МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ЕТИЧНОГО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ МОНІТОРИНГУ В ІНФОРМАЦІЙНІЙ ТА КІБЕРБЕЗПЕЦІ: БАЛАНС МІЖ ПРИВАТНІСТЮ ТА НАЦОНАЛЬНОЮ БЕЗПЕКОЮ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Данило Пічкур

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Данило ПІЧКУР

Керівник:
д-р іст. н., професор Володимир ШУЛЬГА

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

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Пічкуру Данилу Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Методи етичного використання технологій моніторингу в інформаційній та кібербезпеці: баланс між приватністю та національною безпекою"

керівник кваліфікаційної роботи Шульга В. П., д-р.іст.н., професор
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи **"**11" грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: етичний моніторинг в кібербезпеці, баланс між приватністю та національною безпекою, технології SIEM та SOC, нормативно-правове регулювання захисту даних..

4. Перелік питань, які потрібно розробити:
   1. Дослідити теоретико-методологічні засади та нормативну базу етичного моніторингу в кібербезпеці.
   2. Проаналізувати проблеми балансу між безпекою та приватністю і методи оцінки ризиків.
   3. Розробити архітектурну модель системи етичного моніторингу та рекомендації щодо її впровадження.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Аналіз теоретико-методологічні засади та нормативну базу етичного моніторингу.	27.10.2025	
4.	Аналіз проблем балансу між безпекою та приватністю і методи оцінки ризиків.	10.11.2025	
5.	Дослідження теоретико-методологічні засади та нормативну базу етичного моніторингу в кібербезпеці.	15.11.2025	
6.	Розроблення архітектурної моделі системи етичного моніторингу та рекомендації щодо її впровадження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Данило ПІЧКУР

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Володимир ШУЛЬГА

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Пічкур Д.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи етичного використання технологій моніторингу в інформаційній та кібербезпеці: баланс між приватністю та національною безпекою"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ПІЧКУР Данило послідовно та ґрунтовно у процесі виконання роботи здійснив аналіз теоретико-методологічних засад етичного моніторингу, дослідив чинну нормативно-правову базу у сфері інформаційної та кібербезпеки, захисту персональних даних і приватності. Проаналізував проблеми забезпечення балансу між національною безпекою та правом на приватність, ключові ризики, пов'язані з надмірним або неетичним застосуванням моніторингових технологій, розробив архітектурну модель системи етичного моніторингу. Отримані результати свідчать про вміння здобувача критично мислити, узагальнювати інформацію та формулювати обґрунтовані висновки. Матеріал викладено логічно, з використанням сучасних наукових джерел та міжнародних стандартів.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ПІЧКУРА Данила на оцінку «добре» та рекомендувати присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Володимир ШУЛЬГА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Пічкур Д.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Пічкура Данила Сергійовича
на тему “ Методи етичного використання технологій моніторингу в інформаційній та кібербезпеці: баланс між приватністю та національною безпекою ”

Актуальність Кваліфікаційна магістерська робота присвячена актуальній та суспільно значущій проблемі етичного застосування технологій моніторингу в умовах зростання кіберзагроз, цифровізації державних і корпоративних систем, а також посилення вимог до захисту персональних даних і прав людини. Вибрана тема є надзвичайно важливою для сфери інформаційної та кібербезпеки, особливо в контексті забезпечення національної безпеки України та гармонізації безпекових заходів із принципами приватності й етики.

Позитивні сторони

У процесі виконання роботи здобувачем послідовно та ґрунтовно реалізовано поставлені завдання, досліджено чинну нормативно-правову базу у сфері інформаційної та кібербезпеки, захисту персональних даних і приватності. Автором розглянуто ключові ризики, пов’язані з надмірним або неетичним застосуванням моніторингових технологій.

Розроблена модель системи етичного моніторингу враховує принципи мінімізації даних, прозорості, підзвітності та контролю доступу. Запропоновані рекомендації щодо впровадження такої системи мають практичну цінність і можуть бути використані в діяльності органів державної влади, об’єктів критичної інформаційної інфраструктури та служб кібербезпеки.

Робота характеризується цілісністю, логічною структурою та належним науково-методичним рівнем. Виклад матеріалу є послідовним, висновки обґрунтованими та відповідають поставленим завданням і меті дослідження. Оформлення роботи відповідає встановленим вимогам до кваліфікаційних магістерських робіт.

Недоліки

1. Доцільно було б приділити більше уваги візуалізації результатів надмірного або неетичного застосування моніторингових технологій. Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач ПІЧКУР Данило Сергійович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою”.

Рецензент: завідувач кафедри
Систем та технологій кібербезпеки

д-р техн. н., професор _____ Галина ГАЙДУР

підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 86 стор., 11 рис., 21 табл., 50 джерел.

Метою роботи є дослідження, розробка та обґрунтування методів моніторингу в інформаційно-телекомунікаційних системах, що дозволяють забезпечити баланс між необхідним рівнем національної безпеки та дотриманням прав громадян на приватність.

Об'єктом дослідження є процеси моніторингу, збору та аналізу даних в системах інформаційної та кібернетичної безпеки.

Предмет дослідження – методи та алгоритми етичного використання технологій контролю інформаційних потоків та виявлення кіберзагроз.

Методи дослідження. Для вирішення поставлених завдань використовуються методи системного аналізу, а також методи інтелектуального аналізу. Для оцінки відповідності моніторингу етичним нормам використовувалися методи порівняльного правового аналізу та моделювання ризиків приватності.

Короткий зміст роботи. Як результат у роботі проведено комплексний аналіз теоретико-методологічних засад та нормативно-правового регулювання моніторингу критичних систем; досліджено проблеми забезпечення балансу між безпекою та приватністю, зокрема систематизовано методи оцінки ризиків та інструменти мінімізації даних; розроблено архітектурну модель системи етичного моніторингу на основі принципів приватності за замовчуванням та сформовано практичні рекомендації щодо її впровадження.

Галузь застосування. Розроблені підходи можуть бути використані при побудові та модернізації центрів операцій з безпеки на об'єктах критичної інфраструктури, в процесах управління ризиками приватності персоналу, а також при розробці нормативно-правових актів та корпоративних стандартів

щодо етичного моніторингу в інформаційно-телекомунікаційних системах.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ЕТИЧНИЙ МОНІТОРИНГ, ПРИВАТНІСТЬ, НАЦІОНАЛЬНА БЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, SIEM, SOC.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 86 pages, 11 figures, 21 tables, 50 sources.

The purpose of the work is to research, develop, and substantiate monitoring methods in information and telecommunication systems that ensure a balance between the necessary level of national security and the observance of citizens' rights to privacy.

Object of research is the processes of monitoring, data collection, and analysis in information and cybersecurity systems.

Subjec*t ***of research is the methods and algorithms for the ethical use of information flow control technologies and cyber threat detection.

Research methods To address the set tasks, methods of system analysis, and data mining were used. To assess monitoring compliance with ethical standards, comparative legal analysis and privacy risk modeling methods were employed.

Brief content of research. As a result, the study conducts a comprehensive analysis of the theoretical-methodological foundations and legal regulation of critical system monitoring. The problems of ensuring a balance between security and privacy were investigated; specifically, risk assessment methods and data minimization tools were systematized. An architectural model of an ethical monitoring system based on "Privacy by Default" principles was developed, and practical recommendations for its implementation were formulated.

Field of research. The developed approaches can be used in building and modernizing Security Operations Centers at critical infrastructure facilities, in personnel privacy risk management processes, as well as in developing regulations and corporate standards regarding ethical monitoring in information and telecommunication systems.

KEYWORDS: INFORMATION SECURITY, CYBERSECURITY, ETHICAL MONITORING, PRIVACY, NATIONAL SECURITY, CRITICAL INFRASTRUCTURE, SIEM, SOC.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ВРУ	–	Верховна Рада України
ІБ	–	Інформаційна безпека
КБ	–	Кібербезпека
КІ	–	Критична інфраструктура
КІІ	–	Критична інформаційна інфраструктура
КІС	–	Критичні інформаційні системи
AI	–	Artificial Intelligence
APT	–	Advanced Persistent Threat
AUP	–	Acceptable Use Policy
CERT-UA	–	Computer Emergency Response Team of Ukraine
CIA	–	Confidentiality, Integrity, Availability
CISO	–	Chief Information Security Officer
CSIRT	–	Computer Security Incident Response Team
DDoS	–	Distributed Denial of Service
DLP	–	Data Loss Prevention
DPI	–	Deep Packet Inspection
DPIA	–	Data Protection Impact Assessment
DPO	–	Data Protection Officer
EDR	–	Endpoint Detection and Response
E-SOC	–	Ethical Security Operations Center
FPC	–	Full Packet Capture
GDPR	–	General Data Protection Regulation
IDS	–	Intrusion Detection System
IPS	–	Intrusion Prevention System
ISO	–	International Organization for Standardization
IEC	–	International Electrotechnical Commission
KPI	–	Key Performance Indicators
LIA	–	Legitimate Interest Assessment

ML	–	Machine Learning
MTTC	–	Mean Time To Contain
MTTD	–	Mean Time To Detect
MTTR	–	Mean Time To Respond
NDR	–	Network Detection and Response

ВСТУП

Актуальність теми. В умовах глобальної цифровізації інформація перетворилася на найбільш цінний актив, а її захист став фундаментом національної безпеки. Сучасні виклики, зокрема гібридні загрози та кібервійна, вимагають від об'єктів критичної інфраструктури переходу від пасивного захисту до активної оборони, що реалізується через системи безперервного моніторингу. Однак, технологічний прогрес у засобах нагляду породив фундаментальний конфлікт: необхідність забезпечення колективної безпеки все частіше вступає у протиріччя з конституційними правами особи на приватність.

Особливої гостроти ця проблема набуває в Україні, яка перебуває у стані війни та одночасно проходить процес євроінтеграції. З одного боку, воєнний стан та постійні кібератаки вимагають тотальної видимості мережевих процесів, що технічно реалізується через глибоку інспекцію пакетів та поведінковий аналіз. З іншого боку, імплементація європейських норм, зокрема GDPR та Директиви NIS2, вимагає суворого дотримання принципу мінімізації даних та захисту персональної інформації.

Існуючі підходи до побудови центрів операцій з безпеки часто ігнорують етичну складову, працюючи за принципом цифрового паноптикому , що призводить до негативних психосоціальних наслідків, таких як ефект «заморожування» ініціативи працівників та зростання тіньового IT. Таким чином, виникає нагальна потреба у розробці нових методів та архітектурних рішень, які дозволять технічно забезпечити баланс між ефективним виявленням кіберзагроз та дотриманням етичних і правових норм. Це обумовлює актуальність теми кваліфікаційної роботи для розвитку галузі інформаційної безпеки в Україні.

Метою роботи є дослідження, розробка та обґрунтування методів і засобів етичного моніторингу в інформаційно-телекомунікаційних системах, що дозволяють забезпечити необхідний рівень національної безпеки при мінімізації

втручання у приватне життя користувачів.

Для досягнення поставленої мети необхідно вирішити такі завдання:

Провести аналіз теоретико-методологічних засад моніторингу критичних систем та виявити специфіку конфлікту між безпекою та приватністю в умовах воєнного стану та євроінтеграції.

1. Дослідити сучасні технології моніторингу та ідентифікувати основні етичні, правові та психологічні ризики їх застосування, зокрема проблему алгоритмічної упередженості та мозаїчного ефекту.

2. Розробити архітектурну модель системи етичного моніторингу, що базується на принципах приватності за замовчуванням та вибіркової видимості.

3. Сформулювати алгоритми псевдонімізації даних та контекстної фільтрації трафіку, а також протоколи деанонімізації інцидентів.

4. Розробити практичні рекомендації щодо впровадження етичного моніторингу та провести експериментальну перевірку ефективності запропонованої моделі.

Об’єктом дослідження є процеси моніторингу, збору та аналізу даних про активність користувачів та систем у контурі інформаційної та кібернетичної безпеки.

Предмет дослідження – методи, алгоритми та архітектурні рішення для забезпечення етичного використання технологій контролю інформаційних потоків та виявлення кіберзагроз.

Методи дослідження. У роботі використано комплексний підхід: методи системного аналізу – для дослідження структури загроз та архітектури SOC; методи порівняльного правового аналізу – для зіставлення вимог українського законодавства та стандартів ЄС; методи моделювання загроз, для оцінки ризиків приватності; емпіричні методи, для апробації розробленої системи та оцінки її ефективності за метриками MTTD/MTTR.

Наукова новизна одержаних результатів полягає у вирішенні завдання гармонізації вимог безпеки та приватності шляхом розробки нових підходів до архітектури систем моніторингу: удосконаленння методу поведінкового аналізу

користувачів шляхом впровадження концепції вибіркової видимості та динамічного зонування цифрового простору, що, на відміну від існуючих бінарних підходів, дозволяє автоматично змінювати глибину моніторингу залежно від рівня ризику та категорії ресурсу; подальшим розвитком архітектури моделі центру операцій з безпеки через введення нового компонента шлюзу приватності, який забезпечує псевдонімізацію та санітизацію даних до моменту їх збереження, що унеможливлює несанкціонований масовий нагляд; формалізацією технічного протоколу деанонімізації інцидентів з використанням криптографічного розділення ключів, що забезпечує невідворотність юридичного контролю над діями адміністраторів безпеки.

Практичне значення одержаних результатів полягає у розробці готового до впровадження на об'єктах критичної інфраструктури комплексу рішень, що дозволяють організаціям мінімізувати юридичні ризики, уникнути штрафів за порушення законодавства про захист даних та підвищити довіру персоналу, що підтверджено розрахунком ROI.

Галузь застосування. Результати роботи можуть бути використані при проектуванні та модернізації систем кіберзахисту державних установ, банківського сектору, енергетичних компаній та інших об'єктів критичної інфраструктури, а також у навчальному процесі при підготовці фахівців з кібербезпеки.

Апробація результатів кваліфікаційної роботи відбулася на науково-практичній конференції «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем» Навчально-наукового інституту кібербезпеки та захисту інформації, кафедра Технічних систем кіберзахисту.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ЕТИЧНОГО МОНІТОРИНГУ В КІБЕРБЕЗПЕЦІ

1.1 Поняття інформаційної та кібербезпеки критичних систем

Глобальна цифровізація призвела до того, що інформація стала найбільш цінним активом, а її захист - основою національної безпеки. Хоча терміни інформаційна безпека та кібербезпека часто використовуються як синоніми в побуті та медіа, фактично це окремі поняття, які займають різні місця в ієрархії захисту даних.

Інформаційна безпека (ІБ) - це комплекс організаційно-правових, технічних та фізичних заходів, спрямованих на захист інформаційних ресурсів від усіх видів загроз, незалежно від форми подання інформації. ІБ є ширшою, всеосяжною дисципліною, що існувала задовго до появи інтернету.

Кібербезпека (КБ), згідно з Законом України Про основні засади забезпечення кібербезпеки України, - це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються кіберстійкість та кіберзахист. На відміну від ІБ, КБ зосереджується виключно на загрозах, що виникають у кіберпросторі, тобто у віртуальному середовищі.

Таблиця 1.1

Порівняння інформаційної безпеки та кібербезпеки

Критерій	**Інформаційна безпека**	**Кібербезпека**
Фокус захисту	Інформація (у всіх формах) та інформаційні системи, що її обробляють.	Кіберпростір, мережі, інфраструктура, програмне забезпечення, підключені пристрої.

Продовження таблиці 1.1

Критерій	**Інформаційна безпека**	**Кібербезпека**
Сфера застосування	Комплексна (включає організаційні політики, навчання персоналу, фізичний захист ЦОД та цифрові технології).	Технічна (захист мережевого периметру, виявлення вразливостей, криптографія, реагування на інциденти).
Ключове питання	Як забезпечити збереження цінності інформації?	Як захистити системи від кібератак та загроз у мережевому середовищі, забезпечуючи кіберстійкість?
Приклади загроз	Крадіжка паперових звітів, промислове шпигунство (прослуховування), фізичний саботаж, злам комп'ютерної системи.	DDoS-атаки, фішинг, віруси-вимагачі, експлойти нульового дня, державне кібершпигунство.

Цілі забезпечення безпеки: тріада CIA та її розширення

Будь-яка система безпеки, особливо в критичній інфраструктурі, будується навколо забезпечення трьох ключових властивостей інформації, відомих як тріада CIA: конфіденційність, цілісність та доступність. Ця тріада є основним критерієм оцінки ефективності будь-якої політики безпеки:

1) конфіденційність - Принцип полягає в обмеженні доступу до інформації лише авторизованими користувачами, об’єктами або процесами. Це досягається за допомогою механізмів автентифікації, авторизації та шифрування. Порушення конфіденційності призводить до витоку чутливих даних (державна таємниця, персональні дані, комерційні секрети), що у випадку критичних систем може мати катастрофічні наслідки для національної безпеки.

2) цілісність - Властивість гарантує, що дані та методи їх обробки є точними, повними та не були змінені несанкціонованим чином. Це особливо критично для систем управління технологічними процесами (SCADA в енергетиці), де модифікація даних про тиск або температуру може спричинити фізичну катастрофу. Забезпечення цілісності вимагає використання контрольних сум, цифрових підписів та строгих процедур керування змінами.

3) доступність - Це гарантія безперебійного доступу авторизованих користувачів та систем до інформаційних ресурсів. Для критичної інфраструктури (наприклад, системи раннього сповіщення, фінансові транзакції)

доступність часто є найпріоритетнішою метою. Найпоширеніші загрози доступності - це атаки типу відмова в обслуговуванні (DDoS), збої обладнання та відсутність резервування.

Визначення та типологія критичних інформаційних систем (КІС)

Концепція критичної інформаційної інфраструктури, а отже і критичних інформаційних систем, виділяє об'єкти, які потребують найвищого рівня захисту. Згідно з європейським та українським законодавством, КІІ - це сукупність систем, порушення функціонування яких матиме серйозний негативний вплив на національну безпеку, оборону, економіку чи життєдіяльність населення.

Критичність системи оцінюється за впливом, а не за її технологічною складністю. Основні критерії включають:

1) ступінь залежності: взаємозв'язок системи з іншими секторами (вихід з ладу системи керування електростанцією зупиняє роботу транспорту, лікарень та фінансових установ);

2) масштаб наслідків: оцінка економічних, соціальних та гуманітарних втрат;

3) час відновлення: якщо час відновлення системи критично довгий, це підвищує її вразливість, оскільки загроза перетворюється на незворотну катастрофу.

