

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія створення політик безпеки для інформаційної системи
організації на основі моделі нульової довіри»**

зі спеціальності

125 Кібербезпека та захист інформації

(код, найменування спеціальності)

освітньо-професійної програми

Інформаційна та кібернетична безпека

(назва програми)

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

Артем МУРАВЙОВ

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61

МУРАВЙОВ Артем

(прізвище, ім'я)

Керівник

д-р техн. наук, професор САВЧЕНКО

Віталій

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

2. Аналіз нормативних документів, сучасних загроз та принципу нульової довіри.

3. Технологія створення політик безпеки на основі моделі нульової довіри.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми відсутності політик безпеки.	05.10.2025 р.	
2.	Аналіз сучасних нормативних документів.	11.10.2025 р.	
3.	Дослідження сучасних загроз для середньої організації.	27.10.2025 р.	
4.	Технологія створення політик безпеки для середніх організацій на основі моделі нульової довіри.	15.11.2025 р.	
5.	Розроблення рекомендацій та прикладів щодо застосування технології розроблення політик безпеки.	28.11.2025 р.	
6.	Оформлення результатів дослідження.	15.12.2025 р.	
7.	Подання роботи на плагіат. Підготовка доповіді до захисту.	24.12.2025 р.	

Здобувач вищої освіти

(підпис)

Артем МУРАВЬОВ

(ім'я, прізвище)

Керівник кваліфікаційної роботи

(підпис)

Віталій САВЧЕНКО

(ім'я, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 72 сторінки, 23 рисунків, 14 джерел.

Об'єкт дослідження – процес формування та впровадження політик інформаційної безпеки в організації середнього масштабу з гібридною моделлю роботи та on-premise доменною інфраструктурою.

Предмет дослідження – технологія створення політик безпеки на основі моделі нульової довіри (Zero Trust) та практичні підходи до її реалізації в Windows-орієнтованому середовищі.

Мета роботи – аналіз сучасних кіберзагроз і нормативно-методичних підходів до управління інформаційною безпекою, проєктування цільової архітектури захисту за принципами Zero Trust, а також розроблення технології формування політик безпеки та прикладу їх реалізації на базі обраного набору засобів захисту.

Методи дослідження – аналіз науково-технічної та нормативної літератури з питань управління інформаційною безпекою, вивчення стандартів ISO/IEC 27001:2022 та ISO/IEC 27002:2022 і концепції NIST SP 800-207 (Zero Trust), узагальнення даних галузевих звітів щодо тенденцій кіберзагроз, системний аналіз типових ланцюгів атак для Windows-орієнтованих on-premise інфраструктур, моделювання архітектури та логічне проєктування зон довіри, формалізація вимог до контролів і процесів, а також розроблення практикоорієнтованих рекомендацій щодо конфігурації засобів захисту.

У роботі обґрунтовано доцільність застосування Zero Trust для організацій із гібридною моделлю роботи та визначено типові вектори атак для Windows-орієнтованої on-premise інфраструктури. Сформовано вимоги до системи захисту та спроектовано цільову архітектуру, принципом найменших привілеїв і явним визначенням дозволених взаємодій. Розроблено технологію формування політик, доступ і керування обліковими записами, захист кінцевих точок і серверів, віддалений доступ, моніторинг і реагування, резервне копіювання) та наведено приклад їх реалізації на базі ESET PROTECT/Endpoint/Server Security, ESET Secure Authentication, ESET Full Disk Encryption у поєднанні з AD/GPO та мережевим IDS-рівнем (Suricata) з передаванням подій до SIEM.

Галузь використання – кібербезпека та управління інформаційною безпекою в організаціях середнього масштабу, зокрема в середовищах із гібридною моделлю роботи та локальною доменною інфраструктурою.

ZERO TRUST, ПОЛІТИКИ БЕЗПЕКИ, ГІБРИДНА РОБОТА, INFORMATION SECURITY MANAGEMENT, ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-207, ACTIVE DIRECTORY, MFA, VPN, RBAC, СЕГМЕНТАЦІЯ МЕРЕЖІ, EDR/EPP, SIEM, ЖУРНАЛЮВАННЯ, РЕАГУВАННЯ НА ІНЦИДЕНТИ, РЕЗЕРВНЕ КОПІЮВАННЯ, ESET PROTECT, SURICATA

ABSTRACT

Text part of the qualification work: 72 pages, 23 figures, 14 sources.

Object of research – the process of developing and implementing information security policies in a mid-sized organization with a hybrid work model and an on-premises domain infrastructure.

Subject of research – a technology (methodology) for creating security policies based on the Zero Trust model and practical approaches to implementing it in a Windows-oriented environment.

The aim of research – to analyze modern cyber threats and regulatory/methodological approaches to information security management, to design a target protection architecture based on Zero Trust principles, and to develop a methodology for security policy creation along with an example of its implementation using a selected set of security tools.

Research methods – analysis of scientific, technical, and regulatory sources on information security management; study of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 standards and the NIST SP 800-207 Zero Trust concept; synthesis of industry threat reports; systematic analysis of typical attack chains for Windows-oriented on-premises infrastructures; modeling of the target architecture; and formalization of requirements for controls and processes.

The thesis substantiates the applicability of Zero Trust for organizations with a hybrid work model and identifies typical attack vectors for a Windows-oriented on-premises infrastructure. Security requirements are formulated and a target architecture is designed based on environment zoning, the principle of least privilege, and explicit definition of allowed interactions. A methodology for policy development is proposed (access and account management, endpoint and server protection, remote access and authentication, monitoring and incident response, and backup), and an example implementation is provided using ESET PROTECT/Endpoint/Server Security, ESET Secure Authentication, and ESET Full Disk Encryption in combination with AD/GPO and a network IDS layer (Suricata) with event forwarding to a SIEM.

Field of application – cybersecurity and information security management in mid-sized organizations, particularly in environments with a hybrid work model and an on-premises domain infrastructure.

ZERO TRUST, SECURITY POLICIES, HYBRID WORK, INFORMATION SECURITY MANAGEMENT, ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-207, ACTIVE DIRECTORY, MFA, VPN, RBAC, NETWORK SEGMENTATION, EDR/EPP, SIEM, LOGGING, INCIDENT RESPONSE, BACKUP, ESET PROTECT, SURICATA

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	9
ВСТУП	10
1 ДОСЛІДЖЕННЯ СУЧАСНИХ КІБЕРЗАГРОЗ ТА МОЖЛИВОСТЕЙ МОДЕЛІ НУЛЬОВОЇ ДОВІРИ.....	13
1.1 Аналіз сучасних кіберзагроз та наслідків відсутності політик безпеки в організаціях.....	13
1.2 Нормативно-правові підходи до інформаційної безпеки.....	20
1.3 Підходи до створення політик на основі моделі нульової довіри.... Висновки до першого розділу.....	24 28
2 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ОРГАНІЗАЦІЇ НА ОСНОВІ МОДЕЛІ НУЛЬОВОЇ ДОВІРИ	30
2.1 Характеристика інформаційної системи організації та методи атак на неї	30
2.2 Визначення вимог до системи захисту реалізації Zero Trust.....	34
2.3 Проектування архітектури Zero Trust для інформаційної системи організації та вибір рішень захисту..... Висновки до другого розділу.....	40 46
3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ СТВОРЕННЯ ПОЛІТИК БЕЗПЕКИ НА ОСНОВІ МОДЕЛІ НУЛЬОВОЇ ДОВІРИ	48
3.1 Варіант технології побудови політик безпеки в умовах Zero Trust	48
3.2 Приклад реалізації політик безпеки на базі обраних програмних продуктів	53
Висновки до третього розділу.....	67
ВИСНОВКИ	68
ПЕРЕЛІК ПОСИЛАНЬ	70
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	72

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GPO — Group Policy Object

RBAC — Role-Based Access Control

VPN — Virtual Private Network

MFA — Multi-Factor Authentication

TOTP — Time-based One-Time Password

RADIUS — Remote Authentication Dial-In User Service

RDP — Remote Desktop Protocol

PAW — Privileged Access Workstation

SAW — Secure Admin Workstation

LAPS — Local Administrator Password Solution

EPP — Endpoint Protection Platform

EDR — Endpoint Detection and Response

XDR — Extended Detection and Response

NGAV — Next-Generation AntiVirus

DMZ — Demilitarized Zone

IDS — Intrusion Detection System

IPS — Intrusion Prevention System

NDR — Network Detection and Response

IPSec — Internet Protocol Security

CVE — Common Vulnerabilities and Exposures

DNS — Domain Name System

URL — Uniform Resource Locator

ВСТУП

Актуальність дослідження. Поширення гібридної моделі роботи та зростання частки сервісів, доступних ззовні корпоративного периметра, істотно змінюють профіль ризиків для організацій. Працівники дедалі частіше взаємодіють із внутрішніми ресурсами з домашніх мереж, мобільних підключень та інших локацій, що розширює площину атаки й ускладнює застосування класичних периметрових підходів. На практиці це підсилює значущість атак, орієнтованих на компрометацію цифрових ідентичностей, механізмів віддаленого доступу та публічно доступних компонентів інфраструктури.

Для on-premise середовищ із доменною інфраструктурою додатковими чинниками ризику виступають слабка сегментація, надмірні привілеї, використання застарілих протоколів, недостатня керованість кінцевих точок поза офісом, а також фрагментоване журналювання й обмежена спостережуваність. У таких умовах формальна наявність політик безпеки без їх відображення в архітектурі, конфігураціях і процесах експлуатації не забезпечує належного рівня захисту та не дозволяє ефективно стримувати розвиток атаки після первинного проникнення.

У відповідь на ці виклики актуальним є підхід Zero Trust, у якому доступ розглядається як динамічне рішення на основі ідентичності, контексту та стану пристрою, а мережеві взаємодії визначаються явно за принципом найменших привілеїв. Водночас практична цінність Zero Trust для організацій середнього масштабу визначається не лише загальними принципами, а насамперед наявністю методично обґрунтованої технології формування політик та прикладної моделі їх реалізації в типових Windows-орієнтованих on-premise середовищах. Саме ці міркування визначають актуальність даної кваліфікаційної роботи.

Об'єкт дослідження – процес формування та впровадження політик інформаційної безпеки в організації середнього масштабу з гібридною моделлю роботи та on-premise доменною інфраструктурою.

Предмет дослідження – технологія створення політик безпеки на основі моделі нульової довіри (Zero Trust) і підходи до їх практичної реалізації в Windows-

орієнтованому середовищі.

Мета роботи – аналіз сучасних кіберзагроз і нормативно-методичних підходів до управління інформаційною безпекою, проєктування цільової архітектури захисту за принципами Zero Trust, а також розроблення технології формування політик безпеки й прикладу їх реалізації на базі обраного набору засобів захисту.

Наукові завдання:

- проаналізувати сучасні кіберзагрози та типові наслідки відсутності або формальності політик безпеки в організаціях;
- узагальнити нормативно-методичні підходи до управління інформаційною безпекою та визначити релевантні вимоги для гібридних сценаріїв;
- охарактеризувати узагальнену інформаційну систему організації середнього масштабу та визначити типові вектори атак на її компоненти;
- сформувати вимоги до системи захисту в парадигмі Zero Trust для Windows-орієнтованого on-premise середовища;
- спроектувати цільову архітектуру Zero Trust з урахуванням сегментації, керування доступом, моніторингу та відновлюваності;
- розробити технологію створення політик безпеки як узгодженого набору вимог, правил і процедур;
- продемонструвати приклад реалізації сформованих політик засобами обраного набору інструментів та визначити практичні рекомендації щодо конфігурації.

Методи дослідження – опрацювання науково-технічної та нормативної літератури за темою роботи, аналіз стандартів і методичних матеріалів, системний аналіз і моделювання архітектури, логічне узагальнення та формалізація вимог до контролів і процесів, розроблення практикоорієнтованих рекомендацій.

Практичне значення одержаних результатів: Запропонована технологія може бути використана як методична основа для створення та впровадження політик безпеки в організаціях середнього масштабу з гібридною моделлю роботи; результати роботи придатні для адаптації під конкретні умови експлуатації,

критичність сервісів і доступні засоби захисту, а також можуть слугувати базою для подальшої деталізації сценаріїв моніторингу, реагування й контролю відповідності.

Результати кваліфікаційної роботи можуть бути використані під час практичного проектування та вдосконалення політик безпеки в Windows-орієнтованих on-premise середовищах із гібридною моделлю доступу, а також у навчально-методичній діяльності за напрямками управління інформаційною безпекою та Zero Trust.

1 ДОСЛІДЖЕННЯ СУЧАСНИХ КІБЕРЗАГРОЗ ТА МОЖЛИВОСТЕЙ МОДЕЛІ НУЛЬОВОЇ ДОВІРИ

1.1. Аналіз сучасних кіберзагроз та наслідків відсутності політик безпеки в організаціях

Сучасні кіберзагрози характеризується стійкою тенденцією до зростання масовості та ускладнення кібератак, спрямованих на інформаційні системи організацій, зокрема на облікові записи користувачів, відкриті сервіси, мережеву інфраструктуру та дані.

Згідно з даними Verizon Data Breach Investigations Report 2025, ransomware та інші форми кібервимагання були зафіксовані у 44% підтверджених порушень безпеки. Аналіз динаміки за останні роки демонструє послідовне зростання частки порушень безпеки, пов'язаних із ransomware. Частка порушень безпеки, пов'язаних із ransomware, зростає з 10% у 2021 році до 25% у 2022 році, знизилася до 24% у 2023 році, знову зростає до 32% у 2024 році та досягла 44% у 2025 році (рисуюнок 1.1).

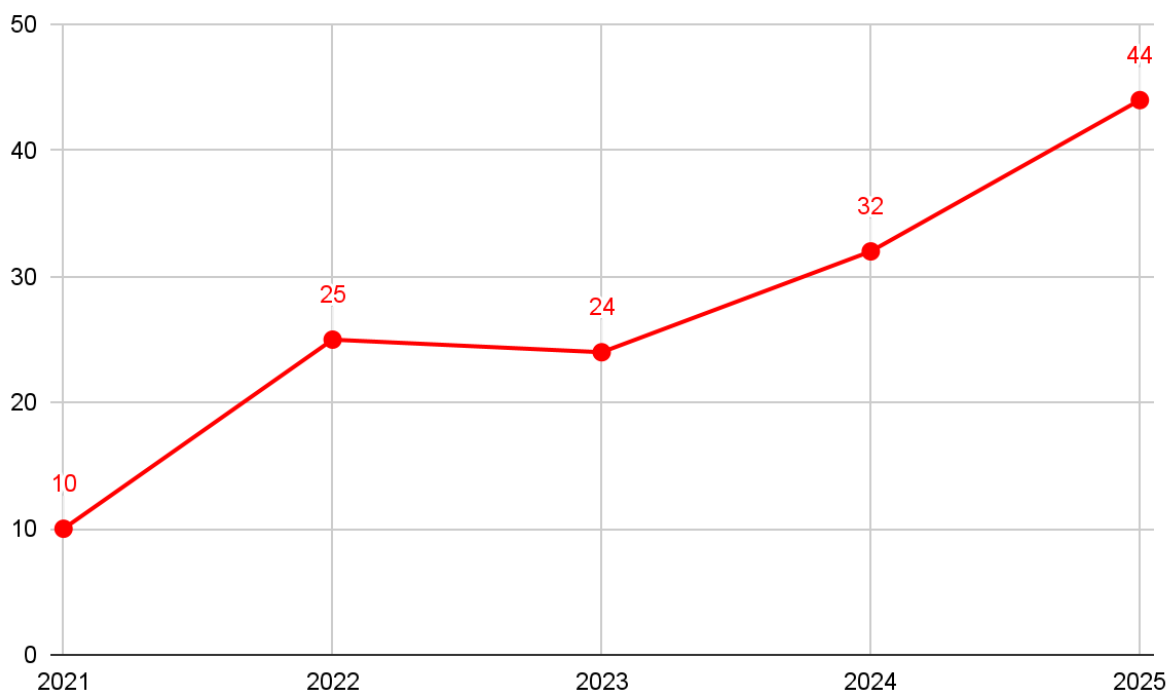


Рис. 1.1 Динаміка частки порушень безпеки, пов'язаних із ransomware, у 2021 – 2025 роках [1][2][3][4][5]

Станом на 2025 рік людський фактор залишається одним із ключових чинників порушень безпеки, будучи залученим приблизно у 60% підтверджених інцидентів. Водночас аналіз даних за попередні роки свідчить про поступову зміну частки порушень безпеки з участю людського фактора, яка зменшилася з 85% у 2021 році до 82% у 2022 році, 74% у 2023 році та 68% у 2024 році. Відповідна динаміка участі людського фактора у порушеннях безпеки у 2021–2025 роках наведена на рисунку 1.2.

