

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно- комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «ПРОЄКТ ПІДСИСТЕМИ ЗАХИСТУ
МЕРЕЖНОЇ ІНФРАСТРУКТУРИ НА БАЗІ
МЕТОДОЛОГІЇ ZEROTRUST»

Виконав: студент 4-го курсу групи КБ 20-2
спеціальності 125 «Кібербезпека»

 Костянтин МОРОЗОВ

Керівник: старший викладач кафедри КІ та КБ

 Наталія ЩУР

Рецензент: доцент кафедри КІ та КБ, к.пед.н

 Олена ГОЛОВНЯ

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Морозов Костянтин Олегович

Тема роботи: «Проект підсистеми захисту мережної інфраструктури на базі методології ZeroTrust»

затверджена Наказом університету від 5 березня 2024 р. №98/с

Термін здачі студентом закінченої роботи 28 червня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процес забезпечення інформаційної безпеки в мережній інфраструктурі організації.

Предметом дослідження є методи та засоби захисту мережної інфраструктури на основі методології ZeroTrust.

Обладнання та програмне забезпечення: операційні системи Windows 10, Cisco IOS.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є.М.	29.05.2024	29.05 
2	Трокоз Є.М.	29.05.2024	29.05 
3	Трокоз Є.М.	29.05.2024	29.05 

Студент  Костянтин МОРОЗОВ

Керівник  Наталія ЩУР

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	4 березня	
2	Пошук теоретичної інформації	28 березня	
3	Вибір програмного забезпечення	26 квітня	
4	Подача чернетки керівнику для перевірки	15 травня	
5	Доопрацювання роботи	26 травня	
6	Формування пояснювальної записки	14 червня	
7	Отримання відгуку керівника	16 червня	
8	Подання роботи на рецензування	20 червня	

Студент  Костянтин МОРОЗОВ

Керівник  Наталія ЩУР

АНОТАЦІЯ

Даний проєкт присвячений розробці підсистеми захисту мережної інфраструктури на основі методології ZeroTrust. Концепція ZeroTrust передбачає відсутність довіри до будь-яких суб'єктів чи ресурсів, незалежно від їхнього місцезнаходження, і здійснення постійної перевірки на відповідність певним критеріям безпеки. Проєкт охоплює вивчення та аналіз існуючих рішень, визначення вимог до підсистеми, проєктування архітектури, розробку компонентів, тестування та впровадження. Основними завданнями є забезпечення гнучкого управління доступом, сегментація мережі, моніторинг та аудит подій безпеки. Очікується, що результатом проєкту стане підвищення рівня захищеності мережної інфраструктури від несанкціонованого доступу, зловмисних атак та витоку даних.

Проєкт підсистеми захисту мережної інфраструктури на основі методології ZeroTrust є актуальним у зв'язку зі зростанням кіберзагроз, віддаленою роботою та хмарними технологіями. Ця методологія забезпечує комплексний захист мережної інфраструктури, працює у динамічному середовищі та допомагає підприємствам підвищити стійкість до кібератак та зменшити ризик компрометації даних.

Загальний обсяг дипломної роботи – 80 сторінок, 2 таблиці, 7 рисунків, 39 літературних джерел.

Ключові слова: ZEROTRUST, КІБЕРБЕЗПЕКА, АВТЕНТИФІКАЦІЯ, ІНДЕНТИФІКАЦІЯ, ЗАХИСТ ІНФОРМАЦІЇ, КІБЕРЗАГРОЗИ, КОНТРОЛЬ ДОСТУПУ, ВРАЗЛИВІСТЬ, МАШИННЕ НАВЧАННЯ, КРИТИЧНА ІНФРАСТРУКТУРА, ШТУЧНИЙ ІНТЕЛЕКТ, СТЕГАНОГРАФІЯ, КОРПОРАТИВНА МЕРЕЖА, КРИПТОГРАФІЯ, ПОЛІТИКА БЕЗПЕКИ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКОЮ.

					КІК.КР.Б – 125 – 24 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	ПРОЄКТ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ НА БАЗІ МЕТОДОЛОГІЇ ZEROTRUST	Літ.	Арк.	Аркушів
Розроб.		Морозов К.О.		28.06				
Керівник		Щур Н.О.		28.06			4	84
Реценз.		Головня О.С.		28.06		ФІКТ, Гр. КБ-20-2		
Н. контр.		Щур Н.О.		28.06				
Затверд.		Єфіменко А.А.		29.06				

ANNOTATION

This project focuses on the development of a network infrastructure protection subsystem based on the ZeroTrust methodology. The ZeroTrust concept assumes no inherent trust for any entity or resource, regardless of its location, and involves continuous verification against defined security criteria. The project encompasses studying and analyzing existing solutions, defining subsystem requirements, designing the architecture, developing components, testing, and implementation. The main objectives are to provide flexible access management, network segmentation, security event monitoring, and auditing. The expected outcome of the project is an enhanced level of network infrastructure security against unauthorized access, malicious attacks, and data leaks.

The project of a network infrastructure protection subsystem based on the Zero Trust methodology is relevant due to the increase in cyber threats, remote work, and cloud technologies. This methodology provides comprehensive protection of the network infrastructure, operates in a dynamic environment, and helps enterprises enhance resilience against cyber attacks and reduce the risk of data compromise.

The total volume of the thesis is 80 pages, 6 tables, 7 figures, 39 literary sources.

Keywords: ZEROTRUST, CYBERSECURITY, AUTHENTICATION, IDENTIFICATION, INFORMATION SECURITY, CYBER THREATS, ACCESS CONTROL, VULNERABILITY, MACHINE LEARNING, CRITICAL INFRASTRUCTURE, ARTIFICIAL INTELLIGENCE, STEGANOGRAPHY, CORPORATE NETWORK, CRYPTOGRAPHY, SECURITY POLICY, INFORMATION SECURITY MANAGEMENT.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	7
ВСТУП.....	8
РОЗДІЛ 1. ВДОСКОНАЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА	10
1.1 Важливість політики та поточний стан інформаційної безпеки.....	10
1.2. Сучасні підходи, методи та компоненти ZeroTrust.....	18
1.3. Переваги та принципи підходу ZeroTrust.....	24
ВИСНОВОК ДО 1 РОЗДІЛУ	35
РОЗДІЛ 2. КІБЕРБЕЗПЕКА ОРГАНІЗАЦІЇ: АНАЛІЗ ТРЕНДІВ ТА УПРАВЛІННЯ КУЛЬТУРОЮ	36
2.1. Кіберзагрози в цивільному секторі	36
2.2. Підвищення та вдосконалення кіберкультури.....	41
2.3. Модель оцінки культури кібербезпеки.....	53
ВИСНОВОК ДО 2 РОЗДІЛУ	56
РОЗДІЛ 3. ПОЛІТИКА БЕЗПЕКИ НА ОСНОВІ ZEROTRUST	57
3.1. Модель загроз та вимоги до апаратного засобу автентифікації ZeroTrust ..	57
3.2. Використання стеганографічного протоколу обміну даними.....	64
3.3. Загрози ІШІ та відновлення після кіберінциденту	67
ВИСНОВОК ДО 3 РОЗДІЛУ	72
ВИСНОВОК	73
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	76

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІКС – Інформаційно-комунікаційна система

ПЕКК – Пасивний електричний коливальний контур

ПВП – Первинний вимірювальний перетворювач

СППР – Система підтримки прийняття рішення

СУІБ – Система управління інформаційною безпекою

СШІ – Система штучного інтелекту

ШІ – Штучний інтелект

DoS – Denial-of-service (відмова в обслуговуванні)

DDoS – Distributed denial-of-service (розподілена відмова в обслуговуванні)

GDPR – General Data Protection Regulation (Загальний регламент про захист даних)

HAD – Hardware authentication device (апаратний пристрій автентифікації)

IAM – Identity & access management (авторизації та управління доступом)

IoT – Internet of things (інтернет речей)

LSB – Least significant bit (найменший значущий біт)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій)

PEP – Policy Enforcement Point (точка застосування політики)

PDP – Policy Decision Point (точка прийняття рішення)

RFID – Radio frequency identification (радіочастотна ідентифікація)

VPN – Virtual private network (віртуальна приватна мережа)

Zerotrust – Нульова довіра

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Стрімкий розвиток цифрових технологій та зростання кіберзагроз вимагає переосмислення підходів до забезпечення інформаційної безпеки в організаціях. Традиційні моделі захисту, засновані на принципі «периметра безпеки», все частіше виявляються неефективними в умовах розподіленої інфраструктури, хмарних обчислень і мобільних пристроїв. У цьому контексті методологія ZeroTrust набуває все більшої актуальності, пропонуючи нову парадигму безпеки, яка ґрунтується на принципі «не довіряй нікому і нічому».

Практичне значення проєкту підсистеми захисту мережної інфраструктури на базі методології ZeroTrust полягає у забезпеченні всеосяжного захисту корпоративних ресурсів та даних, незалежно від їх розташування чи способу доступу. Це дозволяє організаціям ефективно протидіяти сучасним кіберзагрозам, підвищити рівень інформаційної безпеки та знизити ризики втрати конфіденційних даних.

Мета роботи: дослідити та розробити вдосконалену політику інформаційної безпеки для сучасного підприємства, базуючись на принципах ZeroTrust, з урахуванням актуальних кіберзагроз та методів їх подолання. Проаналізувати тренди кібербезпеки в організаціях, запропонувати шляхи підвищення кіберкультури та створити модель оцінки культури кібербезпеки. Розробити модель загроз та вимоги до апаратного засобу автентифікації на основі ZeroTrust, дослідити використання стеганографічного протоколу для обміну даними, а також розглянути загрози, пов'язані з штучним інтелектом, та методи відновлення після кіберінцидентів.

Для досягнення поставленої мети необхідно виконати такі **завдання**:

- 1) Проаналізувати важливість та поточний стан інформаційної безпеки на сучасних підприємствах.
- 2) Дослідити сучасні підходи, методи та компоненти концепції ZeroTrust.
- 3) Визначити переваги та основні принципи підходу ZeroTrust.
- 4) Розглянути актуальні кіберзагрози в цивільному секторі.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

5) Розробити рекомендації щодо підвищення та вдосконалення кіберкультури в організаціях.

6) Створити модель оцінки культури кібербезпеки.

7) Розробити модель загроз та сформулювати вимоги до апаратного засобу автентифікації на основі ZeroTrust.

8) Дослідити можливості використання стеганографічного протоколу для обміну даними в контексті політики безпеки.

9) Проаналізувати загрози, пов'язані з використанням штучного інтелекту в сфері кібербезпеки.

10) Розробити стратегію відновлення після кіберінцидентів.

Об'єктом дослідження є процес забезпечення інформаційної безпеки в мережній інфраструктурі організації.

Предметом дослідження є методи та засоби захисту мережної інфраструктури на основі методології ZeroTrust.

Методи дослідження включають аналіз наукових публікацій, нормативних документів та галузевих стандартів у сфері інформаційної безпеки, а також моделювання та проектування підсистеми захисту мережної інфраструктури.

Інформаційною базою дослідження є наукові праці вітчизняних та зарубіжних авторів, матеріали конференцій, галузеві звіти та рекомендації провідних організацій з кібербезпеки.

Практичне значення одержаних результатів полягає у можливості використання розробленого проекту підсистеми захисту мережної інфраструктури на базі методології ZeroTrust для підвищення рівня інформаційної безпеки в організаціях різних галузей.

Структура роботи складається зі вступу, анотації, переліку умовних позначень, трьох розділів, висновків та списку використаних джерел (39 позицій). Має 7 рисунків та 2 таблиці. Загальний обсяг дипломної роботи складає 80 с., з них обсяг тексту основної частини – 65 с.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ВДОСКОНАЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА

1.1 Важливість політики та поточний стан інформаційної безпеки

У сучасну епоху цифрових технологій багато компаній перейшли на електронний документообіг для підвищення ефективності. Однак захист інформаційних систем та цифрових активів залишається серйозною проблемою. Пандемія COVID-19 ще більше загострила цю ситуацію, оскільки більшість бізнес-процесів перемістилися в онлайн, привернувши увагу кіберзлочинців.

Численні дослідження засвідчують зростання корпоративних кіберінцидентів. Згідно зі звітом Агентства ЄС з кібербезпеки ENISA, у 2020-2021 роках зросла кількість атак на «домашні офіси» та програмне забезпечення для віддаленої роботи. Результатом стало збільшення загрози витоку корпоративних даних з 8,7% у 2020 році до 81% у другому кварталі 2021 року.

Щорічні звіти IBM «Cost of a Data Breach Study» також демонструють негативну тенденцію. У 2022 році середня вартість витоку даних для підприємств у всьому світі зросла приблизно на 20% порівняно з 2017 роком - до 4,35 млн доларів США. Найпоширенішими векторами атак, які призводять до витоку даних, є фішинг, викрадені/скомпрометовані дані, вразливості програмного забезпечення, витік від інсайдерів та компрометація ділової електронної пошти [15, с. 98].

Для зміцнення конфіденційності та безпеки даних підприємства впроваджують різноманітні засоби захисту інформації, такі як міжмережеві екрани, VPN, контроль доступу, управління оновленнями, резервне копіювання, централізований моніторинг безпеки, виявлення вторгнень, контроль поведінки користувачів, запобігання витокам даних, захист від спаму та DDoS-атак тощо.

Проте, незважаючи на широкий вибір технологій інформаційної безпеки, їх впровадження не приносить прямої фінансової вигоди для підприємства. Вони лише дозволяють зменшити потенційні збитки від можливих інцидентів. Будь-яка спроба несанкціонованого доступу, кібератака або порушення безпеки можуть мати критичні наслідки та спричинити прямі й непрямі збитки [13, с. 32].

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Тому для підприємств надзвичайно важливо раціонально інвестувати ресурси та час у вирішення проблем інформаційної безпеки, щоб мінімізувати потенційні ризики. Замість того, щоб сліпо витратити кошти на різноманітні засоби захисту, потрібно ретельно оцінювати та вибирати найбільш ефективні та економічно вигідні рішення.

Політика інформаційної безпеки – це комплексний набір превентивних заходів, правил та принципів, що спрямовані на захист інформаційних активів підприємства, включаючи конфіденційні дані. Вона визначає чіткі правила та стандарти роботи з інформацією, доступ до неї та її обробку. Політика інформаційної безпеки розробляється з урахуванням специфіки кожного підприємства, його галузевої приналежності, розміру, структури та інформаційних потреб.

Ключові цілі політики інформаційної безпеки:

1) Захист інформаційних ресурсів: політика інформаційної безпеки мінімізує ризики витоків, компрометації або втрати інформації, гарантуючи її конфіденційність, цілісність та доступність.

2) Підвищення стійкості до кіберзагроз: політика інформаційної безпеки допомагає протистояти актуальним кіберзагрозам, таким як хакерські атаки, фішинг, DDoS-атаки та інші.

3) Зниження ризиків фінансових втрат: витік або втрата даних може призвести до значних фінансових втрат для підприємства. Політика інформаційної безпеки допомагає мінімізувати такі ризики.

4) Підвищення іміджу та репутації: впровадження політики інформаційної безпеки демонструє відповідальність та турботу про інформаційну безпеку, що позитивно впливає на імідж та репутацію компанії.

5) Забезпечення безперервності бізнесу: політика інформаційної безпеки сприяє мінімізації простоїв та збоїв в роботі інформаційних систем, гарантуючи безперервність бізнес-процесів.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

6) Збільшення довіри клієнтів: політика інформаційної безпеки гарантує захист конфіденційної інформації клієнтів та партнерів, що сприяє формуванню довіри та лояльності.

Основні функції політики інформаційної безпеки:

1) Встановлення норм та вимог: політика інформаційної безпеки визначає чіткі правила та стандарти роботи з інформацією, доступ до неї та її обробку.

2) Захист конфіденційності та цілісності даних: політика інформаційної безпеки регламентує заходи щодо захисту інформації від несанкціонованого доступу, розголошення або модифікації.

3) Мінімізація інформаційних ризиків: політика інформаційної безпеки передбачає аналіз та оцінку потенційних загроз, розробку методів їх нейтралізації та мінімізацію ризиків виникнення інцидентів інформаційної безпеки.

4) Відповідність законодавству: політика інформаційної безпеки допомагає підприємствам дотримуватися вимог законодавства у сфері захисту інформації.

5) Формування культури безпеки: політика інформаційної безпеки сприяє формуванню культури безпеки на підприємстві, де безпека інформації є важливою складовою кожного бізнес-процесу.

Політики інформаційної безпеки – це невід’ємний елемент сучасної інформаційної культури підприємства, який гарантує стійкість та надійність його інформаційних ресурсів.

Впровадження політики інформаційної безпеки, адаптованої до потреб конкретного підприємства, є одним з ключових методів ефективного управління інформаційними ризиками.

Хоча раніше деякі експерти в галузі інформаційної безпеки вважали політику інформаційної безпеки неефективним інструментом, недооцінюючи її вплив на захист інформації. Вони помилково вважали, що для забезпечення безпеки достатньо лише технологічних рішень.

Насправді, політика інформаційної безпеки відіграє важливу роль у комплексному захисті інформаційних ресурсів, адже вона:

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

1) Визначає чіткі правила та стандарти: встановлює норми та вимоги щодо роботи з інформацією, доступу до неї та її обробки.

2) Регламентує дії з захисту інформації: описує процедури та практики, спрямовані на захист конфіденційності, цілісності та доступності даних.

3) Сприяє формуванню культури безпеки: підкреслює важливість інформаційної безпеки для всіх співробітників, роблячи її невід’ємною частиною корпоративної культури.

