ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТУ ІМЕНІ С.П.КОРОЛЬОВА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

здобувача вищої освіти ступеня «бакалавр» заочної форми навчання
за спеціальністю «Кібербезпека»

Тема: «СИСТЕМА КОНТРОЛЮ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРОЇВ МЕРЕЖІ»

Виконавець: Емін ФАРАДЖОВ

м. Житомир

2026

РЕФЕРАТ

Кваліфікаційна робота присвячена розробленню системи контролю безпеки кінцевих пристроїв мережі. У роботі розглянуто сучасний стан захисту кінцевих пристроїв, проаналізовано основні класи рішень EPP, EDR, XDR, NAC, UEM і ZTNA, визначено проблеми централізованого моніторингу та обґрунтовано потребу в інтегрованій системі контролю.

У першому розділі розкрито актуальність теми, наведено характеристику загроз для кінцевих пристроїв, описано чинники, що збільшують поверхню атаки, зокрема BYOD, IoT, віддалену роботу, застарілі операційні системи та недостатню видимість активів. Окремо враховано український контекст кіберзагроз і вимоги національної системи кібербезпеки.

У другому розділі досліджено технології моніторингу та виявлення загроз, порівняно провідні засоби захисту кінцевих пристроїв, розглянуто методи контролю відповідності політикам безпеки, механізми збору телеметрії, використання поведінкового аналізу, машинного навчання та фреймворку MITRE ATT&CK.

У третьому розділі розроблено структурну схему системи контролю безпеки кінцевих пристроїв, визначено склад і призначення її підсистем, описано алгоритм виявлення відхилень від політик безпеки, запропоновано категорії перевірок відповідності, вагові коефіцієнти критичності та механізм автоматизованого реагування.

Практична цінність роботи полягає у формуванні архітектурного рішення, яке може бути використане як основа для впровадження системи безперервного контролю безпеки кінцевих пристроїв у корпоративних мережах різного масштабу. Запропонований підхід поєднує моніторинг стану пристроїв, контроль відповідності, кореляцію подій і реагування на інциденти.

Кваліфікаційна робота містить 67 сторінок, 7 рисунків, 11 таблиць, 31 джерело, 1 додаток.

Ключові слова: кінцевий пристрій, endpoint security, EDR, XDR, NAC, UEM, Zero Trust, телеметрія, політики безпеки, контроль відповідності, кібербезпека, корпоративна мережа.

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ

AI - Artificial Intelligence, штучний інтелект.

API - Application Programming Interface, програмний інтерфейс застосунку.

APT - Advanced Persistent Threat, цілеспрямована довготривала кібератака.

AWL - Application Whitelisting, контроль дозволених застосунків.

BYOD - Bring Your Own Device, використання особистих пристроїв у корпоративній мережі.

CASB - Cloud Access Security Broker, брокер безпеки доступу до хмарних сервісів.

CERT-UA - урядова команда реагування на комп'ютерні надзвичайні події України.

CIS - Center for Internet Security.

CPU - Central Processing Unit, центральний процесор.

CVE - Common Vulnerabilities and Exposures, база ідентифікаторів вразливостей.

CVSS - Common Vulnerability Scoring System, система оцінювання критичності вразливостей.

DMZ - Demilitarized Zone, демілітаризована мережева зона.

EDR - Endpoint Detection and Response, виявлення та реагування на загрози на кінцевих пристроях.

EPP - Endpoint Protection Platform, платформа захисту кінцевих пристроїв.

FDE - Full Disk Encryption, повне шифрування диску.

FIDO2 - стандарт безпарольної аутентифікації на основі криптографічних ключів.

FIM - File Integrity Monitoring, моніторинг цілісності файлів.

GDPR - General Data Protection Regulation, Загальний регламент захисту даних ЄС.

HIPS - Host-based Intrusion Prevention System, система запобігання вторгненням на рівні хоста.

IoA - Indicators of Attack, індикатори атаки.

IoC - Indicators of Compromise, індикатори компрометації.

IoT - Internet of Things, Інтернет речей.

JSON - JavaScript Object Notation, формат структурованого опису даних.

LotL - Living-off-the-Land, атаки з використанням легітимних системних інструментів.

MDM - Mobile Device Management, управління мобільними пристроями.

MFA - Multi-Factor Authentication, багатофакторна аутентифікація.

MITRE ATT&CK - база знань про тактики, техніки та процедури кібератак.

ML - Machine Learning, машинне навчання.

MTTD - Mean Time to Detect, середній час виявлення інциденту.

MTTR - Mean Time to Respond, середній час реагування.

NAC - Network Access Control, контроль мережевого доступу.

NDR - Network Detection and Response, мережеве виявлення та реагування.

NGAV - Next-Generation Antivirus, антивірус нового покоління.

NIS2 - Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union.

NIST - National Institute of Standards and Technology.

PAM - Privileged Access Management, управління привілейованим доступом.

PoLP - Principle of Least Privilege, принцип найменших привілеїв.

RADIUS - Remote Authentication Dial-In User Service, протокол централізованої аутентифікації.

SCAP - Security Content Automation Protocol, протокол автоматизації контролю безпеки.

SIEM - Security Information and Event Management, управління інформацією та подіями безпеки.

SOC - Security Operations Center, центр операцій безпеки.

SOAR - Security Orchestration, Automation and Response, оркестрація та автоматизація реагування.

TPM - Trusted Platform Module, апаратний модуль довіри.

TLS - Transport Layer Security, протокол захищеного передавання даних.

UEM - Unified Endpoint Management, уніфіковане управління кінцевими пристроями.

USB - Universal Serial Bus, універсальна послідовна шина.

VPN - Virtual Private Network, віртуальна приватна мережа.

WMI - Windows Management Instrumentation.

XDR - Extended Detection and Response, розширене виявлення та реагування.

ZTNA - Zero Trust Network Access, мережевий доступ за моделлю нульової довіри.

ВСТУП

Розвиток інформаційно-комунікаційних технологій, масштабна цифровізація підприємств та установ, перехід на гібридні та повністю дистанційні моделі роботи кардинально змінили корпоративний IT-ландшафт. Якщо ще десятиліття тому корпоративний периметр безпеки чітко окреслювався фізичними межами офісу та мережевим обладнанням, то сьогодні він розширився до кожного пристрою, що отримує доступ до корпоративних ресурсів, незалежно від його місцезнаходження. Смартфони співробітників у домашній мережі, особисті ноутбуки на платформі BYOD, промислові контролери на виробництві, медичні прилади в лікарнях, камери відеоспостереження – усе це стало частиною корпоративної мережі, кожен елемент якої є потенційною точкою входу для зловмисника.

