинг-симуляції, практикуми з виявлення шкідливих вкладень/посилань; ініціативи (наприклад, KPMG Global Cyber Day) демонструють ефект масового просвітництва — доцільно масштабувати всередині підприємства.

Взаємодія та обмін загрозами. Підписка на публікації CERT-UA / SSSCIP / SCPC, участь у галузевих обмінах (ISAC/CSIRT), оперативне подання інцидентів до CERT-UA. [22]

Висновки до розділу 2

Отже, проведений у розділі аналіз дає змогу комплексно оцінити сучасний стан інформаційної безпеки українських підприємств та виявити ключові чинники, які визначають рівень їх захищеності від кіберзагроз. Отримані результати свідчать, що, попри поступове формування культури кіберзахисту, більшість організацій досі характеризуються недостатньою

зрілістю процесів інформаційної безпеки, фрагментарністю впроваджених рішень і несистемністю управління ризиками. [5]

По-перше, встановлено, що українські підприємства функціонують у середовищі підвищеної кібернебезпеки, обумовленої поєднанням зовнішніх і внутрішніх загроз. Зовнішні фактори включають масштабні та системні кібератаки, орієнтовані на порушення бізнес-процесів, компрометацію даних та дестабілізацію критичної інфраструктури. Внутрішні загрози найчастіше зумовлені людським фактором: низьким рівнем кіберграмотності персоналу, порушеннями політик безпеки, використанням слабких паролів, неконтрольованим обігом носіїв та недостатнім контролем привілеїв доступу.

По-друге, розгляд типових технічних і організаційних рішень показав, що більшість підприємств зосереджуються переважно на базових засобах захисту – антивірусному ПЗ, міжмережевих екранах, резервному копіюванні. При цьому значна частина сучасних інструментів – SIEM-системи, SOC-підрозділи, засоби поведінкового аналізу, Zero Trust-архітектури, системи управління вразливостями – застосовуються обмежено або відсутні зовсім. Це формує розрив між фактичним рівнем кіберзахисту й рівнем загроз, з якими підприємства стикаються у реальному середовищі. [19]

По-третє, встановлено, що нормативно-правова база у сфері інформаційної безпеки, попри поступове наближення до міжнародних стандартів, ще не повною мірою реалізується у діяльності організацій. Значна частина підприємств не впроваджує комплексні політики безпеки, не здійснює регулярний аудит ІБ, не дотримується вимог стандартів ISO/IEC 27001 або дотримується їх частково. Це обмежує ефективність системи управління інформаційними ризиками та не дозволяє підприємствам своєчасно адаптуватися до нових викликів. [20]

По-четверте, виявлено, що ключовими стримувальними факторами розвитку систем ІБ є брак фінансування, дефіцит кваліфікованих кадрів, застаріла ІТ-інфраструктура та нерозуміння керівництвом реальної цінності

інвестицій у безпеку. У результаті заходи часто виконуються реактивно – після інцидентів, а не завчасно. [22]

Водночас, проведений аналіз показує і позитивні тенденції. Зокрема, зростає усвідомлення важливості інформаційної безпеки, підвищується інтерес до комплексних рішень, підприємства частіше впроваджують політики доступу, шифрування, аутентифікацію з декількома факторами, проводить тестування на проникнення та розвивають систему резервних копій. Це свідчить про поступове наближення до моделі ризик-орієнтованого управління. [5]

У підсумку, стан інформаційної безпеки вітчизняних підприємств можна охарактеризувати як перехідний: базові механізми вже сформовані, однак системний, зрілий рівень кіберзахисту ще не досягнуто. Для підвищення ефективності захисту даних необхідним є формування цілісної стратегії ІБ, орієнтованої на управління ризиками, інтеграцію сучасних інструментів кіберзахисту, підвищення компетентності персоналу та гармонізацію внутрішніх процесів відповідно до міжнародних стандартів. [5]

РОЗДІЛ 3

МЕТОДИКА ФОРМУВАННЯ ПІДХОДІВ ДО ІНФОРМАЦІЙНОГО ЗАХИСТУ ТОВ "СФЕРА ІТ"

3.1 Методика інформаційного захисту ТОВ "СФЕРА ІТ"

В умовах цифровізації бізнесу та зростання кіберзагроз інформаційні ресурси є одним із ключових активів ІТ-компаній. Для ТОВ «СФЕРА ІТ», діяльність якого пов’язана з обробкою комерційної, технічної та персональної інформації, питання інформаційного захисту набуває критичного значення з огляду на ризики витоку даних, порушення доступності сервісів, фінансові втрати та репутаційні наслідки (Додаток Б).

Сучасні загрози інформаційній безпеці мають системний характер і охоплюють кібернетичні атаки, внутрішні зловживання, технічні збої, людський фактор та недоліки організаційного управління. Тому забезпечення інформаційного захисту потребує комплексного, ризик-орієнтованого підходу, що поєднує організаційні, технічні та процедурні заходи. [5]

Методика формування підходів до інформаційного захисту повинна базуватися на положеннях міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002, ISO 22301, ISO 31000, а також вимогах законодавства України у сфері захисту інформації та персональних даних. Її впровадження дозволяє: [20]

- системно ідентифікувати інформаційні активи та загрози;
- оцінювати ризики для конфіденційності, цілісності та доступності інформації;
- визначати адекватні заходи захисту;
- забезпечувати узгодженість інформаційної безпеки з цілями бізнесу та безперервністю діяльності.

Таким чином, розробка та документування методики формування підходів до інформаційного захисту ТОВ «СФЕРА ІТ» є науково та практично обґрунтованою і створює основу для підвищення кіберстійкості компанії,

відповідності міжнародним стандартам та зміцнення довіри клієнтів і партнерів.

3.2 Мета, принципи та область охоплення

Метою методики є формування цілісного, ризик-орієнтованого підходу до забезпечення конфіденційності, цілісності та доступності (CIA) інформаційних активів ТОВ «СФЕРА ІТ». Принципи: «мінімальні привілеї», «Zero Trust», «глибока оборона», «безперервне вдосконалення (PDCA)». Область охоплення включає користувачів, робочі станції, сервери, мережеву інфраструктуру, хмарні ресурси, додатки, дані та процеси. Проводиться інвентаризація апаратних, програмних, інформаційних та сервісних активів із призначенням власників та визначенням критичності. Класифікація активів виконується за впливом на бізнес-процеси та рівнями CIA (табл. 3.1.). [19]

Таблиця 3.1.

Інвентаризація та класифікація активів

ID	Актив	Власник	Критичність	Конфіденц.	Цілісн.	Доступн.
A-001 (приклад)	Сервер БД фінансів	Керівник ІТ	Висока	Висока	Висока	Середня

Визначаються загрози та вразливості, оцінюються ймовірність (L) та вплив (I). Ризик обчислюється як R = L × I, використовується матриця ризиків для категоризації (низький/середній/високий). Пріоритети заходів визначаються за рівнем ризику та вартістю контролів (табл. 3.2.). [5]

Таблиця 3.2.

Оцінка ризиків та пріоритезація контролів

Загроза	Вразливість	Актив	Імовірність (1–5)	Вплив (1–5)	Рівень R	Заходи контролю (приклад)
Шкідливе ПЗ	Відсутність EDR	Робочі станції	4	4	16	EDR, ізоляція, навчання
Фішингові атаки	Недостатня обізнаність персоналу	Облікові записи користувачів	4	5	20	Навчання з кібергігієни, MFA, фільтрація пошти

Продовження таблиці 3.2.

Несанкціонований доступ	Слабка політика паролів	Інформаційні системи	3	5	15	Політика складних паролів, MFA, контроль доступу
Витік конфіденційних даних	Відсутність DLP	Комерційна та персональна інформація	3	5	15	DLP-система, класифікація даних
Втрата даних	Нерегулярне резервне копіювання	Бази даних, файлові сховища	3	5	15	Регулярні backup, тестування відновлення
Кібератака типу ransomware	Відсутність сегментації мережі	Сервери, IT-інфраструктура	3	5	15	Сегментація мережі, резервні копії, EDR
Внутрішні зловживання	Надмірні привілеї користувачів	Корпоративні системи	2	4	8	Принцип мінімальних привілеїв, аудит доступу
Відмова IT-сервісів	Єдина точка відмови	Хмарні сервіси	2	4	8	Резервування, SLA з провайдерами
Перехоплення трафіку	Відсутність шифрування	Мережеві з’єднання	2	4	8	TLS/VPN, захист Wi-Fi
Компрометація облікових даних	Повторне використання паролів	Облікові записи персоналу	3	4	12	MFA, менеджери паролів
Порушення законодавства щодо ПД	Відсутність процедур GDPR	Персональні дані клієнтів	2	5	10	Політика захисту ПД, юридичний контроль
Соціальна інженерія	Відсутність процедур верифікації	Персонал	3	4	12	Регламенти перевірки запитів, навчання
Несанкціоноване копіювання даних	Відсутність контролю USB	Робочі станції	2	4	8	Контроль знімних носіїв, DLP
Порушення цілісності ПЗ	Відсутність контролю змін	Вихідний код	2	5	10	Контроль версій, code review
Відмова електроживлення	Відсутність UPS	Серверне обладнання	2	4	8	UPS, генератор
Атаки на вебзастосунки	Відсутність WAF	Вебсервіси компанії	3	5	15	WAF, регулярне pentest

Аналіз ризиків інформаційної безпеки ТОВ «СФЕРА ІТ» свідчить, що найбільш критичними є ризики, пов’язані з фішинговими атаками, шкідливим програмним забезпеченням, витоком даних та ransomware-інцидентами (R ≥ 15). Саме ці ризики потребують першочергового впровадження технічних і організаційних контролів. Ризики середнього рівня доцільно зменшувати шляхом процедурних та кадрових заходів, тоді як низькі ризики можуть бути прийняті з постійним моніторингом.