Основні аспекти, які охоплює політику інформаційної безпеки:

- 1) забезпечення конфіденційності даних;
- 2) класифікація інформації за рівнем конфіденційності;
- 3) контроль доступу до систем, мереж та даних;
- 4) шифрування даних під час їх передачі та зберігання;
- 5) фізичний захист приміщень та обладнання;
- 6) заборона на несанкціонований обмін конфіденційною інформацією;
- 7) безпечне видалення конфіденційної інформації з пристроїв;
- 8) забезпечення цілісності даних;
- 9) контроль цілісності та автентичності даних;
- 10) резервне копіювання та відновлення даних;
- 11) забезпечення доступності даних;
- 12) відновлення систем після відмов;
- 13) формування технічних резервів обладнання та серверів;
- 14) балансування навантаження на сервери;
- 15) запобігання атакам DoS/DDoS;
- 16) забезпечення безпеки мережі;
- 17) захист мережевих ресурсів і даних від несанкціонованого доступу;
- 18) застосування брандмауерів, антивірусного програмного забезпечення та інших захисних інструментів;
- 19) моніторинг та аудит безпеки;
- 20) виявлення та фіксація несанкціонованих дій;
- 21) перевірка відповідності вимогам політики інформаційної безпеки;

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

- 22) превентивні механізми;
- 23) виявлення та усунення вразливостей в системах та програмному забезпеченні;
- 24) запобігання кібератак;
- 25) навчання співробітників;
- 26) ознайомлення з політикою інформаційної безпеки, загрозами безпеці та правилами поведінки в Інтернеті;
- 27) постійне підвищення обізнаності в питаннях інформаційної безпеки.

Важливо зазначити, що політика інформаційної безпеки не є самодостатнім інструментом. Її ефективність залежить від комплексного підходу до інформаційної безпеки, який включає впровадження технологічних рішень, організаційних заходів та постійне навчання персоналу. Це не пасивний документ, а активний інструмент, який допомагає підприємствам захистити свої інформаційні активи та мінімізувати ризики витоків, компрометації або втрати даних [27].

Важливість чіткої політики інформаційної безпеки полягає не лише у встановленні правил та процедур, але й у їх фактичному дотриманні співробітниками. Вона робить це двома ключовими способами:

1) Забезпечує чітке розуміння очікувань: Документована політика чітко прописана і чітко окреслює, що очікується від співробітників у сфері інформаційної безпеки. Усунення неоднозначності усуває плутанину та невизначеність щодо того, що є прийнятним, а що ні, зменшуючи ймовірність ненавмисних порушень. Підвищення відповідальності: маючи чіткі правила, співробітники несуть більшу відповідальність за свої дії.

2) Сприяє впровадженню та дотриманню: Інтеграція в робочі процеси включення політики інформаційної безпеки до щоденних робочих процесів робить її невід’ємною частиною роботи, роблячи дотримання правил звичним. Навчання та підтримка: регулярні тренінги та навчання з питань інформаційної безпеки гарантують, що співробітники знають і розуміють політику, а також знають, як її дотримуватися. Внутрішній контроль: впровадження системи моніторингу та

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

аудиту допомагає гарантувати, що правила дотримуються, а порушення виявляються та вирішуються.

Важливо зазначити, що простого існування політики інформаційної безпеки недостатньо. Щоб вона дійсно впливала на дії суб'єктів, вона повинна бути доступною та зрозумілою, регулярно оновлюватися та підтримуватися керівництвом. Впровадження та дотримання чіткої та ефективної ПІБ є необхідною умовою для забезпечення інформаційної безпеки на підприємстві. Вона допомагає мінімізувати ризики витоків, компрометації або втрати даних, а також забезпечує відповідність законодавству та галузевим стандартам. Ця політика включає в себе визначення відповідальностей за захист інформації, процедури забезпечення безпеки даних, контроль доступу до інформації, а також навчання та свідоме використання працівниками правил безпеки. Важливо, щоб кожен працівник був ознайомлений з політикою безпеки та дотримувався її в усіх аспектах своєї роботи. Тільки таким чином можна забезпечити надійний захист даних інформаційної системи підприємства..

Однак, отримавши підтримку, виникає проблема забезпечити, щоб положення політики безпеки дійсно покращували безпеку. Оцінити ефективність організаційних заходів, таких як політика безпеки, значно складніше, ніж технічних засобів захисту, ефективність яких можна виміряти статистичними даними. Без чіткого дотримання положень політики безпеки вона залишається лише на папері і не впливає на стан інформаційної безпеки на підприємстві.

Це підтверджується опитуванням SANS Institute, яке виявило, що близько 15% працівників взагалі не знають про діючу політику безпеки у своїх компаніях і, відповідно, не дотримуються її основних положень.

Співробітники, які не дотримуються політики інформаційної безпеки або мають зловмисні наміри, становлять значну загрозу для інформаційних активів підприємства. Однак, також поширена ситуація, коли співробітники порушують політику безпеки, вважаючи, що це корисно для бізнесу. Це може бути спричинено тиском з боку клієнтів, прагненням до підвищення продуктивності або недостатньою обізнаністю. Дослідження показали, що понад 50% співробітників

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

свідомо порушують політику безпеки, вважаючи, що ризики незначні. Однак, наслідки порушення політики безпеки можуть бути серйозними, включаючи втрату конфіденційних даних, перебої в роботі та штрафи та санкції. Для мінімізації ризиків, пов'язаних з людським фактором, підприємства повинні розробляти та впроваджувати чітку політику безпеки, навчати співробітників з питань інформаційної безпеки, створювати культуру кібербезпеки, використовувати технічні засоби для захисту даних та заохочувати співробітників повідомляти про підозрілу активність. Ці заходи допоможуть підприємствам захистити свої інформаційні активи від кіберзагроз і зменшити ризики порушення політики безпеки з боку співробітників.

Успішність політики інформаційної безпеки залежить не тільки від технічних аспектів, а й від розуміння людської природи. Дослідження демонструють важливість врахування організаційних, технологічних та індивідуальних чинників, що впливають на поведінку співробітників щодо дотримання правил безпеки. Однак, коли вимоги безпеки суперечать ефективності роботи, працівники часто надають перевагу бізнес-цілям. Щоб сформувати позитивне ставлення до безпеки, політика повинна узгоджуватися з робочими завданнями та сприяти їх ефективному виконанню.

Більшість досліджень концентрується на оцінці впливу факторів на поведінкові наміри, а не на фактичну поведінку. Ця різниця пояснюється мотивацією поступливості та іншими чинниками, такими як суб'єктивні норми, самоефективність, ставлення, очікувані переваги, сприйнятливість до загроз, їхня серйозність, ефективність і вартість реагування, а також досвід. Фундаментальною теорією у вивченні людської поведінки є «теорія запланованої поведінки», згідно з якою поведінкові наміри залежать від особистого ставлення, соціального тиску та відчуття контролю. Поведінкові наміри активізуються лише тоді, коли поведінка знаходиться під вольовим контролем і відповідає соціальним нормам. Дослідники також застосовують інші теорії, такі як «загальна теорія стримування» та «теорія мотивації до захисту», для вивчення людського фактору в сфері інформаційної безпеки.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

Людський фактор суттєво впливає на ефективність політики інформаційної безпеки компанії. Проте, існують й інші проблеми, що впливають на реалізацію політики, зокрема рівень прийнятного ризику, процедурні відмінності між відділами, юридичні обмеження, особисті погляди та культурні аспекти. Внутрішні зміни в структурі компанії можуть призводити до впровадження жорстких заходів безпеки, які обмежують доступ співробітників до конфіденційної інформації та створюють перешкоди для діяльності компанії. Крім того, погляди працівників на реальність можуть суперечити положенням політики безпеки, а сама політика може бути недостатньо чіткою та зрозумілою, що призводить до плутанини щодо дозволених і заборонених дій.

Розробка політик інформаційної безпеки є складним завданням через різні точки зору спеціалістів та співробітників, що може призводити до непорозумінь і нереалістичних припущень. Часто спеціалісти ігнорують важливість прислухатися до співробітників, що призводить до неефективності прийнятої політики безпеки. Недостатня зрозумілість, ясність та ігнорування з боку працівників також можуть спричинити неефективність політики безпеки.

Політика безпеки є важливим аспектом ефективного управління інформаційною безпекою в підприємствах. Проте, впровадження такої політики може викликати труднощі, особливо коли вона не адаптована до конкретних потреб і умов функціонування підприємства. Важливо ретельно аналізувати цілі, ризики, норми та обставини підприємства при розробці політики безпеки, а також регулярно оновлювати її для забезпечення актуальності і ефективності. Шаблони політики безпеки можуть бути корисним інструментом, але вони повинні бути адаптовані до конкретних умов підприємства для досягнення оптимальних результатів.

Політика безпеки повинна бути постійно оновлюваною, щоб відповідати сучасним потребам і цілям безпеки підприємства. Ознаки застарілості включають у себе застарілі дати, технології та нормативні документи, а також непридатні обов'язки для структурних підрозділів. Недоліки сучасних політик інформаційної безпеки включають в себе відсутність структури, неузгодженість, складність,

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

двозначність, занадто великий обсяг та застарілу інформацію. Дієва політика безпеки повинна бути зрозумілою, послідовною, легко сприйманою та актуальною для відповіді на сучасні загрози та потреби підприємства.

1.2. Сучасні підходи, методи та компоненти ZeroTrust

Враховуючи посилення регуляторних вимог щодо збереження та захисту інформації, компаніям необхідно ефективно інвестувати час та ресурси у розробку політики інформаційної безпеки. Це допоможе відповідати високим стандартам безпеки, уникнути кібератак, а також серйозних юридичних та репутаційних ризиків. Існують різні архітектурні рішення для структурування політики інформаційної безпеки, найпоширенішими з яких є часткова, повна та модульна політики. Кожна з них має свої особливості та переваги, але повна політика є найбільш розповсюдженою на сьогодні.

Структура політики інформаційної безпеки зазвичай складається з трьох ієрархічних рівнів: стратегічного, тактичного та операційного. Стратегічний рівень визначає загальну концепцію інформаційної безпеки, корпоративні вимоги та принципи управління безпекою. Тактичний рівень включає розробку документації для конкретних питань, зокрема інструкцій та рекомендацій щодо використання технологій. Операційний рівень охоплює технічні стандарти та налаштування систем. Багато дослідників вважають модульну структуру політики інформаційної безпеки найбільш ефективною на сьогодні [5, с. 242].

Розробка, вдосконалення, отримання схвалення та впровадження повноцінної політики інформаційної безпеки вимагають значних зусиль. Деякі можуть спокуситися використати шаблони або придбати готовий набір політик. Хоча ці шаблони можуть бути корисними прикладами для розробки власної політики безпеки, їх не слід розглядати як готовий продукт. Вся цінність та ефективність таких шаблонів базується на загальноприйнятих розуміннях інформаційної безпеки. Проте, політика інформаційної безпеки має бути унікально створена та адаптована для кожної компанії. Нижче наведено причини, які

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

підкреслюють важливість унікальності та адаптації політики інформаційної безпеки для кожної компанії:

1) Бізнес-цілі: кожен бізнес, кожна компанія є унікальною, тому політика інформаційної безпеки має узгоджуватися з бізнес-цілями компанії, забезпечувати економічну ефективність та конкурентні переваги.

2) Організаційна структура: політика інформаційної безпеки повинна визначати чіткі обов'язки, підзвітність та нагляд за інформаційною безпекою відповідно до структури компанії.

3) Культурний фактор: культурні відмінності можуть впливати на сприйняття різних ресурсів забезпечення інформаційної безпеки. Політика безпеки повинна враховувати ці відмінності, щоб бути ефективною.

4) Особливості інформаційних загроз за галузями: потужність та інтенсивність контролю, суворість покарань і рівень нагляду повинні відповідати загрозам конкретної компанії та галузі.

5) Законодавчі особливості регіону: формування політики інформаційної безпеки повинно враховувати законодавство країни, в якій діє компанія. Кожна країна має свої принципи та норми щодо регулювання інформаційної безпеки.

Крім стандартного підходу до побудови політики інформаційної безпеки компанії, досить поширеними є ризик-орієнтований, ітеративний, низхідний та висхідний підходи.

Ризик-орієнтований підхід до безпеки інформації передбачає систематичний аналіз та управління ризиками, пов'язаними з інформацією. Основна мета цього підходу - забезпечити ефективний та пропорційний захист інформації, зосереджуючись на найважливіших та найбільш небезпечних вразливих ділянках. Цей метод дозволяє визначити пріоритети та конкретні заходи безпеки, які необхідно впровадити. Для цього необхідно ідентифікувати всі інформаційні активи компанії, виявити потенційні загрози, оцінити ризики, пов'язані з інформацією, визначити конкретні заходи для забезпечення безпеки інформації та розробити офіційну політику безпеки компанії [16, с. 174].

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Ітеративний підхід передбачає формування політики безпеки компанії на основі послідовних ітерацій, з покроковим вдосконаленням, починаючи з базової політики, яка з часом вдосконалюється та доповнюється.

При побудові політики інформаційної безпеки підприємства використовуються два основні підходи: низхідний і висхідний.

Низхідний підхід передбачає розробку політики безпеки зверху вниз, починаючи з вищого рівня керівництва, яке встановлює стратегічні цілі та принципи безпеки, які потім конкретизуються у правила та процедури. Цей підхід забезпечує узгодженість політики безпеки зі стратегією підприємства.

Висхідний підхід, з іншого боку, ґрунтується на розробці політики безпеки знизу вгору, спираючись на розуміння ризиків та потреб підприємства рядовими співробітниками та технічними експертами, з підтримкою керівництва.

Одним з найбільш ефективних підходів є використання національних та міжнародних стандартів, таких як ISO/IEC 27001, ISO/IEC 27002, НД ТЗІ (Україна), BSI Standards (Німеччина), NIST Special Publication (США) та інші. Ці стандарти та фреймворки допомагають забезпечити інформаційну безпеку на підприємстві.

Політика безпеки автоматизованих систем може бути ефективною, якщо використовуються різні підходи, що дозволяють забезпечити баланс між стратегічністю та конкретністю заходів безпеки. Нормативний документ НД ТЗІ 1.4-001 визначає можливість створення політики безпеки у вигляді модульної архітектури, яка включає різні підходи, такі як політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації.

На основі аналізу типів архітектури політики безпеки та підходів до її побудови можна узагальнити процес формування політики інформаційної безпеки підприємства, який складається з таких етапів:

1) Дослідження підприємства як об'єкта захисту. На цьому етапі проводиться детальне вивчення об'єкта, включаючи обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію та технології її обробки. Визначаються ключові інформаційні активи та ресурси, які потребують захисту, а також основні загрози для інформації.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

2) Аналіз ризиків інформаційної безпеки. На цьому етапі вивчаються моделі загроз і потенційних порушників, визначаються можливі наслідки від реалізації загроз і формується модель захисту інформації. Визначаються компоненти та ресурси, які можуть бути об'єктами атаки або джерелами порушення інформаційної безпеки. Також оцінюються гранично припустимі та реальні ризики реалізації загроз, а також збитки, що можуть бути завдані підприємству.

3) Визначення вимог до заходів, методів та засобів захисту. На цьому етапі встановлюються вимоги до заходів, методів та засобів захисту інформації.

Розробка концепції інформаційної безпеки. На цьому етапі розробляється концепція інформаційної безпеки, яка включає в себе всі вимоги, методи та засоби захисту, а також рекомендації щодо зниження ризиків інформаційної безпеки.

Отже, процес формування політики інформаційної безпеки підприємства включає дослідження об'єкта захисту, аналіз ризиків, визначення вимог до захисту та розробку концепції безпеки. Розробка концепції інформаційної безпеки на підприємстві включає в себе формування загальних положень безпеки, визначення мети, пріоритетів, напрямків діяльності, а також основних аспектів забезпечення безпеки інформації. Вибір рішень забезпечення інформаційної безпеки передбачає комплексний підхід, який включає правовий рівень (нормативно-правове регулювання, підтримка керівництвом, контроль) та організаційний рівень (режимні заходи, фізичний захист, доступ до ресурсів, профілактика порушень). Важливо визначити відповідальність персоналу за дотримання політики безпеки.

Серед найважливіших компонентів політики безпеки виділяють правила розмежування доступу, які регламентують доступ користувачів та процесів до ресурсів ІКС підприємства.

Технічний рівень забезпечення інформаційної безпеки повинен включати:

- планування, експлуатацію та супровід інженерно-технічного обладнання;
- реєстрацію та авторизацію користувачів;
- керування доступом до ресурсів з розподілом ролей;
- виявлення та реєстрацію загрозливих подій;
- забезпечення цілісності та конфіденційності даних;

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

- резервне копіювання та відновлення після збоїв;
- захист програмного забезпечення від несанкціонованих змін;
- забезпечення функціонування засобів контролю.

Організація відновлювальних робіт і забезпечення неперервності бізнес-процесів передбачає:

- виявлення критичних компонентів ІКС для бізнес-процесів;
- оцінку впливу надзвичайних ситуацій;
- визначення обов'язків персоналу під час інцидентів;
- підготовку персоналу до дій в надзвичайних ситуаціях;
- опис сценаріїв надзвичайних ситуацій;
- процедури реагування та тимчасового аварійного режиму;
- процедури відновлення після інцидентів;
- тестування плану і навчання персоналу.

Політика безпеки повинна бути належним чином документально оформлена.

Загальна політика інформаційної безпеки повинна охоплювати широкий спектр питань і включати в себе ключові компоненти, які ви зазначили. Давайте розглянемо кожен з них більш детально:

1) Загальна стратегія, цілі, завдання, обсяг і підходи до забезпечення інформаційної безпеки: Цей розділ визначає основні напрямки, на які буде спрямована політика безпеки, а також методи та підходи, які будуть використовуватися для досягнення поставлених цілей.

2) Декларація намірів керівництва щодо підтримки цілей інформаційної безпеки: Цей розділ демонструє прихильність вищого керівництва до забезпечення інформаційної безпеки та надає політиці необхідну вагу та авторитет.

3) Визначення об'єктів захисту, виявлення та оцінка загроз: У цьому розділі ідентифікуються ключові інформаційні активи, які потребують захисту, а також потенційні загрози для цих активів. Це дозволяє розробити ефективні заходи безпеки.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

4) Визначення ролей, відповідальних осіб та їхніх обов'язків: Цей розділ визначає, хто відповідає за різні аспекти інформаційної безпеки та які обов'язки вони мають виконувати. Це забезпечує чіткий розподіл відповідальності.

5) Встановлення відповідальності за забезпечення безпеки інформації: Цей розділ покладає загальну відповідальність за інформаційну безпеку на певних осіб або групи осіб, таких як керівництво, IT-відділ або співробітників.

6) Процедури доступу, управління та захисту інформації: Цей розділ описує, як слід керувати доступом до інформації, як її захищати та як нею управляти протягом усього життєвого циклу.