За даними галузевих звітів Verizon та ENISA, значна частина кібератак починається з компрометації кінцевого пристрою або облікових даних користувача. Серед основних причин такого сценарію: відсутність своєчасного патч-менеджменту, слабкі або викрадені облікові дані, шкідливе програмне забезпечення, завантажене через фішингові посилання, та несанкціоноване підключення зовнішніх носіїв. Кожна з цих причин свідчить про принципову неможливість побудови ефективної кібербезпеки без комплексного контролю стану захищеності кінцевих пристроїв [2], [3].

Актуальність теми кваліфікаційної роботи зумовлена тим, що сучасні організації потребують комплексних систем контролю безпеки кінцевих пристроїв, здатних виконувати безперервний моніторинг захищеності всього парку обладнання, виявляти відхилення від встановлених політик, автоматично реагувати на порушення та надавати повну аудиторську документацію для виконання вимог регуляторів. Ринок засобів захисту кінцевих пристроїв є одним із найдинамічніших у галузі кібербезпеки, що підтверджується аналітичними прогнозами Gartner щодо зростання попиту на endpoint security-рішення [5].

Метою кваліфікаційної роботи є розроблення системи контролю безпеки кінцевих пристроїв корпоративної мережі, що забезпечує безперервний моніторинг стану захищеності, автоматичне виявлення відхилень від встановлених політик безпеки та ефективне реагування на виявлені загрози.

У межах цієї роботи під системою контролю безпеки кінцевих пристроїв розуміється сукупність програмних агентів, серверних модулів, політик перевірки відповідності, засобів кореляції подій і механізмів реагування, які дозволяють не тільки виявляти зараження шкідливим програмним забезпеченням, а й постійно перевіряти, чи відповідає кожен пристрій вимогам корпоративної політики безпеки.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз сучасного стану та ключових проблем забезпечення безпеки кінцевих пристроїв корпоративних мереж;

– дослідити та систематизувати основні підходи, методи та технологічні рішення у галузі контролю безпеки кінцевих пристроїв;

– провести порівняльний аналіз сучасних засобів захисту кінцевих пристроїв (EPP, EDR, XDR, NAC, UEM);

– дослідити технології моніторингу та виявлення загроз: сигнатурний аналіз, поведінкове виявлення, машинне навчання, фреймворк MITRE ATT&CK;

– розробити структурну схему системи контролю безпеки кінцевих пристроїв з визначенням усіх компонентів та їхньої взаємодії;

– розробити формалізований алгоритм виявлення відхилень від політик безпеки;

– оцінити ефективність розроблених рішень та надати рекомендації щодо їхнього впровадження.

Об’єктом дослідження є процеси забезпечення інформаційної безпеки корпоративних мереж на рівні кінцевих пристроїв.

Предметом дослідження є методи, алгоритми та технологічні рішення для побудови системи контролю безпеки кінцевих пристроїв мережі.

Методи дослідження: системний аналіз і синтез; порівняльний аналіз технічних рішень; методи структурного проєктування інформаційних систем; алгоритмізація; методи оцінки ефективності систем виявлення вторгнень.

Практична цінність роботи полягає у розробці конкретного архітектурного рішення та алгоритму виявлення відхилень від політик безпеки, придатних для реалізації та впровадження в корпоративних середовищах різного масштабу.

1. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ СТВОРЕННЯ СИСТЕМИ КОНТРОЛЮ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРОЇВ МЕРЕЖІ

1.1 Аналіз сучасного стану забезпечення безпеки кінцевих пристроїв

Кінцеві пристрої мережі (endpoint devices) – це будь-які комп'ютеризовані пристрої, що є кінцевими точками мережевих комунікацій: персональні комп'ютери, ноутбуки, мобільні телефони, планшети, принтери, мережеві сканери, IP-камери, сервери застосунків, а також пристрої Інтернету речей (IoT). З розвитком концепції BYOD та дистанційної роботи їхня кількість у корпоративних середовищах зросла в рази, що суттєво розширило поверхню атаки.

За даними звіту Ponemon Institute «2024 State of Endpoint Security», середньостатистичне підприємство з 1000 співробітників щодня генерує понад 5 мільйонів подій безпеки, пов'язаних із кінцевими пристроями. При цьому більшість організацій здатна аналізувати лише незначну частку цих подій через обмеженість ресурсів служби інформаційної безпеки (SOC) [1].

Статистика кіберінцидентів свідчить про стійке зростання атак, спрямованих на кінцеві вузли мережі. Особливо тривожною є тенденція до зростання середньої вартості інциденту, пов'язаного з компрометацією кінцевого пристрою, – з 4,35 млн доларів США у 2022 році до 4,88 млн у 2024 році. Це зростання пояснюється підвищенням складності атак, збільшенням часу їхнього неявного перебування в системі (dwell time) та наслідками для ділової репутації організацій. [4].

Ситуацію ускладнює різноманіття операційних систем і конфігурацій кінцевих пристроїв. Корпоративне середовище сучасної організації може включати кілька версій Windows (7/10/11/Server), різні дистрибутиви Linux, macOS, мобільні ОС Android та iOS, а також специфічні вбудовані ОС для IoT-пристроїв. Кожна з цих платформ має власні механізми безпеки, власний формат журналів подій та власні інструменти управління, що надзвичайно ускладнює централізований моніторинг.

На рисунку 1.1 наведено розподіл типів загроз кінцевих пристроїв та динаміку кіберінцидентів за 2020–2024 роки, що ілюструє масштаб і характер сучасного ландшафту загроз.