Системи КІІ класифікуються за секторами, кожен з яких має унікальні цілі безпеки. Моніторинг у кожному секторі потребує різної специфіки, наприклад, моніторинг промислових протоколів в енергетиці чи моніторинг фінансових транзакцій у банківській сфері.

Рис.1.1. Класифікація секторів критичної інфраструктури

Значення безпеки критичних систем у контексті національної безпеки

Безпека КІС є складовою національної безпеки. Кіберзагрози більше не обмежуються крадіжкою коштів чи даних; вони перетворилися на інструмент геополітичного впливу та ведення війни. Порушення функціонування КІС може призвести до:

1) економічного колапсу: зупинка енергетичного сектору або фінансових транзакцій;

2) соціальної дестабілізації: збій у наданні критичних послуг (водопостачання, охорона здоров’я);

3) військової переваги противника: використання кіберзасобів для виведення з ладу військових комунікацій або систем керування.

Сучасні кіберзагрози національного масштабу включають:

1) кібервійна: атаки, спонсоровані державами (Розвинені постійні загрози, APT), спрямовані на довгострокове проникнення та руйнування інфраструктури, як це було з атаками на енергетичну систему України у 2015-2016 роках.

2) гібридні загрози: використання кіберзасобів для поширення дезінформації, яка підриває довіру до державних інститутів, посилюючи ефект від фізичних або економічних атак.

3) кібершпигунство: крадіжка технологій та військових секретів, що прямо впливає на обороноздатність.

Усвідомлення загрози змусило держави закріпити вимоги до захисту КІС на законодавчому рівні. Ці закони прямо або опосередковано вимагають впровадження систем постійного моніторингу та контролю.

Рис.1.2.Регуляторні вимоги до безпеки КІС

Моніторинг як невід'ємна функція забезпечення безпеки

У динамічному середовищі кіберзагроз пасивні засоби захисту (антивіруси, фаєрволи) є необхідною, але недостатньою умовою безпеки. Критичні системи вимагають активної та проактивної оборони, що реалізується через безперервний моніторинг.

У контексті кібербезпеки моніторинг - це систематичний, автоматизований процес збору, нормалізації, агрегації, аналізу та довготривалого зберігання журналів подій, мережевого трафіку та телеметрії системи з метою виявлення ознак компрометації, відхилень у нормальній поведінці або порушень політики безпеки.

Моніторинг КІС охоплює три основні рівні:

1) мережевий рівень: аналіз пакетів даних, що проходять через мережу. Інструменти, такі як системи виявлення вторгнень (IDS/IPS), сканують трафік на

наявність відомих сигнатур атак або аномалій протоколів (особливо важливих для промислових мереж).

2) хостовий (системний) рівень: збір журналів подій з операційних систем, серверів, баз даних та додатків.

3) аналітичний рівень: централізований аналіз мільйонів подій, зібраних з мережевого та хостового рівнів. Ключовий інструмент тут - системи керування інформацією та подіями безпеки (SIEM).

SIEM (Управління інформацією та подіями безпеки) не просто збирає логи, а й корелює події в реальному часі. Наприклад, виявляє, що неуспішна спроба входу з одного пристрою одразу супроводжується незвично великим вихідним трафіком, що може вказувати на атаку.

Окремо варто виділити UEBA (Аналітика поведінки користувачів і сутностей) - аналіз поведінки користувачів та об'єктів. Цей метод будує базову нормальну поведінку (користувач ніколи не заходить на сервер о 3-й ночі) і сигналізує про будь-які відхилення, що є критичним для виявлення внутрішніх загроз.

Останній пункт - аналіз поведінки користувачів (UEBA), який вимагає глибокого та всебічного збору даних про їхню активність - виводить на головну проблему дослідження. Необхідність захисту національної безпеки через глибокий моніторинг вступає у прямий конфлікт із фундаментальним правом особи на приватність. Цей конфлікт, що лежить на межі технічних вимог та етичних норм, детально розглянуто далі у роботі.

1.2 Сучасні технології моніторингу: SIEM, SOC, Network Monitoring, AI/ML

Захист критичної інформаційної інфраструктури (КІІ) вимагає переходу від статичних, периметральних засобів захисту (міжмережевих екранів) до проактивного, безперервного моніторингу активності. Сучасна кібербезпека ґрунтується на концепції Видимість - це захист, що реалізується через інтеграцію

високотехнологічних рішень, які спільно формують комплексний захисний простір.

Системи управління інформацією та подіями безпеки (SIEM)

SIEM є технологічним фундаментом і центральною точкою збору даних для будь-якого сучасного центру кібербезпеки. Це комплексне рішення, яке поєднує функції управління інформацією безпеки (SIM - збір та зберігання логів) та управління подіями безпеки (SEM - аналіз у реальному часі).

SIEM-системи забезпечують не просто журналювання, а цілісну картину безпеки завдяки чітко структурованому процесу обробки даних (Data Pipeline):

1) збір та агрегація: агрегація логів з усього IT/OT ландшафту: мережеві пристрої, сервери (ОС, вебсервери), системи безпеки (IDS/IPS, Firewalls), додатки, бази даних. Використовуються агенти (для кінцевих точок), стандартизовані протоколи (Syslog, SNMP) або API;

2) нормалізація та розбір: перетворення тисяч різнорідних форматів логів (від Windows Event Log до Cisco ASA) у єдиний, стандартизований формат (CEF або LEEF). Цей етап критично важливий для подальшої кореляції;

3) зберігання та індексування: збереження очищених та нормалізованих даних, часто у вигляді озера даних безпеки, для швидкого пошуку та судового аналізу. Обсяги даних вимірюються терабайтами на день;

4) кореляція: найважливіша функція SIEM. Це зіставлення розрізнених подій у реальному часі для виявлення послідовності дій, що відповідає сценарію кібератаки. Кореляція здійснюється за правилами, які можуть бути сигнатурними (виявлення відомих загроз) або поведінковими (виявлення аномалій).

Для критичних систем (КІІ) SIEM виконує кілька незамінних функцій:

1) виявлення APT та TTP. SIEM дозволяє виявляти складні, багатоетапні атаки (APT) шляхом зіставлення індикаторів компрометації з різних джерел, що відповідають тактикам MITRE ATT&CK (поєднання невдалої

автентифікації на сервері з подальшим запуском рідкісної команди PowerShell на кінцевій точці).

2) відповідність та аудит. Довготривале зберігання аудиторських слідів (до 1 року і більше) є обов'язковим для дотримання регуляторних вимог, таких як ISO/IEC 27001 та національне законодавство про КІІ. Це забезпечує підзвітність та неможливість відмови від виконаних дій.

3) моніторинг OT-мереж. Інтеграція з пасивними моніторами OT-мереж дозволяє SIEM корелювати події з IT-периметра з аномаліями в OT-середовищі (наприклад, несанкціонована зміна налаштувань PLC через легітимний шлюз).

Таблиця 1.2

Приклади логів SIEM та їхня етична чутливість

Джерело логів	**Тип логів**	**Приклад етичної чутливості**
Робочі станції користувачів (EDR)	Запуск програм, доступ до файлів.	Моніторинг неробочої діяльності (соціальні мережі, особисті документи).
Проксі-сервери	Повний URL, час доступу.	Історія відвідувань вебресурсів, що є чутливою інформацією.
VPN-шлюзи	Час входу, зовнішня IP-адреса.	Визначення місцеперебування співробітника поза робочим місцем.

Центр операцій з безпеки (SOC)

SOC - це не просто технологічний інструмент, а організаційно-технічна структура, що забезпечує безперервне функціонування захисту. SOC об'єднує людей, процеси та технології (SIEM, EDR, TI) для моніторингу, виявлення, аналізу та реагування на інциденти в режимі 24/7.

Ефективний SOC функціонує на основі чіткої ієрархії, що забезпечує швидкість та якість реагування (табл. 1.3).

Таблиця 1.3

Ієрархія аналітиків SOC

Рівень (Tier)	**Основні обов'язки**	**Кваліфікація**	**Роль у моніторингу**
Tier 1 (Сортування/ Моніторинг)	Первинний відсів, валідація тривог, фільтрація фальшивих спрацьовувань.	Початковий/середній рівень.	Цілодобовий моніторинг SIEM-консолі.
Tier 2 (Реагування та аналіз)	Глибокий аналіз підтверджених інцидентів, розслідування, визначення кореневої причини.	Середній/високий рівень, навичоч цифрової криміналістики.	Використання NDR, EDR для розслідування конкретних дій користувача.
Tier 3 (Полювання на загрози та інженерія)	Проактивний пошук прихованих загроз, розробка нових правил кореляції, управління системами безпеки.	Експертний рівень, знання MITRE ATT&CK.	Створення профілів поведінки та правил, що підвищують чутливість моніторингу.
Tier 4 (SOC Manager/CSIRT Lead)	Стратегічне управління, комунікація з керівництвом, координація дій з командою реагування на інциденти.	Управлінський рівень.	Прийняття рішень про зупинку критичних систем.

SOC керується стандартизованим процесом реагування на інциденти, який, згідно з NIST SP 800-61 Rev. 2 або методологією SANS, складається з шести основних фаз:

Рис.1.3. Процеси SOC

1) Підготовка. Розробка політик, налаштування інструментів моніторингу (SIEM, NDR), навчання персоналу.

2) Виявлення та аналіз. Збір логів, валідація тривог, визначення масштабу інциденту. Це пряма функція Tier 1 аналітиків.

3) Стримування. Ізоляція скомпрометованих систем або користувачів для запобігання подальшому поширенню атаки. Наприклад, відключення мережевого доступу для підозрілої робочої станції.

4) Викорінення. Видалення кореневої причини атаки (шкідливе ПЗ, скомпрометовані облікові записи).

5) Відновлення. Повернення систем до нормальної роботи, верифікація захисних механізмів.

6) Діяльність після інциденту. Складання звіту, документування уроків та оновлення політик моніторингу.

Усі ці фази вимагають безперервного доступу до даних моніторингу. Найбільш етично чутливою є фаза Виявлення та аналіз, оскільки вона передбачає глибоке вивчення активності конкретних осіб.

Ефективність SOC вимірюється набором кількісних метрик (KPI), які демонструють здатність організації забезпечувати кіберстійкість:

1) MTTD: середній час на виявлення інциденту. Чим менше, тим краще. Прямо залежить від якості SIEM та UEBA;

2) MTTR: середній час на реагування на інцидент. Прямо залежить від ефективності Tier 1/2 та SOAR;

3) MTTC: середній час на стримування атаки. Критична метрика для КІІ, де швидка ізоляція запобігає фізичній шкоді.

NDR фокусується на трафіку даних, який є автомагістраллю для горизонтального переміщення зловмисника всередині мережі КІІ. Традиційні системи виявлення вторгнень (IDS) працюють за сигнатурами, виявляючи відомі атаки. NDR використовує більш просунуті, поведінкові методи:

1) аналіз потоків (NetFlow/IPFIX). Збір лише метаданих про мережевий потік (час початку/закінчення, джерело, призначення, порт, обсяг переданих

байтів). Це менш інвазивний метод, який ідеально підходить для виявлення аномальної передачі даних (наприклад, незвичний обсяг трафіку з сервера бази даних на зовнішню IP-адресу);

2) глибока інспекція пакетів (DPI). Аналіз вмісту пакета на рівні додатків (Layer 7). DPI дозволяє ідентифікувати, який саме протокол використовується (наприклад, HTTP, FTP, або навіть OT-протокол Modbus) та чи відповідає вміст пакета цьому протоколу. DPI може виявити тунелювання зловмисника в легітимному трафіку;

3) повне захоплення пакетів (FPC). Повний запис усього мережевого трафіку для подальшого судового аналізу. Це найефективніший, але і найбільш етично чутливий метод, оскільки FPC може містити незашифровані паролі, особисті комунікації та чутливу комерційну інформацію.

У критичних системах NDR є ключовим, оскільки сенсори працюють у пасивному режимі (мережеве дзеркалювання, SPAN-порти), не взаємодіючи з чутливим OT-обладнанням (PLC, RTU), що є безпечним. Крім того, NDR використовує специфічні OT-протоколи (Modbus, DNP3, IEC 61850). Моніторинг виявляє не лише аномалії, але й несанкціоновані команди (команду на вимкнення обладнання, що не була ініційована з легітимної HMI-станції).

Використання FPC та DPI створює пряму загрозу приватності. Необхідність аналізувати вміст пакетів для виявлення шкідливих команд (особливо у внутрішньому трафіку) вступає в конфлікт з конституційним правом на таємницю листування та комунікацій, навіть якщо йдеться про робочий простір.

Штучний інтелект та машинне навчання у моніторингу (AI/ML)

Обсяги даних, що генеруються КІІ, досягають рівня, коли людський аналіз стає фізично неможливим. AI/ML став обов'язковим елементом для автоматизації виявлення та реагування.

UEBA є найбільш революційною та найбільш етично значущою областю застосування AI/ML у КБ. UEBA фокусується на виявленні аномалій у поведінці, що є єдиним ефективним методом виявлення інсайдерів та скомпрометованих

облікових записів (APT).

Алгоритмічні принципи роботи UEBA:

1) збір поведінкових даних: збираються мільйони точок даних, що описують активність користувача: час входу, географія, частота доступу до серверів, швидкість набору тексту, типові команди;

2) побудова базової лінії: алгоритми машинного навчання створюють динамічний відбиток нормальної поведінки для кожного користувача. Наприклад, формується профіль: Інженер ніколи не працює з базою даних А після 18:00;

3) виявлення аномалій: поточна активність постійно порівнюється з базовою лінією. Відхилення (наприклад, о 23:00 вперше завантажує 5 ГБ даних) призводить до підвищення балу ризику.

UEBA є надзвичайно ефективним, але його робота цілком залежить від постійного, глибокого та індивідуального профілювання кожного співробітника. Це прямо порушує принцип мінімізації даних, що є наріжним каменем приватного життя[35].

SOAR використовує AI/ML для автоматизації рутинних завдань SOC, прискорюючи час реагування до секунд, що є критичним для запобігання каскадним збоям у КІІ.

Таблиця 1.4

Компоненти SOAR та пов'язані ризики

Компонент SOAR	**Опис та роль**	**Етичний ризик**
Оркестрація	Координація різних інструментів (SIEM, EDR, Firewall) за стандартизованими плейбуками.	Ризик прийняття помилкових рішень із каскадними наслідками.
Автоматизація	Виконання рутинних завдань без втручання людини.	Ненавмисне знищення важливих даних під час автоматизованого викорінення.

Продовження таблиці 1.4

Компонент SOAR	**Опис та роль**	**Етичний ризик**
Реагування	Забезпечення стандартизованих сценаріїв для швидкої реакції.	Блокування легітимних користувачів або критичних процесів через помилкове спрацювання AI.

Роль SOAR полягає у перетворенні виявленої аномалії (UEBA/SIEM) на негайну дію, але швидкість тут прямо корелює з ризиком помилки та неправомірним втручанням у діяльність легітимного користувача.

1.3 Етичні аспекти використання технологій моніторингу

Цифровий Паноптиком та парадокс безпеки

В умовах сучасної гібридної війни захист критичної інформаційної інфраструктури (КІІ) трансформувався з суто технічної задачі у фундаментальну проблему національної безпеки. Технології SIEM, SOC, NDR та UEBA фактично перетворюють робоче середовище об'єктів КІІ на цифровий аналог Паноптикому (концепція Джеремі Бентама та Мішеля Фуко) - простір, де кожен суб'єкт (користувач) потенційно перебуває під наглядом у будь-який момент часу, але ніколи не знає напевно, чи спостерігають за ним саме зараз.

Ця ситуація створює фундаментальний парадокс безпеки: для захисту демократичного суспільства та його критичних активів необхідно застосовувати інструменти тотального контролю, які за своєю природою є авторитарними та обмежують права цього ж суспільства. Конфлікт між імперативом колективної безпеки та індивідуальним правом на приватність стає центральною етичною проблемою сучасної кібербезпеки.

Теоретико-філософські засади: зіткнення етичних парадигм

Для академічного розуміння конфлікту безпека проти приватності необхідно вийти за рамки технічних термінів і звернутися до етичної філософії, яка пропонує різні моделі виправдання державного втручання.

Утилітаризм проти деонтології та теорії суспільного договору

У контексті моніторингу КІІ стикаються три основні течії:

1) Утилітаризм, суть: моральна цінність дії визначається її корисністю. Правильним є те рішення, що приносить найбільше щастя найбільшій кількості людей. Аргумент за моніторинг: потенційна шкода від успішної кібератаки на енергосистему (блекаут, зупинка лікарень, паніка) є катастрофічною для мільйонів. Втрата приватності кількох сотень співробітників КІІ є незначною ціною за відвернення цієї катастрофи. Безпека розглядається як вище суспільне благо. Ризик: цей підхід може виправдати будь-які, навіть найбільш жорстокі заходи контролю, якщо вони ефективні.

2) Деонтологія, суть: етика ґрунтується на моральних обов'язках та правилах (імперативах). Певні права людини є невідчужуваними та абсолютними, незалежно від наслідків. Аргумент проти моніторингу: людина має право на автономію та гідність (Іммануїл Кант). Використання людини лише як об'єкта спостереження (засобу для досягнення безпеки) є аморальним. Порушення таємниці листування є неприпустимим, навіть якщо це підвищує ризики.

3) Теорія суспільного договору, суть: громадяни добровільно поступаються частиною своїх свобод державі (або роботодавцю) в обмін на захист і порядок. Синтез: співробітники КІІ, приймаючи посаду, вступають у специфічний договір. Вони добровільно погоджуються на підвищений рівень прозорості своєї діяльності в обмін на привілей працювати на стратегічно важливому об'єкті та отримувати відповідну винагороду.

Концепція контекстуальної цілісності

Сучасна дослідниця Хелен Ніссенбаум пропонує теорію “контекстуальної цілісності”. Згідно з нею, приватність - це не просто приховування інформації, а дотримання норм потоку інформації, відповідних конкретному контексту.

Приклад порушення: якщо лікар передає медичні дані пацієнта страховій компанії - це порушення контексту. Застосування до КІІ: якщо дані моніторингу

(логи активності, листування), зібрані для кібербезпеки, використовуються для оцінки продуктивності або політична лояльність - це є етичним порушенням, навіть якщо самі дані були зібрані законно.