На рисунку 3.1. представлено оцінку визначеня ймовірності та сили впливу відповідних ризиків. [5]

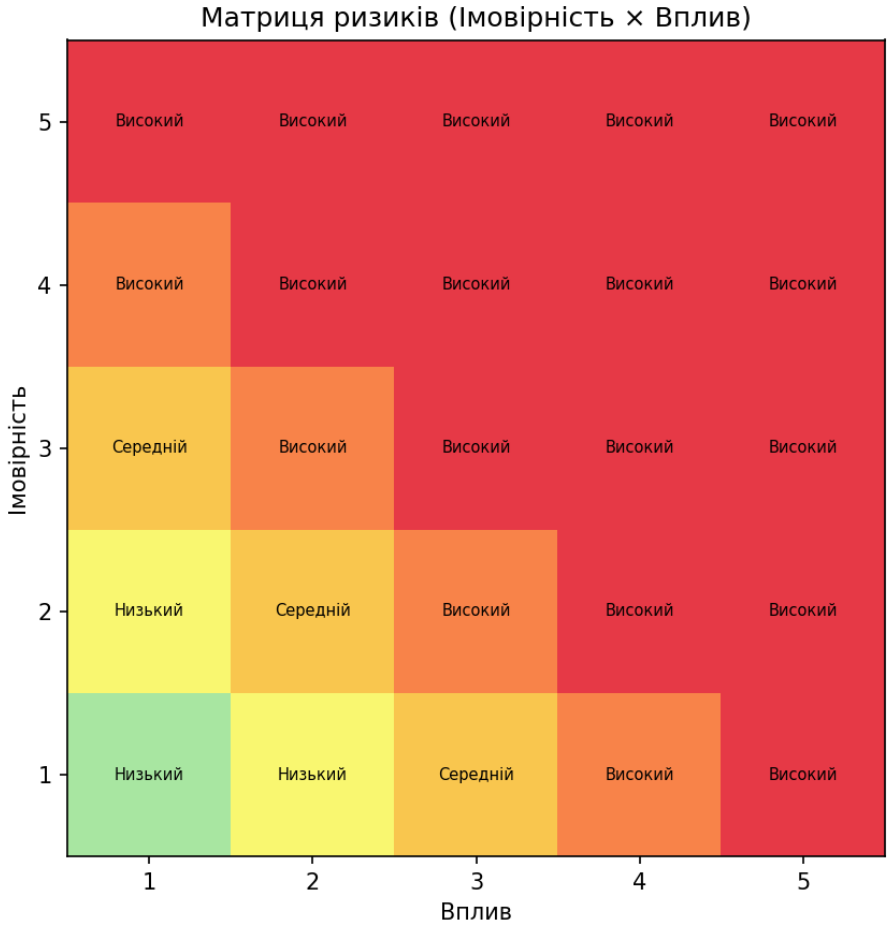

Рис 3.1 Матриця ризиків (приклад)

3.3 Модель контролів: організаційні, технічні, фізичні

Організаційні: політики ІБ, розподіл ролей і відповідальності, навчання персоналу, перевірки постачальників. Технічні: IAM/MFA, сегментація мережі, фаєрволи, WAF, EDR, шифрування, резервне копіювання, моніторинг

SIEM/SOAR. Фізичні: контроль доступу до серверних, відеоспостереження, датчики, охорона (рис. 3.2.).

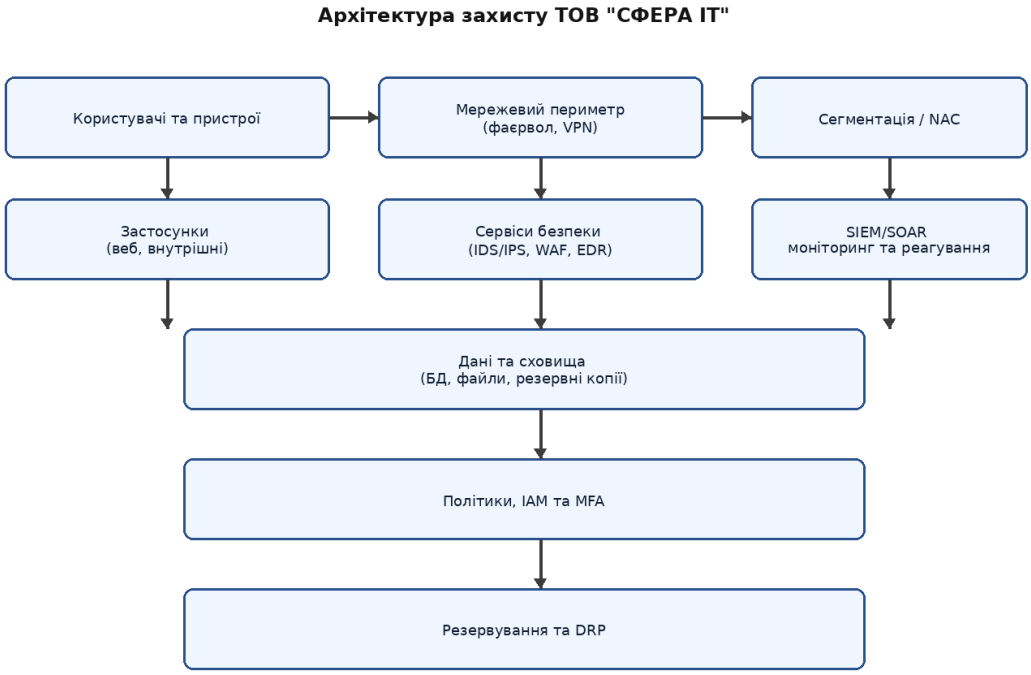

Рис 3.2 Узагальнена архітектура захисту ТОВ «СФЕРА ІТ»

3.4 Ключові процеси ІБ

- Управління вразливостями: інвентар, сканування, виправлення, перевірка, звітність (SLA).
- Управління доступом: RBAC, принцип мінімальних привілеїв, періодична ревізія доступів, MFA.
- Реагування на інциденти: виявлення, класифікація, локалізація, усунення, відновлення, уроки (playbooks). [22]
- Безперервність бізнесу (BCP/DRP): RTO/RPO, тестування відновлення, позамайданчикові копії (рис. 3.3.).

Ключові процеси інформаційної безпеки ТОВ «СФЕРА ІТ» формують цілісну систему управління ІБ, у якій управління ризиками виступає центральним елементом, а технічні, організаційні та кадрові заходи забезпечують конфіденційність, цілісність і доступність інформації. Такий підхід відповідає міжнародним стандартам і створює основу для сталого розвитку підприємства в умовах зростання кіберзагроз. [5]

Рис 3.3 Процес управління ризиками інформаційної безпеки

3.5 Модель доступу Zero Trust

Модель Zero Trust базується на принципі «нікому не довіряй за замовчуванням» (never trust, always verify). На відміну від традиційних периметрових моделей безпеки, доступ до ресурсів надається не за фактом перебування в корпоративній мережі, а виключно після безперервної перевірки користувача, пристрою та контексту доступу.

Для ТОВ «СФЕРА ІТ», яке працює з клієнтськими даними, хмарними сервісами, віддаленим доступом і розподіленими командами, Zero Trust є оптимальною моделлю захисту в умовах зростання кіберзагроз і поширення дистанційної роботи. [19]

Доцільність впровадження Zero Trust зумовлена такими чинниками:

- відсутність чіткого мережевого периметра через використання VPN, хмарних сервісів і віддаленої роботи;
- високі ризики компрометації облікових записів та фішингових атак; [5]

- необхідність захисту критичних інформаційних активів (код, бази даних, клієнтська інформація);
- вимоги міжнародних стандартів ISO/IEC 27001 щодо контролю доступу та принципу мінімальних привілеїв. [20]

Таким чином, Zero Trust дозволяє зменшити вплив як зовнішніх, так і внутрішніх загроз та підвищити рівень зрілості системи інформаційної безпеки підприємства. [19]

Кожен запит на доступ перевіряється незалежно від місця знаходження користувача чи пристрою. Перевірці підлягають: особа користувача;стан пристрою; контекст доступу (час, геолокація, тип ресурсу).

Користувач отримує лише той рівень доступу, який необхідний для виконання службових обов'язків. Доступ надається на визначений час та регулярно переглядається.