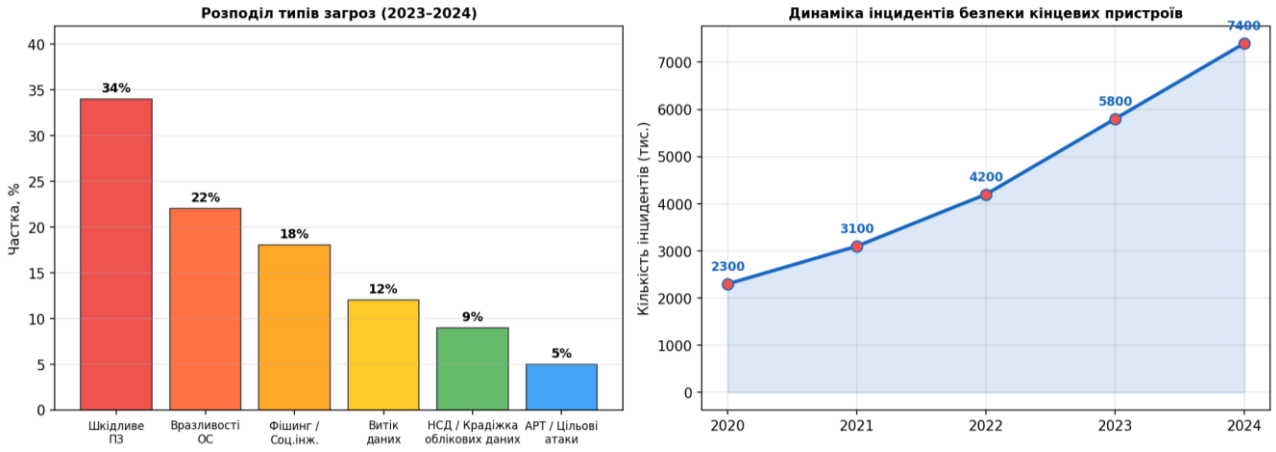

Рисунок 1.1 – Розподіл загроз кінцевих пристроїв та динаміка інцидентів

Як видно з рисунку, шкідливе програмне забезпечення залишається найпоширенішою загрозою для кінцевих пристроїв – його частка становить 34% від загальної кількості інцидентів. Вразливості операційних систем та прикладного ПЗ займають 22%, фішингові атаки та соціальна інженерія – 18%. Загальна кількість інцидентів зросла більш ніж у три рази: з 2,3 тисячі у 2020 році до 7,4 тисячі у 2024 році, що є виразним свідченням ескалації кіберзагроз. [2]

Окрему увагу привертають атаки типу «живлення від землі» (Living-off-the-Land, LotL), які стрімко зросли в популярності серед зловмисників. Ці атаки використовують легітимні системні інструменти – PowerShell, Windows Management Instrumentation (WMI), PsExec, CertUtil, Mshta – для виконання шкідливих дій. Перевага такого підходу полягає в тому, що він не залишає типових ознак шкідливого ПЗ (виконуваних файлів), що суттєво ускладнює виявлення традиційними антивірусними інструментами.

Серед ключових проблем сучасного стану безпеки кінцевих пристроїв, виявлених у ході аналізу, виділяють: [3]

– неоднорідність парку кінцевих пристроїв – різнорідні операційні системи (Windows різних версій, macOS, Linux, Android, iOS), версії програмного

забезпечення та конфігурації ускладнюють впровадження єдиних стандартів безпеки та централізований моніторинг стану захищеності;

– застаріле або непатчоване програмне забезпечення – за даними Verizon DBIR 2024, близько 60% успішних зломів використовували відомі вразливості, для яких патчі були доступні понад 90 днів. Таким чином, проблема полягає не у відсутності виправлень, а у їхньому несвоєчасному застосуванні;

– слабкий контроль доступу – відсутність або неналежна реалізація принципу найменших привілеїв (Principle of Least Privilege, PoLP) дозволяє зловмисникам горизонтально переміщуватися мережею після початкового злому одного пристрою;

– недостатній рівень обізнаності користувачів – людський фактор є однією з ключових причин успішних атак. Фішинг залишається провідним вектором початкового проникнення: за даними ENISA, 74% інцидентів починалися з соціальної інженерії у 2024 році;

– тіньові IT-ресурси (Shadow IT) – несанкціоноване використання хмарних сервісів та зовнішніх пристроїв зберігання даних уводить активи з-під корпоративного контролю та створює неконтрольовані канали передачі даних;

– відсутність централізованого моніторингу – ізольовані засоби захисту без механізмів кореляції подій не забезпечують своєчасного виявлення складних багатоетапних атак. Зловмисники використовують цей недолік, розподіляючи шкідливу активність між численними системами;

– проблема BYOD та мобільних пристроїв – особисті пристрої співробітників, як правило, мають слабший захист і виходять за межі корпоративного управління, при цьому маючи доступ до корпоративних даних через електронну пошту, хмарні сервіси та VPN;

– недостатня видимість активів – організації не завжди мають актуальний перелік усіх кінцевих пристроїв у своїй мережі, особливо якщо частина обладнання підключається дистанційно, використовується за моделлю BYOD або належить до IoT-сегмента. За таких умов адміністратор не може своєчасно

оцінити стан захищеності кожного пристрою і коректно застосувати політики безпеки;

Важливим індикатором системної проблеми є середній час виявлення інцидентів. Незважаючи на поступове скорочення – з 204 днів у 2022 до 184 днів у 2024 році, – цей показник залишається неприйнятно високим. За такий час зловмисники отримують можливість вільно досліджувати корпоративну інфраструктуру, встановлювати додаткові засоби закріплення (persistence mechanisms), викрадати конфіденційні дані та готувати деструктивні атаки. [4]

Типова корпоративна мережа з різноманітними кінцевими пристроями та захисною інфраструктурою наведена на рисунку 1.2. Схема демонструє триярусну ієрархію мережі з розподілом пристроїв за відділами, наявність демілітаризованої зони (DMZ), централізованих серверів безпеки (SIEM та NAC) та встановлених на кінцевих пристроях агентів моніторингу.

