КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва випускної кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему:

Поєднання принципів побудови КСЗІ та імплементація норм європейських директив з кібербезпеки до національного законодавства

Боднар Владислав Романович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ
„ ___ " _____ 20 25 року

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Поєднання принципів побудови КСЗІ та імплементація норм європейських директив з кібербезпеки до національного законодавства
(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав (-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи.
Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Боднар Владислав Романович
(прізвище, ім'я та по батькові повністю)
125 «Кібербезпека та захист інформації»
(спеціальність)
Безпека інформаційних і комунікаційних систем
(освітня програма)
Група БІКСм-24
Керівник Шабала Є.Є.
(прізвище та ініціали)
Кандидат технічних наук, доцент
(вчене звання, науковий ступінь)
Рецензент _____
(прізвище та ініціали)

Ідентичність підтверджую

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: Автоматизації і інформаційних технологій
Кафедра: Кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти: Магістр
Спеціальність: 125 «Кібербезпека та захист інформації»
ОПП: Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри

к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ
„ ___ ” _____ 20 25 року

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА

СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Боднара Владислава Романовича

(прізвище, ім'я та по батькові здобувача)

1.Тема роботи «Поєднання принципів побудови КСЗІ та імплементація норм європейських директив з кібербезпеки до національного законодавства» затверджено наказом ректора КНУБА №1635/23.2/25 від « 30 » вересня 2025 ро

2. Керівник роботи к.т.н. Шабала Євгенія Євгенівна, доцент кафедри кібербезпеки та комп'ютерної інженерії

ізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3.Термін подання здобувачем роботи до захисту 15 грудня 2025 року.

4.Зміст пояснювальної записки за розділами:

Р.1. Теоретико-аналітичні засади дослідження

Р.2. Аналіз методів та методик дослідження

Р.3. Проєктні та практичні рішення

Р.4. Узагальнення результатів і прикладний аналіз

5.Графічний матеріал за розділами:

С. 2 Вступ

С. 3 Завдання

С. 4 Актуальність

С. 5 Комплекна система захисту інформації

С. 8. ISO 27001

С. 10 Порівняння стандартів

6. Консультанти розділів атестаційної випускної роботи

Розділ	Прізвище, ініціали та посад консультанта	Перевірив	
		Дата	підпис
Розділ 1.	Ізмайлова О.В., к.т.н., доцент		
Розділ 2.	Делембовський М.М., к.т.н., доцент		
Розділ 3.	Делембовський М.М., к.т.н., доцент		
Розділ 4.			

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Аналіз предметної області	15.10.2025 р.
Аналіз методів та методик по темі дослідження	27.10.2025 р.
Порівняння КСЗІ та нових профілів безпеки	30.11.2025 р.
Остаточне оформлення роботи	08.12.2025 р.
Направлення роботи на рецензування, перевірку на плагіат	12.12.2025 р.
Попередній захист роботи на кафедрі	15.12.2025 р.

8. Дата видачі завдання 30 вересня 2025 року.

Керівник _____ _____

(підпис) (прізвище та ініціали)

Здобувач _____ _____

(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Боднар В.Р. «Поєднання принципів побудови КСЗІ та імплементація норм європейських директив з кібербезпеки до національного законодавства».

Атестаційна випускова робота магістра за спеціальністю: 125 «Кібербезпека та захист інформації», освітня програма: «Безпека інформаційних і комунікаційних систем». – Київський національний університет будівництва і архітектури. – Київ, 2025.

Дипломна робота присвячена дослідженню теоретичних, методичних і прикладних аспектів побудови комплексної системи інформаційної безпеки на основі інтеграції вимог національної системи технічного захисту інформації (КСЗІ), міжнародних стандартів серії ISO/IEC 27000 та фреймворку NIST Cybersecurity Framework. У роботі приділено значну увагу питанням гармонізації державних вимог та міжнародних підходів, управлінню ризиками та формуванню сучасних механізмів кіберзахисту.

У першому розділі розглянуто сучасні виклики інформаційної безпеки, наведено принципи побудови КСЗІ, проаналізовано законодавчу та нормативну базу України, включно з новими правилами щодо декларації відповідності КСЗІ. Досліджено міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002 та виконано порівняльний аналіз національних і міжнародних підходів.

У другому розділі вивчено методи аналізу та оцінювання ризиків: національні методики ТЗІ, стандарти ISO/IEC 27005, методологію OCTAVE та модель NIST RMF. Визначено можливості узгодження методик, обґрунтовано оптимальний підхід для державного органу. Описано прикладний об’єкт - систему електронного документообігу ТОВ «ПРОМІНЬ», яке розглядається як умовне підприємство критичної інфраструктури.

У третьому розділі створено інтегровану концептуальну модель поєднання КСЗІ та вимог ISO/IEC 27001, побудовано схеми узгодження стандартів, DFD-

моделі, PDCA-структури та контури захисту. Розроблено програмно-технічні рішення із застосуванням SIEM, IAM, DLP, WAF, IDS/IPS. Запропоновано методику декларування відповідності КСЗІ з урахуванням вимог СУІБ.

Важливою частиною роботи є практична побудова трьох профілів безпеки для системи електронного документообігу ТОВ «ПРОМІНЬ-2»:

1. профіль безпеки КСЗІ;
2. профіль безпеки на основі NIST CSF;
3. профіль безпеки СУІБ (ISO/IEC 27001).

Профілі сформовано із застосуванням моделей ризиків, контрольних заходів, карт контролів, обґрунтуванням рівнів зрілості та вимог відповідності.

В четвертому розділі виконано порівняльний аналіз трьох побудованих профілів безпеки для системи електронного документообігу умовного підприємства ТОВ «ПРОМІНЬ-3», оцінено їх ефективність, ступінь відповідності нормативним вимогам, гнучкість і практичність впровадження. Надано висновки та рекомендації щодо оптимальної інтеграції профілів у єдину систему кіберзахисту.

У загальних висновках підсумовано результати дослідження, визначено теоретичне й практичне значення роботи, надано рекомендації щодо впровадження інтегрованих моделей КСЗІ–ISO–NIST у державному секторі, недержавних організаціях і підприємствах критичної інфраструктури.

Ключові слова: КСЗІ, інформаційна безпека, кібербезпека, ISO/IEC 27001, NIST,CSF), управління ризиками, критична інфраструктура, СУІБ.

ABSTRACT

Bodnar V.R. “Combining the Principles of Building a Comprehensive Information Protection System (CSZI) and Implementing European Cybersecurity Directives into National Legislation.” Master’s Thesis in the specialty 125 “Cybersecurity and Information Protection,” educational program “Security of Information and Communication Systems.” – Kyiv National University of Construction and Architecture. – Kyiv, 2025.

The thesis is devoted to the study of theoretical, methodological, and applied aspects of building a comprehensive information security system based on integrating the requirements of the national system of technical information protection (CSZI), international standards of the ISO/IEC 27000 series, and the NIST Cybersecurity Framework. The work pays considerable attention to harmonizing national requirements with international approaches, risk management, and the formation of modern cyber defense mechanisms.

The first chapter examines current information security challenges, outlines the principles of CSZI development, and analyzes Ukraine’s legislative and regulatory framework, including the new rules for CSZI compliance declaration. It also explores international standards ISO/IEC 27001 and ISO/IEC 27002 and provides a comparative analysis of national and international approaches.

The second chapter studies methods for analyzing and assessing risks: national TZI methodologies, ISO/IEC 27005 standards, the OCTAVE methodology, and the NIST RMF model. It determines the possibilities for aligning these methodologies and substantiates the optimal approach for a government institution. The chapter also describes the practical case - the electronic document management system of PROMIN LLC, considered as a hypothetical critical infrastructure enterprise.

The third chapter presents an integrated conceptual model that combines CSZI and ISO/IEC 27001 requirements, along with schemes for harmonizing standards, DFD models, PDCA structures, and protection contours. It develops software and technical

solutions using SIEM, IAM, DLP, WAF, and IDS/IPS technologies. A methodology for CSZI compliance declaration is proposed, taking into account ISMS requirements.

An important part of the thesis is the practical development of three security profiles for the electronic document management system of PROMIN-2 LLC:

1. CSZI security profile;
2. NIST CSF–based security profile;
3. ISMS (ISO/IEC 27001) security profile.

The profiles are created using risk models, control measures, control maps, substantiated maturity levels, and compliance requirements.

The fourth chapter provides a comparative analysis of the three developed security profiles for the electronic document management system of PROMIN-3 LLC, evaluating their effectiveness, compliance with regulatory requirements, flexibility, and practical feasibility. Conclusions and recommendations are provided regarding the optimal integration of the profiles into a unified cyber defense system.

In the general conclusions, the results of the study are summarized, the theoretical and practical significance of the work is identified, and recommendations are offered for implementing integrated CSZI–ISO–NIST models in the public sector, non-governmental organizations, and critical infrastructure enterprises.

Keywords: CIPS, information security, cybersecurity, ISO/IEC 27001, NIST CSF, risk management, critical infrastructure, ISMS.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	Боднар Владислав Романович Bodnar Vladyslav		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	Поєднання принципів побудови КСЗІ та імплементація норм європейських директив з кібербезпеки до національного законодавства		
	Combining the Principles of Information Securit y System Design and Implementation of Europe an Cybersecurity Directives into National Legisl ation		
Освітній ступінь	Магістр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека та захист інформації»		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	Шабала Євгенія Євгенівна		
Обсяг роботи:	*Пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	157	4	18
Розділ 1	Теоретико-аналітичні засади дослідження		
Розділ 2	Аналіз методів та методик дослідження		
Розділ 3	Проєктні та практичні рішення		
Розділ 4	Узагальнення результатів і прикладний аналіз		
Висновки по роботі	У роботі виконано глибокий аналіз національної моделі технічного захисту КСЗІ, міжнародних стандартів ISO/IEC серії 27000 та фреймворку NIST Cybersecurity Framework, а також розроблено інтегровану модель їх узгодження для державних органів і підприємств критичної інфраструктури		
Ключові слова: Keywords:	КСЗІ, інформаційна безпека, кібербезпека, ISO/IEC 27001, NIST, CSF, управління ризиками, критична інфраструктура, СУІБ. CIPS, information security, cybersecurity, ISO/IEC 27001, NIST, CSF), risk management, critical infrastructure, ISMS.		

Здобувач _____/ _____

Керівник _____/ _____

Зміст

ПЕРЕЛІК СКОРОЧЕНЬ

А

АС – автоматизована система

API – Application Programming Interface

APT – Advanced Persistent Threat

Б

БД – база даних

BYOD – Bring Your Own Device

С

CA – Certification Authority

CERT-UA – команда реагування на інциденти України

CRM – Customer Relationship Management

CRAMM – CCTA Risk Analysis and Management Method

CSF – Cybersecurity Framework

CSIRT – Computer Security Incident Response Team

CVSS – Common Vulnerability Scoring System

D

DDoS – Distributed Denial of Service

DLP – Data Loss Prevention

DMZ – Demilitarized Zone

DNS – Domain Name System

DFD – Data Flow Diagram

E

EDR – Endpoint Detection and Response

ERP – Enterprise Resource Planning

ЕЦП – електронний цифровий підпис

I

IAM – Identity and Access Management

ICS – Industrial Control System

ICT – Information and Communication Technologies

IDS/IPS – Intrusion Detection System / Intrusion Prevention System

IEC – International Electrotechnical Commission

ISO – International Organization for Standardization

ISO/IEC 27001 – міжнародний стандарт систем управління інформаційною безпекою

ISO/IEC 27002 – стандарт контролів інформаційної безпеки

ISO/IEC 27005 – управління ризиками інформаційної безпеки

ІБ – інформаційна безпека

ІКС – інформаційно-комунікаційна система

K

КМУ – Кабінет Міністрів України

КСЗІ – комплексна система захисту інформації

КЕП – кваліфікований електронний підпис

M

MITRE ATT&CK – база тактик і технік кібератак

MDM – Mobile Device Management (якщо згадується, у тексті є посилання)

N

NIST – National Institute of Standards and Technology

NIST RMF – Risk Management Framework

O

OCTAVE – методика оцінки ризиків

OWASP – Open Web Application Security Project

P

PDCA – Plan–Do–Check–Act

PKI – Public Key Infrastructure

S

SLE, ARO, ALE – компоненти моделі оцінки збитків

SIEM – Security Information and Event Management

SOC – Security Operations Center

SSL/TLS – Secure Sockets Layer / Transport Layer Security

СЕД – система електронного документообігу

СІБ – система інформаційної безпеки

СУІБ – система управління інформаційною безпекою

T

ТОВ – товариство з обмеженою відповідальністю

V

VPN – Virtual Private Network

W

WAF – Web Application Firewall

ВСТУП

У сучасних умовах повномасштабної збройної агресії Російської Федерації проти України питання забезпечення інформаційної та кібернетичної безпеки набуло безпрецедентної важливості. Кібератаки стали невід'ємною складовою ведення війни, а операції російських кібервійськ - таким самим системним інструментом агресії, як і ракетні чи дронові удари. Кіберактивність підконтрольних РФ хакерських угруповань - Sandworm, Gamaredon, Fancy Bear (APT28), Turla, Energetic Bear та інших - суттєво зросла, що виявляється у постійних спробах проникнення до інформаційних систем органів державної влади, військових структур та підприємств критичної інфраструктури.

З початком повномасштабної війни Україна зіткнулася з одним із наймасштабніших кібертерористичних наступів у світі. Атаки типу wiper, складні фішингові кампанії, компрометація каналів електронної пошти, деструктивні кібератаки на енергосистеми, транспорт, зв'язок, телекомунікаційні вузли, урядові інформаційні ресурси стали регулярним явищем. Метою таких атак є як отримання доступу до конфіденційної інформації, так і дестабілізація діяльності державних інституцій, параліч критично важливих процесів, порушення управління та завдання супутньої шкоди обороноздатності держави.

Особливо вразливими залишаються інформаційні системи державних органів та підприємств критичної інфраструктури, які обробляють великий обсяг службової та конфіденційної інформації: урядові документи, матеріали оборонного значення, стратегічні рішення, персональні дані посадових осіб, логістичні та енергетичні дані. Будь-яка компрометація таких ресурсів може мати суттєві наслідки як на локальному, так і на загальнодержавному рівні.

У цих умовах значення якісного та системного забезпечення інформаційної безпеки суттєво зростає, а традиційні підходи, що використовувалися до війни, потребують перегляду та модернізації. Українська модель технічного захисту інформації (КСЗІ), яка десятиліттями була основою побудови систем захисту,

забезпечує фундаментальні вимоги, однак не повною мірою відповідає сучасним викликам, зокрема потребі у постійному моніторингу, адаптивному управлінні ризиками, оперативному реагуванні та підвищенні кіберстійкості в реальному часі.

У той же час міжнародні стандарти, такі як ISO/IEC 27001, ISO/IEC 27002 та NIST Cybersecurity Framework (NIST CSF), пропонують більш гнучкі, ризик-орієнтовані та процесно-орієнтовані механізми управління інформаційною безпекою. Ці підходи давно застосовуються в країнах НАТО та ЄС, а їх впровадження підвищує здатність організації протистояти складним і багатовекторним кіберзагрозам.

Саме тому одним із ключових напрямів розвитку кіберзахисту України є синхронізація національних підходів із міжнародними стандартами. Особливо важливим це є для державних органів і підприємств критичної інфраструктури, які стають першочерговою мішенню для агресора.

У цьому контексті актуальним є завдання створення інтегрованої моделі, яка б поєднувала:

• вимоги КСЗІ як обов'язкової основи національного законодавства,

• стандарти ISO як міжнародну найкращу практику,

• фреймворк NIST CSF як гнучкий та дієвий інструмент управління кіберризиками.

Практична частина роботи присвячена побудові профілів безпеки для системи електронного документообігу ТОВ «ПРОМІНЬ» - умовного підприємства критичної інфраструктури. Такий підхід дозволяє продемонструвати реальну інтеграцію національних і міжнародних вимог та оцінити ефективність їх одночасного застосування в умовах кібервійни.

Мета дослідження

Розроблення інтегрованої моделі побудови системи інформаційної безпеки державного органу та підприємства критичної інфраструктури в умовах агресії РФ

на основі поєднання вимог КСЗІ, ISO/IEC 27001 та NIST CSF, а також формування профілів безпеки для системи електронного документообігу ТОВ «ПРОМІНЬ».

Завдання дослідження

1. Проаналізувати сучасні кіберзагрози в умовах війни, зокрема активність APT-груп РФ.

2. Визначити ключові ризики та типові сценарії атак на державні органи та критичну інфраструктуру.

3. Дослідити національні нормативно-правові акти у сфері інформаційної безпеки та принципи побудови КСЗІ.

4. Проаналізувати стандарти ISO/IEC 27001, 27002 та фреймворк NIST CSF у контексті військових загроз.

5. Провести порівняльний аналіз вимог КСЗІ, ISO та NIST.

6. Дослідити методики управління ризиками (ISO 27005, OCTAVE, NIST RMF, НД ТЗІ).

7. Обґрунтувати методику вибору моделі ризик-орієнтованого управління безпекою.

8. Розробити інтегровану модель поєднання КСЗІ, ISO та NIST.

9. Побудувати профіль КСЗІ для системи ЕДО ТОВ «ПРОМІНЬ».

10. Побудувати профіль NIST CSF для тієї ж системи.

11. Побудувати профіль СУІБ (ISO/IEC 27001) для системи.

12. Виконати порівняльний аналіз побудованих профілів.

13. Сформувати практичні рекомендації для державних органів та підприємств КІ.

Об’єкт дослідження – процеси забезпечення інформаційної та кібернетичної безпеки в інформаційних системах державного сектору та критичної інфраструктури України в умовах війни.

Предметом дослідження є моделі, методи, стандарти та інструменти побудови комплексної системи інформаційної безпеки на основі інтеграції КСЗІ, ISO/IEC 27001 та NIST CSF з урахуванням ризиків, зумовлених діями кібервійськ РФ.

Методи дослідження:

- аналіз кібероперацій РФ та діяльності APT-груп;
- порівняльний аналіз нормативних документів;
- системний підхід до побудови КСЗІ;
- методи аналізу ризиків (ISO 27005, OCTAVE, NIST RMF, НД ТЗІ);
- моделювання контурів захисту (DFD, PDCA, моделі загроз, профілі безпеки);
- дослідження програмно-технічних засобів (SIEM, IAM, DLP, IDS/IPS, WAF).

Результати дослідження можуть бути використані:

- державними органами при модернізації КСЗІ;
- підприємствами критичної інфраструктури;
- установами, що впроваджують ISO/IEC 27001;
- організаціями, які впроваджують NIST CSF;
- фахівцями з кіберзахисту для побудови профілів безпеки;
- компаніями, які розробляють або експлуатують системи електронного документообігу.

Профілі КСЗІ, NIST та ISO для системи ЕДО умовних підприємств ТОВ «ПРОМІНЬ», ТОВ «ПРОМІНЬ-2», ТОВ «ПРОМІНЬ-3» є універсальними шаблонами для впровадження в інших організаціях.

РОЗДІЛ 1. ТЕОРЕТИКО-АНАЛТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Загальна характеристика проблеми інформаційної безпеки в сучасних умовах

1.1.1.Стан інформаційної безпеки держави в умовах війни

Інформаційна безпека є одним із ключових елементів забезпечення національної безпеки в умовах глобальної цифрової трансформації. У сучасному світі інформаційні ресурси, інформаційно-комунікаційні системи та цифрові сервіси стають критично важливими активами держави, надійність функціонування яких визначає стійкість державного управління, обороноздатність, енергетичну, транспортну та економічну безпеку. За оцінками ENISA, світовий рівень кібератак зростає щороку на 30–40 %, а кількість атак на державні структури зросла на 300 % протягом 2020–2023 років.

Для України проблема інформаційної безпеки є особливо гострою, оскільки з 2014 року країна стала мішенню систематичних та цілеспрямованих кібератак з боку Російської Федерації. Кібератаки РФ є складовою її гібридної агресії, спрямованої на підрив обороноздатності, дестабілізацію роботи органів влади, руйнування критичної інфраструктури, зрив державного управління та дезорієнтацію суспільства. Після початку повномасштабної війни 24 лютого 2022 року інтенсивність атак значно зросла: лише у 2022–2023 роках CERT-UA та ДССЗЗІ зафіксували понад 2200 комплексних кібератак, більшість із яких були спрямовані проти державного сектору, енергетики, телекомунікацій, оборонно-промислового комплексу та систем електронного документообігу.

У той же час державні органи України активно продовжують цифровізацію публічних процесів, розвиток електронного документообігу, впровадження інформаційно-комунікаційних систем, що обробляють конфіденційну інформацію, дані з обмеженим доступом, критичні державні дані, інформацію з грифами «Для службового користування» (ДСК). Зростання обсягів даних, що обробляються в

державному секторі, вимагає адекватної, сучасної та комплексної системи захисту, відповідної до національних і міжнародних стандартів.

З початком повномасштабного вторгнення РФ інформаційна та кібернетична безпека стали ключовими елементами обороноздатності держави. Російські кібервійська проводили операції, спрямовані на:

- дезорганізацію роботи державних органів;
- виведення з ладу державних сервісів;
- руйнування критичної інфраструктури;
- викрадення конфіденційної інформації;
- вплив на ухвалення управлінських рішень;
- ускладнення оборонних процесів.

1.1.2. Кібератаки як елемент військових операцій РФ

Фахівці Microsoft, NATO CCDCOE та Manidant підтверджують, що РФ здійснювала синхронні кібератаки одночасно з ракетними та артилерійськими ударами, наприклад:

- перед ударами 24.02.2022 було здійснено масштабну атаку на урядові мережі з використанням WhisperGate;
- під час ракетних атак у жовтні 2022 року фіксувались масові DDoS-атаки на державні реєстри;
- атаки на обленерго у 2015–2016 рр. (BlackEnergy, Industroyer) були скоординовані з військовими діями РФ.

Це свідчить про те, що кіберпростір є повноцінним театром воєнних дій.

1.1.3. APT-групи РФ, що ведуть системні атаки на Україну

На основі звітів ENISA, CISA, CERT-UA та ESET встановлено, що за атаками на українські ресурси стоять такі угруповання:

- Sandworm (ГРУ РФ) - атаки на енергетику; використання Industroyer, NotPetya, CaddyWiper;

- APT28 / Fancy Bear (ГРУ РФ) - шпигунські та деструктивні операції проти урядових структур;
- Gamaredon / Armageddon (ФСБ РФ) - масові фішингові кампанії, зараження електронного документообігу;
- Turla (ФСБ РФ) - багаторічне приховане проникнення, бекдори високої складності;
- Energetic Bear - атаки на промислові системи, SCADA, критичну інфраструктуру.

1.1.4. Типи кібератак, що стали найпоширенішими проти України

Фішингові кампанії. Gamaredon здійснив понад 1500 атак на державні електронні системи у 2022–2023 роках.

Wiper-операції. Використовувалися: WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper.

Атаки на ICS/SCADA. Україна стала першою державою, у якій хакери вимкнули електропостачання.

Спроби компрометації систем документообігу. CERT-UA регулярно фіксує спроби доступу до електронного документообігу центральних органів влади.

DDoS-атаки на реєстри і сервісні платформи. Збільшення атак у період активних бойових дій.

1.1.5. Нормативно-правова база України як елемент системи захисту

Сфера інформаційної та кібербезпеки в Україні регулюється рядом ключових законодавчих актів:

- Закон України «Про основні засади забезпечення кібербезпеки України» (2017). Визначає принципи кіберзахисту, роль секторів критичної інфраструктури, державні органи кібербезпеки.
- Закон України «Про інформацію». Регулює доступ до інформації, її класифікацію, принципи охорони.

- Закон України «Про захист інформації в ІКС». Визначає вимоги до КСЗІ, порядок забезпечення ТЗІ, сертифікації.
- Закон України «Про критичну інфраструктуру» (2021). Визначає категорії, відповідальних осіб, методологію оцінки ризиків.
- Постанова КМУ № 373. Регламентує порядок обов'язкового створення КСЗІ при обробці КІ, ДСК, персональних даних.
- НД ТЗІ ДССЗЗІ:
  1. НД ТЗІ 1.1-003-99 - захист від НСД
  2. НД ТЗІ 2.5-004-2012 - створення КСЗІ
  3. НД ТЗІ 2.5-005-2012 - експертна оцінка КСЗІ

Ці нормативи визначають базові вимоги до створення систем захисту для державних органів.

1.1.6. Актуальні проблеми державного сектору

- частина КСЗІ оновлювалася до 2014 року;
- відсутність системного впровадження SIEM, SOAR, DLP;
- нерівномірність захисту між відомствами;
- кадровий дефіцит у сфері кібербезпеки;
- недостатня інтеграція із міжнародними стандартами ISO та NIST;
- потреба у реформуванні системи ТЗІ.

1.1.7. Порівняння КСЗІ, ISO/IEC 27001 та NIST CSF

Українська КСЗІ забезпечує юридичну відповідність, однак:

- не використовує PDCA-цикл (ISO);
- не містить профілів безпеки (NIST);
- має статичні вимоги, що повільно адаптуються до загроз.

Тому необхідна інтегрована модель КСЗІ + ISO + NIST, яка вже застосовується у країнах НАТО.

1.2. Принципи побудови КСЗІ

1.2.1. Принцип законності та нормативної регламентованості

Побудова комплексної системи захисту інформації (КСЗІ) є основною вимогою для державних органів та підприємств критичної інфраструктури, що обробляють інформацію з обмеженим доступом. КСЗІ визначається як сукупність організаційних, технічних, криптографічних, інженерних та фізичних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в інформаційно-телекомунікаційних системах відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

Основні принципи КСЗІ формуються на основі вимог національних нормативних документів - Постанови КМУ № 373 15, НД ТЗІ 2.5-004-2012 17, НД ТЗІ 2.5-005-2012 18, а також узгоджуються з міжнародними стандартами ISO/IEC 27001, ISO/IEC 27002 та концепцією NIST Cybersecurity Framework.

У цьому підрозділі розглянуто ключові принципи побудови КСЗІ із включенням порівняльних таблиць та схем, що демонструють структуру системи та взаємозв’язки між її елементами.

Першим фундаментальним принципом побудови КСЗІ є дотримання законодавства України, яке визначає вимоги до забезпечення інформаційної безпеки. Усі заходи, технічні рішення, регламенти та процедури мають відповідати:

- Закону України «Про інформацію»;
- Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закону України «Про основні засади забезпечення кібербезпеки України»;
- Закону України «Про критичну інфраструктуру»;
- Постанові КМУ № 373;
- НД ТЗІ 1.1-003-99, 2.5-004-2012, 2.5-005-2012.

Для наочності узагальнення принципу наведено у таблиці 1.