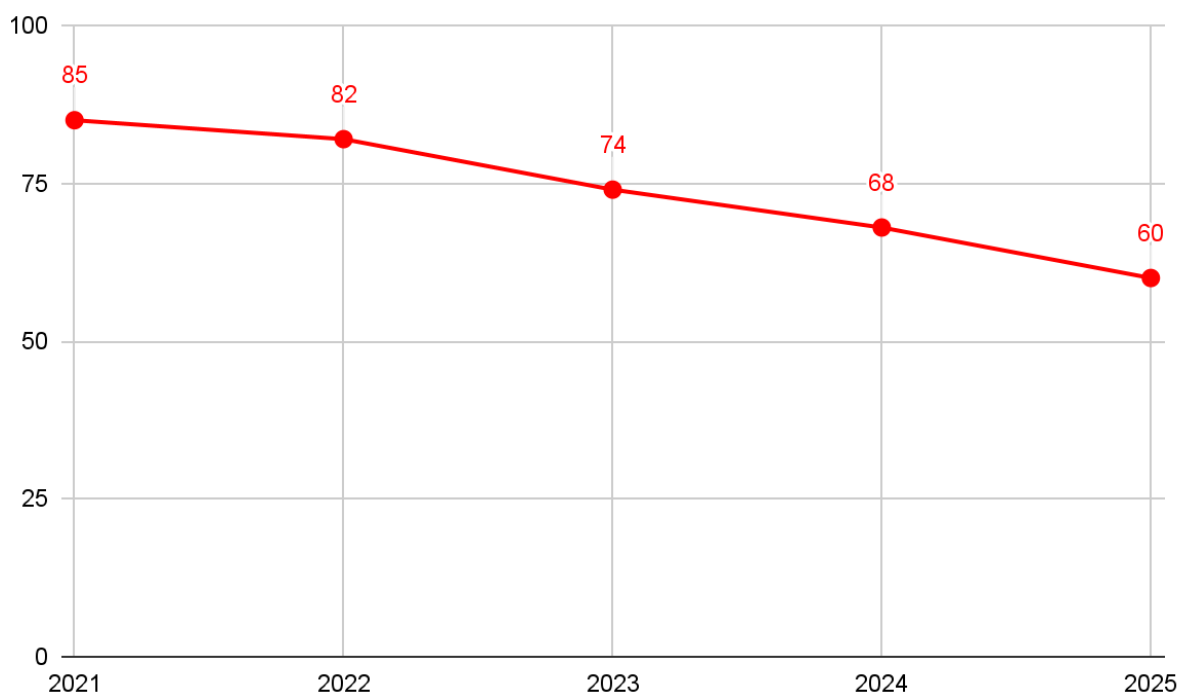


Рис. 1.2 Динаміка частки порушень безпеки з участю людського фактора у 2021 – 2025 роках [1][2][3][4][5]

Окремої уваги набуває зростання ролі третіх сторін у порушеннях безпеки. У звіті Verizon Data Breach Investigations Report 2024 [4] було вперше розширено трактування порушень із залученням третіх сторін, включивши вплив партнерської інфраструктури та прямі й опосередковані атаки на ланцюжок постачання програмного забезпечення. У межах такого підходу частка відповідних порушень становила близько 15%. Згідно з даними Verizon Data Breach Investigations Report 2025 [5], частка порушень безпеки із залученням третіх сторін зросла до 30%, що свідчить про подальше посилення значущості цього чинника в сучасному ландшафті кіберзагроз.

За оцінками Microsoft, щодня блокується близько 600 мільйонів атак на ідентичності, під якими маються на увазі масові спроби несанкціонованого доступу до облікових записів шляхом підбору, повторного використання або компрометації облікових даних. Як показано на рисунку 1.3, переважна більшість атак на ідентичності має паролезалежний характер. За даними Microsoft Threat Intelligence [6], понад 99% атак на облікові записи базуються на зловживанні паролями, зокрема шляхом підбору облікових даних, password spraying, повторного використання паролів та фішингу. Такі атаки експлуатують передбачувану поведінку користувачів, включно з використанням слабких або повторно застосовуваних паролів. Частка атак, спрямованих безпосередньо на механізми багатофакторної автентифікації або післяавтентифікаційні етапи (зокрема MFA fatigue, Adversary-in-the-Middle чи викрадення токенів), становить менше 1%, що підкреслює домінування паролінової моделі як основного вектора компрометації цифрових ідентичностей.

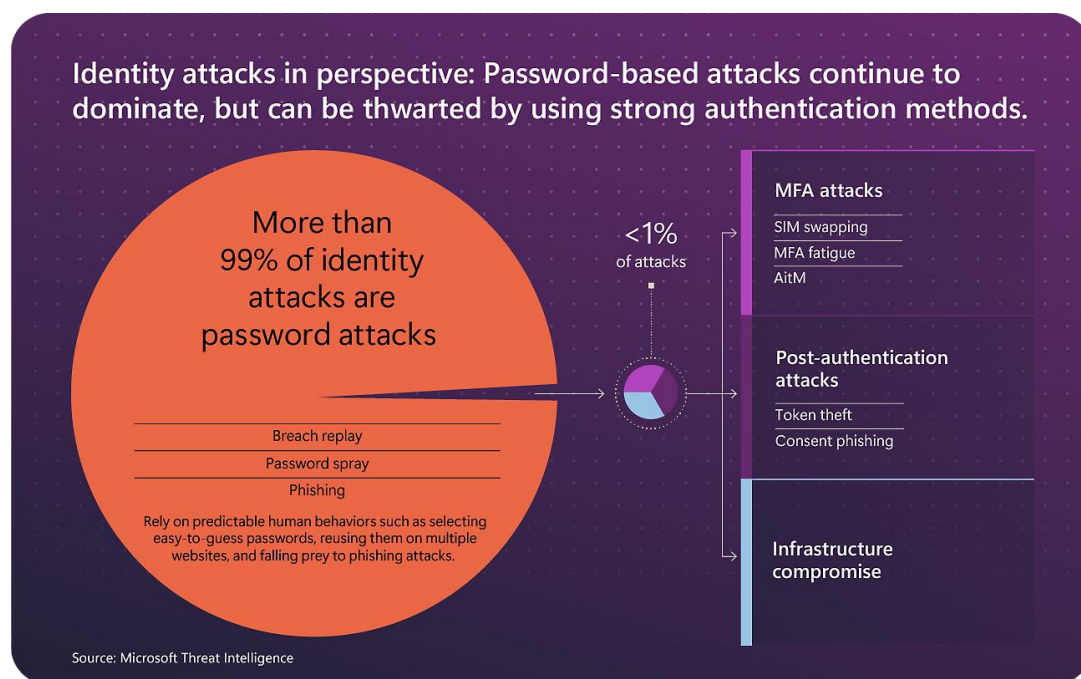


Рис 1.3 - Структура атак на ідентичності за типами векторів компрометації [6]

Зазначена перевага паролезалежних атак підтверджується також високою інтенсивністю їх фіксації, яка в середньому становить близько 7 000 спроб за секунду [6].

Також варто зазначити, що у 2024 році було відзначено 2,75-кратне зростання кількості зіткнень із human-operated ransomware, але частка випадків, де атакувальникам вдається дійти до стадії шифрування, навпаки, знизилась утричі, значною мірою завдяки автоматизованому виявленню та перериванню ланцюжка атаки. Понад 90% успішних випадків шифрування припадали на сценарії, де початковою точкою доступу або майданчиком для віддаленого шифрування були некеровані пристрої, тобто девайси поза контуром централізованого управління [6]. Для гібридної моделі роботи це особливо критично, тому що саме поза офісом найчастіше використовуються пристрої, які або не підпорядковані корпоративній політиці, або підпорядковані лише частково.

Паралельно зростає роль експлуатації технічних вразливостей, насамперед у публічно доступних сервісах і периметрових компонентах. За даними Verizon DBIR 2025, експлуатація вразливостей як початковий вектор доступу до інцидентів з підтвердженим порушенням безпеки зростає до 20%, наблизившись за поширеністю до зловживання обліковими даними, і становила +34% порівняно з попереднім роком. При цьому частка атак на периметрові пристрої та VPN у межах експлуатації вразливостей досягла 22%, що є зростанням майже у 8 разів минулого року, а темпи усунення таких вразливостей залишаються недостатніми, оскільки упродовж року повністю було виправлено лише близько 54% виявлених вразливостей периметра, із медіаною в 32 дні на виправлення [5]. У цій логіці підтверджується і практичне спостереження, що саме незакриті вразливості на периметрі стають масштабованою точкою входу для кібератак. У вибірці DBIR для системних вторгнень/випадків із ransomware експлуатація вразливостей фіксується як провідний шлях первинного доступу. Додатково звіт IBM X-Force Threat Intelligence Index 2025 [7] підкреслює, що значна частка атак пов'язана з публічно доступними застосунками, у звіті зазначено як високу роль експлуатації вразливостей у common public-facing/internet-accessible застосунках, так і загальну тенденцію до зростання кількості вразливостей, що частково пояснюється залежністю від спільної хмарної інфраструктури та сервісів, де компрометація поширених компонентів потенційно масштабує вплив на багато організацій

одночасно. На цьому фоні проблема застарілого ПЗ в on-premise інфраструктурах зберігає системний характер: публічно доступні веб-додатки, VPN шлюзи й засоби віддаленого адміністрування, що не оновлюються належним чином, залишаються одними з найпривабливіших цілей через наявність добре відомих експлойтів і прогнозованість шляхів компрометації.

Вектор первинного доступу також еволюціонує. Аналітика Microsoft показує, що традиційний «простий» фішинг рідше виступає єдиною причиною компрометації, натомість стає частиною багатостадійних ланцюжків, де поєднуються соціальна інженерія, технічні експлойти, зловживання легітимними хмарними сервісами та використання програм крадіїв інформації [6]. Фішинговий лист у такому сценарії часто лише запускає процес, а саме змушує користувача перейти за посиланням на легітимну, але скомпрометовану платформу, пройти авторизацію, після чого зловмисники перехоплюють токени доступу або встановлюють на пристрій крадія інформації. Подальший розвиток атаки це розповсюдження всередині іншого середовища, збір та фільтрація даних, закріплення в новій інфраструктурі, шифрування чи крадіжка інформації реалізується вже за рахунок інших технічних засобів, при цьому значна частина активності маскується під звичайний користувацький або службовий трафік.

Особливо показовими в контексті уразливості ланцюжків постачання є гучні інциденти останніх років. Атака NotPetya, що стартувала в Україні в 2017 році зі скомпрометованих оновлень бухгалтерського ПЗ М.Е.Дос, офіційно визнана однією з найдорожчих кібератак в історії: сукупні збитки оцінюються приблизно у 10 млрд доларів США, окремі міжнародні компанії, такі як Merck, Saint-Gobain, Reckitt Benckiser та Maersk — втратили сотні мільйонів кожна [8]. Шкідливий код поширювався як законне і офіційне оновлення довіреного програмного забезпечення, що дозволило миттєво обійти класичні периметрові засоби захисту. Аналогічно у випадку з компрометацією платформи Solar Winds Orion зловмисники вбудовували шкідливий код в офіційні збірки продукту, які завантажили до 18 000 клієнтів по всьому світу, хоча фактично злом було підтверджено для менш ніж

сотні організацій, інцидент продемонстрував системний характер ризиків ланцюжка постачання для урядових структур і великого бізнесу [9]. У підсумку саме ці атаки стали одним із каталізаторів популяризації підходів нульової довіри, де довіра до будь-якого компонента, включно з офіційними оновленнями, не вважається безумовною.

Український кіберпростір у цьому контексті виступає одночасно полігоном і мішенню для складних кампаній, особливо у рамках війни з російською стороною. За даними CERT-UA, у другому півріччі 2024 році урядова команда опрацювала 4 315 кіберінцидентів, що майже на 70% більше, ніж роком раніше; основними цілями виступали органи державної влади, місцевого самоврядування, сектор безпеки й оборони, енергетика, телеком-оператори та комерційні організації. У другому півріччі 2024 року було зафіксовано 2 576 атак, пов'язаних із російськими хакерськими угрупованнями, що на 48% більше, ніж у першому півріччі; при цьому значна частина кампаній поєднувала збір розвідданих, розповсюдження шкідливого ПЗ та використання supply chain-підходів через постачальників ПЗ [10].



Рис. 1.4 Статистика CERT - UA щодо кількості кіберінцидентів

Гібридна модель роботи додатково розширює площу атаки. Після пандемії робота поза офісом стала постійним елементом операційної моделі значної частини організацій. Згідно з галузевими дослідженнями ринку безпеки віддаленої роботи, обсяг сегмента рішень для захисту розподілених робочих місць у 2024 році оцінювався приблизно у 61,2 млрд доларів США, а основними драйверами зростання називаються саме поширення гібридної роботи, ескалація атак на віддалені кінцеві точки та посилення регуляторних вимог [11]. Практично це означає, що значна частина критичного трафіку сьогодні проходить через домашні маршрутизатори, публічні Wi-Fi, персональні пристрої та хмарні сервіси, які не завжди перебувають під контролем класичних засобів захисту мережевого периметра. Статистика Microsoft щодо того, що понад 90% успішних атак, які доходять до стадії шифрування, стартують із некерованих пристроїв, фактично описує типову ситуацію гібридної роботи, де співіснують корпоративні та приватні девайси.

Окремим, але тісно пов'язаним із цим блоком загроз є інсайдерський фактор. Оскільки більшість сучасних атак так чи інакше спираються на людський фактор, статистика DBIR 2025 про участь людини у 60% порушень безпеки вказує не лише на зовнішні фішингові кампанії, а й на внутрішні помилки, помилкові конфігурації та зловживання привілеями [5]. У гібридній моделі роботи це проявляється у використанні несанкціонованих каналів обміну даними, перенесенні службової інформації до особистих хмарних сховищ, зберіганні конфіденційних файлів на незашифрованих домашніх пристроях, встановленні стороннього ПЗ або відкритті фішингових вкладень із приватної пошти, яку користувач переглядає з корпоративного ноутбука. До цього додаються навмисні інсайдерські дії, наприклад, передача доступів третім особам або цілеспрямоване збирання даних, які за відсутності належного журналювання та розмежування повноважень залишаються непоміченими до моменту настання суттєвих збитків.

Сукупність наведених статистичних даних демонструє, що класична модель захисту, орієнтована на жорсткий мережевий периметр і базову перевірку

користувача лише на етапі входу в систему, більше не відповідає характеру загроз. Рішення про доступ приймаються на основі скомпрометованих облікових даних, атаки розгортаються через ланцюжки постачання та довірену інфраструктуру, а значна частина активності відбувається на некерованих пристроях у домашніх мережах. У таких умовах відсутність формалізованих і впроваджених на практиці політик управління доступом, автентифікації, сегментації, журналювання, не просто погіршують безпеку, а створює сприятливе середовище для повної реалізації ланцюжка атаки. Саме тому в подальших підрозділах роботи розглядатимуться підходи, що спираються на принципи нульової довіри (Zero Trust) та системний перегляд політик безпеки, однак вже в цьому підрозділі статистичний аналіз показує, що без переходу від формального до реального управління безпекою організації залишаються вразливими як до глобальних трендів кібератак, так і до специфічних загроз українського контексту.

1.2. Нормативно-правові підходи до інформаційної безпеки

Як показав аналіз сучасних кіберзагроз, відсутність формалізованих політик безпеки та їх реального впровадження безпосередньо пов'язана з успішною реалізацією атак, що починаються з компрометації облікових записів, несанкціонованого віддаленого доступу або використання вразливостей у хмарних сервісах. У гібридній моделі роботи, коли співробітники поєднують офісний режим, віддалену роботу з дому та тимчасові робочі місця, традиційні моделі захисту, орієнтовані на жорсткий периметр корпоративної мережі, втрачають ефективність. У результаті значна частина критичного трафіку проходить за межами класично захищеної зони, а пристрої користувачів опиняються в умовах, які важко контролювати засобами традиційного мережевого захисту.

У відповідь на ці виклики сформувалися стандартизовані підходи до побудови систем управління інформаційною безпекою. Ключовими серед них є стандарти ISO/IEC 27001:2022 та ISO/IEC 27002:2022, а також концепція Zero Trust, описана в документі NIST SP 800-207. В українських реаліях важливе місце займають також рекомендації CERT-UA, які враховують специфіку загрозового

середовища, пов'язаного з тривалими та цілеспрямованими кібератаками проти державного і критичного секторів.

Стандарт ISO/IEC 27001:2022 задає рамки побудови системи управління інформаційною безпекою на основі ризик-орієнтованого підходу. Організація повинна ідентифікувати свої інформаційні активи, включно з тими, що використовуються гібридними працівниками, оцінити ризики, які виникають у сценаріях віддаленого доступу, використання власних пристроїв, роботи через публічні мережі, та обрати набір контрольних заходів, достатній для зменшення цих ризиків до прийнятного рівня. Подальше удосконалення системи передбачає регулярний перегляд ризиків, результатів аудиту та інцидентів [13].

Розгорнутий опис заходів контролю наведено в стандарті ISO/IEC 27002:2022. У ньому запропоновано оновлену тематичну структуру контролів, яка добре узгоджується із завданнями захисту середовищ із гібридною моделлю роботи [14]. Найбільш релевантними для таких умов є контролі, пов'язані з управлінням ідентифікацією та доступом, журналюванням і моніторингом подій, управлінням конфігураціями та мережевою безпекою, а також реагуванням на інциденти й забезпеченням готовності ІКТ-інфраструктури до підтримання безперервності діяльності. Водночас у багатьох українських організаціях відповідні політики нерідко мають формальний характер, вони або не враховують специфіку гібридної роботи, або не трансформуються у практичні налаштування засобів аутентифікації, віддаленого доступу, мережевої інфраструктури та систем моніторингу.

Концепція Zero Trust, формалізована в документі NIST SP 800-207, ґрунтується на принциповому запереченні попередньої довіри до будь-яких компонентів інформаційної системи, незалежно від їх ролі, розташування чи належності до внутрішнього мережевого середовища. У контексті гібридної моделі роботи це положення набуває особливої важливості, оскільки фізичне перебування користувача в межах корпоративної мережі або факт його підключення до внутрішнього сегмента більше не може розглядатися як достатня підстава для визнання такого доступу безпечним. Традиційна модель безпеки, що пов'язує підвищений рівень довіри з приналежністю до внутрішнього периметра,

поступається підходу контекстно зумовленого прийняття рішень щодо доступу. У межах цього підходу авторизація здійснюється на основі сукупної оцінки ідентичності суб'єкта, поточного стану та керованості пристрою, характеристик сеансу взаємодії, а також рівня чутливості запитуваного ресурсу. Відповідно, політики безпеки мають формалізувати не лише перелік дозволених дій, а й критерії та умови їх виконання, механізми оцінювання контексту доступу, підстави для обмеження або відкликання прав, а також процедури регулярного перегляду й актуалізації таких рішень з урахуванням змін у середовищі та профілі загроз [12].

Важливим джерелом практичних рекомендацій для українських організацій є CERT-UA. Національна команда реагування регулярно публікує аналітичні матеріали і рекомендації, в яких узагальнює досвід відбиття реальних атак, зокрема фішингових кампаній проти державних установ і бізнесу, атак із компрометацією облікових записів у хмарних сервісах, використання вразливостей публічних сервісів та lateral movement у внутрішніх мережах. На основі публічних рекомендацій CERT-UA та Державного центру кіберзахисту можна виокремити кілька базових напрямів підвищення стійкості: повсюдне застосування багатофакторної автентифікації для доступу до критичних сервісів, чітке розмежування прав доступу до внутрішніх ресурсів, мінімізацію або повну відмову від прямого оприлюднення служб адміністрування в мережі Інтернет, централізоване журналювання та кореляцію подій безпеки, а також формалізацію процедур реагування на кіберінциденти.