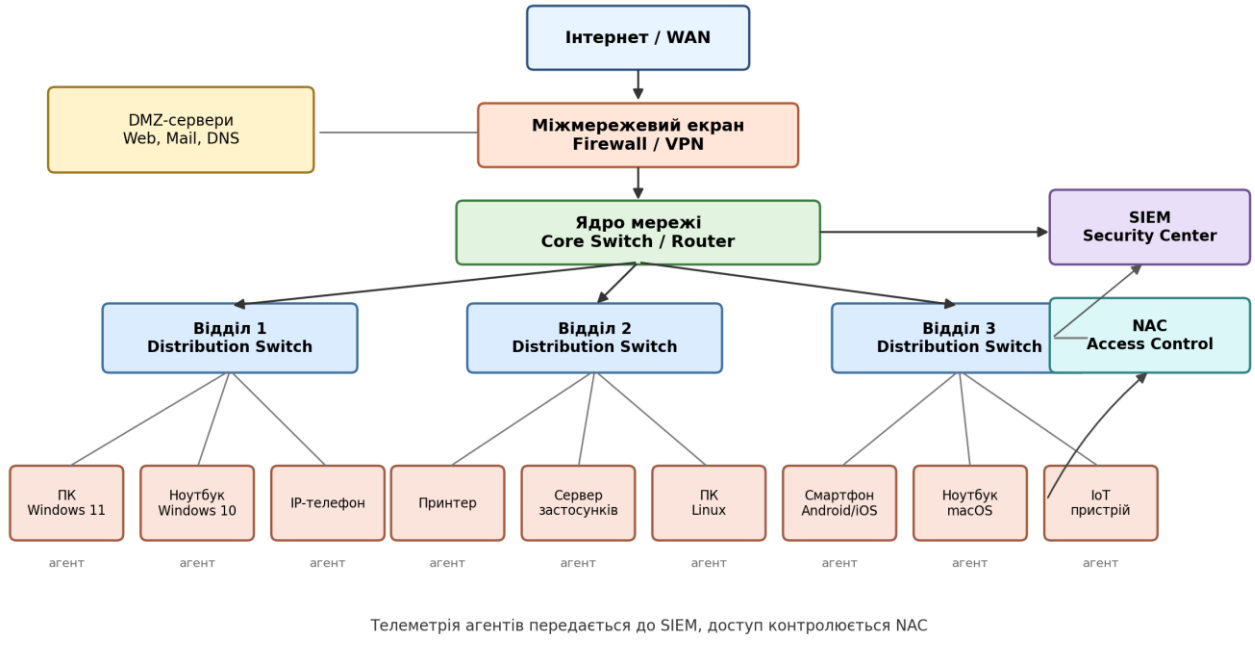

Рисунок 1.2 – Типова корпоративна мережа з кінцевими пристроями та системою безпеки

На рисунку 1.2 відображено три категорії кінцевих пристроїв у трьох відділах: робочі станції, ноутбуки, IP-телефони (Відділ 1), принтери, сервери

застосунків (Відділ 2), смартфони та IoT-пристрої (Відділ 3). Кожен кінцевий пристрій оснащений програмним агентом безпеки. Усі агенти передають телеметрію до централізованого SIEM-сервера через шифрований канал зв'язку, тоді як NAC-сервер контролює надання мережевого доступу відповідно до встановлених політик відповідності. [6]

Ситуацію додатково ускладнює зростання кількості пристроїв Інтернету речей у корпоративних середовищах. IoT-пристрої часто мають обмежені можливості безпеки: застаріле вбудоване програмне забезпечення, жорстко закодовані паролі, відсутність підтримки шифрування та неможливість встановлення агентів безпеки. За даними дослідницької компанії Armis, 72% корпоративних мереж мають щонайменше один критично вразливий IoT-пристрій. [7]

Розгляд питання безпеки кінцевих пристроїв неможливий без аналізу еволюції загрозового середовища. Ще у 2015 році більшість атак на корпоративні мережі використовували зовнішній периметр як основний вектор – вразливості веб-застосунків, відкриті порти, незахищені VPN-шлюзи. Сьогодні зловмисники воліють придбати доступ до вже скомпрометованих кінцевих пристроїв через ринки початкового доступу (Initial Access Brokers, IAB) у darknet або здійснити цільовий фішинг проти конкретних співробітників організації. Ця зміна парадигми пояснює, чому частка атак, що починаються з кінцевих пристроїв, зростала з 52% у 2018 до 71% у 2024 році. [4]

Особливо гострою є проблема застарілих (legacy) систем у корпоративних мережах. Організації часто не можуть оновити критичні виробничі або медичні системи через ризики переривання операційної діяльності або відсутність підтримки з боку виробника. Windows 7 та Windows Server 2008, для яких Microsoft припинила підтримку у 2020 та 2019 роках відповідно, досі зустрічаються в мережах великих організацій. Відповідно до дослідження Lansweeper, у 2023 році близько 18% корпоративних кінцевих пристроїв у глобальному масштабі все ще використовували застарілі ОС, що не отримують оновлення безпеки. Кожна така система є потенційними відкритими воротами

для зловмисника, оскільки нові CVE для застарілих платформ більше не закриваються патчами. [3]

Проблема вразливості кінцевих пристроїв має й психологічний вимір. Дослідження в галузі когнітивної безпеки показують, що навіть обізнані з ризиками користувачі в умовах часового тиску, когнітивного перевантаження або у нетиповому середовищі схильні приймати хибні рішення щодо безпеки: клікати на підозрілі посилання, відхиляти оновлення безпеки, використовувати слабкі паролі. Це означає, що технічні засоби захисту повинні бути побудовані так, щоб компенсувати людський фактор, а не покладатися виключно на належну поведінку користувачів. [1]

Статистика CERT-UA за 2023-2024 роки свідчить, що значна частина успішних атак на українські організації також пов'язана з компрометацією кінцевих пристроїв. Угруповання APT28 (Fancy Bear) та Sandworm активно використовували шкідливі документи Microsoft Office з макросами, архіви, LNK-файли, легітимні хмарні сервіси та інструменти віддаленого доступу для розповсюдження шкідливого ПЗ та організації каналів командного управління [29].

Вітчизняні наукові роботи також підкреслюють необхідність переходу від ізольованих антивірусних засобів до системного моніторингу стану кінцевих пристроїв. Зокрема, у дослідженні Д. А. Михайлишина розглянуто побудову системи моніторингу host security, що поєднує аналіз стану пристрою, виявлення вторгнень та централізоване спостереження за подіями безпеки [30].

Таблиця 1.1 – Статистика кіберінцидентів, пов'язаних із кінцевими пристроями

Показник	**2021**	**2022**	**2023**	**2024**
Кількість інцидентів (тис./рік)	3100	4200	5800	7400
Частка атак на endpoint (%)	62	64	68	71
Середній час виявлення (дні)	212	204	197	184
Середня вартість інциденту (млн доларів США)	4,24	4,35	4,45	4,88
Частка LotL-атак серед endpoint (%)	28	34	41	48

З таблиці 1.1 видно чітку тенденцію до погіршення ситуації за всіма ключовими показниками. Особливо тривожним є зростання частки LotL-атак з 28% у 2021 до 48% у 2024 році. Цей вид атак особливо складно виявляти традиційними засобами, оскільки зловмисники використовують легітимні системні інструменти, що не викликають підозри у стандартних антивірусних рішень [3].

Аналіз географічного розподілу джерел кіберзагроз для кінцевих пристроїв показує, що найбільш організовані та технічно складні атаки походять від державно спонсорованих угруповань. Кіберзлочинні угруповання є більш чисельними та мотивованими фінансово. Для захисту від обох категорій зловмисників необхідні різні підходи: проти державних акторів ефективні поведінковий аналіз та виявлення аномалій; проти кримінальних груп – управління вразливостями та контроль доступу.

Таким чином, проведений аналіз дозволяє сформулювати узагальнену характеристику поточного стану безпеки кінцевих пристроїв: зростання кількості та різноманіття кінцевих пристроїв, ускладнення ландшафту загроз, неефективність ізольованих точкових рішень та критична необхідність у комплексній системі контролю безпеки. Наступний підрозділ присвячено аналізу наявних підходів і методів вирішення цієї проблеми.