Таблиця 1.5

Порівняльний аналіз етичних підходів до моніторингу

Етична теорія	**Фокус уваги**	**Погляд на моніторинг КІІ**	**Ключовий недолік**
Утилітаризм	Наслідки	Виправданий, якщо запобігає катастрофі.	Ризик тиранії більшості, ігнорування прав меншості.
Деонтологія	Обов'язки та права	Проблематичний, якщо порушує фундаментальні права.	Ризик негнучкості перед лицем екзистенційних загроз.
Суспільний договір	Згода	Легітимний за умови свідомої згоди сторін.	Проблема примусової згоди при працевлаштуванні.
Контекстуальна цілісність	Потік інформації	Прийнятний, поки дані не виходять за межі контексту безпеки.	Складність технічного забезпечення меж контексту.

Анатомія інвазивності: технологічний розріз етичних ризиків

Мережевий моніторинг: проблема зламу печатки

Технології DPI (глибокий аналіз пакетів) та SSL/TLS розшифровка трафіку на льоту є найбільш суперечливими. Більшість сучасного вебтрафіку (HTTPS) є зашифрованим. Для ефективного аналізу загроз (виявлення шкідливого ПЗ у трафіку) системи безпеки КІІ використовують техніку MitM (людина посередині): вони підміняють сертифікати та розшифровують увесь трафік користувача на шлюзі безпеки.

Етична проблема полягає в тому, що разом із робочим трафіком (доступ до SCADA-серверів) часто перехоплюється приватний трафік (онлайн-банкінг, доступ до медичних порталів, особиста пошта), якщо співробітник використовує робочий комп'ютер для особистих потреб (що часто трапляється, незважаючи на заборони). Існує ризик отримання доступу до паролів, фінансового стану,

діагнозів. Це є еквівалентом читання паперових листів та прослуховування телефонних розмов.

AI та UEBA

Системи поведінкового аналізу (UEBA) створюють динамічні профілі користувачів. Тут виникають специфічні ризики штучного інтелекту:

1) алгоритмічна упередженість: якщо навчальна вибірка складалася переважно з даних про поведінку певної групи людей (наприклад, чоловіків віком 30–40 років, що працюють у стандартні години), то поведінка жінки, яка працює віддалено через догляд за дитиною і має нестандартний графік, може бути розцінена системою як аномальна та ризикована;

2) проблема пояснюваності: сучасні нейромережі часто діють як чорні скриньки. Система може видати вердикт високий ризик інсайдерської загрози для співробітника, але навіть оператори SOC не зможуть пояснити, чому було прийнято таке рішення. Це робить неможливим ефективне оскарження рішення та захист честі співробітника;

3) предиктивна поліція: UEBA намагається передбачити порушення до того, як воно сталося. Етично це межує з покаранням за роздуми, коли людину піддають додатковим перевіркам лише на основі ймовірнісних прогнозів алгоритму.

Endpoint Monitoring: кейлогери та знімки екрана

У найбільш критичних зонах (диспетчерські центри АЕС) можуть застосовуватися агенти моніторингу активності користувачів (UAM), які роблять знімки екрана кожні 5 секунд або записують натискання клавіш. Ризик полягає в абсолютній втраті приватності. Будь-яке випадково відкрите приватне вікно, переписка у месенджері або введення пароля стає надбанням служби безпеки.

Психосоціальні та організаційні наслідки: ефект спостерігача

Вплив моніторингу виходить далеко за межі суто технічного збору даних. Він трансформує соціальну тканину організації.

Ефект заморожування

Психологічні дослідження підтверджують, що люди, які знають про

спостереження, змінюють свою поведінку у бік пристосування. Суть явища полягає в тому, що співробітники уникають гострих тем у комунікації, бояться висловлювати критику керівництва, менше експериментують з новими методами роботи, побоюючись, що будь-яке відхилення від інструкції буде зафіксовано як аномалія.

Для КІІ це має наслідком зниження безпеки. Співробітники можуть приховувати дрібні помилки замість того, щоб повідомляти про них, боячись покарання. Це заважає культурі справедливості, яка є критичною для авіації та енергетики.

Феномен повзучого розширення функцій

Розширення функцій - це використання даних або систем, впроваджених для однієї мети (кібербезпеки), для інших, не заявлених цілей. Наприклад, система перепусток та логів входу в комп'ютер, встановлена для запобігання несанкціонованому доступу, починає використовуватися HR-відділом для автоматичного штрафування співробітників за запізнення на 5 хвилин.

Етичний наслідок цього - порушення довіри та первинного суспільного договору. Співробітники починають сприймати службу безпеки як каральний орган (цифрова тюрма), а не як захисників, і починають шукати шляхи обходу систем моніторингу, що створює нові дірки у безпеці.

Таблиця 1.6

Типологія повзучого розширення у системах моніторингу

Тип розширення	**Опис**	**Приклад загрози**
Функціональне	Зміна мети використання даних.	Використання DLP-системи для аналізу лояльності персоналу або пошуку профспілкових активістів.
Масштабне	Розширення об'єктів моніторингу.	Поширення моніторингу з корпоративних ПК на особисті смартфони (BYOD), підключені до Wi-Fi.
Данні	Збір надлишкових даних про всяк випадок.	Запис повного аудіо в диспетчерській замість лише службових переговорів.

Принципи етично збалансованого моніторингу

Для вирішення описаних дилем необхідно впровадити жорсткий етичний фреймворк, який базується на міжнародних стандартах (GDPR, Guidelines 2/2017 on data processing at work, NIST Privacy Framework).

Принцип пропорційності та необхідності

Це золотий стандарт легітимності моніторингу. Перед впровадженням будь-якого засобу контролю необхідно пройти трискладовий тест:

1) тест на придатність: чи справді цей захід (наприклад, SSL-декрипція) дозволяє досягти мети (виявлення вірусів)?;

2) тест на необхідність: чи є це найменш інвазивний спосіб досягнення мети? Якщо загрозу можна виявити за допомогою аналізу метаданих, то читання вмісту пакетів (DPI) є етично неприпустимим;

3) тест на пропорційність у вузькому сенсі: чи не перевищує шкода для прав особистості переваги для безпеки?

Принцип прозорості та гранулярної згоди

Просте підписання згоди на обробку даних при наймі є недостатнім. Необхідна активна прозорість.

1) чіткі політики (AUP): документи мають бути написані зрозумілою мовою, без юридичного жаргону. Співробітник повинен знати: Мій екран записують, коли я працюю з системою SCADA, але не записують, коли я перевіряю пошту в обідню перерву;

2) візуальні індикатори: ідеальним етичним рішенням є наявність іконки в треї системи, яка світиться, коли ведеться активний запис екрана або перехоплення трафіку. Це повертає суб'єкту відчуття контролю та розуміння контексту.

Принцип мінімізації даних

Етика має бути вбудована в архітектуру системи:

1) псевдонімізація: у системі SIEM імена користувачів мають бути замінені на хеші (User_A123). Аналітик Tier 1 бачить лише аномалію користувача User_A123. Деанонімізація (зіставлення хешу з прізвищем) можлива

лише при ескалації інциденту до Tier 2/3 і вимагає цифрового ключа від менеджера;

2) фільтрація приватного контенту: налаштування SSL-інспекції таким чином, щоб автоматично виключати з розшифровки домени категорій Health, Banking, Legal, Government Services. Це технічно реалізовано у більшості сучасних NGFW (Palo Alto, Fortinet).

Обмеження мети

Дані, зібрані для безпеки, повинні мати технічні та юридичні запобіжники від використання в інших цілях. Це означає, що HR-департамент фізично не повинен мати доступу до консолі SIEM або звітів UEBA.

Механізми контролю та управління

Етичні принципи не працюють без механізмів примусу.

Наглядова рада з етики даних

Для великих об'єктів КІІ рекомендується створення колегіального органу:

1) склад: CISO (Головний директор з інформаційної безпеки), DPO (Спеціаліст із захисту даних), представник профспілки/колективу, юрист;

2) повноваження: розгляд скарг співробітників, затвердження нових правил кореляції UEBA (щоб уникнути дискримінації), періодичний аудит логів доступу аналітиків SOC.

Аудит спостерігачів

Необхідно встановити контроль за тими, хто здійснює спостереження:

1) імутабельні логи: дії адміністраторів безпеки та аналітиків SOC повинні записуватися у захищене сховище (наприклад, на базі блокчейну або WORM-носіїв), яке вони самі не можуть стерти;

2) регулярний аудит доступу: вибіркова перевірка (наприклад, чому аналітик переглядав листування директора у певну дату та чи був відкритий відповідний тікет інциденту). Якщо тікета немає - це посадовий злочин.

1.4 Нормативно-правова база та міжнародні стандарти

Юридична колізія у кіберпросторі

Етичний моніторинг у кібербезпеці функціонує в умовах складної правової архітектури, яка часто характеризується внутрішніми суперечностями. Оператори критичної інформаційної інфраструктури (КІІ) знаходяться під тиском подвійного імперативу:

1) імператив безпеки: національне та міжнародне законодавство про критичну інфраструктуру зобов'язує їх забезпечувати повну видимість мережевих процесів, що технічно неможливо без глибокого моніторингу (DPI, UEBA);

2) імператив приватності: конституційні норми та законодавство про захист даних (GDPR) вимагають мінімізації втручання у приватне життя, навіть на робочому місці.

Метою даного підрозділу є системний аналіз нормативно-правового поля, що регулює моніторинг.

Міжнародні стандарти управління інформаційною безпекою та приватністю

Технічні стандарти є фундаментом, який визначає, що і як необхідно моніторити. Вони слугують доказовою базою належної обачності (Due Diligence) у суді.

Еволюція ISO/IEC 27001:2022 та роль ISO/IEC 27701

Стандарт ISO/IEC 27001 є глобальним стандартом для побудови систем управління інформаційною безпекою (СУІБ).

1) Технічні вимоги до моніторингу (ISO/IEC 27001:2022 Annex A):

Контроль A.8.15: цей контроль вимагає не просто наявності логів, а забезпечення їхньої цілісності (захист від модифікації інсайдерами) та доступності для аналізу. Логи повинні містити: ID користувача, тип події, дату/час, успіх/неуспіх, джерело (IP). Стандарт рекомендує виключати чутливу інформацію (паролі) з логів, що відповідає принципу Privacy by Design.

Контроль A.8.16: визначає необхідність виявлення аномальної поведінки. Це є прямою вказівкою на використання систем класу UEBA/SIEM. Стандарт зазначає, що рівень моніторингу має відповідати рівню ризику .

Контроль A.5.7: вимагає збору інформації про загрози, що включає профілювання потенційних зловмисників.

2) ISO/IEC 27701: розширення приватності (PIMS).

Для вирішення етичних конфліктів було розроблено стандарт ISO/IEC 27701, який розширює СУІБ до Системи управління приватною інформацією (PIMS). Він вводить поняття PII (Особиста ідентифікаційна інформація) у контекст кібербезпеки. Оператори КІІ повинні розглядати логи активності співробітників як PII та застосовувати до них відповідні заходи захисту (шифрування, обмеження доступу).

NIST SP 800-53 (Ревізія 5): підхід урядового рівня

Стандарти NIST є більш детальними і є обов'язковими для багатьох секторів КІІ (енергетика, оборона):

1) Family AU (Аудит та підзвітність):

a. AU-3 (Вміст аудиторських записів): встановлює жорсткі вимоги до атрибуції дій. Система повинна однозначно пов'язувати кожну дію з конкретною фізичною особою. Це ускладнює використання спільних облікових записів (наприклад, admin), що є позитивним для безпеки, але підвищує рівень індивідуального нагляду.

b. AU-12 (Формування аудиторських записів): вимагає автоматизованого збору аудиторських записів з усіх компонентів інформаційної системи.

2) Family SI (Цілісність систем та інформації):

a. SI-4 (Моніторинг систем): це ключовий контроль. Він дозволяє моніторинг трафіку, але містить важливе застереження

b. SI-4(18) (Вплив на приватність): Організація повинна консультуватися з юридичним радником та офіцером з приватності щодо легітимності моніторингу. Це пряме посилання на необхідність юридичної

валідації технічних дій SOC.

NIST Структура управління ризиками (RMF): вимагає категоризації системи не лише за впливом на безпеку, але й за впливом на приватність.

Таблиця 1.7

Порівняльний аналіз підходів до моніторингу в ISO та NIST 13

Параметр порівняння	**ISO/IEC 27001:2022**	**NIST SP 800-53 Rev. 5**
Природа стандарту	Міжнародний, комерційний, гнучкий.	Урядовий (США), жорсткий, детальний.
Підхід до моніторингу	Ризик-орієнтований (визначається організацією).	Обов'язковий перелік контролів.
Інтеграція приватності	Через окремий стандарт ISO 27701.	Вбудована.
Рекомендація для України	Основа для корпоративного сектору.	Орієнтир для державних органів та військових.

Європейський регламент захисту даних (GDPR) та права людини

GDPR (Загальний регламент про захист даних) є найбільш впливовим нормативним актом у світі, що регулює обробку персональних даних. Оскільки логи активності користувачів є персональними даними (вони дозволяють ідентифікувати особу), GDPR прямо регулює діяльність SOC/SIEM.

Принципи обробки даних (Art. 5 GDPR) у контексті моніторингу:

1) Законність, справедливість та прозорість: співробітники повинні знати, що їх моніторять. Прихований моніторинг дозволений лише у виняткових випадках розслідування злочину.

2) Обмеження мети: дані, зібрані для кібербезпеки (логи входу в систему), не можуть бути використані для оцінки продуктивності праці (для штрафування за запізнення), якщо про це не було заявлено окремо. Це захист від повзучого розширення.

3) Мінімалізація даних: SOC повинен збирати лише ті дані, які необхідні для виявлення інциденту. Збір повного змісту приватного листування

без вагомих підстав є порушенням цього принципу.

4) Обмеження зберігання: логи не повинні зберігатися безстроково. Необхідно встановити чіткі терміни, 6 або 12 місяців, після чого дані мають бути видалені або анонімізовані.

Правові підстави (Art. 6) та балансувальний тест

Для легалізації моніторингу роботодавець (оператор КІІ) не може покладатися на згоду працівника, оскільки у трудових відносинах існує дисбаланс влади. Основною підставою є Законний інтерес (Art. 6(1)(f)).

Вступ 49 GDPR прямо стверджує: Обробка персональних даних в тій мірі, в якій це суворо необхідно та пропорційно для забезпечення мережевої та інформаційної безпеки... становить законний інтерес відповідного контролера даних. Це положення фактично дозволяє роботу SOC, але вимагає проведення LIA - документального обґрунтування того, чому інтерес безпеки переважає інтерес приватності.

Автоматизовані рішення та профілювання (Art. 22)

Стаття 22 GDPR забороняє прийняття рішень, що базуються виключно на автоматизованій обробці (включаючи профілювання), якщо вони мають юридичні наслідки. Якщо система UEBA автоматично (без участі людини) блокує обліковий запис співробітника та позбавляє його доступу до роботи на основі поведінкового балу, це може бути порушенням. Вирішення полягає в тому, щоб у контурі прийняття рішень завжди був аналітик SOC.

Нормативно-правова база України: стан війни та євроінтеграція

Українське законодавство є динамічним, адаптуючись до вимог ЄС (євроінтеграція) та реалій повномасштабної кібервійни.

Закон України Про критичну інфраструктуру (2021) та підзаконні акти

Цей Закон є рамковим документом, що визначає правовий статус КІІ. Стаття покладає на оператора КІ відповідальність за забезпечення кіберзахисту. Невиконання цієї вимоги тягне за собою юридичну відповідальність.

Постанова КМУ № 518 (від 19.06.2019) Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури прямо вимагає:

впровадження систем виявлення вторгнень (IDS/IPS), проведення аудиту подій безпеки та забезпечення безперервного моніторингу.

Закон України Про захист персональних даних

Національний закон здебільшого відповідає Конвенції 108+, але є менш деталізованим, ніж GDPR. Він не містить прямого аналога Recital 49 GDPR (про кібербезпеку як законний інтерес), що створює певну правову невизначеність. Однак, практика Уповноваженого ВРУ з прав людини вказує на те, що забезпечення безпеки (особливо національної) є легітимною метою обробки даних, за умови дотримання принципу пропорційності.

Особливості регулювання в умовах воєнного стану

Введення воєнного стану суттєво змінює баланс безпека проти приватності:

1) конституція України (Ст. 64): допускає обмеження конституційних прав (в т.ч. таємниці листування, ст. 31) в умовах воєнного стану;

2) повноваження Держспецзв'язку: під час війни роль Держспецзв'язку як регулятора посилюється. Їхні рекомендації та накази щодо моніторингу трафіку на об'єктах КІІ стають обов'язковими до виконання;

3) сенсорна мережа: держава розгортає національну систему сенсорів (на рівні провайдерів та об'єктів КІІ) для виявлення кібератак. Це означає, що метадані трафіку можуть передаватися до CERT-UA. Це створює додатковий рівень моніторингу, який є легальним, але вимагає чітких протоколів захисту цих даних від витоку.

Директива NIS2: майбутнє українського регулювання

Україна активно імплементує норми ЄС. Директива NIS2 (набула чинності в ЄС у 2023 році) стане основою для оновлення українського законодавства. NIS2 значно розширює коло суб'єктів. Вона вводить персональну відповідальність керівників за стан кібербезпеки. Це змушує топменеджмент виділяти ресурси на системи моніторингу, щоб уникнути штрафів або дискваліфікації.

Таблиця 1.8

Порівняльний аналіз регуляторних режимів моніторингу

Аспект регулювання	**Законодавство України (мирний час)**	**Реалії воєнного стану**	**Вимоги ЄС (NIS2/GDPR)**
Обов'язок моніторингу	Для банків та держорганів.	Для всіх об'єктів КІІ (жорсткий контроль).	Для широкого кола важливих суб'єктів.
Приватність комунікацій	Гарантується Конституцією.	Може бути обмежена (за рішенням військового командування/суду).	Гарантується, але з винятком для цілей безпеки.
Передача даних державі	Лише за рішенням суду.	Спрощена процедура для CERT-UA/СБУ.	Співпраця з CSIRT (обов'язкова звітність про інциденти).
Відповідальність	Адміністративна, дисциплінарна.	Кримінальна (за недбалість, що призвела до диверсії).	Співпраця з CSIRT (обов'язкова звітність про інциденти).