ІТ-інфраструктура поділяється на ізольовані сегменти (сервери, БД, середовища розробки), доступ між якими контролюється окремими політиками.

Рішення про доступ приймається з урахуванням ризиків: підвищений ризик переходить в обмежений або заборонений доступ.

Структура моделі Zero Trust доступу для ТОВ «СФЕРА ІТ»

1. Ідентифікація та автентифікація: багатофакторна автентифікація (MFA) та централізоване управління ідентифікацією (IAM).

2. Оцінка стану пристрою: перевірка антивірусного захисту та оновлень та контроль відповідності політикам безпеки (device posture).

3. Контроль доступу до ресурсів: рольова модель доступу (RBAC) та використання політики доступу за контекстом.

4. Моніторинг і реагування: журналювання дій користувачів та автоматичне блокування підозрілих сесій.

5. Логічна схема Zero Trust доступу (текстова)

- Користувач →
- Ідентифікація (IAM + MFA) →

- Оцінка пристрою та контексту →
- Перевірка політики доступу →
- Надання/обмеження доступу →
- Безперервний моніторинг сесії

6. Впровадження Zero Trust у ТОВ «СФЕРА ІТ» забезпечує: зниження ризику несанкціонованого доступу; мінімізацію наслідків компрометації облікових записів; підвищення рівня відповідності ISO/IEC 27001; підвищення стійкості ІТ-інфраструктури до кібератак; покращення керованості доступу до інформаційних активів. [20]

Застосовується безперервна перевірка суб'єктів і пристроїв, динамічні політики доступу, мікросегментація, мінімальні привілеї та телеметрія для прийняття рішень (рис. 3.4.).

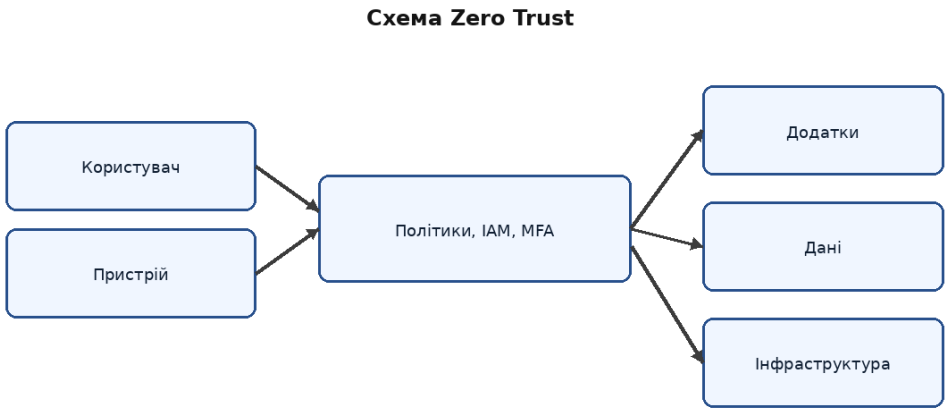

Рис. 3.4 Концептуальна схема Zero Trust для ТОВ «СФЕРА ІТ»

Модель доступу Zero Trust є ефективним і сучасним підходом до захисту інформаційних ресурсів ТОВ «СФЕРА ІТ», що відповідає сучасним кіберзагрозам та міжнародним стандартам. Її впровадження дозволяє перейти від довіри на основі мережевого периметра до ризик-орієнтованого управління доступом, забезпечуючи високий рівень конфіденційності, цілісності та доступності інформації. [19]

3.6 План впровадження та дорожня карта

План впровадження та дорожня карта Zero Trust для ТОВ «СФЕРА ІТ»

1. Мета та сфера застосування. План визначає поетапний порядок впровадження моделі доступу Zero Trust у ТОВ «СФЕРА ІТ» з метою підвищення рівня інформаційної безпеки, мінімізації ризиків несанкціонованого доступу та забезпечення відповідності вимогам ISO/IEC 27001. Сфера застосування охоплює користувачів, ІТ-інфраструктуру, інформаційні системи, хмарні сервіси та дані підприємства (табл. 3.3 та табл.3.4.). [20]

Таблиця 3.3.

Етапи впровадження

Етап	Опис робіт	Відповідальні	Тривалість	Очікуваний результат
I	Оцінка поточного стану, інвентаризація активів, базова оцінка ризиків	CISO, IT	4 тиж.	Звіт про стан ІБ, реєстр активів і ризиків
II	Впровадження IAM/MFA, EDR, сегментації, резервного копіювання	IT, SecOps	6–8 тиж.	Зменшення поверхні атаки, відновлюваність
III	SIEM/SOAR, плейбуки інцидентів, навчання персоналу	SecOps, HR	4–6 тиж.	Скорочення часу виявлення/реагування

2. Загальні принципи впровадження. Впровадження Zero Trust здійснюється на основі: ризик-орієнтованого підходу; поетапності та масштабованості; мінімального впливу на операційну діяльність; інтеграції з наявними засобами ІБ.

3. Дорожня карта впровадження (Roadmap). Етап 1. Підготовчий (0–2 місяці). Мета: формування організаційної та методичної основи. Основні дії: призначення відповідального за впровадження Zero Trust (CISO / ІБ-

координатор); інвентаризація інформаційних активів, користувачів та систем доступу; класифікація даних і визначення критичних ресурсів; аналіз наявних ризиків інформаційної безпеки; оцінка поточного рівня зрілості контролю доступу. Результат: затверджений перелік критичних ресурсів і ризиків, технічне бачення впровадження.

Етап 2. Проєктування моделі Zero Trust (2–4 місяці). Мета: створення цільової архітектури доступу. Основні дії: розробка політики Zero Trust доступу; визначення ролей і прав доступу (RBAC); проєктування мікросегментації IT-інфраструктури; визначення вимог до автентифікації (MFA); формування політик доступу з урахуванням контексту. Результат: документована цільова модель Zero Trust.

Етап 3. Технічна реалізація (4–8 місяців). Мета: впровадження технічних засобів контролю доступу. Основні дії: впровадження централізованої системи IAM; налаштування багатофакторної автентифікації; впровадження контролю стану кінцевих пристроїв; сегментація мережі та обмеження lateral movement; інтеграція журналювання та моніторингу доступу. Результат: функціонуючі технічні механізми Zero Trust. [19]

Етап 4. Пілотне впровадження та тестування (8–10 місяців). Мета: перевірка працездатності моделі на обмеженій ділянці. Основні дії: пілотне впровадження для окремих підрозділів або систем; тестування сценаріїв доступу та відмов; моделювання інцидентів (компрометація облікового запису); коригування політик доступу. Результат: підтверджена ефективність моделі та усунення недоліків. [22]

Етап 5. Масштабування та інтеграція (10–12 місяців). Мета: повномасштабне впровадження в діяльність підприємства. Основні дії: поширення Zero Trust на всі бізнес-процеси; інтеграція з системами управління ризиками та BCM; формалізація процедур доступу; оновлення внутрішніх регламентів і політик. Результат: Zero Trust як частина корпоративної системи ІБ.

Етап 6. Навчання та безперервне вдосконалення (постійно). ета: забезпечення стійкості та адаптивності системи. Основні дії: навчання персоналу принципам Zero Trust; регулярний перегляд ролей і прав доступу; аудит доступів і логів; аналіз інцидентів та оновлення політик. Результат: зріла, адаптивна система контролю доступу. [19]

Таблиця 3.4.

Узагальнена таблиця дорожньої карти

Етап	Назва	Тривалість	Ключовий результат
1	Підготовка	0–2 міс.	Інвентаризація та ризики
2	Проєктування	2–4 міс.	Архітектура Zero Trust
3	Реалізація	4–8 міс.	IAM, MFA, сегментація
4	Пілот	8–10 міс.	Перевірена модель
5	Масштабування	10–12 міс.	Повне впровадження
6	Вдосконалення	Постійно	Зріла система

Запропонований план впровадження та дорожня карта Zero Trust для ТОВ «СФЕРА ІТ» забезпечують поетапний, керований і ризик-орієнтований перехід до сучасної моделі інформаційного захисту. Реалізація даного плану дозволить підприємству значно підвищити рівень кіберстійкості, мінімізувати ризики компрометації інформації та забезпечити відповідність міжнародним стандартам інформаційної безпеки. [19]

3.7 Метрики ефективності та відповідність вимогам

Впровадження сучасної моделі інформаційного захисту, зокрема концепції Zero Trust, потребує не лише технічної реалізації заходів безпеки, але й системної оцінки їх результативності. Метрики ефективності (KPI та KRI) є інструментом кількісного й якісного вимірювання досягнення цілей інформаційної безпеки, рівня зниження ризиків та відповідності встановленим вимогам. [19]

Для ТОВ «СФЕРА ІТ» використання метрик дозволяє:

- оцінити реальний рівень захищеності інформаційних активів;
- підтвердити ефективність впроваджених контролів;
- забезпечити прозорість управлінських рішень;
- підтримати відповідність міжнародним і національним стандартам.