1.2 Основні підходи та методи контролю безпеки кінцевих пристроїв

Еволюція підходів до захисту кінцевих пристроїв пройшла кілька ключових етапів. Перше покоління – традиційний антивірус на основі сигнатур – з’явилося в 1990-х роках і до середини 2000-х залишалося стандартним засобом захисту. Принцип роботи полягав у порівнянні MD5-хешів або бінарних патернів файлів з базою відомих зразків шкідливого ПЗ. Ефективний проти відомих загроз, цей метод виявився безсилим проти поліморфних вірусів, безфайлового шкідливого ПЗ та атак нульового дня. [8]

Друге покоління – поведінковий аналіз та евристика – з’явилося на початку 2000-х як відповідь на обмеження сигнатурного підходу. Замість порівняння з

базою відомих зразків, поведінковий аналіз оцінює дії програм та процесів у реальному часі, виявляючи підозрілі патерни поведінки: масове шифрування файлів, спроби доступу до привілейованих API, підозрілі мережеві з'єднання тощо.

Третє покоління – платформи захисту кінцевих пристроїв (EPP) та технологія виявлення і реагування (EDR) – ознаменувало перехід від реактивного захисту до проактивного виявлення та реагування. Запропонований аналітиком Gartner Антоном Чувакіним у 2013 році, термін EDR визначає клас рішень, що безперервно збирають та аналізують телеметрію кінцевих пристроїв для виявлення загроз, що обійшли превентивні засоби захисту. [9]

Сучасне четверте покоління представлено рішеннями класу XDR (Extended Detection and Response), що інтегрують телеметрію не лише від кінцевих пристроїв, а й від мережевого обладнання, хмарних сервісів, серверів ідентифікації та систем електронної пошти. Завдяки кореляції даних із різних джерел XDR забезпечує набагато точніше виявлення складних атак та суттєво скорочує кількість хибних спрацьовувань (false positives) [10].

Нижче наведено докладний опис кожного із ключових підходів до контролю безпеки кінцевих пристроїв.

1. Endpoint Protection Platform (EPP). Платформа захисту кінцевих пристроїв є базовим засобом превентивного захисту та включає антивірусний захист нового покоління (Next-Generation Antivirus, NGAV) на основі поведінкового аналізу та машинного навчання; захист від шкідливих скриптів PowerShell та макросів Office; систему репутаційного аналізу файлів та URL на основі хмарних баз даних; особистий брандмауер хоста (Host-based Firewall) з розширеними можливостями фільтрації; систему запобігання вторгненням на рівні хоста (Host-based Intrusion Prevention System, HIPS); управління USB та переносними носіями (Device Control); захист від експлойтів (Exploit Protection).

2. Endpoint Detection and Response (EDR). EDR-рішення безперервно збирають телеметричні дані: виклики системних API (Windows ETW, Linux

eBPF), мережеві з’єднання (IP, порти, протоколи, обсяги трафіку), операції з файловою системою (створення, модифікація, видалення), зміни в реєстрі ОС (Windows Registry), запуск та завершення процесів, виконання команд у консолі. На основі поведінкового аналізу та правил фреймворку MITRE ATT&CK система виявляє індикатори компрометації (Indicators of Compromise, IoC) та індикатори атаки (Indicators of Attack, IoA). EDR надає інструменти для розслідування інцидентів: візуалізацію ланцюжка атаки (attack chain), ретроактивний пошук (threat hunting) та дистанційне реагування (ізоляція пристрою, завершення процесу, збір криміналістичних даних).

3. Extended Detection and Response (XDR). XDR долає основне обмеження EDR – обмеженість видимістю лише кінцевих пристроїв. Платформа агрегує телеметрію з кількох джерел: кінцевих пристроїв (через EDR), мережевого обладнання (через NDR – Network Detection and Response), хмарних сервісів (CASB – Cloud Access Security Broker), систем ідентифікації (Active Directory, Azure AD) та електронної пошти. Завдяки єдиній аналітичній платформі XDR забезпечує наскрізну видимість атак, що переміщуються між доменами, та автоматичну кореляцію пов’язаних подій у єдиний інцидент.

4. Network Access Control (NAC). Технологія контролю мережевого доступу перевіряє відповідність пристрою встановленим вимогам безпеки перед наданням доступу до корпоративної мережі. Перевірки включають: наявність та актуальність антивірусного ПЗ; встановлені критичні оновлення безпеки; наявність агента EDR; шифрування диску; відповідність операційної системи вимогам. NAC-системи застосовують динамічну сегрегацію невідповідних пристроїв у карантинний VLAN, де вони мають доступ лише до ресурсів для самовиправлення (оновлення, встановлення агентів). Реалізується за допомогою стандарту IEEE 802.1X у поєднанні із протоколом RADIUS та сервером політик (Policy Engine) [12].

5. Unified Endpoint Management (UEM). Уніфіковане управління кінцевими пристроями об’єднує функції MDM (Mobile Device Management), MAM (Mobile Application Management) та традиційні інструменти управління клієнтами

Windows/macOS в єдину платформу. UEM дозволяє централізовано розгортати конфігурації та застосунки, примусово застосовувати налаштування безпеки, виконувати дистанційне очищення даних (remote wipe), відстежувати відповідність пристроїв корпоративним стандартам та управляти сертифікатами та ідентифікацією [13].

6. Zero Trust Network Access (ZTNA). Модель нульової довіри, деталізована в публікації NIST SP 800-207, є концептуальним фундаментом сучасного підходу до безпеки кінцевих пристроїв. Принцип «ніколи не довіряй, завжди перевіряй» передбачає безперервну верифікацію ідентичності користувача, стану захищеності пристрою та контексту доступу перед наданням кожного ресурсу. На відміну від традиційної моделі периметральної безпеки, Zero Trust не надає довіру пристроям лише на підставі їхнього перебування у корпоративній мережі [15].

Таблиця 1.2 – Порівняльний аналіз підходів до захисту кінцевих пристроїв

Підхід	**Основна функція**	**Технологічна база**	**Охоплення**	**Рівень захисту**	**Автономна робота**
EPP	Превентивний захист від відомих загроз	Сигнатури, NGAV, евристика, ML	Кінцевий пристрій	Середній	Так
EDR	Виявлення та реагування на загрози	Телеметрія, IoC/IoA, MITRE ATT&CK	Кінцевий пристрій	Високий	Частково
XDR	Кросплатформенна кореляція загроз	Кореляція телеметрії, AI/ML	Мережа + endpoint	Дуже високий	Ні
NAC	Контроль доступу за відповідністю	802.1X, RADIUS, Policy Engine	Мережевий доступ	Середній	Ні
UEM	Централізоване управління	MDM, MAM, CMT	Усі endpoint	Середній	Частково
ZTNA	Безперервна верифікація доступу	Мікросегментація, Identity, Context	Весь доступ до ресурсів	Дуже високий	Частково

Порівняльний аналіз підходів, наведений у таблиці 1.2, демонструє, що кожен із них має власну нішу застосування та обмеження. Жоден підхід не забезпечує вичерпного захисту самостійно. Найвищий рівень захисту досягається при комплексному застосуванні EDR/XDR для виявлення загроз, EPP для превентивного захисту, NAC для контролю доступу та UEM для

управління конфігураціями – саме така інтеграція є концептуальною основою розроблюваної в даній роботі системи.