7) Процедури виявлення та повідомлення про порушення безпеки: Цей розділ визначає, як слід виявляти та повідомляти про інциденти безпеки, а також як на них реагувати.

8) Програма навчання працівників з питань інформаційної безпеки: Цей розділ підкреслює важливість навчання та підвищення обізнаності співробітників щодо інформаційної безпеки та описує, як це буде здійснюватися.

9) Перехресні посилання на додаткові документи: Цей розділ забезпечує зв'язок політики безпеки з іншими релевантними документами, такими як процедури, керівництва тощо.

10) Загальні елементи: Цей розділ містить інформацію про авторів політики, дати її затвердження та перегляду, що допомагає відстежувати актуальність документа.

Включення всіх цих компонентів до загальної політики інформаційної безпеки допомагає створити всебічну та ефективну основу для захисту інформаційних активів організації. Це також забезпечує залучення всіх відповідних зацікавлених сторін і створює культуру безпеки в організації.

Компанія Cisco розробила свій власний концептуальний підхід до побудови політики інформаційної безпеки. Цей підхід базується на кількох ключових принципах, включаючи стратегічне планування, ризик-орієнтований підхід, відповідність вимогам законодавства, інтеграцію з передовими технологіями, підвищення обізнаності та навчання працівників, постійне вдосконалення,

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

комунікацію та співпрацю з партнерами та впровадження принципу захисту «від периметра до кінцевого пристрою».

Отже, підхід до побудови політики інформаційної безпеки, як і аналогічні йому, спрямовані на створення глибокої, комплексної та адаптивної системи з урахуванням винятків та ризиків. Проте важливо, щоб сама політика була зрозумілою, простою та орієнтованою на цільову аудиторію, включала визначення технічних термінів та чітко визначала ролі та обов'язки користувачів. Недоліки у формулюванні політики можуть призвести до недотримання правил та порушень, що в свою чергу може стати внутрішньою загрозою для підприємства. Тому важливо враховувати всі аспекти інформаційної безпеки, включаючи індивідуальні обов'язки користувачів, для ефективного управління інформаційною безпекою.

Багато дослідників підтримують ідею побудови політики інформаційної безпеки на принципі найменших привілеїв, який передбачає надання користувачам лише необхідних прав доступу для виконання їх завдань. Це допомагає запобігти неналежному використанню даних та зменшити ризики, пов'язані з працівниками. Концепція *zerotrust*, яка базується на цих принципах, переносить увагу з захисту мережевих периметрів на користувачів, активи та ресурси, стверджуючи, що ніщо не може бути автоматично довіреним, навіть у межах підприємства.

1.3. Переваги та принципи підходу *ZeroTrust*

Сучасний ландшафт організацій зазнав трансформації через цифровий розвиток, пандемію COVID-19 та інші чинники. Зросла кількість віддалених працівників, використання особистих пристроїв (BYOD) та впровадження хмарних технологій. Це призвело до того, що більше пристроїв та сервісів стали доступними через відкриті мережі, створюючи нові вразливості та можливості для кібератак.

Традиційні політики інформаційної безпеки зосереджені на захисті від зовнішніх загроз, вважаючи внутрішню корпоративну мережу безпечною. Вони базуються на концепції «периметра безпеки» - поділі на довірену внутрішню та недовірену зовнішню мережі. Однак така модель стає вразливою, оскільки

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

зловмисник, отримавши доступ всередину периметра, може легко розвивати атаку далі [1, с.12].

Філософія «ніколи не довіряти» (ZeroTrust) була запропонована як відповідь на проблему зловживання довірою ще в 1990-х роках. Проте як концептуальний підхід до забезпечення інформбезпеки вона була розвинена лише у 2010 році.

Підхід zerotrust використовує технології автентифікації, керування доступом, шифрування та мережевої безпеки для створення захищених мікропериметрів. Доступ до ресурсів регламентується політиками на основі принципу «ніколи не довіряй, завжди перевіряй». Будь-який запит на доступ до ресурсу, незалежно від суб'єкта чи його місцезнаходження, підлягає повній автентифікації, авторизації та шифруванню в середовищі ZeroTrust.

Незважаючи на те, що ZeroTrust – це концепція, її основна структура вже визначена такими організаціями, як NIST, Gartner, Forrester, IDC та ESG. У спеціальній публікації SP 800-207 NIST визначає ключові аспекти реалізації принципів ZeroTrust та сценарії розгортання відповідної архітектури. Публікація зосереджена на запобіганні несанкціонованому доступу до всіх корпоративних ресурсів, включно з даними, пристроями, обчислювальними потужностями тощо, забезпечуючи деталізований контроль доступу.

Абстрактна модель надання доступу в ZeroTrust архітектурі включає політику прийняття рішень (PDP) та політику виконання рішень (PEP) через «контрольно-пропускний пункт». Система керування доступом охоплює перевірку автентичності суб'єкта та легітимності самого запиту, застосовуючи концепцію Zero Trust до автентифікації та авторизації. В автентифікації йдеться про рівень впевненості в достовірності суб'єкта на основі різних факторів - імені користувача, паролів, біометрії, багатофакторної автентифікації тощо.

В авторизації виконується перевірка прав доступу суб'єкта до певного ресурсу на основі політик керування доступом. В авторизації визначається, чи має суб'єкт дозволений доступ до запитуваного ресурсу на основі встановленого рівня впевненості в його достовірності.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

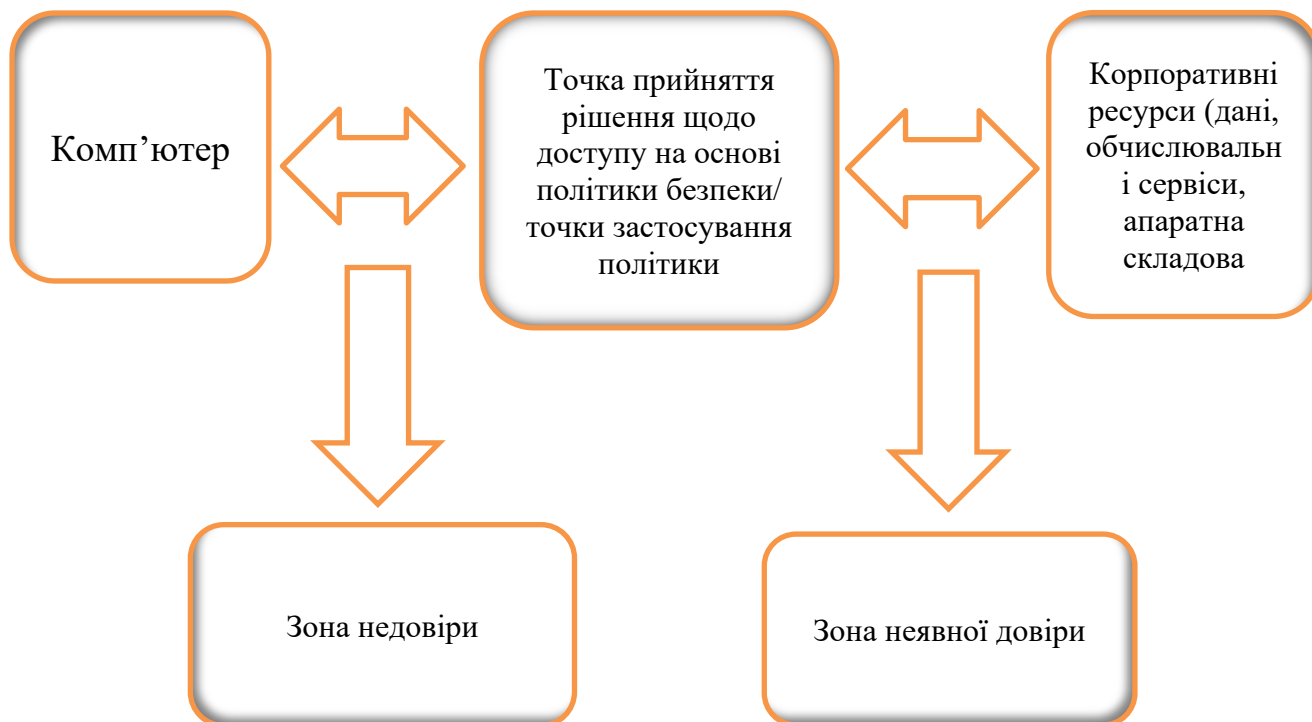


Рисунок 1. Модель надання доступу згідно архітектури ZeroTrust

Система оцінює, чи відповідає рівень доступу суб'єкта його «особистості» та вимогам безпеки ресурсу. Враховується стан безпеки пристрою, з якого надходить запит, а також інші контекстні фактори, що можуть впливати на рівень довіри. Ключовим є послідовне і точне застосування авторизаційних політик для кожного окремого запиту без покладання на попередню автентифікацію. «Зона неявної довіри», де всім довіряють на рівні PDP/PEP, має бути мінімальною для максимальної конкретики. Ці малі зони неявної довіри формують мікропериметри безпеки (Рисунок 1).

Отже, авторизація в ZeroTrust вимагає ретельної перевірки прав доступу з урахуванням багатьох факторів для кожного запиту, не покладаючись на загальну довіру всередині традиційного периметра безпеки.

Концепція ZeroTrust базується на ідеї, що жодному суб'єкту (користувачу, пристрою чи додатку) не можна довіряти за замовчуванням, незалежно від його місцезнаходження в мережі. Замість цього, доступ надається лише після ретельної перевірки на підставі таких принципів:

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Усі ресурси підприємства (пристрої, сервіси, дані тощо) розглядаються як корпоративні активи, незалежно від їхнього місцезнаходження.

1) довіра не ґрунтується на присутності в корпоративній мережі - запити з будь-якого джерела мають відповідати однаковим вимогам безпеки.

2) доступ надається лише на одну сесію і з мінімально необхідними привілеями для виконання завдання.

3) доступ визначається динамічною політикою на основі факторів, як-от стан суб'єкта, його поведінка та контекстні атрибути.

4) передбачається постійний моніторинг активності та стану безпеки всіх активів через безперервну діагностику та виправлення.

5) процеси автентифікації та авторизації є динамічними, контрольованими, з багатофакторною перевіркою.

6) відбувається постійний збір та аналіз даних для удосконалення політик безпеки.

Архітектура ZeroTrust може складатися з різних компонентів, які можуть бути як локальними, так і хмарними сервісами (Рисунок 2).

Немає універсальної архітектури ZeroTrust, оскільки кожне підприємство є унікальним і потребує індивідуального підходу до реалізації цих принципів. Архітектура ZeroTrust повинна постійно переоцінюватися та модернізуватися для того, щоб максимально посилити ефективність застосування цього підходу. NIST пропонує базову абстрактну модель концептуального ядра архітектури ZeroTrust, яку можна використовувати як основу для адаптації під конкретні умови функціонування підприємства.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

```

def verify_token(self, username, token):
    user = self.users.get(username)
    if user and user["token"] == token:
        if time.time() - user["last_auth"] < self.session_duration:
            return True
        else:
            user["token"] = None
            print("Session expired. Please authenticate again.")
    return False

def check_permission(self, username, resource):
    user = self.users.get(username)
    if user["role"] == "admin":
        return True
    elif user["role"] == "user" and resource != "admin_panel":
        return True
    return False

def main():
    auth = ZeroTrustAuth()

    # Симуляція автентифікації та доступу
    username = input("Enter username: ")
    password = input("Enter password: ")

    token = auth.authenticate(username, password)
    if not token:
        print("Authentication failed.")
        return

    while True:
        resource = input("Enter resource to access (or 'quit' to exit): ")
        if resource.lower() == 'quit':
            break

        if auth.verify_token(username, token):
            if auth.check_permission(username, resource):
                print(f"Access granted to {resource}")
            else:
                print(f"Access denied to {resource}")
        else:
            print("Invalid or expired token. Please authenticate again.")
            break

if __name__ == "__main__":
    main()

```

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

```

import random
import time

class ZeroTrustAuth:
    def __init__(self):
        self.users = {
            "alice": {"password": "password123", "token": None, "role": "user"},
            "bob": {"password": "securepass", "token": None, "role": "admin"}
        }
        self.session_duration = 300 # 5 minutes

    def generate_token(self):
        return ''.join(random.choices('0123456789ABCDEF', k=16))

    def authenticate(self, username, password):
        user = self.users.get(username)
        if user and user["password"] == password:
            user["token"] = self.generate_token()
            user["last_auth"] = time.time()
            print(f"Authentication successful. Token: {user['token']}")
            return user["token"]
        return None

```

Рисунок 2. Код програми

Ця програма демонструє кілька ключових принципів ZeroTrust:

1. Постійна перевірка: Кожен запит на доступ перевіряється, незалежно від того, чи був користувач раніше автентифікований.
2. Обмежений термін дії сесії: Токени автентифікації мають обмежений термін дії (у цьому випадку 5 хвилин).
3. Мінімальні привілеї: Різні користувачі мають різні ролі та права доступу.
4. Багатофакторна автентифікація: Хоча в цьому прикладі використовується лише пароль і токен, ви можете легко розширити цю систему, додавши додаткові фактори.
5. Перевірка на основі ідентичності: Кожен запит на доступ перевіряється на основі ідентичності користувача.

Ця програма є спрощеною демонстрацією і не повинна використовуватися в реальних системах без додаткових заходів безпеки. У реальному середовищі ви б

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

використовували надійніші методи зберігання паролів (наприклад, хешування), безпечніші методи генерації токенів, шифрування даних при передачі, тощо.

1. Імпорт та ініціалізація: Код починається з імпорту необхідних модулів: `random` для генерації випадкових токенів та `time` для роботи з часом. Клас `ZeroTrustAuth` ініціалізується з словником `users`, який містить інформацію про користувачів, включаючи їхні паролі, ролі та початково порожні токени. Також встановлюється тривалість сесії (`session_duration`) у 300 секунд (5 хвилин).

2. Генерація токена: Метод `generate_token()` створює випадковий 16-символьний рядок, використовуючи цифри та літери A-F. Цей токен служить тимчасовим ідентифікатором для автентифікованого користувача.

3. Автентифікація: Метод `authenticate(username, password)` перевіряє надані облікові дані користувача. Якщо користувач існує і пароль правильний, генерується новий токен, зберігається час автентифікації, і токен повертається. В іншому випадку повертається `None`.

4. Перевірка токена: `verify_token(username, token)` перевіряє, чи дійсний токен користувача. Токен вважається дійсним, якщо він збігається зі збереженим токеном користувача і не минуло більше 5 хвилин з моменту останньої автентифікації. Якщо сесія закінчилася, токен анулюється.

5. Перевірка прав доступу: Метод `check_permission(username, resource)` реалізує просту систему контролю доступу. Адміністратори мають доступ до всіх ресурсів, тоді як звичайні користувачі мають обмежений доступ (не можуть отримати доступ до «`admin_panel`»).

6. Основна функція: Функція `main()` симулює процес автентифікації та доступу до ресурсів. Вона запитує у користувача ім'я та пароль, автентифікує його, а потім дозволяє робити запити на доступ до різних ресурсів.

7. Цикл перевірки доступу: Після успішної автентифікації програма входить у цикл, де користувач може запитувати доступ до різних ресурсів. Для кожного запиту відбувається перевірка токена (чи не закінчилася сесія) та прав доступу. Це демонструє принцип постійної перевірки в ZeroTrust.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

8. Виконання програми: Останній рядок `if __name__ == '__main__':` забезпечує, що функція `main()` виконується лише якщо скрипт запускається безпосередньо, а не імпортується як модуль. Це стандартна практика в Python для відокремлення виконуваного коду від коду, який можна імпортувати.

Цей код демонструє базові принципи ZeroTrust, такі як постійна перевірка, обмежений час життя сесій, та перевірка прав доступу для кожного запиту. Однак, для реального застосування потрібно було б впровадити додаткові заходи безпеки, такі як безпечне зберігання паролів, надійніша генерація токенів, та більш складна система контролю доступу.

NIST пропонує базову абстрактну модель концептуального ядра архітектури zerotrust, яка може бути використана як основа для подальшої адаптації під конкретні умови функціонування підприємства (*Рисунок 3*). Ця модель показує важливу взаємодію між основними логічними компонентами концептуального ядра архітектури ZeroTrust.

1) Механізм політики (Policy Engine):

- приймає остаточне рішення про надання доступу суб'єкту до певного ресурсу;
- використовує політики безпеки підприємства та контекстні дані з зовнішніх джерел (системи моніторингу, аналітики загроз тощо);
- на основі алгоритму оцінки достовірності суб'єкта формує рішення про надання, відмову або скасування доступу;
- передає прийняте рішення адміністратору політики.

2) Адміністратор політики (Policy Administrator):

- відповідає за встановлення або закриття з'єднання між суб'єктом і ресурсом;
- видає відповідні команди точці виконання політики (PEP);
- у деяких реалізаціях може бути об'єднаний з механізмом політики в єдину службу прийняття рішень (PDP).

3) Точка виконання політики (PEP - Policy Enforcement Point):

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

– відповідає за встановлення, моніторинг та розрив з'єднань між суб'єктом і корпоративним ресурсом;

– виконує команди, що надходять від адміністратора політики.

Ці компоненти тісно взаємодіють для забезпечення динамічного контролю доступу на основі оцінки достовірності суб'єктів та застосування відповідних політик безпеки в середовищі ZeroTrust [6].

Архітектура ZeroTrust включає не лише основні компоненти, але й додаткові елементи, які забезпечують необхідну інформацію для прийняття рішення щодо надання доступу:

– системи безперервної діагностики та пом'якшення (CDM) - збирають дані про стан корпоративних активів (оновлення ПЗ, наявні вразливості тощо) для механізму політики;

– система відповідності галузевим стандартам - забезпечує дотримання підприємством нормативних вимог;

– сервіс керованої аналітики загроз - надає інформацію про нові вразливості та атаки з внутрішніх і зовнішніх джерел;

– сервіс журналювання активності - об'єднує дані про активи, мережевий трафік, доступ до ресурсів для моніторингу стану безпеки;

– політики доступу - визначають правила та привілеї доступу до ресурсів для авторизації;

– корпоративна РКІ - створює та реєструє сертифікати для ресурсів, суб'єктів та додатків;

– система керування ідентифікаторами - створює та керує обліковими записами користувачів;

– SIEM - збирає та аналізує дані безпеки для виявлення можливих атак та коригування політик.