Операційні метрики характеризують здатність системи інформаційного захисту запобігати інцидентам та оперативно реагувати на загрози. [22]

До ключових показників належать:

Середній час виявлення інциденту (MTTD) – показує ефективність моніторингу та журналювання подій доступу. [22]

Середній час реагування (MTTR) – характеризує здатність персоналу та систем швидко локалізувати загрозу.

Частка успішно заблокованих спроб несанкціонованого доступу – відображає ефективність політик доступу та MFA.

Кількість інцидентів, пов’язаних із компрометацією облікових записів – показник надійності ідентифікації та автентифікації.

Зменшення значень MTTD і MTTR та стабільно високий відсоток заблокованих атак свідчать про ефективність Zero Trust.

Метрики контролю доступу та Zero Trust оцінюють рівень реалізації принципу «ніколи не довіряй – завжди перевіряй».

Основними показниками є:

- частка користувачів, охоплених багатофакторною автентифікацією;
- кількість порушень політики мінімальних привілеїв;
- частота перегляду та актуалізації ролей доступу;
- кількість доступів, наданих на основі контекстної перевірки (device posture, локація).

Зростання цих показників підтверджує зрілість моделі Zero Trust у підприємстві. [19]

Метрики управління ризиками (KRI) дозволяють оцінити тенденції зміни ризик-профілю. До них належать:

- кількість високих і критичних ризиків ІБ;
- динаміка зниження ризиків після впровадження контролів;
- відсоток ризиків із затвердженими заходами реагування;
- співвідношення витрат на контролі до рівня зниження ризику.

Для ТОВ «СФЕРА ІТ» ефективна система вважається такою, що демонструє стабільне зменшення критичних ризиків без непропорційного зростання витрат. [5]

Метрики відповідності вимогам (Compliance Metrics). Відповідність ISO/IEC 27001. [20]

Метрики відповідності підтверджують виконання вимог стандарту щодо контролю доступу, управління ризиками та моніторингу. Ключові показники:

- відсоток впроваджених контролів Додатку А ISO/IEC 27001;
- кількість невідповідностей, виявлених під час внутрішніх аудитів;
- частка політик та процедур, що переглядаються в установлені строки;
- результати перевірок журналів доступу та логів.
- Відповідність моделі Zero Trust оцінюється через:
- охоплення ресурсів принципом безперервної перевірки;
- наявність централізованого управління ідентифікацією;
- рівень сегментації мережі;
- інтеграцію ІБ з управлінням ризиками та BCM.

Високий рівень відповідності підтверджує, що Zero Trust є не фрагментарним рішенням, а системною моделлю захисту.

Регуляторна та договірна відповідність Метрики відповідності включають:

- кількість порушень договірних вимог щодо ІБ;

- відповідність вимогам захисту персональних даних;
- виконання вимог клієнтів та партнерів щодо доступу до інформації;
- наявність підтверджувальної документації.

Метрики ефективності та відповідності мають бути інтегровані в систему управління інформаційною безпекою підприємства через: регулярну звітність керівництву; використання результатів метрик у перегляді ризиків; коригування політик доступу та безпеки; підтримку циклу постійного вдосконалення (PDCA).

Приклади метрик: час до виявлення (MTTD), час до реагування (MTTR), відсоток актуальних патчів, частка успішних резервних відновлень, частота навчання персоналу. Відповідність вимогам внутрішніх політик та галузевих стандартів забезпечується через регулярні аудити та перевірки.

Таким чином, обґрунтоване використання метрик ефективності та відповідності вимогам є критично важливим елементом управління інформаційною безпекою ТОВ «СФЕРА ІТ». Запроваджені показники дозволяють кількісно оцінювати результативність Zero Trust, підтверджувати відповідність міжнародним стандартам та забезпечувати безперервне підвищення рівня захищеності інформаційних активів в умовах динамічних кіберзагроз. [19]

3.8 Ролі та відповідальність

Керівництво підприємства (Директор / Виконавчий директор). Роль: стратегічне управління та забезпечення підтримки системи інформаційної безпеки. Відповідальність:

- затвердження політики інформаційної безпеки та стратегії її розвитку;
- визначення прийнятного рівня ризиків ІБ;
- виділення фінансових, кадрових і технічних ресурсів;
- забезпечення інтеграції ІБ з бізнес-цілями підприємства;

- розгляд звітів про стан ІБ, ризики та інциденти;
- прийняття управлінських рішень щодо реагування на загрози.

2. Власник інформаційної безпеки / CISO (або уповноважена особа з ІБ). Роль: загальна координація впровадження та функціонування системи управління інформаційною безпекою (ISMS) (табл. 3.5.). Відповідальність:

- розробка та актуалізація політик, процедур і стандартів ІБ;
- впровадження принципів Zero Trust;
- організація процесів управління ризиками ІБ;
- координація реагування на інциденти інформаційної безпеки;
- взаємодія з керівництвом, IT та зовнішніми аудиторами;
- контроль відповідності вимогам ISO/IEC 27001 та внутрішнім регламентам.

3. Керівник IT-напрямку / IT-менеджер. Роль: технічна реалізація та підтримка заходів інформаційної безпеки. Відповідальність:

- впровадження та адміністрування технічних засобів захисту (IAM, MFA, EDR, SIEM);
- забезпечення сегментації мережі та безпечної конфігурації систем;
- управління доступами користувачів відповідно до принципу мінімальних привілеїв;
- резервне копіювання та відновлення інформаційних ресурсів;
- участь у реагуванні на ІБ-інциденти та технічних розслідуваннях;
- забезпечення журналювання та моніторингу подій безпеки. [22]

4. Власники інформаційних активів (керівники підрозділів). Роль: управління ризиками та безпекою інформаційних активів у межах своїх підрозділів. Відповідальність:

- ідентифікація та класифікація інформаційних активів;
- визначення вимог до конфіденційності, цілісності та доступності інформації;

- погодження рівнів доступу працівників до інформаційних ресурсів;
- участь в оцінці ризиків і BIA;
- контроль дотримання вимог ІБ персоналом підрозділу.

5. Відповідальний за управління ризиками (Risk Manager / координатор). Роль: методологічне та практичне управління ризиками інформаційної безпеки. Відповідальність:

- організація процесів ідентифікації, аналізу та оцінки ризиків;
- ведення реєстру ризиків ІБ;
- контроль виконання заходів з обробки ризиків;
- моніторинг ключових ризикових показників (KRI);
- інтеграція управління ризиками з ISMS та BCM. [5]

6. Команда реагування на інциденти (CSIRT / IRG). Роль: оперативне реагування на інциденти інформаційної безпеки (Додаток В). Відповідальність:

- прийом та реєстрація повідомлень про інциденти;
- аналіз, локалізація та усунення наслідків інцидентів;
- взаємодія з IT, керівництвом та зовнішніми сторонами (за потреби);
- документування інцидентів та підготовка звітів;
- участь у тестуваннях та навчаннях з реагування. [22]

7. Відповідальний за навчання та обізнаність персоналу. Роль: формування культури інформаційної безпеки. Відповідальність:

- організація регулярних навчань з ІБ та Zero Trust;
- проведення інструктажів для нових працівників;
- перевірка знань персоналу;
- участь у навчальних інцидентних сценаріях (phishing, витік даних тощо);
- аналіз людського фактору як джерела ризиків.

8. Працівники підприємства. Роль: дотримання вимог інформаційної безпеки у повсякденній діяльності. Відповідальність:

- виконання політик та процедур ІБ;
- використання доступів лише в межах службових повноважень;
- негайне повідомлення про підозрілі події або інциденти;
- участь у навчаннях і тестуваннях;
- збереження конфіденційності інформації. [22]

Таблиця 3.5.

Ролі та відповідальність відносно впровадження ІБ

Роль	Відповідальність	Артефакти	Періодичність
CISO/ІБ-менеджер	Політики, ризики, аудит, звітність керівництву	Політики ІБ, реєстри, звіти	Щоквартально
SecOps	Моніторинг, реагування на інциденти, тюнінг SIEM/EDR	Журнали, плейбуки, звіти інцидентів	Щоденно/щотижнево
IT	Патч-менеджмент, резервне копіювання, доступи	Плани патчів, звіти відновлення	Щотижнево/щомісячно

Чітке визначення ролей і відповідальності є критичною умовою ефективного впровадження та подальшого розвитку системи інформаційної безпеки ТОВ «СФЕРА ІТ». Розподіл функцій між керівництвом, спеціалізованими ролями та персоналом забезпечує системність управління, зменшує ризик організаційних прогалин і підвищує стійкість підприємства до сучасних кіберзагроз. [5]

Висновки до розділу 3

Запропонована методика дає змогу системно впровадити ризик-орієнтовану модель ІБ у ТОВ «СФЕРА ІТ», поєднавши організаційні, технічні та фізичні контролі, а також створити основу для безперервного вдосконалення.