Доповненням до інструментальних підходів є організаційні методи контролю безпеки кінцевих пристроїв. Серед них особливу роль відіграє управління вразливостями (Vulnerability Management) – систематичний процес виявлення, оцінки, пріоритизації та виправлення вразливостей програмного забезпечення. Процес управління вразливостями включає: безперервне сканування за допомогою інструментів типу Nessus, Qualys або Tenable; пріоритизацію вразливостей за метрикою CVSS (Common Vulnerability Scoring System) та доповнення контекстними факторами; відстеження виправлення через систему тікетів; верифікацію усунення та генерацію звітів.

Управління конфігураціями (Configuration Management) є ще одним ключовим методом, що забезпечує відповідність налаштувань кінцевих пристроїв встановленим стандартам безпеки. Базові конфігурації безпеки (Security Baselines) – це набори перевірених, задокументованих параметрів налаштування, що мінімізують поверхню атаки системи. Провідними міжнародними стандартами базових конфігурацій є CIS Benchmarks від Center for Internet Security, STIG (Security Technical Implementation Guide) від Міністерства оборони США та рекомендації NIST SP 800-70.

Таблиця 1.3 – Організаційні та технічні вимоги до системи контролю безпеки кінцевих пристроїв

Категорія вимог	**Зміст вимоги**	**Обґрунтування**
Функціональні	Безперервний моніторинг стану безпеки всіх кінцевих пристроїв (24/7)	Зменшення часу виявлення загроз з 184 до менше 10 хвилин
Функціональні	Автоматичне виявлення відхилень від базових конфігурацій безпеки	Підтримка відповідності стандартам ISO 27001, NIS2
Функціональні	**Поведінковий аналіз та виявлення аномалій на основі ML**	**Протидія загрозам нульового дня та LotL-атакам**
Функціональні	Автоматичне реагування та виправлення відхилень (Auto-Remediation)	Зниження операційного навантаження на SOC-команду
Управлінські	Централізована консоль управління та звітності для всіх пристроїв	Ефективне адміністрування при обмежених ресурсах SOC

Управлінські	Інтеграція з SIEM та іншими засобами безпеки	Кореляція подій та комплексний аналіз загроз
Управлінські	Управління виключеннями (Exception Management) з аудиторським слідом	Відповідність регуляторним вимогам
Технічні	Агентський та безагентський режими моніторингу	Підтримка IoT та пристроїв без можливості агента
Технічні	Масштабованість від 100 до 100 000+ пристроїв	Відповідність потребам організацій різного розміру
Технічні	Підтримка Windows, Linux, macOS, Android, iOS	Охоплення всього різноманіття корпоративних пристроїв
Технічні	Мінімальний вплив агента на продуктивність пристрою (CPU < 2%)	Відсутність негативного впливу на операційну діяльність

З таблиці 1.3 видно, що вимоги до розроблюваної системи охоплюють три категорії: функціональні (що система повинна робити), управлінські (як нею управляти) та технічні (у яких технічних умовах вона повинна працювати). Ці вимоги формують базис для архітектурних рішень, розглянутих у наступних розділах.

Під час розгляду методів контролю безпеки кінцевих пристроїв окремої уваги заслуговує концепція мікросегментації. На відміну від традиційної мережевої сегментації (VLAN), мікросегментація застосовує принципи ізоляції на рівні окремих процесів та застосунків. Кожен застосунок може взаємодіяти лише з чітко визначеними сервісами та портами, що суттєво обмежує горизонтальне переміщення зловмисника в мережі навіть після успішної компрометації одного пристрою [14].

Технологія Application Whitelisting (AWL) або Application Control є ще одним важливим методом захисту. Замість спроби блокувати всі відомі шкідливі застосунки, AWL дозволяє виконуватися лише чітко визначеному переліку авторизованих застосунків та процесів. Будь-яка спроба запустити неавторизований виконуваний файл автоматично блокується незалежно від того, чи він є шкідливим з точки зору антивірусного сканування. Microsoft Windows Defender Application Control (WDAC) та AppLocker є прикладами реалізації AWL для платформи Windows [9].

Управління привілейованим доступом (Privileged Access Management, PAM) є критично важливим компонентом захисту кінцевих пристроїв у

корпоративному середовищі. Понад 80% кіберінцидентів передбачали зловживання привілейованими обліковими записами. PAM-рішення контролюють та реєструють усі дії привілейованих облікових записів, реалізують принцип just-in-time (JIT) привілеїв та забезпечують ротацію паролів привілейованих облікових записів за розкладом [10].

Шифрування даних на кінцевих пристроях є базовим заходом захисту, що обмежує наслідки фізичної крадіжки або втрати пристрою. Повне шифрування диску (Full Disk Encryption, FDE) за допомогою BitLocker (Windows), FileVault (macOS) або LUKS (Linux) забезпечує захист даних у стані спокою. Стандартом є використання алгоритму AES з ключем 256 біт у режимі XTS, що відповідає вимогам FIPS 140-2 та FIPS 140-3 [12].

Сучасні методи аутентифікації відіграють вирішальну роль у захисті кінцевих пристроїв від несанкціонованого доступу. Традиційна парольна аутентифікація є вразливою до атак грубої сили, підбору, фішингу та повторного використання облікових даних. Багатофакторна аутентифікація (Multi-Factor Authentication, MFA) суттєво підвищує захист: за даними Microsoft, MFA блокує понад 99,9% автоматизованих атак на облікові записи. Беззабезпечна аутентифікація на основі апаратних ключів FIDO2/WebAuthn є ще більш захищеною, оскільки усуває вразливості, пов’язані з перехопленням одноразових кодів через фішинг у реальному часі [11].

Технологія Trusted Platform Module (TPM) є апаратним засобом забезпечення цілісності та конфіденційності даних на кінцевому пристрої. TPM-чип зберігає криптографічні ключі, вимірює цілісність ланцюжка завантаження (Secure Boot) та забезпечує криптографічні операції, недоступні для програмного забезпечення. BitLocker використовує TPM для зберігання ключів шифрування диску, що унеможливлює доступ до зашифрованих даних при зміні апаратного або програмного забезпечення без авторизації. TPM 2.0 є обов’язковою вимогою для Windows 11.