Логічні компоненти архітектури zerotrust взаємодіють через окрему площину керування, а взаємодія суб'єктів відбувається через площину даних.

—

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

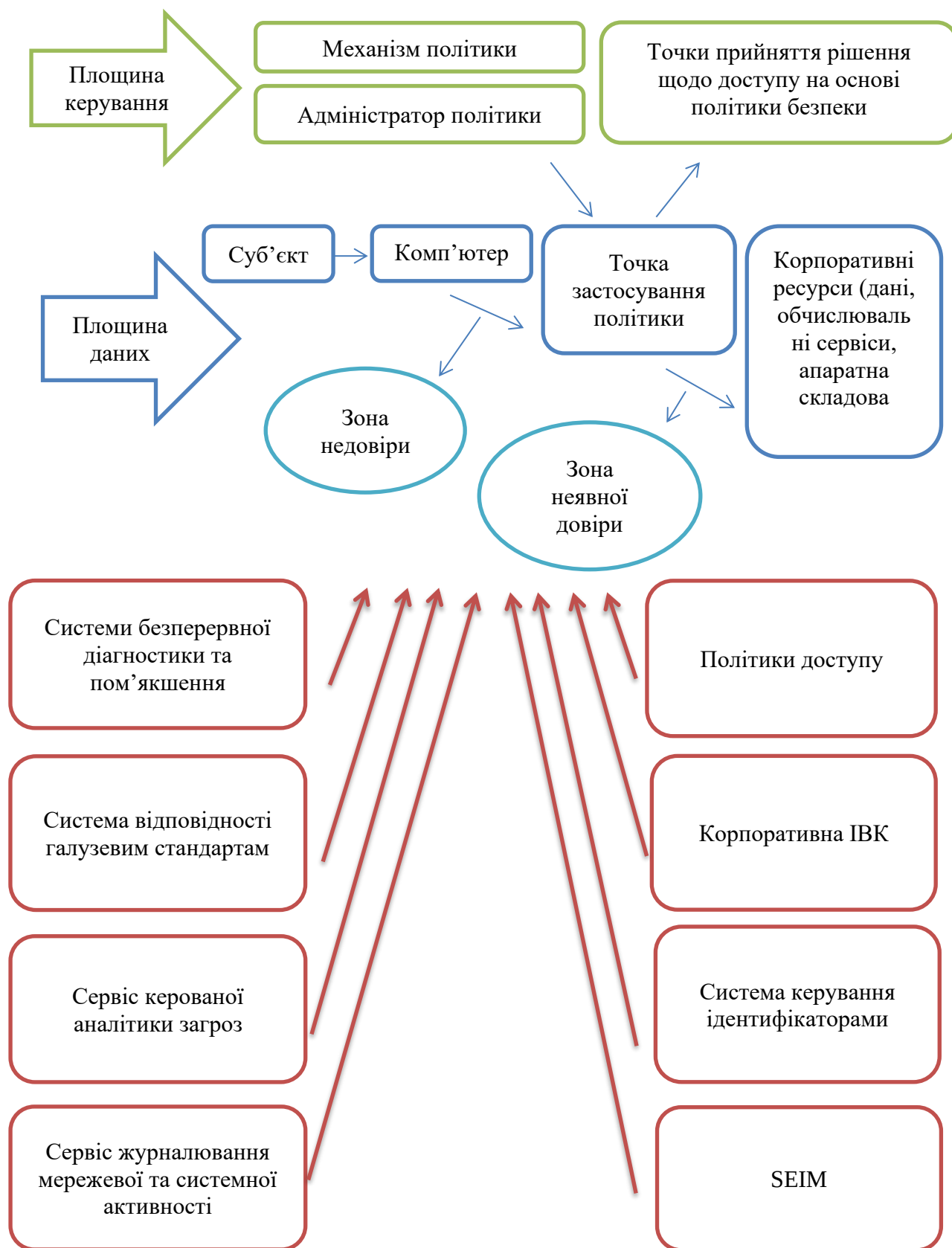


Рисунок 3. Модель концептуального ядра архітектури ZeroTrust

Незважаючи на потужність концепції, її впровадження залишається низьким - лише близько 15% команд успішно її реалізували на підприємствах. 47% опитаних не впевнені у своїй здатності забезпечити принципи «нульової довіри» наявними технологіями безпеки. Основними перешкодами впровадження є складність трансформації систем безпеки, технологічні, політичні та культурні фактори, а також ризики створення нових вразливостей. Дослідження акцентують увагу на важливості суворої автентифікації, авторизації для локальних і хмарних ресурсів, застосуванні zerotrust для безпеки хмарних середовищ та IoT. Наведено кроки переходу до zerotrust архітектури для підприємств з традиційними периметровими системами безпеки. NIST та MITRE надають детальні сценарії впровадження архітектури zerotrust.

Незважаючи на переваги, впровадження zerotrust залишається викликом для багатьох організацій через складність трансформації та необхідність ретельного планування.

Zerotrust з Kubernetes використовується для вирішення проблем безпеки на різних рівнях моделі OSI. Впровадження zerotrust систем безпеки застосовується для захисту ключових пристроїв віртуальних електростанцій. У банківському секторі zerotrust модель має переваги у протидії несанкціонованому доступу і покращенні репутації. В університетському середовищі створено структуру оцінки достовірності суб'єктів з прототипом для Moodle. Мікросервіси периметризуються на основі zerotrust принципів, що не залежать від мережі. Безпека центрів обробки даних перебудовується з використанням zerotrust з контролем передачі та автентифікацією пакетів. Архітектура безпеки IoT з нульовою довірою базується на автентифікації пристроїв через блокчейн. Zerotrust є універсальним і ефективним рішенням для сучасних проблем безпеки в різних галузях та технологічних сферах.

Отже, концепція zerotrust активно досліджується і впроваджується в багатьох контекстах як потужний інструмент забезпечення кібербезпеки, що виходить за межі традиційних периметрових рішень.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

ВИСНОВОК ДО 1 РОЗДІЛУ

Підхід ZeroTrust стає все більш актуальним у сучасних умовах, коли традиційні периметрові рішення безпеки вже не можуть забезпечити необхідний рівень захисту. Концепція ZeroTrust передбачає, що жодному суб'єкту або ресурсу не довіряється за замовчуванням, а доступ надається лише після ретельної перевірки, незалежно від місцезнаходження в мережі. Основними компонентами архітектури ZeroTrust є механізм політики, адміністратор політики та точки виконання політики, які тісно взаємодіють для динамічного контролю доступу. Додатковими критичними елементами є системи моніторингу, аналітики загроз, ідентифікації, авторизації та журналювання.

Ключовими принципами ZeroTrust є: розгляд усіх ресурсів як корпоративних активів, незалежність від місцезнаходження в мережі, надання доступу лише на одну сесію з мінімальними привілеями, динамічна політика на основі контексту, постійний моніторинг станів та безперервні процеси автентифікації/авторизації. Застосування концепції ZeroTrust дозволяє значно підвищити рівень безпеки, знизити ризики витоку даних та підвищити стійкість до сучасних кіберзагроз. Ця парадигма забезпечує гнучкість, масштабованість та можливість адаптації до змінливого ландшафту загроз, і тому все більше досліджується та впроваджується в різних галузях - від хмарних обчислень та IoT до центрів обробки даних та банківської сфери.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. КІБЕРБЕЗПЕКА ОРГАНІЗАЦІЇ: АНАЛІЗ ТРЕНДІВ ТА УПРАВЛІННЯ КУЛЬТУРОЮ

2.1. Кіберзагрози в цивільному секторі

Кіберзагрози в цивільному секторі - це серйозна проблема, яка охоплює широкий спектр викликів та потенційних ризиків для індивідумів, організацій та суспільства в цілому. В умовах зростаючої цифровізації та інтеграції інформаційних технологій у повсякденне життя, захист кіберпростору набуває критичного значення. Кіберзагрози можуть призвести до втрати конфіденційних даних, фінансових збитків, порушення діяльності критично важливої інфраструктури та навіть загрожувати національній безпеці.

З розвитком Інтернету речей (IoT) та підключенням усе більшої кількості пристроїв до мережі, зростає потенційна уразливість систем до кібератак. Хакерські групи, злочинні організації та навіть держави можуть намагатися отримати несанкціонований доступ до конфіденційних даних або здійснити кібершпигунство з метою отримання стратегічної переваги. Крадіжка персональних даних, таких як номери банківських рахунків чи медичні записи, може мати катастрофічні наслідки для окремих осіб і призвести до фінансових втрат або шахрайства.

Крім того, кіберзлочинці можуть цілеспрямовано атакувати критично важливу інфраструктуру, таку як енергетичні системи, транспортні мережі або системи зв'язку. Порушення роботи цих систем може призвести до серйозних перебоїв у наданні послуг, економічних збитків та навіть загрози життю людей. Кібератаки на промислові об'єкти, такі як підприємства чи заводи, також можуть спричинити значні збитки та порушити виробничі процеси [7].

Поширення шкідливого програмного забезпечення, такого як віруси, черв'яки або трояни, може завдати шкоди комп'ютерним системам, викрасти конфіденційні дані або навіть використовувати заражені пристрої для здійснення розподілених атак на інші цілі. Фішинг та інші методи соціальної інженерії також можуть бути використані для обману користувачів та отримання несанкціонованого доступу до їхніх облікових даних або систем.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Крім технічних аспектів, кіберзагрози в цивільному секторі також мають правові, етичні та політичні виміри. Необхідно розробити ефективні закони та політики щодо кібербезпеки, які будуть захищати приватне життя громадян та забезпечувати належний баланс між безпекою та свободами. Міжнародне співробітництво та координація зусиль є важливими для боротьби з транснаціональними кіберзагрозами та створення спільних стандартів і практик.

Організації та установи в цивільному секторі повинні інвестувати в кібербезпеку, проводити навчання співробітників, впроваджувати ефективні заходи контролю та моніторингу, а також розробляти плани реагування на інциденти. Підвищення обізнаності громадськості щодо кіберзагроз та заходів із захисту є також важливим кроком у зміцненні кібербезпеки в цивільному секторі.

Принципове значення для побудови системи кіберзахисту в хмарному середовищі згідно з концепцією ZeroTrust і подальшого управління нею має процедура попереднього вивчення стану безпеки навколишнього та внутрішнього середовища підприємства, а також визначення тенденцій їх розвитку.

Для аналізу зовнішнього середовища проєктанти систем безпеки можуть використовувати дані дослідників щодо впровадження інструментів кібербезпеки в сучасних інформаційних системах, а також аналітику проблем кібербезпеки.

Наразі існує обмежена кількість актуальних статистичних даних про кількість кіберінцидентів та їхній секторальний розподіл протягом тривалого періоду часу. Однак, деяка інформація була зібрана та систематизована.

Зібрані статистичні дані можуть бути недостатніми для системного дослідження окремих аспектів кібербезпеки. Вони можуть бути суперечливими залежно від джерел їх походження, а також можуть бути неповними та нерепрезентативними. Також виникають проблеми з математичною обробкою різноманітних даних.

Тому важливо приділити особливу увагу проблемам аналізу стану кібербезпеки. Нижче наведено кілька прикладів кіберзагроз у цивільному секторі протягом 2022-2024 років.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

1) Кібератака на Colonial Pipeline у травні 2022 року за допомогою вірусу-вимагача, що призвела до тимчасового припинення роботи найбільшого нафтопроводу на Східному узбережжі США.

2) Масштабна фішингова атака на клієнтів Microsoft у червні 2023 року, в результаті якої були викрадені дані облікових записів та конфіденційна інформація.

3) Витік даних понад 10 мільйонів користувачів популярного додатку для знайомств Tinder у січні 2024 року, включаючи імена, дати народження та геолокаційні дані.

4) Кібератака на системи управління авіаційним рухом у Німеччині у березні 2022 року, яка призвела до скасування сотень рейсів та тимчасового припинення роботи кількох аеропортів.

5) Атака вірусу-вимагача на мережу лікарень у Великій Британії у жовтні 2023 року, що завдало великої шкоди ІТ-системам та призвело до затримок у наданні медичної допомоги.

6) Масштабна DDoS-атака на кілька великих банків у США у липні 2022 року, що паралізувала їхні онлайн-сервіси протягом кількох годин.

7) Витік конфіденційних документів у результаті хакерської атаки на урядову установу Канади у грудні 2023 року, включаючи секретну інформацію про національну безпеку.

8) Кібератака на енергетичну систему Іспанії у квітні 2024 року, що призвела до тимчасового відключення електроенергії у кількох регіонах країни.

9) Поширення нового деструктивного вірусу-вимагача під назвою «CryptoLocker» у січні 2023 року, який заразив сотні тисяч комп'ютерів по всьому світу та вимагав викуп за розблокування даних.

10) Інцидент з витоком даних у провідній хмарній платформі AWS у листопаді 2022 року, що вплинув на безліч клієнтів і компаній, які використовували її сервіси.

Ці приклади демонструють постійну загрозу кібератак і необхідність посилення заходів кібербезпеки в цивільному секторі для захисту конфіденційних

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

даних, критичної інфраструктури та забезпечення безперебійної роботи організацій та установ.

Ось кілька способів, якими боролися з кіберзагрозами в цивільному секторі у 2022-2024 роках:

1) Посилення заходів кібербезпеки: Багато організацій та установ інвестували значні кошти в оновлення систем безпеки, встановлення новітнього захисного програмного забезпечення, навчання персоналу з питань кібербезпеки та наймання фахівців із цієї галузі.

2) Співпраця з правоохоронними органами та розвідувальними службами: Для протидії складним кібератакам організації тісно співпрацювали з національними та міжнародними правоохоронними органами, розвідувальними службами та групами кібербезпеки, обмінюючись інформацією та спільно розслідуючи інциденти.

3) Розробка та впровадження нових технологій: Були розроблені нові інноваційні рішення в галузі кібербезпеки, такі як штучний інтелект для виявлення аномалій, блокчейн для забезпечення безпеки даних та квантові технології для посилення шифрування.

4) Підвищення обізнаності громадськості: Уряди, компанії та некомерційні організації активно проводили кампанії з підвищення обізнаності громадськості щодо кіберзагроз, організовували тренінги та розповсюджували рекомендації щодо безпечного використання інтернету та захисту даних.

5) Законодавчі ініціативи: Багато країн посилили законодавство у сфері кібербезпеки, запровадили нові нормативні акти та правила, спрямовані на боротьбу з кіберзлочинністю, захист критичної інфраструктури та забезпечення безпеки громадян в інтернеті.

6) Міжнародне співробітництво: Кіберзагрози мають транснаціональний характер, тому країни об'єднували зусилля для боротьби з ними. Були укладені багатосторонні угоди, створені спільні оперативні центри та налагоджений обмін розвідувальними даними між партнерами.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

7) Реагування на інциденти: Після кібератак організації активували плани реагування на інциденти, відновлювали резервні копії даних, усували вразливості в системах та посилювали заходи безпеки, щоб запобігти подальшим атакам.

8) Страхування від кіберризиків: Деякі компанії та організації почали страхувати себе від фінансових втрат, пов'язаних із кіберінцидентами, оскільки такі ризики стали дуже реальними.

Комплексний підхід, що поєднував технічні, правові, освітні та організаційні заходи, був ключовим для ефективної боротьби з кіберзагрозами в цивільному секторі протягом 2022-2024 років.

Кіберзагрози в цивільному секторі залишаються однією з найсерйозніших проблем сучасності. Зростаюча залежність від інформаційних технологій у поєднанні зі зловмисними діями хакерів, кіберзлочинців та держав-агресорів створюють небезпечне середовище, в якому приватні особи, організації та критично важлива інфраструктура перебувають під постійною загрозою [22, с. 226].

Протягом 2022-2024 років ми стали свідками численних кібератак, що призвели до витоку конфіденційних даних, фінансових збитків, порушення роботи життєво важливих систем та навіть загрози національній безпеці. Незважаючи на зусилля з боку урядів, компаній та міжнародних організацій, кіберзагрози продовжують еволюціонувати та ставати все більш витонченими та руйнівними.

Ефективна боротьба з цими загрозами вимагає комплексного підходу, що поєднує технічні рішення, законодавчі ініціативи, підвищення обізнаності громадськості та міжнародне співробітництво. Інвестиції в кібербезпеку, розвиток нових технологій, таких як штучний інтелект та блокчейн, а також посилення заходів захисту критичної інфраструктури мають вирішальне значення.

Крім того, необхідно приділяти більше уваги навчанню персоналу та формуванню культури кібербезпеки на всіх рівнях організацій та установ. Людський фактор часто залишається найслабшою ланкою в ланцюзі захисту, і тому підвищення обізнаності та освіта співробітників мають вирішальне значення.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

Нарешті, міжнародне співробітництво та координація зусиль є ключовими для боротьби з транснаціональними кіберзагрозами. Обмін розвідувальними даними, спільні операції та гармонізація законодавства можуть значно посилити глобальну кібербезпеку та знизити ризики для цивільного сектору.

Підсумовуючи, кіберзагрози в цивільному секторі вимагають пильної уваги та невинних зусиль з боку всіх зацікавлених сторін. Лише шляхом об'єднання ресурсів, експертних знань та рішучих дій ми зможемо створити більш безпечний кіберпростір для громадян, бізнесу та держави в майбутньому.

2.2. Підвищення та вдосконалення кіберкультури

Підвищення та вдосконалення кіберкультури є надзвичайно важливим аспектом забезпечення кібербезпеки в сучасному цифровому світі. Кіберкультура охоплює сукупність знань, навичок, цінностей та практик, пов'язаних з безпечним та етичним використанням інформаційних технологій. Вона відіграє ключову роль у формуванні свідомого ставлення до кібербезпеки та зміцненні захисту від кіберзагроз.

Перш за все, підвищення обізнаності громадськості щодо ризиків та загроз у кіберпросторі є фундаментальним кроком у розвитку кіберкультури. Люди повинні усвідомлювати потенційні наслідки, пов'язані з кібератаками, витоком даних та іншими інцидентами у сфері кібербезпеки. Лише за умови розуміння важливості цього питання можна очікувати, що громадяни будуть більш обережними та дбатимуть про захист своїх персональних даних і пристроїв [2, с. 90].