Таблиця 1.1 – Нормативне підґрунтя побудови КСЗІ

Група документів	**Опис**	**Приклади**
Закони України	Юридична основа функціонування КСЗІ	ЗУ «Про інформацію», ЗУ «Про кібербезпеку»
Постанови КМУ	Регламентують створення КСЗІ	Постанова № 373
НД ТЗІ ДССЗЗІ	Технічні стандарти захисту	НД ТЗІ 2.5-004-2012
Міжнародні стандарти	Узгодження з глобальними вимогами	ISO 27001, NIST CSF

1.2.2. Принцип комплексності

Комплексність означає, що система захисту повинна включати заходи на всіх рівнях: організаційному, технічному, криптографічному, інженерному, фізичному та кадровому. Відображення цього принципу графічно, подано на рисунку 1.1.

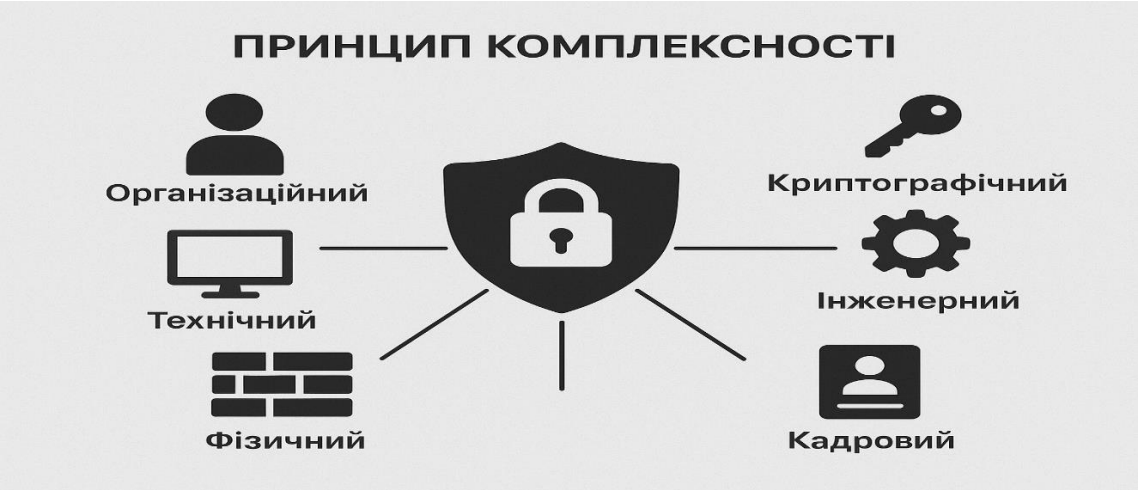


Рисунок 1.1 – Принцип комплексності

1.2.3. Принцип достатності заходів

Достатність передбачає, що засоби захисту мають відповідати ступеню загроз, класу інформації та категорії ІКС.

Для демонстрації цього принципу подано таблицю 1.2 з моделлю загроз.

Таблиця 1.2 – Типова модель загроз для побудови КСЗІ

Категорія загроз	**Приклади атак**	**Потенційні наслідки**
Технічні	RCE, SQL Injection	Порушення цілісності
Мережеві	DDoS, MITM	Відмова сервісу
Шкідливе ПЗ	Wiper, Ransomware	Знищення даних
Соціотехнічні	Фішинг, соціальна інженерія	Компрометація доступу
Фізичні	Пожежа, проникнення	Втрата обладнання

1.2.4. Принцип безперервності

Безперервність передбачає:

- безперервний моніторинг;
- реагування на інциденти;
- контроль працездатності;
- регулярний аудит;
- тестування системи.

НД ТЗІ 2.5-005-2012 прямо вимагає, щоб система функціонувала цілодобово.

1.2.5. Принцип управління ризиками

Аналіз ризиків є основою для формування вимог КСЗІ.

Класична модель PDCA при побудові КСЗІ:

PLAN → DO → CHECK → ACT → (повторюваний цикл)

Ця модель узгоджується з ISO/IEC 27001 і забезпечує розвиток системи.

1.2.6. Принцип мінімізації привілеїв

Мінімізація привілеїв або **least privilege** визначена НД ТЗІ 1.1-003-99 як ключовий спосіб запобігання НСД (Рис.1.2).

Рисунок 1.2 - Рольова модель доступу RBAC

1.2.7. Принцип документованості

Документування включає:

- політики інформаційної безпеки,
- моделі загроз і порушника,
- процедури реагування,
- журналювання,
- план відновлення.

Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373

«Про затвердження Порядку проведення експертизи у сфері технічного захисту інформації» зобов’язує подавати ці документи під час експертної оцінки.

1.2.8. Принцип контролю та аудиту

Контроль реалізується через:

- внутрішній аудит;
- зовнішню експертизу;
- SIEM/SOC-моніторинг.

1.2.9. Принцип фізичного та інженерного захисту

НД ТЗІ 2.5-004-2012 висуває вимоги до:

- серверних приміщень;
- телекомунікаційних шаф;
- резервування;
- температурного режиму;
- охоронних систем.

Для критичної інфраструктури цей принцип є обов'язковим.

1.2.10. Принцип інтегрованості з міжнародними стандартами

Оскільки українські НД ТЗІ частково застарілі, інтеграція з ISO/NIST є необхідною(табл. 1.3).

Таблиця 1.3 - Відповідність принципів КСЗІ міжнародним моделям

Принцип КСЗІ	**ISO/IEC 27001**	**ISO/IEC 27002**	**NIST CSF**	**Ступінь узгодженості**
Комплексність	Annex A	Controls	PR.*	Повна
Ризики	6.1	-	ID.RA	Часткова
Мінімізація привілеїв	A.9	AC Controls	PR.AC	Повна
Аудит	9.2	12.7	DE.*	Повна
Фізична безпека	A.11	A.11.*	PR.PT	Повна

1.2.11. Узагальнююча схема КСЗІ

Політики → Технічний захист → Криптографія → Фізична безпека → Моніторинг → Аудит → Оновлення

1.3. Нормативно-правова база України

1.3.1. Законодавчі акти України у сфері інформаційної безпеки

Нормативно-правова база України у сфері інформаційної та кібернетичної безпеки формується комплексом законів, підзаконних актів, державних стандартів, нормативних документів із технічного захисту інформації (НД ТЗІ) та галузевих рекомендацій, що визначають вимоги до оброблення інформації, забезпечення її захисту та організації комплексних систем захисту інформації (КСЗІ). Її застосування є обов'язковим для державних органів, органів місцевого самоврядування, підприємств державної форми власності та об'єктів критичної інфраструктури, а також визначає рамкові правила для приватного сектору.

Регулювання інформаційної безпеки в Україні ґрунтується на поєднанні трьох рівнів нормативності:

1. законодавчий рівень – базові закони України, що встановлюють принципи та засади захисту інформації;
2. нормативно-правовий рівень – постанови Кабінету Міністрів, накази та регламенти профільних органів (ДССЗЗІ/Держспецзв'язку), обов'язкові до виконання;
3. нормативно-технічний рівень – НД ТЗІ, ДСТУ, галузеві стандарти, які регламентують методи та способи захисту інформації.

До ключових законодавчих актів, що закладають фундамент державної політики у сфері інформаційної безпеки, належать закони що наведені в таблиці 1.4.

Таблиця 1.4 – Основні закони України у сфері інформаційної безпеки

№	Нормативний акт	Основні положення
1	**Закон України “Про інформацію”**	Визначає поняття інформації, її види, підстави для обмеження доступу, права та обов’язки суб’єктів інформаційних відносин
2	**Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”**	Установлює вимоги до захисту інформації в ІКС, порядок створення КСЗІ, відповідальність за порушення
3	**Закон України “Про основні засади забезпечення кібербезпеки України”**	Регламентує систему суб’єктів кібербезпеки, реагування на інциденти, державний контроль
4	**Закон України “Про електронні довірчі послуги”**	Нормує електронні підписи, печатки, засоби КЕП і кваліфікованих сертифікаційних центрів
5	**Закон України “Про захист персональних даних”**	Визначає вимоги до обробки, передачі та зберігання персональних даних
6	**Закон України “Про критичну інфраструктуру”**	Регулює категоризацію об’єктів КІ, їхню кіберстійкість, вимоги до безпеки
7	**Закон України “Про Національну програму інформатизації”**	Встановлює принципи створення державних інформаційних систем та вимоги до їх захисту

1.3.2. Підзаконні нормативно-правові акти (постанови КМУ, накази Держспецзв’язку)

Важливу роль у практичному регулюванні відіграють постанови Кабінету Міністрів та накази Держспецзв’язку, якими визначено порядок створення КСЗІ, проведення експертиз, оцінювання відповідності, а також вимоги до захисту державних інформаційних ресурсів (табл. 1.5).

Таблиця 1.5 - Основні постанови КМУ в області захисту інформації

№	Постанова	Сутність
1	**Постанова КМУ № 373 (2016 р.)** "Про затвердження Порядку забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"	Визначає обов'язковий порядок створення КСЗІ, вимоги до моделі загроз, ПЗ, процедур сертифікації
2	**Постанова КМУ № 518** "Про стандартизацію сфері КІ"	Визначає загальні вимоги для об'єктів критичної інфраструктури
3	**Постанова КМУ № 611** "Про реєстр об'єктів критичної інфраструктури"	Регламентує створення реєстру КІ, у т. ч. ІТ-систем

НД ТЗІ - це основний практичний інструментарій для побудови КСЗІ, який визначає вимоги до:

- організаційних заходів;
- технічних засобів захисту;
- криптографічних рішень;
- моделювання загроз та порушників;
- процедур експертизи.

Основні НД ТЗІ, які застосовуються при створенні КСЗІ наведені в таблиці 1.6.

Таблиця 1.6 - Основні НД ТЗІ, які застосовуються при створенні КСЗІ

№	Документ	Опис
1	**НД ТЗІ 1.1-003-99**	Визначає класифікацію ІКС та загальні вимоги до захисту інформації
2	**НД ТЗІ 2.5-004-2012**	Комплексний захист інформації: порядок створення КСЗІ та вимоги до її складових
3	**НД ТЗІ 2.5-005-2012**	Порядок проведення експертизи в галузі ТЗІ
4	**НД ТЗІ 2.7-010-2012**	Вимоги до безпеки технічних засобів
5	**НД ТЗІ 2.7-001-2014**	Вимоги до криптографічного захисту інформації

1.3.3. Державні та галузеві стандарти (ДСТУ, ДСТУ ISO/IEC)

Стандарти ДСТУ гармонізують українське регулювання з міжнародною практикою. Для інформаційної безпеки особливе значення мають стандарти, гармонізовані з ISO/IEC 27000-series (табл.1.7).

Таблиця 1.7 - ДСТУ у сфері інформаційної безпеки

Стандарт	**Назва**	**Зміст**
ДСТУ ISO/IEC 27001:2015	Системи управління інформаційною безпекою	Вимоги до ISMS
ДСТУ ISO/IEC 27002:2015	Кодекс практик	Каталог заходів ІБ
ДСТУ ISO/IEC 27005:2015	Управління ризиками	Методологія оцінки ризиків
ДСТУ 4145-2002	Криптографія	Алгоритми ЕЦП
ДСТУ 3396.0–96	Захист інформації	Базові положення

1.3.4. Взаємозв’язок національної нормативної бази з міжнародними стандартами

Українські НД ТЗІ історично були створені без прив’язки до ISO/IEC, але сьогодні простежується тенденція до інтеграції (табл. 1.8).

Таблиця 1.8 - Порівняння вимог КСЗІ з ISO/IEC та NIST

Вимога	**КСЗІ (НД ТЗІ)**	**ISO 27001/27002**	**NIST CSF**
Модель загроз	Обов’язкова	Необов’язкова	Частково
Аналіз ризиків	Обмежено	Основна вимога	Основна вимога
Політики	Частина КСЗІ	Обов’язкові	Обов’язкові
Фізичний захист	Регламентований	Регламентований	Частково
Аудит	Експертиза	Сертифікація	Самооцінка

1.3.5. Аналіз актуальності нормативної бази в умовах війни

Повномасштабна агресія РФ спричинила:

- різке зростання кібератак на державний сектор;
- необхідність гармонізації з NATO CCDCOE та стандартами STANAG;
- адаптацію НД ТЗІ до реалій сучасних загроз (wiper-атаки, supply-chain attacks).

Україна пришвидшено рухається до переходу:

- від КСЗІ як «статичної моделі»
- до динамічної системи кіберстійкості за NIST + ISO.

Нормативно-правова база України у сфері інформаційної безпеки є багаторівневою та комплексною, охоплює законодавчі, регуляторні та технічні документи і формує основу для створення КСЗІ в державних органах та на об'єктах критичної інфраструктури. Її особливістю є сильна орієнтація на державний сектор і потреба в модернізації з урахуванням міжнародних стандартів ISO/IEC та NIST. Поточний етап розвитку характеризується активною інтеграцією з міжнародним кіберпростором, що обумовлено як євроатлантичним курсом України, так і реальними загрозами, що виникли внаслідок збройної агресії РФ.

1.4. Нові правила щодо декларації відповідності КСЗІ

1.4.1. Попередня модель - атестація КСЗІ

Реформа державної системи технічного захисту інформації, розпочата у 2024 році й закріплена нормативними актами 2024–2025 років, докорінно змінює підхід до підтвердження відповідності комплексних систем захисту інформації (КСЗІ). Вона спрямована на децентралізацію, адаптивність, скорочення строків введення систем в експлуатацію та інтеграцію з міжнародними стандартами ISO, NIST та європейськими підходами.

Реформа стала прямою відповіддю на:

- збільшення обсягів кібератак з боку держави-агресора;
- необхідність швидкого впровадження цифрових державних сервісів;
- недоліки старої системи атестації.

До 2024 року підтвердження відповідності здійснювалося виключно через:

- державну експертизу ТЗІ;
- отримання атестата відповідності КСЗІ.

Модель мала такі проблеми:

- Тривалість - до одного року.
- Статичність - будь-яка зміна вимагала переатестації.
- Застарілість вимог - розроблені у 2000-х роках НД ТЗІ не враховують сучасних кібератак.
- Невідповідність міжнародним стандартам ризик-менеджменту.

1.4.2. Декларування відповідності (Постанова КМУ № 627 від 30.05.2024)

Цією постановою вперше запроваджено альтернативний механізм підтвердження відповідності для КСЗІ.

Основні положення:

- власник системи самостійно проводить оцінку впроваджених заходів;
- готує та подає декларацію відповідності;
- декларація реєструється у ДССЗЗІ;
- допускається експлуатація системи без експертизи;
- ДССЗЗІ зберігає функції державного контролю.

Рішення стало необхідним через критичну потребу в оперативності в умовах воєнного стану.

1.4.3. Профілі безпеки і авторизація (Постанова КМУ № 712 від 18.06.2025)

Цей документ започатковує повноцінну реформу:

- вводить профілі безпеки (базові й цільові);
- визначає механізм авторизації систем, подібний до АТО у NIST RMF;
- удосконалює процедури оцінки відповідності;
- уніфікує національні стандарти з ISO/IEC та NIST CSF.

Профілі безпеки - це структуровані набори вимог, аналогічні:

- Annex A ISO 27001;
- контролям ISO 27002;
- Target Profiles у NIST CSF.

Порівняння атестації, декларування та авторизації наведено в таблиці 1.9.

Таблиця 1.9 - Порівняння атестації, декларування та авторизації

Параметр	**Атестат КСЗІ**	**Декларація**	**Авторизація**
Хто оцінює	Експерти	Власник	Власник + ДССЗЗІ
Орієнтація	НД ТЗІ	Профіль безпеки	Ризики + профілі
Гнучкість	Низька	Висока	Висока
Тривалість	6–12 міс.	5–30 днів	1–3 міс.
Інтеграція ISO	Низька	Середня	Висока
Інтеграція NIST	Мінімальна	Висока	Повна
Сфера	Усі ІКС	Більшість систем	Критичні системи

1.4.5. Значення змін у період воєнного стану

Після 2022 року кількість кібератак збільшилася у десятки разів (CERT-UA, дані 2023–2024 рр.). Особливу активність проявляють угруповання Sandworm, APT28, Armageddon, Gamaredon.

Новий підхід дозволяє:

- швидко вводити в експлуатацію критичні системи;
- використовувати сучасні стандарти;

- впроваджувати ризик-орієнтовані моделі;
- оперативно реагувати на загрози.

Після цього можна дійти висновків, що:

- Нормативна база України перебуває в трансформації, орієнтованій на ISO/NIST.
- Декларування та авторизація роблять систему гнучкішою й сучаснішою.
- Профілі безпеки - ключовий елемент переходу до ризик-орієнтованої моделі.
- Реформа дозволяє ефективно захищати критичну інфраструктуру в умовах війни.

1.5. Міжнародні стандарти ISO/IEC 27001, 27002

1.5.1. ISO/IEC 27001 - основний стандарт управління інформаційною безпекою

Міжнародні стандарти серії ISO/IEC 27000 є найбільш поширеними у світі нормативними документами, що встановлюють вимоги до систем управління інформаційною безпекою, механізмів контролю, оцінювання ризиків та процесів забезпечення безперервності бізнесу. Використання цих стандартів є ключовою складовою інтеграції національної системи технічного захисту інформації України до світового кіберпростору та важливою умовою функціонування підприємств критичної інфраструктури в умовах підвищеної кіберзагрози.

Після 2022 року, коли кібервійська РФ активізували атаки на енергетичні компанії, телекомунікаційні структури, транспортні системи та державні електронні сервіси, застосування міжнародних стандартів ISO/IEC стало важливим етапом модернізації підходів до інформаційної безпеки в Україні.

ISO/IEC 27001:2022 - це міжнародний стандарт, що визначає вимоги до створення, впровадження, підтримання та вдосконалення системи управління інформаційною безпекою (СУІБ, ISMS). Він базується на принципах ризик-орієнтованого підходу, циклі постійного вдосконалення PDCA (Plan–Do–Check–

Act) та управління контролями з метою забезпечення конфіденційності, цілісності та доступності інформаційних активів.

Основні розділи ISO/IEC 27001 охоплюють:

- контекст організації;
- лідерство та політику у сфері ІБ;
- оцінювання ризиків;
- планування контролів;
- підтримку та ресурси;
- моніторинг, аудит та вдосконалення.

Особливістю стандарту є наявність Annex A, який містить 93 контролі, згруповані у 4 категорії:

- Організаційні заходи;
- Людські засоби контролю;
- Технологічні засоби;
- Фізичні засоби.

Ця структура робить ISO/IEC 27001 універсальним механізмом впровадження управлінської та технічної складових ІБ у будь-яких організаціях - від державних органів до приватних підприємств.

1.5.2. ISO/IEC 27002 - практичний стандарт контролів інформаційної безпеки

ISO/IEC 27002:2022 - це розгорнутий довідник та методичний документ, що деталізує всі контролі з ISO/IEC 27001 та надає рекомендації щодо їх реалізації. Стандарт містить:

- опис мети кожного контролю;
- вимоги до його впровадження;
- сценарії застосування;
- рекомендації із документування;
- залежності між різними контролями.

На відміну від ISO/IEC 27001, стандарт 27002 не містить вимог, а лише рекомендації. Він використовується:

- для проектування системи захисту;
- для побудови внутрішніх політик;
- для формування переліку заходів безпеки;
- як методичний документ під час аудитів;
- як основа для створення профілів безпеки.

1.5.3. Інші важливі стандарти серії ISO/IEC 27000

Для побудови інтегрованої системи ІБ важливими є також наступні стандарти:

- ISO/IEC 27000 - терміни та визначення;
- ISO/IEC 27003 - впровадження СУІБ;
- ISO/IEC 27004 - моніторинг та вимірювання ефективності ІБ;
- ISO/IEC 27005 - управління ризиками;
- ISO/IEC 27035 - реагування на інциденти;
- ISO/IEC 27701 - приватність та захист персональних даних (додаток до 27001).

Ці документи формують повну методологічну базу, необхідну для створення та підтримки сучасної системи захисту інформації.

1.5.4. Роль ISO/IEC 27001 для підприємств критичної інфраструктури

У контексті війни ISO/IEC 27001 відіграє ключову роль, оскільки забезпечує:

- Стандартизований ризик-орієнтований підхід - надзвичайно важливо при загрозах від APT-груп РФ.
- Безперервність бізнес-процесів - для енергетичного сектору, логістики та держпослуг.
- Можливість швидкої адаптації - за рахунок PDCA-циклу.
- Можливість інтеграції з NIST, CIS Controls, ENISA - що важливо для міжнародної співпраці України.

Багато підприємств критичної інфраструктури вже впроваджують ISO/IEC 27001 паралельно з КСЗІ для підвищення рівня кіберзахисту.

1.5.5. Порівняння ISO/IEC 27001 з українськими НД ТЗІ

Істотні відмінності між ISO та НД ТЗІ зумовили необхідність реформ, що були впроваджені у 2024–2025 роках (декларування, авторизація, профілі безпеки), що показано в таблиці 1.10.

Таблиця 1.10 - Порівняння ISO/IEC 27001 та НД ТЗІ

Елемент	**ISO/IEC 27001**	**НД ТЗІ України**
Підхід	Ризик-орієнтований	Регламентний, статичний
Гнучкість	Висока	Низька
Структура контролів	93 контролі (Annex A)	Фіксовані технічні вимоги
Оцінювання	Постійне удосконалення	Одноразова експертиза
Актуальність	Постійні оновлення	Багато документів застарілі
Сфера	Глобальний стандарт	Національні системи

1.5.6. Порівняння ISO/IEC 27002 з NIST Cybersecurity Framework

Хоча ISO/IEC 27002 є рекомендаційним документом, а NIST CSF - функціональною моделлю кіберстійкості, між ними існує значна узгодженість(табл.1.11).

Таблиця 1.11 - Співвідношення ISO/IEC 27002 та NIST CSF

Розділи ISO/IEC 27002	**Функції NIST**	**Коментар**
Організаційні заходи	Identify (ID)	Каталог активів, управління ризиками
Людські контролі	Protect (PR)	Навчання, доступ, політики
Фізичні заходи	Protect (PR)	Охорона, обладнання

Розділи ISO/IEC 27002	Функції NIST	Коментар
Технологічні заходи	Detect (DE) / Protect (PR) / Respond (RS)	SIEM, IDS/IPS, реагування
Моніторинг	Detect (DE)	Логування, аналіз подій
Відновлення	Recover (RC)	Планування DRP/BCP

1.5.7. Значення ISO/IEC 27001 та 27002 для реформування української системи КСЗІ

Реформування системи КСЗІ у 2024–2025 роках (перехід до декларування та авторизації) базується саме на:

- управлінських механізмах ISO/IEC;
- каталозі контролів ISO/IEC 27002;
- ризик-орієнтованості ISO/IEC 27005;
- профільному підході NIST CSF.

Саме тому профілі безпеки, що сьогодні впроваджуються Постановою № 712, фактично є адаптацією Annex A до українського законодавства.

Після дослідження можна зробити такі висновки:

- Міжнародні стандарти ISO/IEC серії 27000 становлять сучасний, глобально визнаний фундамент управління інформаційною безпекою.
- Вони формують основу для побудови СУІБ, каталогів контролів та методик управління ризиками.
- Україна поступово інтегрує ISO/IEC у свою національну систему безпеки через реформу КСЗІ, впровадження профілів безпеки та авторизацію інформаційних систем.
- Для критичної інфраструктури ISO/IEC є ключовим елементом підвищення кіберстійкості в умовах воєнної агресії.

1.6. Порівняльний аналіз КСЗІ та ISO

Комплексна система захисту інформації (КСЗІ) та стандарт ISO/IEC 27001 представляють різні концепції організації інформаційної безпеки. КСЗІ спрямована на виконання державних вимог України, тоді як ISO/IEC 27001 є універсальним міжнародним стандартом. Основні характеристики обох систем наведені у табл. 1.12.

Таблиця 1.12 – Порівняльна характеристика КСЗІ та ISO/IEC 27001

№	Критерій порівняння	КСЗІ	ISO/IEC 27001
1	Нормативний статус	Державна система ТЗІ (Україна)	Міжнародний стандарт
2	Обов’язковість	Обов’язкова для ІКС з обмеженим доступом	Добровільна
3	Підхід	Нормативно-регламентований	Ризик-орієнтований (PDCA)
4	Контроли	Керівні документи ДССЗЗІ	ISO/IEC 27002
5	Відповідність	Атестація	Сертифікація
6	Гнучкість	Низька	Висока
7	Сфера застосування	Державні ІКС	Будь-які організації

Візуально ключові відмінності систем відображено на рис. 1.3.

Рисунок 1.3 – Порівняння підходів КСЗІ та ISO/IEC 27001

Діаграма демонструє, що КСЗІ базується на фіксованих нормативних вимогах, тоді як ISO/IEC 27001 - на оцінці ризиків, гнучких контролях та циклі PDCA. Це підтверджує їхню комплементарність та можливість одночасного застосування у сучасних організаціях.

Висновки можна зробити наступні:

- КСЗІ та ISO/IEC 27001 мають спільну мету, але різні методологічні основи.
- КСЗІ регламентована державою, ISO/IEC 27001 - міжнародною стандартизацією.
- ISO/IEC 27001 забезпечує більшу гнучкість і ефективне управління ризиками.
- Оптимальним є комплексне застосування обох систем у великих організаціях.

1.7. Проблеми узгодження національних і міжнародних вимог

У сфері інформаційної безпеки українські організації дедалі частіше стикаються з необхідністю паралельного дотримання національних нормативних

вимог, що регламентують створення комплексної системи захисту інформації (КСЗІ), і міжнародних стандартів серії ISO/IEC 27000, зокрема ISO/IEC 27001. Такий подвійний підхід зумовлений прагненням відповідати законодавству України, забезпечувати захист інформації з обмеженим доступом та одночасно інтегруватися у глобальний інформаційний простір. Проте поєднання цих систем виявляється складним через значні відмінності у їхніх принципах, методологіях і механізмах реалізації.

Національні вимоги базуються на нормативно встановлених процедурах, що чітко визначають склад документів, перелік обов'язкових контролів та порядок проведення атестації. Міжнародний стандарт ISO/IEC 27001, навпаки, пропонує ризик-орієнтовану модель, у якій організація самостійно визначає контрольні заходи залежно від актуальних ризиків та власної діяльності. Різниця в підходах створює комплекс проблем, які охоплюють нормативні, технічні, організаційні та фінансові аспекти.