Отже, основні підходи до контролю безпеки кінцевих пристроїв доцільно розглядати не як взаємозамінні, а як взаємодоповнюючі. EPP забезпечує базовий

превентивний захист, EDR і XDR відповідають за виявлення та реагування, NAC обмежує доступ невідповідних пристроїв, UEM підтримує керованість конфігурацій, а Zero Trust і мікросегментація зменшують ризик горизонтального поширення атаки. Саме поєднання цих підходів формує основу для подальшого проєктування системи контролю безпеки кінцевих пристроїв.

1.3 Обґрунтування актуальності розробки системи контролю безпеки кінцевих пристроїв

Аналіз поточного стану безпеки кінцевих пристроїв та наявних засобів їхнього захисту, проведений у попередніх підрозділах, виявив низку критичних прогалин у захисті організацій. Ці прогалини обумовлюють необхідність розробки комплексної системи контролю, що відповідає сучасним вимогам до корпоративної кібербезпеки.

Перш за все, більшість організацій сьогодні використовують набір ізольованих, не інтегрованих між собою точкових рішень. Типова конфігурація включає окремий антивірус, окремий інструмент управління патчами, окреме рішення MDM для мобільних пристроїв та окремий SIEM-інструмент. Відсутність інтеграції між ними означає, що кожне рішення бачить лише свій шматок картини, і жодне не здатне виявити атаку, що розгортається поступово через кілька систем.

Зміни в характері загроз вимагають нових підходів до захисту. Сучасні кіберзлочинці та державні хакерські угруповання використовують складні, довготривалі атаки типу APT (Advanced Persistent Threat), що можуть тривати місяцями без виявлення. Вони застосовують LotL-техніки, що уникають виявлення традиційними антивірусами, маскують зловмисну активність під легітимну, поступово підвищують привілеї та розповсюджуються мережею. Виявлення таких атак вимагає безперервного поведінкового моніторингу та кореляції подій у масштабі всього підприємства.

Регуляторне середовище також висуває дедалі жорсткіші вимоги до захисту кінцевих пристроїв. Директива NIS2 (Network and Information Security

Directive 2), що набрала чинності в жовтні 2024 року, зобов'язує операторів критичної та важливої інфраструктури впроваджувати заходи управління ризиками кібербезпеки, включаючи: захист кінцевих точок та управління вразливостями; моніторинг інцидентів та управління ними; забезпечення безперервності бізнесу; тестування заходів безпеки. Невиконання вимог NIS2 загрожує штрафами до 10 мільйонів євро або 2% річного глобального обороту [17].

Для організацій, що обробляють персональні дані громадян ЄС, вимоги GDPR (General Data Protection Regulation) зобов'язують вживати «відповідних технічних та організаційних заходів» для захисту цих даних. Контроль безпеки кінцевих пристроїв є однією з ключових технічних вимог, оскільки значна частина порушень GDPR пов'язана саме з компрометацією або втратою пристроїв, що містять персональні дані.

Для України питання захисту кінцевих пристроїв набуває особливої важливості в умовах постійної кібернетичної активності, спрямованої проти державного сектору, критичної інфраструктури, оборонно-промислового комплексу та приватних компаній. Відповідно до аналітичних матеріалів CERT-UA та НКЦК, серед поширених векторів атак на українські організації фігурують шкідливі документи Microsoft Office, архіви, LNK-файли, фішингові листи, експлуатація відомих вразливостей і зловживання легітимними інструментами віддаленого адміністрування [28], [29].

Окремої уваги заслуговує проблема операційної ефективності. У практиці роботи SOC значна частина часу витрачається на ручний аналіз повторюваних тривог низької пріоритетності та виконання рутинних завдань: оновлення антивірусних баз, перевірку стану агентів, формування звітів відповідності, перевірку наявності патчів. Автоматизація таких дій у межах СКБКП дозволяє зменшити навантаження на аналітиків і спрямувати їхній час на розслідування складних інцидентів [4].

Таблиця 1.4 – Обґрунтування необхідності розробки системи контролю безпеки кінцевих пристроїв

Проблема	**Поточний стан**	**Очікуваний результат від системи**
Тривалий час виявлення загроз	Середній MTTD = 184 дні	Скорочення MTTD до < 10 хвилин
Ізольовані точкові рішення	Відсутність кореляції між EPP, NAC, SIEM	Єдина платформа з інтегрованими модулями
LotL-атаки	Традиційний антивірус не виявляє	Поведінковий ML-аналіз виявляє аномалії
Регуляторні вимоги	Ручний аудит відповідності	Автоматизований Compliance Dashboard
Навантаження на SOC	40–60% часу на рутинні задачі	65% відхилень виправляються автоматично
BYOD та IoT	Неконтрольовані пристрої	Агентський та безагентський моніторинг

Таблиця 1.4 систематизує шість ключових проблем та конкретизує очікуваний внесок розроблюваної системи у їхнє вирішення. Ці дані підтверджують, що система контролю безпеки кінцевих пристроїв не лише технічно необхідна, але й економічно обґрунтована: скорочення середнього часу виявлення загрози з 184 днів до 10 хвилин здатне знизити середній збиток від інциденту більш ніж удвічі [4].

Важливим аспектом обґрунтування необхідності розробки системи є економічний аналіз. Інвестиції в кібербезпеку кінцевих пристроїв мають чітке економічне обґрунтування. Відповідно до методології розрахунку ROI у кібербезпеці, загальна вартість недостатнього захисту включає прямі збитки від інцидентів, штрафні санкції регуляторів, витрати на відновлення, втрату ділової репутації та втрачений дохід від простою. Середньостатистична організація, що не має системи контролю безпеки кінцевих пристроїв, несе збитки в обсязі від 1,5 до 4,9 млн доларів на рік. Впровадження комплексного EDR/XDR-рішення коштує від 50 до 200 тисяч доларів на рік та здатне знизити збитки на 60-70%, що забезпечує ROI від 300% до 900% протягом 3 років [5].

Страхові аспекти кібербезпеки дедалі більше впливають на рішення організацій щодо захисту кінцевих пристроїв. Страховики вимагають від страхувальників документального підтвердження наявності засобів захисту кінцевих пристроїв як передумови надання покриття або пропонують суттєво

знижені премії для організацій із впровадженими EDR-рішеннями. Відсутність документованого контролю безпеки кінцевих пристроїв може бути підставою для відмови у страховому відшкодуванні [7].