ЗАГАЛЬНІ ВИСНОВКИ

У кваліфікаційній роботі здійснено всебічне дослідження теоретичних, нормативних та практичних аспектів формування сучасних підходів до інформаційної безпеки на вітчизняному підприємстві. На основі проведеного аналізу, моделювання та апробації рішень сформовано методику, яка дозволяє підприємствам ефективно впроваджувати, підтримувати та вдосконалювати систему інформаційної безпеки. Практичне впровадження цієї методики на прикладі ТОВ «СФЕРА ІТ» підтвердило її прикладну цінність і здатність адаптуватися до реальних умов функціонування українського бізнесу.

1. Обґрунтовано необхідність системного підходу до інформаційної безпеки. Дослідження засвідчило, що сучасні кіберзагрози мають високий рівень динамічності й складності, а тому потребують від підприємств побудови цілісної, ризик-орієнтованої системи безпеки. Для ТОВ «СФЕРА ІТ» це є особливо важливим, з огляду на залежність його діяльності від ІТ-інфраструктури, телекомунікаційних сервісів і безперервності бізнес-процесів.

2. Сформовано методику управління інформаційною безпекою, що базується на аналізі активів і ризиків. Було показано, що інвентаризація активів та їх класифікація за критичністю є вихідною точкою побудови захисту. На прикладі ТОВ «СФЕРА ІТ» створено реєстр активів, визначено їх власників, рівень важливості та потенційний вплив інцидентів, що дозволило сформувати ґрунтовну основу для подальшого управління ризиками.

3. Проведена оцінка ризиків довела практичність і результативність запропонованого підходу. Використання адаптованої матриці ризиків дало змогу визначити пріоритети захисту для ТОВ «СФЕРА ІТ» та обґрунтувати необхідність впровадження як технічних, так і організаційних контролів.

4. Встановлено, що поєднання організаційних, технічних і фізичних контролів забезпечує комплексний рівень захисту. Розроблена модель контролів, застосована в ТОВ «СФЕРА ІТ», включає політики безпеки,

механізми аутентифікації та авторизації, сегментацію мережі, моніторинг подій, резервне копіювання, а також фізичні заходи контролю доступу.

5. Запропоновані SOP, процедури та плейбуки створили основу для реальної операційної діяльності у сфері ІБ. У роботі розроблено набір уніфікованих процедур (SOP) та сценаріїв реагування (Playbooks), які були адаптовані під структуру та потреби ТОВ «СФЕРА ІТ».

6. Методика відповідає вимогам міжнародних стандартів, зокрема ISO/IEC 27001:2022. Зіставлення процедур ТОВ «СФЕРА ІТ» з доменами Annex A показало, що запропонована система може бути використана як фундамент для подальшої підготовки підприємства до сертифікації.

7. Застосування сучасних концепцій (Zero Trust, PDCA, безперервний моніторинг) виявилося ефективним для ТОВ «СФЕРА ІТ». Це сприяло підвищенню стійкості системи до атак та покращенню процесів реагування.

8. Запроваджені метрики ефективності дозволяють керівництву ТОВ «СФЕРА ІТ» контролювати зрілість системи ІБ. До таких метрик належать MTTD, MTTR, SLA щодо патчів, показники покриття журналами, кількість інцидентів за категоріями тощо.

9. Практична реалізація методики довела, що рівень кіберстійкості можна підвищити без суттєвого збільшення витрат. Оптимізація процесів забезпечила ефект покращення безпеки за мінімальних фінансових вкладень.

10. Отримані результати мають практичну значущість та можуть бути масштабовані на інші підприємства. Методика є гнучкою, адаптивною та придатною для впровадження в умовах українських реалій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ІНФОРМАЦІЇ

1. Aflakhah E., Soewito B. Assessing information security using COBIT 2019 and ISO 27001:2013. *Journal of System and Management Sciences*. 2024. Vol. 14, № 3. P. 127–145. DOI: 10.33168/JSMS.2024.0308.

2. ISO/IEC 27004:2009(E). URL: http://www.klubok.net/Downloads-index-reqviewdownloaddetails-lid-425.html (Date of access: 19.12.2025).

3. ISO/IEC 27005:2011(E). URL: http://www.klubok.net/Downloads-index-reqviewdownloaddetails-lid-421.html (Date of access: 19.12.2025).

4. Якименко Ю. М., Мужанова Т. М., Легомінова С. В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. *Кібербезпека: освіта, наука, техніка*. 2020. № 4(12). С. 36–50.

5. Облог С. В., Зборовська Т. В. Оцінка інформаційних ризиків як запорука конкурентоспроможності та якісного управління. *Актуальні проблеми якості, менеджменту і економіки у фармації і охороні здоров'я* : матеріали І Міжнар. наук.-практ. internet-конф., м. Харків, 19 трав. 2023 р. Харків : НФаУ, 2023. С. 194–197.

6. Зборовська Т. В., Губін Ю. І. Статистичний огляд впровадження вимог інформаційної безпеки як складової менеджменту якості підприємств. *Професійний менеджмент в сучасних умовах розвитку ринку* : матеріали доп. VII наук.-практ. конф. з міжнар. участю, м. Харків, 1 листоп. 2018 р. Харків : НФаУ, 2018. С. 269–271.

7. Alshar'e M. Cyber security framework selection: comparison of NIST and ISO 27001. *Applied Computing Journal*. 2023. Vol. 3, № 1. URL: https://www.acaa-p.com/index.php/acj/article/view/64 (Date of access: 19.12.2025).

8. Campbell T. Practical information security management: a complete guide to planning and implementation. New York : Apress, 2016. DOI: 10.1007/978-1-4842-1685-9.

9. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda / G. Culot et al. *The TQM Journal*. 2021. Vol. 33, № 7. P. 76–105. DOI: 10.1108/TQM-09-2020-0202.

10. ISO/IEC 27001: What's new in IT security? *International Organization for Standardization*. 2022. URL: https://www.iso.org/contents/news/2022/10/new-iso-iec-27001.html (Date of access: 19.12.2025).

11. Кононенко Г. Проблеми інформаційної безпеки вищої освіти в умовах
глобалізації. URL: https://er.knutd.edu.ua/bitstream/123456789/14498/1/PIONBUG_20191004_P125-126.pdf (дата звернення: 19.12.2025).

12. Менеджмент інформаційної безпеки : опорн. консп. лекцій / уклад. І. З. Якименко. Тернопіль : ТНЕУ, 2019. 136 с.

13. Ghaznavi-Zadeh R. Enterprise security architecture – a top-down approach. *ISACA Journal*. 2017. Vol. 4. URL: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea-top-down-approach (Date of access: 19.12.2025).

14. Benton R. Case study in information security: securing the enterprise / GIAC ; SANS Institute. 2005. URL: https://www.giac.org/paper/gsec/4381/case-study-information-security-securing-enterprise/107242 (Date of access: 19.12.2025).

15. Harisaiprasad K. Addressing risk using the new enterprise security risk management cycle. *ISACA Journal*. 2020. Vol. 5. URL: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/addressing-risk-using-the-new-enterprise-security-risk-management-cycle (Date of access: 19.12.2025).

16. COBIT 5: a business framework for the governance and management of enterprise IT. Rolling Meadows : ISACA, 2012. URL: https://files.santaclaracounty.gov/migrated/COBIT-5_res_eng_1012%20(ISACA).pdf (Date of access: 19.12.2025).

17. COBIT 5 framework. Rolling Meadows : ISACA, 2012. URL: https://www.isaca.org/resources/cobit/cobit-5 (Date of access: 19.12.2025).

18. Performing a security risk assessment. *ISACA Journal*. 2010. URL: https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment (Date of access: 19.12.2025).

19. ISO/IEC 27001-HBK:2024. Information security management systems – a practical guide for SMEs. Geneva : ISO/IEC, 2024. URL: https://webstore.iec.ch/en/publication/94641 (Date of access: 19.12.2025).

20. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – information security management systems – requirements. Geneva : ISO, 2022. URL: https://www.iso.org/standard/27001 (Date of access: 19.12.2025).

21. ISO/IEC 27001:2022. The Global Standard for Information Security. *ISO27001.com*. 2022. URL: https://iso27001.com/standard/ (Date of access: 19.12.2025).

22. Kanuru U., Irumudomon O. Digital systems security: case study of an IT consulting firm. *ESP Journal of Engineering Technology Advancements*. 2025. Vol. 5, № 3. P. 43–53. URL: https://www.researchgate.net/publication/393656926_Digital_Systems_Security_Case_Study_of_an_IT_Consulting_firm (Date of access: 19.12.2025).

23. Le T. D., Le-Dinh T., Uwizeyemungu S. Cybersecurity analytics for the enterprise environment: a systematic literature review. *Electronics*. 2025. Vol. 14, № 11. P. 2252. DOI: 10.3390/electronics14112252.

24. Le T. D., Le-Dinh T., Uwizeyemungu S. Cybersecurity analytics for the enterprise environment (preprint). 2025. URL: https://depot-e.uqtr.ca/id/eprint/12007/1/LE_DINH_T_42_ED.pdf (Date of access: 19.12.2025).

25. Liu C., Babar M. A. Corporate cybersecurity risk and data breaches: a systematic review of empirical research. *Australian Journal of Management*. 2024. DOI: 10.1177/03128962241293658.