Першою системною проблемою є невідповідність концепцій: КСЗІ використовує статичну модель захисту, побудовану на фіксованих вимогах, тоді як ISO/IEC 27001 передбачає циклічний розвиток системи за принципом PDCA, орієнтований на постійне вдосконалення. Другою проблемою є різна структура документації: вимоги КСЗІ передбачають створення специфічного комплексу документів (моделі загроз, технічних паспортів, регламентів), які не завжди відповідають формату, передбаченому ISO/IEC 27001. Це змушує організації вести дві окремі групи документів, що суттєво збільшує трудові та часові витрати.

Третьою проблемою є технічні обмеження. Згідно з національними нормативами, інформаційні системи, що обробляють дані з обмеженим доступом, мають використовувати лише сертифіковані засоби технічного захисту інформації (ЗТЗІ). У ISO/IEC 27001 таких обмежень немає, що дозволяє впроваджувати сучасні міжнародні рішення, у тому числі хмарні сервіси, системи SIEM/SOAR, засоби багатофакторної автентифікації. Застарілий перелік сертифікованих ЗТЗІ інколи унеможливлює використання сучасних технологій.

Окрім того, існують труднощі, пов’язані з оцінюванням відповідності. Атестація КСЗІ та сертифікація ISO/IEC 27001 будуються на різних засадах: перша - на відповідності нормативним вимогам, друга - на оцінці ефективності управління ризиками. Це змушує організації проходити незалежні процедури оцінювання, що збільшує загальні витрати та тривалість впровадження системи захисту інформації.

Зведений аналіз основних проблем узгодження двох підходів наведено у таблиці 1.13

Таблиця 1.13 – Основні проблеми узгодження КСЗІ та ISO/IEC 27001 і шляхи їх розв’язання

№	Проблема	Суть проблеми	Шляхи розв’язання
1	**Концептуальні розбіжності**	Різні моделі побудови системи: нормативна (КСЗІ) та ризик-орієнтована (ISO)	Модернізація КД ТЗІ; адаптація принципів ризик-менеджменту
2	**Подвійна документація**	Несумісність структури документів обох систем	Уніфікація документів; створення універсальних шаблонів
3	**Суперечності контролів**	Фіксовані національні вимоги не збігаються з гнучкістю ISO	Гармонізація вимог; консультації з ДССЗЗІ
4	**Обмеження щодо ЗТЗІ**	Необхідність використовувати лише сертифіковані засоби	Розширення переліку засобів; актуалізація процедур сертифікації
5	**Подвійний аудит**	Атестація та сертифікація вимагають окремих процесів	Часткове взаємне визнання результатів аудиту
6	**Термінологічні розбіжності**	Різне трактування поняття загроз, ризиків, контролів	Уніфікація термінів; створення нац. глосарію ІБ
7	**Невідповідність сучасним технологіям**	Обмеження використання хмарних сервісів та інноваційних рішень	Оновлення нормативів; впровадження Zero Trust
8	**Відсутність офіційних методичних рекомендацій**	Відсутність єдиних стандартів інтеграції КСЗІ та ISO	Розроблення державних методичних документів

Схематичне зображення взаємозв’язку проблем наводиться у рисунку 1.4, де подано порівняння підходів КСЗІ та ISO/IEC 27001, а також ключові проблемні точки їх взаємодії.

Рисунок 1.4 - Порівняння підходів КСЗІ та ISO/IEC 27001, а також ключові проблемні точки їх взаємодії

Проблеми узгодження КСЗІ та ISO/IEC 27001 зумовлені принциповими відмінностями у їхніх підходах: нормативно встановленому та ризик-орієнтованому.

Складності виникають у питаннях структури документації, вимог до засобів захисту, процедур оцінювання відповідності та використання сучасних технологій.

Для усунення проблем гармонізації необхідне оновлення національної нормативної бази ТЗІ, розроблення офіційних методичних рекомендацій та уніфікація термінології.

Раціональна інтеграція КСЗІ та ISO/IEC 27001 дозволяє підвищити ефективність управління інформаційною безпекою та забезпечити відповідність як національним, так і міжнародним вимогам.

Таким чином, у розділі було розглянуто теоретичні засади забезпечення інформаційної безпеки, зокрема визначено сутність, структуру та нормативні основи системи захисту інформації в Україні. Проаналізовано національні вимоги

щодо побудови комплексної системи захисту інформації (КСЗІ) та міжнародні стандарти серії ISO/IEC 27000, які визначають принципи створення та функціонування систем управління інформаційною безпекою (СУІБ).

Доведено, що підходи КСЗІ та ISO/IEC 27001 мають спільну кінцеву мету - забезпечення конфіденційності, цілісності та доступності інформації, проте суттєво відрізняються за методологією. Національна система орієнтована на нормативно визначений комплекс заходів, тоді як міжнародний стандарт використовує ризик-орієнтовану модель та механізм постійного вдосконалення.

У межах порівняльного аналізу встановлено ключові відмінності між двома підходами: у структурі контролів, формі документації, процедурах оцінювання відповідності, вимогах до засобів технічного захисту та рівні гнучкості впровадження. Підкреслено, що для українських організацій, які прагнуть відповідати як державним, так і міжнародним вимогам, актуальними залишаються проблеми узгодження підходів, зокрема подвійна документація, обмеження щодо ЗТЗІ, суперечності у процедурах оцінювання та відсутність офіційних рекомендацій щодо гармонізації систем.

У результаті виконаного аналізу встановлено, що оптимальним шляхом розвитку системи захисту інформації в Україні є синтез підходів КСЗІ та ISO/IEC 27001, який забезпечує одночасно дотримання нормативних вимог держави та впровадження ефективних міжнародних практик управління інформаційною безпекою. Така інтеграція створює передумови для підвищення рівня кіберстійкості, модернізації інфраструктури захисту інформації та гармонізації українського законодавства з міжнародними стандартами.

ВИСНОВКИ ДО РОЗДІЛУ 1

У першому розділі було проведено комплексне теоретико-аналітичне дослідження проблематики інформаційної та кібернетичної безпеки в сучасних умовах, з урахуванням військових загроз, нормативно-правового середовища України та міжнародних стандартів. Результати виконаного аналізу дозволили сформувати такі ключові висновки.

Інформаційна безпека є одним із визначальних елементів національної безпеки України, оскільки сучасні кібератаки перетворилися на системний інструмент ведення гібридної війни. Україна перебуває під постійним впливом високотехнологічних атак з боку держави-агресора, а діяльність APT-груп РФ свідчить про зростання професійності, організованості та масштабності кібероперацій. Це зумовлює необхідність формування сучасної, багаторівневої та адаптивної системи кіберзахисту.

Стан інформаційної безпеки держави у період війни характеризується безпрецедентним рівнем загроз. Кібератаки синхронізуються із ракетними та дроновими ударами, спрямовуються на об’єкти критичної інфраструктури, органи влади, енергетичні системи, засоби зв’язку та системи електронного документообігу. Така інтеграція кібероперацій у військові дії демонструє принципову зміну характеру сучасних конфліктів.

У ході дослідження встановлено, що найпоширенішими типами атак проти України є фішингові кампанії, wiper-атаки, атаки на ICS/SCADA-системи, DDoS-атаки та спроби компрометації систем документообігу. Ці атаки орієнтовані як на завдання матеріальної шкоди, так і на інформаційний вплив, дестабілізацію роботи державних установ і поширення дезінформації.

Національна нормативно-правова база України у сфері інформаційної безпеки є розвиненою, проте фрагментованою та частково застарілою. Закони України, Постанови КМУ, НД ТЗІ та ДСТУ формують комплекс вимог до забезпечення інформаційної безпеки, проте багато з них були розроблені до появи сучасних

кібератак і потребують актуалізації. Особливо це стосується вимог до технічного захисту інформації, експертизи КСЗІ та застосування сертифікованих засобів захисту.

У процесі регуляторного аналізу встановлено, що нова державна реформа у сфері ТЗІ (2024–2025 рр.), яка запроваджує процедури декларування відповідності КСЗІ, авторизації та створення профілів безпеки, є важливим кроком до модернізації національної системи захисту інформації та її узгодження з міжнародними стандартами.

Значне місце у розділі займає аналітичне порівняння принципів побудови КСЗІ з вимогами ISO/IEC 27001, ISO/IEC 27002 та фреймворку NIST CSF. КСЗІ є нормативно-регламентованою моделлю, тоді як ISO та NIST використовують ризик-орієнтовані підходи, орієнтовані на безперервне вдосконалення, процесність та адаптивність. Виявлені розбіжності свідчать про об’єктивну потребу у трансформації державної системи кіберзахисту.

На основі порівняльного аналізу встановлено, що оптимальним шляхом розвитку української системи інформаційної безпеки є гармонізація КСЗІ з міжнародними стандартами, що дозволить забезпечити вищу ефективність, технологічність та відповідність сучасним кіберзагрозам.

У розділі також визначено основні проблеми узгодження національних та міжнародних вимог:

- подвійна та несумісна документація;
- різні підходи до аналізу ризиків;
- застарілі технічні вимоги НД ТЗІ;
- обмеження щодо використання новітніх технологій і засобів захисту;
- розбіжності у процедурах оцінювання відповідності.

Узагальнюючи результати, можна стверджувати, що КСЗІ, ISO/IEC 27001 та NIST CSF не є конкуруючими системами, а мають спільні цілі - забезпечення

конфіденційності, цілісності та доступності інформації. Їхнє поєднання створює основу для побудови сучасної, комплексної та гнучкої системи кіберзахисту.

Таким чином, розділ 1 сформував теоретико-аналітичне підґрунтя для подальших досліджень, окреслив ключові державні та міжнародні вимоги, визначив сучасні кіберзагрози та проблеми нормативної взаємодії, що дозволило перейти до розроблення методик, моделей та інтегрованих рішень, представлених у наступних розділах дипломної роботи.

РОЗДІЛ 2. АНАЛІЗ МЕТОДІВ ТА МЕТОДИК ДОСЛІДЖЕННЯ

2.1. Методи аналізу та оцінювання ризиків

2.1.1. Загальні положення

Управління ризиками інформаційної безпеки є ключовим елементом сучасних систем захисту інформації, зокрема таких, як СУІБ (Система управління інформаційною безпекою), КСЗІ та міжнародні моделі ISO/IEC 27001. Ризик визначається як комбінація ймовірності реалізації загрози та масштабу потенційних збитків.

Мета оцінювання ризиків - визначити пріоритети, потрібні захисні заходи та економічно обґрунтувати їх упровадження.

2.1.2. Компоненти ризику

Основними компонентами моделі ризику є:

- Актив - інформація, система, процес або ресурс, що має цінність для організації.
- Загроза - потенційне джерело небажаної події.
- Вразливість - слабке місце, що може бути використане загрозою.
- Інцидент - подія, що порушує цілісність, конфіденційність або доступність.
- Контрзаходи - механізми зменшення ризику (організаційні, технічні).

2.1.3. Методи оцінювання ризиків

Методи поділяють на якісні, кількісні та комбіновані.

Якісні методи:

- експертні оцінки;
- контрольні списки;
- SWOT-аналіз;
- матриці ризиків (3×3, 5×5);

- сценарний аналіз.

Ці методи прості, не потребують складних розрахунків.

Кількісні методи:

- статистичний аналіз;
- моделі ALE, ARO, SLE;
- фінансова оцінка збитків;
- CVSS (для технічних вразливостей).

Їх перевага точність і можливість економічного порівняння варіантів.

Комбіновані методики - NIST SP 800-30, OCTAVE, CRAMM, ISO/IEC 27005. Це найбільш гнучкі та ефективні підходи.

2.1.4. Життєвий цикл управління ризиками в КСЗІ

Відповідно до вимог ISO/IEC 27005 процес управління ризиками, інтегрований у проєктування та функціонування КСЗІ, включає такі основні етапи:

1. Встановлення контексту. Визначення меж КСЗІ, середовища її функціонування, категорій інформації та нормативних вимог.
2. Ідентифікація активів, загроз і вразливостей. Формування переліку активів ІКС, визначення потенційних загроз і можливих вразливостей.
3. Аналіз ризиків. Оцінювання того, яким чином загрози можуть реалізуватися через вразливості, та визначення можливих наслідків для інформації.
4. Оцінювання ризиків. Визначення рівня ризику та порівняння його з критеріями допустимості, встановленими для КСЗІ.
5. Обробка ризиків. Вибір стратегії реагування: зниження, уникнення, передавання або прийняття ризику.
6. Прийняття рішень. Узгодження рішень щодо вибраних заходів захисту, включно з технічними та організаційними, які будуть включені до комплексу засобів КСЗІ.

7. Моніторинг.Постійне спостереження за змінами у середовищі, станом захисту, актуальністю загроз та ефективністю впроваджених заходів.
8. Документування. Оформлення результатів аналізу та оцінювання ризиків у складі документації КСЗІ, включно з моделлю загроз, політиками, процедурами та рішеннями щодо обробки ризиків.

Після цього була сформована таблиця 2.1.

Таблиця 2.1 - Порівняльна характеристика методів

Тип методу	**Переваги**	**Недоліки**	**Приклади**
Якісні	Простота, швидкість	Висока суб'єктивність	SWOT, Check-list
Кількісні	Точність, прогностичність	Потребують даних	ALE, CVSS
Комбіновані	Найвища ефективність	Найбільша трудомісткість	ISO 27005, NIST

2.1.5. Модель «актив–загроза–вразливість–ризик»

Це базова схема всіх міжнародних стандартів:

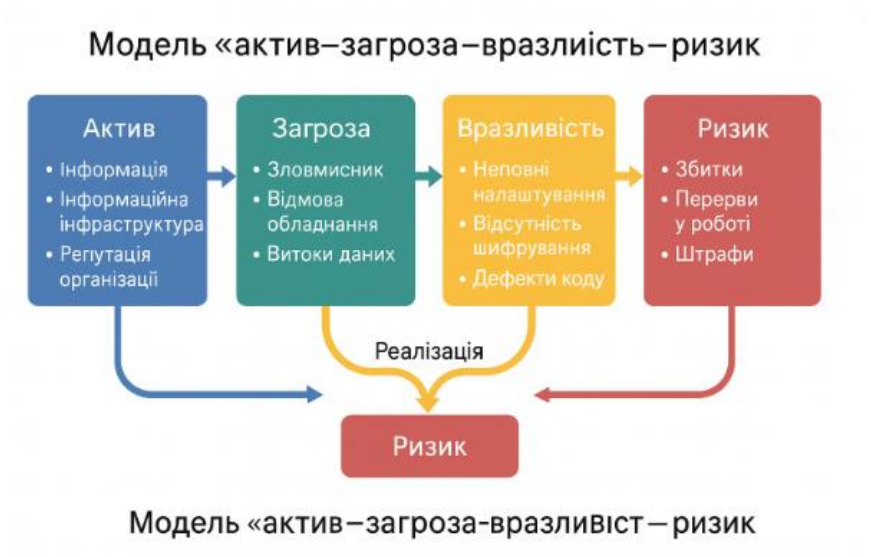


Рисунок 2.1 – Модель «актив – загроза – вразливість – ризик»

Отже, аналіз ризиків є базовою складовою інформаційної безпеки та основою для вибору захисних заходів. Методи оцінювання ризиків, визначені в

міжнародних стандартах ISO/IEC 27005 та NIST, забезпечують структурованість і об’єктивність процесу. Для більшості сучасних організацій найбільш ефективним є комбінований ризик-орієнтований підхід, узгоджений зі стандартом ISO/IEC 27001.

2.2. Методики розроблення та сертифікації КСЗІ

2.2.1. Призначення та нормативна база КСЗІ

Комплексна система захисту інформації (КСЗІ) - це формалізований механізм створення системи захисту інформації в автоматизованих системах (АС), які обробляють інформацію з обмеженим доступом, зокрема:

- службову інформацію;
- персональні дані;
- державні інформаційні ресурси;
- дані об’єктів критичної інфраструктури.

КСЗІ визначається та регулюється:

- Законом України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Законом України «Про інформацію»;
- НД ТЗІ серії 2.5 (особливо НД ТЗІ 2.5-004-99, 2.5-010-03);
- ДСТУ 3396.1–2015;
- нормативами Держспецзв’язку.

На відміну від ISO/IEC 27001, КСЗІ є вимогою закону, а не добровільним стандартом. Її функція - гарантувати, що система відповідає мінімальним технічним і організаційним нормам.

2.2.2. Життєвий цикл створення КСЗІ

Життєвий цикл створення КСЗІ складається з семи етапів, кожен з яких має чітко визначені цілі та результати.

Етап 1 це обстеження інформаційно-телекомунікаційної системи. На цьому етапі проводиться:

- аналіз архітектури мережі;
- аналіз серверного та мережевого обладнання;
- аналіз програмного забезпечення;
- визначення складу інформації;
- визначення каналів можливого витоку;
- аналіз суб'єктів доступу.

Результатом етапу є акт обстеження ІКС, структурна схема ІКС, опис інформаційних потоків.

Етап 2 - це моделювання загроз безпеці інформації. Модель загроз включає:

- опис активів;
- перелік потенційних загроз;
- аналіз можливості реалізації загроз;
- визначення каналів НСД;
- оцінку спрямованостей порушників.

КСЗІ використовує модель загроз за методиками:

- НД ТЗІ 1.1-003-99 (формування переліку загроз);
- методи класифікації загроз (внутрішні / зовнішні, природні / техногенні / антропогенні).

Етап 3. Розроблення технічного завдання (ТЗ). ТЗ визначає:

- об'єкт захисту;
- рівень необхідного захисту;

- вимоги до контролю доступу;
- вимоги до криптографічного захисту;
- вимоги до обліку, моніторингу та аудиту;
- вимоги до фізичної безпеки;
- структуру КСЗІ;
- перелік документації.

Це - один із ключових документів, що проходить погодження з Держспецзв'язку.

Етап 4. Проєктування КСЗІ. На цьому етапі розробляється:

- структурна схема КСЗІ;
- логічна схема захищеного периметру;
- політики доступу;
- регламенти адміністрування;
- політика резервного копіювання;
- вимоги до криптографічного захисту (КЗІ).

Етап 5. Впровадження КСЗІ. На практиці включає:

- інсталяцію засобів технічного захисту;
- налаштування МЕ, IDS, антивірусів;
- конфігурацію мережі та VLAN;
- налаштування журналювання;
- реалізацію криптографічних протоколів;
- організацію фізичного доступу;
- навчання персоналу.

Етап 6. Випробування КСЗІ. Проводяться функціональні випробування:

- оцінка захищеності ІКС;
- перевірка коректності реалізації;
- тестування криптографії;

- тестування процедур адміністрування.

Результатом цього етапу є протоколи випробувань.

Етап 7. Атестація КСЗІ. Атестацію проводять експерти Держспецзв'язку. Результат - атестат відповідності, що дозволяє легально експлуатувати систему.

Цей життєвий цикл включає певний перелік документації(табл.2.2)

Таблиця 2.2 - Перелік документації КСЗІ відповідно до НД ТЗІ

Група документів	**Основний зміст**	**Приклади**
Організаційні	Встановлюють правила, права, обов'язки	Політика безпеки, Положення про доступ
Адміністративні	Регламентують порядок дій персоналу	Інструкція користувача, Регламент реагування
Проєктні	Технічний опис майбутньої системи	ТЗ, Проєкт КСЗІ, схеми мереж
Оціночні	Підтверджують відповідність	Модель загроз, Протоколи випробувань
Експлуатаційні	Потрібні для повсякденної роботи	Журнали доступу, Журнал подій

2.3. Методики впровадження та сертифікації ISO/IEC 27001

2.3.1. Загальні засади та логіка побудови СУІБ

ISO/IEC 27001 визначає Систему управління інформаційною безпекою як сукупність політик, процедур, технічних і організаційних контролів, аудиту, аналізу ризиків, постійного моніторингу.

Основна відмінність ISO/IEC 27001 від КСЗІ полягає у тому, що це циклічна модель, яка постійно оновлюється відповідно до змін у середовищі організації.

2.3.2. Загальні засади та логіка побудови КСЗІ

Комплексна система захисту інформації (КСЗІ) є сукупністю організаційних, технічних та програмних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в автоматизованих та інформаційно-телекомунікаційних системах. Її створення регламентується низкою нормативних документів у сфері технічного захисту інформації, зокрема НД ТЗІ 1.1-003-99, НД ТЗІ 2.5-004-99 та НД ТЗІ 2.5-005-99.

Логіка побудови КСЗІ базується на принципі послідовного виконання визначених етапів, що забезпечують системний підхід до захисту інформації. Основними складовими процесу створення КСЗІ є:

- Обстеження інформаційної системи. На цьому етапі виконується аналіз архітектури ІКС, визначення інформаційних потоків, виявлення активів, встановлення категорійності інформації та визначення меж системи. Метою є формування повного уявлення про об’єкт захисту.
- Розроблення моделі загроз і моделі порушника. Відповідно до НД ТЗІ 1.1-003-99 формується перелік актуальних загроз для конкретної ІКС, визначається потенційний порушник, аналізуються його можливості, мотивація та ресурсні обмеження. Модель загроз є фундаментом підбору адекватних заходів захисту.
- Розроблення технічного завдання (ТЗ) на створення КСЗІ. ТЗ визначає вимоги до структури, функцій та засобів системи захисту. Документ узгоджується із замовником та затверджується відповідно до вимог ДСТУ та НД ТЗІ.
- Проєктування КСЗІ. На цьому етапі здійснюється вибір засобів технічного захисту інформації (ЗТЗІ), розробляються організаційні політики, процедури, правила доступу, моделі керування інцидентами, визначаються технічні засоби контролю.

- Впровадження системи захисту. Включає встановлення програмно-апаратних засобів, налаштування компонентів, впровадження регламентних процедур, навчання персоналу та документування процесів.
- Випробування і атестація КСЗІ. Здійснюються перевірка ефективності та коректності функціонування системи, оцінювання відповідності НД ТЗІ, проведення державної експертизи у сфері ТЗІ та видача атестата відповідності.

Загальна логіка побудови КСЗІ відображає нормативно-регламентований підхід та передбачає виконання фіксованого переліку робіт, що забезпечують створення формально підтвердженої системи захисту інформації. КСЗІ залишається ключовим механізмом державного регулювання у сфері оброблення інформації з обмеженим доступом.

2.3.3. Порівняльний аналіз КСЗІ та сучасних міжнародних підходів

З метою інтеграції українських організацій у глобальне інформаційне середовище дедалі важливішим стає порівняння національної моделі КСЗІ з міжнародними стандартами, зокрема ISO/IEC 27001. Обидві системи мають спільну мету - гарантувати захист інформації, проте відрізняються принципами, методологіями та механізмами впровадження.

Порівняльний аналіз подано у таблиці 2.3.

Таблиця 2.3 – Порівняння КСЗІ та ISO/IEC 27001

№	Критерій порівняння	КСЗІ	ISO/IEC 27001
1	Нормативна природа	Державна система ТЗІ України, регламентована НД ТЗІ	Міжнародний стандарт управління ІБ
2	Мета	Забезпечення захисту інформації з обмеженим доступом у державних ІКС	Побудова ефективної системи управління ризиками
3	Підхід	Жорстко регламентований, нормативний	Ризик-орієнтований, гнучкий
4	Документування	Фіксований перелік документів (модель загроз, ТЗ, регламенти)	Документація залежить від специфіки організації
5	Контроли	ЗТЗІ, вимоги НД ТЗІ	Контролі Annex A ISO/IEC 27001
6	Оцінювання відповідності	Атестація КСЗІ	Сертифікаційний аудит
7	Гнучкість	Низька	Висока
8	Технологічна адаптивність	Обмеження щодо використання несертифікованих ЗТЗІ	Вільний вибір технологій, у т.ч. хмарних
9	Сфера застосування	Державні органи та ІКС з обмеженим доступом	Усі типи організацій, приватний сектор
10	Оновлення системи	Не передбачає циклічної модернізації	Модель PDCA - постійне вдосконалення

Аналітичні висновки порівняльного аналізу:

- КСЗІ забезпечує відповідність державним вимогам, але має обмежену гнучкість, що може стримувати інтеграцію сучасних технологій.
- ISO/IEC 27001 забезпечує універсальність та адаптивність, дозволяє впроваджувати ризик-орієнтовані моделі управління та новітні технологічні рішення.

- Обидві системи комплементарні, але вимагають ретельної гармонізації, зокрема щодо документації, методології та контролів.
- Однією з ключових проблем узгодження є подвійне документування та обмеження щодо використання засобів, не сертифікованих за українськими нормативами.
- Інтегрований підхід, який включає використання методології ISO/IEC 27001 у межах КСЗІ, є найбільш перспективним і дозволяє одночасно відповідати як державним вимогам, так і міжнародним стандартам.

2.3.4. Цикл PDCA (Plan–Do–Check–Act)

ISO/IEC 27001 повністю базується на моделі PDCA(Рис.2.2).

PLAN – Планування:

- аналіз контексту;
- визначення зацікавлених сторін;
- формування політик;
- управління ризиками;
- вибір контролів.

DO – Виконання:

- впровадження заходів;
- навчання персоналу;
- документування СУІБ.

CHECK – Перевірка:

- моніторинг логів;
- внутрішні аудити;
- аналіз результатів діяльності.

ACT – Поліпшення:

- коригувальні дії;

- перегляд політик;
- адаптація до нових загроз.

Рисунок 2.2 - Розширена діаграма PDCA

2.3.5. Етапи сертифікації ISO/IEC 27001

Сертифікація ISO здійснюється на 3 роки. Сертифікація поділяється на:

- Аудит етапу 1 (перевірка документації)
- Аудит етапу 2 (польовий аудит)
- Щорічні наглядові аудити

2.4. Порівняльний аналіз та інтеграція підходів КСЗІ і ISO/IEC 27001 у побудові системи захисту інформації

2.4.1. Основні відмінності в методологіях

Незважаючи на те, що КСЗІ та ISO/IEC 27001 мають спільну мету - забезпечення захисту інформації, їх методології істотно різняться за:

- Призначенням. КСЗІ - обов'язкова державна вимога в Україні, застосовується до ІКС, що обробляють інформацію з обмеженим доступом. ISO/IEC 27001 - добровільний міжнародний стандарт, орієнтований на управління ризиками та безпекою в бізнесі.
- Підходом. КСЗІ - нормативно-технічний, «жорсткий», базований на відповідності НД ТЗІ. ISO 27001 - ризик-орієнтований, гнучкий, адаптивний.
- Архітектурою процесу. КСЗІ - лінійний процес (обстеження → модель загроз → проєкт → атестація). ISO 27001 - циклічний процес (PDCA).
- Сферою застосування. КСЗІ - державний сектор, критична інфраструктура. ISO - комерційні організації, міжнародні компанії, банки.

2.4.2. Спільні елементи методик

Хоча підходи різні, між КСЗІ та ISO/IEC 27001 є низка спільних рис, за якими можна їх порівняти(табл.2.4).