Освіта та навчання є невід'ємною частиною формування кіберкультури. Від шкільного віку необхідно вводити основи кібербезпеки та цифрової грамотності до навчальних програм. Це дозволить молодим людям набути необхідних знань і навичок для безпечного користування Інтернетом та захисту своєї онлайн-присутності.

На робочих місцях компаніям та організаціям слід проводити регулярні тренінги з кібербезпеки для своїх співробітників. Це допоможе їм зрозуміти важливість дотримання політик безпеки, розпізнавати потенційні загрози та знати,

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

як діяти у разі інциденту. Створення культури кібербезпеки в організації є життєво важливим для захисту її активів та даних.

Крім того, слід заохочувати відповідальне та етичне використання інформаційних технологій. Кіберкультура повинна засуджувати будь-які форми кібершахрайства, крадіжки даних чи зловмисної діяльності в Інтернеті. Замість цього вона має пропагувати повагу до конфіденційності, інтелектуальної власності та прав людини в кіберпросторі.

Держави також відіграють важливу роль у сприянні розвитку кіберкультури. Вони можуть розробляти та впроваджувати національні стратегії кібербезпеки, здійснювати інформаційні кампанії та забезпечувати відповідне законодавче регулювання сфери кібербезпеки.

Важливо також заохочувати співпрацю та обмін досвідом між різними зацікавленими сторонами, такими як уряди, приватний сектор, академічні кола та громадянське суспільство. Об'єднання зусиль сприятиме поширенню найкращих практик та інновацій у галузі кібербезпеки та підвищенню рівня кіберкультури в суспільстві [14, с. 145].

Ось кілька прикладів ініціатив та заходів, спрямованих на підвищення та вдосконалення кіберкультури:

1) Національна програма підвищення обізнаності з питань кібербезпеки у Великій Британії: Ця програма, розпочата у 2014 році, має на меті інформувати громадян про ризики та загрози в Інтернеті, а також надавати практичні поради щодо безпечного використання онлайн-сервісів та захисту персональних даних.

2) Кампанія «Stop.Think.Connect» у США: Ця масштабна національна кампанія, запущена у 2010 році, об'єднує зусилля уряду, приватного сектору та неурядових організацій з метою підвищення обізнаності населення про кіберзагрози та пропагування безпечної поведінки в Інтернеті.

3) Програма «е-Гарант» в Естонії: Ця програма, започаткована у 2007 році, спрямована на навчання школярів основам кібербезпеки та цифрової грамотності. Вона включає інтерактивні онлайн-курси, тренінги для вчителів та інші ініціативи.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

4) Тренінги з кібербезпеки для співробітників Microsoft: Ця технологічна компанія регулярно проводить обов'язкові тренінги для своїх працівників, щоб підвищити їхню обізнаність щодо кіберзагроз, навчити розпізнавати фішингові атаки та дотримуватися політик безпеки.

5) Програма «Кіберпатруль» у Сінгапурі: Ця ініціатива об'єднує волонтерів, які проводять навчальні сесії та інформаційні кампанії для підвищення обізнаності громадськості з питань кібербезпеки, зокрема для дітей та літніх людей.

6) «Місяць кібербезпеки» в Європейському Союзі: Щороку в жовтні проводиться масштабна кампанія з метою підвищення обізнаності громадян та організацій щодо кіберзагроз. Вона включає різноманітні заходи, такі як конференції, тренінги, онлайн-ресурси та публікації.

7) Програма «Безпечний інтернет» у Канаді: Ця федеральна програма пропонує ресурси та навчальні матеріали для батьків, вчителів та дітей, щоб допомогти їм безпечно користуватися Інтернетом та розуміти пов'язані з цим ризики.

8) Тренінги з кібербезпеки для малого та середнього бізнесу: Багато організацій та асоціацій проводять навчальні курси для представників малого та середнього бізнесу, щоб допомогти їм зміцнити свої системи безпеки та підвищити стійкість до кіберзагроз.

Ці приклади демонструють різноманітні підходи та зусилля, спрямовані на підвищення кіберкультури серед громадян, працівників, учнів та організацій в усьому світі [31, с. 158].

Згідно з міжнародними стандартами у галузі інформаційної безпеки та кібербезпеки, забезпечення відповідного рівня захисту інформаційних активів вимагає впровадження узгоджених заходів, таких як визначення пріоритетних завдань з інформаційної безпеки, детальне планування робіт, контроль за їх виконанням та коригування системи захисту в залежності від цінності інформації та виявлених вразливостей. Дослідження системи управління інформаційною безпекою (СУІБ) вказує на важливість урахування культурних особливостей на

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

різних рівнях розробки стандартів, що може бути корисним для різних типів підприємств.

У загальному випадку аналізуються навмисні загрозливі дії, що можуть завдати шкоди власнику інформаційної системи як з боку хакерів, так і персоналу системи, чия небезпечна поведінка може бути спричинена помилками процедури розподілу повноважень (Таблиця 1).

Види вірогідних небезпечних дій в рамках концепції «повної недовіри»

Таблиця 1

№	Опис небезпечної дії	Особливості реалізації
1.	Відмова від факту відправлення деякого повідомлення.	Без доступу до ІС
2.	Маскування (імітація прав) – доступ в систему з використанням прав і привілеїв іншого користувача з метою нелегального отримання доступу до конфіденційної інформації або до деяких (можливо платних) сервісів, або ініціалізації та запуску процесів і програм.	Несанкціонований Доступ Доступ з боку глобальної мережі
3.	Модифікація переданого або прийнятого повідомлення і спроба стверджувати, що воно прийнято саме у такому вигляді від будь-кого.	Легальний доступ Доступ з боку глобальної мережі
4.	Підробка – створення фіктивного повідомлення, зокрема, від імені конкретного користувача системи	Несанкціонований доступ Доступ з боку глобальної мережі
5.	Повтор повідомлення, яке передавалось раніше	Легальний доступ Доступ з боку глобальної мережі
6.	Перехоплення активне (перехоплення типу А) – втручання в роботу інформаційної системи з метою вилучення або блокування повідомлень, що передаються.	Несанкціонований доступ Доступ з боку глобальної мережі
7.	Перехоплення пасивне (перехоплення типу П) – втручання в роботу інформаційної системи з метою ознайомлення із змістом повідомлень, що передаються	Несанкціонований доступ Доступ з боку глобальної мережі

Культурні фактори здатні значно впливати на організацію управління підприємством та цілі діяльності, включаючи прийняття рішень, впровадження інновацій та нових практик, забезпечення комунікацій, мотивацію персоналу та його мобілізацію на досягнення позитивних результатів.

Питання управління кіберкультурою на підприємстві в корпоративному та індивідуальному сенсі розглянуто обмежено, тому акцентується увага на підвищенні її рівня, виходячи з концепції ZeroTrust.

Для протидії навмисним загрозливим діям, що можуть завдати шкоди власнику інформаційної системи, використовуються різноманітні механізми технічного та криптографічного захисту інформації. Це включає:

1) Розмежування доступу - контроль та обмеження прав доступу користувачів до інформаційних ресурсів відповідно до їх ролей та повноважень.

2) Ведення захищених журналів обліку дій в системі - реєстрація та моніторинг активності користувачів та системних подій для виявлення потенційних загроз та інцидентів безпеки.

3) Застосування геш-функцій та кодів автентифікації повідомлень - використання криптографічних методів для забезпечення цілісності та автентичності даних при передачі та зберіганні.

4) Формування та перевірка цифрового підпису та цифрових сертифікатів - використання асиметричної криптографії для підтвердження автентичності та неспростовності електронних документів та ідентифікації користувачів.

5) Реалізація організаційних заходів, таких як навчання, виховання та моніторинг дій персоналу - підвищення обізнаності співробітників щодо інформаційної безпеки, формування культури кібербезпеки та контроль за дотриманням правил безпеки.

Згідно з принципами системи управління інформаційною безпекою (СУІБ), ці заходи відображаються в керівному документі вищого рівня - політиці інформаційної безпеки підприємства. На основі цієї політики формуються конкретні правила безпеки, які визначають припустимі та обов'язкові процедури в

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

системі захисту. Це забезпечує системний та комплексний підхід до забезпечення інформаційної безпеки на підприємстві.

Згідно з публікаціями про кіберінциденти, основними суб'єктами концепції «повної недовіри» є користувачі 1 до N, які отримують доступ до інформаційних активів підприємства на підставі затверджених функціональних обов'язків та визначених повноважень (Рисунок 4).

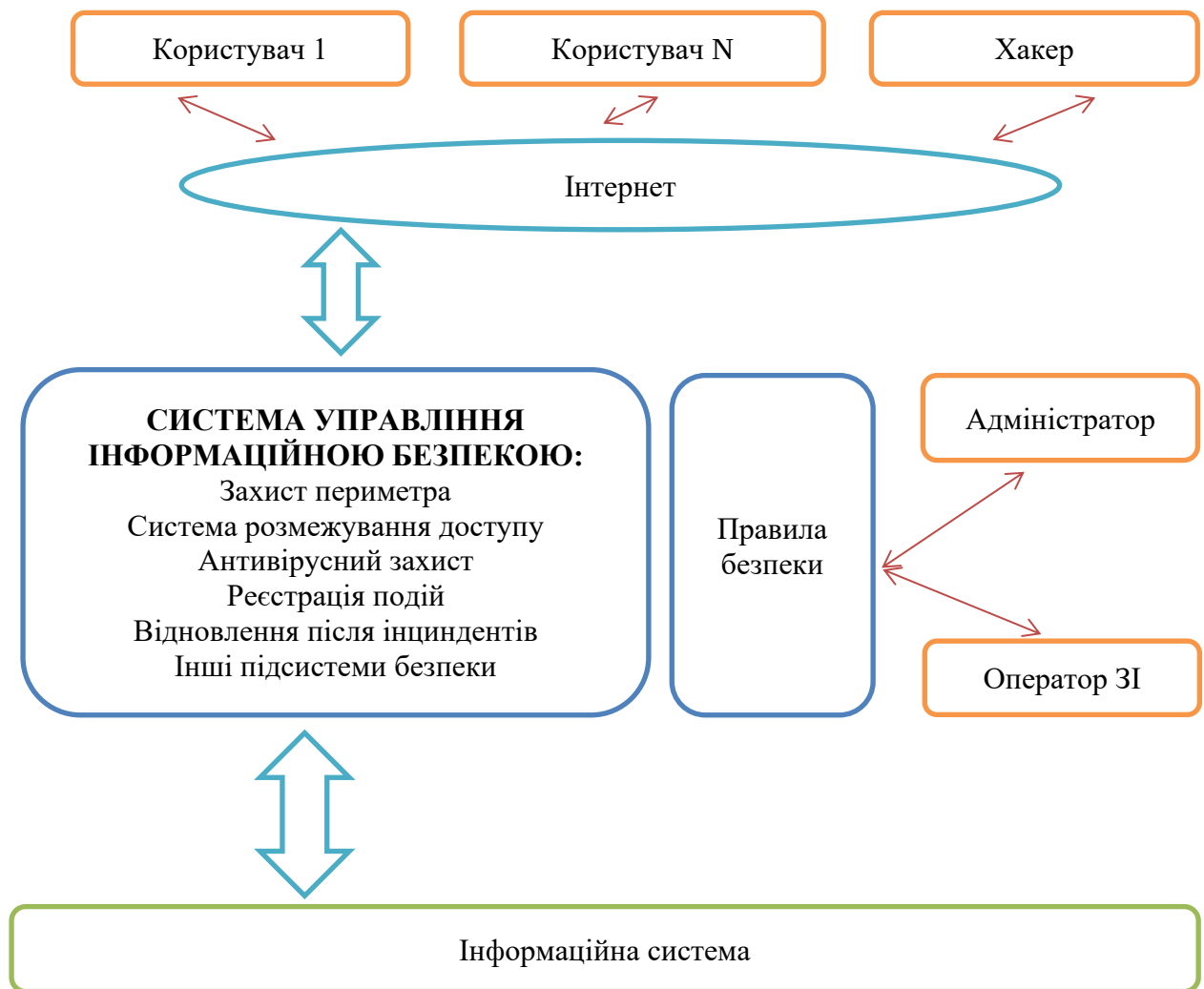


Рисунок 4. Основні суб'єкти концепції «повної недовіри»

Політика інформаційної безпеки є вищим керівним документом, що встановлює загальні вимоги та принципи забезпечення інформаційної безпеки на підприємстві. Вона визначає пріоритетні завдання, методи їх вирішення, відповідальних осіб та загальні організаційно-технічні заходи захисту інформаційних активів. На основі політики безпеки розробляються більш детальні

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

інструкції, процедури та правила, що регламентують конкретні дії персоналу та застосування технічних засобів захисту.

Згідно з концепцією повної недовіри, користувачі, адміністратори безпеки, оператори систем захисту інформації та хакери можуть свідомо або навмисно сприяти небезпечним діям у комп'ютерних системах. Це може вплинути на загальну безпеку інформаційної системи, а також на її політику безпеки. Необхідно ретельно контролювати дії цих суб'єктів і вживати заходів для запобігання можливим загрозам.

Система управління якістю є важливою складовою управління бізнесом, яка базується на аналізі ризиків. Вона включає в себе планування, виконання, контроль і коригування дій для досягнення поставлених цілей організації. Методологія побудови такої системи ґрунтується на наукових і практичних ідеях з управління якістю, визначених міжнародними стандартами серії ISO 9001 [36, с. 50].

Один з ключових принципів стандарту ISO 9001 - максимальне залучення персоналу для досягнення успіху. Це означає, що кожен співробітник повинен бути включений у процес досягнення цілей підприємства, що сприяє розвитку їхніх навичок та компетентності.

Фактично, заходи кіберзахисту, що мають технічний характер, не є достатніми для ефективного захисту системи, оскільки більшість кібератак пов'язані з помилковими діями або недбалістю людей. Щоб поліпшити ситуацію, необхідно:

- 1) Оперативно реагувати на ситуації, що виникають в інформаційній інфраструктурі.
- 2) Покращувати технічні та організаційні навички з кібербезпеки персоналу шляхом проведення тренінгів та навчань.
- 3) Використовувати принципи управління якістю згідно зі стандартом ISO 9001 та стандартами ISO/IEC 27000 для розробки стратегії захисту інформаційних активів.

Етапи реалізації процесів управління культурою кібербезпеки підприємства збігаються з загальними етапами системи управління інформаційною безпекою:

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

1) Планування - визначення цілей, політики та процедур кібербезпеки, оцінка ризиків.

2) Реалізація - впровадження заходів безпеки, навчання персоналу, розподіл ролей та обов'язків.

3) Перевірка - моніторинг ефективності системи, проведення аудитів та тестування на проникнення.

4) Дії - коригування системи на основі результатів перевірки, безперервне вдосконалення.

Таким чином, поєднання принципів управління якістю та інформаційною безпекою дозволяє створити комплексну систему кіберзахисту, яка враховує як технічні, так і людські фактори. (Рисунок 5).

На етапі Планування побудови СУІБ визначаються головні завдання:

1) Визначення області дії СУІБ - встановлення меж системи управління інформаційною безпекою, враховуючи специфіку діяльності підприємства, його структуру та інформаційні активи.

2) Формування вихідних вимог до проєктування - визначення цілей, принципів та критеріїв ефективності СУІБ, які повинні бути досягнуті в результаті її впровадження.

3) Збирання даних про об'єкт захисту - інвентаризація та класифікація інформаційних активів, аналіз бізнес-процесів та інформаційних потоків.

4) Вивчення вимог державних та відомчих нормативних актів - дослідження законодавчої та нормативної бази у сфері інформаційної безпеки, які стосуються діяльності підприємства.

5) Визначення правил та обмежень, що стосуються конкретного виду підприємств - врахування галузевих стандартів та кращих практик забезпечення інформаційної безпеки.

Одним з важливих аспектів цього етапу є визначення початкового стану індивідуальної та групової культури інформаційної безпеки серед персоналу підприємства. Для отримання первинної інформації використовується опитування персоналу, яке може проводитися у зручний спосіб, наприклад, шляхом

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

електронного анкетування. Важливими елементами методики опитування є формування змістовної частини анкет та методика подальшої обробки отриманих даних.



Рисунок 5. Організаційна модель СУБ

Етап реалізації побудови СУБ передбачає впровадження запланованих організаційно-технічних заходів та керування механізмами контролю. Для успішної реалізації цього етапу необхідно мати:

- 1) Документовані процедури впровадження - детальні інструкції та плани реалізації заходів безпеки, визначення відповідальних осіб та термінів виконання.

2) Планування й управління необхідними ресурсами - забезпечення необхідних фінансових, технічних та людських ресурсів для ефективного функціонування СУІБ.

3) Керування інцидентами безпеки - розробка процедур виявлення, реєстрації, аналізу та реагування на інциденти інформаційної безпеки.

4) Процедури навчання і інформування персоналу - проведення регулярних тренінгів та підвищення обізнаності співробітників щодо питань інформаційної безпеки, їх ролі та обов'язків у забезпеченні безпеки.

Ці заходи спрямовані на забезпечення ефективного функціонування СУІБ та мінімізацію ризиків інформаційної безпеки для підприємства.

На етапі побудови СУІБ - Контроль - здійснюється аналіз безпекової обстановки, перевірка досягнення мети, моніторинг вразливостей і недоліків, періодичні оцінки та актуалізація. Ця процедура вимагає від учасників найвищого рівня професійної підготовки. У разі можливості, вона реалізується залученням зовнішніх незалежних експертів.

На етапі «Дії» необхідно виправити виявлені на попередньому етапі циклу вразливості, помилки та недоліки СУІБ, забезпечуючи тим самим підвищення ефективності.

Політика інформаційної безпеки є основою для побудови системи управління інформаційною безпекою підприємства (СУІБ). Вона визначає стратегію організації в цій області, включаючи пріоритетність завдань і виділення ресурсів. Політика інформаційної безпеки також є джерелом для розробки часткових політик безпеки, які регулюють процедури різних складових системи інформаційної безпеки, таких як:

1) Розмежування доступу - визначення прав та повноважень користувачів щодо доступу до інформаційних ресурсів.

2) Облік подій - реєстрація та моніторинг дій користувачів та системних подій.