Судова практика: Тест Барбулеску

Для розуміння того, як норми застосовуються на практиці, критично важливим є рішення Європейського суду з прав людини (ЄСПЛ) у справі Bărbulescu в Румунії (2017). Суд сформулював критерії правомірності моніторингу, який є обов'язковим для врахування українськими судами:

1) попереднє інформування: чи був працівник ясно і завчасно повідомлений про можливість моніторингу?

2) ступінь втручання: чи був моніторинг обмеженим у часі та просторі (чи перехоплювався зміст, чи лише метадані)?

3) легітимна мета: чи надав роботодавець вагомі причини для моніторингу?

4) менш інвазивні методи: чи можна було досягти мети без прямого доступу до змісту повідомлень?

5) наслідки: чи були наслідки для працівника пропорційними?

Синтез: правовий алгоритм легалізації

Алгоритм легалізації етичного моніторингу в Україні включає наступні

кроки :

1) аудит: визначити обсяг КІІ та вимоги Постанови № 518 (чи підпадає організація під вимоги).

2) DPIA: провести оцінку впливу на захист даних для систем SIEM/DLP/UEBA.

3) внутрішня політика: розробити та затвердити Політику моніторингу та використання ІТ-ресурсів, що відповідає Тесту Барбулеску.

4) оповіщення: ознайомити кожного працівника з Політикою під підпис (електронний або фізичний).

5) контроль доступу: встановити жорсткі права доступу до логів моніторингу та забезпечити аудит дій адміністраторів.

Висновки до розділу 1

У першому розділі роботи здійснено теоретичний аналіз проблеми балансу між необхідністю жорсткого контролю критичних систем та збереженням права на приватність. За результатами проведеного дослідження зроблено такі висновки:

Проаналізовано еволюцію загроз для критичної інфраструктури. Встановлено, що в сучасних умовах традиційні пасивні методи захисту (антивіруси, фаєрволи) втратили свою ефективність. Для забезпечення тріади безпеки (конфіденційність, цілісність, доступність) критично важливим стає перехід до активної оборони - безперервного моніторингу, який дозволяє бачити загрозу в реальному часі .

Досліджено сучасний технологічний інструментарій (SIEM, SOC, UEBA) та роль штучного інтелекту в ньому. Виявлено, що технології глибокого аналізу трафіку (DPI) та поведінки користувачів (UEBA) є потужними інструментами проти кібератак, але фактично перетворюють робоче місце на цифровий паноптиком. Використання AI створює ризик того, що система може помилково звинуватити співробітника через алгоритмічну упередженість, а пояснити це

рішення буде неможливо через непрозорість нейромереж.

Визначено основні психологічні та етичні ризики тотального нагляду. Обґрунтовано, що надмірний тиск безпеки призводить до зворотного ефекту: виникає ефект заморожування, коли працівники бояться проявляти ініціативу, та феномен повзучого розширення функцій, коли інструменти безпеки починають використовувати для стеження за дисципліною чи продуктивністю . Це руйнує довіру в колективі та парадоксально знижує загальний рівень безпеки.

Встановлено наявність правової колізії в законодавстві України та ЄС. З одного боку, оператори критичної інфраструктури зобов'язані знати все, що відбувається в мережі (вимоги національної безпеки), а з іншого - повинні мінімізувати збір даних про людей (вимоги GDPR та Конституції). З’ясовано, що єдиним шляхом легалізації моніторингу є дотримання принципу пропорційності та документальне оформлення законного інтересу, навіть в умовах воєнного стану .

РОЗДІЛ 2

АНАЛІЗ ПРОБЛЕМ ТА ПІДХОДІВ ДО БАЛАНСУ МІЖ ПРИВАТНІСТЮ ТА НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ

2.1 Проблеми та дилеми етичного моніторингу

Психосоціальна дилема: ефект Цифрового Паноптикому та ерозія довіри

Фундаментальною проблемою впровадження інструментів нагляду є не стільки сам факт збору даних, скільки зміна поведінки людей коли вони знають, що за ними спостерігають.

Класичний Паноптиком, описаний Джеремі Бентамом та пізніше проаналізований Мішелем Фуко, це архітектура в’язниці, де наглядач перебуває в центральній вежі й бачить усіх в’язнів, але в’язні не бачать наглядача. Головний принцип цієї системи асиметрія видимості. Суб’єкт ніколи не знає напевно, чи дивляться на його екран саме в цю секунду, тому змушений постійно контролювати свою поведінку. Він стає наглядачем для самого себе.

У контексті сучасних кіберсистем (SIEM, DLP) ця проблема набуває нових, більш загрозливих рис. На відміну від фізичного наглядача, цифровий алгоритм не втомлюється, не відвертається і має ідеальну пам'ять. Це створює постійний фоновий стрес, який призводить до двох деструктивних психологічних ефектів.

1) Ефект охолодження

Під постійним цифровим наглядом працівники схильні до надмірного конформізму. Це явище, проявляється у відмові від реалізації своїх прав або свобод через страх санкцій.

В умовах об’єктів критичної інфраструктури це створює парадоксальний ризик для самої безпеки:

Страх помилки: Оператор системи, знаючи, що кожен його клік записується, боїться приймати нестандартні рішення в критичній ситуації,

обираючи безпечну бездіяльність замість ризикованої дії.

Замовчування проблем: Працівники уникають обговорення вразливостей або помилок керівництва в корпоративних чатах, оскільки знають, що семантичний аналіз DLP-системи може інтерпретувати критику як нелояльність.

2) Ерозія довіри та формування Тіньового IT

Довіра є економічним активом. Коли система безпеки будується на тотальній підозрі, працівники сприймають це як сигнал. Відповіддю стає симетрична недовіра до роботодавця.

Це провокує явище Тіньового IT, використання несанкціонованих програмних та апаратних засобів для виконання робочих завдань поза периметром нагляду. Інженери пересилають код на особисту пошту, щоб працювати з дому без VPN; менеджери обговорюють угоди через месенджери замість корпоративних рішень.

Результатом стає нескінченне коло перевірок безпеки: чим більше організація посилює моніторинг, тим більше процесів йдуть у тінь, стаючи невидимими для служби безпеки, що змушує керівництво впроваджувати ще жорсткіші заходи контролю.

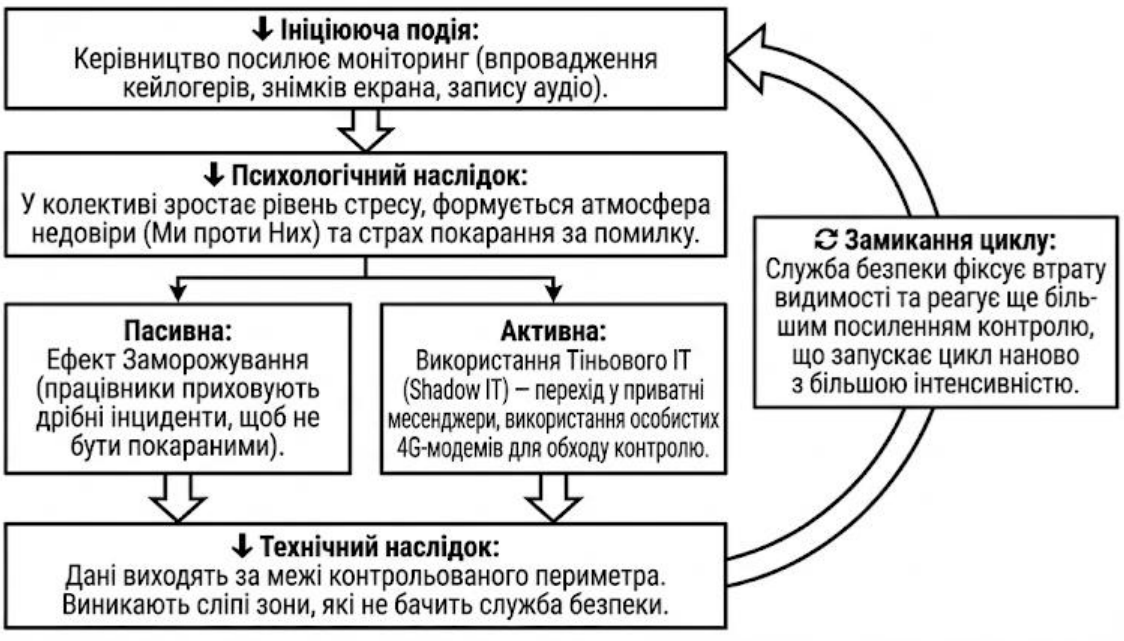

Рис.2.1. Цикл ескалації ризиків через надмірний контроль

Інформаційно-аналітична дилема: Мозаїчний ефект

Наступною критичною проблемою є ілюзія анонімності метаданих. Часто відповідні за моніторинг стверджують: Ми не читаємо ваші листи, ми лише дивимося, кому і коли ви пишете.

Це явище отримало назву Мозаїчний ефект. Його суть полягає у тому, що поєднання розрізнених, на перший погляд, безпечних фрагментів даних дозволяє реконструювати повний профіль приватного життя людини з точністю, яка часто перевищує результати прямого спостереження.

Для аналітика SOC окремі події в логах можуть виглядати як інформаційний шум, але для алгоритмів кореляції SIEM вони складаються в чіткий патерн, що розкриває чутливу інформацію.

Таблиця 2.1.

Приклад реконструкції приватного контексту через метадані

Джерело даних (метадані)	**Зафіксована подія**	**Інтерпретація системи**	**Етичний та правовий ризик**
Proxy-сервер	Доступ до сайту onco-help.org та форуму підтримки пацієнтів. Контент не перехоплено.	Інтерес до важких захворювань.	Розкриття медичної таємниці (GDPR). Дискримінація.
Геолокація (MDM)	Перебування корпоративного смартфона за адресою: вул. Ломоносова, протягом 3 годин у робочий час.	Підтвердження фізичного візиту до медзакладу.	Порушення права на приватність пересувань.
DLP-система	Зниження активності клавіатури, часті паузи, пошукові запити «кредит на лікування».	Фінансова нестабільність та емоційний стрес.	Використання вразливого стану людини.

Продовження таблиці 2.1

Джерело даних (метадані)	Зафіксована подія	Інтерпретація системи	Етичний та правовий ризик
Висновок SIEM	**Рівень ризику: 95/100.** Вирок: Співробітник є вразливим, потребує грошей, високий ризик вербування або крадіжки активів.	Система автоматично таврує людину як загрозу через її життєві обставини.	

Дилема полягає в тому, що з точки зору національної безпеки, ця інформація є критично важливою. Служба безпеки повинна знати, що співробітник, який має доступ до важливої інформації або енергомереж, став вразливим до шантажу.

Однак з точки зору прав людини, збір такої інформації без прямої згоди та санкції суду є грубим втручанням у приватність. Технології моніторингу наразі не вміють автоматично відокремлювати безпековий контекст від приватного, перетворюючи службу безпеки на небажаного свідка особистого життя співробітників.

Алгоритмічна дилема: Чорна скринька ШІ та упередженість

Еволюція засобів моніторингу від сигнатурних методів до поведінкової аналітики на основі штучного інтелекту (UEBA) породила нову проблему – алгоритмічну упередженість.

На відміну від детермінованих алгоритмів (де є чітке правило: 3 помилки пароля = блокувати), моделі машинного навчання працюють як Чорна скринька. Вони приймають рішення на основі нелінійних кореляцій мільйонів параметрів, які часто не можливо пояснити.

Проблема пояснюваності

Коли система присвоює співробітнику високий бал ризику і блокує його обліковий запис, людина має право знати причину (GDPR). Проте система часто не може видати чітку причину, окрім абстрактного відхилення від базової лінії. Це створює ситуацію презумпції вини , де працівник змушений виправдовуватися перед машиною, не розуміючи звинувачення.

Алгоритмічна упередженість

Нейромережі навчаються на історичних даних. Якщо ці дані містили соціальні упередження, модель їх вивчить і посилить.

Упередження: Якщо в компанії історично частіше звільняли або карали молодих співробітників, а помилки топменеджменту ігнорували, система навчиться, що молодий вік = високий ризик, і буде моніторити молодих спеціалістів ретельніше. Це призводить до циклу самопідтвердження: кого більше перевіряють, у того більше знаходять помилок.

Також виникає проблема Хибнопозитивних спрацювань. У кібербезпеці прийнято вважати, що краще заблокувати звичайного користувача, ніж пропустити хакера. Але коли об'єктом є жива людина, хибне звинувачення у крадіжці даних або шпигунстві завдає непоправної шкоди репутації та психіці.

Організаційна дилема: феномен Розширення функцій

Найбільш підступною проблемою, яка лежить у площині менеджменту, є розширення функцій. Це процес, коли система, впроваджена та легалізована для однієї мети (наприклад, фізична безпека), з часом починає використовуватися для інших цілей без відома та згоди суб'єктів.

В організаціях часто відбувається ерозія цільового призначення даних під тиском бізнес-потреб.

Таблиця 2.2.

Типологія розширення функцій у системах моніторингу

Інструмент моніторингу	**Легітимна заявлена мета (Кібербезпека/ Безпека)**	**Несанкціонована вторинна мета (HR / Управління/ Політики)**	**Етичний та соціальний наслідок**
DLP-система	Запобігання витоку інтелектуальної власності та комерційної таємниці.	Контроль лояльності: Аналіз резюме, надісланих працівником, пошук ознак підготовки до звільнення, виявлення профспілкових активістів.	Порушення трудової етики, тиск на працівника, перешкоджання захисту трудових прав.

Продовження таблиці 2.2

Інструмент моніторингу	**Легітимна заявлена мета (Кібербезпека/ Безпека)**	**Несанкціонована вторинна мета (HR / Управління/ Політики)**	**Етичний та соціальний наслідок**
СКУД	Фізична безпека периметра, запобігання проникненню сторонніх осіб.	Мікроменеджмент: Автоматичне вирахування із зарплати за запізнення на 2 хвилини, контроль перекурів.	Створення атмосфери «цифрової тюрми», демотивація, формалізм.
Відеоспосте-реження	Розслідування інцидентів крадіжок, контроль технологічних процесів.	Оцінка ефективності: Підрахунок часу, проведеного працівником за кавою або у розмовах з колегами.	Втручання в особистий простір, підвищення рівня стресу.
SSL-декрипція	Виявлення вірусів та C&C каналів у шифрованому трафіку.	Цензура: Блокування доступу до новинних ресурсів з певною політичною позицією.	Порушення свободи слова та доступу до інформації.

Цей феномен є найбільш руйнівним для етики, оскільки він порушує базовий принцип GDPR – Обмеження мети. Це перетворює інструменти захисту на інструменти адміністративного тиску та репресій.

Технологічна дилема: розмивання меж та проблема тунелювання

Сучасні моделі роботи (віддалена робота, гібридні офіси) та широке використання власних пристроїв фактично знищили чіткий периметр безпеки. Разом із периметром зникла і чітка межа між робочим та особистим часом і простором.

Проблема SSL/TLS

Більше 90% сучасного вебтрафіку зашифровано. Щоб виявити шкідливе ПЗ або витік даних, шлюз безпеки повинен дешифрувати трафік. Технічно це реалізується як атака Людина посередині: шлюз підміняє сертифікат сайту своїм власним, розшифровує пакет, аналізує його, зашифровує знову і відправляє користувачу.

Етичний конфлікт тут є бінарним і жорстким:

1) повна інспекція: Організація розшифровує все. Це гарантує максимальну безпеку, але означає, що адміністратор мережі має технічну можливість бачити паролі від приватного банкінгу, листування з адвокатом,

фотографії в особистій пошті. Це є кримінальним злочином, якщо не оформлено належним чином, але технічно це найпростіше рішення.

2) відсутність інспекції: Організація не розшифровує трафік. Це зберігає приватність, але створює гігантську сліпу зону, через яку зловмисники можуть виводити гігабайти даних або керувати ботнетом.

Окремою проблемою є, коли працівник використовує власний ноутбук для роботи, встановлення на нього корпоративного агента (EDR/DLP) фактично надає роботодавцю повний контроль над приватною власністю людини. Всі особисті фото, документи, історія браузера на власному пристрої стають доступними службі безпеки. Технології контейнеризації (розділення простору) існують, але вони складні в налаштуванні і часто ігноруються на користь більш простих, але інвазивних рішень.

2.2 Методи оцінки ризиків порушення приватності при моніторингу

Методологія DPIA в екосистемі SOC

DPIA (Оцінка впливу на захист даних) - це не просто бюрократична вимога GDPR, а системний процес аналізу архітектури системи безпеки на предмет її токсичності для користувачів.

Для систем моніторингу критичної інфраструктури (SIEM, UEBA, EDR) можливо зробити адаптований алгоритм проведення DPIA, який складається з чотирьох фаз.

Фаза 1: Ідентифікація тригерів

Не кожна система потребує глибокої оцінки. DPIA є обов'язковим, якщо технологія моніторингу відповідає хоча б двом критеріям:

1) систематичний моніторинг: Постійне спостереження за робочими станціями (EDR/DLP).

2) обробка чутливих даних: Можливість перехоплення медичних або фінансових даних.

3) автоматизоване прийняття рішень: Використання AI/ML для блокування користувачів (UEBA/SOAR).

4) масштабність: Обробка даних великої кількості суб'єктів.

Рис.2.2. Оцінка впливу на захист даних (DPIA)

Фаза 2: Картографування потоків даних

На цьому етапі необхідно візуалізувати, як саме дані рухаються від користувача до аналітика. Часто ризики ховаються не в самій системі, а в каналах передачі або місцях зберігання.

Таблиця 2.3.

Карта потоків даних та вразливостей приватності у SOC

Етап життєвого циклу даних	**Технічний процес**	**Приклад ризику приватності**	**Метод оцінки**
Збір	Агент EDR знімає дамп пам'яті (RAM) або скріншот.	Захоплення відкритого вікна з особистим листуванням у месенджері.	Перевірка налаштувань фільтрації .