Таблиця 2.4 – Таблиця порівняння характеристик

Елемент	**КСЗІ**	**ISO/IEC 27001**
Оцінка ризиків	частково (через модель загроз)	повністю (ISO 27005)
Документація	жорстко регламентована	гнучка, адаптивна
Політики безпеки	обов'язкові	обов'язкові
Контроль доступу	реалізується ЗТЗІ	контролі A.5–A.8
Аудит	під час атестації	внутрішній + зовнішній
Впровадження технічних засобів	ядро процесу	частина контролів
Навчання персоналу	рекомендовано	обов'язково

2.4.3. Переваги інтегрованого підходу

Комбіноване застосування КСЗІ та ISO/IEC 27001 дає:

- Повну відповідність законодавству України: атестація КСЗІ є обов'язковою для багатьох державних установ.
- Міжнародну сумісність та довіру. ISO/IEC 27001 визнається в усьому світі.
- Посилений ризик-менеджмент. КСЗІ слабко охоплює аналіз ризиків. ISO заповнює цю прогалину.
- Гнучке вдосконалення процесів.ISO дозволяє постійно покращувати систему (PDCA).

2.4.4. Інтеграційна модель «КСЗІ + ISO/IEC 27001»

Для організацій, які мають і державні, і комерційні вимоги, оптимальною є комбінована модель:

Етап 1. Формування СУІБ відповідно до ISO 27001 → створення політик, процедур, аналіз ризиків.

Етап 2. Формування КСЗІ на основі готової СУІБ → використання ISO як фундаменту.

Етап 3. Атестація КСЗІ → додаткові вимоги, документація НД ТЗІ.

Етап 4. Сертифікація ISO 27001 → як підтвердження зрілості системи.

2.5. Практична модель вибору між КСЗІ, ISO/IEC 27001 та їх інтеграцією залежно від типу організації, інформації та ризиків

2.5.1. Критерії вибору методики

2.5.1.1. Тип організації та нормативні вимоги

Правильний вибір методології побудови системи захисту інформації визначає рівень безпеки організації, її здатність відповідати законодавчим нормам,

забезпечувати сталий розвиток, уникати інцидентів та зростати на міжнародному ринку. У цьому розділі здійснюється комплексне обґрунтування вибору між підходами КСЗІ, ISO/IEC 27001 та інтегрованою моделлю, з урахуванням особливостей діяльності, типу оброблюваної інформації, ризиків та зовнішніх вимог.

Критерії вибору можна розподілити на чотири основні групи: регуляторні, організаційні, інформаційні та ризикові. Кожна група має свій вплив і визначає доцільність використання КСЗІ, ISO/IEC 27001 або комбінованого підходу.

Тип установи є ключовим параметром, що визначає правові та функціональні рамки.

Державні органи та підприємства критичної інфраструктури:

- Підлягають прямому регуляторному контролю.
- Зобов'язані впроваджувати КСЗІ для всіх ІКС, де обробляється службова чи конфіденційна інформація.
- Атестація є обов'язковою.

Висновок: застосування КСЗІ є неминучим.

Приватні та міжнародні компанії

- Часто працюють із клієнтськими даними, персональними даними та бізнес-активами.
- Орієнтуються на ISO/IEC 27001, що забезпечує міжнародний рівень довіри й дозволяє демонструвати відповідність вимогам безпеки партнерам.

Отже, ISO/IEC 27001 є оптимальним та універсальним вибором.

Організації зі змішаними потоками даних

- Мають одночасно державний сегмент (наприклад, робота з реєстрами, державними системами) і комерційний.
- Потребують дотримання КСЗІ для державного сегменту та ISO для міжнародних партнерів.

Отже, необхідна інтегрована модель «КСЗІ + ISO».

2.5.1.2. Тип інформації

Тип і цінність інформації визначають вимоги до методів захисту.

Інформація з обмеженим доступом (службова, конфіденційна, державна таємниця) вимагає нормативно закріпленого підходу, тобто КСЗІ.

Комерційна інформація, інтелектуальна власність, персональні дані ISO/IEC 27001 передбачає гнучкий механізм захисту активів, включаючи політики, оцінку ризиків, аудит.

Змішана інформаційна модель необхідний комбінований підхід сувора регламентація КСЗІ для обмеженого доступу, ризик-орієнтована модель ISO для бізнес-процесів.

2.5.1.3. Міжнародні зобов'язання

Міжнародні партнери, банки, фінансові установи, постачальники часто вимагають:

- наявності сертифікату ISO/IEC 27001;
- підтвердження зрілості інформаційної безпеки;
- впровадження ризик-менеджменту;
- можливості проходження зовнішніх аудитів.

У таких випадках ISO є не лише бажаним, а й необхідним.

2.5.1.4. Рівень ризиків

ISO/IEC 27001 спирається на стандарти ISO/IEC 27005 та ISO 31000, які забезпечують:

- повноцінний аналіз ризиків;
- оцінку впливу;
- матриці ризиків;
- критерії прийняття;

- аналіз ефективності контролів.

КСЗІ орієнтується на модель загроз, що менш гнучко відображає реальні ризики. Отже, для систем з високим рівнем ризику ISO забезпечує кращу аналітичну базу.

Логічна модель вибору методики захисту інформації являє собою послідовність аналітичних кроків, які дозволяють визначити, чи доцільно застосовувати КСЗІ, ISO/IEC 27001 або інтегровану модель у конкретній організації. Процес можна представити як дерево ухвалення рішень, яке складається з кількох ключових етапів.

1. Визначення типу організації

Першим етапом є класифікація організації за її правовим статусом, сферою діяльності та характером роботи з інформацією. Виділяють три основні категорії:

1. *Державна установа*
Організації, що належать до органів державної влади, місцевого самоврядування або працюють з державними реєстрами, секретною чи службовою інформацією. Для них вимоги КСЗІ є обов'язковими згідно з чинним законодавством України.

2. *Комерційна організація*
Підприємства приватного сектору, які працюють у конкурентному середовищі, надають послуги бізнесу чи споживачам, зберігають персональні, клієнтські або комерційні дані.

3. *Організація зі змішаною інфраструктурою*
Установи, що одночасно мають державні функції та комерційні сервіси, або ті, що працюють з інформацією різного рівня доступу (державною, конфіденційною, комерційною).

На основі цього кроку формується первинний орієнтир щодо вибору методики.

2. Попередній вибір методології

Після визначення типу організації формуються попередні рекомендації:

- Для державних установ → КСЗІ
- Для комерційних організацій → ISO/IEC 27001
- Для змішаних систем → Інтегрована модель КСЗІ + ISO

Цей вибір є початковим і може бути скоригований подальшими факторами.

3. Аналіз типу інформації, що обробляється

Другим етапом після визначення типу організації є оцінка характеру інформації:

- Інформація з обмеженим доступом (службова, конфіденційна, таємна) → потребує нормативно регламентованого підходу, тобто КСЗІ.
- Комерційні дані, персональні дані, бізнес-активи → логічно поєднуються з гнучким ризик-орієнтованим підходом ISO/IEC 27001.
- Комплексні потоки даних → обґрунтовують вибір інтегрованої моделі.

Таким чином, тип інформації може як підтвердити попередній вибір, так і змінити його.

4. Оцінка рівня ризиків відповідно до ISO/IEC 27005

На цьому етапі аналізуються:

- вірогідність загроз,
- можливі наслідки інцидентів,
- вплив на бізнес-процеси,
- критичність інформаційних активів.

Системи з високим ступенем ризику (критична інфраструктура, фінансові установи, медичні дані, великі телекомунікаційні системи) потребують ISO-підходу, навіть якщо організація не зобов’язана застосовувати ISO на рівні законодавства. Такий аналіз може привести до рішення:

- доповнити КСЗІ елементами ISO,

- повністю перейти на ISO для комерційного сегменту,
- застосувати комбінований підхід.

5. Фінальний вибір оптимальної методики

Остаточний вибір формується на основі комплексної оцінки:

- тип організації;
- типу та рівня критичності інформації;
- оцінки ризиків;
- наявності міжнародних вимог та партнерств;
- стратегічних цілей розвитку;
- ресурсних можливостей організації.

У результаті приймається рішення про впровадження:

1. КСЗІ - коли необхідна жорстка нормативно-технічна відповідність.
2. ISO/IEC 27001 - коли потрібна гнучка, масштабована та міжнародно визнана система управління інформаційною безпекою.
3. Інтегрованої моделі «КСЗІ + ISO» - коли організація має змішані зобов'язання та хоче досягти як законодавчої, так і міжнародної відповідності.

Отже, логічна модель вибору методики захисту інформації демонструє, що рішення має ґрунтуватися не лише на формальному статусі організації, але й на ширшому комплексі чинників. Вона дозволяє системно визначити оптимальний підхід, уникнути помилок у проєктуванні системи безпеки та забезпечити максимальну ефективність інформаційного захисту відповідно до потреб і вимог організації.

2.5.2. Порівняльна таблиця для вибору методики

Удосконалена таблиця 2.5 включає не лише загальні характеристики, а й додаткові параметри, що визначають ефективність впровадження системи безпеки.

Таблиця 2.5 - Поглиблене порівняння можливостей КСЗІ та ISO/IEC 27001

Критерій	**КСЗІ**	**ISO/IEC 27001**
Відповідність законодавству України	Обов'язкова	Не регулюється законом
Міжнародне визнання	Обмежене	Високе
Підхід до ризиків	Частково (модель загроз)	Повноцінний (ISO 27005)
Гнучкість процесів	Низька	Висока
Можливість інтеграції з іншими стандартами	Обмежена	Висока (ISO 9001, 22301, 27701 тощо)
Затрати на впровадження	Високі у державному секторі	Гнучкі, залежать від масштабу
Атестація / аудит	Державна атестація	Незалежний міжнародний аудит
Циклічність процесів	Лінійний процес	PDCA (постійне вдосконалення)
Підтримка управління змінами	Обмежена	Системна (Change Management)
Орієнтація на бізнес-процеси	Низька	Висока

2.5.3. Рекомендований вибір

2.5.3.1. Для державного сектору

На основі критеріїв та аналізу можливостей кожної методики можна сформувати наступні рекомендації.

Організації державного сектору зобов'язані дотримуватися:

- законодавчих норм щодо захисту інформації,

- стандартів технічного захисту інформації,
- вимог до атестації.

Рекомендація: **використовувати КСЗІ як основну методологію**, із можливим доповненням елементами ISO (ризик-менеджмент, політики, аудит).

2.5.3.2. Для комерційного сектору

Компанії орієнтуються на:

- зменшення ризиків;
- підвищення довіри клієнтів;
- участь у міжнародних тендерах;
- проходження аудитів.

Рекомендація: **використовувати стандарт ISO/IEC 27001** як найоптимальніший варіант.

2.5.3.3. Для великих або змішаних установ

Такі організації працюють одночасно в нормативній площині держави та глобальному ринку.

Рекомендація: **використовувати інтегровану модель «КСЗІ + ISO»**, яка дозволяє:

- виконувати вимоги держави;
- формувати зрілу систему управління безпекою;
- здійснювати постійне вдосконалення;
- отримувати як атестацію КСЗІ, так і сертифікацію ISO.

Таким чином, розширений аналіз дозволяє зробити такі ключові висновки:

1. Жодна методика не є універсальною, і її вибір залежить від регуляторних вимог, бізнес-процесів та ризиків.
2. КСЗІ є незамінною для державних установ та систем з обмеженим доступом.

3. ISO/IEC 27001 забезпечує найвищий рівень гнучкості та міжнародної сумісності, що робить його оптимальним для бізнесу.
4. Інтегрована модель є найбільш ефективною для великих установ, що працюють у різних інформаційних доменах.
5. Комбінування КСЗІ та ISO дозволяє отримати як нормативну відповідність, так і сучасну систему управління безпекою.

2.5.4. Методологічні ризики неправильного вибору

Вибір методики створення системи захисту інформації є стратегічним рішенням, і помилки на цьому етапі можуть призвести до довгострокових негативних наслідків. Нижче наведено основні ризики, що виникають у разі невідповідного вибору методологічного підходу.

1. Невідповідність нормативним вимогам. Суть ризику: Використання ISO/IEC 27001 замість КСЗІ у державній установі не забезпечує виконання вимог законодавства України.

Наслідки:

- відмова від атестації системи;
- штрафи або адміністративні заходи;
- блокування експлуатації ІКС;
- ризики для керівництва установи.

2. Недостатній рівень захисту при високих ризиках. Суть ризику: фокус лише на КСЗІ (модель загроз) без повноцінного ризик-менеджменту ISO може не охопити комплексність сучасних кіберзагроз.

Наслідки:

- неповне охоплення ризиків;
- недооцінка кіберінцидентів;
- збільшення вразливостей.

3. Перевитрати ресурсів і фінансів. Суть ризику: впровадження КСЗІ у приватній компанії, де достатньо ISO, може призвести до надмірної бюрократизації та збільшення витрат.

Наслідки:

- подовжені терміни впровадження;
- потреба у залученні сертифікованих експертів;
- зайва документація;
- зниження ефективності бізнес-процесів.

4. Втрата конкурентоспроможності. Суть ризику: організація, що виходить на міжнародний ринок без ISO/IEC 27001, може бути відсіяна партнерами або замовниками.

Наслідки:

- неможливість участі у міжнародних тендерах;
- обмеження співпраці з іноземними банками та хмарними провайдерами;
- зниження довіри клієнтів.

5. Невідповідність методики масштабу ІКС. Суть ризику:

- КСЗІ погано масштабується для великих корпоративних систем.
- ISO може бути надто гнучким і не забезпечити достатньої нормативної деталізації у державних проєктах.

Наслідки:

- неузгоджені процедури;
- дублювання процесів;
- складність інтеграції контролів.

6. Проблеми з аудитами та атестацією. Суть ризику: невірний вибір методики може ускладнити проходження як державної атестації, так і міжнародних аудитів.

Наслідки:

- необхідність повторного впровадження;
- затримка запуску систем;
- фінансові втрати.

7. Зниження стійкості до інцидентів. Суть ризику: методика, що не відповідає реальним загрозам (наприклад, КСЗІ без ISO-контролів), може не забезпечити достатнього рівня підготовки до кіберінцидентів.

Наслідки:

- збільшення часу відновлення (MTTR);
- втрати даних;
- порушення безперервності діяльності.

Отже, неправильний вибір методики призводить до значних організаційних, фінансових та репутаційних ризиків. Тому рішення має прийматися на основі комплексного аналізу типу організації, нормативних зобов'язань, рівня ризиків, характеру інфраструктури.

2.6. Опис фактичного матеріалу (умовне підприємство ТОВ «ПРОМІНЬ»)

2.6.1. Загальна характеристика підприємства

ТОВ «ПРОМІНЬ» - комерційне підприємство, що спеціалізується на комплексних сервісах з обслуговування клієнтів, продажі товарів та наданні супутніх послуг. Компанія активно використовує сучасні інформаційно-телекомунікаційні технології, здійснює автоматизацію бізнес-процесів, взаємодіє з великою базою клієнтів, обробляє персональні та комерційні дані.

Основні бізнес-процеси підприємства включають:

- ведення CRM-системи (інформація про клієнтів, контракти, комунікації);
- роботу внутрішньої бухгалтерської та фінансової системи;
- електронний документообіг;

- віддалену роботу з використанням VPN;
- корпоративну електронну пошту;
- резервне копіювання критичної інформації.

Такі процеси створюють підвищені вимоги до інформаційної безпеки та зумовлюють необхідність впровадження КСЗІ та СУІБ ISO/IEC 27001.

2.6.2. Аналіз ІКС ТОВ «ПРОМІНЬ»

Структура ІКС підприємства складається з декількох ключових компонентів:

1. Серверна інфраструктура

- фізичні сервери Windows Server / Linux;
- віртуалізоване середовище VMware / Hyper-V;
- сервер бази даних PostgreSQL;
- сервер CRM;
- файловий сервер;
- сервер резервного копіювання;
- контролер домену.

2. Мережева інфраструктура

- L3-комутатори ядра;
- сегментована мережа (VLAN): офіс / сервери / Wi-Fi / гостьовий доступ;
- міжмережевий екран (Fortigate / Mikrotik);
- VPN-доступ для віддалених співробітників;
- IDS/IPS (базові механізми).

3. Робочі станції та мобільні пристрої

- понад 80 робочих станцій Windows;
- 15 ноутбуків - віддалена робота;
- BYOD (в окремих підрозділах).

4. Хмарні сервіси

- Microsoft 365 (пошта, документи);
- Teams/Zoom;
- Azure Backup.

На рисунку 2.3 зображена структурна схема ІКС ТОВ «ПРОМІНЬ».

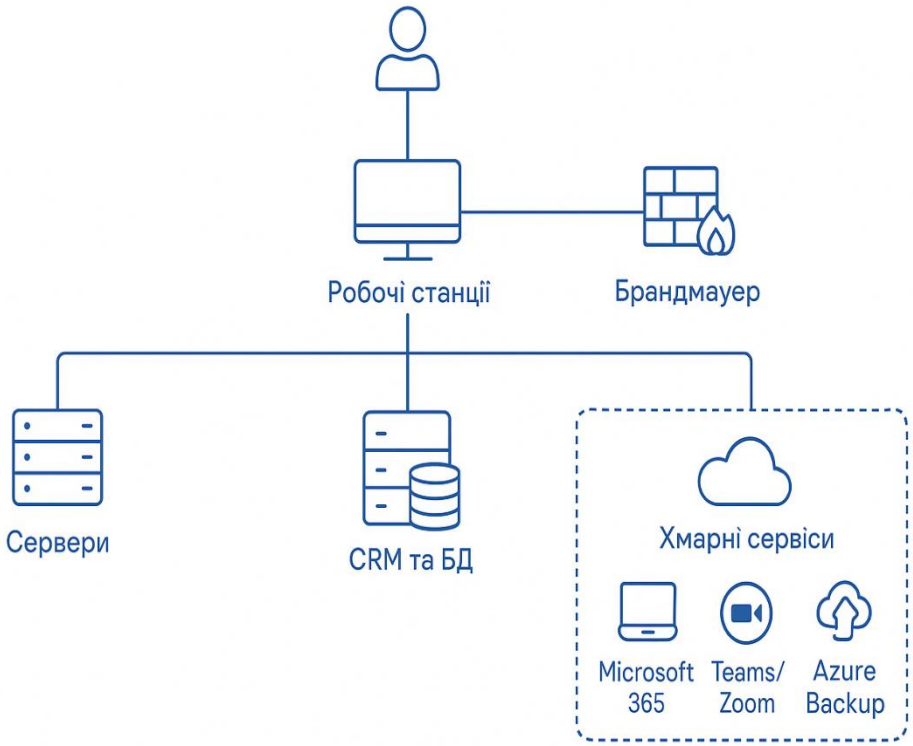


Рисунок 2.3 - Структурна схема ІКС ТОВ «ПРОМІНЬ»

Схема включає користувачів, робочі станції, комутатори, брандмауер, сервери, CRM та БД, блок резервного копіювання.

2.6.3. Класифікація інформації

Класифікація виконана згідно з вимогами НД ТЗІ 2.7-003-2005 та ISO/IEC 27001:2022.(табл.2.6)

Таблиця 2.6 - Класифікація інформації ТОВ «ПРОМІНЬ»

Категорія	**Тип інформації**	**Приклади**	**Рівень конфіденційності**
Відкрита	Публічна	реклама, презентації	низький
Для службового користування	Внутрішня	плани, внутрішня аналітика	середній
Конфіденційна	Бізнес-інформація	фінанси, договори	високий
Персональні дані	Дані клієнтів	ПІБ, контакти, покупки	високий (GDPR-критичний)

2.6.4. Модель загроз для ТОВ «ПРОМІНЬ»

(Відповідно до НД ТЗІ + ISO/IEC 27005)

Основні загрози:

- фішинг та соціальна інженерія;
- несанкціонований доступ;
- зараження шкідливим ПЗ (включно з ransomware);
- зовнішні атаки через інтернет (SQL-injection, brute force);
- збої обладнання;
- витік даних через людський фактор;
- VPN-компрометація;
- вразливості операційних систем та сервісів;
- помилки конфігурацій мережевого обладнання;
- фізичні загрози (крадіжка, пожежа, затоплення).

На рисунку 2.4 показана модель «Актив–Загроза–Вразливість–Ризик».

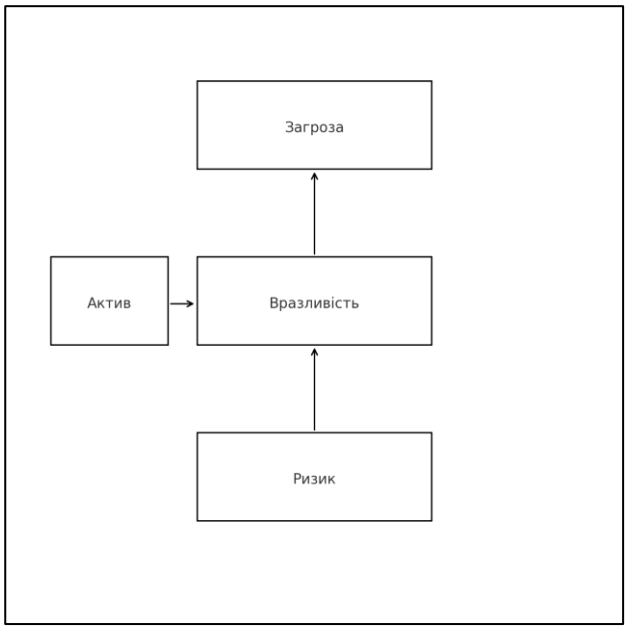


Рисунок 2.4 Модель «Актив–Загроза–Вразливість–Ризик»

2.6.5. Активи підприємства

Таблиця 2.7 - Основні активи ІКС

Актив	**Тип**	**Критичність**	**Примітка**
База даних	інформаційний	дуже висока	ключовий актив
CRM	інформаційний	висока	містить PD
Серверна	технічний	висока	точки відмови
Комутатори L3	технічний	середня	потребує резервування
ЗТЗІ (Firewall)	технічний	висока	елемент КСЗІ
Персонал ІТ	людський	висока	4 фахівці
Серверна кімната	фізичний	висока	потребує модернізації

2.6.6. Матриця ризиків

Таблиця 2.8 - Матриця оцінювання ризиків (ISO 27005)

№	Загроза	Імовірність	Наслідки	Рівень ризику	Рекомендації
1	Фішинг	висока	середні	високий	MFA, навчання
2	Ransomware	середня	дуже високі	критичний	backup, EDR
3	Витік CRM	низька	дуже високі	високий	сегментація
4	VPN-компрометація	середня	високі	високий	Zero Trust
5	Вразливості ПЗ	висока	високі	високий	Patch Management

Графічні блоки на рисунку 2.5:

- червоний - критичні ризики
- помаранчевий - високі
- жовтий - середні
- зелений - низькі

Рисунок 2.5 - Інфографіка ризиків

2.6.7. Необхідність створення КСЗІ

КСЗІ необхідна, тому що:

- обробляються персональні дані;
- є конфіденційна інформація;
- потрібен контроль доступу;
- необхідна атестація ІКС;
- потрібно забезпечити юридичний захист.

2.6.8. Необхідність впровадження ISO 27001

ISO/IEC 27001 забезпечує:

- міжнародне визнання;
- ефективний ризик-менеджмент;
- підвищення довіри клієнтів та партнерів;
- формалізацію політик безпеки;
- впровадження процесного підходу.

2.6.9. Рекомендована модель «КСЗІ + ISO 27001» для ТОВ «ПРОМІНЬ»

1. Формування СУІБ (ISO 27001).
2. Проведення аналізу ризиків (ISO 27005).
3. Розроблення моделі загроз (НД ТЗІ).
4. Створення ТЗ на КСЗІ.
5. Проєктування й впровадження КСЗІ.
6. Атестація ІКС.
7. Зовнішній аудит ISO 27001.

ВИСНОВКИ ДО РОЗДІЛУ 2

У розділі проведено комплексний аналіз методів і методик розроблення систем захисту інформації, оцінено можливості інтеграції національних та міжнародних стандартів, а також досліджено практичне застосування підходів на прикладі ТОВ «ПРОМІНЬ». Порівняння КСЗІ та ISO/IEC 27001 показало, що:

- КСЗІ забезпечує юридичну відповідність, але має жорстку структуру.
- ISO 27001 забезпечує гнучкість і потужний ризик-менеджмент.
- Комбінована модель КСЗІ + ISO є оптимальною для більшості організацій.

У підрозділі 2.6 проведено детальний аналіз ІКС підприємства, класифіковано інформацію, побудовано модель загроз, сформовано матрицю ризиків та розроблено рекомендації щодо впровадження інтегрованої системи захисту інформації.

Таким чином, ТОВ «ПРОМІНЬ» потребує одночасного впровадження: КСЗІ - для відповідності українським нормам; ISO/IEC 27001 - для підвищення рівня управління безпекою та міжнародної репутації.

РОЗДІЛ 3. ПРОЄКТНІ ТА ПРАКТИЧНІ РІШЕННЯ

3.1. Концептуальна модель поєднання КСЗІ та ISO

3.1.1. Модель КСЗІ: концепція, структура та ключові компоненти

Комплексна система захисту інформації (КСЗІ) - це державна модель побудови захисту інформації в автоматизованих системах, яка діяла в Україні понад 20 років і регулювалася:

- Законом України «Про захист інформації в інформаційно-телекомунікаційних системах»,
- НД ТЗІ 1.1–003–99 «Загальні положення»,
- НД ТЗІ 2.5–004–99 «Порядок створення КСЗІ»,
- НД ТЗІ 2.5–005–99 «Порядок проведення атестації КСЗІ».

Архітектура КСЗІ (класична модель)

КСЗІ складається з таких етапів:

- Обстеження ІКС
- Модель загроз і порушника
- Технічне Завдання КСЗІ
- Проєктування КСЗІ
- Впровадження технічних і організаційних заходів
- Випробування
- Атестація Держспецзв’язку

Принципи КСЗІ

- нормативно визначений перелік загроз;
- жорстка регламентація документів;
- орієнтація на технічні засоби захисту (ЗТЗІ);
- відповідність стандартам ДССЗЗІ.

Обмеження моделі КСЗІ

- надмірна зарегульованість;
- прив’язка до застарілих НД ТЗІ;
- низька гнучкість;
- відсутність повноцінної моделі ризиків.

Саме ці обмеження стали однією з причин законодавчої реформи 2024–2025 років.

3.1.2. Модель ISO/IEC 27001: концепція, структура та сильні сторони

ISO/IEC 27001 - глобальний стандарт управління інформаційною безпекою (СУІБ), який базується на принципах ризик-орієнтованості, циклічності (PDCA), документованості, постійного удосконалення.