Узагальнення вимог стандартів і практичних рекомендацій дозволяє виділити кілька груп політик, які є визначальними для безпечної роботи гібридних працівників. Першу групу становлять політики доступу та управління обліковими записами. Вони регламентують повний життєвий цикл облікових записів, порядок надання, модифікації та періодичного перегляду прав доступу, передбачають використання рольової моделі замість індивідуального «ручного» призначення повноважень, а також встановлюють правила управління службовими й адміністративними обліковими записами. В умовах гібридної моделі роботи принциповим є те, що рішення щодо надання доступу має ґрунтуватися насамперед

на ідентичності та ролі користувача, а не на фізичному місці його підключення чи належності до певного мережевого сегмента.

Другим важливим напрямом є політики автентифікації, які визначають вимоги до формування, зберігання та використання паролів, регламентують застосування багатофакторної автентифікації, а також встановлюють механізми періодичної або безперервної перевірки автентичності користувачів. Аналіз інцидентів інформаційної безпеки свідчить, що використання слабких або повторюваних паролів залишається одним із найбільш поширених початкових чинників компрометації облікових записів. Водночас упровадження багатофакторної автентифікації для доступу до електронної пошти, віртуальних приватних мереж, хмарних сервісів та адміністративних інтерфейсів істотно підвищує стійкість організацій до фішингових атак і масового підбору облікових даних. У межах концепції Zero Trust політики автентифікації розглядаються як один із базових інструментів практичної реалізації принципу постійної перевірки суб'єктів доступу незалежно від контексту їх взаємодії з інформаційною системою.

Третю групу становлять політики сегментації та мережевої безпеки, спрямовані на усунення характерної для традиційних підходів помилки, коли вся внутрішня мережа розглядається як однорідне довірене середовище. Такі політики визначають логічну структуру мережі, правила взаємодії між її сегментами, вимоги до застосування захищених каналів зв'язку та технологій VPN, а також порядок ізоляції вузлів, щодо яких є підозра на компрометацію. На практиці в багатьох українських організаціях внутрішня мережа й досі залишається фактично однорідною, із мінімальним рівнем сегментації, що суттєво спрощує зловмиснику переміщення всередині інфраструктури після отримання початкового доступу.

Четвертий блок становлять політики аудиту та журналювання. Вони фіксують вимоги до реєстрації подій на рівні операційних систем, прикладних сервісів і мережевих пристроїв, визначають місце та строки зберігання журналів, порядок доступу до них, а також підходи до їх аналізу та кореляції. Відсутність повноцінного журналювання або фрагментований характер наявних логів

практично унеможливлюють своєчасне виявлення атак у гібридному середовищі й істотно ускладнюють проведення ретроспективних розслідувань інцидентів.

Окремий напрямок становлять політики реагування на інциденти. Вони мають визначати класифікацію кіберінцидентів, порогові значення їх критичності, процедури ескалації, типовий перелік першочергових дій для найбільш поширених сценаріїв (зокрема, фішингові розсилки, підозра на компрометацію облікового запису, виявлення програм-шифрувальників, ознаки витоку конфіденційних даних), а також механізми інформування керівництва та, за потреби, регуляторних органів. Публічні рекомендації CERT-UA можуть розглядатися як важлива практична основа для розроблення таких політик, оскільки спираються на аналіз реальних інцидентів та апробовані на практиці сценарії реагування.

Узагальнюючи, можна констатувати, що сучасні підходи до забезпечення безпечної роботи гібридних працівників ґрунтуються на поєднанні вимог стандартів сімейства ISO/IEC, принципів архітектури Zero Trust та національних рекомендацій профільних органів, зокрема CERT-UA. Їх реалізація має призводити не до формального створення набору документів, а до формування узгодженої системи політик і процедур, які безпосередньо впливають на архітектуру, конфігурацію та повсякденну експлуатацію інформаційних систем організації.

1.3. Підходи до створення політик на основі моделі нульової довіри

Поширення гібридної моделі роботи та зростання використання хмарних сервісів зумовлюють ситуацію, за якої співробітники організацій дедалі частіше здійснюють доступ до корпоративних ресурсів із різних мереж, географічних локацій і з використанням різномірних пристроїв. За таких умов традиційна модель захисту, що ґрунтується на мережевому периметрі та припущенні про довірений характер внутрішнього середовища, втрачає ефективність. Практика сучасних кібератак, орієнтованих на компрометацію облікових записів, механізмів віддаленого доступу, VPN-шлюзів і хмарних ідентичностей, демонструє, що сам факт розміщення ресурсу в межах внутрішньої мережі не може гарантувати належного рівня захисту. Сукупність цих чинників сприяла формуванню та

поширенню підходів до забезпечення інформаційної безпеки, об'єднаних у межах концепції Zero Trust.

Базова ідея Zero Trust полягає в тому, що довіра не надається автоматично жодному користувачу, пристрою або сервісу лише на підставі їхнього розташування у мережі. Кожен запит на доступ розглядається як потенційно небезпечний і підлягає окремій перевірці. У цьому контексті принцип найменших привілеїв набуває практичного значення, користувач отримує тільки ті права, які є необхідними для виконання його службових функцій, і лише на той час, коли ці права необхідні. Для об'єктів інфраструктури це означає відмову від надмірно широких груп доступу та перехід до більш гнучких, у тому числі тимчасових, моделей надання прав.

Іншим важливим елементом є перевірка стану пристрою. Рішення про доступ приймається не тільки на основі того, хто звертається до ресурсу, але й з урахуванням того, з якого саме пристрою здійснюється цей запит і чи відповідає цей пристрій мінімальним вимогам безпеки. У загальному випадку йдеться про актуальність оновлень операційної системи, наявність та працездатність антивірусного рішення, налаштовані механізми блокування робочого столу, увімкнене шифрування дисків та інші заходи, які зменшують ймовірність успішної атаки на кінцеву точку. У низці сучасних рішень для віддаленого доступу, зокрема VPN клієнтів, така перевірка стану кінцевої точки реалізується як невід'ємна частина політик доступу, перед встановленням захищеного тунелю клієнт виконує тестування відповідності пристрою заданому профілю безпеки (posture check), а у разі невідповідності доступ або повністю блокується, або обмежується лише мінімально необхідним набором ресурсів. У гібридній моделі, де один і той самий співробітник може чергувати роботу з корпоративного ноутбука та особистого пристрою, значення цього принципу особливо велике.

Суттєве місце в архітектурі Zero Trust займає багатofакторна автентифікація. Вона розглядається як базовий компонент безпеки для більшості сервісів, корпоративної пошти, внутрішніх веб-ресурсів, VPN доступу, хмарних платформ і адміністративних інтерфейсів. З огляду на те, що більшість цільових атак

починається із фішингових листів та викрадення облікових даних, повсюдне впровадження MFA дозволяє суттєво ускладнити подальший розвиток атаки, навіть у випадку компрометації пароля.

Ще один принцип стосується контекстно-орієнтованого доступу. Доступ до одного і того самого ресурсу може бути дозволений або заборонений залежно від додаткових обставин. Такими обставинами можуть бути дані про географічне розташування користувача, час доби, тип мережі, історія попередніх підключень, обсяг чи характер запитуваних даних. Наприклад, спроба підключення до внутрішньої системи обліку з IP-адреси, яка географічно не відповідає звичній країні чи регіону перебування користувача, може вимагати додаткової перевірки або повністю блокуватися. Таким чином, контекст стає невід'ємним елементом процесу авторизації.

Реалізація Zero Trust неможлива без розвиненого моніторингу та телеметрії. Рішення про доступ, виявлення аномалій, реакція на інциденти спираються на дані про події автентифікації та авторизації, дії користувачів, поведінку пристроїв, мережеві з'єднання, DNS-запити тощо. Ці дані збираються, нормалізуються, корелюються і аналізуються, у тому числі за допомогою систем класу SIEM та поведінкового аналізу. Для гібридної моделі особливо важливо, щоб моніторинг охоплював як внутрішню інфраструктуру, так і хмарні сервіси, які активно використовуються працівниками.

У документі NIST SP 800-207 запропоновано узагальнену референсну архітектуру Zero Trust. Її ядро складають компоненти, відповідальні за прийняття та застосування рішень щодо доступу. Політики й правила безпеки реалізуються у вигляді логіки Policy Engine, який, отримуючи від поінформованих джерел дані про користувача, пристрій, ресурс і контекст, визначає, чи має бути дозволено, обмежено чи заборонено певний запит. Policy Administrator забезпечує технічне втілення цих рішень, трансформуючи їх у конкретні дії для мережевих пристроїв, проксі-серверів, агентів на кінцевих точках та інших засобів контролю. Безпосереднє ж застосування рішень відбувається на рівні точок примусового виконання політики, це можуть бути VPN шлюзи, веб-проксі, мережеві екрани або

програмні агенти, що контролюють доступ до ресурсів на робочих станціях.

Робота такої архітектури може бути описана послідовністю дій. Коли користувач із певного пристрою звертається до корпоративного ресурсу, трафік перехоплюється засобом, який виконує роль точки примусового виконання. До компонента прийняття рішень передається інформація про ідентичність користувача, належність до груп, стан пристрою, тип і чутливість запитуваного сервісу, а також поточний контекст підключення. На підставі заздалегідь визначених політик Policy Engine формує рішення, яке або дозволяє повний доступ, або вводить ті чи інші обмеження, або повністю блокує запит. Це рішення через Policy Administrator доводиться до відповідних технічних засобів. Важливо, що оцінка не обмежується моментом початкової автентифікації: у разі зміни контексту, наприклад, появи аномальної активності, підозрілих мережевих з'єднань чи зміни геолокації, рішення щодо доступу може бути переглянуто вже в ході активної сесії.

У межах корпоративної інформаційної інфраструктури впровадження принципів Zero Trust, як правило, здійснюється поетапно та з урахуванням наявного рівня зрілості системи безпеки. На початковому етапі основна увага зосереджується на переосмисленні ролі ідентичності, яка починає виконувати функцію ключового контрольного елемента доступу, фактично замінюючи традиційний мережевий периметр. Це передбачає централізацію управління обліковими записами, уніфікацію вимог до автентифікації та забезпечення широкого застосування багатофакторної автентифікації для користувачів і привілейованих ролей. На наступному етапі реалізується мікросегментація середовища, у межах якої внутрішня мережа поділяється на логічно ізольовані зони, а взаємодія між ними регламентується правилами, побудованими за принципом найменших привілеїв. Такий підхід істотно обмежує можливості горизонтального переміщення зловмисника в разі компрометації окремих компонентів інфраструктури та підвищує загальну стійкість системи до складних багатовекторних атак.

Наступним кроком стає поглиблення контекстно-орієнтованого доступу.

Якщо на початковому етапі рішення про доступ приймалися здебільшого на основі ролі користувача, то поступово до уваги береться все ширший набір атрибутів, таких як географія, тип і стан пристрою, тип мережі, звичайні патерни поведінки. Паралельно розвиваються засоби моніторингу й аналітики, що дозволяють не лише фіксувати факти доступу, а й виявляти аномалії та автоматично реагувати на них, наприклад, шляхом примусової повторної автентифікації або блокування деяких дій.

Узагальнюючи, можна зробити висновок, що сучасні рішення із забезпечення безпечної роботи гібридних працівників втілюють принципи Zero Trust незалежно від конкретних технологічних платформ. Вони поєднують жорстке управління ідентичностями, оцінку стану пристроїв, багатофакторну автентифікацію, контекстно-орієнтований доступ та розвинений моніторинг. Для подальших розділів ці принципи виступають методологічною основою, на якій будуватиметься опис конкретних технологій та технологічних рішень щодо захисту гібридної роботи.

Висновки до першого розділу

У першому розділі проаналізовано сучасний ландшафт кіберзагроз і визначено ключові фактори, що підвищують ризики для організацій у гібридній моделі роботи: зростання частки ransomware, домінування компрометації ідентичностей як вектора первинного доступу, підвищення ролі експлуатації вразливостей у публічно доступних сервісах і периметрових компонентах, а також посилення загроз, пов'язаних із третіми сторонами та атаками на ланцюжок постачання. Окремо підкреслено актуальність українського контексту, де інтенсивність і спрямованість атак вимагають орієнтації на практичні рекомендації профільних органів реагування та посилення контролю віддалених сценаріїв доступу.

На основі стандартів ISO/IEC 27001:2022 та ISO/IEC 27002:2022 і концепції Zero Trust (NIST SP 800-207) обґрунтовано, що ефективна безпека в умовах гібридної роботи потребує не формального набору документів, а узгодженої системи політик і процедур, які реально відображені в архітектурі та конфігураціях

середовища. Це визначає методологічну основу подальших розділів: формування цільової архітектури та розроблення політик, орієнтованих на керування ідентичностями й доступом, мікросегментацію, контроль стану пристроїв, централізоване журналювання та готовність до реагування на інциденти.

2 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ОРГАНІЗАЦІЇ НА ОСНОВІ МОДЕЛІ НУЛЬОВОЇ ДОВІРИ

2.1. Характеристика інформаційної системи організації та методи атак на неї

У подальшому дослідженні як об'єкт захисту розглядається узагальнена інформаційна система типової організації середнього масштабу, що об'єднує кілька фізичних майданчиків і використовує гібридну модель роботи персоналу. Такий підхід дозволяє уникнути надмірної прив'язки до специфіки конкретної галузі або компанії, зосередившись натомість на характерних архітектурних рішеннях і поширених помилках побудови систем захисту, притаманних значній частині організацій з on-premise-інфраструктурою та віддаленим доступом.

Інформаційна система налічує кілька сотень користувачів та орієнтовно десятків серверів. В основі лежить одна доменна інфраструктура Microsoft Active Directory з єдиним доменом і двома контролерами домену, що забезпечують аутентифікацію та авторизацію користувачів, а також централізоване управління робочими станціями. До домену включені файловий сервер, поштовий сервер, декілька внутрішніх серверів прикладних сервісів та окремий сервер, на якому розміщується веб-сайт організації та частина служб, доступних із мережі Інтернет. Робочі станції представлені переважно клієнтськими ОС сімейства Windows, інтегрованими до домену. Використання інших платформ (Linux, macOS) у цій моделі не розглядається, що спрощує опис, але певною мірою відображає переважаючу на практиці ситуацію.

Мережева топологія включає два основні майданчики, з'єднані між собою захищеним тунелем. На периметрі використовується базова DMZ зона, в якій розміщено окремі публічні сервіси, зокрема веб-сервер та вузол для організації VPN-доступу. Втім, внутрішня мережа в межах кожного майданчика залишається практично не сегментованою: серверні ресурси та робочі станції користувачів знаходяться в загальному адресному просторі з мінімальним рівнем логічної сегментації. Резервне копіювання реалізоване за допомогою виділених серверів або сховищ, проте резервні копії не є ізольованими в повному розумінні цього терміна, оскільки вони доступні з того ж рівня мережі, що й робочі системи, і можуть бути

досяжні у випадку компрометації облікових записів із розширеними правами.

Модель доступу до ресурсів базується на доменних облікових записах користувачів. Співробітники працюють у гібридному режимі: частина часу в офісі, частина віддалено з дому або з інших регіонів, у тому числі за межами основного географічного розташування організації. Віддалений доступ реалізується через VPN клієнт, після встановлення тунелю користувачі отримують можливість підключатися безпосередньо до внутрішніх веб-застосунків або використовувати RDP доступ до робочих станцій чи серверів у внутрішній мережі. Спеціалізованої термінальної станції не розгорнуто, підключення здійснюються безпосередньо до окремих хостів. Для частини співробітників використовуються корпоративні ноутбуки, однак підтримується і модель BYOD. Доступ до внутрішніх ресурсів може здійснюватися з особистих пристроїв, які формально не підпорядковані єдиній політиці безпеки, а вимоги до наявності засобів захисту, оновлень та шифрування на таких пристроях не є жорстко регламентованими.

Публічно доступна частина інфраструктури включає веб-сайт організації, окремі веб-застосунки для взаємодії з контрагентами та партнерськими організаціями, а також поштовий сервер, що приймає та відправляє електронну пошту безпосередньо в Інтернет. Окремого поштового шлюзу безпеки, який здійснював би глибоке фільтрування вкладень, URL посилань і контенту, не використовується. Захист обмежується базовими можливостями поштового сервера та антивірусом на кінцевих точках. Версії окремих публічних сервісів є застарілими, а регулярне оновлення та тестування на вразливості здійснюється епізодично, що створює додаткове вікно можливостей для експлуатації відомих вразливостей з боку зовнішнього злоумисника.

На рівні кінцевих точок використовується традиційна антивірусна система без розширених функцій поведінкового аналізу та XDR. Для частини домашніх пристроїв, які застосовуються у рамках BYOD моделі, жодних централізовано нав'язаних засобів захисту немає; організація покладається на добросовісність користувачів у питаннях оновлення операційної системи, використання засобів захисту та дотримання базових правил інформаційної безпеки. При цьому VPN

доступ надається як із корпоративних, так і з особистих пристроїв, без обов'язкової попередньої перевірки їх відповідності мінімальному профілю безпеки. Механізми перевірки стану кінцевої точки, які можуть бути реалізовані сучасними VPN-клієнтами (posture check, network access control), у даній ІС або не використовуються, або застосовуються у спрощеному варіанті, що не запобігає підключенню потенційно вразливих пристроїв.

Ідентифікація та автентифікація користувачів у більшості випадків здійснюються за допомогою облікових записів домену із застосуванням лише пароля. Багатофакторна автентифікація, за винятком окремих хмарних сервісів або зовнішніх систем, не є обов'язковою вимогою, а її використання для доступу до VPN, RDP та адміністративних інтерфейсів не впроваджено. Низка легасі-компонентів (зокрема підтримка NTLMv1 та SMBv1) лишається ввімкненою через залежність окремих застарілих сервісів, що створює додаткові можливості для атак, пов'язаних із перехопленням та релеюванням облікових даних. Крім того, у файловій інфраструктурі присутні спільні ресурси з надмірно широкими правами доступу, коли великі набори даних доступні практично всім користувачам домену без прив'язки до їхніх реальних службових обов'язків.