Продовження таблиці 2.3

Етап життєвого циклу даних	Технічний процес	Приклад ризику приватності	Метод оцінки
Передача	Відправка логів на SIEM-колектор через Syslog/TLS.	Перехоплення трафіку інсайдером-адміном.	Аналіз шифрування каналу передачі.
Зберігання	Запис у гарячий індекс бази даних Elasticsearch/Splunk.	Доступ до логів мають усі аналітики L1, включно зі стажерами.	Аудит матриці доступу (RBAC).
Використання	Кореляція подій, збагачення даних через розвідку загроз.	Об'єднання професійного профілю з даними із соцмереж.	Перевірка на обмеження мети.
Знищення	Ротація логів	Логи не видаляються роками, створюючи історичний профіль на людину.	Перевірка політик ротації.

Фаза 3: Оцінка ризиків та їх наслідків

На цьому етапі застосовується матриця оцінки, де поєднуємо ймовірність негативного впливу та тяжкість наслідків для людини.

Приклад розрахунку:

1) сценарій: Повна дешифрація HTTPS-трафіку без виключень.

2) загроза: Адміністратор мережі отримує паролі до онлайн-банкінгу співробітників.

3) ймовірність: Середня (залежить від доброчесності адміна).

4) тяжкість: Критична (фінансові втрати, крадіжка особистості).

5) ризик: Високий**.** Висновок: Впровадження без додаткових заходів захисту заборонено.

Фаза 4: Інтеграція заходів мінімізації

Результатом DPIA є план дій. Якщо ризик високий, потрібно або відмовитися від технології, або модифікувати її. Наприклад, замість повної дешифрації впровадити селективну дешифрацію.

Тест Барбулеску: юридичний стандарт пропорційності

Якщо DPIA – це інженерний підхід, то Тест Барбулеску - це юридично-

етичний алгоритм, який має застосовувати кожен керівник служби безпеки (CISO) перед початком розслідування інциденту.

Цей тест базується на прецедентному рішенні Європейського суду з прав людини у справі Барбулеску в Румунії (2017). Він встановлює п'ять бар'єрів, які легітимізують втручання.

Для зручності використання у корпоративному секторі, потрібно формалізувати цей тест.

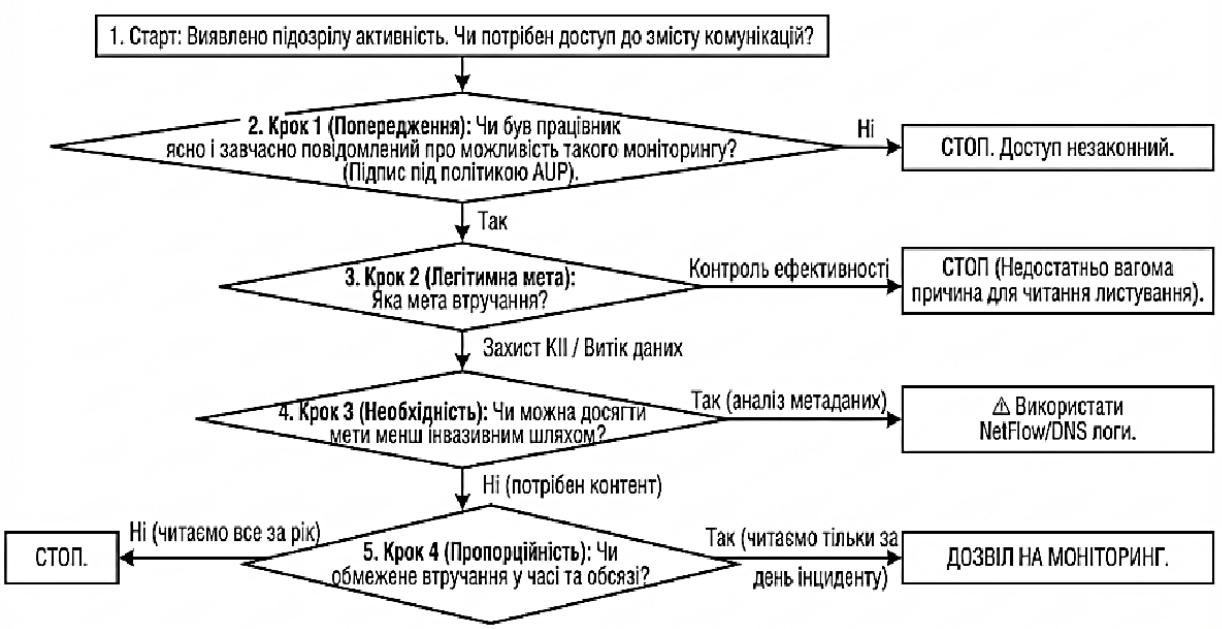

Рис.2.3. Дерево прийняття рішень

Впровадження цього алгоритму в регламент роботи SOC дозволить мінімізувати юридичні ризики та забезпечити дотримання прав людини навіть під час розслідувань.

Методологія LIA (Оцінка законного інтересу)

У трудових відносинах, особливо на об'єктах критичної інфраструктури, отримання згоди на моніторинг часто є фікцією через дисбаланс влади (працівник не може відмовити, не втративши роботу). Тому GDPR та українське законодавство вимагають спиратися на Законний інтерес.

LIA – це процедура доведення того, що інтерес компанії (захист мережі) переважає над інтересом працівника (приватність).

Тест балансу інтересів

Використовувати бальну систему оцінки для LIA.

Таблиця 2.4.

Карта оцінки законного інтересу

Фактор	**Вага**	**Оцінка ситуації (Відеоспостереження в серверній)**	**Оцінка ситуації (Приклад: Кейлогер на ПК бухгалтера)**
Важливість інтересу компанії	+1 ... +5	**+5** (Захист фізичного доступу до критичного обладнання).	**+3** (Запобігання помилкам або шахрайству).
Очікування приватності	-1 ... -5	**-1** (Серверна – це технічна зона, очікування приватності мінімальне).	**-5** (ПК використовується для особистих паролів, високе очікування приватності).
Вплив на суб'єкта	-1 ... -5	**-1** (Жодного впливу, якщо немає порушень).	**-4** (Постійний стрес, ризик витоку особистих даних).
Додаткові гарантії	+1 ... +3	**+2** (Записи доступні тільки начальнику охорони).	**0** (Дані доступні всьому IT-відділу).
РЕЗУЛЬТАТ	Сума	**+5 (Позитивний).** Моніторинг дозволено.	**-6 (Негативний).** Моніторинг заборонено.

Інженерна модель загроз приватності LINDDUN

Для глибшого технічного аналізу адаптували методологію LINDDUN, яка використовується для моделювання загроз приватності на етапі проєктування систем. LINDDUN – це акронім шести типів загроз.

Таблиця відповідності загроз LINDDUN та інструментів моніторингу, щоб показати, де саме виникають дірки у приватності.

Таблиця 2.5.

Аналіз загроз приватності у системах моніторингу (LINDDUN)

Тип загрози (LINDDUN)	**Опис у контексті моніторингу**	**Вразливий компонент системи**	**Метод протидії**
L - Linkability (Зв'язність)	Можливість зв'язати дві анонімні події (наприклад, DNS-запит та час входу в офіс) і ідентифікувати особу.	SIEM Механізм кореляції	Диференційна приватність, додавання шуму в дані.
I - Identifiability (Ідентифікованість)	Можливість дізнатися реальне ім'я користувача за його логами.	UEBA	Псевдонімізація (заміна ID).
N - Non-repudiation (Неможливість відмови)	Користувач не може заперечити, що це був він (навіть якщо його зламали).	Журнал аудиту	Багатофакторна автентифікація (MFA) для підтвердження дій.
D - Detectability (Виявлюваність)	Можливість визначити, чи належить запис конкретній особі, не знаючи її імені.	Аналіз трафіку	Агрегація даних (зберігати статистику відділу, а не особи).
D - Disclosure of information (Розкриття)	Витік зібраних логів третім особам.	Elasticsearch / Splunk DB	Шифрування даних у спокої та рольовий доступ.
U - Unawareness (Необізнаність)	Користувач не знає, що його моніторять, і поводиться приватно.	Тихий агент	Активні індикатори запису

Кількісні метрики оцінки (KPIs)

Для управління процесом необхідні кількісні показники. Пропонується ввести нові KPI для оцінки ефективності балансу:

1) DMR:

Чим вище цей показник, тим етичніша система. Якщо зібрати 1 ТБ логів, а для розслідувань використовується 1 МБ, система неефективна та інвазивна.

2) FPR у контексті персоналу:

Відсоток помилкових звинувачень співробітників у інсайдерстві. Високий FPR свідчить про низьку якість налаштування UEBA та високий рівень необґрунтованого тиску на людей.

3) TtdA:

Час, необхідний для отримання санкції на розкриття особистості. Якщо цей час дорівнює 0 (адмін бачить імена відразу) – це погано. Оптимальний час – 15-30 хвилин (час на збір Чотирьох очей для прийняття рішення).

2.3 Порівняльний аналіз практик моніторингу у державному та корпоративному секторі

Державна парадигма: імператив суверенітету та колективної безпеки

У державному секторі практика моніторингу базується на концепції суспільного договору у його найбільш жорсткій інтерпретації. Громадяни делегують державі монопольне право на нагляд та застосування сили в обмін на гарантії фізичної безпеки, стабільність конституційного ладу та захист суверенітету.

Філософія та цілепокладання

Головним пріоритетом державного моніторингу є не економічна ефективність, а виживання держави як інституції. В умовах гібридної війни, яка є перманентним станом для сучасної України, поріг толерантності до втручання у приватність суттєво знижується.

Встановлено, що державна парадигма характеризується:

1) пріоритет колективного над індивідуальним: Безпека нації важить більше, ніж таємниця листування окремої особи. Цей принцип закріплено навіть у Конституції (ст. 64), яка дозволяє обмежувати права в умовах воєнного стану.

2) нульова толерантність до ризику: Якщо в бізнесі ризик можна прийняти, якщо вартість захисту перевищує збитки, то в національній безпеці ризик теракту, диверсії на АЕС або витоку державної таємниці є неприйнятним

за будь-яку ціну.

3) презумпція обов'язку: Суб'єкт моніторингу розглядається не як найманий працівник, а як носій обов'язку. Відмова від частини прав є свідомою частиною присяги.

Інструментарій та масштаб

Державний сектор оперує інструментами, недоступними для бізнесу. Це передусім SIGINT – радіоелектронна розвідка та перехоплення трафіку на рівні магістральних каналів зв'язку

Рис.2.4. Ієрархічна модель державного моніторингу у кіберпросторі

Відмінною рисою є використання СОРМ / Законне перехоплення – апаратно-програмних комплексів, встановлених у провайдерів, які дозволяють спецслужбам отримувати доступ до трафіку конкретного абонента без відома самого провайдера.

Корпоративна парадигма: імператив прибутку та комплаєнсу

У корпоративному секторі відносини між суб'єктом та об'єктом нагляду будуються на основі цивільно-правового контракту. Головним драйвером

впровадження систем моніторингу тут є захист економічних інтересів: інтелектуальної власності, комерційної таємниці та репутації.

Філософія та цілепокладання

Бізнес прагне максимізувати прибуток. Моніторинг розглядається як інвестиція, що має окупитися. Якщо система захисту коштує дорожче, ніж потенційні збитки від крадіжки даних, бізнес від неї відмовиться.

Другим критичним фактором є відповідність вимогам. Штрафи за порушення GDPR (до 4% від річного обігу) або вимог PCI DSS можуть бути руйнівними. Тому часто бізнес впроваджує моніторинг саме для того, щоб захистити приватність клієнтів (шляхом контролю за співробітниками).

Специфіка підходу:

1) контент-орієнтованість: Якщо державу цікавлять зв'язки (хто з ким комунікує – метадані), то бізнес більше цікавить контент (що саме передається – база клієнтів, вихідний код, фінансові звіти). Тому ключовим інструментом є DLP (Запобігання втраті даних) з глибоким аналізом вмісту файлів.

2) орієнтація на продуктивність: Часто засоби безпеки (UAM – Моніторинг активності користувачів) використовуються не за призначенням, а для мікроменеджменту: скільки годин програміст писав код, а скільки дивився YouTube. Це створює специфічний етичний конфлікт, відсутній у державному секторі (де результат важливіший за процес).

3) приватність як актив: Для IT-компаній повага до приватності співробітників є частиною HR-бренду. Тотальний нагляд може призвести до відтоку талантів, що є неприпустимим економічним ризиком.

Глибокий порівняльний аналіз: «Два світи – одна технологія»

Хоча обидва сектори використовують ідентичний технологічний стек (SIEM, EDR, NGFW), логіка їх налаштування та застосування є діаметрально протилежною.

Для системного порівняння розроблено детальну аналітичну таблицю, яка структурує відмінності за шістьма ключовими вимірами.

Таблиця 2.6.

Порівняльний аналіз практик моніторингу в державному та корпоративному секторах

Критерій порівняння	Державний сектор	Корпоративний сектор
Ключовий об'єкт захисту	**Низька до приватності.** Принцип: Краще перевірити невинного, ніж пропустити терориста. Висока кількість хибних спрацювань вважається нормою.	Інтелектуальна власність, грошові потоки, клієнтська база, репутація бренду.
Толерантність до помилок	**Низька до приватності.** Принцип: Краще перевірити невинного, ніж пропустити терориста. Висока кількість хибних спрацювань вважається нормою.	**Низька до перешкод бізнесу.** Принцип: Безпека не повинна заважати бізнесу. Якщо DLP блокує легітимний контракт – це збитки.
Правова основа моніторингу	Публічне право: Конституція, Закони про нацбезпеку, КПК, Закон про КІІ. В умовах воєнного стану – накази військового командування.	Приватне право: Трудовий кодекс, NDA (угода про нерозголошення), GDPR, внутрішні політики, згода суб'єкта.
Статус Інсайдера	**Шпигун / Диверсант.** Мотивація: ідеологічна, вербування спецслужбами ворога. Дії кваліфікуються як державна зрада.	**Крадій / Конкурент.** Мотивація: фінансова нажива, перехід до конкурента, помста роботодавцю. Дії кваліфікуються як шахрайство.
Технічна глибина втручання	**Максимальна.** Використання поліграфа, перевірка родичів, доступ до банківських рахунків, негласні слідчі дії.	**Обмежена.** Лише робочі пристрої та акаунти. Доступ до особистих смартфонів або домашнього життя є табу.
Наслідки виявлення порушення	Кримінальна відповідальність, арешт, довготривале ув'язнення.	Дисциплінарне стягнення, звільнення, рідше – цивільний позов про відшкодування збитків.

Це визначає агресивність налаштувань систем моніторингу: державні системи налаштовані на параноїдальний режим, корпоративні – на збалансований.

Зона конфлікту: Критична інфраструктура (КІІ) як точка перетину

Найскладнішою зоною, де виникає найбільше етичних та правових колізій,

є об'єкти критичної інфраструктури (енергетика, транспорт, телеком, банкінг), які перебувають у приватній власності.

Тут виникає фундаментальний конфлікт інтересів:

1) держава вимагає: Встановити державні сенсори на технологічній мережі (ОТ) та передавати сирі дані до CERT-UA або НКЦК для виявлення атак рівня APT.

2) бізнес опирається: Передача телеметрії може розкрити комерційні таємниці (обсяги генерації, клієнтські транзакції). Крім того, бізнес побоюється, що державні органи можуть використати ці дані для тиску (рейдерства).

3) працівник КІІ: Опиняється під подвійним пресом. З одного боку, він підписав корпоративний NDA. З іншого боку, його дії (помилка при перемиканні рубильника) можуть трактуватися СБУ як диверсія, що вимагає тотального контролю його дій, аж до прослуховування телефону.

Приклад колізії: Системний адміністратор приватного банку.

1) Корпоративна логіка: Його дії моніторяться DLP-системою для запобігання крадіжці бази клієнтів.

2) Державна логіка: Банк є об'єктом КІІ. Дії адміністратора моніторяться на предмет встановлення закладок для російських спецслужб.

3) Результат: Адміністратор перебуває під перехресним моніторингом, який часто дублюється і не узгоджується між собою.

Вплив воєнного стану на конвергенцію практик

Особливістю українського контексту є фактор повномасштабної війни. В умовах воєнного стану відбувається процес сек'юритизації корпоративного сектору. Межа між бізнесом і державою стирається.

Спостерігаються такі тенденції:

1) імперативна передача даних: Відповідно до рішень РНБО та наказів Держспецзв'язку, приватні провайдери та оператори мобільного зв'язку зобов'язані надавати доступ до метаданих трафіку для виявлення ворожої активності. Питання приватності користувачів при цьому відходить на другий план перед загрозою фізичного знищення.

2) феномен «Цифрового волонтерства»: Приватні IT-фахівці використовують корпоративні ресурси (сервери, канали зв'язку) для атак на інфраструктуру ворога (DDoS, OSINT). Це створює нову етичну дилему: чи має право роботодавець моніторити та забороняти таку діяльність, яка формально є порушенням політики компанії, але патріотично вмотивована?

3) мілітаризація інструментів: Корпоративний сектор починає закуповувати та використовувати інструментів військового рівня (системи Криміналістичного-аналізу мобільних пристроїв), які раніше були прерогативою поліції, для проведення внутрішніх розслідувань.

Висновки до Розділу 2

У другому розділі кваліфікаційної роботи проведено комплексний аналіз проблематики практичної реалізації моніторингу в інформаційно-телекомунікаційних системах та методів оцінки супутніх ризиків. За результатами дослідження зроблено наступні висновки:

Проаналізовано ключові дилеми етичного моніторингу. Встановлено, що впровадження тотального нагляду створює ефект «Цифрового Паноптикому», що призводить до негативних психосоціальних наслідків: ефекту охолодження та формування Тіньового IT, що парадоксально знижує загальний рівень безпеки організації. Виявлено технічні ризики, зокрема мозаїчний ефект (де-анонімізація через агрегацію метаданих) та проблему «чорної скриньки» в алгоритмах штучного інтелекту, що може призводити до упередженості рішень.

Систематизовано методи оцінки ризиків порушення приватності. Обґрунтовано доцільність застосування адаптованої методології DPIA для превентивного аналізу архітектури систем безпеки. Визначено, що для юридичної легітимізації розслідувань інцидентів необхідне застосування Тесту Барбулеску та процедури LIA. Для моделювання технічних загроз приватності адаптовано модель LINDDUN.