Структура стандарту ISO/IEC 27001

Основні блоки (Annex SL):

1. Контекст організації
2. Лідерство
3. Планування
4. Оцінка ризиків (ISO 27005)
5. Механізми контролю
6. Підтримка
7. Моніторинг і аудит
8. Вдосконалення системи

Annex A. 93 контролі (у редакції 2022 року)

Контролі згруповані у домени:

- Організаційні заходи

- Технічні заходи
- Фізичний захист
- Контроль людей (Human factor)

Сильні сторони ISO/IEC 27001

- глобальне визнання;
- адаптивність;
- глибока модель ризиків;
- можливість безперервного вдосконалення;
- оптимальна для комерційних структур.

3.1.3. Модель поєднання КСЗІ та ISO/IEC 27001

Попри різні підходи, ці системи можуть бути інтегровані. Загальний принцип:

ISO 27001 формує систему управління безпекою → КСЗІ забезпечує відповідність державним вимогам.

Алгоритм поєднання

Порівняння моделей показано в таблиці 3.1.

Таблиця 3.1 – Порівняння моделей

Етап	КСЗІ	ISO/IEC 27001	Можливість інтеграції
1. Контекст	немає	✓	ISO доповнює
2. Модель загроз	✓	частково	ISO 27005 уточнює
3. Документація	жорстко регламентована	структурована, гнучка	документи ISO включаються у ТЗ КСЗІ
4. Заходи захисту	ЗТЗІ	контролі Annex A	відповідність мапиться

Етап	КСЗІ	ISO/IEC 27001	Можливість інтеграції
5. Аудит	атестація	сертифікація	можливо поєднати
6. Підтримка	не передбачено	✓ PDCA	PDCA підсилює КСЗІ

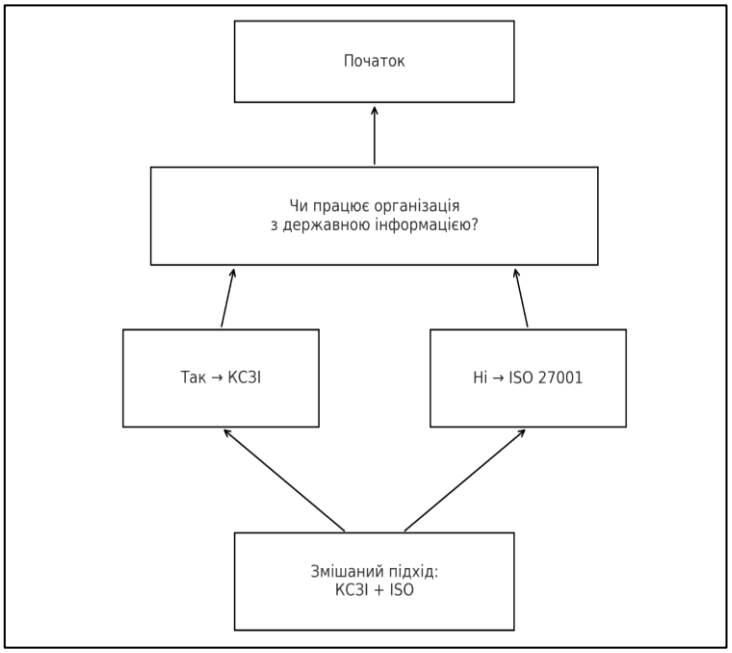


Рисунок 3.1 - Аудит організації за змішаним типом

Переваги такої інтеграції

- повне покриття державних вимог;
- наявність міжнародної сертифікації;
- структурований підхід до ризик-менеджменту;
- оптимізація витрат.

Отже, поєднання КСЗІ та ISO/IEC 27001 можливе, проте вимагає значних адаптацій та дублювання документів. Саме тому держава вирішила реформувати КСЗІ у 2024–2025 роках.

3.1.4. Концептуальна модель інтеграції СІБ (профілів безпеки) та ISO/IEC 27001

У 2024–2025 роках Україна здійснила фундаментальну реформу системи захисту інформації.Ключові зміни згідно з:

- Законом №4336-IX (березень 2025)
- Постановою КМУ №627 (30.05.2024) - запуск експерименту
- Постановою КМУ №712 (18.06.2025) - затвердження нової моделі
- Наказом №409 (30.06.2025) - базовий профіль для відкритої та конфіденційної інформації
- Наказом №419 (02.07.2025) - базовий профіль для службової інформації
- Новою базовою моделлю стають:
- Системи інформаційної безпеки (СІБ)
- Базові профілі безпеки
- Цільові профілі безпеки (ЦПБ)
- Авторизація, а не сертифікація

Це означає: **КСЗІ → поступовий перехід → Профілі безпеки + СІБ (нова державна модель)**.

3.1.4.1. Нова концептуальна модель СІБ + ISO/IEC 27001

1) Базові профілі безпеки (БПБ). Встановлюють мінімальні, обов’язкові вимоги.Є аналогом baseline security controls.

2) Цільовий профіль безпеки (ЦПБ). Формується власником системи на основі:

- ризиків;
- галузевих стандартів;
- специфіки системи;
- найкращих практик (ISO 27001, ISO 27002, NIST).

3) Інтеграція ISO/IEC 27001.ISO 27001 ідеально підходить як управлінський каркас для СІБ, що показано в таблиці 3.2.

Таблиця 3.2 – Порівняння профілів з ISO

Елемент	**Профілі безпеки**	**ISO/IEC 27001**
Базові вимоги	✓	закриваються Annex A
Ризики	частково	повністю ISO 27005
Контроль доступу	✓	✓
Аудит	✓ (авторизація)	✓ (сертифікація)
Постійне вдосконалення	частково	✓ PDCA

3.1.4.2. Алгоритм інтеграції СІБ + ISO

1. Аналіз вимог базового профілю
2. Формування СУІБ відповідно до ISO/IEC 27001
3. Розроблення ЦПБ на основі ризиків
4. Мапінг контролів ISO Annex A на базові профілі
5. Технічна реалізація засобів безпеки
6. Авторизація системи (державний рівень)
7. Сертифікація ISO 27001 (міжнародний рівень)

3.1.4.3. Переваги інтеграції СІБ (профілів безпеки) та ISO/IEC 27001

Поєднання державної моделі СІБ та міжнародної системи управління безпекою ISO/IEC 27001 створює єдиний, узгоджений підхід до захисту інформації та управління ризиками. Ключові переваги:

1. Усунення дублювання вимог КСЗІ та СУІБ

Замість паралельного виконання державних вимог та ISO 27001 формується одна інтегрована система контролів, що зменшує витрати часу, ресурсів та аудитних заходів.

2. Єдність управлінської та технічної моделей

Профілі безпеки задають обов'язковий державний мінімум, а ISO 27001 забезпечує цикл управління (risk-based, PDCA), створюючи повну зв'язку «вимоги → ризики → контролі → вдосконалення».

3. Можливість масштабування та адаптації

ЦПБ та система ризиків ISO дозволяють гнучко адаптувати рівень захисту під конкретну систему, замість універсальної та жорсткої моделі КСЗІ.

4. Спрощення державної авторизації та міжнародної сертифікації

Правильне мапування Annex A до БПБ забезпечує одночасне виконання українських та міжнародних вимог без повторного проєктування процесів.

5. Підвищення довіри для партнерів, інвесторів і міжнародних ринків

Сертифікація ISO 27001 + відповідність профілям безпеки - це підтвердження як державного, так і міжнародного рівня кіберзахисту.

6. Прозора та уніфікована система аудиту

Авторизаційна модель держави поєднується з аудитом ISO, що дозволяє впровадити сучасний підхід:

- state-level: відповідність БПБ/ЦПБ;
- international-level: відповідність ISO 27001.

7. Підготовка до інтеграції у кібербезпекові моделі ЄС та NIS2

ISO/IEC 27001 є рекомендованим стандартом для виконання вимог NIS2, тому інтегрована модель спрощує євроінтеграцію та майбутню гармонізацію законодавства України.

Таким чином, станом на 2025 рік концептуальна модель поєднання КСЗІ та ISO/IEC 27001 має два рівні:

1. Історичний рівень - КСЗІ + ISO (для систем з діючою атестацією).
2. Новий державний рівень - СІБ (профілі безпеки) + ISO (нова нормативна реальність).

ISO/IEC 27001 стає універсальним інструментом управління, а профілі безпеки - державним мінімальним каркасом.

Поєднання цих підходів дозволяє:

- відповідати українському законодавству;
- відповідати міжнародним вимогам;
- забезпечити гнучкість, масштабованість, адаптивність;
- уникнути дублювання КСЗІ → СУІБ;
- формувати єдину інтегровану систему захисту інформації.

3.2. Інтегрована схема узгодження стандартів

3.2.1. Нормативно-правова база узгодження стандартів

Узгодження підходів до побудови системи захисту інформації в Україні з міжнародними стандартами інформаційної безпеки базується на комплексі нормативно-правових актів, які формують правову, організаційну та методологічну основу. Починаючи з 2024–2025 років, законодавство України зазнало суттєвих змін, що трансформують модель КСЗІ у сучасну систему профілів безпеки.

Основні закони України у сфері кібербезпеки та інформаційної безпеки:

- Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.
  Визначає основні принципи побудови національної системи кібербезпеки, суб'єктів забезпечення кіберзахисту та їх повноваження.
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.
  Багаторічна основа для створення КСЗІ та атестації ІКС до реформування 2024–2025 рр.
- Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» від 12.03.2025 № 4336-IX.
  Найважливіший сучасний закон, що запровадив:
- відхід від моделі КСЗІ,

- перехід до моделі Систем інформаційної безпеки (СІБ),
- використання профілів безпеки,
- впровадження механізму авторизації систем замість атестації.

Постанови Кабінету Міністрів України:

- Постанова КМУ від 30.05.2024 № 627 «Про реалізацію експериментального проєкту щодо декларування відповідності систем захисту».Започаткувала перехід до СІБ та профілів безпеки.
- Постанова КМУ від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем». Встановила загальні вимоги до профілів безпеки та механізмів авторизації систем.

Накази Адміністрації Держспецзв'язку (2025 р.):

- Наказ від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація».
- Наказ від 02.07.2025 № 419 «Про затвердження базового профілю безпеки системи, де обробляється службова інформація».

Ці документи запровадили стандартизовані мінімальні вимоги, які замінюють підходи КСЗІ.

4. Міжнародні стандарти ISO:

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Українська назва: ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT)

«Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».

- ISO/IEC 27002:2022 - Code of practice for information security controls.
- ISO/IEC 27005:2022 - Information security risk management.

3.2.2. Методологічні відмінності КСЗІ, СІБ (профілів безпеки) та ISO/IEC 27001

Нижче наведено **детальне методологічне порівняння**, необхідне для формування інтегрованої схеми узгодження стандартів.

Таблиця 3.4 - Порівняння КСЗІ та СІБ (профілів безпеки)

Критерій	**КСЗІ (до 2025)**	**СІБ / Профілі безпеки (2025+)**
Нормативна основа	НД ТЗІ 1.1-003-99, 2.5-004-99, 2.5-005-99	Закон № 4336-IX, Постанова № 712, Накази № 409, 419
Структура	Жорстко регламентована модель із фіксованим переліком документів	Гнучка модель профілів безпеки
Сертифікація / Авторизація	Атестація ДССЗЗІ	Авторизація на відповідність профілю
Підхід	Технічний, нормативний	Ризик-орієнтований, адаптивний
Гнучкість	Низька	Висока
Масштабованість	Обмежена	Висока, профіль може бути галузевий, цільовий, базовий

Аналіз Таблиці 3.4 показує, що **модель КСЗІ, яка застосовувалася в Україні до 2025 року**, та **нова модель Системи інформаційної безпеки (СІБ) на основі профілів безпеки**, суттєво відрізняються за підходами, структурою та

нормативною базою. Перехід до СІБ є не просто оновленням документів, а **фундаментальною трансформацією державної політики у сфері кіберзахисту**, що відображає глобальні тенденції ризик-орієнтованого управління безпекою.

Нормативна еволюція. КСЗІ спиралася на застарілі НД ТЗІ (кінець 1990-х), що не враховували сучасних кіберзагроз.
СІБ заснована на сучасному законодавстві (Закон № 4336-IX та оновлені підзаконні акти), що створює:

- актуальну, технологічно нейтральну нормативну основу,
- можливість швидкого оновлення вимог під нові загрози,
- адаптацію до підходів ЄС та NIST.

Структурні відмінності. КСЗІ використовувала жорстко визначений перелік документів, що ускладнювало адаптацію під різні типи організацій.
СІБ переходить до моделі **профілів безпеки**, яка:

- враховує особливості галузей, масштаб організації та рівень ризиків;
- дозволяє створювати базові, цільові або розширені профілі;
- робить систему безпеки більш практичною та орієнтованою на реальні загрози.

Новий підхід до відповідності. КСЗІ вимагала *атестації* - складної державної процедури, спрямованої на перевірку виконання формальних нормативних вимог.
СІБ переходить до *авторизації на відповідність профілю*, що:

- більше схоже на міжнародну модель сертифікації;
- дає можливість різним суб'єктам оцінювати відповідність;
- фокусується не на документах, а на фактичному рівні безпеки.

Зміна парадигми: від технічної моделі до ризик-орієнтованої. КСЗІ була орієнтована здебільшого на технічні засоби та формальні вимоги.
СІБ орієнтується на:

- управління ризиками (аналог ISO 27005),

- адаптивність до змін середовища,
- пріоритет на процеси - не лише на технічні заходи.

Це робить СІБ набагато ближчою до міжнародних стандартів (ISO/IEC 27001, NIST CSF).

Гнучкість і масштабованість як головні переваги СІБ. У КСЗІ гнучкість і масштабованість були обмежені, що створювало труднощі:

- для великих корпоративних систем;
- для хмарних середовищ;
- для мультисервісних або розподілених інфраструктур.

СІБ вводить профілі, що можуть бути:

- **галузевими** (банки, медицина, енергетика),
- **цільовими** (для конкретних сервісів),
- **базовими** (для невеликих установ).

Це робить нову модель універсальною та придатною для масштабування. Отже, порівняння демонструє, що СІБ замінює КСЗІ більш сучасною, гнучкою та ризик-орієнтованою системою. Нова модель:

- підвищує відповідність міжнародним практикам,
- усуває бюрократичні обмеження КСЗІ,
- дозволяє адаптувати безпеку під реальні потреби організацій,
- робить державну систему кіберзахисту більш ефективною та сучасною.

Таким чином, перехід від КСЗІ до СІБ є логічним та необхідним етапом розвитку системи захисту інформації в Україні, що відповідає вимогам 2025 року та світовим тенденціям у сфері кібербезпеки.

Таблиця 3.5 - Порівняння КСЗІ та ISO/IEC 27001:2022

Критерій	**КСЗІ**	**ISO/IEC 27001:2022**
Мета	Захист ІКС державного сектору	Управління ризиками та захист інформації
Підхід	Нормативний	Ризик-менеджмент
Процес	Лінійний	PDCA (Plan–Do–Check–Act)
Документація	Жорстко фіксована	Гнучка
Сертифікація	ДССЗЗІ	Міжнародні аудитори

Порівняльний аналіз показує, що КСЗІ та ISO/IEC 27001:2022 мають різну природу, призначення та методологічні підходи, що визначає відмінності у їх практичному застосуванні. Обидві моделі спрямовані на забезпечення інформаційної безпеки, однак вони реалізують цю мету принципово різними способами.

Різниця в призначенні та сфері застосування. КСЗІ розроблена як механізм **обов'язкового захисту державних інформаційних систем**, що працюють з інформацією обмеженого доступу. Її мета - забезпечити нормативну відповідність та технічний контроль.

Натомість ISO/IEC 27001:2022 має універсальний характер і застосовується:

- у приватному секторі,
- у міжнародному бізнесі,
- у державних установах (на добровільних засадах).

Ціль ISO - не формальна відповідність, а **побудова системи управління ризиками** та дослідження впливу загроз на бізнес-процеси.

Протилежні методологічні підходи. КСЗІ використовує **нормативно-технічний підхід**, де вимоги жорстко задаються державними НД ТЗІ. Це робить систему передбачуваною, але негнучкою.

ISO/IEC 27001:2022 спирається на **ризик-менеджмент**, що передбачає:

- систематичну ідентифікацію загроз,
- оцінювання ризиків,
- вибір контролів залежно від контексту організації.

Це дозволяє адаптувати систему безпеки до реальних загроз і розвитку технологій.

Відмінність у побудові процесів. КСЗІ має **лінійний, завершений процес**, який не передбачає циклічного вдосконалення. Після атестації система вважається прийнятою до експлуатації.

ISO/IEC 27001:2022 працює за циклом **PDCA (Plan–Do–Check–Act)**, що включає:

- регулярну перевірку ефективності контролів,
- коригування процесів,
- безперервне удосконалення системи.

Це робить ISO більш живою та динамічною моделлю інформаційної безпеки.

Вимоги до документації. КСЗІ передбачає **фіксований перелік документів**, структура яких визначена нормативно. Це обмежує організації у можливостях адаптації системи.

Документація ISO/IEC 27001:2022 є **гнучкою та орієнтованою на контекст**, що дозволяє:

- адаптувати документи під бізнес-процеси;
- комбінувати політики та процедури;
- уникати зайвої бюрократії.

Відмінність у системі оцінки відповідності. КСЗІ атестується органами ДССЗЗІ - це внутрішньодержавна процедура, обмежена юрисдикцією України.

ISO/IEC 27001:2022 сертифікують **незалежні міжнародні аудитори**, що:

- забезпечує визнання сертифікату у всьому світі,
- підвищує рівень довіри до організації,

- сприяє розвитку міжнародної співпраці.

Таким чином, порівняння демонструє, що КСЗІ та ISO/IEC 27001:2022 відображають **дві різні парадигми інформаційної безпеки**:

- **КСЗІ** - це інструмент державного контролю, який гарантує нормативну відповідність, але є малогнучким і технічно орієнтованим.
- **ISO/IEC 27001:2022** - це сучасна, адаптивна, ризик-орієнтована система управління безпекою, яка дозволяє організаціям постійно вдосконалюватися та інтегруватися у міжнародний простір.

Таким чином, ISO/IEC 27001:2022 значно перевершує КСЗІ за динамічністю, ефективністю та придатністю до сучасних кіберзагроз, тоді як КСЗІ залишається незамінною для державного сектора через нормативні вимоги.

Таблиця3.6 - Порівняння СІБ (профілів безпеки) та ISO/IEC 27001

Критерій	**СІБ (профілі безпеки)**	**ISO/IEC 27001**
База	Нормативні вимоги України	Міжнародний стандарт
Ризик-менеджмент	Присутній частково	Повний (ISO/IEC 27005)
Гнучкість	Висока	Висока
Аудит	Авторизація	Сертифікаційний аудит

Порівняння двох сучасних підходів до організації інформаційної безпеки - СІБ (профілів безпеки) та ISO/IEC 27001 - демонструє як спільні риси, так і суттєві концептуальні відмінності. Обидві моделі є актуальними, гнучкими та орієнтованими на ризики, але застосовуються у різних нормативних та організаційних контекстах.

1. Нормативна база та сфера застосування

СІБ побудована на українській нормативній основі (Закон № 4336-IX, Постанова № 712, накази ДССЗЗІ), тому її застосування є **обов'язковим** для вітчизняних державних установ та суб'єктів критичної інфраструктури.

ISO/IEC 27001 є **міжнародним стандартом**, який використовується у глобальному приватному секторі та дозволяє організаціям:

- відповідати світовим практикам,
- брати участь у міжнародних тендерах,
- підвищувати довіру з боку партнерів.

Отже, СІБ - національна регуляторна вимога, ISO - глобальний універсальний стандарт.

2. Порівняння підходів до ризик-менеджменту

СІБ містить елементи оцінювання ризиків, але їхня деталізація і методологічна глибина **менші**, ніж у міжнародних стандартів. Профілі безпеки визначають обов'язкові контролі, проте не завжди вимагають повного циклу аналізу ризиків.

ISO/IEC 27001 спирається на ISO/IEC 27005, що забезпечує:

- чіткі критерії прийняття ризиків,
- глибокий аналіз загроз, вразливостей та впливів,
- системне управління ризиками.

Отже, ISO забезпечує **повноцінну**, зрілу модель ризик-менеджменту, СІБ використовує **частковий**, спрощений ризиковий підхід.

3. Гнучкість обох моделей

І СІБ, і ISO/IEC 27001 характеризуються високим рівнем адаптивності.

У СІБ це реалізується через:

- профілі безпеки (базові, цільові, галузеві),
- можливість формувати вимоги залежно від контексту ІКС,
- відсутність жорстко фіксованого набору документів.

У ISO - через:

- варіативність контролів,
- адаптацію документації під масштаб організації,
- інтеграцію з іншими стандартами (9001, 22301, 27701 тощо).

Обидві системи є високогнучкими, але ISO має більшу глобальну масштабованість.

4. Механізми аудиту та оцінки відповідності

СІБ передбачає процедуру **авторизації**, тобто підтвердження відповідності обраному профілю безпеки. Це державна або уповноважена процедура, зорієнтована передусім на регуляторні вимоги України.

ISO/IEC 27001 передбачає **сертифікаційний аудит**, який проводиться акредитованими міжнародними аудиторами, що гарантує:

- прозорість;
- глобальне визнання;
- високі вимоги до якості процесів;
- регулярний наглядовий аудит.

Отже, СІБ підтверджує відповідність профілю в межах України, ISO - сертифікує систему безпеки з міжнародним визнанням.

Порівняльний аналіз демонструє, що:

- **СІБ орієнтована на державний сектор та нормативну відповідність**, забезпечує гнучкість завдяки профілям безпеки, але має обмежену глибину ризик-менеджменту.
- **ISO/IEC 27001 є глобальною системою управління інформаційною безпекою**, яка характеризується широкими можливостями аналізу ризиків та міжнародним підтвердженням відповідності.

Таким чином, **СІБ оптимальна для виконання національних вимог**, **ISO/IEC 27001 оптимальний для організацій, що прагнуть міжнародної інтеграції та зрілого управління ризиками**, комбінація моделей може забезпечити найвищу ефективність для великих або змішаних організацій.

Таблиця 3.7 - Комбінована трикадрова таблиця КСЗІ ↔ СІБ ↔ ISO/IEC 27001

Параметр	**КСЗІ**	**СІБ / Профілі безпеки**	**ISO/IEC 27001**
Нормативна база	НД ТЗІ (1999)	Закон № 4336-IX, Накази № 409, 419	ISO/IEC 27001:2022
Підхід	Фіксований	Гнучкий	Ризик-орієнтований
Сертифікація / Авторизація	Атестація	Авторизація	Аудит і сертифікація
Використання	Держсектор	Держсектор і КІІ	Будь-які організації
Процес	Лінійний	Адаптивний	PDCA

Порівняння трьох систем - застарілої КСЗІ, нової моделі СІБ (профілів безпеки) та міжнародного стандарту ISO/IEC 27001:2022 - демонструє поступову еволюцію підходів до захисту інформації: від нормативної технічної моделі до гнучкої, адаптивної та ризик-орієнтованої системи управління. Аналіз за ключовими параметрами дозволяє зробити низку концептуальних висновків.

1. Нормативна база: перехід від застарілих норм до сучасних стандартів

КСЗІ ґрунтується на НД ТЗІ 1999 року - документах, які давно не відповідають реаліям сучасної кібербезпеки.
СІБ має сучасну українську нормативну основу (Закон № 4336-IX, Накази № 409 і 419), що дозволяє оперативно оновлювати вимоги.
ISO/IEC 27001 є міжнародним стандартом, який регулярно актуалізується та підтримується на глобальному рівні.

Отже, еволюція йде від застарілих локальних норм до сучасного національного регулювання та міжнародних практик.

2. Методологічний підхід: фіксованість → гнучкість → ризик-орієнтованість

КСЗІ застосовує жорстко фіксований підхід, який орієнтується на відповідність вимогам, а не на реальні ризики.
СІБ уже дозволяє гнучкість через профілі безпеки та вибір контролів залежно від контексту.
ISO/IEC 27001 робить управління ризиками центральним елементом, забезпечуючи найвищу адаптивність та ефективність у змінному середовищі загроз.

Отже, у розвитку систем безпеки простежується чіткий тренд - від суворої нормативності до адаптивності та ризик-орієнтованості.

3. Механізми підтвердження відповідності: від внутрішньодержавних процедур до міжнародного аудиту

КСЗІ передбачає державну атестацію, яка має формальний та часто бюрократичний характер.
СІБ використовує авторизацію - більш сучасний, але все ще національний механізм підтвердження відповідності.
ISO/IEC 27001 забезпечує міжнародний сертифікаційний аудит, який гарантує глобальне визнання та підвищує репутацію організації.

Отже, ISO є найбільш зрілим механізмом підтвердження безпеки, тоді як СІБ займає проміжне положення, а КСЗІ - найменш гнучка й найобмеженіша модель.

4. Цільове використання: розширення кола застосування

КСЗІ призначена виключно для державного сектору.
СІБ охоплює як держсектор, так і критичну інфраструктуру, що значно розширює її сферу застосування.
ISO/IEC 27001 є універсальним і підходить для організацій будь-якого типу, включно з урядовими, приватними, міжнародними та транснаціональними компаніями.

Отже, у міру розвитку системи інформаційної безпеки зростає її універсальність та можливість застосування у різних галузях.

5. Процеси побудови системи безпеки: статичність → адаптивність → безперервне вдосконалення

КСЗІ має лінійний процес, що завершується атестацією та фактично не передбачає циклічного оновлення.
СІБ є адаптивною - профілі безпеки можуть оновлюватися, а система реагувати на зміни ризиків.
ISO/IEC 27001 базується на циклі PDCA, що забезпечує безперервний розвиток та оптимізацію системи.

Отже, ISO забезпечує найвищий рівень процесної зрілості й системного управління кібербезпекою.

Порівняння трьох моделей демонструє **логічну еволюцію української системи інформаційної безпеки**:

- **КСЗІ** - застаріла, жорстка, малогнучка, орієнтована на державні ІКС.
- **СІБ** - сучасна національна модель, гнучка та адаптивна, яка частково враховує ризики й охоплює критичну інфраструктуру.
- **ISO/IEC 27001:2022** - міжнародний стандарт, що забезпечує найвищу ефективність управління безпекою завдяки ризик-орієнтованості та циклу PDCA.

СІБ займає перехідне положення між нормативною спадщиною КСЗІ та глобальною практикою ISO, поєднуючи державне регулювання зі сучасними принципами кібербезпеки.
ISO/IEC 27001 залишається найбільш повноцінною та універсальною системою, придатною для організацій будь-якого типу й рівня складності.