Система моніторингу та журналювання у такій організації має обмежений характер. Логування подій залишається переважно на рівні налаштувань «за замовчуванням», журнали зберігаються локально на окремих серверах і робочих станціях, централізований збір та кореляція подій або відсутні, або реалізовані частково. Автоматизоване сповіщення про критичні події безпеки (спроби перебору паролів, аномальну активність облікових записів, нетипові підключення з віддалених регіонів) або не налаштоване, або генерує надмірну кількість хибно-позитивних спрацьовувань, унаслідок чого не використовується в оперативній роботі. У випадку інциденту це суттєво ускладнює як своєчасне виявлення атаки, так і побудову повної картини її перебігу заднім числом, зокрема у гібридних сценаріях, коли частина активності відбувається з домашніх мереж та особистих пристроїв.

Окреслена архітектура формує низку типових векторів атаки. На

зовнішньому периметрі до них належать атаки на служби VPN і RDP методом перебору або масового підбору паролів, використання раніше скомпрометованих облікових записів користувачів, чиї паролі потрапили до публічних баз даних унаслідок витоків з інших ресурсів, а також експлуатація відомих вразливостей у публічних веб-сервісах і мережевих пристроях. Через відсутність багатфакторної автентифікації навіть одноразовий успішний підбір чи повторне використання пароля дає змогу зломиснику отримати VPN-доступ, після чого він опиняється в умовах майже повної відсутності внутрішньої сегментації. Усередині домену додаткові можливості створюють застарілі протоколи та слабка ізоляція серверів, що полегшує використання технік, спрямованих на перехоплення та повторне використання облікових даних, дослідження мережі, переміщення між вузлами й подальшу компрометацію файлових і поштових сервісів. У разі розгортання програм-шифрувальників або інших деструктивних навантажень відсутність ізольованих копій резервних даних збільшує ризик одночасної втрати як робочих систем, так і актуальних резервів.

Таким чином, описувана інформаційна система поєднує риси, характерні для значної частини сучасних організацій з централізованою доменною інфраструктурою та відсутності повноцінної сегментації мережі, змішаною моделлю доступу з використанням як корпоративних, так і особистих пристроїв, наявність публічних сервісів у поєднанні з обмеженою зрілістю процесів управління доступом, журналювання та реагування на інциденти. Сукупність перелічених недоліків формує надмірно вразливий профіль, однак на практиці для реалізації успішної атаки зовнішньому зломиснику часто достатньо лише одного з них, наприклад, відсутності багатфакторної автентифікації на VPN, наявності застарілої вразливої служби на периметрі чи можливості неконтрольованого переміщення всередині однорідної мережі. Окреслені характеристики не є гіперболою опубліковані звіти міжнародних і національних команд реагування на інциденти та мій власний досвід свідчать, що подібний стан справ є цілком типовим як для комерційних організацій, так і для окремих державних установ. У наступних підрозділах на прикладі цієї узагальненої моделі буде розглянуто, яким чином

застосування принципів Zero Trust та формалізованих політик безпеки дозволяє знизити зазначені ризики та підвищити стійкість такої інфраструктури до сучасних кіберзагроз.

2.2. Визначення вимог до системи захисту реалізації Zero Trust

З огляду на модель Zero Trust, архітектура захисту має забезпечувати зменшення ймовірності первинного проникнення, обмеження можливостей розвитку атаки всередині домену, своєчасне виявлення підозрілої активності та здатність до локалізації інцидентів і відновлення працездатності. Відповідно вимоги до комплексу засобів захисту мають формуватися від типових ланцюгів атак для Windows орієнтованих on-premise інфраструктур, описаних у попередніх розділах.

Першочерговим напрямом є підвищення надійності ідентифікації та автентифікації в точках доступу, оскільки у гібридній моделі віддалений доступ фактично визначає межі оперативного периметра організації. У разі використання лише пароля як основного чинника автентифікації компрометація облікових даних через масовий підбір, повторне використання паролів, витоки з зовнішніх ресурсів або фішинг створює безпосередню можливість входу до середовища. Тому необхідним є застосування класу рішень багатофакторної автентифікації як обов'язкового компенсуючого механізму, що суттєво підвищує стійкість до компрометації паролів. Вимоги до такого рішення в межах даної інформаційної системи включають підтримку інтеграції з доменною інфраструктурою, можливість розгортання та експлуатації у локальній моделі, сумісність із типовими сценаріями доступу для Windows орієнтованого середовища, а також підтримку взаємодії з механізмами віддаленого доступу на основі RADIUS для VPN, що дозволить централізовано керувати доступами. Додатково важливими є централізоване адміністрування, можливість диференціації політик за групами користувачів і сервісами, а також ведення журналів подій автентифікації для подальшого використання в системах моніторингу.

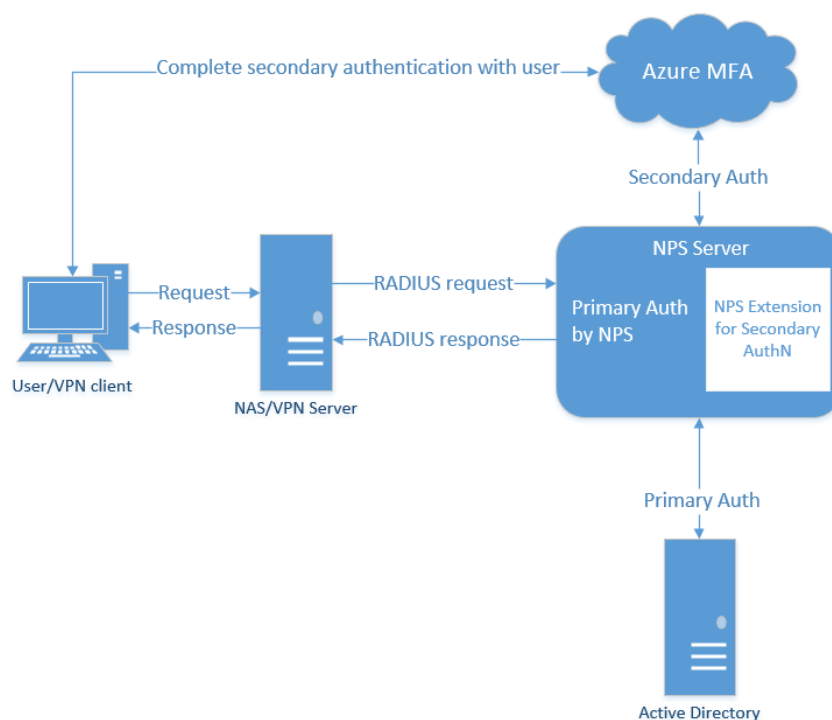


Рис. 2.1 Приклад роботи такої системи за використання Azure MFA

Наступним напрямом є забезпечення керованого захисту кінцевих точок і серверів як основної складової контролю виконання політик безпеки безпосередньо на рівні ресурсів. Оскільки значна частина операційних процесів реалізується через робочі станції та сервери домену, компрометація одного вузла може бути використана як стартова позиція для подальшої ескалації. Для зниження ймовірності зараження, закріплення в системі та масового поширення шкідливого коду необхідним є застосування класу засобів захисту кінцевих точок (EPP/AV або NGAV) як базового рівня захисту. Вимоги до цього класу включають централізоване застосування політик, розмежування політик для серверів і робочих станцій, контроль актуальності модулів захисту та баз, керованість оновлень, а також наявність подій і статусів у форматі, придатному для централізованого збору та аналізу. Окремо для середовищ із віддаленими користувачами актуальною є вимога збереження керованості захисних агентів поза офісною мережею.

Разом із тим для сучасних атак на Windows інфраструктури характерне широке використання легітимних інструментів і вбудованих механізмів операційної системи, що ускладнює їх виявлення виключно засобами класичного антивірусного контролю. У таких умовах доцільним є застосування класу рішень

EDR як засобів розширеного виявлення та реагування на рівні хоста. Вимоги до EDR у межах даної інформаційної системи передбачають збір деталізованої телеметрії про виконання процесів, підозрілі ланцюги запуску, мережеві з'єднання з кінцевої точки, зміни критичних налаштувань та прояви закріплення в системі. Важливою складовою є можливість підтримки розслідувань інцидентів і виконання дій реагування, зокрема обмеження взаємодії вузла з мережею або припинення підозрілих процесів. Для організації середнього масштабу додатковою вимогою виступає прийнятний рівень експлуатаційної складності та можливість використання без розгортання повноцінного центру моніторингу з високими витратами.

Ефективність вищезазначених класів засобів суттєво залежить від наявності платформи централізованого керування захистом, оскільки за відсутності єдиного механізму застосування політик і контролю їх виконання неминуче виникає неоднорідність налаштувань і втрачається цілісність управління. Тому необхідним є клас платформ централізованого керування, які забезпечують інвентаризацію вузлів, розгортання та контроль агентів, ієрархічне застосування політик, делегування повноважень адміністраторам, а також консолідацію статусів і подій. Вимоги до таких платформ в даній інформаційній системі включають підтримку роботи з віддаленими вузлами, механізми контролю відповідності встановленим профілям безпеки та здатність інтегрувати події з іншими системами моніторингу.

Окремою складовою, що впливає з гібридної моделі роботи та поступового обмеження використання непідконтрольних пристроїв, є контроль допуску кінцевих точок до віддаленого доступу. Надання VPN-доступу пристроям без перевіреного профілю безпеки підвищує ризики, пов'язані з компрометацією домашніх середовищ і некерованих конфігурацій. Тому доцільним є впровадження вимоги, відповідно до якої доступ до внутрішніх ресурсів надається корпоративним пристроям, що перебувають під централізованим управлінням, мають актуальний стан оновлень і встановлені засоби захисту, а також відповідають визначеним політикам безпеки. У технічній частині це може вимагати застосування механізмів перевірки відповідності пристрою мінімальному профілю

безпеки перед наданням доступу або організаційно-технічної моделі видачі доступів, у якій керованість пристрою є обов'язковою умовою.

Оскільки в попередніх підрозділах визначено наявність публічних сервісів і поштового обміну без спеціалізованого глибокого фільтрування, окремим необхідним напрямом є захист поштового контуру як одного з основних каналів первинної компрометації через фішингові кампанії та доставку шкідливих вкладень і посилок. У таких умовах доцільним є застосування класу засобів поштової безпеки, здатних забезпечувати перевірку вкладень, аналіз посилок, контент-фільтрацію та формування подій, що можуть бути використані для централізованого моніторингу. Вимоги до цього класу включають сумісність із локальною поштовою інфраструктурою, централізоване керування політиками перевірки й журналювання, а також можливість інтеграції подій із загальним контуром спостережуваності.

У частині мережевих ризиків визначальною є обмежена сегментація внутрішньої мережі, що знижує здатність локалізувати інциденти та обмежувати переміщення зловмисника. Це обумовлює необхідність застосування класу мережевих міжмережевих екранів і шлюзів віддаленого доступу як засобів контролю периметра, реалізації VPN, а також впровадження політик доступу між сегментами. Вимоги до цього класу включають підтримку сегментації на рівні зон довіри, детальне керування правилами доступу між сегментами, можливість інтеграції з доменними механізмами авторизації, журналювання мережевих подій і забезпечення керованого віддаленого доступу. У контексті Zero Trust принциповим є те, що мережевий контроль має застосовуватися не тільки на межі з Інтернетом, а також у внутрішніх напрямках між користувацьким сегментом, серверними зонами та DMZ.

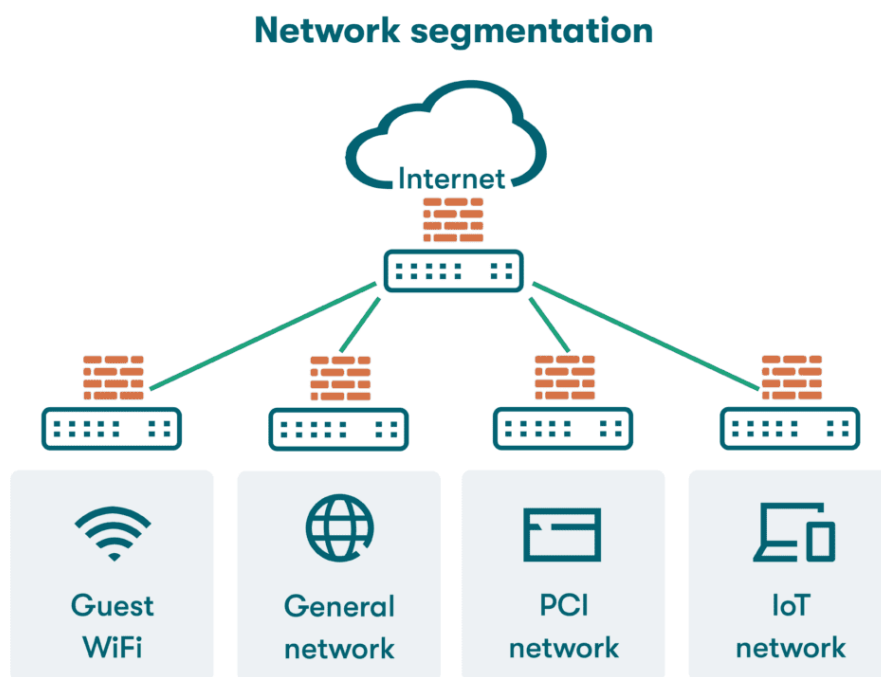


Рис. 2.2 Приклад базової сегментації мережі

Додатково, для підвищення рівня спостережуваності та незалежної детекції мережових атак, доцільним є використання класу засобів мережевого аналізу та виявлення (IDS/IPS або NDR), які забезпечують виявлення характерних ознак експлуатації вразливостей, підозрілої активності в трафіку та потенційних командно-керуючих з'єднань. Вимоги до цього класу включають можливість розміщення на периметрі та/або на межі ключових сегментів, підтримку актуалізації правил детекції, керованість порогів спрацювань для зменшення хибнопозитивних подій, а також формування повідомлень у форматі, придатному для подальшої централізації та кореляції.

Важливою передумовою реалізації принципів Zero Trust у розглянутій інформаційній системі є побудова централізованого моніторингу, оскільки фрагментоване зберігання журналів і відсутність кореляції подій не дозволяють своєчасно виявляти інциденти та відтворювати послідовність дій зломисника. У зв'язку з цим необхідним є клас засобів централізованого збору, зберігання та кореляції подій, тобто базова SIEM складова або централізована система керування журналами з функціями сповіщення. Вимоги до цього класу визначаються необхідністю інтеграції подій із доменної інфраструктури, засобів захисту кінцевих

точок і EDR, периметрових систем і віддаленого доступу, а також засобів мережевого аналізу. Система має забезпечувати узгодження подій за часовими параметрами, користувачами та вузлами, а також підтримувати формування сповіщень щодо подій, що мають підвищений рівень ризику.

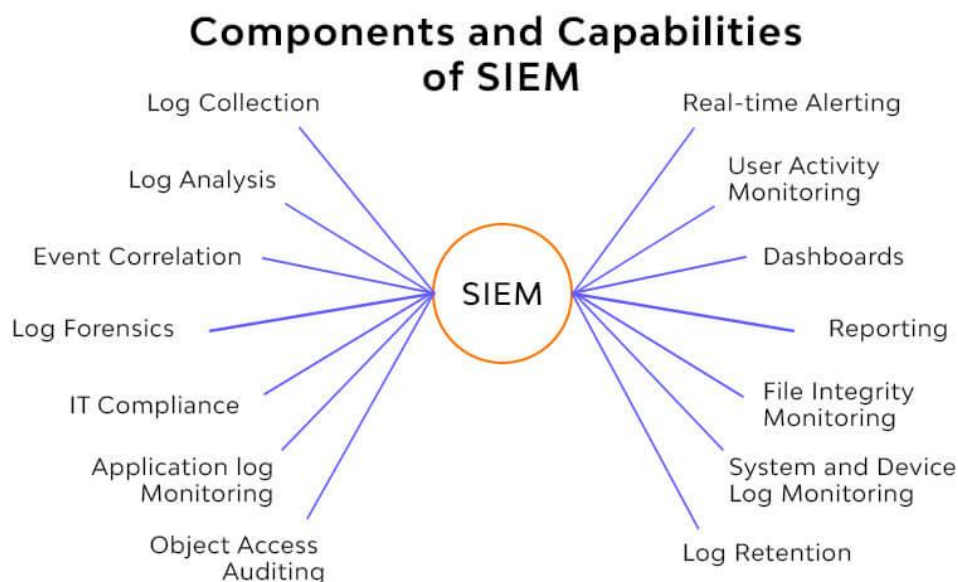


Рис. 2.3 Можливості SIEM систем

Окремо доцільно визначити вимогу створення захищеного репозиторію журналів з обмеженням прав запису на рівні *only upload*, а також з посиленням режимом адміністративного доступу, що знижує ризики знищення або модифікації журналів у разі інциденту.

З огляду на характеристики резервного копіювання, де резерви можуть бути доступними в межах того ж доменного середовища, необхідною є модернізація підходів до резервного копіювання і відновлення з забезпеченням ізоляції принаймні одного рівня резервів. Отже потрібним є клас засобів резервного копіювання та відновлення, доповнений вимогами до ізоляції резервного фонду від доменної інфраструктури та обмеження адміністративного доступу до резервного контуру. У рамках даної моделі це доцільно формалізувати як наявність процедурно-технічного механізму, що забезпечує фізичне або логічне відокремлення частини резервів від робочого середовища, а також як вимогу мінімізації прав облікових записів, що виконують операції копіювання, і посилення контролю доступу до серверів резервного копіювання.

Окремо визначальною є потреба у системному керуванні вразливостями та оновленнями, оскільки епізодичне оновлення публічних і внутрішніх сервісів створює умови для експлуатації відомих вразливостей. У зв'язку з цим необхідним є клас засобів керування вразливостями та версіями, який забезпечує інвентаризацію активів, регулярне оцінювання стану щодо відомих вразливостей, пріоритизацію усунення за рівнем ризику та контроль факту застосування оновлень. Для організації середнього масштабу важливою є практична здійсненність процесу та його сталість у часі, що потребує формалізації порядку перевірок і відповідальності за усунення виявлених дефектів.