Здійснено порівняльний аналіз практик моніторингу в державному та

корпоративному секторах. Визначено фундаментальну розбіжність у підходах: державний сектор орієнтований на модель нульової толерантності до ризиків та пріоритет колективної безпеки, тоді як корпоративний сектор керується економічною доцільністю та вимогами комплаєнсу .

Встановлено, що об’єкти критичної інфраструктури є зоною конфлікту інтересів, де працівники підпадають під подвійний тиск корпоративних політик та державних вимог. З’ясовано, що в умовах воєнного стану відбувається процес «сек'юритизації» приватного сектору, що вимагає впровадження гібридних моделей моніторингу, здатних інтегрувати державну глибину аналізу загроз із корпоративними стандартами захисту прав людини.

Результати аналізу, проведеного у другому розділі, доводять неможливість вирішення конфлікту між безпекою та приватністю виключно адміністративними методами. Це обумовлює необхідність розробки технічної моделі системи етичного моніторингу, що буде реалізовано у третьому розділі роботи.

РОЗДІЛ 3
РОЗРОБКА ЕТИЧНОЇ СИСТЕМИ МОНІТОРИНГУ

3.1 Постановка завдань та принципи етичного моніторингу

Формулювання науково-технічної задачі: перехід до Вибіркової видимості

Головна інженерна проблема, яку необхідно вирішити в рамках розробки, полягає у зміні базового принципу нагляду.

Проблема: Існуючі системи працюють за принципом прозорого акваріума: адміністратор безпеки має технічну можливість бачити будь-яку дію користувача. Це створює ефект Паноптикому і покладає всю відповідальність за етичність на совість адміністратора.

Завдання**:** Спроєктувати систему за принципом Одностороннього дзеркала з керованим затемненням. Система повинна бути сліпою до приватного життя користувача за замовчуванням, але миттєво ставати прозорою при виявленні ознак реальної кібератаки.

Формулюється концепцію Вибіркової видимості, яка базується на трьох аксіомах:

1) контекст визначає доступ: Рівень моніторингу залежить не від посади працівника, а від контексту його дій (які програми він використовує, до яких даних звертається).

2) анонімність до моменту провини: Ідентичність користувача прихована від аналітика доти, доки алгоритм не підтвердить наявність інциденту з високою ймовірністю.

3) неможливість непомітного нагляду: Будь-яке розкриття приватної інформації має залишати незмивний цифровий слід.

Етичний фреймворк: Чотири стовпи архітектури

Для переведення філософії Приватність за замовчуванням у площину

технічних вимог, потрібені етичні фреймворк системи, що складається з чотирьох фундаментальних принципів.

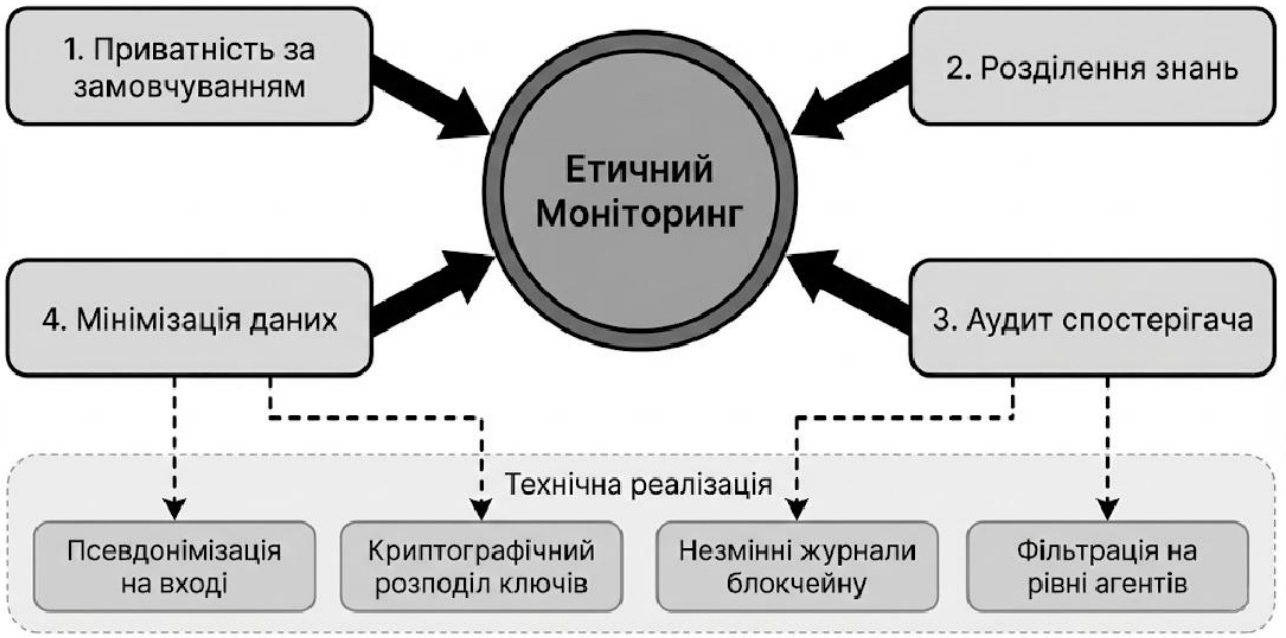

Рис.3.1. Архітектурні принципи Етичного SOC

Деталізація принципів:

1) приватність за замовчуванням:

Система налаштована на максимальну приватність з коробки. Якщо користувач не давав згоди на запис особистих чатів, система технічно не може їх записати, навіть якщо адміністратор спробує увімкнути цю функцію (функція заблокована на рівні ядра).

2) розділення знань:

Впровадження принципу: Правило двох ключів. Жодна посадова особа в організації - CISO, IT-директор, CEO - не повинна мати технічної можливості одноосібно переглядати повну історію дій конкретного працівника.

a. Аналітик бачить загрозу, але не бачить імені.

b. HR знає ім'я, але не бачить технічних логів.

c. Тільки їхня спільна авторизація дозволяє поєднати ці дані.

3) аудит спостерігача:

Вирішення проблеми Хто стереже вартових. Дії адміністраторів безпеки є найбільш критичними для приватності. Тому система повинна вести окремий, захищений журнал аудиту, до якого адміністратори не мають прав на видалення.

4) мінімізація даних:

Замість принципу збирати усе, потім розбиратися, застосовувати принцип, збираються лише ті телеметричні дані, які необхідні для детектування атаки (TTPs за MITRE ATT&CK), а не весь цифровий слід людини.

Функціональні вимоги до системи

На основі сформульованих принципів розроблено матрицю функціональних вимог до системи. Ці вимоги є основою для вибору програмного забезпечення або розробки власних модулів.

Таблиця 3.1.

Матриця функціональних вимог до системи Етичного SOC

ID	Функціональна група	Опис вимоги	Етичне обґрунтування
FR-01	Збір даних	Система повинна підтримувати чорні списки додатків та URL (наприклад, банкінг, здоров'я), дані з яких не збираються агентом на рівні кінцевої точки.	Запобігання випадковому збору чутливих даних (PII/PHI), навіть якщо трафік зашифрований.
FR-02	Знеособлення	Усі ідентифікатори користувачів (Login, IP, Email, Hostname) повинні замінюватися на криптографічний хеш до моменту запису в базу даних SIEM.	Захист від упередженості аналітика та випадкового розкриття особистості при перегляді логів.
FR-03	Вибіркова дешифрація (Робота з SSL)	Шлюз безпеки повинен підтримувати категоризацію веб-ресурсів і автоматично вимикати SSL-інспекцію для особливих данних (фінанси, право, медицина).	Збереження таємниці листування та банківської таємниці.
FR-04	Реагування на основі оцінки ризиків (Адаптивність)	Агресивні методи моніторингу (скріншоти, кейлогер) повинні активуватися автоматично і тимчасово лише при досягненні великого рівня ризику.	Дотримання принципу пропорційності: суворі заходи лише для суворих загроз.

Продовження таблиці 3.1

ID	Функціональна група	Опис вимоги	Етичне обґрунтування
FR-05	Доступ з подвійним контролем (Доступ)	Модуль деанонімізації (перетворення хешу в ПІБ) повинен вимагати підтвердження від двох ролей.	Унеможливлення зловживання владою та несанкціонованого стеження.
FR-06	Прозорий інтерфейс користувача (Прозорість)	Агент на робочій станції повинен мати візуальний індикатор, який змінює колір/іконку залежно від активності режиму запису.	Реалізація права суб'єкта знати про факт спостереження.

Нефункціональні вимоги: надійність та захищеність

Крім того, що система робить, важливо, як вона це робить. Етична система має бути надійною, інакше витік зібраних даних стане катастрофою для приватності.

1) Незмінність: Журнали доступу до системи (хто і коли шукав інформацію про співробітника) повинні зберігатися на незмінних носіях або в блокчейні.

2) Життєвий цикл: Автоматичне видалення детальних (сирих) даних через 30–90 днів. Статистичні дані можуть зберігатися до року.

3) Продуктивність: Процеси псевдонімізації та фільтрації не повинні створювати затримку більше 100 мс, щоб не заважати роботі користувача.

Операційна модель: Концепція Скляного дому

Запропонована система змінює філософію роботи SOC. Замість моделі Чорної скриньки, де рішення про блокування приймаються непрозоро, пропонується модель Скляного дому.

Це означає технічну реалізацію концепції Гранулярної згоди(самостійно обирати які данні компанія може збирати). Замість бінарного вибору (дозволити або заборонити все), простір моніторингу розділяється на зони.

Таблиця 3.2.

Зонування цифрового простору в Етичному SOC

Зона	Тип ресурсів	Рівень доступу системи	Дії при інциденті
Зелена (Корпоративна)	Корпоративна пошта, CRM, ERP, файлові сервери.	Повний контроль. Запис контенту, метаданих, дій.	Автоматичне блокування, повне розслідування.
Жовта (Публічна)	Новинні сайти, освітні ресурси.	Тільки метадані. Час, URL, тривалість. Контент не аналізується.	Аналіз аномалій (8 годин на YouTube), попередження користувачу.
Червона (Приватна)	Приватний банкінг, портали здоров'я, особиста пошта, держпослуги.	Дані ігноруються агентом. SSL-тунель не розкривається.	Втручання неможливе, крім випадків виявлення сигнатури відомого вірусу в зашифрованому потоці.

Критерії ефективності системи

Як зрозуміти, що побудована система працює ефективно. Для цього потрібно ввести набір метрик (KPIs), які оцінять не лише безпеку, а й етичність.

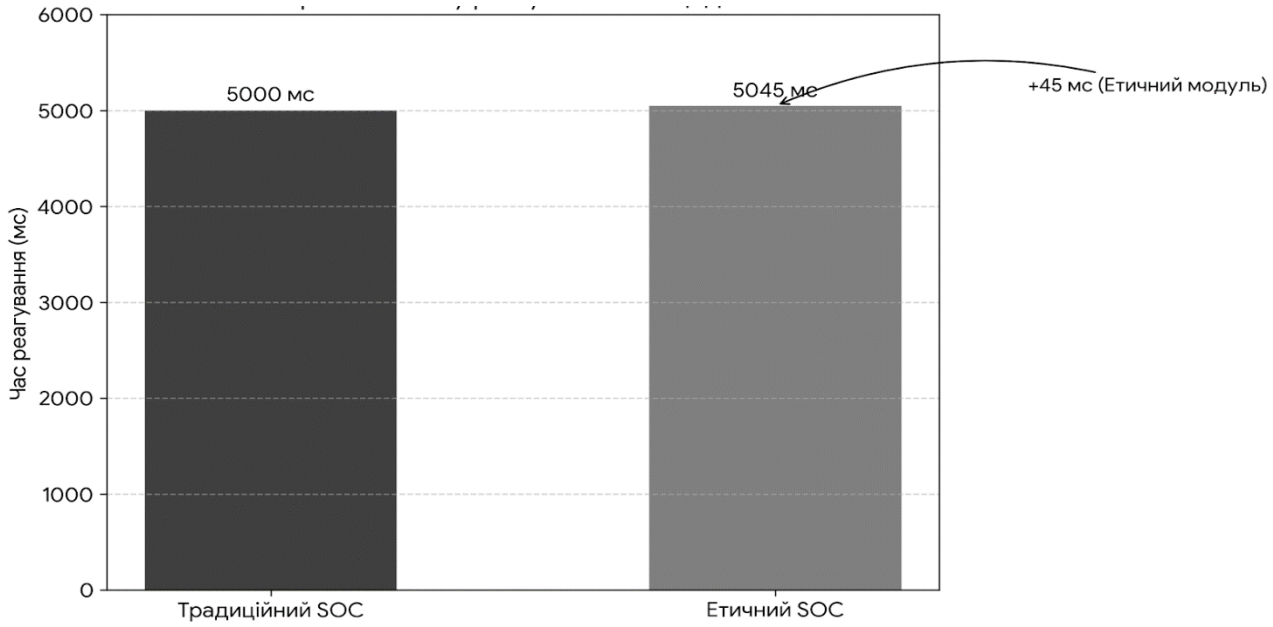

Рис.3.2.Порівняння часу реагування на інциденти

Таблиця 3.3.

Критерії оцінки ефективності Етичного SOC

Показник	**Традиційна мета**	**Етична мета**	**Формула розрахунку / Індикатор**
Середній час виявлення	Мінімізувати (< 10 хв)	Зберегти на рівні традиційного (< 15 хв)	Час від початку атаки до створення алерту в SIEM.
Хибні спрацьовування	Допустимо високий	Мінімізувати	Кількість помилкових звинувачень співробітників у порушеннях.
Витік даних	Не вимірюється	Мінімізувати (наближати до 0)	Обсяг приватних даних (PII), доступних аналітику L1.
Витік даних	Низька (Безпека через приховування)	Висока	Відсоток співробітників, які розуміють, які саме дані про них збираються.

3.2 Модель системи моніторингу з урахуванням етичних принципів та захисту персональних даних

Розробка дієвої системи етичного моніторингу вимагає переходу від абстрактних принципів приватність за замовчуванням до конкретних інженерних рішень. У цьому підрозділі представлено авторську архітектурну модель E-SOC.

Головна концептуальна відмінність запропонованої моделі від традиційних рішень полягає у зміні вектору обробки даних. Традиційна модель працює за схемою Збір → Зберігання → Аналіз, де питання приватності вирішуються вже на етапі аналізу. Запропонована модель впроваджує проміжний, бар'єрний шар - Шлюз Приватності, який виконує функцію інтелектуальної мембрани, фільтруючи та знеособлюючи дані до моменту їх запису в систему.

Багаторівнева архітектура системи

Для забезпечення балансу між функціональністю безпеки та захистом

даних, архітектуру системи було розділено на чотири логічні рівні. Кожен рівень має чітко визначену зону відповідальності та правила обробки інформації.

Рівнів архітектури:

Рівень 1. Сенсорний рівень

Це очі та вуха системи. Сюди входять агенти EDR на робочих станціях, мережеві аналізатори та збирачі логів з серверів.

Особливість етичної моделі: Агенти налаштовані в режимі обмеженої довіри. Вони мають локальні конфігураційні файли, які забороняють збір даних з певних процесів (банківських клієнтів) ще на етапі генерації події.

Рівень 2. Шлюз приватності

Ключовий інноваційний компонент моделі. Це проміжний сервер або кластер серверів, через який проходять усі сирі логи.

Функції:

1) санітизація: Видалення випадково перехоплених чутливих даних (номерів кредитних карток) за допомогою регулярних виразів.

2) псевдонімізація**:** Заміна ідентифікаторів користувачів на криптографічні токени.

3) категоризація**:** Розмітка подій тегами Публічне, Приватне, Корпоративне.

Рівень 3. Аналітичне ядро

Сюди потрапляють вже очищені та знеособлені дані.

Процес: Аналітики та алгоритми UEBA працюють з анонімними сутностями (User_Hash_A1). Система виявляє аномалії та атаки, не знаючи реальних імен.

Рівень 4. Рівень управління ідентичністю

Це ізольоване, захищене сховище, де зберігаються ключі шифрування та таблиці відповідності хешів реальним іменам. Доступ до цього рівня суворо регламентований процедурою мультипідпису.

Алгоритм обробки даних: механізм динамічної псевдонімізації

Центральним елементом захисту приватності в моделі є алгоритм

перетворення ідентифікаторів (PII). Просте видалення імен неможливе, оскільки це унеможливить кореляцію подій (ми не зможемо зв'язати вхід у систему і завантаження файлу).

Тому в моделі застосовано метод динамічного хешування з сіллю.

Математична модель перетворення:

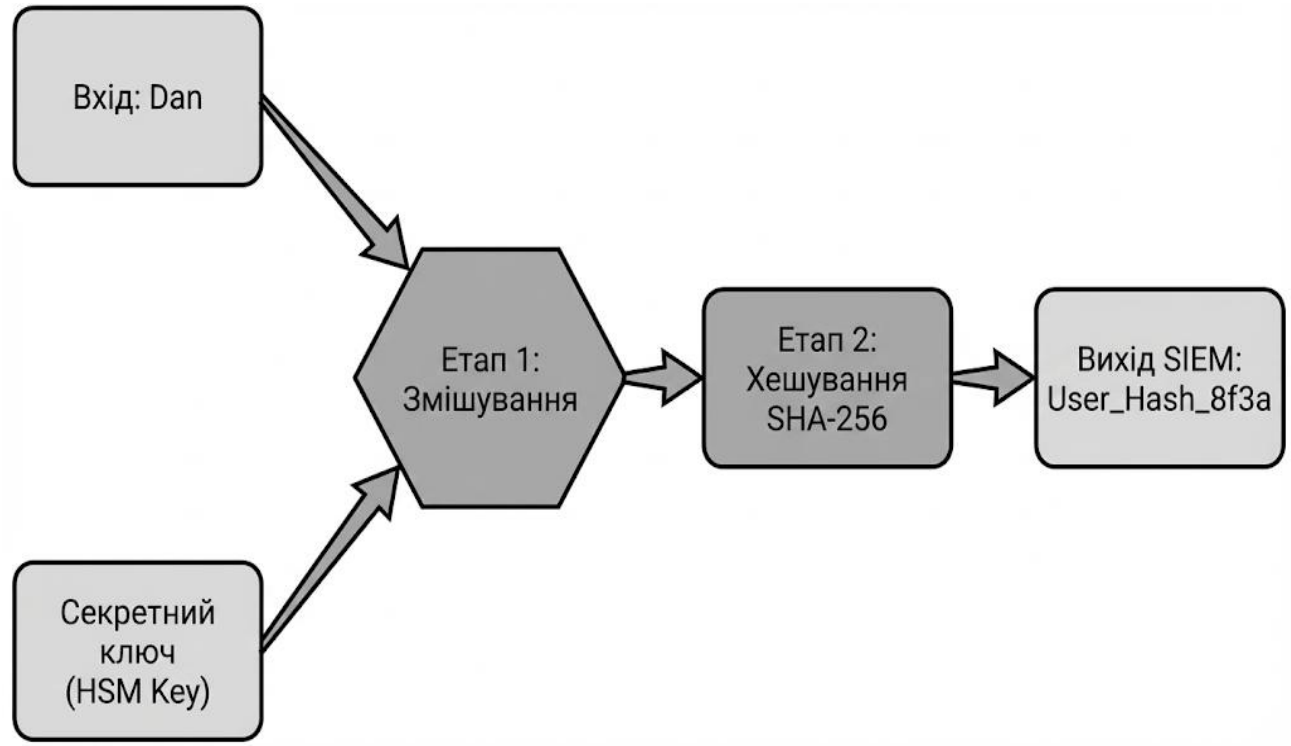

Рис.3.3. Потік даних при псевдонімізації

Такий підхід забезпечує виконання вимоги GDPR щодо мінімізації даних. Аналітик бачить, що користувач 8f3a... здійснив підозрілу дію, але не може використати це знання для особистих цілей (переслідування колеги), оскільки не знає, хто ховається за хешем.