3) Антивірусний захист - використання спеціалізованого програмного забезпечення для виявлення та запобігання шкідливому коду.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

4) Шифрування - застосування криптографічних методів для захисту конфіденційності та цілісності даних.

5) Резервування і відновлення - створення резервних копій та планування процедур відновлення після збоїв та інцидентів.

6) Реагування на інциденти - розробка планів та процедур виявлення, аналізу та усунення наслідків інцидентів інформаційної безпеки.

Формування політики інформаційної безпеки включає в себе:

1) Визначення нормативних документів і стандартів - врахування законодавчих вимог та галузевих стандартів.

2) Управління ризиками - ідентифікація, аналіз та оцінка ризиків інформаційної безпеки, вибір методів обробки ризиків.

3) Оцінку відповідності стандартам - перевірка системи на відповідність вимогам стандартів та нормативних документів.

4) Визначення ефективності системи захисту від загроз безпеки - моніторинг та вимірювання результативності заходів безпеки.

Це допомагає забезпечити конфіденційність, цілісність та доступність інформаційних активів підприємства.

Для побудови ефективної системи захисту інформації необхідно визначити границі системи, в межах яких повинен бути забезпечений режим інформаційної безпеки (границі СУІБ). Опис границь системи повинен включати:

1) Опис структури організації

2) Розміщення комп'ютерів і підтримуючої інфраструктури

3) Ресурси інформаційних систем, що підлягають захисту

4) Технології обробки інформації

5) Розв'язувані завдання

Для підвищення рівня кіберкультури доцільно уточнити архітектуру системи управління кібербезпекою, враховуючи специфіку підприємства та принципи концепції ZeroTrust.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				51
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 6. Онтологічна модель формування вимог до системи правління інформаційної безпеки

Відстежені ланцюги визначення вимог до процедур безпеки дозволили створити онтологічну модель визначення та коригування вимог в СУІБ (Рисунок 6). Процедури оцінки відповідності в онтологічній моделі виконують роль арбітра в питанні досягнення мети щодо забезпечення інформаційної безпеки або необхідного коригування політики інформаційної безпеки. Концепція «повної недовіри» визначає додаткові умови для політики інформаційної безпеки, яка в свою чергу визначає вимоги до часткових політик безпеки, які встановлюють правила та обмеження для створення системи захисту, включаючи підсистему управління культурою кібербезпеки підприємства. Для побудови системи захисту інформації необхідно визначити границі системи, для якої повинен бути забезпечений режим інформаційної безпеки (границі СУІБ). Опис границь системи включає опис структури організації, розміщення комп'ютерів і підтримуючої інфраструктури, ресурсів інформаційних систем, що підлягають захисту, технології обробки інформації та розв'язуваних завдань. Для підвищення кіберкультури доцільно уточнити архітектуру системи управління кібербезпекою.

Підвищення та вдосконалення кіберкультури на підприємстві є важливим аспектом забезпечення інформаційної безпеки. Це охоплює знання, навички,

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

ставлення та поведінку персоналу щодо інформаційної безпеки та кібербезпеки. Високий рівень кіберкультури сприяє підвищенню обізнаності працівників про загрози, ризики та належні практики захисту інформації. Впровадження концепції zerotrust, регулярне навчання, тренінги та комунікаційні кампанії, чітке визначення політик та відповідальності, моніторинг та аналіз інцидентів інформаційної безпеки, а також прихильність керівництва до принципів інформаційної безпеки - це всі ключові елементи ефективної кіберкультури. Підвищення та вдосконалення кіберкультури є невід’ємною частиною комплексного підходу до забезпечення інформаційної безпеки та кібербезпеки на підприємстві.

2.3. Модель оцінки культури кібербезпеки

Модель оцінки культури кібербезпеки є важливим інструментом для організацій, які прагнуть підвищити рівень захищеності своїх інформаційних систем та даних. Ця модель допомагає визначити сильні та слабкі сторони організаційної культури в контексті кібербезпеки, а також надає рекомендації щодо вдосконалення процесів та практик [24, с.345].

Культура кібербезпеки охоплює сукупність цінностей, переконань, звичок та моделей поведінки, які визначають ставлення співробітників до питань інформаційної безпеки. Вона впливає на те, як працівники взаємодіють з технологіями, обробляють конфіденційні дані та реагують на потенційні загрози кібербезпеки.

Ефективна модель оцінки культури кібербезпеки повинна враховувати різноманітні чинники, такі як рівень обізнаності співробітників, наявність політик та процедур безпеки, підтримка керівництва, навчання та підвищення кваліфікації персоналу, а також загальний підхід організації до управління ризиками [8].

Одним з ключових компонентів моделі є проведення опитувань та інтерв’ю з працівниками різних рівнів та підрозділів організації. Це дозволяє отримати цінні відомості про сприйняття кібербезпеки, ставлення до правил та процедур, а також виявити можливі прогалини в знаннях чи навичках.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Крім того, модель передбачає аналіз існуючих політик, процедур та технічних засобів захисту. Це допомагає оцінити відповідність організації нормативним вимогам та галузевим стандартам, а також визначити потенційні ризики та вразливості.

Після збору та аналізу даних модель пропонує конкретні рекомендації щодо вдосконалення культури кібербезпеки. Це може включати розробку навчальних програм, впровадження нових процедур, посилення технічних засобів захисту, а також заходи з підвищення обізнаності та залучення співробітників.

Регулярна оцінка культури кібербезпеки дозволяє організаціям відстежувати прогрес у вдосконаленні безпекових практик та своєчасно реагувати на нові виклики та загрози. Це сприяє створенню стійкої та ефективної системи захисту інформаційних ресурсів організації.

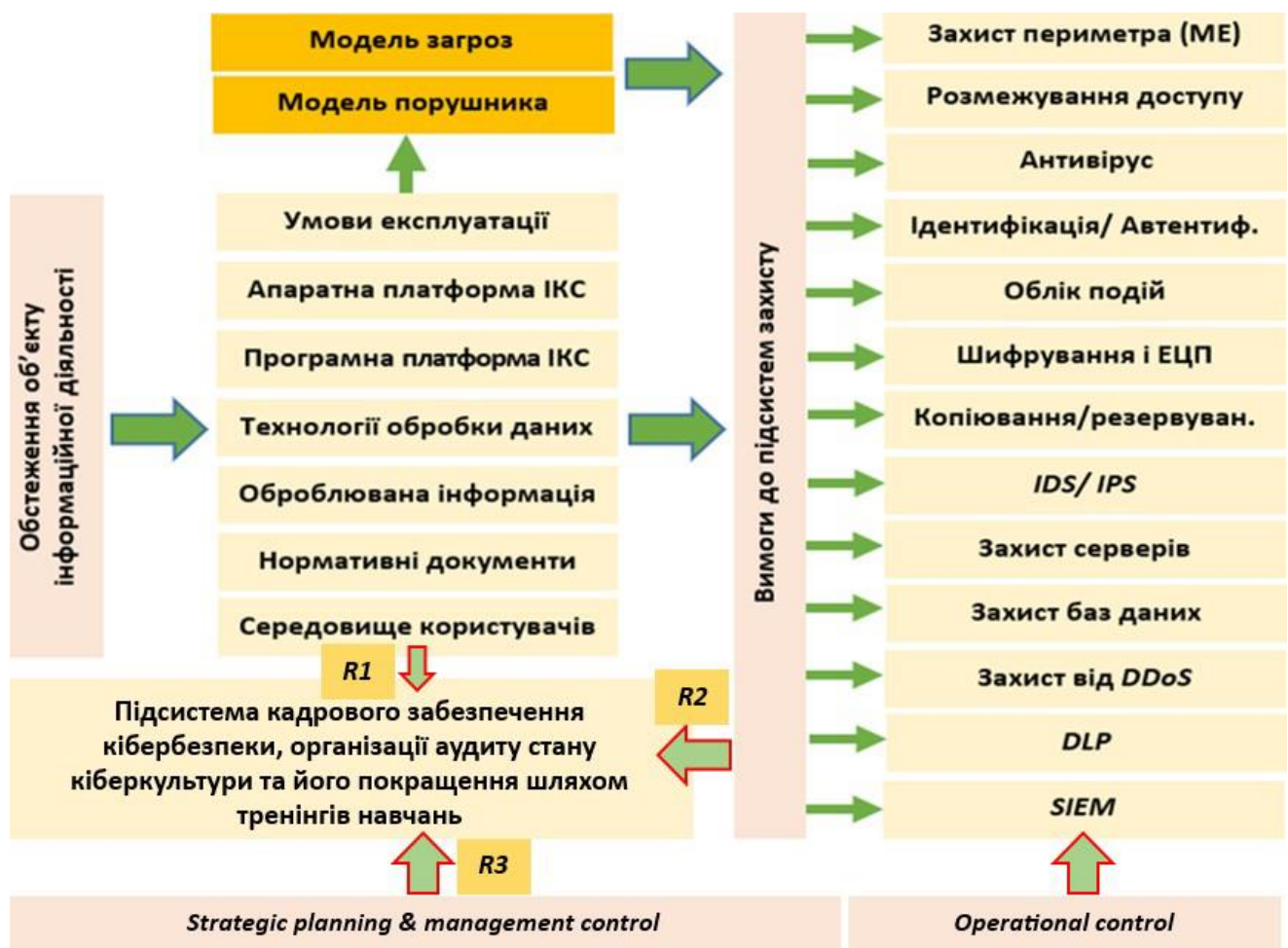


Рисунок 7. Модель формування системи кібербезпеки

Результати вивчення та порівняння сучасних підходів до побудови систем кібербезпеки дозволили узагальнити існуючі засади створення моделі формування системи та внести деякі вдосконалення. На основі цього запропоновано Модель формування системи кібербезпеки, яка має такі особливості:

- 1) Визначає умовні межі різних рівнів управління.
- 2) Враховує особливості формування та функціонування підсистеми кадрового забезпечення кіберкультури.

Модель бере до уваги три регуляторних впливи на підсистему кадрового забезпечення кіберкультури (Рисунок 7):

- 1) Висновки за результатами обстежень та аудитів об'єктів інформаційної діяльності та середовищ інформаційних систем.
- 2) Вимоги щодо побудови підсистем кіберзахисту.
- 3) Вказівки, доручення та інші дії організаційно-просвітнього характеру з боку керівного складу організації.

Для визначення деталей побудови як системи кіберзахисту в цілому, так і її окремих підсистем (на рисунку їх налічується чотирнадцять), необхідно провести системний аналіз реального проєкту інформаційної мережі об'єкту критичної інфраструктури та обстеження всіх ключових об'єктів інформаційної діяльності щодо впровадження заходів з кіберзахисту.

У випадку побудови інформаційної мережі на основі технології корпоративної хмари, доступ до хмари повинен здійснюватися за допомогою захищених каналів (наприклад, VPN). Концентрація основних сервісів безпеки в хмарі розподіляється між клієнтами та провайдером сервісних послуг, що знижує матеріальні, фінансові та організаційні витрати на забезпечення кіберзахисту [12].

Для підприємства, яке має статус державного або обробляє державні інформаційні ресурси, пріоритетними процедурами системи захисту інформації вважаються технології, що реалізуються такими підсистемами:

- 1) Автентифікації та ідентифікації
- 2) Розмежування доступу
- 3) Антивірусного захисту

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

- 4) Обліку подій
- 5) Копіювання і резервування
- 6) Шифрування трафіку та цифрового підпису
- 7) Захисту периметра

Побудова захищеної розподіленої корпоративної мережі, яка має логічне або фізичне з'єднання з глобальною мережею, повинна враховувати тенденції розвитку стану безпеки у кіберпросторі та базуватися на системному аналізі трендів розвитку кіберінцидентів у світі. Це дозволить створити ефективну та адаптивну систему кіберзахисту, здатну протистояти сучасним загрозам та мінімізувати ризики для інформаційних ресурсів організації.

ВИСНОВОК ДО 2 РОЗДІЛУ

Сучасні публікації про кібербезпеку містять багато статистичних даних, але не надають достатньо інформації для системного аналізу розвитку подій у кіберпросторі. Запропоновані математичні методи та аналіз трендів загроз кібербезпеці можуть допомогти сформулювати пріоритети політики безпеки на основі концепції ZeroTrust. Важливо також підвищити кіберкультуру персоналу та забезпечити відповідну навчально-тренувальну програму. Оцінка поточного стану кіберкультури та трендів загроз кібербезпеці дозволяє оперативно реагувати та коригувати політику безпеки. Визначення базових завдань управління кібербезпекою та формування системи кібербезпеки на основі цих завдань є важливим кроком у дослідженні. Організаційно-технічні положення політики безпеки підприємства на основі концепції ZeroTrust також потребують уваги.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

РОЗДІЛ 3. ПОЛІТИКА БЕЗПЕКИ НА ОСНОВІ ZEROTRUST

3.1. Модель загроз та вимоги до апаратного засобу автентифікації ZeroTrust

Модель загроз та вимоги до апаратного засобу автентифікації в контексті концепції ZeroTrust являють собою важливі складові забезпечення кібербезпеки в сучасних умовах. Підхід ZeroTrust базується на принципі «не довіряй нікому», що означає відсутність довіри до будь-яких користувачів, пристроїв або додатків, незалежно від їхнього місцезнаходження в мережі.

Ефективна реалізація концепції ZeroTrust вимагає ретельного аналізу потенційних загроз та ризиків, пов'язаних з доступом до інформаційних ресурсів. Модель загроз передбачає ідентифікацію та класифікацію можливих векторів атак, уразливостей систем та потенційних порушників безпеки.

Одним з ключових елементів захисту в рамках ZeroTrust є використання надійних засобів автентифікації. Апаратні засоби автентифікації, такі як смарт-картки або апаратні токени, забезпечують вищий рівень безпеки порівняно з традиційними методами, заснованими лише на паролях [37, с. 124].

Вимоги до апаратного засобу автентифікації в концепції ZeroTrust включають високий рівень захисту від підробки та компрометації даних, стійкість до спроб зламу та фізичних атак, а також простоту інтеграції з існуючими системами інформаційної безпеки.

Важливим аспектом є забезпечення конфіденційності та цілісності даних автентифікації протягом усього їх життєвого циклу, починаючи від генерації та завершуючи знищенням. Це вимагає використання криптографічних методів захисту даних та впровадження процедур безпечного управління ключами.

Крім того, апаратний засіб автентифікації повинен підтримувати багатофакторну автентифікацію, яка поєднує кілька різних факторів, таких як щось, що користувач знає (наприклад, пароль), щось, що він має (наприклад, апаратний токен), та щось, що він є (наприклад, біометричні дані).

Ефективна реалізація концепції ZeroTrust також вимагає постійного моніторингу та аудиту доступу до інформаційних ресурсів, а також своєчасного

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

реагування на виявлені загрози та інциденти безпеки. Це дозволяє своєчасно виявляти та запобігати можливим порушенням безпеки.

Впровадження моделі загроз та використання надійних апаратних засобів автентифікації в рамках концепції ZeroTrust є важливим кроком у забезпеченні високого рівня кібербезпеки організації. Проте, це лише один з елементів комплексного підходу до захисту інформаційних ресурсів, який також повинен включати належне управління ризиками, навчання персоналу та постійне вдосконалення процесів безпеки.

Створення складних систем інформаційної взаємодії та управління структурними підрозділами організації, яка є об'єктом критичної інфраструктури або забезпечує прийняття критично важливих рішень в інтересах суспільства або держави, потребує розв'язку низки складних завдань. Це включає визначення архітектури системи управління та застосовних механізмів захисту інформаційних ресурсів. Результати обстеження об'єктів інформатизації та розроблення моделей загроз та порушників є важливими для розробки Політики інформаційної безпеки. З урахуванням розвитку хмарних технологій та потенційних загроз безпеці, важливим стає дослідження та розробка методів побудови систем захисту інформації з використанням концепції ZeroTrust, яка передбачає відсутність довіри до будь-якого суб'єкта чи об'єкта в інформаційній системі, навіть у межах контуру безпеки.

Дослідження та розробка ефективних рішень для підвищення кібербезпеки інформаційних систем державного рівня в умовах збройної агресії та потужних кібератак на критичну інфраструктуру є актуальним завданням. Основними механізмами захисту інформаційних ресурсів в комп'ютерних системах є процедури ідентифікації суб'єктів, процесів і об'єктів, авторизація суб'єктів та управління доступом до об'єктів згідно з Політикою безпеки. Правильно ідентифіковані та автентифіковані суб'єкти та процеси отримують право на доступ до інформації з певного носія, передачу інформації на носій або запуск обчислювального процесу в системі.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Початкова концепція системи управління доступом та ідентифікації (ІАМ) передбачала централізований механізм обмеження доступу до ресурсів системи на основі надання дозволів користувачам. Початкова мета полягала у наданні прав доступу, а не в контролі за ним. Однак з часом ця модель була модифікована для посилення надійності та ефективності процедур ідентифікації та автентифікації, включаючи багатфакторну аутентифікацію. Також було уточнено повноваження користувачів та менеджменту безпеки, з централізованим прийняттям рішень щодо надання доступу в системі.

Сьогодні поняття потенційного порушника включає не лише конкретну особу, але й альянс осіб, які можуть діяти для досягнення зловмисної мети. Це може бути порушення конфіденційності, цілісності та доступності інформації. Спостерігаються випадки, коли спочатку лояльні співробітники згодом діють на користь конкурентів або зловмисників. Використання мобільних пристроїв для доступу до інформаційних систем підвищує ризики їх втрат та крадіжок. ІАМ є ключовим механізмом будь-якої моделі розмежування доступу до ресурсів системи, тому важливо постійно вдосконалювати його для забезпечення безпеки комп'ютерних мереж.

Для цього, на основі аналізу публікацій та повідомлень у ЗМІ про інциденти та негативні явища в комп'ютерних системах, було розроблено описове доповнення до моделі загроз безпеки з урахуванням концепції ZeroTrust (Таблиця 2).