Поряд із технічними засобами, реалізація зазначених вимог потребує супровідних організаційних заходів, без яких навіть сучасні рішення не забезпечують необхідної стійкості. До таких заходів доцільно віднести запровадження та обов'язкове виконання політики віддаленого доступу і допуску пристроїв із орієнтацією на керовані корпоративні вузли; впровадження рольової моделі доступу до інформаційних ресурсів та періодичного перегляду прав доступу; плановий перехід від застарілих протоколів і компонентів через керовану міграцію залежностей; формалізацію вимог до журналювання та реагування на інциденти, включно з визначенням джерел подій, строків зберігання, критеріїв критичності та процедур реагування; а також регламент резервного копіювання й відновлення із визначенням вимог до ізоляції резервів, порядку контролю доступу та перевірок відновлюваності резервних копій.

2.3. Проектування архітектури Zero Trust для інформаційної системи організації та вибір рішень захисту

Проектування архітектури здійснюється з урахуванням того, що інформаційна система є Windows орієнтованою та базується на локальній доменній інфраструктурі Active Directory, що забезпечує централізовану ідентифікацію та керування ресурсами. Додатковими чинниками, які впливають на побудову захисту, є наявність публічних сервісів у DMZ, потреба в організації віддаленого доступу для гібридної моделі роботи, а також необхідність підвищення спостережуваності середовища за рахунок централізованого збору й кореляції

подій. За таких умов підхід нульової довіри розглядається як спосіб упорядкування доступів і контролів безпеки таким чином, щоб перевірка доступу та виконання політик відбувалися не лише на периметрі, а й на рівні ресурсів, ідентичностей та мережових взаємодій.

Також передумовою є наявність двох фізичних майданчиків, об'єднаних захищеним міжмайданчиковим з'єднанням, тунелем, а також єдина доменна інфраструктура Active Directory з одним лісом і доменом та двома контролерами домену для забезпечення відмовостійкості. Між майданчиковий зв'язок розглядається як транспортний канал, що забезпечує зв'язаність середовища, однак не формує підвищеного рівня довіри. Хмарні сервіси в межах архітектури не розглядаються, всі ключові компоненти безпеки плануються до розгортання в локальній інфраструктурі.

Архітектура нульової довіри для даного середовища проектується як сукупність взаємопов'язаних контролів на рівні ідентичностей, кінцевих точок, мережових взаємодій та моніторингу, що забезпечують явну перевірку кожного доступу, надання прав за принципом найменших привілеїв і припущення можливості компрометації окремих елементів. Практична реалізація цих принципів у Windows орієнтованій on-premise інфраструктурі досягається насамперед через логічний поділ середовища на зони з різним рівнем довіри та через модель доступу, у якій за замовчуванням відсутні широкі мережеві дозволи, а всі необхідні взаємодії визначаються явно.

Цільова мережева модель передбачає виділення окремих логічних зон (сегментів) для публічних сервісів, для користувацьких робочих станцій, для контролерів домену, для серверних ресурсів, для віддаленого доступу, для серверів безпеки та для резервного копіювання. З огляду на підвищені вимоги до ізоляції публічних компонентів, DMZ зона проектується з деталізацією щонайменше до рівня окремого сегмента для кожного веб-застосунку або публічного сервісу, що дозволяє обмежувати взаємодії кожного такого сервісу лише необхідними внутрішніми напрямками. Для серверної частини доцільним є логічне розділення щонайменше до рівня сегментації, у якому на один сервер виділено один сегмент,

коли сервери що мають ризики компрометації ізольовані від іншого середовища. Контролери домену виділяються в окремий сегмент із жорстко обмеженими правилами доступу з інших зон, зокрема з користувацьких і DMZ зон.

Функції маршрутизації та мережевого контролю в кожному майданчику доцільно покласти на периметровий шлюз, який одночасно виконує роль міжмережевого екрана та вузла віддаленого доступу. У об'єктній моделі передбачається по одному такому шлюзу на кожному майданчику з подальшим об'єднанням мереж через тунель. Політика міжзонних взаємодій задається за принципом білого списку з базовим правилом заборони іншого. Це означає, що користувацький сегмент отримує доступ лише до тих серверних ресурсів, які потрібні для виконання службових обов'язків, а доступ до інших зон блокується. Аналогічно, DMZ зона має строго визначені напрями доступу до внутрішніх сервісів, необхідні для роботи публічних застосунків, без можливості широкої взаємодії з внутрішнім середовищем. Міжмайданчикові взаємодії також підпорядковуються цій моделі, наявність тунелю не розширює дозволи автоматично, а лише створює транспорт для вже визначених правил між сегментами.

Окремим елементом цільової архітектури є віддалений доступ у гібридній моделі роботи. У рамках Zero Trust віддалений доступ розглядається як контрольована точка входу, де автентифікація та авторизація мають бути посилені, а мережеві маршрути мінімізованими. Проектом передбачається організація VPN доступу через відкритий і безпечний протокол на периметровому шлюзі з використанням різних профілів для різних груп користувачів. Такі профілі відрізняються не лише обліковими групами, а й доступними маршрутами, користувачам надаються лише ті мережеві напрямки, які потрібні для роботи, без надмірного доступу до внутрішньої мережі. Для сценаріїв, де співробітники використовують прикладні системи без веб-інтерфейсу, передбачається контрольований доступ до прикладного сервера через RDP у межах дозволених маршрутів і політик, з урахуванням того, що прямі широкі RDP-доступи до довільних хостів всередині мережі не допускаються.

Критичною умовою віддаленого доступу є впровадження багатofакторної автентифікації як обов'язкової вимоги. У цільовій архітектурі для цього використовується окреме рішення класу MFA, інтегроване з доменною інфраструктурою та з механізмом авторизації VPN через RADIUS. Таким чином, під час встановлення VPN з'єднання користувач проходить автентифікацію з додатковим фактором, а контроль доступу реалізується централізовано для визначених груп користувачів і визначених сервісів. Це дозволяє розглядати компрометацію пароля як недостатню умову для отримання доступу до внутрішнього середовища, що відповідає принципу явної перевірки доступу в Zero Trust-моделі.

У межах проектування також закріплюється підхід до поступового відходу від підключень з невідконтрольованих пристроїв. Віддалений доступ має надаватися переважно з корпоративних кінцевих точок, які перебувають під централізованим управлінням і відповідають встановленому профілю безпеки. У контексті архітектури верхнього рівня це означає, що контроль доступу розглядається у зв'язці користувач, пристрій, контекст, де пристрій має бути керованим, мати актуальний стан оновлень і встановлені засоби захисту. Конкретні механізми перевірки відповідності пристрою профілю безпеки та порядок надання/відкликання доступів доцільно деталізувати на етапі розроблення політик і технології їх впровадження.

Наступним ключовим блоком Zero Trust-архітектури є керований захист робочих станцій і серверів, який забезпечує контроль виконання політик безпеки безпосередньо на вузлах і формує телеметрію для виявлення підозрілої активності. У об'єктній моделі для цього обирається платформа централізованого керування захистом із розгортанням агентів на всіх робочих станціях і серверах, а також компонент захисту вузлів (EPP) для базового багатoshарового запобігання шкідливим впливам. Центральні сервери керування та безпекові сервіси розміщуються в окремому сегменті серверів безпеки, що відокремлює їх від користувацького трафіку і дозволяє застосовувати посилені правила доступу.

З урахуванням сучасних сценаріїв атак на Windows-інфраструктури, де

значну роль відіграє зловживання легітимними інструментами та прихована ескалація привілеїв, базового EPP-рівня недостатньо для забезпечення спостережуваності. Тому в архітектурі передбачається застосування EDR рішення, яке збирає розширену телеметрію з кінцевих точок і серверів, підтримує виявлення аномалій та надає можливості реагування на рівні хоста. EDR сервер розміщується в сегменті серверів безпеки та інтегрується з платформою централізованого керування захистом, формуючи єдину адміністративну площину для політик і подій. Такий підхід дозволяє розглядати агент на кінцевій точці як механізм виконання політик і джерело контексту для прийняття рішень щодо інцидентів, що практично реалізує принцип перевірки на рівні ресурсу, характерний для Zero Trust архітектури.

Для забезпечення мережевої видимості та незалежного від кінцевих точок джерела детекції в архітектурі передбачається використання IDS компонента. Сенсор IDS доцільно розміщувати як елемент у сегменті серверів безпеки із підключенням до копії трафіку периметра та/або між ключовими логічними зонами. Така побудова дозволяє фіксувати ознаки експлуатації вразливостей, підозрілі мережеві патерни та потенційні командно-керуючі взаємодії як додатковий контур спостережуваності. Події IDS формуються у форматі, придатному для централізованого збору й кореляції. Після створення всіх необхідних виключень для інфраструктури буде логічним переключити IDS в режим IPS.

Централізований моніторинг і кореляція подій реалізуються шляхом розгортання SIEM платформи в сегменті серверів безпеки та підключення до неї ключових джерел телеметрії. Передбачається щонайменше одна центральна SIEM нода з агентами на серверах і з прийманням подій через syslog від мережевих та моніторингових компонентів та через агенти інтегратори. До обов'язкових джерел подій належать контролери домену та доменні служби, серверні вузли, периметрові шлюзи, IDS компонент, а також події з платформи захисту кінцевих точок і EDR компонента. Строк зберігання подій у межах SIEM контуру визначається на рівні 90 днів, що забезпечує достатню ретроспективу для розслідування інцидентів і аналізу повторюваних загроз у гібридних сценаріях.

У межах проектування визначається орієнтовний перелік прикладних сценаріїв виявлення, які демонструють практичне застосування централізованого моніторингу в архітектурі нульової довіри. Зокрема, доцільним є контроль нетипових підключень віддаленого доступу, коли під час встановлення VPN з'єднання SIEM отримує параметри сесії, включно з адресою джерела, виконує її оцінювання за географічною ознакою та формує сповіщення у випадках підключень з нетипових регіонів, зокрема поза межами визначеного допустимого пулу. Подібні сценарії можуть доповнюватися кореляцією з подіями автентифікації у домені, з подіями EDR на кінцевих точках та з сигналами IDS, забезпечуючи зв'язність доказової бази при розслідуванні.

Окремим контуром у цільовій архітектурі є резервне копіювання та відновлення, оскільки в базовій моделі середовища резерви не мають достатньої ізоляції від доменної інфраструктури. У проектній архітектурі резервний контур виділяється в окремий сегмент, а сервер резервного копіювання планується як ізольований вузол, розміщений поза середовищем віртуалізації, з обмеженим доступом і мінімально необхідними правами для виконання операцій копіювання. Як базовий підхід розглядається періодичне формування резервів шляхом знімків (snapshot) або експорту образів серверів у віртуалізованому середовищі з подальшим зберіганням на ізольованому файловому сховищі, що не є частиною платформи віртуалізації та не підпорядковується звичайним адміністративним сценаріям доменного доступу. Періодичність повного дублювання у межах даної моделі визначається як тижнева, з урахуванням компромісу між обсягами даних і вимогами до відновлення. Архітектурно важливим є те, що резервний контур розглядається як окрема зона з підвищеним рівнем захисту, а порядок доступу до нього має бути формалізований політикою (включно з обмеженням адміністративних операцій та посиленням автентифікації).

На рівні доменної інфраструктури в архітектурі закріплюються базові принципи управління ідентичностями та привілеями. Передбачається розділення адміністративних ролей щонайменше на доменних адміністраторів і адміністраторів окремих сервісів/серверів з делегованими правами, що зменшує

масштаб наслідків компрометації облікового запису та підтримує принцип найменших привілеїв. Для підвищення стійкості до атак на автентифікацію доцільно визначити цільовий стан політик паролів і блокувань (захист від масового підбору та повторюваних спроб входу), а також цільовий стан відмови від застарілих протоколів і механізмів взаємодії, зокрема NTLMv1 і SMBv1, з поетапним приведенням середовища до сучасних безпечних конфігурацій. Додатково в цільовій архітектурі фіксується централізоване керування оновленнями робочих станцій через доменні політики, зокрема в частині примусового застосування автоматичних оновлень операційної системи на всіх корпоративних вузлах.

Висновки до другого розділу

У другому розділі охарактеризовано узагальнену інформаційну систему організації середнього масштабу з доменною інфраструктурою Active Directory, двома майданчиками, DMZ для публічних сервісів і гібридною моделлю роботи персоналу. Показано, що поєднання слабкої сегментації, парольної аутентифікації без обов'язкової MFA, наявності публічно доступних компонентів, часткового використання BYOD та обмеженої спостережуваності формує типові вектори атак: компрометацію облікових записів і віддаленого доступу, експлуатацію вразливостей периметра, подальше горизонтальне переміщення в однорідній внутрішній мережі та ураження критичних сервісів і резервних копій.

На основі принципів Zero Trust сформовано вимоги до системи захисту та спроектовано цільову архітектуру, що орієнтована на явну перевірку доступів, мінімізацію привілеїв і припущення можливості компрометації окремих компонентів. Запропонований підхід передбачає посилення автентифікації (MFA для VPN/RDP та привілейованих сценаріїв), відхід від некерованих пристроїв, логічну сегментацію середовища на зони (користувачі, сервери, DC, DMZ, безпекові сервіси, резервне копіювання) із правилами взаємодії за принципом білого списку, керований захист кінцевих точок і серверів (EPP/EDR), розгортання IDS для мережевої видимості, централізоване журналювання та кореляцію подій у SIEM, а також ізоляцію резервного контуру й формалізацію процесів оновлень та

управління вразливостями. Це створює практичну основу для подальшого розділу, де вимоги архітектури трансформуються в конкретні політики та технологію їх реалізації.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ СТВОРЕННЯ ПОЛІТИК БЕЗПЕКИ НА ОСНОВІ МОДЕЛІ НУЛЬОВОЇ ДОВІРИ

3.1. Варіант технології побудови політик безпеки в умовах Zero Trust

Запропонована технологія формування політик інформаційної безпеки ґрунтується на принципах Zero Trust та орієнтована на узагальнену організацію середнього масштабу з гібридною моделлю роботи та локальною доменною інфраструктурою. Вихідні умови передбачають наявність від 2 до 5 фізичних майданчиків, об'єднаних захищеним тунелем, використання DMZ для публічних сервісів і необхідність організації віддаленого доступу через VPN, а також підвищення спостережуваності середовища шляхом централізованого збору, зберігання та кореляції подій безпеки.

Технологія спрямована на досягнення цільового стану, в якому надається лише мінімально необхідний, постійно верифікований доступ до ресурсів, а мережеві взаємодії визначаються явно за принципом білого списку. Доцільним є логічний поділ середовища на зони з різним рівнем довіри (користувацький сегмент, серверний сегмент, контролери домену, DMZ, сегменти безпекових сервісів, резервного копіювання тощо) із жорстким контролем міжзонних правил і мінімізацією транзитивної довіри між компонентами.

У межах цього підрозділу політики формулюються як вимоги, правила та організаційні процедури. Практична реалізація зазначених політик засобами конкретних програмних продуктів і налаштувань розглядається окремо в підрозділі 3.2.

3.1.1. Політики доступу та керування обліковими записами

Метою політик доступу є зниження ризиків компрометації ідентичностей та ескалації привілеїв, забезпечення керованого життєвого циклу облікових записів і впровадження принципу найменших привілеїв у межах усіх компонентів інформаційної системи.

У межах інформаційної системи впроваджується рольова модель (RBAC) із поділом користувачів щонайменше на такі групи:

- офісні користувачі;

- користувачі з підвищеними правами (наприклад, бухгалтери з доступом до окремих серверів або віртуальних робочих місць, керівники команд);
- адміністратори інфраструктури (сервери, віртуалізація, мережа);
- адміністратори безпеки (керування засобами захисту, моніторингом та політиками);
- головні адміністратори (рівень Tier-0 із доступом до критичних компонентів домену та керувальних систем).

Права доступу надаються переважно через групи Active Directory із мінімізацією широких дозволів, заборонаю нецільових членств у привілейованих групах та явним описом доступних ресурсів для кожної ролі (файлові сервери, пошта, прикладні сервіси, доступ до визначених вузлів за RDP тощо). Періодичний перегляд прав доступу є обов'язковою процедурою. Доцільним є диференційований підхід: для привілейованих доступів перегляд проводиться щокварталу, для стандартних ролей раз на пів року, а також позапланово у разі інцидентів або організаційних змін.

Встановлюються вимоги до паролів: мінімальна довжина 16 символів, високі вимоги до складності, заборона повторного використання щонайменше трьох попередніх паролів. Рекомендується застосування генерації паролів та їх зберігання в менеджерах паролів, що відповідають сучасним практикам безпеки. Обов'язкове застосування багатофакторної автентифікації передбачається для віддаленого доступу через VPN, для адміністративних підключень, для доступу до серверів за RDP, а також для входу в операційну систему у випадках, що мають підвищений ризик (насамперед для привілейованих ролей і привілейованих робочих станцій). Дозволяються сучасні методи підтвердження, зокрема push-сповіщення та TOTP.

Для всіх адміністративних ролей запроваджується розділення облікових записів: окремий користувацький акаунт для повсякденної діяльності та окремий адміністративний акаунт для виконання привілейованих операцій. Використання адміністративних акаунтів обмежується визначеними вузлами та сегментами, а також підлягає посиленому логуванню. Рекомендується створювати і

використовувати такі акаунти лише за необхідності.

Користувачі не повинні мати прав локального адміністратора на робочих станціях. Для технічних потреб адміністрування застосовується централізоване керування локальними адміністративними паролями (підхід класу LAPS) і принцип тимчасового підвищення привілеїв лише за обґрунтованої необхідності.

Життєвий цикл облікового запису (Joiner–Mover–Leaver). Процес створення, зміни та деактивації облікових записів має бути формалізованим і відтворюваним. Для сценарію звільнення передбачається узгоджена взаємодія адміністративної та безпекової функцій: адміністратори виконують деактивацію/видалення акаунта в домені та залежних системах, тоді як служба безпеки забезпечує фіксацію події у системі моніторингу, підтримує контроль на спроби реактивації відключеного акаунта та налаштовує детектування аномальних дій, пов'язаних із таким обліковим записом.