Контекстна фільтрація трафіку

Однією з найбільших технічних та етичних проблем є аналіз зашифрованого вебтрафіку (HTTPS). Повна дешифрація є еквівалентом читання паперових листів і є неприпустимою для певних категорій .

У розробленій моделі запропоновано механізм селективної інспекції, який

базується на категоризації ресурсів у реальному часі. На рівні шлюзу безпеки (NGFW) налаштовується матриця правил, що визначає глибину втручання.

Таблиця 3.4

Матриця правил контекстної обробки трафіку в системі E-SOC

Категорія ресурсу	**Приклади URL**	**Рівень довіри**	**Дія системи**	**Етичне обґрунтування**
Фінанси та Банкінг	privat24.ua, monobank.ua, paypal.com	Високий	Пропуск. Трафік не дешифрується. Логується тільки факт з'єднання (IP).	Захист банківської таємниці та фінансових даних працівника. Ризик впровадження шкідливого коду через банківські сайти мінімальний.
Медицина та Здоров'я	helsi.me, synevo.ua, сайти клінік	Високий	Пропуск	Захист медичної таємниці.
Державні послуги	diia.gov.ua, податкова	Високий	Пропуск	Захист персональних даних громадянина.
Соціальні мережі та Особиста пошта	facebook.com, gmail.com (personal)	Середній	Тільки метаданні. Дешифрація заголовків для контролю вірусів, але без запису контенту повідомлень.	Баланс між контролем робочого часу та таємницею листування.
Корпоративні ресурси	salesforce, office365 (corp account)	Довірений	Повна інспекція. Повний запис та аналіз контенту.	Дані належать компанії. Необхідний захист від витоку.
Невідомі / Ризикові	unknown-site.xyz, tor-exit-node	Низький	Пова інспекція + Блокування. Дешифрація, пісочниця, блокування.	Високий ризик кібератаки. Пріоритет безпеки.

Протокол деанонімізації: Принцип чотирьох очей

Система захисту не може бути абсолютно анонімною, інакше розслідування інцидентів стане неможливим. Однак процес розкриття особистості має бути суворо регламентованим, щоб уникнути зловживань

владою.

У моделі реалізовано протокол Чотирьох очей, який технічно унеможливлює одноосібне рішення про деанонімізацію.

Алгоритм роботи протоколу:

1) детектування: SIEM виявляє критичний інцидент, пов'язаний з User_Hash_X.

2) запит: Аналітик SOC ініціює в системі тікет Запит на деанонімізацію, додаючи докази (скріншоти аномалії, логи).

3) затвердження (Key A): Керівник SOC (CISO) перевіряє технічну обґрунтованість запиту і накладає свій цифровий підпис.

4) легалізація (Key B): Офіцер із захисту даних (DPO) або представник HR перевіряє юридичну обґрунтованість (чи відповідає це політиці компанії) і накладає другий підпис.

5) виконання: Тільки за наявності двох валідних ключів система звертається до Сховища ідентичності і повертає аналітику реальне ім'я.

Цей механізм трансформує деанонімізацію з рутинної дії (подивитися, хто це) у документовану юридичну процедуру.

Рольова модель доступу (RBAC) та матриця повноважень

Для технічної реалізації описаних процесів розроблено рольову модель доступу. Вона чітко розмежовує, хто і що може бачити в системі моніторингу.

Таблиця 3.5.

Матриця доступу до даних моніторингу в моделі E-SOC

Роль у системі	**Рівень доступу до "сирих" даних**	**Видимість імен (PII)**	**Право на деанонімізацію**	**Доступ до журналів аудиту**
L1 Аналітик SOC (Черговий)	Обмежений. Бачить лише алерти та агреговані графіки.	Приховано. Бачить тільки хеші (Hash_X).	Ні. Може лише ескалювати інцидент.	Ні.

Продовження таблиці 3.5

Роль у системі	**Рівень доступу до "сирих" даних**	**Видимість імен (PII)**	**Право на деанонімізацію**	**Доступ до журналів аудиту**
L2/L3 Аналітик (Розслідувач)	Повний (в межах інциденту). Бачить детальні логи.	Приховано. Бачить хеші.	Ініціатор. Може подати запит.	Ні.
CISO (Керівник ІБ)	Повний.	Приховано	Затверджувач (Ключ А).	Тільки читання.
DPO (Юрист / Комплаєнс)	Ні. Не має доступу до технічних логів.	Ні.	Затверджувач (Ключ В).	Повний контроль. Може бачити всі дії CISO та аналітиків.
SysAdmin (Інженер системи)	Технічний. Бачить стан серверів, але не дані.	Ні. Дані зашифровані ключем, який адмін немає.	Ні	Ні

Захист журналів аудиту

Останнім, але критично важливим елементом моделі є забезпечення невідворотності відповідальності для самих наглядачів. Система повинна реалізувати концепцію Спостереження за спостерігачами.

Для цього всі дії адміністраторів та аналітиків (пошукові запити, перегляди екранів, запити на деанонімізацію) записуються в окремий журнал аудиту.

Технологічна реалізація:

1) WORM-сховище: Логи пишуться на носій, який на апаратному рівні забороняє перезапис або видалення даних протягом визначеного періоду (3 роки).

2) Blockchain-hashing**:** Кожен запис у журналі хешується разом із попереднім, утворюючи нерозривний ланцюжок. Будь-яка спроба видалити запис про несанкціонований перегляд даних призведе до порушення цілісності всього ланцюжка, що буде миттєво виявлено системою моніторингу цілісності (FIM).

Резюме підрозділу

Представлена модель E-SOC вирішує фундаментальну проблему етичного моніторингу шляхом впровадження технічних обмежень замість адміністративних.

- Шлюз приватності та псевдонімізація захищають користувача від

масового нагляду.

- Селективна інспекція гарантує збереження особистих таємниць навіть при роботі з корпоративної мережі.
- Протокол Чотирьох очей та незмінні логи захищають систему від зловживань з боку адміністраторів.

Така архітектура дозволяє досягти мети роботи: побудувати систему, яка є ефективною проти кіберзагроз, але безпечною для прав людини. Наступним кроком є розробка практичних рекомендацій щодо впровадження цієї моделі в реальні бізнес-процеси.

3.3 Розробка рекомендацій щодо впровадження етичного моніторингу

Розробка архітектурної моделі E-SOC є необхідною, але недостатньою умовою для успішної реалізації етичного моніторингу. Світова практика показує, що найскладніші ризики таких проєктів лежать не в площині технологій, а в площині організаційних процесів, правового оформлення та корпоративної культури. Без належного впровадження навіть найбільш досконала система SIEM може перетворитися на інструмент репресій або, навпаки, стати мертвим вантажем, який ігнорується персоналом.

У цьому підрозділі сформульовано комплекс практичних рекомендацій для керівників служб інформаційної безпеки (CISO) та менеджменту підприємств КІІ щодо імплементації запропонованої моделі. Рекомендації структуровано за трьома критичними векторами: організаційно-правовий, технічний та соціально-комунікаційний.

Організаційно-правовий вектор: перехід від сірої зони до прозорих правил

Фундаментом етичного моніторингу є юридична визначеність. Потрібно відмовитися від стандартної практики використання розмитих формулювань у трудових договорах (Компанія залишає за собою право моніторити використання обладнання) на користь створення деталізованої нормативної бази.

Рекомендація 1. Впровадження концепції Зонування цифрового простору

У внутрішніх нормативних документах (Політика інформаційної безпеки, Положення про моніторинг) необхідно чітко зафіксувати поділ цифрової активності на зони відповідальності. Це дозволяє працівнику чітко розуміти межі своєї приватності.

Рекомендація 2. Інституціоналізація етичного контролю

Для вирішення спірних питань, які неминуче виникають у Жовтій зоні (чи можна деанонімізувати працівника, якщо він не вкрав дані, але порушив корпоративну етику), одноосібного рішення CISO недостатньо.

Рекомендується створення постійно діючого колегіального органу - Комітету з етики даних**.**

Склад:

1) директор з інформаційної безпеки (CISO) - технічна експертиза.
2) офіцер із захисту даних (DPO) або Юрист - правова експертиза.
3) HR-директор - кадрова експертиза.
4) представник трудового колективу (Профспілка) - захист прав працівників.

Функція: Санкціонування доступу до даних при складних розслідуваннях та розгляд апеляцій працівників щодо неправомірного моніторингу.

Рекомендація 3. Оновлення процедури Прийому на роботу

Процес ознайомлення з правилами моніторингу має змінитися з формального підписання пачки паперів на Активне інформування.

Дія: Замість дрібного шрифту в договорі, новому співробітнику надається Односторінкова пам'ятка з інфографікою: Що видно, а що - ні.

Мета: Зняти страх перед невидимим наглядачем з першого дня роботи.

Технічний вектор: налаштування Шлюзу приватності

На етапі технічного впровадження критично важливо правильно конфігурувати інструменти захисту, щоб вони відповідали заявленим політикам. Розбіжність між тим, що написано в політиці (ми не читаємо особисту пошту), і тим, що налаштовано на сервері (повна дешифрація всього), є головним ризиком

для репутації.

Рекомендація 4. Тонке налаштування SSL/TLS Inspection

Необхідно налаштувати шлюз безпеки (NGFW) на роботу з динамічними списками категорій URL.

Алгоритм налаштування:

1) активація URL Filtering: Увімкнути ліцензію на категоризацію веб-ресурсів.

2) створення політики Bypass: Створити правило Не розшифровувати для категорій: Фінансові послуги, Охорона здоров'я та медицина, Юридична сфера, Державні дані, персональний контент.

3) обробка виключень: Для сайтів, які не мають категорії, налаштувати правило Дешифрувати, але не зберігати контент, щоб перевірити на віруси, але не записувати дані користувача.

4) регулярний аудит: Раз на квартал проводити перевірку категорій, щоб переконатися, що нові критичні ресурси (наприклад, новий портал електронної черги до лікаря) потрапляють у вірну категорію.

Рекомендація 5. Реалізація життєвого циклу даних

Дані моніторингу є токсичним активом - чим довше вони зберігаються, тим вищий ризик їх витоку та зловживання. Рекомендується налаштувати автоматичну ротацію логів у SIEM-системі.

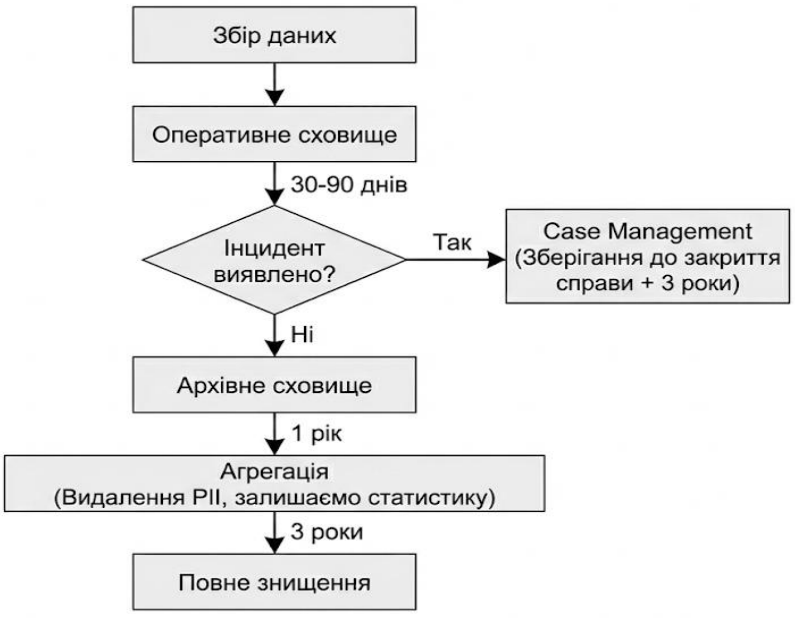

Рис.3.4. Життєвий цикл даних моніторингу в системі E-SOC

Для реалізації принципу Auditability (підзвітності адміністраторів) необхідно забезпечити технічну неможливість зачистки слідів.

Дія: Налаштувати пересилку логів дій адміністраторів на зовнішній сервер Syslog або в хмарне сховище (AWS S3 / Azure Blob) з увімкненою функцією Object Lock (WORM). Це гарантує, що навіть маючи права root, зловмисник не зможе видалити запис про свій вхід.

Соціально-комунікаційний вектор: подолання опору змінам

Найскладнішим завданням є зміна ставлення персоналу до моніторингу. Необхідно змінити наратив з “Ми стежимо за вами, щоб покарати” на “Ми захищаємо систему, частиною якої є ви”.

Рекомендація 6. Впровадження активної прозорості

Психологічний дискомфорт виникає від невизначеності. Рекомендується використовувати програмні агенти, які візуалізують стан моніторингу для користувача.

Технічна реалізація:

У системному треї має бути іконка агента безпеки, яка змінює стан:

1) зелений колір: Режим пасивної оборони. Система працює як антивірус. Екран не записується. Приватність - 100%.

2) червоний колір: Увага! Режим запису. Активується, коли користувач відкриває критичні корпоративні додатки (SAP, Admin Panel). Це попереджає користувача, що він знаходиться в Зеленій зоні, і повертає йому відчуття контролю.

Рекомендація 7. Підштовхування

Використовувати дані моніторингу не для репресій, а для навчання в моменті.

Сценарій: Система DLP фіксує спробу відправки файлу з персональними даними на зовнішню пошту.

Традиційна реакція: Блокування + Доповідна керівнику.

Етична реакція: Користувач отримує спливаюче вікно: Схоже, ви намагаєтесь відправити документ, що містить Персональні данні. Це безпечно?

Нагадуємо, що для обміну з партнерами краще використати захищений SharePoint. [Відправити через SharePoint] / [Я впевнений, відправити поштою].

Такий підхід виховує культуру безпеки, не створюючи конфлікту.

Дорожня карта впровадження

Для систематизації процесу трансформації існуючого SOC в E-SOC розроблено покрокову дорожню карту. Вона розрахована на типове підприємство КІІ і займає орієнтовно 3–6 місяців.

Таблиця 3.7.

Дорожня карта впровадження системи етичного моніторингу

Етап	Ключові заходи	Тривалість	Відповідальний	Результат
1.Аудит	Інвентаризація активів та потоків даних. Класифікація ресурсів на зони (Green/Red). Інтерв'ю з HR та Юристами.	2-4 тижні	CISO, IT Dept	Карта потоків даних. Проєкт Політики зонування.
2. Легалізація	Проведення DPIA. Затвердження нової Політики моніторингу. Оновлення трудових договорів (додаткові угоди). Створення Етичного комітету.	4 тижні	DPO, HR, Legal	Підписані згоди персоналу. Протоколи LIA та DPIA.
3. Технічне налаштування	Налаштування SSL Bypass на шлюзах. Впровадження модуля псевдонімізації в SIEM. Налаштування рольового доступу (RBAC).	4-8 тижнів	SOC Engineers, Vendors	Працюючий прототип системи (MVP).
4. Пілот	Запуск системи на тестовій групі (IT-відділ + Бухгалтерія). Калібрування хибних спрацювань.	4 тижні	SOC Analysts	Відлагоджені правила кореляції. Звіт про пілот.
5. Комунікація	Тренінги для персоналу. Розсилка пам'яток. Пояснення принципу Вибіркової видимості на загальних зборах.	2 тижні	CISO, HR	Зниження рівня тривожності та опору змінам.
6. Повний запуск	Активація системи для всієї організації. Включення механізму ротації ключів.	-	CISO	Функціонуюча система E-SOC в режимі Production.

3.4 Апробація системи на умовному кейсі

Мета та методологія експерименту

Мета: Порівняльний аналіз ефективності двох архітектурних підходів до побудови SOC - традиційного та розробленого етичного.

Гіпотеза дослідження: Впровадження механізмів псевдонімізації та селективної інспекції трафіку не призводить до критичного збільшення часу реагування на інциденти (MTTD/MTTR), проте забезпечує зниження ризиків порушення приватності на понад 90%.

Методологія:

Експеримент проводився за сценарієм A/B тестування.

- Сценарій А (Контрольна група): Типова конфігурація SIEM та DLP, де адміністратор має повний доступ до даних.
- Сценарій В (Експерементальна група): Конфігурація E-SOC з модулем Шлюз приватності та рольовим доступом.

Через обидві системи було пропущено ідентичний набір даних, що містив суміш легітимної робочої активності, приватної активності користувача та ознак кібератаки.

Опис тестового середовища

Для проведення експерименту було розгорнуто віртуалізований полігон із наступною топологією:

1) сегмент користувача:

a. віртуальна машина: Windows 10 Enterprise.

b. програмне забезпечення: MS Office, Web Browser, Telegram Desktop.

c. агент моніторингу: Wazuh Agent (Open Source EDR).