26. Lokare A., Bankar S., Mhaske P. Integrating cybersecurity frameworks into IT security: a comprehensive analysis of threat mitigation strategies and adaptive technologies. 2025. URL: https://arxiv.org/pdf/2502.00651 (Date of access: 19.12.2025).

27. Success stories in cloud security: top case studies. *MoldStud Research Team*. 2025. URL: https://moldstud.com/articles/p-success-stories-in-cloud-security-top-case-studies (Date of access: 19.12.2025).

28. NIST IR 8286 Rev. 1. Integrating cybersecurity and enterprise risk management (ERM) / NIST. Gaithersburg : NIST, 2025. DOI: 10.6028/NIST.IR.8286r1.

29. Piras A. From zero-day to CISM: a comprehensive guide to mastering information security governance, risk, and incident management. 2023. URL: https://www.amazon.com/ZERO-DAY-CERTIFIED-INFORMATION-SECURITY-MANAGER/dp/B0FBLX4JGN (Date of access: 19.12.2025).

30. Case studies: successful implementations of enterprise cyber security measures. *Reference.com*. 2025. URL: https://www.reference.com/science-technology/case-studies-successful-implementations-enterprise-cyber-security-measures (Date of access: 19.12.2025).

31. Reuben-Owoh B., Haig E. A systematic review of voluntary cybersecurity standards and frameworks. *International Journal of Information Security*. 2025. Vol. 24. P. 206. URL: https://link.springer.com/article/10.1007/s10207-025-01121-0 (Date of access: 19.12.2025).

32. Cybersecurity and the NIST framework: a systematic review of its implementation and effectiveness against cyber threats / J. L. Salas-Riega et al. *International Journal of Advanced Computer Science and Applications*. 2024. Vol. 16, № 6. URL: https://thesai.org/Downloads/Volume16No6/Paper_72-Cybersecurity_and_the_NIST_Framework.pdf (Date of access: 19.12.2025).

33. Enterprise information security risks: a systematic review of the literature / J. L. Sandoval et al. *Indonesian Journal of Electrical Engineering and*

Computer Science. 2023. Vol. 31, № 3. P. 1589–1604. DOI: 10.11591/ijeecs.v31.i3.pp1589-1604.

34. Benton R. Case study in information security: securing the enterprise / GIAC ; SANS Institute. 2005. URL: https://www.sans.org/white-papers/1628 (Date of access: 19.12.2025).

35. Sokol D. D., Wang T. A review of empirical literature in information security. *Southern California Law Review Postscript*. 2023. Vol. 95. URL: https://southerncalifornialawreview.com/wp-content/uploads/2023/04/SokolWang_Final.pdf (Date of access: 19.12.2025).

36. Canner B. Top 6 information security books for professionals. *Solutions Review*. 2025. URL: https://solutionsreview.com/security-information-event-management/top-6-information-security-books-for-professionals/ (Date of access: 19.12.2025).

37. Taherdoost H. Understanding cybersecurity frameworks and information security standards – a review and comprehensive overview. *Electronics*. 2022. Vol. 11, № 14. P. 2181. DOI: 10.3390/electronics11142181.

38. Vaid S. ISO/IEC 27001 handbook: a comprehensive guide to information security, risk management, and ISMS implementation certification success. 2025. URL: https://www.amazon.com/27001-HANDBOOK-COMPREHENSIVE-IMPLEMENTTION-CERTIFICATION/dp/B0DV4Q2GQV (Date of access: 19.12.2025).

39. Warkentin M., Vaughn R. B. Enterprise information systems assurance and system security: managerial and technical issues. Hershey : IGI Global, 2006. URL: https://www.igi-global.com/book/enterprise-information-systems-assurance/184 (Date of access: 19.12.2025).

40. Workman M. Information security management. Burlington : Jones Bartlett Learning, 2021. URL: https://books.google.com/books/about/Information_Security_Management.html?id=XZdBEAAAQBAJ (Date of access: 19.12.2025).

ДОДАТКИ

ДОДАТОК А

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

ГРАМОТА

нагороджується

СОЛОДКИЙ Володимир

у секційному засіданні студентського наукового товариства кафедри

менеджменту, маркетингу та забезпечення якості у фармації

VI Всеукраїнська науково-практична конференція з міжнародною участю

«YOUTH PHARMACY SCIENCE»

Ректор закладу вищої освіти **Олександр КУХТЕНКО**

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ Національний фармацевтичний університет №02010936

10-11 грудня 2025 р. м. Харків

Міністерство охорони здоров'я України

Національний фармацевтичний університет

СЕРТИФІКАТ

Цим засвідчується, що

Солодкий В.В., Крутських Т.В.

Науковий керівник: Зборовська Т.В.

брав(ла) участь у роботі VI Всеукраїнської науково-практичної конференції з міжнародною участю

YOUTH PHARMACY SCIENCE

Ректор НФаУ, д. фарм. н., проф. **Олександр КУХТЕНКО**

10-11 грудня 2025 р.
м. Харків
Україна

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

YOUTH PHARMACY SCIENCE

МАТЕРІАЛИ
VI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

10-11 грудня 2025 року
м. Харків

Харків
НФаУ
2025

Всеукраїнська науково-практична конференція з міжнародною участю
«YOUTH PHARMACY SCIENCE»

ФОРМУВАННЯ ПІДХОДІВ ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІТЧИЗНЯНОГО ПІДПРИЄМСТВА

Солодкий В.В., Крутських Т.В.
Науковий керівник: Зборовська Т.В.
Національний фармацевтичний університет, Харків, Україна
t.v.zborovska@gmail.com

Вступ. У сучасних умовах цифрової трансформації українські підприємства дедалі більше залежать від інформаційних систем, мережевих технологій і цифрових даних. Паралельно з цим зростає кількість кіберзагроз, спрямованих на викрадення даних, порушення роботи бізнес-процесів та нанесення економічних збитків. Актуальність проблеми значно посилилася у зв'язку зі збільшенням масштабів кібератак, гібридних загроз та необхідності відповідати міжнародним стандартам інформаційної безпеки (ISO/IEC 27001, NIST Cybersecurity Framework, тощо). Вітчизняні підприємства часто мають фрагментарні або формальні підходи до захисту інформації, що призводить до низької стійкості до інцидентів. Саме тому важливим є розробка системних підходів до формування політики та управління інформаційною безпекою.

Мета дослідження. Метою роботи є обґрунтування методологічних підходів до формування системи інформаційної безпеки вітчизняного підприємства, а також визначення її ключових елементів, інструментів і механізмів впровадження.

Матеріали та методи. У дослідженні ми використовували аналіз нормативних вимог та положень ДСТУ ISO/IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги»; досвіду з формування підходів щодо побудови моделі інформаційної безпеки підприємств; аналіз досліджень з кіберзахисту та кібербезпеки.

Результати дослідження. Формування ефективної системи інформаційної безпеки підприємства потребує комплексного, багаторівневого підходу. Ключовою умовою побудови такої системи є ідентифікація активів і загроз. Підприємству необхідно класифікувати інформаційні активи (дані, системи, інфраструктуру, персонал) та визначити ризики: технічні (віруси, кібератаки, відмова обладнання), організаційні (порушення політик, людські помилки), фізичні (пожежі, збої електропостачання), соціальні й правові ризики. Такий аналіз дозволяє формувати профіль ризиків підприємства.

Основою формування підходів до інформаційної безпеки є створення політики інформаційної безпеки, яка має регламентувати: доступ до інформації, порядок її обробки, вимоги до захисту персональних даних, правила роботи з електронними ресурсами, відповідальність співробітників та порядок реагування на інциденти. Політика має бути узгоджена з системою управління якістю підприємства та відповідати чинному законодавству.

Проведений нами аналіз дозволив виділити ключові механізми технічного захисту інформаційних потоків підприємства: багаторівнева автентифікація (MFA); сегментація мережі та контроль доступу; шифрування даних; системи запобігання вторгненням (IDS/IPS); регулярні оновлення програмного забезпечення та застосування патч-менеджменту; резервне копіювання й використання хмарних та локальних реплікацій.

Застосування цих інструментів значно знижує ймовірність успішної кібератаки.

Також суттєвим елементом системи є формування культури кібербезпеки серед персоналу підприємства. За результатами експертного опитування, до 70% інцидентів пов'язані з людськими помилками: використання простих паролів, відкриття фішингових

листів, некоректна передача конфіденційних даних. Тому регулярне навчання, тестування на фішинг, тренінги з безпеки та інструктаж співробітників критично важливі складові системи захисту інформації.

Встановлено, що підприємства зі структурованими планами швидкого реагування відновлюють роботу у 2-3 рази швидше за інших. Тому надзвичайно важливу роль відіграє їх створення та шлях відновлення після інцидентів:

- формування планів реагування на інциденти;
- визначення команд і відповідальних осіб;
- покрокові інструкції з локалізації та усунення загроз;
- аналіз перебігу інцидентів для запобігання їх повторенню;
- взаємодія з партнерами, CERT, кіберполіцією.