3.1.2. Політики захисту кінцевих точок та серверів

Метою політик захисту кінцевих точок і серверів є встановлення єдиного базового безпечного стану для Windows-інфраструктури, зменшення площини атаки та підвищення стійкості до поширених векторів компрометації.

Визначається обов'язкова наявність керованого засобу захисту кінцевих точок із можливістю проактивного виявлення та блокування шкідливої активності, зокрема поведінкових ознак шифрувальників і спроб вимкнення захисту. Налаштування політик захисту мають бути максимально наближеними до агресивного профілю для критичних сценаріїв, із контрольованими винятками для легітимних бізнес-процесів.

У межах технології встановлюється вимога до відключення або обмеження використання застарілих протоколів і механізмів автентифікації/обміну, що підвищують ризик компрометації та lateral movement. Винятки допускаються лише через формалізований процес, із визначенням строків дії та компенсуючих контролів.

Оновлення операційних систем і базового програмного забезпечення виконуються централізовано. Доцільно застосовувати короткий етап попереднього

тестування (до 24 годин) із подальшим розгортанням оновлень, пріоритизуючи вузли на периметрі, у DMZ та критичні сервери. Окремо визначається процес моніторингу вразливостей та оперативного реагування на критичні CVE, що стосуються публічних сервісів і компонентів віддаленого доступу. За це може відповідати окремий автоматичний компонент системи захисту.

Дозволяється використання флеш-накопичувачів із обов'язковим скануванням, тоді як інші типи периферійних пристроїв забороняються за замовчуванням. Надання винятків здійснюється через адміністратора за погодженням представника відділу кібербезпеки та документуванням причин.

Макроси в офісних документах блокуються за замовчуванням; дозволи надаються лише у визначених випадках за принципом мінімізації ризику (наприклад, через використання підписаних макросів або довірених розташувань). Веб-доступ підлягає посиленій фільтрації з орієнтацією на блокування шкідливих і високоризикових категорій, із журналюванням подій блокування для подальшого аналізу.

Сервери підлягають окремому підходу, що включає мінімізацію встановлених компонентів, обмеження адміністративних інтерфейсів, посилене журналювання та контроль віддалених підключень. Доступ до серверів за RDP допускається лише для визначених ролей та за умови багатофакторної автентифікації. Для бізнес-процесів (наприклад, бухгалтерії) допускається доступ до окремих серверів або віртуальних робочих місць за умови формального опису необхідності, обмеження кола користувачів і застосування додаткових засобів контролю.

3.1.3. Політики автентифікації та віддаленого доступу

Метою політик віддаленого доступу є зведення точок входу до контрольованих, верифікованих і моніторингових сценаріїв, зменшення ризику компрометації через VPN та забезпечення доступу лише з корпоративних керованих пристроїв.

З'єднання між фізичними майданчиками реалізується захищеним тунелем на транспортному рівні (наприклад, IPSec) із обмеженням дозволених мережевих

взаємодій між сегментами за принципом білого списку. Такі з'єднання не мають бути привілейовані, і підлягати загальній системі перевірки та верифікації.

Віддалений доступ надається гібридним працівникам і здійснюється через VPN. Доцільним є використання повного тунелю (маршрутизація всього трафіку через корпоративний периметр) для забезпечення єдиних політик фільтрації, моніторингу та зниження ризику обходу контролів.

Доступ через VPN надається лише з корпоративних керованих пристроїв, що відповідають мінімальним вимогам безпеки. Передбачаються перевірки наявності та актуального стану засобу захисту, а також факту нещодавнього успішного підключення кінцевої точки до серверів керування. При невиконанні умов доступ блокується або переводиться в обмежений режим.

Після встановлення VPN з'єднання доступ обмежується переліком дозволених сервісів, необхідних для виконання робочих завдань. Адміністративні сегменти, серверні зони та критичні компоненти домену доступні лише з привілейованих робочих станцій і з багатофакторною аутентифікацією, прямий доступ із користувацького сегмента до критичних зон забороняється.

Підключення з територій поза дозволеного регіону, скажімо України, має розглядатися як подія підвищеного ризику та підлягає детектуванню, сповіщенню та додатковій перевірці. Політика може передбачати як попереджувальний режим, так і обмежувальний режим залежно від допустимого рівня ризику.

3.1.4. Політики виявлення та реагування на інциденти

Метою цього блоку політик є забезпечення спостережуваності інфраструктури, своєчасного виявлення атак і формалізованого реагування на інциденти, зокрема на компрометацію облікових записів, lateral movement та ransomware-атаки.

Визначається перелік джерел подій безпеки, що мають передаватися до централізованої системи збору та кореляції: доменна інфраструктура, VPN, сервери і робочі станції, публічні сервіси та компоненти в DMZ, мережеві події від засобів класу IDS/IPS, події засобів захисту кінцевих точок. Події зберігаються щонайменше 90 днів. Додатково фіксується вимога синхронізації часу на

критичних вузлах (зокрема на контролерах домену) для забезпечення коректного розслідування.

Пріоритетні сценарії детекції. Мінімальний набір правил детектування має охоплювати:

- аномалії автентифікації (багаторазові невдалі спроби, нетиповий час, зміна географії підключень);
- підвищення привілеїв і нетипові адміністративні дії в домені;
- ознаки lateral movement (нетипові RDP/SMB-з'єднання, використання адміністративних інструментів за нетипових умов);
- використання застарілих протоколів або спроби їх активації;
- поведінкові ознаки ransomware та спроби саботажу засобів захисту.

Реагування формалізується через розподіл ролей і ескалацію, первинний аналіз та стримування виконує чергові адміністратор та працівник відділу безпеки, подальші рішення головний адміністратор із залученням голови команди кібербезпеки за потреби. Для критичних інцидентів пріоритетною дією визначається ізоляція ураженої кінцевої точки або сервера засобами захисту, блокування скомпрометованих облікових записів і зупинка поширення в межах сегментів. Усі інциденти підлягають фіксації та документуванню з подальшим урахуванням результатів під час перегляду політик.

3.2. Приклад реалізації політик безпеки на базі обраних програмних продуктів

У цьому підрозділі наведено приклад того, як вимоги та правила, сформульовані у підрозділі 3.1, можуть бути реалізовані засобами обраного набору інструментів. Акцент зроблено не на процесі розгортання програмних компонентів, а на підході до їх конфігурації, логічній організації політик, структурі груп і прикладах налаштувань, які забезпечують досягнення цільового стану безпеки. Запропонований опис має демонстраційний характер і може бути адаптований залежно від складу активів, критичності сервісів, вимог безперервності бізнесу та результатів тестування сумісності з прикладними системами.

Для реалізації прикладу використано такі складові:

- ESET PROTECT як централізований інструмент керування політиками

та станом захисту;

- ESET Endpoint Security для робочих станцій;
- ESET Server Security для серверів;
- ESET Secure Authentication для багатофакторної автентифікації;
- ESET Full Disk Encryption для шифрування ноутбуків;
- механізми Active Directory та Group Policy Objects як базовий рівень керування Windows-середовищем;
- Suricata в режимі IDS як мережевий шар виявлення атак і підозрілої активності, із передаванням подій до платформи SIEM (без деталізації SIEM у цьому підрозділі).

Були обрані такі рішення спираючись на досвід в їх практичному використанні та високій доведеній ефективності.

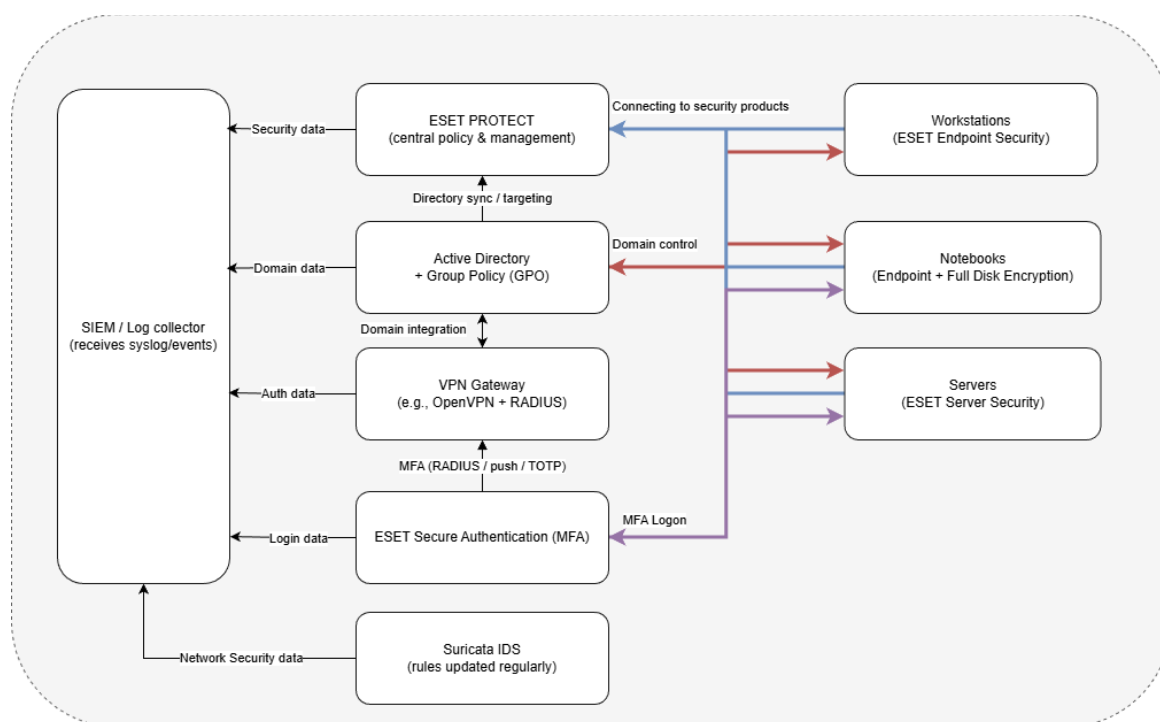


Рис. 3.1 Принципова схема взаємодії об'єктів системи та її компонентів

3.2.1. Організація керування ESET PROTECT та інтеграція з Active Directory

У запропонованому прикладі ESET PROTECT використовується як централізована точка керування політиками, інвентаризацією агентів, та ініціюванням реакцій на інциденти. Інсталяційні кроки та розгортання інфраструктури не розглядаються; натомість описується логіка організації керування, що забезпечує керованість, масштабованість і відповідність політикам.

Завдяки інтеграції платформи ESET PROTECT з Active Directory досягається уніфікація таргетингу політик, та спрощення моделі адміністрування, оскільки рольовий доступ в ESET PROTECT доцільно організовувати у відповідності до організаційних ролей та принципу найменших привілеїв.

Для практичної керованості доцільно застосовувати поєднання статичних і динамічних груп:

- статичні групи відображають організаційну структуру і автоматично синхронізуються з Active Directory;
- динамічні групи формуються за статичними чи динамічними атрибутами хоста, такими як тип операційної системи чи наявність продуктів захисту, та використовуються для автоматизації застосування політик і контролю відповідності.

Практично доцільно мати щонайменше такі логічні групи:

- workstations (стаціонарні робочі станції);
- notebooks (ноутбуки, з окремими вимогами до шифрування та мобільного профілю ризику);
- servers (сервери загального призначення);
- privileged workstations (PAW/SAW для адміністрування);

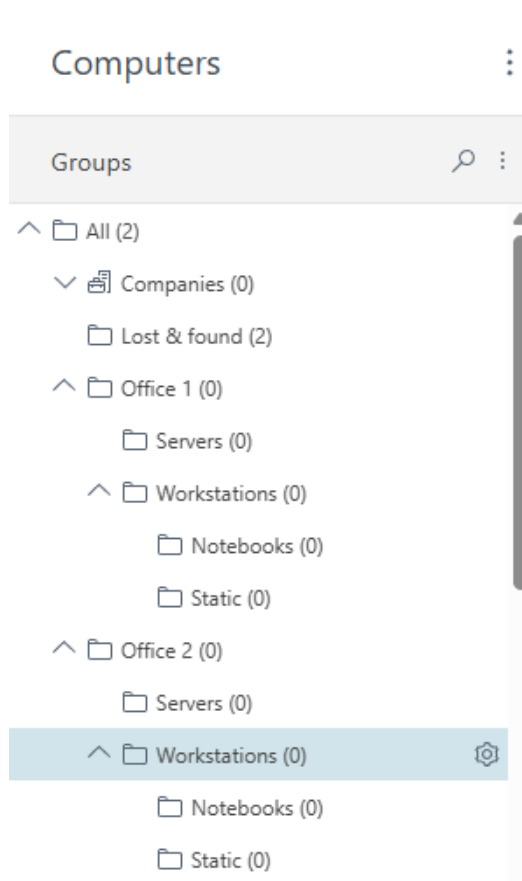


Рис. 3.2 Приклад структури статичних груп в ESET Protect

Відповідно до вимог розмежування доступів, доцільно визначити щонайменше такі ролі:

- **lead administrators:** повний доступ до керування політиками, групами, агентами та адміністративними функціями платформи;
- **lead security:** повний доступ до політик безпеки, інцидентів, звітів, реакцій, керування винятками;
- **security operators:** перегляд інцидентів і запуск стандартних реакцій, без права змінювати “базові” політики;
- **helpdesk:** обмежений доступ для підтримки (типові операції з агентом, збір базової діагностики), без права модифікувати політики захисту;
- **read-only:** аудит і контроль, без дій, що впливають на конфігурацію.

Permission Sets 			ACCESS GROUP Select 	Tags... 
☐	NAME	TAGS		
☐	 Administrator permission set			
☐	Reviewer permission set			
☐	Server assisted installation permission set			
☐	ESET Inspect server permission set			
☐	ESET Inspect user permission set			
☐	ESET Inspect reviewer permission set			
☐	Security Operator			
☐	Helpdesk			

Рис. 3.3 Приклади наборів привілеїв

3.2.3. Реалізація політик захисту кінцевих точок (ESET Endpoint Security)

Політика захисту робочих станцій у межах цільового стану повинна забезпечувати стабільний рівень протидії типовим загрозам, а також підтримувати керовані реакції безпеки. У цьому прикладі політика для робочих станцій розглядається як агресивна, із мінімізацією можливості локального відключення контролів та із централізованим управлінням винятками.

Базові компоненти політики можуть включати:

- увімкнення поведінкових механізмів виявлення та блокування загроз, з орієнтацією на активності, характерні для шифрувальників і пост-експлуатації;
- увімкнення самозахисту агента та продукту безпеки, заборону зміни критичних параметрів користувачем;

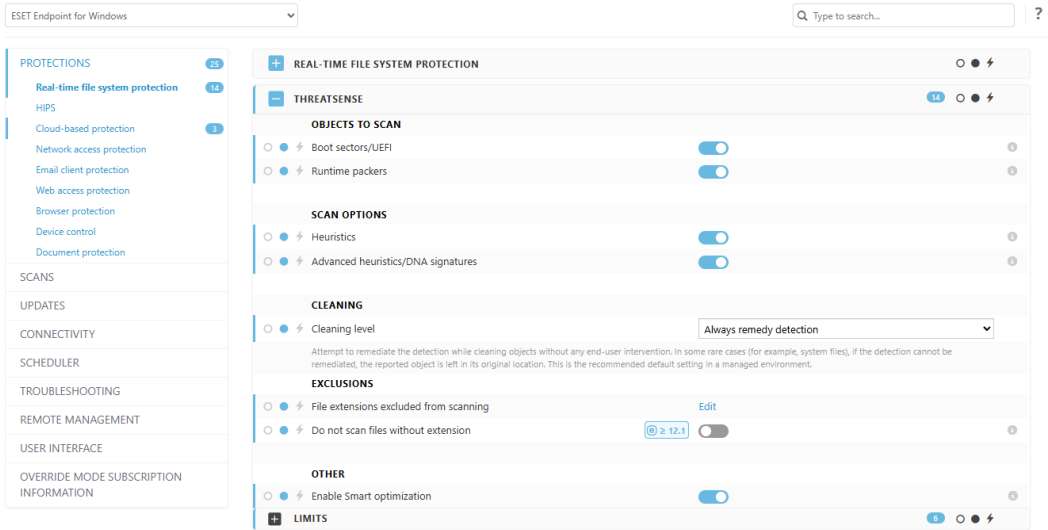


Рис. 3.4 Приклад налаштувань об’єктів сканування

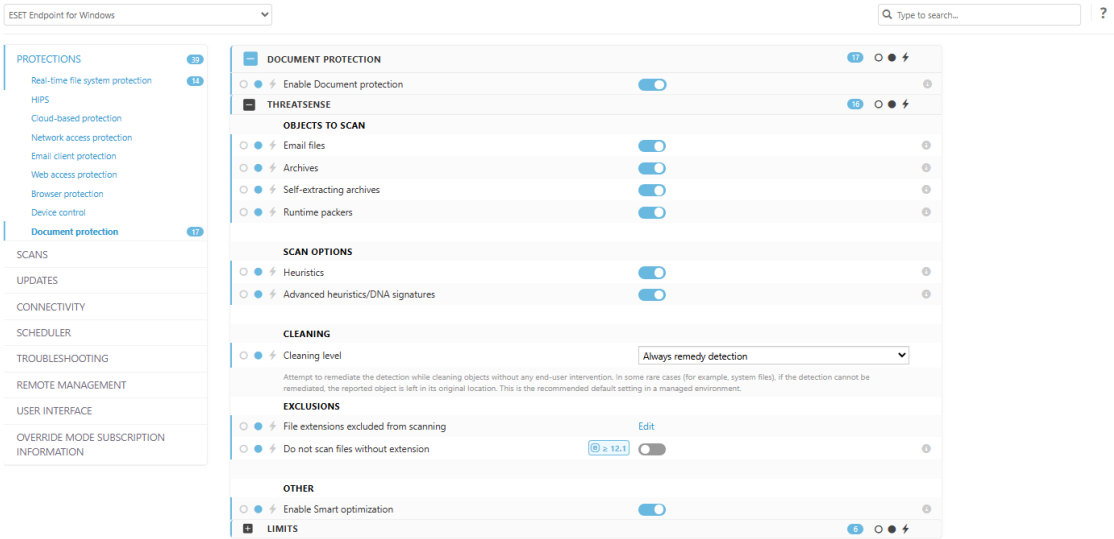


Рис. 3.5 Приклад налаштувань модулю перевірки документів

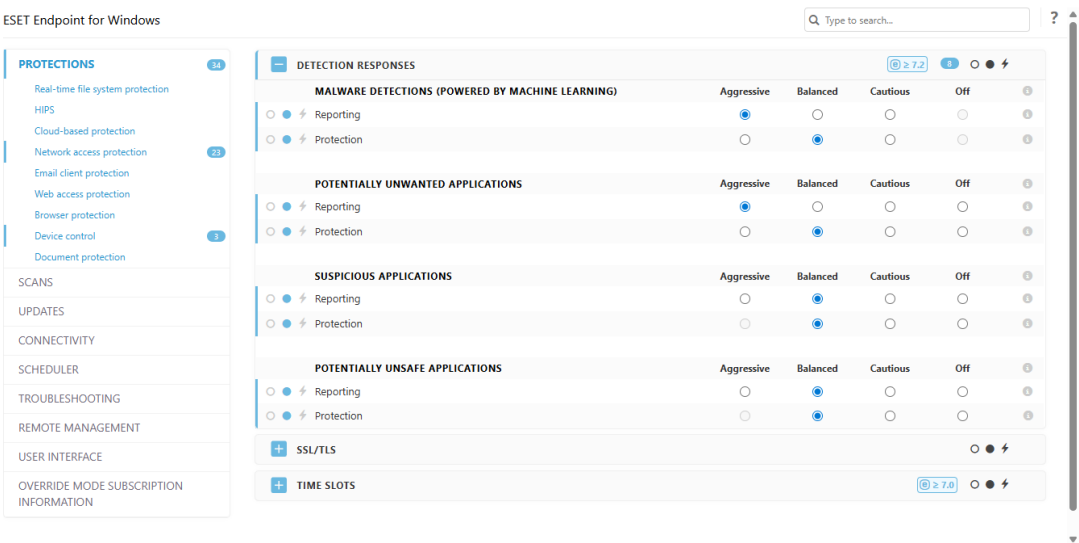


Рис. 3.6 Приклад налаштувань матриці реагування

В умовах сегментації та принципу білого списку частина мережових обмежень реалізується на рівні інфраструктури, однак додатковий контроль на хості дозволяє зменшити ризик lateral movement та неконтрольованих з'єднань. У роботі доцільно зафіксувати підхід, за якого:

- правила мережевої фільтрації керуються централізовано;
- порядок оцінювання правил може враховувати взаємодію із вбудованим Windows Firewall. Наприклад, застосування базових правил Windows як першого рівня, а специфічних через політики захисту;
- деталізація конкретних правил не наводиться через значну варіативність прав доступу та груп у реальній організації, натомість формулюється вимога білого списку.

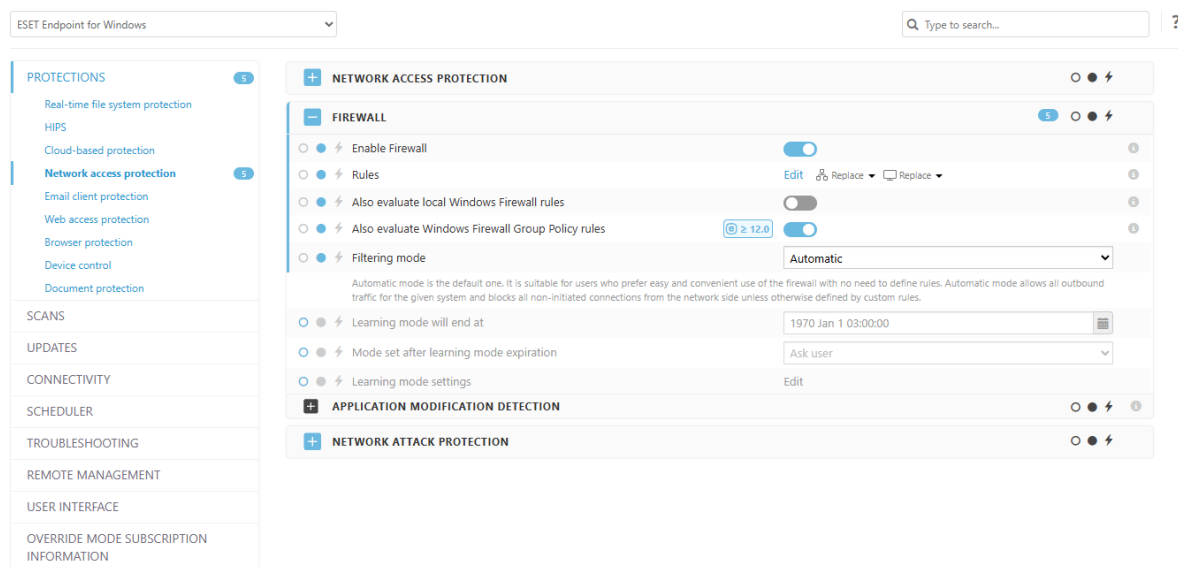


Рис. 3.7 Приклад налаштувань мережевого захисту

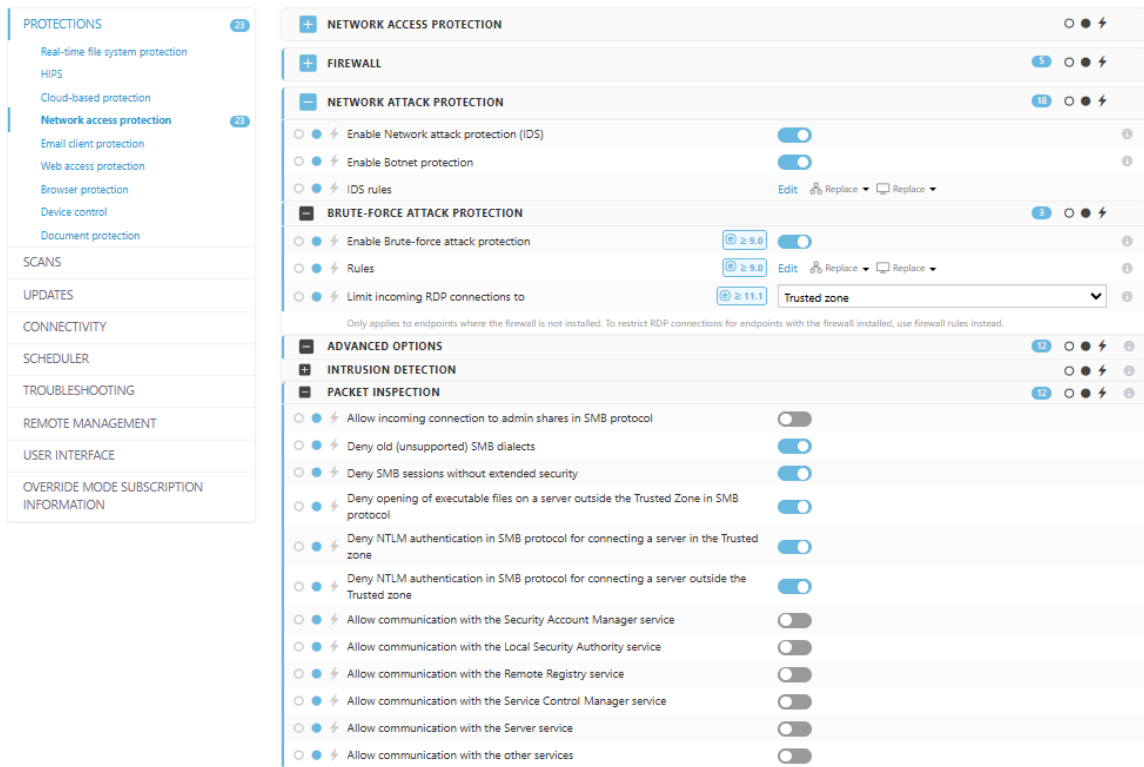


Рис. 3.8 Приклад налаштувань мережевого захисту

Відповідно до політики, дозволяються лише USB-накопичувачі як клас, тоді як інші класи периферійних пристроїв забороняються за замовчуванням. Винятки мають надаватися адміністративно та фіксуватися як контрольований процес.

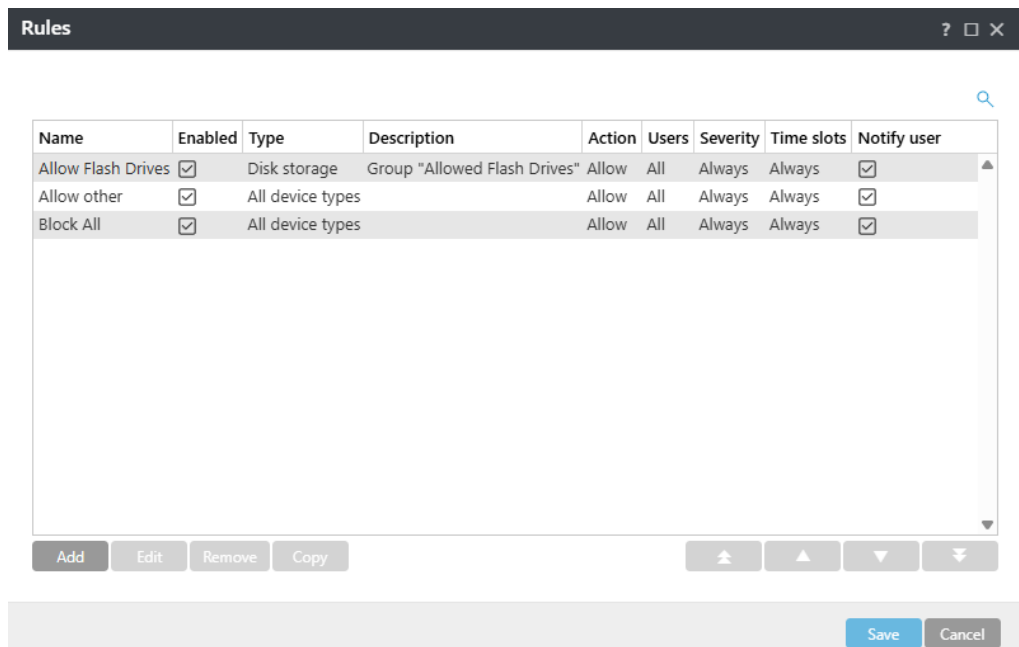


Рис. 3.9 Приклад оформлення правил модулю контролю пристроїв

Для підтримки керованості середовища необхідно контролювати:

- статус агента та актуальність модулів;

- відповідність застосованим політикам;
- тривалість “offline” стану пристрою.

У прикладі встановлюється правило: якщо кінцева точка не виходить на зв’язок із системою керування понад один тиждень і це не узгоджена причина (відпустка, ремонт), ініціюється розслідування причин, оскільки така ситуація може бути наслідком технічної несправності, обходу контролів або ознак компрометації.

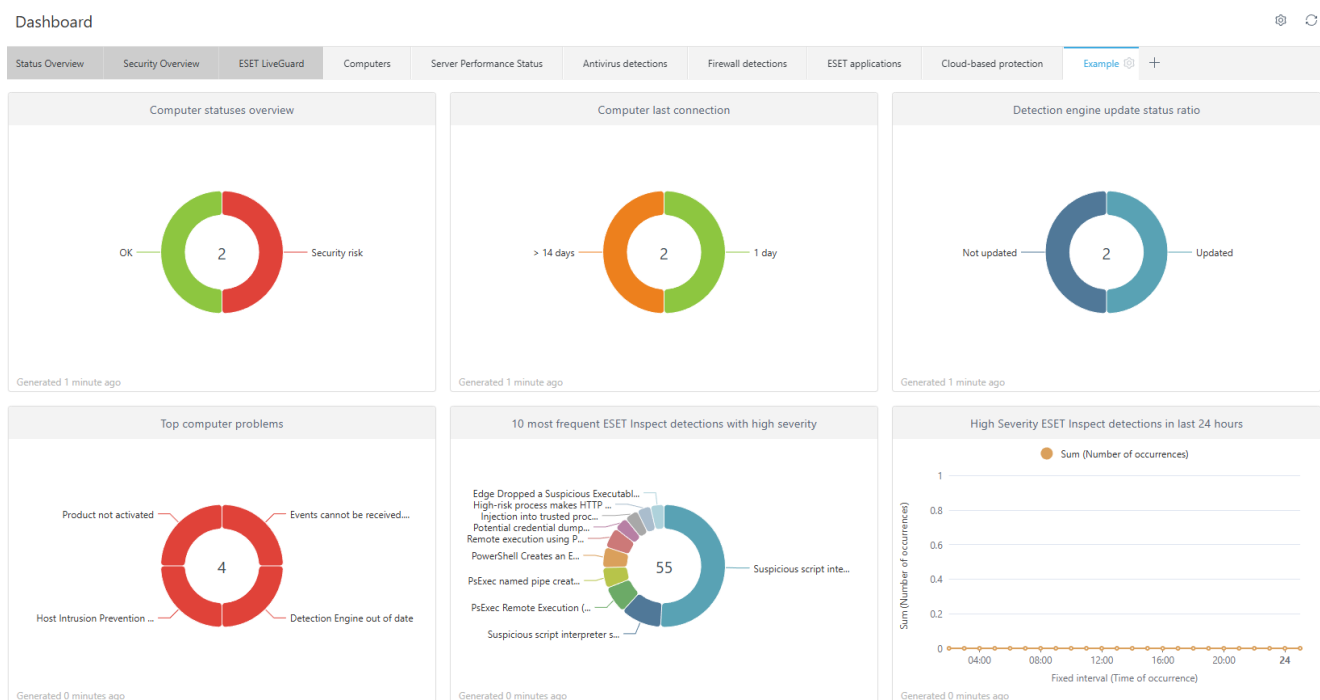


Рис. 3.10 Приклад оформлення панелі моніторингу організації

3.2.4. Реалізація політик захисту серверів (ESET Server Security)

Для серверів у цьому прикладі застосовується єдина стандартна політика, що забезпечує посилений рівень контролю порівняно з типовими налаштуваннями, але є дещо менш агресивною, ніж політика для робочих станцій, щоб зменшити ймовірність збоїв у критичних сервісах і хибнопозитивних спрацювань.

Ключові принципи серверної політики:

- посилений контроль шкідливої активності та поведінкових ознак атак із урахуванням серверних ролей;
- жорсткий самозахист і обмеження локальної модифікації налаштувань;
- керований процес винятків для високонавантажених таких систем як віртуалізація, бази даних, поштові компоненти, де винятки повинні бути документовані й затверджені функцією безпеки;

- сценарії реагування на інциденти, що враховують критичність сервісів: для частини інцидентів допускається ручне підтвердження дій (наприклад, ізоляції), щоб не спричинити сценарій неконтрольованого простою.

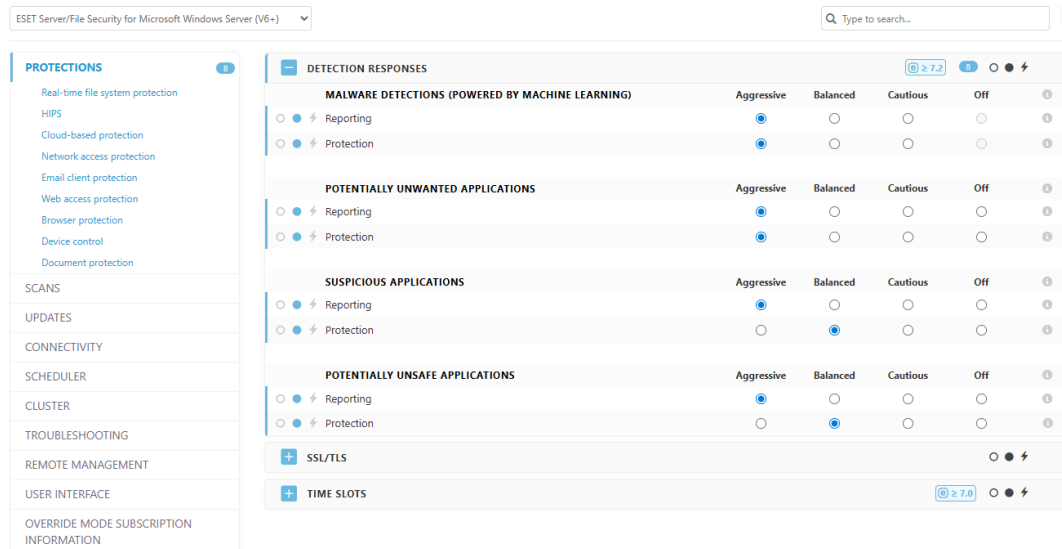


Рис. 3.11 Приклад матриці реагування серверної політики

3.2.5. Реалізація багатфакторної автентифікації (ESET Secure Authentication)

У межах цільового стану MFA використовується для посилення контролю доступу у сценаріях, що мають підвищений ризик, насамперед для віддаленого доступу та адміністративних операцій. Для прикладу приймається використання push-підтвердження та TOTP.

Віддалений доступ організовується через OpenVPN, де другий фактор підключається на рівні централізованої автентифікації (наприклад, через RADIUS).

З урахуванням вимог практичності та впливу на користувацький досвід, у цьому прикладі MFA для Windows logon застосовується не для всіх користувачів, а для привілейованих ролей (адміністратори інфраструктури, адміністратори безпеки, головні адміністратори). Аналогічний підхід застосовується для віддаленого доступу, MFA вимагається для адміністративних підключень до серверів і критичних вузлів, навіть якщо доступ здійснюється з внутрішньої мережі, оскільки внутрішній периметр не розглядається як безумовно довірений. Інтеграція з Active Directory такого рішення та постійна синхронізація користувачів та їх статусів, дозволить максимально точно керувати авторизацією користувачів по ролям, призначених в централізованій системі.

Відновлення доступу у разі втрати другого фактора (заміна телефону, втрата генератора кодів) виконується адміністраторами за регламентом, із фіксацією дій та перевіркою особи користувача.