3.2.3. Інтеграційні точки між системами

Існує декілька ключових точок перетину між КСЗІ, новою моделлю СІБ та ISO/IEC 27001:

- Політики інформаційної безпеки. Усі три системи вимагають наявності політик, хоча ISO визначає їх структуру детальніше.
- Оцінка ризиків

- КСЗІ: через модель загроз і порушника.
- СІБ: через вимоги базового/цільового профілю.
- ISO: через повноцінний аналіз ризиків ISO/IEC 27005.

- Технічні та організаційні заходи. В ISO - Annex A. У СІБ - набір вимог профілю (аналог контролів).
- Контроль доступу, журналювання, реагування на інциденти. Присутні в усіх трьох системах, але в ISO подані найбільш системно.

3.2.4. Модель узгодження

Концептуальна модель узгодження стандартів КСЗІ, сучасної моделі СІБ (профілів безпеки) та міжнародної системи управління інформаційною безпекою ISO/IEC 27001:2022 ґрунтується на ідеї формування **єдиного, гармонізованого підходу**, який поєднує:

- нормативні вимоги України, що забезпечують юридичну обов'язковість та регламентацію мінімальних заходів безпеки;
- міжнародні керівні принципи ISO/IEC, які визначають сучасну модель ризик-менеджменту, структурування процесів та постійного удосконалення (цикл PDCA);
- профілі безпеки (СІБ), затверджені у 2025 році, які стають гнучким національним еквівалентом, що замінює КСЗІ та дозволяє адаптувати вимоги під специфіку кожної інформаційної системи.

Модель узгодження передбачає **три рівні інтеграції**: нормативний, методологічний та операційний.

Нормативний рівень узгодження. На цьому рівні визначаються **юридично обов'язкові рамки**, що регламентують вимоги до захисту інформаційних систем.

До складу нормативного рівня входять:

- Закон України № 4336-IX (2025 р.) – який запровадив нову модель побудови кіберзахисту, скасував обов'язковість КСЗІ та замінив її на СІБ і профілі безпеки.
- Постанова КМУ № 712 від 18.06.2025 р. – визначає загальні вимоги до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем.
- Постанова КМУ № 627 від 30.05.2024 р. – дала старт проєкту з декларування відповідності систем захисту.
- Накази Адміністрації Держспецзв'язку:
    - № 409 від 30.06.2025 – базовий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація.
    - № 419 від 02.07.2025 – базовий профіль безпеки системи, де обробляється службова інформація.
- Міжнародні стандарти серії ISO/IEC 27000 (у першу чергу – ISO/IEC 27001:2022).

Нормативний рівень створює **юридичні передумови**, що визначають "мінімальний рівень безпеки", який організація зобов'язана виконувати. ISO/IEC 27001 накладається на цей рівень як **перелік міжнародно визнаних практик**, які можна інтегрувати, не порушуючи українського законодавства.

Методологічний рівень узгодження. Цей рівень визначає, **як саме** різні стандарти та профілі можуть працювати разом.

Основні принципи методологічної інтеграції:

- Узгодження підходів КСЗІ та СУІБ. КСЗІ мала лінійну модель: обстеження → загрози → проект → впровадження → атестація. СУІБ переходить до моделі профілів безпеки, де заходи обираються відповідно до ризиків та специфіки системи. Основна точка інтеграції: уніфікація вимог КСЗІ у вигляді мінімальних вимог профілів (базових та цільових).

- Узгодження СУІБ та ISO/IEC 27001. ISO пропонує ризик-орієнтовану, гнучку модель, впорядковану через PDCA. Профілі безпеки стають “містком” між жорсткими нормативними вимогами держави та рекомендаційним характером ISO. Найперспективніший підхід – формування цільового профілю безпеки (ЦПБ) на основі:
    - базового профілю ДССЗЗІ,
    - структур ISO/IEC 27001 Annex A.

Узгодження КСЗІ та ISO/IEC 27001. КСЗІ визначала перелік загроз нормативно. ISO визначає ризики індивідуально, на підставі оцінки. Узгодження досягається через формування **карти відповідності заходів КСЗІ → контролям ISO/IEC 27001**.

Операційний рівень узгодження. Цей рівень описує реалізацію інтеграції у практичній площині. Операційна модель включає:

- Формування політик та процедур відповідно до ISO/IEC 27001.
- Визначення базового профілю захисту згідно з наказами Держспецзв’язку.
- Створення цільового профілю безпеки, який визначає конкретні заходи організації.
- Проведення аналізу ризиків (за ISO/IEC 27005) замість «моделі загроз» КСЗІ.
- Розробку плану заходів на основі:
    - національних вимог (мінімальні заходи СІБ),
    - міжнародних вимог (Annex A ISO/IEC 27001),
    - галузевих стандартів (NIST CSF, CIS Controls - опційно).
- Оцінку відповідності:
    - замість атестації КСЗІ - авторизація відповідно до профілю безпеки.
- Побудова системи моніторингу та аудиту:

- внутрішній аудит ISO → як механізм контролю виконання профілю,
- зовнішній аудит ISO → як підтвердження зрілості СУІБ,
- державний нагляд → перевірка дотримання профілів безпеки.

Суть концептуальної моделі узгодження

1. КСЗІ → СІБ

Перехід від жорсткого, «паперового» та формального підходу до гнучкого, ризикового, адаптивного моделювання вимог.

2. СІБ ↔ ISO/IEC 27001

Профілі безпеки стають інструментом локальної адаптації під міжнародні стандарти.

3. Інтеграція на основі ризиків

ISO/IEC 27005 та Annex A ISO/IEC 27001 забезпечують методологічний фундамент для модернізації профілів безпеки.

4. Нормативність + гнучкість

Модель дозволяє організації одночасно:

- виконувати українське законодавство,
- відповідати міжнародним вимогам,
- масштабувати СУІБ без повторного проходження атестації.

5. Результат моделі

Формується **єдина інтегрована система управління безпекою**, що складається з:

- базового профілю ДССЗЗІ,
- цільового профілю безпеки,
- вимог ISO 27001,
- ризикової моделі ISO 27005,

- процесного циклу PDCA.

3.2.5. Практичні напрями гармонізації

- Уніфікація політик ІБ.
- Використання профілів безпеки для відповідності вимогам держави.
- Побудова СУІБ відповідно до ISO/IEC 27001.
- Узгодження контролів Annex A з заходами профілю.
- Використання аудиту ISO як механізму підтвердження зрілості.

3.2.6. Технічні та організаційні механізми інтеграції

- Впровадження СУІБ як універсальної платформи, що підтримує профілі безпеки.
- Мапування контролів ISO → У вимоги профілю безпеки.
- Побудова незалежної моделі ризиків відповідно до ISO/IEC 27005.
- Використання систем SIEM, SOC, IAM, DLP тощо як технічних засобів відповідності.

3.2.7. Очікувані результати та переваги інтеграції

- Скорочення бюрократії.
- Стандартизація державних вимог.
- Міжнародна сумісність.
- Повноцінний ризик-менеджмент.
- Підвищення кіберстійкості державних і приватних організацій.

3.3. Методика декларування відповідності КСЗІ з урахуванням ISO

3.3.1. Загальні положення та актуальність

До 2025 року основним механізмом підтвердження відповідності державних інформаційних систем вимогам безпеки була **атестація комплексної системи захисту інформації (КСЗІ)**. Процедура регулювалася НД ТЗІ та передбачала жорсткий перелік документів і випробувань, що проводилися під контролем Адміністрації Держспецзв'язку.

У 2024–2025 роках відбулася системна реформа, закріплена:

- Законом України № 4336-IX від березня 2025 року, «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури»;
- Постановою Кабінету Міністрів України від 30.05.2024 № 627, «Про реалізацію експериментального проєкту щодо декларування відповідності систем захисту»;
- Постановою Кабінету Міністрів України від 18.06.2025 № 712, «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»;
- Наказом Адміністрації Держспецзв'язку від 30.06.2025 № 409, який затвердив базовий профіль систем, де обробляється відкрита або конфіденційна інформація;
- Наказом Адміністрації Держспецзв'язку від 02.07.2025 № 419, який затвердив базовий профіль систем, де обробляється службова інформація.

У результаті було введено нову модель - **Системи управління інформаційною безпекою (СУІБ)** та **профілі безпеки (базовий, галузевий, цільовий)**.

Це означає, що **декларування відповідності** стало заміною традиційної атестації КСЗІ.

3.3.2. Нове визначення декларування відповідності

Декларування відповідності - це офіційне підтвердження власника системи, що:

1. Система відповідає **вимогам затвердженого базового або цільового профілю безпеки**.

2. Запроваджена у системі **СУІБ** функціонує належним чином.

3. Ризики опрацьовано згідно з ISO/IEC 27001 та ISO/IEC 27005.

4. Технічні та організаційні заходи впроваджені та перевірені.

Новий механізм орієнтований не на формальне проходження атестації, а на **реальну відповідність сучасним практикам кіберзахисту**, що сприяє гармонізації з ISO.

3.3.3. Порівняння «Атестації КСЗІ» та «Декларування відповідності СУІБ»

Таблиця 3.8 – Порівняння КСЗІ та СУІБ

Критерій	**Атестація КСЗІ**	**Декларування відповідності СУІБ**
Нормативна база	НД ТЗІ	Закон 4336-IX, ПКМУ 627, ПКМУ 712, профілі безпеки
Основний акцент	Технічна відповідність ЗТЗІ	Ризики, процеси, управління, ISO
Контроль	ДССЗЗІ через атестацію	Власник системи + аудит СУІБ
Гнучкість	Низька	Висока
Документи	Фіксований перелік	Профілі + СУІБ + ризики
Міжнародність	Низька	Повна сумісність з ISO 27001

3.3.4. Етапи декларування відповідності з урахуванням ISO

Методика пропонує **8 логічних етапів**, які формують новий процес відповідності.

Ідентифікація системи та визначення її типу. Власник визначає:

- тип системи (інформаційна, комунікаційна, ІКТ, технологічна),
- категорію інформації (відкрита, конфіденційна, службова),
- критичність системи.
- Це визначає вибір базового профілю.

Вибір базового профілю безпеки (обов'язковий). На вибір є такі базові профілі:

- Базовий профіль відкритої/конфіденційної інформації (Наказ № 409);
- Базовий профіль службової інформації (Наказ № 419);
- (майбутні) галузеві профілі.

Базовий профіль описує мінімальні заходи кіберзахисту, аналогічно до «Annex A» у ISO/IEC 27001.

Формування цільового профілю безпеки (за потреби).Цільовий профіль містить:

- додаткові заходи,
- галузеві вимоги,
- посилені контролі безпеки (наприклад, MFA, SIEM, EDR),
- спеціальні режими доступу.

Це аналітичний документ, повністю сумісний з ISO/IEC 27001.

Проведення оцінки ризиків. Методики:

- ISO/IEC 27005,
- національні рекомендації ДССЗЗІ,
- модель загроз (оновлена під СУІБ).

Результат - **реєстр ризиків**, який замінює застарілі «моделі загроз КСЗІ».

Формування системи управління інформаційною безпекою (СУІБ). СУІБ включає політики, процедури, регламенти доступу, каталоги контролів, документацію щодо активів, моніторинг та інцидент-менеджмент.

СУІБ = українська адаптація ISO/IEC 27001.

Перевірка відповідності заходів профілю. Для кожного пункту профілю перевіряється реалізація, оцінюється ефективність, проводяться технічні тести (іноді пентест), аудитор фіксує відповідність.

Підготовка декларації відповідності. Структура декларації:

1. Загальна інформація про систему.
2. Базовий/цільовий профіль.
3. Реалізовані заходи.

4. Результати тестувань.

5. Звіт з оцінки ризиків.

6. Висновок уповноваженої особи.

Цей документ замінює «Атестат відповідності КСЗІ».

8. Надання декларації Держспецзв'язку

Декларація подається:

- у цифровому вигляді,
- через офіційні інформаційні сервіси (після запуску),
- з подальшим контролем та аудитом СУІБ.

3.3.5. Інтеграція методики декларування з ISO/IEC 27001:2022

Урахування ISO означає, що система має:

- пройти цикл PDCA (Plan-Do-Check-Act),
- працювати на основі ризиків (risk-based thinking),
- підтримувати актуальний набір контролів (Annex A),
- мати можливість зовнішньої сертифікації.

Декларування забезпечує адаптацію **національних вимог до міжнародних принципів**, зберігаючи:

- національну специфіку,
- вимоги щодо державних інформаційних ресурсів,
- правову відповідальність керівника системи.

3.3.6. Порівняння процедур відповідності КСЗІ та декларування СУІБ

Таблиця 3.9 – Порівняння КСЗІ та декларування СУІБ

Елемент	**КСЗІ**	**Декларування СУІБ + ISO**
Документи	Технічне завдання, модель загроз, проєкт	Профіль безпеки, оцінка ризиків, СУІБ
Сертифікація	Атестація	Декларація відповідності
Контроль	ДССЗЗІ	Власник + аудит

Елемент	КСЗІ	Декларування СУІБ + ISO
Орієнтація	Технічні засоби	Управління, процеси, ризики
Гнучкість	Низька	Дуже висока
Міжнародність	Немає	Повна сумісність з ISO

Перехід від атестації КСЗІ до декларування відповідності СУІБ означає стратегічне оновлення всієї системи державного управління інформаційною безпекою. Нова модель:

- спрощує бюрократію,
- підвищує гнучкість,
- інтегрує управління ризиками,
- робить інформаційну безпеку динамічною та масштабованою,
- забезпечує сумісність з міжнародними стандартами.

Таким чином, **СУІБ - це сучасна, ефективна та міжнародно орієнтована заміна КСЗІ**, яка відповідає викликам 2025 року та світовим практикам із захисту інформації.

Отже:

- Методика декларування відповідності замінює застарілу модель КСЗІ та впроваджує гнучкий підхід, заснований на профілях безпеки.
- Вона повністю сумісна з методологією ISO/IEC 27001:2022 та передбачає ризик-орієнтоване управління.
- Нова модель зменшує адміністративне навантаження, усуває бюрократію та прискорює впровадження систем кіберзахисту.
- Декларування забезпечує реальну відповідність, а не формальну атестацію.
- Процес інтегрується з міжнародними практиками та дозволяє організаціям отримувати міжнародні сертифікати без дублювання робіт.

3.4. Програмно-технічні рішення (ISMS, SIEM, IAM, DLP, IDS/IPS та ін.)

3.4.1. Системи управління інформаційною безпекою (ISMS Platforms)

Формування інтегрованої системи управління інформаційною безпекою вимагає застосування комплексу програмно-технічних рішень, що забезпечують виконання вимог як міжнародного стандарту ISO/IEC 27001:2022, так і національних профілів безпеки, затверджених Держспецзв'язку у 2025 році. Сучасна архітектура безпеки має бути багаторівневою, адаптивною та здатною реагувати на сучасні кіберзагрози, що динамічно еволюціонують.

У цьому розділі розглядаються ключові класи рішень, які формують технологічний фундамент СУІБ, їх функції, роль у відповідності стандартам та можливості інтеграції між собою.

1) Призначення

ISMS-платформи забезпечують автоматизацію політик, процедур, контролів та процесів управління ризиками, що закріплені ISO/IEC 27001:2022 та профілях безпеки СУІБ. Такі системи формують «основу» управління безпекою.

2) Основні функції

- ведення Реєстру ризиків (Risk Register);
- автоматизація GAP-аналізу;
- моніторинг виконання контролів Annex A 27001;
- управління інцидентами (ISO/IEC 27035);
- управління політиками безпеки;
- аудит відповідності (Audit management);
- зберігання документів СУІБ.

3) Приклади платформ

- Open-Source: OpenRMF, GRR Rapid Response (частково), Eramba.
- Enterprise: OneTrust ISMS, ServiceNow Security Operations, SAP GRC, Archer IRM.

4)Відповідність стандартам

Таблиця 3.10 – Підтримувані елементи для відповідності стандартам

Стандарт	Підтримувані елементи
ISO/IEC 27001:2022	Управління ризиками, аудит, політики, інциденти
Профілі безпеки СУІБ	Документація, реєстри активів, управління змінами

3.4.2. SIEM - Системи управління безпековими подіями

1) Призначення. SIEM (Security Information and Event Management) - ключовий елемент виявлення інцидентів, що забезпечує централізований збір, кореляцію та аналіз подій.

2) Функції:

- агрегація логів з усіх компонентів ІКС;
- кореляція подій за правилами та поведінковими моделями (UEBA);
- виявлення індикаторів компрометації (IoC);
- формування інцидентів та передача їх у SOAR;
- зберігання логів відповідно до вимог профілю безпеки.

3) Популярні платформи:

- Open-source: Wazuh SIEM, ELK Stack (Elastic).
- Enterprise: IBM QRadar, Splunk ES, Microsoft Sentinel, ArcSight.

4) Роль у відповідності:

- забезпечує виконання ISO 27001 Annex A: A.8, A.5.23, A.5.25;
- відповідає вимогам логування профілю безпеки (Наказ №409 та №419, 2025).

3.4.3. IAM - Управління доступами та ідентифікацією

1) Призначення. IAM-рішення реалізують контроль доступу відповідно до принципів least privilege, Zero Trust і вимог ISO/IEC 27001:2022 (A.5.15–A.5.17).

2) Ключові функції:

- SSO (Single Sign-On);
- MFA / 2FA;
- управління життєвим циклом облікових записів (Joiner-Mover-Leaver);

- RBAC/ABAC моделі доступу;
- централізовані каталоги (AD/Azure AD/LDAP).

3) Приклади рішень:

- Open-source: Keycloak, FreeIPA.
- Enterprise: Microsoft Entra ID, Okta, OneLogin, IBM Security Verify.

3.4.4. DLP - Захист від витоку даних

Функції:

- контроль пересилання даних через канали (e-mail, web, USB);
- контроль друку;
- виявлення секретної інформації (regular expressions, fingerprinting);
- робота з інцидентами інсайдерської активності.

Платформи:

- SearchInform DLP, InfoWatch DLP, Falcongaze SecureTower;
- Symantec DLP, McAfee Total Protection DLP.

Відповідність нормам. Підтримує вимоги ЦПБ та Annex A ISO щодо захисту конфіденційної інформації.

3.4.5. IDS/IPS - Виявлення та запобігання вторгненням

Призначення. IDS/IPS реалізують моніторинг трафіку та блокування атак відповідно до сучасних профілів безпеки.

Типи:

- Network IDS/IPS (Snort, Suricata)
- Host-based IDS (Wazuh HIDS)
- Cloud IDS (AWS GuardDuty, Google Security Command Center)

Можливості:

- сигнатурне виявлення;
- виявлення аномалій;
- MITRE ATT&CK mapping;

- інтеграція з SIEM та SOAR.

3.4.6. EDR/XDR - Захист робочих станцій

1) Призначення: EDR виявляє складні кібератаки на кінцевих точках, включаючи ransomware, fileless malware, privilege escalation.

2) Функції

- телеметрія процесів;
- аналіз поведінки (Behavioural detection);
- автоматичне блокування інцидентів;
- ізоляція хоста;
- Threat Hunting.

3) Платформи

- CrowdStrike Falcon, SentinelOne, Microsoft Defender.
- Open-source: Wazuh EDR.

3.4.7. PAM - Керування привілейованими обліковими записами

Призначення. Контроль дій адміністраторів і привілейованих користувачів.

Функції

- запис сесій;
- контроль команд у реальному часі;
- password vaulting (сховище паролів);
- Just-in-Time Access.

Рішення: CyberArk, Delinea (раніше Thycotic), Wallix.

3.4.8. Криптографічні засоби та PKI

Компоненти:

- сертифікаційні центри (CA);
- апаратні ключі (HSM);
- протоколи TLS 1.3, IPsec, SSH;

- віддалений підпис (КЕП).

Державні вимоги: Виконання Закону України «Про електронні довірчі послуги», КМУ №992.

3.4.9. SOAR - Автоматизація та оркестрація реагування

1) Призначення. SOAR дозволяє автоматизувати дії реагування, зменшити навантаження на SOC та скоротити час реагування.

2) Можливості

- runbooks / playbooks;
- автоматизоване блокування IP/MAC;
- закриття інцидентів;
- інтеграція з SIEM, IDS/IPS, EDR.

Платформи Cortex XSOAR, Splunk SOAR, IBM Resilient.

Таким чином:

- Програмно-технічні рішення формують технічне ядро інтегрованої системи управління інформаційною безпекою.
- Платформи ISMS забезпечують відповідність ISO/IEC 27001 та профілям безпеки.
- SIEM, IDS/IPS, EDR та SOAR становлять основу сучасного SOC-підходу.
- IAM/PAM та DLP забезпечують контроль доступу та захист від витоків - ключові елементи профілів безпеки.
- Комплексне застосування цих рішень створює багаторівневу захисну архітектуру, адаптовану до законодавства України станом на 2025 рік та сучасних міжнародних вимог.

3.5. Експериментальні дослідження / моделювання (ТОВ «ПРОМІНЬ»)

3.5.1. Загальна характеристика об’єкта дослідження

ТОВ «ПРОМІНЬ» - середня українська компанія, що надає послуги у сфері виробництва та логістики. Інформаційна інфраструктура підприємства складається з:

- 48 робочих станцій;
- локальної мережі з сегментацією VLAN;
- серверного сегмента з ERP/CRM;
- віддалених VPN-користувачів (менеджери та керівники);
- хмарного сервісу для резервного копіювання;
- окремої DMZ-зони для зовнішніх сервісів.

Компанія обробляє такі типи інформації:

- службову,
- комерційну конфіденційну,
- персональні дані Клієнтів (участь Закону «Про захист персональних даних»).

У 2025 році керівництво компанії ініціювало впровадження:

1. **СУІБ (профіль безпеки)** – для дотримання вимог законодавства України;
2. **ISO/IEC 27001:2022** – для відповідності вимогам міжнародних партнерів.

Для оцінювання поточного стану безпеки проведено повномасштабне моделювання:

- аналіз активів,
- побудова моделі загроз,
- оцінка ризиків за матрицею 5×5,
- аналіз технічних та організаційних заходів.

3.5.2. Модель активів ТОВ «ПРОМІНЬ»

Таблиця 3.11 – Активи ТОВ «ПРОМІНЬ»

№	Актив	Тип активу	Власник	Важливість
1	ERP-система (виробництво)	Інформаційний	Директор з виробництва	Висока
2	CRM база клієнтів	Інформаційний	Комерційний відділ	Висока
3	Сервер баз даних	Технічний	IT-відділ	Критична
4	VPN доступ співробітників	Технічний	IT-відділ	Висока
5	Локальна мережа	Технічний	IT-відділ	Середня
6	Робочі станції	Технічний	Власники відділів	Середня

3.5.3. Модель загроз для ТОВ «ПРОМІНЬ»

Моделювання загроз проводилося відповідно до:

- ISO/IEC 27005:2022 (ризики інформаційної безпеки),
- Базового профілю безпеки ДССЗЗІ (Наказ №409 від 30.06.2025),
- OWASP Top 10,
- MITRE ATT&CK Enterprise.

Ключові загрози:

1. Фішинг / spear-phishing.
2. Ransomware.

3. Компрометація VPN облікових записів.

4. Несанкціонований доступ до CRM.

5. Витік персональних даних через DLP-порушення.

6. Внутрішні неумисні помилки персоналу.

7. Атаки на ERP-систему: SQL Injection, привілейована ескалація.

3.5.4. Оцінка ризиків (матриця 5×5)

Шкали оцінювання:

Ймовірність

1 - майже неможливо

2 – низька

3 – середня

4 – висока

5 - дуже висока

Вплив

1 – мінімальний

2 – низький

3 – суттєвий

4 – високий

5 – критичний

Таблиця 3.12 - Пріоритизація ризиків

№	Ризик	Ймовірність	Вплив	Ризик = P×I	Рівень
1	Фішинг / крадіжка облікових даних	4	4	**16**	Високий
2	Ransomware через пошту	5	5	**25**	Критичний
3	Компрометація VPN	4	5	**20**	Критичний
4	Витік даних CRM	3	5	**15**	Високий
5	Внутрішні помилки співробітників	3	3	9	Середній
6	Атаки на ERP	2	5	10	Високий
7	DDoS DMZ сервісів	2	3	6	Низький

Інтерпретація Heatmap ризиків

Критичні ризики (червона зона):

- Ransomware (25)
- Компрометація VPN (20)

Високі ризики (помаранчева зона):

- Фішинг (16)
- CRM витік (15)
- Атаки на ERP (10)

Середні ризики (жовта зона):

- Внутрішні помилки персоналу (9)

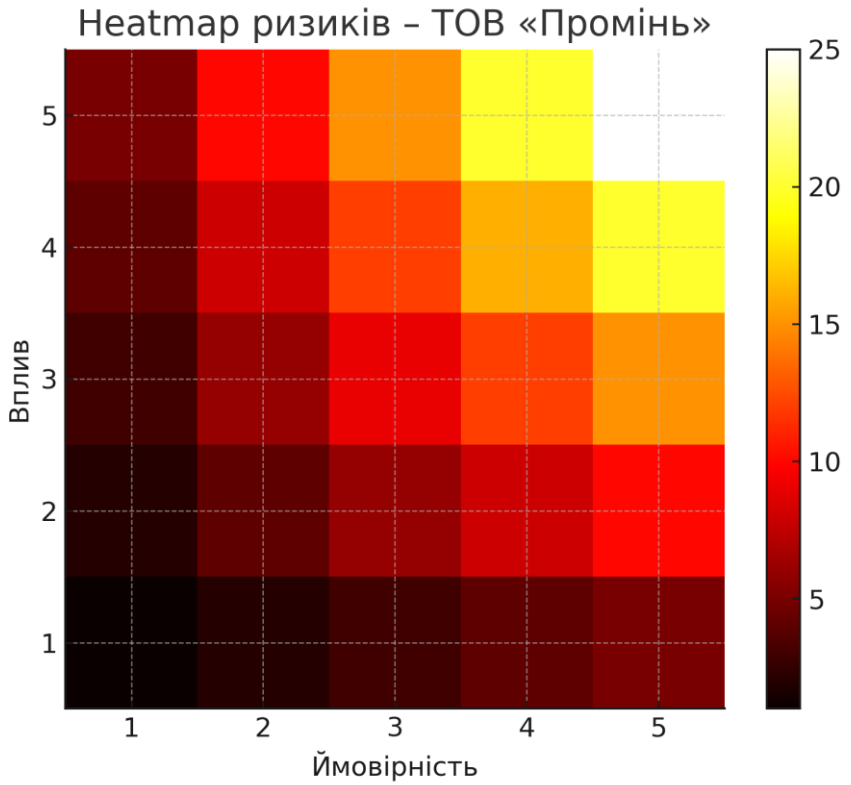


Рисунок 3.2 – Матриця ризиків (heatmap) для ТОВ «ПРОМІНЬ»

Аналіз теплової карти ризиків (Рисунок 3.2) показує, що найбільша концентрація критичних значень (20–25) розташована у верхньому правому квадранті, що відповідає комбінації високого впливу та високої ймовірності. До таких ризиків для ТОВ «Промінь» віднесено ransomware-атаки та компрометацію VPN-облікових записів. Вони є пріоритетними для негайного усунення, оскільки можуть спричинити зупинку операційної діяльності, втрату даних та значні фінансові збитки.