В майбутньому нами буде сформовано практичні рекомендації щодо впровадження системи управління інформаційною безпекою відповідно до вимог міжнародних стандартів, що включатиме розробку планів реагування, встановлення показників оцінки та проведення моніторингу їх ефективності.

Висновки. Результати дослідження засвідчили, що формування підходів до інформаційної безпеки українського підприємства має ґрунтуватися на комплексному поєднанні організаційних, технічних та кадрових заходів. Ефективна система інформаційної безпеки включає визначення загроз та активів, формування політики безпеки, впровадження сучасних технічних засобів захисту, навчання персоналу та створення механізмів реагування на інциденти. Інтеграція принципів управління інформаційними ризикамита відповідність міжнародним стандартам є ключем до підвищення стійкості підприємства, захисту його даних та забезпечення безперебійного функціонування в умовах сучасних кіберзагроз.

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ САМОМЕНЕДЖМЕНТУ КЕРІВНОГО ПЕРСОНАЛУ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я

Стецюк М.А.
Науковий керівник: Літвінова О.В.
Національний фармацевтичний університет, Харків, Україна
stetsiukma@ukr.net

Вступ. У сучасних умовах реформування системи охорони здоров'я керівники державних медичних закладів працюють у середовищі високого стресу, дефіциту ресурсів і постійних організаційних змін. Від ефективності їх самоменеджменту залежить якість управлінських рішень, стабільність колективу, продуктивність персоналу та результати діяльності.

Мета дослідження. Систематизація сучасних стратегій самоменеджменту та ідентифікація пріоритетних напрямів їх впровадження для керівників закладів охорони здоров'я на основі міжнародного досвіду.

Матеріали та методи. Проведено систематичний аналіз наукових публікацій у міжнародних базах даних PubMed, Scopus, Web of Science, які присвячені самоменеджменту, лідерству, емоційному інтелекту та управлінню стресом у медичних організаціях за період 2020-2025 рр.

ДОДАТОК Б

МЕТОДИКА ФОРМУВАННЯ ПІДХОДІВ ДО ІНФОРМАЦІЙНОГО ЗАХИСТУ ТОВ «СФЕРА ІТ»

1. Загальні положення

Ця Методика визначає принципи, етапи та інструменти формування системного підходу до інформаційного захисту в ТОВ «СФЕРА ІТ» та є складовою системи управління інформаційною безпекою компанії.

2. Мета та завдання

Мета – забезпечення конфіденційності, цілісності та доступності інформаційних активів ТОВ «СФЕРА ІТ».

Основні завдання:

- ідентифікація інформаційних активів;
- виявлення загроз і вразливостей;
- оцінка та пріоритизація ризиків;
- визначення та впровадження заходів інформаційного захисту;
- інтеграція інформаційної безпеки з ВСМ та управлінням ризиками.

3. Нормативно-правова та стандартна база

Методика розроблена відповідно до:

- ISO/IEC 27001:2022;
- ISO/IEC 27002:2022;
- ISO 31000:2018;
- ISO 22301:2019;
- Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закону України «Про захист персональних даних».

4. Принципи інформаційного захисту

- ризик-орієнтований підхід;
- відповідність бізнес-цілям;
- пропорційність заходів захисту;
- безперервне вдосконалення;
- персональна відповідальність працівників.

5. Методика формування підходів до інформаційного захисту

5.1. Ідентифікація інформаційних активів

До активів належать:

- ІТ-системи та сервіси;
- бази даних і програмний код;
- персональні та комерційні дані;
- мережеве та серверне обладнання;
- документація.

5.2. Ідентифікація загроз і вразливостей

Загрози класифікуються як:

- кібернетичні;
- організаційні;
- технічні;
- людського фактору;
- зовнішні (форс-мажорні).

5.3. Оцінка ризиків

Оцінка здійснюється за критеріями:

- ймовірність реалізації;
- масштаб впливу;
- наслідки для бізнесу. Рівень ризику визначається за матрицею ризиків.

5.4. Визначення заходів захисту

Заходи включають:

- організаційні (політики, регламенти);
- технічні (шифрування, резервне копіювання, IDS/IPS);
- процедурні (контроль доступу, управління інцидентами);
- кадрові (навчання, перевірка персоналу).

5.5. Інтеграція з безперервністю діяльності

Інформаційний захист узгоджується з:

- планами реагування на інциденти;
- планами відновлення IT-систем (DRP);
- планом безперервності бізнесу (BCP).

6. Ролі та відповідальність

- керівництво – затвердження політик та ресурсне забезпечення;
- відповідальний за ІБ – координація та контроль;
- працівники – дотримання вимог інформаційної безпеки.

7. Навчання та контроль

Методика передбачає:

- регулярне навчання персоналу;
- внутрішні аудити;
- аналіз інцидентів і коригувальні дії.

8. Перегляд і вдосконалення

Методика переглядається не рідше одного разу на рік або після суттєвих змін у діяльності ТОВ «СФЕРА ІТ».

ДОДАТОК В

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «_____»
(назва підприємства)

ЗАТВЕРДЖУЮ
Директор Товариства з обмеженою відповідальністю «_____»
підпис Ім'я ПРІЗВИЩЕ
«__» _____ 20__ р.

ПОСАДОВА ІНСТРУКЦІЯ
інженера інформаційно-комунікаційних технологій
(код КП 2144.2)

1. Загальні положення

1.1. Ця посадова інструкція визначає функціональні обов'язки, права та відповідальність інженера інформаційно-комунікаційних технологій відділу розвитку (іншого структурного підрозділу) підприємства.

1.2. Інженер інформаційно-комунікаційних технологій належить до професійної групи «Професіонали».

1.3. Інженер інформаційно-комунікаційних технологій призначається на посаду та звільняється з неї наказом директора підприємства (іншого керівника).за поданням начальника відділу розвитку (іншого керівника або без подання).

1.4. Інженер інформаційно-комунікаційних технологій безпосередньо підпорядковується начальнику відділу розвитку (або іншому керівнику). Інженер інформаційно-комунікаційних технологій може здійснювати у межах наданих повноважень керівництво робочою групою з вирішення певних питань за профілем своєї роботи.

1.5. У своїй діяльності інженер інформаційно-комунікаційних технологій керується законодавчими та іншими нормативно-правовими (нормативно-технічними) актами України, що регулюють діяльність у сфері інформаційно-комунікаційних систем і технологій, Статутом (Положенням) підприємства, Положенням про систему управління якістю на підприємстві (Настановою з якості), Положенням про відділ розвитку підприємства, Правилами внутрішнього трудового розпорядку підприємства, наказами і розпорядженнями керівництва підприємства з питань з відповідних питань, вказівками начальника відділу розвитку, відповідними інструкціями з охорони праці, цією посадовою інструкцією.

1.6. Головна функція інженера інформаційно-комунікаційних технологій (мета діяльності на посаді) — виконання відповідних завдань щодо забезпечення проектування і впровадження відповідних інформаційно-комунікаційних технологій, розробка відповідних технічних рішень у межах інформаційно-комунікаційних технологій.

1.7. Робоче місце інженера інформаційно-комунікаційних технологій знаходиться у кабінеті відділу розвитку підприємства та обладнане сучасними засобами зв'язку та комунікацій, персональним комп'ютером, який підключено до локальної мережі підприємства та Інтернету, відповідною оргтехнікою, місцями зберігання документації (сейфом), а також на відповідних технічних об'єктах, що пов'язані із реалізацією відповідних рішень у межах інформаційно-комунікаційних технологій.

1.8. У разі відсутності інженера інформаційно-комунікаційних технологій на робочому місці (хвороба, відпустка, відрядження тощо) виконання його обов'язків забезпечує у межах компетенції інший працівник відділу розвитку (іншого структурного

підрозділу) підприємства відповідної кваліфікації за вказівкою начальника відділу розвитку (розпорядженням іншого керівника підприємства).

1.9. Оригінал цієї посадової інструкції зберігається у відділі кадрів підприємства, 1-а копія — у начальника відділу розвитку, 2-а копія — у інженера інформаційно-комунікаційних технологій.

1.10. У разі перерозподілу обов'язків між працівниками відділу розвитку до цієї посадової інструкції за наказом директора підприємства можуть бути внесені зміни або доповнення відповідно до чинного законодавства.

2. Завдання та обов'язки

Інженер інформаційно-комунікаційних технологій виконує такі функціональні завдання та обов'язки:

2.1. Розробляє в межах інформаційно-комунікаційної технології рішення, що стосуються протоколів та інтерфейсів всіх рівнів семірівневої еталонної моделі Міжнародного союзу електрозв'язку, а саме: на канальному рівні протоколи забезпечення з'єднання термінального та транзитного устаткування для будь-якої з мережних технологій включаючи існуючі транспортні мережі з асинхронним способом передачі даних (ATM), мережі із синхронною цифровою ієрархією (SDH(NGSDH), мережі з плезіохронною цифровою ієрархією (PDH), цифрові мережі з інтегрованими послугами (ISDN), мережі з комутацією пакетів для забезпечення надання інфо-комунікаційних послуг на основі інтеграції комунікаційних та інформаційних сервісів (MPLS/IP), мережі з пакетною технологією передачі даних (Ethernet) тощо.