Рис. 3.12 Приклад налаштування вимог до мобільних автентифікаторів

Рис. 3.13 Приклад дозволених методів підтвердження другого фактору

3.2.6. Реалізація повнодискового шифрування ноутбуків (ESET Full Disk Encryption)

Шифрування застосовується до ноутбуків як до найбільш ризикованого класу пристроїв з огляду на мобільність і підвищену ймовірність фізичної втрати. У межах прикладу визначаються такі вимоги:

- обов'язкове повнодискове шифрування;
- вимога введення паролю розшифрування перед завантаженням системи;

- централізоване зберігання ключів відновлення в системі керування;
- контроль відповідності та оперативне реагування на відхилення.

Зберігання ключів відновлення організовується централізовано з обмеженням доступу до них: доступ повинні мати лише привілейовані ролі (lead administrators / lead security), тоді як операційні ролі підтримки діють через ескалацію та регламентовану процедуру.

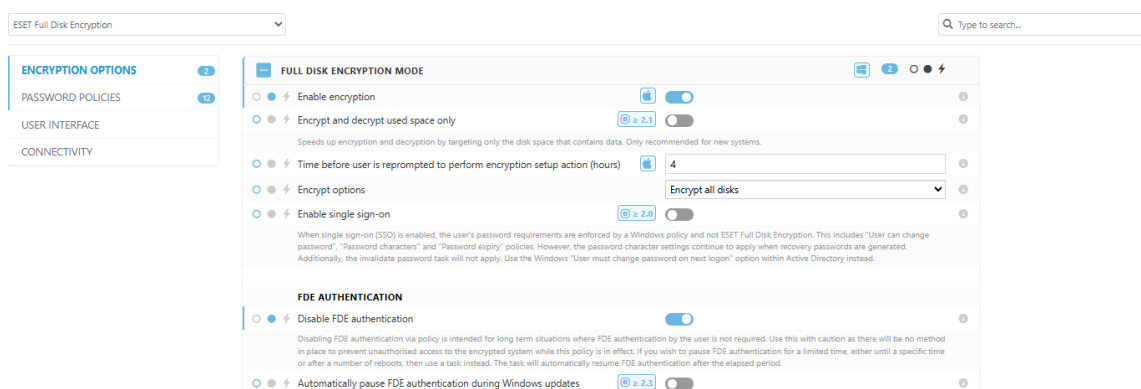


Рис. 3.14 Приклад налаштувань політики повнодискового шифрування

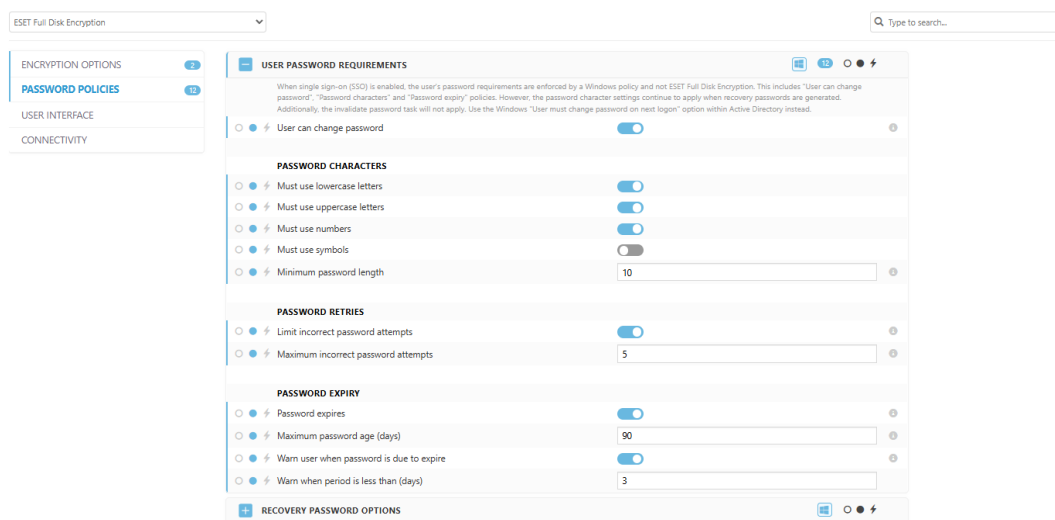


Рис. 3.15 Приклад налаштувань пароліної політики до паролю розшифрування

3.2.7. Базові налаштування Windows-середовища засобами AD/GPO як доповнення до ESET

Значна частина вимог 3.1 логічно реалізується на рівні доменної інфраструктури та групових політик, оскільки вони визначають базову конфігурацію безпеки Windows середовища і є фундаментом для ефективності захисту.

У межах прикладу доцільно зафіксувати такі напрями GPO:

- політики паролів і блокувань облікових записів (довжина, складність, історія, правила блокування після невдалих спроб);
- заборона локальних адміністраторів для користувачів та контроль привілейованих груп;
- обмеження використання застарілих протоколів і механізмів автентифікації;
- обмеження доступу до адміністративних інтерфейсів критичних вузлів (доступ до контролерів домену лише з привілейованих робочих станцій/адмін-сегмента);
- базові налаштування аудиту й журналювання, а також синхронізація часу на критичних вузлах.

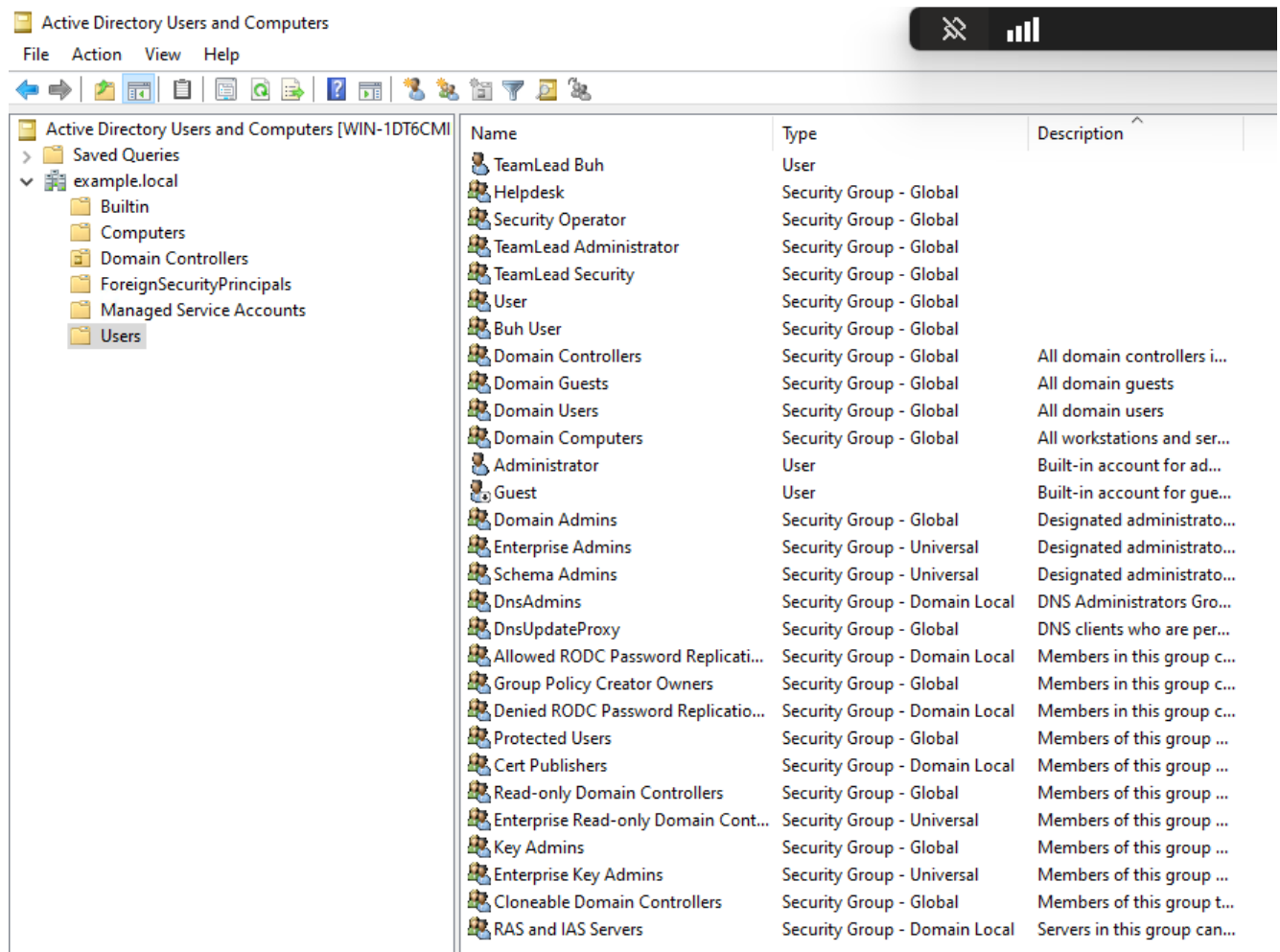


Рис. 3.16 Приклад створених груп користувачів

3.2.8. Використання Suricata у режимі IDS як мережевого рівня виявлення атак

У межах запропонованого прикладу Suricata застосовується в режимі IDS, тобто виконує функції виявлення мережових атак і підозрілої активності без активного блокування трафіку. Такий підхід є доцільним для прикладу і початку роботи з таким рішенням, оскільки дозволяє підвищити спостережуваність мережевого середовища та отримувати сигнали про потенційні інциденти без ризику впливу на доступність сервісів через помилкові спрацювання, що є критичним для виробничих мереж.

Вибір Suricata як мережевого сенсора обґрунтовується тим, що вона є зрілим серверним програмним продуктом із відкритим вихідним кодом, який активно підтримується спільнотою та має регулярні оновлення. Практична цінність такого рішення полягає в тому, що навіть у базовій конфігурації Suricata забезпечує достатній рівень видимості мережових подій і алертів, що охоплюють типові для сучасних атак сценарії, такі як сканування, спроби експлуатації вразливостей, підозрілі комунікації, а також окремі прояви горизонтального переміщення зломисника (lateral movement) у мережі. Додатковим аргументом є широка поширеність Suricata як технологічної основи або сумісного компонента для інших класів систем мережевого моніторингу, що підвищує переносимість підходу та релевантність результатів.

У межах цього прикладу не є доцільним розробляти власні правила детектування. Практичні рекомендації щодо використання Suricata зводяться до забезпечення коректної експлуатації на основі загальнодоступних наборів правил та належної організації журналювання. Зокрема, доцільно:

- використовувати актуальні джерела правил детектування та забезпечувати їх регулярне оновлення, що дозволяє враховувати нові техніки атак і зміни в інфраструктурі загроз;
- налаштувати журналювання подій у форматі, придатному для централізованого збору, з урахуванням вимог до точності часових міток та зручності подальшої обробки;
- забезпечити передавання детектувань і технічних подій до платформи SIEM для подальшого аналізу, агрегації та кореляції з подіями від інших засобів

захисту, що дозволяє поєднувати мережеві індикатори з телеметрією кінцевих точок у межах єдиного процесу моніторингу.

Таким чином, застосування Suricata у режимі IDS у запропонованій архітектурі розглядається як практичний спосіб підсилення мережевої видимості та підвищення якості виявлення інцидентів за рахунок використання відкритого, активно підтримуваного інструмента, який не потребує складного налаштування для отримання корисних результатів на базовому рівні.

Висновки до третього розділу

У цьому розділі розроблено технологію створення політик безпеки для узагальненої організації середнього масштабу з гібридною моделлю роботи та on-premise доменною інфраструктурою, орієнтовану на принципи Zero Trust. Сформульовано цільовий стан і набір взаємоузгоджених політик як сукупність вимог, правил та процедур, що охоплюють управління доступом і життєвим циклом облікових записів, захист кінцевих точок і серверів, віддалений доступ і автентифікацію, а також моніторинг, детекцію та реагування на інциденти. Запропонований підхід базується на мінімізації привілеїв, явному визначенні дозволених взаємодій за принципом білого списку, зменшенні площини атаки та посиленні керованості середовища.

Наведено приклад практичної реалізації визначених політик на основі обраного набору інструментів, з фокусом на конфігурації та організації керування: ESET PROTECT як централізована платформа, ESET Endpoint Security і Server Security для реалізації хостових контролів, ESET Secure Authentication для MFA, ESET Full Disk Encryption для захисту ноутбуків, а також AD/GPO як базовий рівень конфігураційної дисципліни Windows-середовища. Додатково запропоновано мережевий рівень видимості за допомогою Suricata у режимі IDS з регулярним оновленням правил і передаванням подій до SIEM для кореляції. Сукупно це демонструє практичну здійсненність переходу від декларативних вимог до реалізованих політик, які можуть бути масштабовані та адаптовані під конкретну організацію й її ризиковий профіль.

ВИСНОВКИ

У кваліфікаційній роботі розглянуто проблему побудови дієвих політик інформаційної безпеки для організацій із on-premise інфраструктурою та гібридною моделлю роботи, де традиційна «периметрова» логіка захисту вже не забезпечує потрібної стійкості. Досягнуто мети роботи — розроблено технологію створення політик безпеки для інформаційної системи організації на основі моделі нульової довіри (Zero Trust) та визначено практичні підходи до її впровадження.

У першому розділі узагальнено сучасний ландшафт кіберзагроз і показано, що найбільш критичними для типових організацій є атаки на ідентичності, зростання частки ransomware, експлуатація вразливостей у публічно доступних компонентах і периметрі, а також посилення ролі третіх сторін і supply chain-атак. Окремо підкреслено український контекст, де інтенсивність кібератак і специфіка противника вимагають системного підходу до політик та опори на стандарти й рекомендації профільних органів реагування.

У другому розділі на прикладі узагальненої Windows-орієнтованої on-premise IC із Active Directory, DMZ і віддаленим доступом визначено типові слабкі місця (парольна автентифікація без MFA, слабка сегментація, частковий BYOD, обмежене логування/моніторинг). На цій основі сформовано вимоги до захисту в парадигмі Zero Trust та спроектовано цільову архітектуру: логічна сегментація на зони, “deny-by-default/allowlist” для міжсегментних взаємодій, обов’язкова MFA для VPN/RDP і привілейованих сценаріїв, керований захист кінцевих точок (EPP/EDR), мережевий рівень видимості (IDS/IPS), централізоване журналювання/кореляція (SIEM), ізоляція резервного контуру та дисципліна оновлень і керування вразливостями.

У третьому розділі розроблено технологію формування політик як узгодженого набору вимог, правил і процедур для ключових напрямів: керування доступом і життєвим циклом облікових записів (RBAC, JML), автентифікація та віддалений доступ (MFA, контроль пристроїв і маршрутів), захист робочих станцій/серверів (базовий безпечний стан, зменшення площини атаки), а також моніторинг і реагування (джерела подій, пріоритетні сценарії детекції, ескалація).

Наведений приклад практичної реалізації політик на базі ESET PROTECT/Endpoint/Server Security, ESET Secure Authentication, ESET Full Disk Encryption, AD/GPO та Suricata (IDS) демонструє, як перейти від “декларативних” документів до реально застосованих і контрольованих налаштувань у середовищі.

Практичне значення отриманих результатів полягає в тому, що запропонована технологія може бути використана як шаблон для організацій середнього масштабу, які прагнуть підвищити керованість безпеки без повної перебудови IT-ландшафту: вона задає цільовий стан, пріоритизацію контролів і зрозумілий маршрут поетапного впровадження Zero Trust. Подальший розвиток роботи доцільно спрямувати на деталізацію SIEM-контенту (use-case’и, кореляції, метрики ефективності), автоматизацію перевірок відповідності (continuous posture), а також розширення моделі на хмарні сервіси та Zero Trust Network Access (ZTNA) для змішаних середовищ.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2021 Data Breach Investigations Report [Electronic resource] URL: <https://www.verizon.com/business/resources/T8fc/reports/2021-dbir-executive-brief.pdf> (дата звернення: 15.11.2025).
2. 2022 Data Breach Investigations Report [Electronic resource] URL: <https://www.verizon.com/business/resources/T67b/reports/2022-dbir-public-sector-snapshot.pdf> (дата звернення: 15.11.2025).
3. 2023 Data Breach Investigations Report [Electronic resource] URL: <https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf> (дата звернення: 15.11.2025).
4. 2024 Data Breach Investigations Report [Electronic resource] URL: <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf> (дата звернення: 15.11.2025).
5. 2025 Data Breach Investigations Report [Electronic resource] URL: <https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf> (дата звернення: 15.11.2025).
6. Microsoft Digital Defense Report 2024 [Electronic resource] URL: <https://www.microsoft.com/en-my/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024> (дата звернення: 16.11.2025).
7. IBM X-Force Threat Intelligence Index 2025 [Electronic resource] URL: <https://2025.aksi.co/ibm-x-force-threat-intelligence-index-2025-2> (дата звернення: 17.11.2025).
8. From NotPetya to Today's Global Conflict Landscape [Electronic resource] URL: <https://www.teneo.com/app/uploads/2024/09/Cyberpolitical-Risk-Emerges-as-a-Critical-Challenge-to-Business-and-Society.pdf> (дата звернення: 19.11.2025).
9. BEYOND SOLARWINDS: PRINCIPLES FOR SECURING SOFTWARE SUPPLY CHAINS [Electronic resource] URL: <https://www.mitre.org/sites/default/files/2021-08/pr-21-0843-beyond-solarwinds-principles-for-securing-software-supply-chains.pdf> (дата звернення: 19.11.2025).
10. РОСІЙСЬКІ КІБЕР ОПЕРАЦІЇ [Electronic resource] URL:

<https://docs.google.com/viewerng/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id%3D68752&a=bi> (дата звернення: 19.11.2025).

11. Remote Work Security Market Outlook [Electronic resource] URL: <https://dataintelo.com/report/remote-work-security-market> (дата звернення: 19.11.2025).

12. Zero Trust Architecture [Electronic resource] URL: <https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf> (дата звернення: 22.11.2025).

13. ISO/IEC 27001:2022 [Electronic resource] URL: <https://www.iso.org/standard/27001> (дата звернення: 22.11.2025).

14. ISO/IEC 27002:2022 [Electronic resource] URL: <https://www.iso.org/standard/75652.html> (дата звернення: 22.11.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)