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Часткова модель загроз згідно концепції ZeroTrust

Таблиця 2

Роль	Точка доступу	Небезпечні дії	Співвідношення рівень SC – ймовірність загрози P
Відправник (sender)	Своє АРМ або АРМ колеги	S1. Помилкове порушення політики безпеки	$\uparrow SC \Rightarrow \downarrow P_3 *$
		S2. ВІДМОВА щодо відправлення даних	Залежить від мотивації
		S3. МАСКАРАД / видача себе за іншу особу	Залежить від мотивації
		S4. ЗМОВА із зловмисником	$\uparrow SC Prob \rightarrow \downarrow P_3 **$
Отримувач (recipient)	Своє АРМ або АРМ колеги	R1. Помилкове порушення політики безпеки	$\uparrow SC \Rightarrow \downarrow P_3$
		R2. ВІДМОВА щодо отримання даних	Залежить від мотивації
		R3. МАСКАРАД / видача себе за іншу особу	Залежить від мотивації
		R4. ЗМОВА із зловмисником	$SC Prob \rightarrow \downarrow P_3$
		R5. МОДИФІКАЦІЯ отриманих даних	-
		R6. ПІДРОБКА / створення фіктивних даних	-
Провайдер (provider)	АРМ безпеки (адміністратор)	P1. Ненавмисні (помилкові) дії	$\uparrow SC \Rightarrow \downarrow P_3$
		P2. ЗМОВА із зловмисником	$\uparrow SC Prob \rightarrow \downarrow P_3$
Зловмисник (intruder)	Легальне АРМ або власний засіб	I1. ПЕРЕХОПЛЕННЯ змісту даних I2. МОДИФІКАЦІЯ перехоплених даних I3. ПІДРОБКА / створення фіктивних даних I4. МАСКАРАД / видача себе за іншу особу I5. ПОВТОР перехопленого повідомлення I6. ПІДБУРЕННЯ до незаконних дій	-

Запропонована модель робить більш очевидними потенційні вразливості існуючих рішень щодо побудови підсистем ІАМ (ідентифікації, автентифікації та управління доступом). Зокрема, вона виявляє такі проблеми: одноразова процедура автентифікації може бути використана іншими користувачами або злоумисниками, особливо якщо легальний користувач залишив робоче місце після успішної автентифікації. Відкрито застосовані логіни користувачів можуть бути використані злоумисником для аналізу трафіку в інформаційній мережі та отримання розвідувальної інформації. Крім того, процедури ідентифікації та автентифікації часто розглядаються як логічні предикати з бінарним результатом («істина» або «хиба»), тоді як насправді вони мають ймовірнісний характер і можуть давати хибні результати через помилки користувачів або збої в роботі.

Також слід зазначити проблему, з якою стикаються користувачі, що мають доступ до декількох систем: їм складно надійно зберігати та запам'ятовувати велику кількість складних стійких паролів, що містять букви, цифри та інші символи. Ця вразливість може призводити до використання слабких або повторюваних паролів, що підвищує ризик компрометації облікових даних.

Символ « $\uparrow SC \Rightarrow \downarrow P_3$ » вказує, що зростання рівня індивідуальної кіберкультури (SC - Security Culture) в загальному випадку сприяє зниженню ймовірності реалізації загрози (P_3).

Водночас, символ « $\uparrow SC \Rightarrow \downarrow P_3$ » також означає, що в результаті реалізації заходів з підвищення рівня корпоративної кіберкультури можуть бути виявлені ознаки ризику реалізації кіберзагрози.

Іншими словами, підвищення індивідуальної кіберкультури personlузвично призводить до зменшення ймовірності загроз. Однак, під час впровадження заходів з покращення корпоративної кіберкультури в організації можуть бути виявлені раніше непоміченні ризики або ознаки потенційних кіберзагроз.

Таким чином, запропонована модель дозволяє виявити низку недоліків та потенційних вразливостей у існуючих підходах до реалізації підсистем ідентифікації, автентифікації та управління доступом, що є важливим кроком для

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

вдосконалення та підвищення ефективності цих підсистем у забезпеченні кібербезпеки [2, с. 90].

Для покращення безпекової ситуації та усунення існуючих вразливостей можна застосувати кілька рішень, які не вимагають великих фінансових інвестицій:

1) Політика безпеки повинна встановлювати максимальний час дійсності процедури автентифікації. Доступ до більш чутливої інформації потребуватиме повторної автентифікації. Частота автентифікації користувачів та пристроїв на основі їх облікових даних має бути інструментом реагування на інциденти безпеки: при збільшенні кількості інцидентів, час дії попередньої автентифікації повинен зменшуватися.

2) Політика безпеки повинна максимально обмежувати надання доступу до ресурсів, дозволяючи доступ лише до необхідної інформації та пристроїв.

3) Управлінські рішення щодо безпеки повинні базуватися на об'єктивній інформації про стан роботи системи ідентифікації, автентифікації та управління доступом (IAM). Загальна статистика помилок автентифікації кожного користувача повинна збиратися протягом певного періоду (місяць, квартал, рік) для аналізу та прийняття рішень щодо тестування або вдосконалення IAM, додаткового навчання персоналу або обмеження прав доступу до критичних ресурсів для певних осіб.

4) Логіни доступу користувачів повинні зберігатися як конфіденційна інформація, а для їх приховування доцільно використовувати криптографічні або стеганографічні протоколи.

5) Для підвищення безпеки процедур автентифікації можна використовувати особисті характеристики співробітника, які не вимагають складних біометричних технологій. Наприклад, автентифікація може здійснюватися шляхом розпізнавання голосу співробітника, який читає послідовність чисел, відображену на екрані. Програмне забезпечення, використовуючи еталонні дані про голос кожного користувача та відомі математичні алгоритми їх обробки, може розраховувати ступінь відповідності тестового повідомлення всім потенційним учасникам процедури автентифікації.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

6) Для переключення IAM в режим автентифікації доцільно використовувати картки користувачів з технологією безконтактного підключення, наприклад, просту та ефективну технологію RFID.

Виходячи з побудованої моделі загроз, визначимо основні функціональні та ергономічні вимоги до апаратного засобу автентифікації (HAD), з урахуванням системних вимог до побудови центру кібербезпеки критичної інфраструктури:

1) Безконтактне підключення до засобів контролю доступу є важливим для зручності та ефективності використання HAD. Ви запропонували використовувати стандартизовані радіо інтерфейси, такі як Bluetooth, WiFi та RFID, що є раціональним рішенням.

2) Малі розміри HAD забезпечать зручність використання та портативність пристрою.

3) Низьке енергоспоживання дозволить збільшити час роботи HAD без необхідності часткої зарядки або заміни батареї.

4) Можливість використання HAD для різних видів автентифікації, таких як доступ до приміщень та двофакторна автентифікація в інформаційній системі, підвищить універсальність та зручність пристрою.

5) Багаторазове використання та можливість перепрограмування параметрів HAD дозволить адаптувати його до змін у системі безпеки та потребах користувачів.

6) Фізичний захист від несанкціонованого доступу до даних, що зберігаються в HAD, є критичним для забезпечення конфіденційності та цілісності інформації.

7) Накопичення даних про поточну активність у системі, включаючи спроби доступу з порушенням правил та облік часу доступу до ресурсів, допоможе виявляти та розслідувати інциденти безпеки.

8) Створення сеансового ключа шифрування для віддаленого доступу та захист даних за допомогою коду автентифікації повідомлень забезпечить безпечну комунікацію між HAD та системою.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

9) Шифрування конфіденційних даних за допомогою ключа симетричного алгоритму, який генерується та зберігається в НАД без можливості вилучення, з процедурою відновлення ключа на основі декількох ключів персоналу системи, забезпечить надійний захист даних.

10) Формування та перевірка електронного підпису власника НАД, а також перевірка підпису посадових осіб за наявності сертифіката відкритого ключа, дозволить забезпечити автентичність та цілісність даних.

Для створення НАД, який відповідає всім цим вимогам, необхідно ретельно проаналізувати доступні варіанти системи ідентифікації та обрати той, який забезпечить надійну роботу з заданою якістю при мінімальних витратах. Це може включати оцінку існуючих рішень на ринку, а також розробку спеціалізованого пристрою, який відповідає специфічним потребам центру кібербезпеки критичної інфраструктури.

Найважливішою складовою системи ідентифікації є її первинний вимірювальний перетворювач (ПВП), який повинен мати високу швидкодію, чутливість до первинного інформативного параметру та стабільність характеристик в умовах впливу дестабілізуючих факторів. Можливими методами вирішення цієї задачі є: математичне моделювання системи ідентифікації НАД, формування та дослідження узагальнених показників системи з використанням графоаналітичного методу, методу «прогресуючого еталону» тощо, а також застосування експертних методів оцінювання, що базуються на «колективній мудрості».

3.2. Використання стеганографічного протоколу обміну даними

У сучасному світі, де інформація стає все більш цінною, зростає потреба в її захисті. Традиційні методи криптографії, хоча й ефективні, не завжди можуть гарантувати повну безпеку, адже вони не приховують сам факт передачі даних. Саме тут на допомогу приходить стеганографія – мистецтво приховування секретних повідомлень всередині інших, нічим не примітних об'єктів.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Суть стеганографії полягає в тому, щоб вбудувати секретне повідомлення (текст, зображення, аудіо, відео) в носій (зображення, аудіо, відео, текст) таким чином, щоб воно стало невидимим для стороннього спостерігача. Це досягається шляхом незначних змін деяких параметрів носія, наприклад, пікселів зображення або бітів аудіофайлу.

Переваги стеганографії:

1) Високий рівень секретності: Секретне повідомлення стає невід’ємною частиною носія, не викликаючи підозр.

2) Стійкість до перехоплення: Навіть якщо носій буде перехоплений, без спеціальних знань та інструментів буде складно або неможливо виявити приховане повідомлення.

3) Широкий спектр носіїв: Стеганографію можна використовувати з різними типами носіїв, включаючи зображення, аудіо, відео, текст та навіть фізичні об’єкти.

4) Відсутність необхідності в спеціальному програмному забезпеченні: Існують безкоштовні та загальнодоступні інструменти для стеганографії, що робить її доступною для широкого кола користувачів.

Недоліки стеганографії:

1) Втрата даних: Вбудовування секретного повідомлення може призвести до незначного погіршення якості носія.

2) Стійкість до атак: Деякі стеганографічні методи можуть бути вразливими до певних типів атак, спрямованих на виявлення та вилучення секретних повідомлень.

3) Обмежена пропускну здатність: Обсяг секретного повідомлення, яке може бути приховано в носії, зазвичай обмежений.

Протоколи стеганографічного обміну даними – це набори правил та алгоритмів, що регламентують процес приховування та вилучення секретних повідомлень з носіїв. Їх можна класифікувати за різними критеріями, наприклад, за типом носія, за методом вбудовування та за рівнем секретності.

Приклади стеганографічних протоколів:

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

1) LSB-стеганографія: Цей метод полягає у зміні найменш значущих бітів пікселів зображення для приховування секретного повідомлення.

2) Метод парних змін: Цей метод використовує парні біти в аудіофайлах для вбудовування секретної інформації.

3) Текстова стеганографія: Цей метод приховує секретне повідомлення в текстовому документі шляхом зміни пробілів, пунктуації або інших символів.

Вибір стеганографічного протоколу залежить від багатьох факторів, таких як тип носія, обсяг секретного повідомлення, необхідний рівень секретності та доступні ресурси [10, с. 223].

Важливо зазначити, що стеганографія не є панацеєю від усіх проблем інформаційної безпеки. Її слід використовувати в поєднанні з іншими методами захисту, такими як криптографія, контроль доступу та фізична безпека.

Сфера застосування стеганографії досить широка. Її можна використовувати для:

- 1) Захисту конфіденційної інформації
- 2) Передачі секретних повідомлень
- 3) Захисту авторських прав
- 4) Маркування цифрового контенту
- 5) Стеження за піратською діяльністю

Стеганографія – це потужний інструмент, який може допомогти захистити інформацію від несанкціонованого доступу. Вона пропонує унікальний підхід до захисту інформації, приховуючи сам факт її передачі. Вона має ряд переваг, таких як високий рівень секретності, стійкість до перехоплення та універсальність носіїв. Однак, слід враховувати і недоліки, як-от втрата даних та обмежена пропускну здатність [11].

Для ефективного захисту стеганографію варто використовувати в комплексі з іншими методами інформаційної безпеки. Завдяки постійному розвитку, стеганографія має великий потенціал стати важливим інструментом захисту даних у майбутньому.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3. Загрози ШІ та відновлення після кіберінциденту

Штучний інтелект (ШІ) став невід’ємною частиною сучасного цифрового світу, вносячи значні зміни у різні сфери нашого життя. Проте, разом з численними перевагами, впровадження ШІ несе з собою й нові види загроз, які необхідно ретельно розглянути та вжити відповідних заходів для забезпечення безпеки. Одним з найбільших ризиків є потенційна вразливість систем ШІ до кіберінцидентів, які можуть спричинити серйозні збої в їхній роботі та призвести до непередбачуваних наслідків.

Кіберінциденти можуть виникати внаслідок навмисних зловмисних дій, таких як хакерські атаки чи цілеспрямовані кібератаки, або через випадкові збої, помилки в програмному забезпеченні чи апаратному забезпеченні. Незалежно від причини, наслідки цих інцидентів для систем ШІ можуть бути катастрофічними, оскільки вони покладаються на величезні обсяги даних та складні алгоритми для прийняття рішень [23, с. 64].

Однією з найбільших загроз є компрометація даних, на яких навчаються моделі ШІ. Зловмисники можуть намагатися маніпулювати чи отруїти навчальні дані, що призведе до неправильного функціонування моделі та прийняття нею хибних рішень. Це може мати серйозні наслідки, особливо в критично важливих галузях, таких як медицина, фінанси чи транспорт.

Крім того, хакери можуть намагатися отримати несанкціонований доступ до систем ШІ та змінити їхню поведінку або навіть повністю перехопити контроль. У такому випадку ШІ може бути використаний для здійснення кібератак, розповсюдження шкідливого програмного забезпечення чи крадіжки конфіденційних даних.

Ще однією загрозою є використання ШІ для створення глибоких підробок (deepfakes), які можуть вводити в оману людей та системи розпізнавання. Deepfakes можуть поширювати дезінформацію, завдаючи шкоди репутації людей чи організацій або навіть підриваючи довіру до достовірних джерел інформації.

У разі виникнення кіберінциденту, пов’язаного з ШІ, важливо вжити швидких та ефективних заходів для відновлення порушених систем та мінімізації

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

негативних наслідків. Це може включати ізолювання та відключення уражених систем, відновлення з резервних копій, оновлення програмного забезпечення та усунення вразливостей.

Однак, відновлення після кіберінциденту в системах ІІІ може бути складним завданням через їхню складність та взаємозалежність з іншими системами. Необхідно ретельно проаналізувати причини інциденту, визначити масштаб збитків та впровадити відповідні заходи безпеки для запобігання повторенню подібних інцидентів у майбутньому.

Організації, які використовують ІІІ, повинні розробити комплексні плани реагування на кіберінциденти та регулярно проводити навчання та тренування персоналу. Крім того, важливо забезпечити належні заходи безпеки, такі як шифрування даних, багаторівневий захист, регулярне оновлення програмного забезпечення та відстеження вразливостей.

Упровадження високих технологій, зокрема штучного інтелекту (ІІІ), відіграє ключову роль у забезпеченні національної безпеки, оборони, функціонуванні об'єктів критичної інфраструктури та фінансово-економічному розвитку суспільства. Проте, принципи роботи та алгоритми систем ІІІ (СІІІ) залишаються практично невідомими для більшості людей. СІІІ часто сприймаються як «чорні скриньки», здатні розуміти природну мову, музику, зображення та надавати статистично вірні відповіді на запитання користувачів. Водночас, користувачі не розуміють джерел формування цих відповідей та методів розв'язання завдань.

З одного боку, СІІІ демонструють ефект непередбачуваності (нетривіальності) результатів, що є ознакою творчості та інноваційної діяльності, притаманної людині. З іншого боку, відсутність прозорих методів перевірки висновків та рекомендацій СІІІ створює невизначеність щодо їхньої вірогідності та практичної цінності. Це означає, що СІІІ можуть бути використані як інструмент інформаційної війни для поширення сумнівних відомостей та фейків.

СІІІ можуть стати потужним засобом в інформаційних війнах, створюючи більш переконливі та цілеспрямовані фейкові новини, а також автоматизуючи їх

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

розповсюдження. Важливо зазначити, що платформи розповсюдження контенту, які використовують алгоритми рекомендацій із підтримкою ШІ, вже були задіяні для маніпулювання емоціями, переконаннями та поведінкою людей.

Поширення сфери застосування систем штучного інтелекту (СШІ) на об'єкти критичної інфраструктури, складність верифікації створених ними інформаційних ресурсів та рішень, а також загрози небезпечного впливу результатів їх функціонування на безпеку людини, суспільства та держави призводять до виникнення ризиків, пов'язаних з використанням СШІ. Це висуває вимогу формування процедур виявлення та обробки таких ризиків, що може мати визначальне значення для майбутнього суспільства та забезпечення національної безпеки [4, с. 56].

На сьогоднішній день серед поширених СШІ генеративного типу, доступних широкому загалу та здатних формувати суспільну думку щодо можливостей ШІ, можна виділити такі: ChatGPT – чат-бот від OpenAI, який підтримує діалог з користувачем природною мовою та генерує тексти на задану тему; Midjourney – сервіс, що генерує зображення на основі текстових описів від користувача. Проте, вкрай складно зробити висновок щодо перспектив застосування технологій ШІ в інтересах державних структур лише на основі вивчення цих засобів. За умови належного проектування систем можливо прогнозувати розвиток певних напрямів, які вимагають від інформаційно-управляючих систем забезпечення якостей, притаманних ШІ.

Згідно з окремими повідомленнями, СШІ включають різні компоненти, такі як алгоритми машинного навчання, глибокого навчання, нейронні мережі, обробку природної мови, комп'ютерний зір, робототехніку та інші технології. Вони також можуть містити комплекси автоматизації, аналітики даних, системи управління знаннями та інші інструменти для обробки інформації та прийняття рішень.

Багато систем штучного інтелекту (СШІ) застосовують інтерпретатори природних мов, що суттєво підвищує їх ефективність у порівнянні зі звичайними програмними системами при обробці неструктурованих даних. В майбутньому, використання потужних комп'ютерних архітектур з високошвидкісними

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

процесорами, здатними підтримувати значну кількість глибоких нейронних мереж, дозволить СШІ вирішувати складні завдання, що потребують великої кількості обчислень, за прийнятний час.