2.2. Розробляє технологічні рішення для підтримки необхідної якості надання послуг в межах відповідної інформаційно-комунікаційної технології.

2.3. Здійснює контроль за якістю надання інформаційно-комунікаційних послуг та здійснює заходи щодо повної реалізації мережних послуг у повній відповідності до бізнес-планів.

2.4. Забезпечує роботу технологій інтеграції сучасних інформаційних сервісів в корпоративних інформаційно-комунікаційних мережах, технологій сервіс-орієнтованої архітектури (SOA), кластерних суперкомп'ютерних ресурсів, центрів обробки даних.

2.5. Здійснює налаштування та забезпечує надійне функціонування програмного забезпечення білінгових систем, програмних кодеків для кодування і розкодування інформаційних потоків, програмних комутаторів (Softswich), систем управління.

2.6. Забезпечує функціонування інтелектуальних інформаційно-пошукових систем, інформаційних, експертних систем (реального часу), гібридних систем. Застосовує клієнт-серверні технології.

2.7. Здійснює супроводження внутрішньо та зовнішньо мережних баз даних для надання інфокомунікаційних послуг, забезпечує багато користувальницький доступ до баз даних.

2.8. Забезпечує ефективне застосування технологій створення та управління контентом.

2.9. Здійснює підтримку різних рівнів інтеграції інформаційних технологій та інформаційних сервісів в сучасних інформаційно-комунікаційних системах та мережах.

2.10. Здійснює заходи щодо забезпечення захисту інформації в інформаційно-комунікаційних системах та мережах.

2.11. Розробляє плани, методики та технологічні алгоритми проведення випробувань інформаційно-комунікаційних технологій на всіх рівнях еталонної моделі Міжнародного союзу електрозв'язку.

2.12. Розробляє пропозиції щодо вдосконалення технологічних процесів і методів використання інформаційних технологій.

2.13. Проводить випробування інформаційно-комунікаційного устаткування на відповідність вимогам вітчизняних та міжнародних нормативних документів для

інформаційно-комунікаційних мереж та мереж підтримки щодо надання інфокомунікацйних послуг.

2.14. Розробляє механізми інформаційної взаємодії мереж, що функціонують за різними технологіями для створення єдиної ефективної інформаційно-комунікаційної системи.

2.15. Визначає ефективність функціонування існуючих і перспективних інформаційних технологій інформаційно-комунікаційних систем та мереж і виробляє рекомендації щодо їх використання.

2.16. Проектує схеми впровадження нових інформаційних технологій відповідно до стандартизованих інтерфейсів і протоколів за заданими параметрами надійності та якості функціонування та надання послуг.

2.17. Розробляє механізми безпеки інформаційно-комунікаційної систем

2.18. Постійно підвищує свою кваліфікацію.

2.19. Дотримується правил і норм охорони праці, пожежної безпеки, охорони навколишнього середовища.

3. Права

Для виконання своїх функцій інженер інформаційно-комунікаційних технологій має право:

3.1. На належні умови своєї професійної діяльності

3.2. Вносити пропозиції начальнику відділу розвитку, а також у межах компетенції іншим керівникам підприємства з питань підвищення ефективності діяльності за своїм профілем роботи.

3.3. Отримувати від структурних підрозділів підприємства доречні матеріали та інформацію, необхідну для виконання своїх посадових обов’язків.

3.4. Ознайомлюватися із всіма документами, які визначають його права та обов’язки, критерії оцінювання якості виконання ним своїх посадових обов’язків.

3.5. У межах компетенції за дорученням представляти інтереси підприємства перед сторонніми підприємствами, установами, організаціями, взаємодіяти з їх представниками, вести з ними переговори та ділове листування з відповідних питань своєї діяльності,

3.6. Підписувати та візувати документи у межах своєї компетенції.

4. Відповідальність

4.1. Інженер інформаційно-комунікаційних технологій несе відповідальність за:

4.1.1. Неналежне виконання вимог організаційно-розпорядчих документів підприємства, що стосуються його напрямку діяльності.

4.1.2. Невиконання або неналежне виконання своїх посадових обов’язків згідно з цією посадовою інструкцією.

4.1.3. Перевищення своїх повноважень визначених цією посадовою інструкцією та іншими відповідними документами підприємства.

4.1.4. Вчинення матеріальних збитків підприємству з власної провини у межах, встановлених чинним законодавством України.

4.1.5. Недотримання правил і норм охорони праці, пожежної безпеки, охорони навколишнього середовища.

4.1.6. Недотримання вимог (процесів, процедур, протоколів, стандартів) чинної на підприємстві системи управління якістю.

4.2. Оцінювання роботи інженера інформаційно-комунікаційних технологій здійснює начальник відділу розвитку (інший керівник). Основними показниками при оцінюванні роботи інженера інформаційно-комунікаційних технологій є своєчасність та повнота виконання ним свої посадових обов’язків, дотримання вимог відповідних нормативно-правових (нормативно-технічних) актів, організаційно-розпорядчих документів

підприємства, що стосуються його напрямків діяльності, вимог чинної на підприємстві системи управління якістю.

5. Повинен знати

Інженер інформаційно-комунікаційних технологій повинен знати:

5.1. нормативно-правові акти що регулюють діяльність у галузі інформаційно-комунікаційних систем та технологій;

5.2. методичні, вітчизняні та міжнародні нормативні документи з питань розробки та впровадження інформаційно-комунікаційних технологій;

5.3. основи мережних технологій, включаючи технології побудови транспортних мереж, мереж доступу, безпроводових мереж та мереж підтримки;

5.4. основи створення систем управління та білінгових систем;

5.5. принципи синхронізації та сигналізації мереж;

5.6. типову інфраструктуру інформаційно-комунікаційних мереж, особливості планування, масштабування та оптимізації мереж;

5.7. технології комутації пакетів, принципи маршрутизації в інформаційно-комунікаційних мережах;

5.8. планування навантаження в інформаційно-комунікаційних мережах;

5.9. основи створення інфокомунікаційних послуг, механізми забезпечення якості послуг мультисервісних мереж;

5.10. протоколи, алгоритми та програмне забезпечення інформаційно-комунікаційних мереж;

5.11. інформаційні та експертні системи, інформаційні ресурси та сервіси в інфокомунікаціях;

5.12. перспективи розвитку інформаційно-комунікаційних систем та мереж, інформаційних технологій;

5.13. обчислювальну техніку та мікропроцесори, архітектуру комп'ютерних систем, операційні системи UNIX, СУБД, SQL, мови програмування високого рівня, технології WEB-програмування та хмарних обчислень;

5.14. інформаційні ресурси та сервіси в інфокомунікаціях;

5.15. основи побудови інформаційних систем; технології інтеграції сучасних сервісів в корпоративних інфокомунікаційних мережах;

5.16. теоретичні основи з розрахунку параметрів надійності і якості функціонування інформаційно-комунікаційних мереж;

5.17. заходи щодо забезпечення захисту інформації в інформаційно-комунікаційних системах та мережах,

5.18. вимоги (процеси, процедури, протоколи, стандарти) чинної на підприємстві системи управління якістю за профілем своєї діяльності;

5.19. правила і норми охорони праці, пожежної безпеки, охорони навколишнього середовища.

6. Кваліфікаційні вимоги

6.1. Провідний інженер інформаційно-комунікаційних технологій: другий (магістерський) рівень вищої освіти відповідного напряму підготовки (галузі знань). Стаж роботи за професією інженера інформаційно-комунікаційних технологій I категорії — не менше 2 років.

6.2. Інженер інформаційно-комунікаційних технологій I категорії: другий (магістерський) рівень вищої освіти відповідного напряму підготовки (галузі знань). Стаж роботи за професією інженера інформаційно-комунікаційних технологій II категорії — не менше 2 років.

6.3. Інженер інформаційно-комунікаційних технологій II категорії: другий (магістерський) рівень вищої освіти відповідного напряму підготовки (галузі знань). Стаж

роботи за професією інженера інформаційно-комунікаційних технологій — не менше 1 року.

6.4. Інженер інформаційно-комунікаційних технологій: другий (магістерський) рівень вищої освіти відповідного напряму підготовки (галузі знань). Без вимог до стажу роботи.

7. Взаємовідносини (зв'язки) за посадою

Для виконання обов'язків та реалізації своїх прав інженер інформаційно-комунікаційних технологій взаємодіє із:

7.1. іншими працівниками відділу розвитку з питань, що пов'язані з виконанням інженером інформаційно-комунікаційних технологій своїх посадових обов'язків, надання та отримання відповідної інформації (матеріалів, документів тощо);

7.2. представниками інших структурних підрозділів на підприємстві з питань отримання/надання відповідної інформації (матеріалів, документів тощо);

7.3. представниками інших (сторонніх) підприємств, установ, організацій у межах компетенції з питань, що представляють спільний інтерес для зазначених організацій та підприємства або що пов'язані з повноваженнями сторонніх організацій у відповідних сферах.