2) сегмент атаки:

a. інструментарій: Atomic Red Team (бібліотека тестів на основі MITRE ATT&CK).

b. C2 Server: Kali Linux для емуляції зовнішнього управління.

3) сегмент захисту:

a. шлюз безпеки: pfsense з налаштованим модулем Squid Proxy.

b. SIEM-система: ELK Stack (Elasticsearch, Logstash, Kibana).

c. модуль етичності: Спеціально написаний Python-скрипт на стороні Logstash, який виконує хешування полів user.name та source.ip перед індексацією.

Схема 3.7. Топологія лабораторного стенда

Легенда сценарію:

Об'єкт спостереження - умовний співробітник відділу продажів (User ID: o.ABc). Він має доступ до конфіденційних даних клієнтів, але, як і більшість людей, іноді вирішує особисті питання в робочий час.

Фабула інциденту: Зловмисники здійснюють цільову фішингову атаку, використовуючи тему, чутливу для користувача, щоб змусити його завантажити шкідливе ПЗ.

Хід експерименту: Покроковий порівняльний аналіз

Експеримент складався з чотирьох хронологічних етапів. На кожному етапі фіксувалося, що саме бачить оператор безпеки в обох системах.

ЕТАП 1. Легітимна приватна активність

Час події: 09:15 – 09:30

Дія користувача: Робітник заходить на портал helsi.me, щоб записатися до

лікаря, а потім перевіряє баланс на privat24.ua. Також веде переписку з дружиною у Web-версії Telegram.

1) система А (Традиційна):

a. SSL-інспекція дешифрує трафік.

b. у логах Proxy зафіксовано повні URL: helsi.me/doctor/oncologist/... (розкриває медичний профіль).

c. кейлогер зафіксував текст повідомлень у чаті.

d. вердикт: Тотальне порушення приватності. Адміністратор отримав доступ до чутливих даних без жодної легітимної мети.

2) система В (Етична):

a. на шлюзі спрацювало правило пропуску для категорій Здоров’я та Фінанси.

b. трафік до банку пройшов зашифрованим тунелем.

c. у SIEM потрапив лог: Time: 09:15 | User: Hash_7x9 | Категорія: Довірений/Конфіденційний | Розмір: 1.5 MB.

d. вердикт**:** Приватність збережено. Система зафіксувала факт активності (для табелювання робочого часу), але сліпа до змісту.

ЕТАП 2. Компрометація та виконання коду

Час події: 10:45

Дія користувача: Отримує лист із темою Терміново: Рахунок-фактура. Завантажує файл Invoice_001.docm. При відкритті спрацьовує макрос, який запускає PowerShell-скрипт (техніка T1059.001).

1) система А (Традиційна):

a. алерт: Suspicious PowerShell execution by o.petrenko.

b. аналітик бачить прізвище і миттєво телефонує співробітнику.

2) система В (Етична):

a. EDR-агент фіксує запуск підозрілого процесу.

b. Logstash хешує ім'я користувача.

c. Алерт у SIEM: Критичний рівень: PowerShell ускладнена команда на Host SALES-PC-04 від User Hash_7x9.

d. вердикт: Обидві системи виявили загрозу. Затримка на хешування в Системі В склала менше 100 мілісекунд, що не впливає на безпеку. Аналітик Системи В бачить атаку, але ще не знає, хто її жертва.

ЕТАП 3. Ексфільтрація даних

Час події: 10:48

Дія зловмисника: Скрипт збирає файли з робочого столу та намагається вивантажити їх на анонімний файлообмінник mega.nz.

1) система А (Традиційна):

a. DLP блокує передачу. Адміністратор переглядає вміст файлів, щоб оцінити збитки.

b. Адміністратор вручну блокує обліковий запис o.petrenko в Active Directory.

2) система В (Етична):

a. система фіксує спробу вивантаження на недовірений ресурс.

b. оскільки подія класифікована як критичний інциденет, автоматично спрацьовує SOAR-плейбук: Ізолювати хост SALES-PC-04.

c. рівень ризику користувача Hash_7x9 досягає 95/100.

d. вердикт: Автоматична реакція спрацювала однаково ефективно. Хост ізольовано.

ЕТАП 4. Розслідування та Деанонімізація (Response)

Час події: 11:00

Завдання: Необхідно провести службове розслідування, опитати працівника та перевірити, чи не був він співучасником.

1) система А (Традиційна):

a. Адміністратор відкриває повну історію дій робітника за тиждень.

b. Читає його чати, бачить відвідування лікаря (Етап 1), робить висновок: Він шукав гроші на лікування, можливо продав пароль. Це упередження, яке веде хибним шляхом.

2) система В (Етична):

a. аналітик ініціює процедуру Чотирьох очей. Створює тікет #INC-

1024.

b. крок 1:CISO перевіряє технічні докази атаки >Підписує ключем A.

c. крок 2: DPO перевіряє правомірність -> Підписує ключем B.

d. результат: Система декодує хеш: Hash_7x9 = Absc.D.

e. важливо: Аналітик отримує доступ лише до подій, пов'язаних з інцидентом (Етап 2 і 3). Події Етапу 1 (Медицина) залишаються прихованими або видаленими фільтром.

Кількісна оцінка результатів

Для об'єктивізації висновків було виміряно ключові метрики ефективності (KPI) під час обох прогонів сценарію.

Таблиця 3.8.

Порівняння KPI традиційної та етичної систем

Метрика ефективності	**Традиційна модель**	**Етична модель (E-SOC)**	**Динаміка / Висновок**
MTTD	45 секунд	45.2 секунди	**+0.4%**. Затримка на криптографічні операції є нехтувано малою.
MTTR	5 хвилин (ручне блокування)	2 хвилини (автоматичний SOAR)	**-60%**. Автоматизація на основі рівня ризику працює швидше, ніж людина.
PII (Кількість розкритих приватних записів)	**14 записів** (URL лікарні, текст чату, банк)	**0 записів** (на етапі моніторингу)	**Абсолютна перевага.** Етична модель повністю захищає приватність до моменту розслідування.
Тиск хибнопозитивних результатів (Психологічний тиск)	Високий (Адмін бачить усе)	Низький (Адмін бачить лише аномалії)	Зниження ризику упередженості.
Адміністративні накладні витрати (Час на процедури)	0 хв	15-20 хв (на деанонімізацію)	**Плата за етику.** Процедура двох ключів вимагає часу, але це запобіжник від свавілля.

Розрахунок економічної ефективності (ROI)

Відповідно до вимог кваліфікаційної роботи, необхідно обґрунтувати економічну доцільність впровадження розробки. Етичний моніторинг часто сприймається як зайві витрати, але розрахунок ризиків доводить зворотне.

Використаємо формулу розрахунку ALE - очікуваних річних втрат.

1) сценарій Традиційний (Ризик штрафів та судів):

a. потенційний штраф за порушення GDPR (або позов від звільненого працівника за втручання в приватне життя): $100,000 (умовний еквівалент для середнього бізнесу з європейськими контрактами).

b. ймовірність події (за 3 роки): 20%.

c. ризик: $20,000 / рік.

2) сценарій Витік даних (Інсайдер):

a. вартість витоку бази клієнтів: $500,000.

b. ймовірність (без ефективного UEBA): 10%.

c. ризик: $50,000 / рік.

3) сартість впровадження E-SOC:

a. налаштування: $5,000 (разово).

b. підтримка процесів: $2,000 / рік.

Розрахунок ROI:

Впровадження E-SOC дозволяє знизити юридичні ризики на 95% (завдяки підходу на основі доказів) та ризики інсайдерів на 70% (завдяки зменшенню сліпих зон тіньового IT).

Навіть при консервативних оцінках, окупність інвестицій в етичні налаштування становить понад 200% у перший рік, оскільки компанія купує страховку від руйнівних репутаційних та юридичних скандалів.

Висновки до Розділу 3

У третьому розділі кваліфікаційної роботи вирішено науково-практичне завдання розробки комплексної системи моніторингу, що дозволяє

гармонізувати вимоги національної безпеки та права на приватність. За результатами проведеної розробки та апробації зроблено такі висновки:

Сформульовано концептуальні засади етичного моніторингу, що базуються на авторському принципі Вибіркової видимості. Встановлено, що перехід від тотального нагляду до контекстно-залежного моніторингу дозволяє зберегти ефективність виявлення загроз, водночас забезпечуючи відповідність принципам GDPR. Визначено чотири архітектурні стовпи системи: приватність за замовчуванням, розділення знань, аудит спостерігача та мінімізація даних.

Розроблено архітектурну модель системи E-SOC, ключовою інновацією якої є впровадження Шлюзу приватності. Цей компонент забезпечує автоматичну псевдонімізацію ідентифікаторів користувачів та санітизацію даних ще до моменту їх запису в базу SIEM. Це технічно унеможливлює використання системи безпеки для несанкціонованого стеження за персоналом.

Запропоновано алгоритм селективної інспекції трафіку та матрицю зонування цифрового простору. Обґрунтовано, що відмова від дешифрації трафіку категорій Банкінг та Медицина є критично необхідною для дотримання етичних норм і не створює критичних вразливостей для периметра безпеки.

Визначено організаційно-технічні механізми контролю за діями адміністраторів. Розроблено протокол деанонімізації Чотирьох очей, який вимагає цифрового підтвердження від двох незалежних ролей для розкриття особистості користувача. Це впроваджує систему стримувань і противаг у роботу служби безпеки.

Експериментально доведено ефективність запропонованої моделі шляхом апробації на імітаційно-теоретичному кейсі. Результати порівняльного тестування показали, що впровадження етичних модулів не призводить до суттєвого збільшення часу реагування на інциденти, проте дозволяє знизити обсяг витоку приватних даних до нуля на етапі моніторингу. Розрахунок ROI підтвердив економічну доцільність впровадження системи як засобу мінімізації юридичних та репутаційних ризиків.

Таким чином, розроблена система є готовим до впровадження рішенням,

яке спростовує тезу про неминучість вибору між безпекою та приватністю, пропонуючи технологічно вивірений баланс інтересів.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-практичне завдання розробки методів етичного моніторингу в інформаційних системах, що дозволяють забезпечити баланс між необхідним рівнем національної безпеки та дотриманням прав громадян на приватність. За результатами проведеного дослідження зроблено такі висновки:

Проаналізовано теоретико-методологічні засади забезпечення кібербезпеки критичних систем. Встановлено, що в умовах гібридних загроз традиційні пасивні методи захисту втратили свою ефективність, що зумовлює необхідність переходу до проактивного моніторингу. Однак виявлено, що існуючі підходи до моніторингу часто ігнорують етичну складову, створюючи конфлікт між імперативом безпеки та фундаментальним правом особи на приватність.

Визначено та систематизовано ключові проблеми етичного моніторингу. Доведено, що впровадження тотального нагляду створює ефект Цифрового Паноптикому, що призводить до негативних психосоціальних наслідків: зниження довіри, «ефекту заморожування» ініціативи та появи Тіньового ІТ. Виявлено технічні ризики, зокрема мозаїчний ефект та проблему алгоритмічної упередженості в системах штучного інтелекту .

Здійснено порівняльний аналіз практик у державному та корпоративному секторах. З’ясовано, що державний сектор орієнтований на пріоритет колективної безпеки, тоді як корпоративний – на економічну доцільність та комплаєнс. Для об'єктів критичної інфраструктури, які перебувають на перетині цих інтересів, обґрунтовано необхідність гібридної моделі, що поєднує глибину аналізу загроз із захистом приватності .

Розроблено архітектурну модель системи етичного моніторингу, яка базується на принципах приватносі за замовчуванням. Ключовою інновацією моделі є впровадження Шлюзу приватності, що забезпечує автоматичну

псевдонімізацію даних та контекстну фільтрацію трафіку до моменту їх запису в систему. Це технічно унеможливлює масовий несанкціонований нагляд .

Запропоновано алгоритм Вибіркової видимості, який динамічно змінює глибину моніторингу залежно від рівня ризику та категорії ресурсу, та формалізовано протокол деанонімізації «Чотирьох очей», що впроваджує систему стримувань і противаг у роботу адміністраторів безпеки .

Експериментально підтверджено ефективність розробленої системи. Апробація на імітаційному кейсі показала, що впровадження етичних модулів не призводить до критичного збільшення часу реагування на інциденти, проте дозволяє знизити ризики порушення приватності та потенційні юридичні витрати компанії. Розрахунок ROI підтвердив економічну доцільність впровадження системи .

Таким чином, у роботі доведено, що дилема «безпека проти приватності» може бути вирішена шляхом застосування сучасних технологій (PETs) та правильної архітектури систем, що дозволяє забезпечити високий рівень кіберстійкості держави без порушення демократичних цінностей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А. Інтернет речей (IoT): правові аспекти захисту персональних даних. *Інформація і право*. 2019. № 1. URL: http://ippi.org.ua/internet-rechei-iot-pravovi-aspekti-zakhistu-personalnikh-danikh (дата звернення: 27.10.2025).

2. Гнатюк С. О. Кібербезпека: сучасні виклики та загрози. *Безпека інформації*. 2020. Т. 26, № 2. URL: https://journals.indexcopernicus.com/search/article?articleId=250123 (дата звернення: 27.10.2025).

3. Данилюк М. В. Правові аспекти моніторингу інформаційного простору. *Юридичний науковий електронний журнал*. 2019. № 3. URL: http://lsej.org.ua/3_2019/22.pdf (дата звернення: 28.10.2025).

4. Державна служба спеціального зв'язку та захисту інформації України. Звіт про кіберзагрози за 2024 рік. URL: https://cip.gov.ua/ua/news/

5. Доктрина інформаційної безпеки України : затв. Указом Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 28.10.2025).

6. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. URL: http://lib.npu.edu.ua/files/dstu-8302-2015.pdf (дата звернення: 28.10.2025).

7. ДСТУ ISO/IEC 27001:2023. Системи керування інформаційною безпекою. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=96866 (дата звернення: 29.10.2025).

8. Захаров Є. Ю. Права людини у сфері кібербезпеки: європейський досвід. *Право і суспільство*. 2021. № 1. URL: http://pravoisuspilstvo.org.ua/archive/2021/1_2021/22.pdf (дата звернення: 29.10.2025).

9. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 р. № 8073-X. URL:

https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення: 29.10.2025).

10. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 29.10.2025).

11. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 30.10.2025).

12. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 30.10.2025).

13. Мельник Р. І. Баланс між безпекою та приватністю: пошук правової моделі. *Інформація і право*. 2018. № 2. URL: http://ippi.org.ua/balans-mizh-bezpekoyu-ta-privatnistyu (дата звернення: 27.10.2025).

14. План заходів з реалізації Стратегії кібербезпеки України : Розпорядження КМУ. URL: https://zakon.rada.gov.ua/laws/show/ (дата звернення: 30.10.2025).

15. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15 (дата звернення: 30.10.2025).

16. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20 (дата звернення: 1.11.2025).

17. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 1.11.2025).

18. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 2.11.2025).

19. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 2.11.2025).

20. Про основні засади забезпечення кібербезпеки України : Закон

України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 3.11.2025).

21. Про телекомунікації : Закон України (втратив чинність, архів). URL: https://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення: 3.11.2025).

22. Рішення Конституційного Суду України у справі про захист даних (справа К. Жадана) від 20.01.2012 р. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12 (дата звернення: 27.10.2025).

23. Стратегія кібербезпеки України : затв. Указом Президента України від 26.08.2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-39909 (дата звернення: 4.11.2025).

24. Стратегія національної безпеки України : затв. Указом Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020 (дата звернення: 4.11.2025).

25. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 5.11.2025).

26. Acquisti A. Privacy and human behavior. *Science*. 2015. URL: https://www.science.org/doi/10.1126/science.aaa1465 (дата звернення: 5.11.2025).

27. Charter of Fundamental Rights of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (дата звернення: 6.11.2025).

28. Cisco Annual Internet Report (2018–2023). URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (дата звернення: 6.11.2025).

29. Electronic Frontier Foundation. Surveillance Self-Defense. URL: https://ssd.eff.org/ (дата звернення: 7.11.2025).

30. ENISA Threat Landscape 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 7.11.2025).

31. European Convention on Human Rights. URL:

https://www.echr.coe.int/documents/convention_eng.pdf (дата звернення: 27.10.2025).

32. Gartner. Top Strategic Technology Trends for 2024. URL: https://www.gartner.com/en/information-technology/insights/top-technology-trends (дата звернення: 8.11.2025).

33. GDPR: Regulation (EU) 2016/679. *Official Journal of the European Union*. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 27.10.2025).

34. ISACA. COBIT 2019 Framework: Introduction and Methodology. URL: https://www.isaca.org/resources/cobit (дата звернення: 9.11.2025).

35. ISO/IEC 27002:2022. Information security controls. URL: https://www.iso.org/standard/75652.html (дата звернення: 10.11.2025).

36. ISO/IEC 27701:2019. Privacy information management. URL: https://www.iso.org/standard/71670.html (дата звернення: 12.11.2025).

37. Kshetri N. Big Data's Role in National Security. *Computer*. URL: https://ieeexplore.ieee.org/document/6924776 (дата звернення: 27.10.2025).

38. Microsoft Digital Defense Report 2024. URL: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report (дата звернення: 13.11.2025).

39. Nagios Core Documentation. URL: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/ (дата звернення: 27.10.2025).

40. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. Version 1.0. URL: https://www.nist.gov/privacy-framework (дата звернення: 14.11.2025).

41. NIST SP 800-53 Rev. 5. Security and Privacy Controls. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 16.11.2025).

42. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. URL:

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (дата звернення: 27.10.2025).

43. OSSEC Documentation. Open Source Host-based Intrusion Detection System. URL: https://www.ossec.net/docs/ (дата звернення: 16.11.2025).

44. Snort Users Manual. URL: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/ (дата звернення: 16.11.2025).

45. Splunk Enterprise Security User Guide. URL: https://docs.splunk.com/Documentation/ES (дата звернення: 17.11.2025).

46. The Universal Declaration of Human Rights. UN. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights (дата звернення: 17.11.2025).

47. Verizon 2024 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 18.11.2025).

48. Wireshark User's Guide. URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата звернення: 19.11.2025).

49. Zabbix 6.0 Manual. URL: https://www.zabbix.com/documentation/6.0/en/manual (дата звернення: 21.11.2025).

50. Zeek User Manual. URL: https://docs.zeek.org/en/current/ (дата звернення: 23.11.2025).