ШІ забезпечує ефективну обробку великих обсягів даних (big data) завдяки застосуванню алгоритмів машинного навчання та аналізу даних. Це автоматизує процеси обробки та аналізу, дозволяє виявляти приховані закономірності, прогнозувати тренди та патерни, оптимізувати прийняття рішень та створювати інтелектуальні системи управління даними. Таким чином, СШІ сприяє отриманню знань з великих обсягів даних та прийняттю обґрунтованих рішень на основі їх аналізу.

Технологія ШІ здатна покращити рівень комп'ютерної безпеки, зокрема, запропоновано використовувати ШІ та нейронні мережі для проектування системи захисту комп'ютерної мережі, що продемонструвало гарний ефект забезпечення безпеки. Перелічені властивості ШІ дають підстави прогнозувати її ефективне застосування для вирішення інших завдань кібербезпеки. Зокрема, ситуаційні центри, що обробляють великі обсяги даних та мають підвищені вимоги до гарантоздатності, кібербезпеки та оперативності прийняття рішень в кризових ситуаціях, є першочерговими об'єктами для впровадження технологій ШІ. Аналогічна ситуація із протидією шифрувальним вірусам-вимагачам, де успіху сприяє здатність ШІ розв'язувати складні завдання, що потребують великої кількості обчислень, без прямого втручання людини.

Технологія штучного інтелекту (ШІ) розвивається надзвичайно швидкими темпами, відкриваючи нові можливості для різних сфер життя та діяльності людини. Однак, незважаючи на численні переваги, які може принести ШІ, його широке застосування також пов'язане зі значними потенційними ризиками [3, с. 128].

Автори відкритого листа наголошують на важливості ефективного управління цими ризиками задля забезпечення безпечного та відповідального розвитку ШІ. Вони вважають, що для досягнення цієї мети необхідна тісна співпраця між розробниками, дослідниками та експертами з різних галузей.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Спільними зусиллями вони повинні розробити та впровадити набір загальних протоколів безпеки, які будуть застосовуватися при проектуванні та розробці передових систем ШІ.

Ці протоколи безпеки мають бути ретельно перевірені та проконтрольовані незалежними зовнішніми експертами. Такий підхід дозволить забезпечити відповідність систем ШІ встановленим стандартам безпеки та мінімізувати ризики, пов'язані з їх використанням.

Необхідність визначення та регулювання ризиків, пов'язаних з використанням систем штучного інтелекту, вже визнана на міжнародному рівні. Європейський Союз, США та інші країни світу активно працюють над розробкою та прийняттям відповідних законодавчих актів та стандартів. Ці зусилля спрямовані на створення правової бази, яка дозволить ефективно контролювати розвиток та застосування ШІ, забезпечуючи при цьому безпеку та дотримання етичних принципів.

Регулювання ризиків, пов'язаних з використанням ШІ, може включати в себе різні аспекти, такі як забезпечення прозорості та підзвітності систем ШІ, захист персональних даних, запобігання дискримінації та упередженості, а також забезпечення безпеки та стійкості систем ШІ до потенційних загроз.

Таким чином, стрімкий розвиток та застосування технології штучного інтелекту вимагає комплексного підходу до управління пов'язаними з ним ризиками. Спільна розробка та впровадження протоколів безпеки, а також законодавче регулювання та стандартизація є ключовими елементами забезпечення безпечного та відповідального розвитку ШІ на благо людства.

Підсумовуючи, загрози, пов'язані з ШІ та кіберінцидентами, є серйозними та потребують ретельної уваги. Лише шляхом вжиття проактивних заходів безпеки, постійного моніторингу та готовності до реагування на інциденти, ми зможемо максимально зменшити ризики та забезпечити безпечне та надійне використання технологій ШІ.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВОК ДО 3 РОЗДІЛУ

У третьому розділі було сформовано часткову модель загроз безпеки корпоративної мережі, що може стати основою покращеної політики безпеки. Проаналізовано загрози, пов'язані з широким застосуванням штучного інтелекту у корпоративних мережах. Запропоновано використання інтелектуальних методів аналізу даних для виявлення аномалій та ідентифікації ризиків у системі управління ризиками.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВОК

У роботі було досліджено питання підвищення безпеки мережної інфраструктури на основі методології ZeroTrust. Розглянуто три основні розділи проєкту підсистеми захисту з відповідними підрозділами.

У першому розділі було обґрунтовано важливість політики інформаційної безпеки в сучасних умовах зростання кіберзагроз. Досліджено вдосконалену політику інформаційної безпеки для сучасного підприємства, базуючись на принципах ZeroTrust, з урахуванням актуальних кіберзагроз та методів їх подолання. Визначено основні переваги впровадження ZeroTrust, зокрема підвищення рівня безпеки, захисту від внутрішніх загроз, гнучкість та масштабованість. Наведено ключові принципи підходу ZeroTrust, серед яких безперервна багаторівнева перевірка, мінімізація довірчих меж, поділ ресурсів мережі на окремі сегменти тощо.

У другому розділі було розглянуто актуальні кіберзагрози у цивільному секторі, такі як шкідливе програмне забезпечення, фішинг, DDoS-атаки, цілеспрямовані кібератаки. Проаналізовано важливість підвищення рівня кіберкультури персоналу організації як ключового елементу забезпечення інформаційної безпеки. Висвітлено необхідність розробки програм вдосконалення кіберкультури, впровадження заходів підвищення обізнаності, навчання та формування навичок безпечної поведінки.

У третьому розділі було сформовано часткову модель загроз безпеки корпоративної мережі, що може стати основою покращеної політики безпеки. Проаналізовано загрози, пов'язані з широким застосуванням штучного інтелекту у корпоративних мережах. Запропоновано використання інтелектуальних методів аналізу даних для виявлення аномалій та ідентифікації ризиків у системі управління ризиками.

У процесі виконання роботи отримано такі основні результати:

1) Аналіз важливості та поточного стану інформаційної безпеки на сучасних підприємствах виявив критичну необхідність постійного вдосконалення політик безпеки. В умовах стрімкого розвитку цифрових технологій та зростання

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

кількості і складності кіберзагроз, традиційні методи захисту інформації стають недостатньо ефективними. Встановлено, що більшість підприємств стикаються з проблемами застарілих систем безпеки, недостатньої обізнаності персоналу та відсутності комплексного підходу до захисту інформаційних активів.

2) Дослідження сучасних підходів, методів та компонентів концепції ZeroTrust продемонструвало їх високу ефективність у забезпеченні комплексного захисту інформаційних систем підприємства. Концепція ZeroTrust, заснована на принципі «не довіряй нікому, завжди перевіряй», дозволяє створити багаторівневу систему захисту, яка постійно верифікує кожен запит доступу до ресурсів. Виявлено, що ключовими компонентами ZeroTrust є: строга автентифікація, мікросегментація мережі, постійний моніторинг та аналіз поведінки користувачів і систем.

3) Визначено ключові переваги та принципи підходу ZeroTrust, які дозволяють суттєво підвищити рівень захищеності корпоративних мереж та даних. Серед основних переваг: зменшення поверхні атаки, покращення видимості та контролю за діями користувачів, підвищення гнучкості та масштабованості систем безпеки. Принципи ZeroTrust, такі як найменші привілеї, багатофакторна автентифікація та шифрування даних у русі та у спокої, створюють потужний фундамент для побудови сучасної системи кібербезпеки.

4) Аналіз актуальних кіберзагроз у цивільному секторі виявив нові тенденції та методи атак, що вимагають адаптації існуючих систем захисту. Зокрема, спостерігається зростання кількості та складності ransomware-атак, збільшення випадків соціальної інженерії та фішингу, а також поява нових видів загроз, пов'язаних з Інтернетом речей (IoT) та хмарними технологіями.

5) Розроблено комплекс рекомендацій щодо підвищення та вдосконалення кіберкультури в організаціях, що сприятиме зміцненню «людської ланки» в системі кібербезпеки. Рекомендації включають: регулярні тренінги та навчання персоналу, створення системи мотивації для дотримання правил безпеки, впровадження програм підвищення обізнаності про кіберзагрози, розробку чітких політик та процедур реагування на інциденти.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

6) Створена модель оцінки культури кібербезпеки дозволяє ефективно вимірювати та покращувати рівень обізнаності та готовності персоналу до протидії кіберзагрозам. Модель включає кількісні та якісні показники, такі як: рівень знань співробітників про кіберзагрози, частота інцидентів, пов'язаних з людським фактором, швидкість реагування на потенційні загрози, ступінь дотримання політик безпеки. Запропонована модель дозволяє не лише оцінювати поточний стан, але й відслідковувати динаміку змін та ефективність впроваджених заходів.

7) Розроблена модель загроз та сформульовані вимоги до апаратного засобу автентифікації на основі ZeroTrust забезпечують надійну основу для впровадження цього підходу в інфраструктуру підприємства. Модель враховує різні типи потенційних атак, включаючи фізичний доступ, мережеві атаки, соціальну інженерію та внутрішні загрози. Вимоги до апаратного засобу автентифікації включають: підтримку багатфакторної автентифікації, використання криптографічних алгоритмів, стійкість до фізичних атак, інтеграцію з системами управління ідентифікацією та доступом.

8) Аналіз загроз, пов'язаних з використанням штучного інтелекту в сфері кібербезпеки, виявив як нові ризики, так і потенційні можливості для посилення захисту. Серед ризиків виділено: використання ШІ для автоматизації та масштабування атак, створення більш реалістичних фішингових повідомлень, генерація шкідливого коду. З іншого боку, ШІ може бути потужним інструментом для виявлення аномалій, прогнозування атак та автоматизації реагування на інциденти. Розроблено рекомендації щодо етичного та безпечного використання ШІ в системах кібербезпеки.

Проведене дослідження дозволило розробити комплексний підхід до вдосконалення політики безпеки сучасного підприємства на основі концепції ZeroTrust, з урахуванням актуальних кіберзагроз та інноваційних методів захисту. Запропоновані рішення охоплюють технічні, організаційні та культурні аспекти кібербезпеки, створюючи багаторівневу систему захисту. Комплексне впровадження запропонованих рішень дозволить підвищити стійкість і безпеку корпоративних мереж організацій до сучасних кіберзагроз.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Азарова А., Дьогтева І., Шиян А. Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. Інформаційні технології та комп'ютерна інженерія. 2022. № 1. С. 12–18.

2) Астапеня В., Соколов Ю., Таждіні М. Результати та засоби оцінки ефективності систем фокусування для підвищення доступності в безпроводових мережах. Кібербезпека: освіта, наука, техніка. 2019. № 4. С. 90–103. DOI: <https://doi.org/10.28925/2663-4023.2019.4.90103>

3) Бідюк П., Кожухівський А., Кожухівська О. Система підтримки прийняття рішень для аналізу і прогнозування стану підприємства. Радіоелектроніка, інформатика, управління. 2013. № 1. С. 128–136.

4) Бідюк П., Терентьев О., Коновалюк М. Байєсівські мережі в технологіях інтелектуального аналізу даних. Штучний інтелект. 2010. № 2. С. 104–113.

5) Бурячок В., Соколов В. Технологія забезпечення об'єктивного контролю захищеності корпоративних інформаційно-телекомунікаційних систем і мереж. Актуальні питання протидії кіберзлочинності та торгівлі людьми: матеріали Всеукр. наук.-практ. конф. 2018. С. 242–247.

6) Бурячок В., Толюпа С., Аносов А., Козачок В., Лукова-Чуйко Н. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. Київ: ДУТ, 2015. 345 с.

7) Про захист персональних даних: Закон України від 27.10.2022 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 14.06.2024).

8) Про основні засади забезпечення кібербезпеки України: Закон України від 17.08.2022 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 14.06.2024).

9) Про захист інформації в інформаційно-комунікаційних системах: Закон України від 01.07.2022 р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80> (дата звернення: 14.06.2024).

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

10) Ворохоб М., Киричок Р., Яскевич В., Добришин Ю., Сидоренко С. Сучасні перспективи застосування концепції ZeroTrust при побудові політики інформаційної безпеки підприємства. Кібербезпека: освіта, наука, техніка. 2023. № 1(21). С. 223–233. DOI: <https://doi.org/10.28925/2663-4023.2023.21.223233>

11) Войцеховська М.М. Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації : дис. ... канд. техн. наук. Чернігів, 2020. 175 с.

12) Волошин О.Ф., Мащенко С.О. Моделі та методи прийняття рішень: навчальний посібник. Київ: Видавничо-поліграфічний центр «Київський університет», 2010. 336 с.

13) Гречанінов В. та ін. Мережа ситуаційних центрів органів державної влади – базис для підвищення ефективності їх діяльності (взаємодії). Математичні машини і системи. 2018. № 3. С. 32–39.

14) Гулак Г. та ін. Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Кібербезпека: освіта, наука, техніка. 2022. № 1(17). С. 145–158. DOI: <https://doi.org/10.28925/2663-4023.2022.17.145158>

15) Гречанінов В., Оксанич І., Лопушанський А. Використання хмарних технологій для вирішення питань інтеграції інформації у багаторівневих системах управління. Системи керування та комп'ютери. 2022. № 4(300). С. 24–34. DOI: <https://doi.org/10.15407/csc.2022.04.024>

16) Добришин Ю., Сидоренко С., Ворохоб М. Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Кібербезпека: освіта, наука, техніка. 2023. № 4(20). С. 174–182. DOI: <https://doi.org/10.28925/2663-4023.2023.20.174182>

17) ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. Київ, 2023. 30 с.

18) ДСТУ ISO/IEC 27032:2016. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. Київ, 2016. 73 с.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

19) ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги. Київ, 2015. 22 с. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910 (дата звернення: 14.06.2024).

20) ДСТУ EN ISO 9001:2018. Системи управління якістю. Вимоги. Київ, 2018. 24 с.

21) ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови. Київ, 2018. 18 с.

22) Крючкова Л., Складанний П., Ворохоб М. Передпроектні рішення щодо побудови системи авторизації на основі концепції ZeroTrust. Кібербезпека: освіта, наука, техніка. 2023. № 3(19). С. 226–242. DOI: <https://doi.org/10.28925/2663-4023.2023.13.226242>

23) Ковтунець В.В., Нестеренко О.В., Савенков О.І. Безпека систем підтримки прийняття рішень: навчальний посібник. Київ: Національна академія управління, 2016. 140 с.

24) Кононович І.В., Маєвський Д.А., Подобний Р.А. Моделі системи забезпечення кібербезпеки із запізнюванням реагування на інциденти. Інформатика та математичні методи в моделюванні. 2015. Т. 5, № 4. С. 339–346.

25) Літвінчук І., Коршун Н., Ворохоб М. Спосіб оцінювання інтегрованих систем безпеки на об'єкті інформаційної діяльності. Кібербезпека: освіта, наука, техніка. 2020. № 2(10). С. 135–143. DOI: <https://doi.org/10.28925/2663-4023.2020.10.135143>

26) Літвінчук І., Корчомний Р., Коршун Н., Ворохоб М. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Кібербезпека: освіта, наука, техніка. 2020. № 2(10). С. 98–112. DOI: <https://doi.org/10.28925/2663-4023.2020.10.98112>

27) Нестеренко О.В., Савенков О.І., Фаловський О.О. Інтелектуальна система підтримки прийняття рішень: навчальний посібник. Київ: Національна академія управління, 2016. 182 с.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

28) НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 1999-04-28]. Київ: ДСТСЗІ СБ України, 1999. 16 с. URL: <https://tzi.com.ua/downloads/1.1-002-99.pdf> (дата звернення: 14.06.2024).

29) НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. [Чинний від 2000-12-04]. Київ: ДСТСЗІ СБ України, 2000. 32 с. URL: <https://tzi.com.ua/downloads/1.4-001-2000.pdf> (дата звернення: 14.06.2024).

30) Ситник В., Дубровіна А. Проблеми моделювання рішень у групових СППР. Моделювання та інформаційні системи в економіці. 2002. Вип. 68. С. 9–14.

31) Скітер І., Ворохоб М. Модель оцінки рівня культури кібербезпеки в інформаційній системі. Кібербезпека: освіта, наука, техніка. 2021. № 1(13). С. 158–169. DOI: <https://doi.org/10.28925/2663-4023.2021.13.158169>

32) Скіцько О. та ін. Загрози та ризики використання штучного інтелекту. Кібербезпека: освіта, наука, техніка. 2023. № 2(22). С. 6–18. DOI: <https://doi.org/10.28925/2663-4023.2023.22.618>

33) Соколов В., Карацюба К. Використання дерев атак для аналізу захищеності безпроводових технологій стандарту IEEE 802.11. Вісник ДУІКТ. 2012. № 10(1). С. 42–49.

34) Соколов В.Ю. Кількісні показники оцінювання захищеності і ризиків від порушення безпеки у розподілених системах рухомого зв'язку. Захист інформації. 2010. № 3(48). С. 19–34. DOI: <https://doi.org/10.18372/2410-7840.12.1957>

35) Стасюк О. та ін. Сучасні стеганографічні методи захисту інформації. Захист інформації. 2011. Т. 13, № 1. С. 72–81. DOI: <https://doi.org/10.18372/2410-7840.13.1994>

36) Цюцюра С., Криворучко О., Цюцюра М. Теоретичні основи та сутність управлінських рішень. Моделі прийняття управлінських рішень. Управління розвитком складних систем. 2012. Вип. 9. С. 50–58.

37) Черненко Р. та ін. Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

обчислювальними ресурсами. Кібербезпека: освіта, наука, техніка. 2021. № 3(11). С. 124–135. DOI: <https://doi.org/10.28925/2663-4023.2021.11.1241351>

38) Шелест М.Є. Цифрова стеганографія та її можливості. Захист інформації. 1999. № 1. С. 11–19.

39) Яцишин А., Попов О., Артемчук В., Ковач В., Зінов'єва І. Автоматизовані інформаційні системи підтримки прийняття управлінських рішень у галузі екологічної безпеки. Інформаційні технології і засоби навчання. 2019. Т. 72, № 4. С. 286–300.

		Морозов К.О.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Щур Н.О.				80
Змн.	Арк.	№ докум.	Підпис	Дата		