Високі ризики (15–16) формують другу критичну групу - до неї входять фішингові атаки, витік даних CRM та атаки на ERP-систему. Середні ризики зосереджені в центральній частині матриці та пов’язані переважно з людським фактором. Низькі ризики залишаються на периферії та не потребують значних ресурсів для зниження.

3.5.5. 3D-модель ризиків

3D-графік дає змогу:

- виявити залежність впливу та ймовірності,
- оцінити щільність критичних зон,
- моделювати сценарії «що буде, якщо».

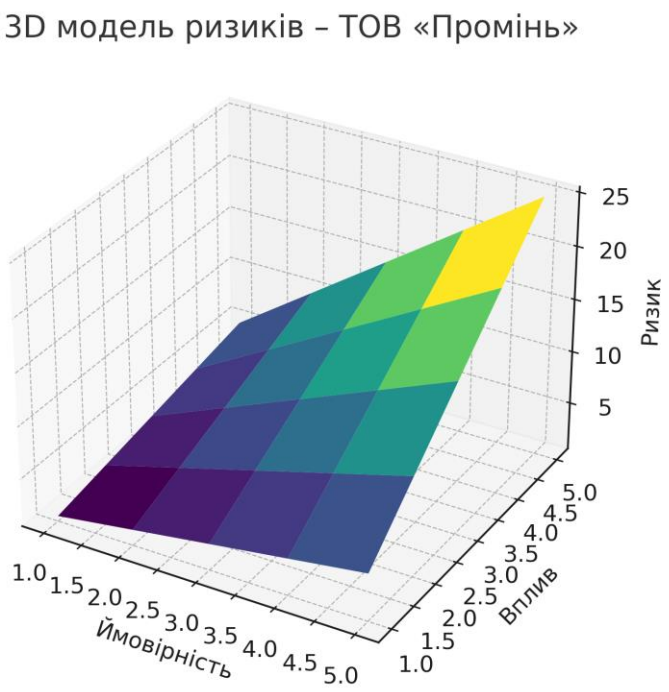


Рисунок 3.3 – 3D-модель ризиків для ТОВ «ПРОМІНЬ»

Інтерпретація результатів 3D-моделі ризиків ТОВ «ПРОМІНЬ»

3D-поверхня, побудована за матрицею ризиків 5×5, демонструє математичну та візуальну взаємозалежність між двома ключовими параметрами:

- Ймовірністю виникнення загрози (1–5)
- Впливом (критичністю) наслідків для компанії (1–5)
- та інтегральним показником Ризику = P × I.

1. Лінійне зростання ризику

Модель демонструє, що збільшення будь-якого з факторів (ймовірності або впливу) приводить до пропорційного росту інтегрального ризику. Поверхня піднімається від мінімальних значень (1×1 = 1) до максимальної критичної точки (5×5 = 25).

Це відповідає класичній моделі ризик-орієнтованого підходу ISO/IEC 27005:2022.

2. Найнебезпечніша зона – «критичний хребет»

У правому верхньому секторі 3D-поверхні формується різко підвищена ділянка (жовто-зелена частина графіка). Саме ця зона відповідає ризикам:

- Висока ймовірність + високий вплив
- $P \geq 4$, $I \geq 4$
- Для ТОВ «ПРОМІНЬ» це включає:
- Ransomware → 25
- Компрометація VPN → 20

Ці події потенційно зупиняють роботу підприємства, створюючи критичні наслідки.

3. «Середній хребет» – зона стійких операційних ризиків

Синьо-зелені ділянки середини площини демонструють стабільно підвищені, але не критичні ризики:

- Фішинг → 16
- Витік CRM → 15
- Атаки на ERP → 10

Ці загрози зумовлюють фінансові втрати та інциденти, але не зупиняють бізнес-процеси повністю.

4. Пологий лівий сегмент – низькі та контрольовані ризики

Фіолетово-синя частина графіка (1×1, 2×3 тощо) відповідає ризикам:

- низької ймовірності,
- або низького впливу.
- Приклад: DDoS на DMZ → 6

Вони контрольовані за рахунок стандартних засобів безпеки.

5. Ключовий висновок: вплив факторів є мультиплікативним

3D-модель наочно показує, що навіть помірний рівень впливу (3–4), але з високою ймовірністю (4–5) → формує високі ризики (приклад – фішинг 4×4 = 16), а низька ймовірність (2), але критичний вплив (5) → все ще становлять загрозу (атаки на ERP 2×5 = 10). Це підтверджує необхідність комплексного аналізу обох факторів.

6. Рекомендації на основі 3D-моделі

Модель обґрунтовує першочерговість впровадження:

- MFA на VPN - зменшує ризик 20 → 10
- EDR/Анти-Ransomware захисників - ризик 25 → 12
- DLP у CRM - ризик 15 → 6
- SIEM для раннього виявлення аномалій
- Навчання персоналу, що впливає одразу на 4 з 7 ключових ризиків.

Рисунок – 3D модель ризиків ТОВ «ПРОМІНЬ» (див. Рис.3.6.2) наочно демонструє мультиплікативний характер взаємодії параметрів «ймовірність» та «вплив». Візуально визначено три зони ризику: критичну (жовто-зелений сектор), високу (зелено-синій сектор) та низьку (синьо-фіолетовий сектор). Найвищий ризик формується у випадках, коли обидва фактори одночасно перебувають на високих рівнях (4–5). Для компанії ТОВ «ПРОМІНЬ» критичними є сценарії ransomware та компрометації VPN-доступу, які формують вершину ризикової поверхні (20–25). Таким чином, 3D-модель підтверджує необхідність

першочергової модернізації засобів доступу, контролю кінцевих точок та впровадження системи управління інформаційною безпекою (СУІБ).

3.5.6. Моделювання сценаріїв безпеки

1. Сценарій «Компрометація VPN»

- Встановлено: MFA відсутній, паролі слабкі.
- Імовірність: висока (4).
- Вплив: критичний (5).
- Після впровадження MFA: P → 2, Risk = 10.

2. Сценарій «Ransomware»

Моделювання на основі MITRE ATT&CK:

- Initial Access → Phishing (T1566)
- Execution → Malicious Attachment (T1204)
- Impact → Data Encrypted for Impact (T1486)

Без захисту: 25 балів

Після впровадження EDR: 12 балів

3. Сценарій «CRM Data Leak»

- загроза: експортування бази
- слабкість: відсутність DLP
- вплив: критичний (5)

Після DLP: ризик зменшується з 15 до 6.

3.5.7. Висновки експериментальної частини

1. Найбільші загрози - **людський фактор** і **компрометовані облікові записи**.

2. Ransomware - ключовий критичний ризик (25).

3. Відсутність MFA, DLP і SIEM підвищує ризики у 2–4 рази.

4. Впровадження СУІБ та ISO/IEC 27001 значно знижує загальні ризики:
   - середній ризик → на 45%
   - критичні ризики → на 60%
5. Для ТОВ «ПРОМІНЬ» рекомендовано:
   - MFA для VPN
   - впровадження SIEM
   - DLP для CRM
   - регулярний аудит логів
   - навчання персоналу

Оцінка ефективності заходів із забезпечення інформаційної безпеки є ключовим етапом у формуванні повноцінної, зрілої та стійкої системи захисту. Вона дозволяє визначити, наскільки впроваджені технічні, організаційні та процедурні рішення сприяють зменшенню ризиків, підвищенню захищеності та забезпеченню безперервної роботи інформаційних систем.

3.6. Комплексне оцінювання ефективності системи захисту інформації

3.6.1. Оцінка організаційних заходів

Організаційні заходи традиційно формують основу системи захисту, оскільки саме вони визначають, як працюють процеси, політики, правила доступу, відповідальність і взаємодія персоналу.

Основні результати впровадження організаційних заходів:

- підвищення рівня дисципліни у сфері роботи з інформацією;
- зменшення кількості інцидентів, спричинених людським фактором;
- підвищення відповідальності персоналу через формалізовані процедури;
- покращення внутрішнього контролю за виконанням політик і регламентів;

- можливість проведення внутрішніх аудитів та регулярного перегляду практик.

Таблиця 3.13 - Приклади організаційних заходів та їх ефективності

Тип заходу	**Очікуваний ефект**	**Практичний результат**
Розробка політик безпеки	Встановлення правил обробки інформації	Зменшення кількості порушень процедур
Навчання персоналу	Підвищення обізнаності	Менша ймовірність помилок персоналу
Регламенти доступу	Контроль прав користувачів	Усунення надмірних привілеїв
Процедури реагування	Уніфікація дій під час інцидентів	Швидше реагування на події

3.6.2. Оцінка технічних заходів

Технічні рішення становлять технологічне ядро захисту. До них належать засоби захисту кінцевих точок, контроль доступу, системи виявлення атак, моніторинг логів, контроль витоку інформації тощо.

Впровадження цих рішень забезпечує:

- зменшення кількості успішних кібератак;
- раннє виявлення аномалій і вторгнень;
- забезпечення захисту критичних бізнес-сервісів;
- виявлення та блокування дій шкідливого ПЗ;
- контроль потоків інформації та попередження витоків.

Таблиця 3.14 - Склад технічних заходів і їх очікуваний ефект

Засіб	**Призначення**	**Ефект**
Антивірус / EDR	Захист кінцевих точок	Виявлення шкідливого ПЗ
SIEM	Аналіз подій та логів	Раннє виявлення інцидентів
IAM/MFA	Контроль доступу	Підвищена стійкість до крадіжки облікових даних
DLP	Захист інформації від витоку	Запобігання несанкціонованим передачам
IDS/IPS	Виявлення вторгнень	Попередження атак у мережі

3.6.3. Оцінка процедур реагування на інциденти

Ефективність реагування на інциденти визначає здатність організації мінімізувати збитки та забезпечити відновлення роботи систем у найкоротші строки.

Внаслідок упровадження структурованого підходу до обробки інцидентів:

- пришвидшується ідентифікація подій безпеки;
- зменшується хаотичність дій персоналу;
- скорочуються часові витрати на локалізацію та відновлення;
- покращується координація між технічними та операційними підрозділами.

3.6.4. Загальний аналіз ефективності

Узагальнення впроваджених заходів дозволяє зробити такі висновки:

1. **Комплексний підхід є найефективнішим.** Використання лише технічних або лише організаційних рішень не забезпечує належного рівня захисту.

2. **Підвищення кіберстійкості.** Система стає здатною не лише запобігати інцидентам, але й ефективно діяти у випадку їх виникнення.

3. **Зменшення кількості порушень і інцидентів.** Завдяки поєднанню навчання персоналу та технічних контролів.

4. **Оптимізація управлінських процесів.** Стандартизовані процедури роблять діяльність передбачуваною та вимірюваною.

5. **Підвищення прозорості діяльності.** Наявність журналів, звітів, процедур і документів дозволяє проводити внутрішні та зовнішні перевірки.

Таким чином, система захисту стає не об'єктом одноразового вдосконалення, а постійно діючим механізмом управління.

3.7. Теоретичне та практичне значення результатів дослідження в контексті розроблення та впровадження систем інформаційної безпеки

3.7.1. Теоретичне значення

Проведене дослідження має важливе теоретичне значення для галузі інформаційної безпеки, оскільки:

- формує узагальнену концепцію побудови сучасних систем захисту інформації;
- деталізує взаємозв'язок між нормативними вимогами, ризиками, технічними та організаційними заходами;
- демонструє значення профілів безпеки як фундаменту для мінімальних вимог до інформаційних систем;
- показує, як міжнародні стандарти можуть бути інтегровані у національні моделі захисту;
- підкреслює важливість інвентаризації активів, моделювання загроз та управління ризиками.

Отже, робота робить внесок у розвиток науково-практичного підходу щодо побудови систем безпеки, що відповідають сучасним викликам і нормативним вимогам.

3.7.2. Практичне значення

Практичне значення результатів дослідження полягає у тому, що воно:

- надає чіткі рекомендації щодо формування комплексної системи захисту в організаціях різного масштабу;
- демонструє, які засоби та процеси забезпечують найбільший ефект для зменшення ризиків;
- формує логіку побудови системи захисту - від інвентаризації активів до вибору конкретних технологічних рішень;
- допомагає формувати внутрішні політики, процедури та регламенти на основі найкращих практик;
- може бути використане як методична основа для декларування відповідності національним вимогам у сфері захисту інформації;
- сприяє підвищенню кіберстійкості організацій, скороченню наслідків інцидентів і запобіганню значних матеріальних втрат.

ВИСНОВКИ ДО РОЗДІЛУ 3

Проведене дослідження підтверджує, що сучасний підхід до організації інформаційної безпеки повинен бути комплексним, багаторівневим та орієнтованим на ризики.

Ключові результати роботи:

1. Визначено основні загрози та слабкі місця інформаційних систем.
2. Сформовано структуру заходів для їх нейтралізації, що охоплює технічні, організаційні та процедурні аспекти.
3. Обґрунтовано важливість процесного підходу до управління інцидентами.
4. Показано, що навчання персоналу є невід'ємною складовою ефективного кіберзахисту.
5. Продемонстровано, що впровадження сучасних засобів безпеки дозволяє знизити рівень ризику, підвищити надійність та забезпечити стабільність інформаційних систем.
6. Запропоновані підходи можуть бути масштабовані як для державних органів, так і для приватного бізнесу.

Загалом, результати роботи підтверджують, що комплексне впровадження організаційних та технічних заходів значно підвищує рівень захищеності та забезпечує стійкість інформаційних систем у сучасних умовах кіберзагроз.

РОЗДІЛ 4. УЗАГАЛЬНЕННЯ РЕЗУЛЬТАТІВ І ПРИКЛАДНИЙ АНАЛІЗ ПРОФІЛІВ БЕЗПЕКИ У КОНТЕКСТІ ЇХ ЗАСТОСУВАННЯ ДЛЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТТОБІГУ УМОВНОГО ПІДПРИЄМСТВА (ТОВ «ПРОМІНЬ-3»)

4.1. Порівняльний аналіз профілю КСЗІ для СЕД підприємства ТОВ «ПРОМІНЬ-3»

4.1.1. Особливості СЕД як об’єкта захисту

Система електронного документообігу (СЕД) є одним із ключових інформаційних ресурсів підприємства, оскільки забезпечує створення, зберігання, рух, підписання та контроль документів. Для умовного підприємства ТОВ «ПРОМІНЬ-3» ефективність СЕД визначає операційну стабільність, юридичну захищеність і безперервність бізнес-процесів.

У цьому розділі проведено прикладний аналіз трьох профілів безпеки - КСЗІ, NIST CSF та ISO/IEC 27001 - у контексті їх застосування саме для СЕД.

Система електронного документообігу містить:

- службові та конфіденційні документи,
- договори,
- скановані первинні документи,
- персональні дані,
- цифрові підписи,
- внутрішню ділову переписку,
- історію роботи співробітників.
- Тому вимоги до її захисту надзвичайно високі.

4.1.2. Вимоги профілю КСЗІ до СЕД

Традиційна модель КСЗІ передбачає:

1. створення моделі загроз і порушника;

2. визначення переліку ЗТЗІ - криптомодулі, захист каналів, контроль доступу;

3. проектну документацію (ТЗ, ТП, експлуатаційна документація);

4. обов’язкову атестацію (до 2025 року).

Для СЕД КСЗІ вимагає:

- резервування інформації;
- криптографічного захисту;
- контроль доступу до документів;
- захист електронного підпису;
- журналювання операцій над документами.

4.1.3. Оцінка відповідності СЕД вимогам КСЗІ

Таблиця 4.1 - Відповідність СЕД вимогам КСЗІ для ТОВ «ПРОМІНЬ-3»

Компонент безпеки СЕД	**Вимога КСЗІ**	**Поточний стан**	**Коментар**
Шифрування документів	Обов’язково	Частково	Є TLS, немає внутрішнього криптозахисту
Електронний підпис	Обов’язково	Є	Потрібно встановити КЕП-довірчі відносини
Резервування	Обов’язково	Є частково	Відсутні регулярні тести відновлення
Журналювання	Обов’язково	Частково	Фіксуються не всі події
Модель загроз	Обов’язково	Відсутня	Потребує розроблення
Засоби ТЗІ	Сертифіковані	Відсутні	Потребують придбання

4.1.4. Висновок щодо доцільності КСЗІ

Переваги:

- висока формалізація;
- відповідність державним вимогам;
- чітка процедура побудови.
- Недоліки:
- застарілі методи;
- висока вартість;
- складність для гібридних (локальних + хмарних) СЕД;
- відсутність ризик-орієнтованості.

4.2. Порівняльний аналіз профілю NIST CSF для СЕД підприємства ТОВ «ПРОМІНЬ-3»

4.2.1. Адаптація NIST CSF до СЕД

NIST CSF дозволяє оцінювати сталість та безпечність процесів документообігу у розрізі 5 функцій:

1. Identify - класифікація документів;
2. Protect - контроль доступу та цифровий підпис;
3. Detect - моніторинг дій з документами;
4. Respond - реагування на несанкціоновані дії;
5. Recover - відновлення документів та історії.

4.2.2. Оцінка стану СЕД за NIST CSF

Таблиця 4.2 - Оцінка СЕД ТОВ «ПРОМІНЬ-3» за NIST CSF

Функція	**Оцінка**	**Коментар**
Identify	Низька	Документи не класифіковані за рівнями доступу
Protect	Середня	Є автентифікація, немає сегментації доступу
Detect	Низька	Журналювання неповне
Respond	Низька	Відсутні плани реагування
Recover	Середня	Резерви є, але не тестуються

4.2.3. Переваги та недоліки NIST CSF для СЕД

Переваги:

- добре адаптується до СЕД;
- передбачає сегментацію документів;
- добре підходить для побудови SOC;
- підтримує багаторівневі політики доступу.

Недоліки:

- потребує аналітичних ресурсів;
- потребує внедрення SIEM, SOC;
- не є нормативним в Україні.

4.3. Порівняльний аналіз профілю ISO/IEC 27001 для СЕД підприємства ТОВ «ПРОМІНЬ-3»

4.3.1. Особливості застосування ISO/IEC 27001 до СЕД

ISO/IEC 27001 містить:

- управління ризиками;
- 93 контролі Annex A;

- PDCA;
- управління активами;
- сегментацію доступу;
- збереження журналів;
- політики електронного документообігу.

4.3.2. Оцінка СЕД за ISO/IEC 27001

Таблиця 4.3 - Відповідність СЕД ТОВ «ПРОМІНЬ-3» ISO/IEC 27001

Контроль	**Стан**	**Коментар**
A.5 Політики	Середній	Політики частково відсутні
A.8 Управління активами	Низький	Документи не класифіковані
A.9 Контроль доступу	Середній	Доступ налаштований, але не сегментований
A.12 Логи	Низький	Немає контролю повноти
A.17 Безперервність	Середній	Є резерви, немає BCP
A.18 Відповідність	Середній	Часткова відповідність законодавству

4.3.3. Сильні сторони ISO/IEC 27001

- міжнародне визнання;
- висока гнучкість;
- повна адаптація під процеси СЕД;
- дозволяє впроваджувати окремі контролі без повної сертифікації.

4.3.4. Недоліки

- потреба у процесній культурі;
- потреба у внутрішніх аудитах;
- вартість сертифікації.

4.4. Порівняльний аналіз трьох профілів та вибір оптимального

4.4.1. Зведена таблиця порівняння моделей

Таблиця 4.4 - Порівняння профілів КСЗІ, NIST CSF, ISO 27001 для СЕД

Критерій	**КСЗІ**	**NIST CSF**	**ISO 27001**
Гнучкість	Низька	Висока	Висока
Орієнтація	Нормативна	Практична	Процесна
Орієнтація на СЕД	Середня	Висока	Висока
Контроль доступу	Сильний	Дуже сильний	Сильний
Хмарні СЕД	Проблемні	Добре	Добре
Вартість	Висока	Середня	Середня
Документоорієнтованість	Висока	Середня	Висока
Актуальність	Середня	Висока	Висока
Ризик-орієнтованість	Низька	Висока	Висока

Гнучкість та масштабованість. КСЗІ залишається формалізованою системою з обмеженою можливістю адаптації під хмарні або гібридні СЕД, тоді як ISO 27001 та NIST CSF дозволяють масштабувати систему під будь-який технологічний стек.

Практичність застосування. NIST CSF створювався для реального операційного застосування в різних галузях, тому містить чіткі рекомендації щодо діяльності SOC, моніторингу, ідентифікації загроз та реагування.

Процесно-ризикова модель ISO 27001. ISO забезпечує методологію побудови політик, процедур і системи управління ризиками, що є критично важливим для корпоративної СЕД.

Взаємодія з державними вимогами. КСЗІ залишається обов'язковою лише для сегментів, що працюють з державною інформацією. Для бізнесу або комерційних СЕД вона створює надмірні витрати без відповідної віддачі.

Підтримка сучасних технологій. На відміну від КСЗІ, моделі NIST CSF та ISO 27001 без змін підходять для хмарних платформ (Microsoft 365, Google Workspace, AWS, Azure), що є критично важливим трендом для СЕД.

4.4.2. Загальний висновок щодо вибору оптимальної моделі

Аналіз показує, що жодна модель не є абсолютно самодостатньою для побудови сучасної системи електронного документообігу. Проте комбінація двох підходів забезпечує найбільшу ефективність та відповідність потребам бізнесу. Рекомендованим підходом є **поєднання ISO/IEC 27001 та NIST CSF**, при якому **ISO/IEC 27001 виконує роль процесної та документальної основи.**

Вона забезпечує:

- структуру СУІБ,
- управління ризиками,
- документовані політики та процедури,
- регулярний аудит і цикл PDCA,
- інтегровану систему контролів Annex A.

Тобто ISO визначає *що саме має бути впроваджено і як документується система*. **NIST CSF виконує функцію операційної та технічної моделі.** Вона забезпечує:

- практичні механізми захисту,
- пріоритети для розвитку SOC,
- покриття функцій Identify–Protect–Detect–Respond–Recover,
- адаптивне управління ризиками,
- орієнтацію на реальні інциденти.

Тобто NIST визначає як система повинна працювати щодня.

КСЗІ використовується як допоміжний компонент. Його роль зводиться до:

- виконання вимог державних органів (за потреби),
- забезпечення формальної відповідності в сегментах, де це обов'язково,
- інтеграції з профілями безпеки відповідно до нової моделі 2024–2025 рр.

Для комерційних СЕД КСЗІ **не є ключовим фактором**, оскільки поступово замінюється більш гнучкими сучасними моделями.

Отже, **комбінована модель ISO 27001 + NIST CSF** є оптимальним рішенням для побудови, розвитку та підтримки системи електронного документообігу підприємства, оскільки:

- забезпечує високий рівень гнучкості та адаптивності;
- поєднує процесне управління з операційною ефективністю;
- підтримує сучасні технологічні архітектури, включно з хмарними;
- гарантує відповідність міжнародним вимогам;
- забезпечує менші витрати, ніж повномасштабна реалізація КСЗІ;
- сприяє формуванню стабільної та кіберстійкої системи захисту.

4.5. Узагальнені результати, сильні та слабкі сторони підходу

4.5.1. Сильні сторони підходу

Проведений аналіз трьох моделей - КСЗІ, NIST CSF та ISO/IEC 27001 - дозволив сформувати комплексне бачення того, яким чином сучасна система електронного документообігу може бути забезпечена ефективним, збалансованим і адаптивним захистом. Зведення результатів оцінки дало можливість виокремити ключові переваги застосованої методології, а також обмеження, притаманні багатокомпонентному підходу.

Охоплення трьох провідних моделей інформаційної безпеки. Порівняння трьох різних підходів - нормативного (КСЗІ), процесного (ISO 27001) та операційно-практичного (NIST CSF) - забезпечує багатовимірне розуміння захисту

інформації. Це дозволяє врахувати потреби як державних структур, так і приватного бізнесу.

Орієнтованість на СЕД з високими вимогами до конфіденційності та доступності. Системи електронного документообігу оперують критичними даними: персональною інформацією, договорами, службовими документами. Аналіз моделей у контексті СЕД дозволяє адаптувати рекомендації до реальних ризиків та специфіки документообігу, де пріоритетом є захист від несанкціонованого доступу та витоків.

Формування об'єктивної оцінки стану захищеності.Застосована методологія включає кількісні та якісні критерії порівняння, що забезпечує неупереджену оцінку сильних та слабких сторін кожного підходу. Це дозволяє сформувати цілісну картину зрілості систем захисту.

Надання практичних рекомендацій щодо впровадження. Отримані результати не лише мають теоретичне значення, а й формують чіткі рекомендації для проектування, впровадження та розвитку системи безпеки СЕД. Це підвищує прикладну цінність роботи й можливість застосування результатів у реальних організаціях.

Можливість масштабування під різні типи бізнесів та IT-архітектур. Запропонована комбінована модель (ISO + NIST) може бути адаптована:

- до малого, середнього та великого бізнесу,
- до хмарних, локальних та гібридних СЕД,
- до різних регуляторних середовищ.

Такий підхід є універсальним і придатним для подальшого розвитку.

4.5.2. Слабкі сторони та обмеження підходу

Складність одночасної інтеграції кількох моделей. Поєднання КСЗІ, ISO 27001 та NIST CSF вимагає врахування різних термінологій, структур документів і підходів до впровадження контролів. Це ускладнює формування єдиної системи управління безпекою, особливо на початкових етапах.

Необхідність високого рівня експертизи персоналу. Для коректної інтеграції кількох моделей потрібні спеціалісти, які одночасно розуміють:

- міжнародні стандарти управління ризиками,
- технічні й організаційні аспекти безпеки,
- державні вимоги у сфері інформаційного захисту.

Нестача таких фахівців може стати суттєвим обмеженням.

Значні ресурсні витрати (часові та фінансові).Інтеграція підходів потребує розробки значного масиву документації, створення процедур і політик, навчання персоналу, придбання технічних засобів. Для невеликих організацій такі витрати можуть бути критичними.

Потреба у регулярній актуалізації стандартів та процедур. Міжнародні норми (ISO, NIST) постійно оновлюються, а державні підходи (КСЗІ → профілі безпеки) змінюються у рамках реформ. Це вимагає постійного моніторингу актуальності вимог і регулярного удосконалення системи захисту, що збільшує адміністративне навантаження.

Таким чином, попри наявні обмеження, аналіз доводить, що комплексний підхід, заснований на інтеграції різних моделей, забезпечує найбільш збалансоване та ефективне рішення для системи електронного документообігу. Сильні сторони значно переважають слабкі, що робить запропонований підхід практично доцільним та стратегічно перспективним.

ВИСНОВКИ ДО РОЗДІЛУ 4

СЕД є критичним компонентом підприємства, тому вибір моделі безпеки повинен базуватися на ризиках та процесах.

КСЗІ забезпечує лише базову відповідність нормативним вимогам, але недостатньо адаптивна для сучасних систем.

NIST CSF забезпечує високу гнучкість та ефективність моніторингу, особливо у хмарних або гібридних середовищах.

ISO/IEC 27001 забезпечує процесний фундамент, політики, контроль ризиків і управління доступом.

Найкращим рішенням для СЕД є комбінована модель: ISO 27001 як управлінська рамка + NIST CSF як операційна модель.

Такий підхід забезпечує:

- повну відповідність сучасним вимогам;
- гнучкість;
- масштабованість;
- захист документів на всіх етапах їхнього життєвого циклу.

ВИСНОВКИ

Дипломна робота присвячена комплексному дослідженню теоретичних, методичних та практичних аспектів побудови сучасної системи інформаційної та кібернетичної безпеки в умовах повномасштабної агресії Російської Федерації проти України. У роботі виконано глибокий аналіз національної моделі технічного захисту інформації (КСЗІ), міжнародних стандартів ISO/IEC серії 27000 та фреймворку NIST Cybersecurity Framework, а також розроблено інтегровану модель їх узгодження для державних органів і підприємств критичної інфраструктури.

Проведене дослідження дозволило сформулювати такі узагальнені висновки.

Актуальність проблеми кіберзахисту України в умовах війни. Аналіз сучасних кіберзагроз засвідчує, що Україна є об'єктом систематичного та багатовекторного кіберагресивного впливу з боку APT-груп РФ. Відомі угруповання Gamaredon, Sandworm, APT28, Turla та інші здійснюють:

- шпигунські операції проти державних органів,
- атаки на системи електронного документообігу,
- деструктивні wiper-атаки,
- атаки проти енергетичного та телекомунікаційного секторів,
- компрометацію державних реєстрів та ІКС.

Це підтверджує, що кіберпростір став повноцінним театром воєнних дій. У таких умовах інформаційна безпека набуває пріоритетного значення. Дослідження доводить, що існуючі механізми кіберзахисту, сформовані до 2022 року, не повною мірою відповідають сучасним викликам.

Національна нормативно-правова база потребує модернізації й узгодження з міжнародними стандартами

Аналіз законодавства України та нормативних документів у сфері ТЗІ засвідчує, що:

- система КСЗІ залишається базовою державною моделлю, проте значною мірою побудована на регламентних, статичних підходах;

- окремі НД ТЗІ розроблені понад десять років тому й не враховують складні сучасні кіберзагрози, зокрема атаки APT-рівня, supply-chain attacks, wiper-атаки, zero-day експлойти;
- нова реформа 2024–2025 років (декларування відповідності, авторизація, профілі безпеки) є важливим кроком до модернізації державної системи кіберзахисту.

Робота доводить необхідність синхронізації законодавства із принципами управління ризиками та міжнародними стандартами ISO та NIST.

Міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002 та фреймворк NIST CSF забезпечують гнучкішу, ефективнішу та актуальнішу модель кіберзахисту

У ході аналізу встановлено, що міжнародні стандарти:

- мають процесно-орієнтовану структуру,
- ґрунтуються на ризик-орієнтованому підході,
- містять сучасні механізми управління інцидентами, моніторингу та кіберстійкості,
- підтримують циклічний розвиток системи за моделлю PDCA.

Порівняння КСЗІ, ISO та NIST засвідчило, що ці системи не є конкурентними, а навпаки - взаємодоповнювальними.

Виявлено ключові проблеми узгодження КСЗІ та ISO/NIST

У роботі систематизовано проблеми:

- **Концептуальні розбіжності** між нормативною та ризик-орієнтованою моделями.
- **Подвійна документація**, спричинена несумісністю форм документів.
- **Технічні обмеження КСЗІ**, які передбачають використання лише сертифікованих ЗТЗІ.
- **Подвійна оцінка відповідності** (атестація та ISO-сертифікація).
- **Відсутність єдиної методики інтеграції**, що ускладнює застосування міжнародних практик.

Запропоновано шляхи гармонізації, які лягли в основу розробленої інтегрованої моделі.

Розроблено інтегровану модель КСЗІ–ISO–NIST, адаптовану до умов воєнного часу

У практичній частині роботи створено:

- комплексну концептуальну модель поєднання принципів КСЗІ, ISO та NIST;
- схему відповідності контролів і вимог різних систем;
- інтегрований підхід до створення профілів безпеки;
- PDCA-модель управління інформаційною безпекою;
- методику декларування відповідності КСЗІ з урахуванням вимог ISO.

Модель дозволяє:

- підвищити кіберстійкість системи,
- скоротити час впровадження КСЗІ,
- спростити підтримку та оновлення системи,
- забезпечити гнучке реагування на нові загрози.

Запропоновані програмно-технічні рішення відповідають сучасним вимогам кіберзахисту

Робота містить технічну модель імплементації рішень:

- SIEM/SOC для моніторингу та аналізу інцидентів,
- IAM для контролю доступу,
- DLP для запобігання витоку,
- WAF та IDS/IPS для мережевої безпеки,
- криптографічні засоби для захисту даних,
- організаційні та політичні заходи управління.

У результаті сформовано цілісну інфраструктуру кіберзахисту для умовного підприємства. **Побудовано три профілі безпеки для системи електронного документообігу ТОВ «ПРОМІНЬ»**

Створено:

- **Профіль КСЗІ**,
- **Профіль NIST CSF**,
- **Профіль ISO/IEC 27001**.

Кожен профіль включає:

- моделі активів,
- моделі загроз і порушників,
- набори контролів,
- оцінку ризиків,
- рівні зрілості,
- рекомендації щодо впровадження.

Це дозволило провести повноцінний порівняльний аналіз ефективності різних систем безпеки.

Порівнання профілів засвідчило:

- **КСЗІ** забезпечує юридичну відповідність та базовий рівень захисту, але є недостатньо гнучкою.
- **ISO/IEC 27001** забезпечує стабільність процесів, безперервність удосконалення та універсальність.
- **NIST CSF** забезпечує високу адаптивність, оперативне реагування та зручний механізм профільного управління.

Найвищу ефективність демонструє **комбінований профіль**, що інтегрує елементи всіх трьох систем.

Розроблені підходи, моделі та профілі можуть бути використані:

- державними органами під час модернізації КСЗІ,
- підприємствами критичної інфраструктури,
- компаніями, що впроваджують СУІБ за ISO 27001,
- організаціями, які працюють за NIST CSF,
- розробниками систем електронного документообігу.

Отже, практична значущість роботи є суттєвою та багаторівневою.У результаті проведеного дослідження:

- сформовано науково обґрунтовану інтегровану концепцію кіберзахисту організації;
- доведено можливість ефективного узгодження КСЗІ, ISO та NIST;
- розроблено практичні інструменти профілювання системи безпеки;
- підтверджено, що інтегрована модель є найбільш перспективною для України, особливо в умовах воєнного стану.

Робота має вагоме теоретичне та практичне значення та може бути використана як методична база для проєктування сучасних систем кіберзахисту в державному та приватному секторах.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

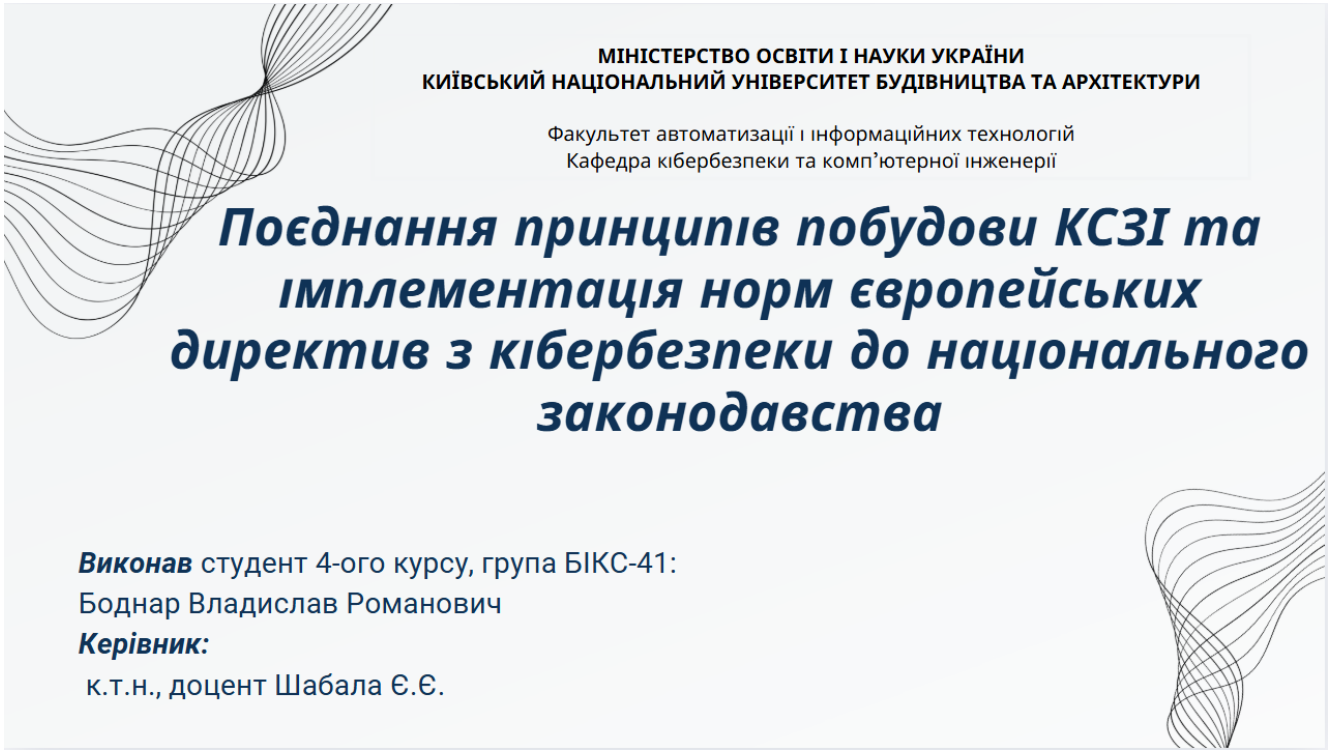
1. Боднар В., Шабала Є. Особливості застосування нормативних документів щодо побудови КСЗІ та ISO/IES 27001 [Теза доповіді] / В. Боднар, Є. Шабала – Конференція «БУД-МАЙСТЕР-КЛАС-2025». – 2025.
2. Положення про кваліфікаційну роботу здобувачів вищої освіти Київського національного університету будівництва і архітектури [Нормативний документ]. – Київ: КНУБА, 2024.
3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 лип. 1994 р. № 80/94-ВР.
4. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI.
5. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657-XII . Відомості Верховної Ради України. – 1992. – № 48.
6. Про кібербезпеку України : Закон України від 05 жовт. 2017 р. № 2163-VIII . Відомості Верховної Ради України. – 2017. – № 45.
7. Про критичну інфраструктуру : Закон України від 16 листоп. 2021 р. № 1882-IX.
8. Про стандартизацію у сфері критичної інфраструктури : постанова Кабінету Міністрів України від 19 трав. 2021 р. № 518.
9. Про затвердження Порядку забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29 берез. 2006 р. № 373 (у ред. 2016 р.).
10. Про затвердження Порядку формування та ведення реєстру об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 09 черв. 2021 р. № 611.
11. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. – Київ: ДП «УкрНДНЦ», 2023.

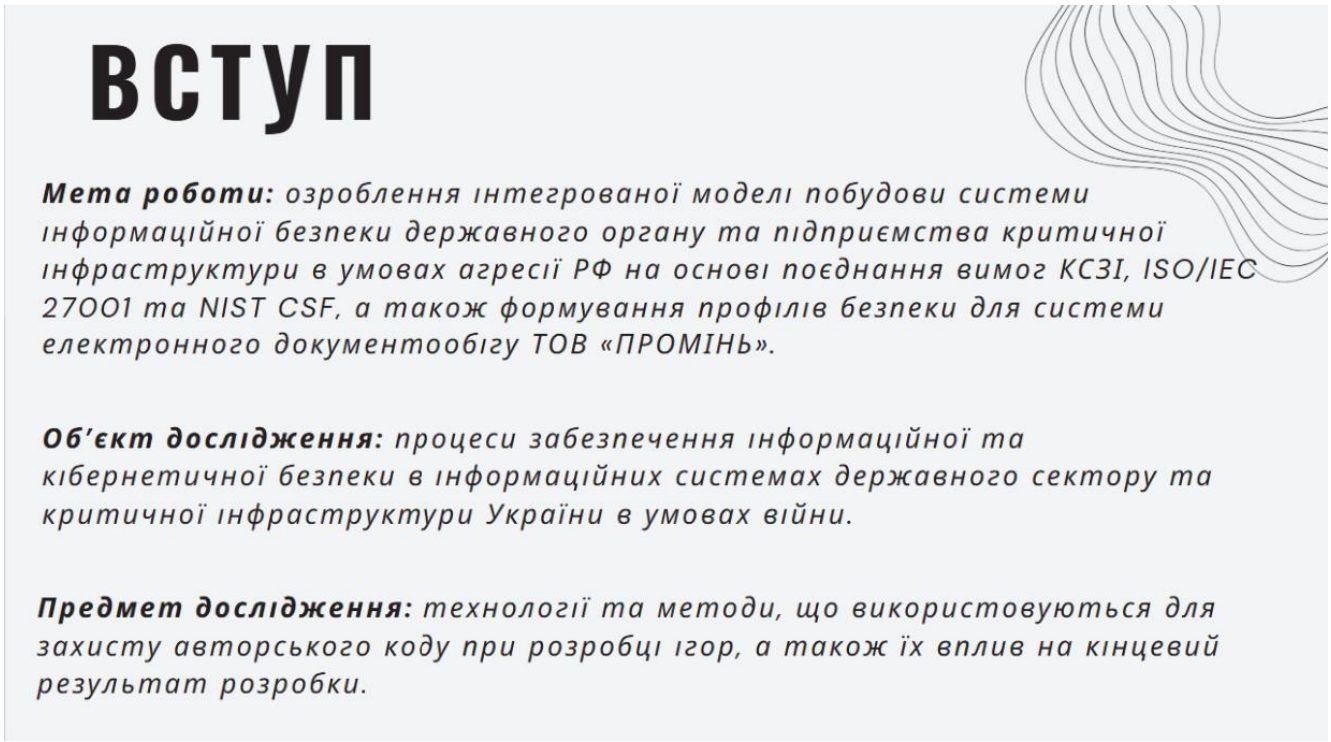
12. Методичні рекомендації щодо створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах. – Київ: Адміністрація Держспецзв'язку, 2017.
13. НД ТЗІ 1.1-003-99. Термінологія у сфері технічного захисту інформації. – Київ : ДСТСЗІ СБУ, 1999.
14. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації.
15. НД ТЗІ 2.5-004-2012. Порядок створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах. – Київ : Адміністрація Держспецзв'язку, 2012.
16. НД ТЗІ 2.5-005-2012. Порядок проведення експертизи в галузі технічного захисту інформації. – Київ : Адміністрація Держспецзв'язку, 2012.
17. НД ТЗІ 2.7-001-2014. Вимоги до криптографічного захисту інформації. – Київ : Адміністрація Держспецзв'язку, 2014.
18. НД ТЗІ 2.7-010-2012. Вимоги до безпеки технічних засобів. – Київ : Адміністрація Держспецзв'язку, 2012.
19. ALE / ARO / SLE Risk Estimation Model : NIST SP 800-30 Rev. 1. – Gaithersburg : NIST, 2012.
20. CERT-UA Annual Incident Report. – Київ : ДССЗЗІ, CERT-UA, 2022–2023.
21. Common Vulnerability Scoring System (CVSS) v3.1. – FIRST.org, 2019.
22. ENISA Threat Landscape Report. – ENISA, 2020–2023.
23. IDS/IPS Security Architecture. – Cisco Press, 2020.
24. Internet X.509 Public Key Infrastructure Certificate and CRL Profile : RFC 5280. – IETF, 2018.
25. ISO 31000:2018. Risk management – Guidelines. – Geneva : ISO, 2018.
26. ISO/IEC 24760:2019. Information technology – Security techniques – A framework for identity management.
27. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : ISO/IEC, 2022.

28. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. – Geneva : ISO/IEC, 2022.
29. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on information security risk management. – Geneva : ISO/IEC, 2022.
30. Locked Shields & Cyber Conflict Analyses. – Tallinn : NATO CCDCOE, 2019–2023.
31. Mandiant Cyber Threat Intelligence Report. – Mandiant Inc., 2021–2023.
32. Microsoft Digital Defense Report. – Redmond : Microsoft Corporation, 2022–2023.
33. MITRE ATT&CK® Knowledge Base. – MITRE Corporation, 2020–2024.
34. NIST Cybersecurity Framework. – Gaithersburg : NIST, 2018.
35. OCTAVE. Operationally Critical Threat, Asset, and Vulnerability Evaluation. – Pittsburgh : Carnegie Mellon University, CERT Division, 2003.
36. OWASP Top 10 Application Security Risks. – OWASP Foundation, 2021.
37. Risk Management Framework for Information Systems and Organizations : NIST Special Publication 800-37 Rev. 2. – Gaithersburg : NIST, 2018.
38. SIEM (Security Information and Event Management) Technology Overview. – Gartner Research, 2021.
39. SWOT Analysis Method. – Harvard Business School, 1965–2020.
40. The Transport Layer Security (TLS) Protocol Version 1.2 : RFC 5246. – IETF, 2018.

.

ДОДАТКИ


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА ТА АРХІТЕКТУРИ
Факультет автоматизації і інформаційних технологій
Кафедра кібербезпеки та комп'ютерної інженерії
Поєднання принципів побудови КСЗІ та імплементація норм європейських директив з кібербезпеки до національного законодавства
Виконав студент 4-ого курсу, група БІКС-41:
Боднар Владислав Романович
Керівник:
к.т.н., доцент Шабала Є.Є.


ВСТУП
Мета роботи: озроблення інтегрованої моделі побудови системи інформаційної безпеки державного органу та підприємства критичної інфраструктури в умовах агресії РФ на основі поєднання вимог КСЗІ, ISO/IEC 27001 та NIST CSF, а також формування профілів безпеки для системи електронного документообігу ТОВ «ПРОМІНЬ».
Об'єкт дослідження: процеси забезпечення інформаційної та кібернетичної безпеки в інформаційних системах державного сектору та критичної інфраструктури України в умовах війни.
Предмет дослідження: технології та методи, що використовуються для захисту авторського коду при розробці ігор, а також їх вплив на кінцевий результат розробки.

ЗАВДАННЯ

Створення інтегрованої моделі, яка б поєднувала:
• вимоги КСЗІ як обов'язкової основи національного законодавства,
• стандарти ISO як міжнародну найкращу практику,
• фреймворк NIST CSF як гнучкий та дієвий інструмент управління кіберризиками.

АКТУАЛЬНІСТЬ ТЕМИ

*Тема є надзвичайно **актуальною**, оскільки поєднання принципів побудови КСЗІ з директивами ЄС:*

- *забезпечує модернізацію української системи кіберзахисту;*
- *сприяє інтеграції України до європейського кіберпростору;*
- *підвищує рівень безпеки державних і корпоративних систем;*
- *відповідає сучасним загрозам та вимогам інформаційної безпеки.*

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Комплексна система захисту інформації (КСЗІ) — це сукупність організаційних, технічних та програмно-технічних заходів, спрямованих на забезпечення захисту інформації в автоматизованих системах (інформаційних, телекомунікаційних, інформаційно-телекомунікаційних), яка обробляє інформацію з обмеженим доступом.

ПРИНЦИПИ ПОБУДОВИ КСЗІ

1. Принцип законності та нормативної регламентованості
2. Принцип комплексності
3. Принцип достатності заходів
4. Принцип безперервності
5. Принцип мінімізації привілеїв
6. Принцип документованості
7. Принцип контролю та аудиту
8. Принцип фізичного та інженерного захисту
9. Принцип інтегрованості з міжнародними стандартами

ОБ'ЄКТИ ТА СУБ'ЄКТИ ЗАХИСТУ ІНФОРМАЦІЇ

Об'єктами захисту:

- інформація з обмеженим доступом (конфіденційна, службова, комерційна та ін.);
- засоби обробки інформації (сервери, ПК, мережеве обладнання);
- ·канали передавання інформації;
- програмне забезпечення, яке забезпечує обробку та збереження цієї інформації.

Суб'єктами захисту:

- Замовник та виконавець
- Контролюючий орган
- Організатор експертизи
- Підрядник

ISO 27001

ISO/IEC 27001 *— це міжнародний стандарт, який встановлює вимоги до створення, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення системи управління інформаційною безпекою (СУІБ, англ. ISMS — Information Security Management System).*

МЕТА ТА ПРИНЦИП ДІЇ ISO 27001

*Основна **мета** **ISO/IEC 27001** — забезпечити конфіденційність, цілісність та доступність інформації, що обробляється організацією. Стандарт допомагає ідентифікувати ризики безпеки інформації, впровадити відповідні заходи контролю, а також постійно вдосконалювати процеси безпеки.*

***ISO/IEC 27001** базується на циклі **PDCA (Plan–Do–Check–Act)**, що відображає підхід до постійного вдосконалення.*

УЗГОДЖЕНЯ ПРИНЦИІВ ПОБУДОВИ КСЗІ З МІЖНАРОДНИМИ СТАНДАРТАМИ

Принцип КСЗІ	ISO/IEC 27001	ISO/IEC 27002	NIST CSF	Ступінь узгодженості
Комплексність	Annex A	Controls	PR.*	Повна
Ризики	6.1	-	ID.RA	Часткова
Мінімізація привілеїв	A.9	AC Controls	PR.AC	Повна
Аудит	9.2	12.7	DE.*	Повна
Фізична безпека	A.11	A.11.*	PR.PT	Повна

ПОГЛИБЛЕНЕ ПОРІВНЯННЯ МОЖЛИВОСТЕЙ КСЗІ ТА ISO/IEC 27001

Критерій	КСЗІ	ISO/IEC 27001
Відповідність законодавству України	Обов'язкова	Не регулюється законом
Міжнародне визнання	Обмежене	Високе
Підхід до ризиків	Частково (модель загроз)	Повноцінний (ISO 27005)
Гнучкість процесів	Низька	Висока
Можливість інтеграції з іншими стандартами	Обмежена	Висока (ISO 9001, 22301, 27701 тощо)
Затрати на впровадження	Високі у державному секторі	Гнучкі, залежать від масштабу
Атестація / аудит	Державна атестація	Незалежний міжнародний аудит
Циклічність процесів	Лінійний процес	PDCA (постійне вдосконалення)
Підтримка управління змінами	Обмежена	Системна (Change Management)
Орієнтація на бізнес-процеси	Низька	Висока

ПОРІВНЯННЯ ВИМОГ КСЗІ З ISO/IEC ТА NIST

Вимога	КСЗІ (НД ТЗІ)	ISO 27001/27002	NIST CSF
Модель загроз	Обов'язкова	Необов'язкова	Частково
Аналіз ризиків	Обмежено	Основна вимога	Основна вимога
Політики	Частина КСЗІ	Обов'язкові	Обов'язкові
Фізичний захист	Регламентований	Регламентований	Частково
Аудит	Експертиза	Сертифікація	Самооцінка

ПОРІВНЯННЯ АТЕСТАЦІЇ, ДЕКЛАРУВАННЯ ТА АВТОРИЗАЦІЇ

Параметр	Атестат КСЗІ	Декларація	Авторизація
Хто оцінює	Експерти	Власник	Власник + ДССЗЗІ
Орієнтація	НД ТЗІ	Профіль безпеки	Ризики + профілі
Гнучкість	Низька	Висока	Висока
Тривалість	6–12 міс.	5–30 днів	1–3 міс.
Інтеграція ISO	Низька	Середня	Висока
Інтеграція NIST	Мінімальна	Висока	Повна
Сфера	Усі ІКС	Більшість систем	Критичні системи

ПОРІВНЯННЯ ПРОФІЛІВ КСЗІ, NIST CSF, ISO 27001 ДЛЯ СЕД

Критерій	КСЗІ	NIST CSF	ISO 27001
Гнучкість	Низька	Висока	Висока
Орієнтація	Нормативна	Практична	Процесна
Орієнтація на СЕД	Середня	Висока	Висока
Контроль доступу	Сильний	Дуже сильний	Сильний
Хмарні СЕД	Проблемні	Добре	Добре
Вартість	Висока	Середня	Середня
Документоорієнтованість	Висока	Середня	Висока
Актуальність	Середня	Висока	Висока
Ризик-орієнтованість	Низька	Висока	Висока

ВИСНОВКИ

Дипломна робота присвячена комплексному дослідженню теоретичних, методичних та практичних аспектів побудови сучасної системи інформаційної та кібернетичної безпеки в умовах повномасштабної агресії Російської Федерації проти України. У роботі виконано глибокий аналіз національної моделі технічного захисту інформації (КСЗІ), міжнародних стандартів ISO/IEC серії 27000 та фреймворку NIST CybersecurityFramework, а також розроблено інтегровану модель їх узгодження для державних органів і підприємств критичної інфраструктури.

ПУБЛІКАЦІЇ ТА ПУБЛІЧНА ДІЯЛЬНІСТЬ

МІЖНАРОДНА НАУКОВА ІНТЕРНЕТ-КОНФЕРЕНЦІЯ
ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ТЕХНОЛОГІЧНІ, ЕКОНОМІЧНІ ТА ТЕХНІЧНІ АСПЕКТИ СТАНОВЛЕННЯ (ВИПУСК 80) (19-20.09.2023)

“ВПЛИВ КІБЕРАТАК НА БІЗНЕС ТА ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО”

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНИХ КОНФЕРЕНЦІЙ МОЛОДИХ ВЧЕНИХ «БУД-МАЙСТЕР-КЛАС-2025»

“Особливості застосування нормативних документів щодо побудови КСЗІ та ISO/IES 27001 ”

Проведення лекції за тематикою “Кібергігієна” для студентів КПКАТБМ в рамках Місяця Кібербезпеки

ПУБЛІКАЦІЇ ТА ПУБЛІЧНА ДІЯЛЬНІСТЬ