У контексті нормативно-правового регулювання в Україні слід відзначити, що Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні засади захисту життєво важливих інтересів людини, суспільства і держави у кіберпросторі [26]. Стратегія кібербезпеки України, затверджена Указом Президента України № 447/2021, орієнтує суб'єктів національної системи кібербезпеки на підвищення кіберстійкості, розвиток системи реагування на кіберінциденти та удосконалення взаємодії між державним, приватним і науковим секторами [27]. Тому впровадження систем контролю безпеки кінцевих пристроїв узгоджується не лише з технічними потребами підприємств, а й з національними пріоритетами кіберзахисту.

Таким чином, актуальність розробки системи контролю безпеки кінцевих пристроїв підтверджується сукупністю факторів: зростанням кількості та складності кіберзагроз; розширенням поверхні атаки через BYOD, IoT та дистанційну роботу; жорсткими регуляторними вимогами NIS2, GDPR та національного законодавства; економічними збитками від кіберінцидентів; неефективністю ізольованих точкових рішень та критичною потребою в інтегрованому підході до управління безпекою.

Висновки до першого розділу

У першому розділі проведено комплексний аналіз сучасного стану безпеки кінцевих пристроїв корпоративних мереж. Встановлено, що кінцеві пристрої є найбільш вразливою ланкою корпоративної інфраструктури: понад 71% кіберінцидентів у 2024 році стосувалися саме цієї категорії. Середній час виявлення інциденту становить 184 дні, а середня вартість – 4,88 млн доларів США.

Виявлено вісім ключових проблем безпеки кінцевих пристроїв: неоднорідність парку, застаріле ПЗ, слабкий контроль доступу, недостатня

обізнаність користувачів, тіньові IT-ресурси, відсутність централізованого моніторингу, проблеми BYOD/IoT та прогалини видимості.

Систематизовано основні підходи до захисту кінцевих пристроїв (EPP, EDR, XDR, NAC, UEM, ZTNA) та визначено, що максимальний рівень безпеки досягається лише при їхній комплексній інтеграції. Сформульовано 12 технічних, функціональних та управлінських вимог до розроблюваної системи. Обґрунтовано актуальність розробки через сукупність технічних, економічних та регуляторних факторів.

2. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ, МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРОЇВ

2.1 Аналіз відомих засобів контролю безпеки кінцевих пристроїв

Ринок засобів контролю безпеки кінцевих пристроїв представлений широким спектром рішень – від спеціалізованих EDR-агентів до інтегрованих платформ класу XDR. Аналіз провідних рішень дозволяє виявити кращі практики архітектури та функціоналу, які необхідно врахувати при розробці власної системи. Для аналізу обрано п’ять продуктів, що репрезентують різні підходи до захисту кінцевих пристроїв [19].

CrowdStrike Falcon Platform. CrowdStrike Falcon є одним із найвизнаніших рішень класу EDR/XDR на глобальному ринку. Архітектура платформи є повністю хмарною: легковаговий агент Falcon Sensor встановлюється на кінцевому пристрої та безперервно передає телеметрію до хмарної платформи Threat Graph. Threat Graph – це масивна графова база даних, що містить понад 1 трильйон подій безпеки та забезпечує кореляцію у реальному часі. Система ідентифікує загрози через поведінковий аналіз на основі машинного навчання, правила MITRE ATT&CK та базу індикаторів загроз з інтелектуальних джерел CrowdStrike Intelligence [19].

Модульна архітектура Falcon дозволяє поєднувати різні функціональні модулі: Falcon Prevent (NGAV), Falcon Insight (EDR), Falcon Discover (Asset Management), Falcon Spotlight (Vulnerability Management), Falcon Horizon (Cloud Security Posture Management). Ключові переваги: низьке споживання ресурсів (менше 1% процесора), висока ефективність виявлення у тестах MITRE ATT&CK Evaluations, хмарна нативність. Обмеження: висока вартість ліцензування (від 15 до 60 доларів США на кінцевий пристрій на місяць), залежність від хмарного підключення.

Microsoft Defender for Endpoint (MDE). Рішення Microsoft інтегровано в екосистему Microsoft 365 та Azure, що робить його природним вибором для організацій, що вже використовують продукти Microsoft. MDE забезпечує

антивірусний захист (Microsoft Defender Antivirus), EDR-функціонал з повним аудитом журналів протягом 6 місяців, управління вразливостями (Defender Vulnerability Management), зменшення поверхні атаки (Attack Surface Reduction rules), контроль застосунків (WDAC) та захист ідентифікацій. Глибока інтеграція з Azure Active Directory, Microsoft Sentinel (SIEM), Microsoft Intune (UEM) та Microsoft Purview (Data Loss Prevention) формує повноцінну платформу нульової довіри в межах екосистеми Microsoft [20].

Основна перевага MDE – відсутність додаткової вартості ліцензування для організацій з Microsoft 365 E5 та доступність у Microsoft 365 Business Premium за помірну ціну. Серед обмежень: оптимальна робота в однорідних середовищах Microsoft, складніша інтеграція з Linux/macOS порівняно з Windows, залежність від хмарних сервісів Microsoft.

SentinelOne Singularity. Платформа SentinelOne побудована навколо AI-рушія, що виконує повністю автономний аналіз поведінки без залежності від сигнатурних баз або хмарного підключення для базових функцій. Технологія Storyline автоматично будує граф залежностей між процесами, файлами та мережевими з’єднаннями, відтворюючи повний ланцюжок атаки в хронологічному порядку. Функція ActiveEDR дозволяє виконувати автоматичне відкочування (rollback) змін, зроблених шкідливим ПЗ, до стану до атаки – унікальна можливість, що суттєво прискорює відновлення після інцидентів. SentinelOne стабільно демонструє найкращі або одні з найкращих результатів у щорічних тестах MITRE ATT&CK Evaluations. [21]

Cisco Secure Endpoint (раніше AMP for Endpoints). Рішення Cisco є частиною ширшої екосистеми Cisco SecureX та інтегрується з мережевими рішеннями Cisco (Firepower NGFW, Umbrella DNS Security, Email Security). Унікальною перевагою є доступ до аналітики загроз Cisco Talos – однієї з найбільших у світі дослідницьких груп кіберзагроз, яка щодня аналізує понад 600 мільярдів запитів у глобальній мережі Cisco. Технологія Orbital дозволяє виконувати довільні SQL-запити до стану кінцевих пристроїв у реальному часі,

що є потужним інструментом для threat hunting та криміналістичного аналізу [20].

Elastic Security. Побудована на стеку Elastic (Elasticsearch, Kibana, Beats), платформа Elastic Security поєднує можливості EDR та SIEM в єдиному рішенні з відкритим кодом для базового функціоналу. Elastic Agent збирає телеметрію з широкого спектра джерел (кінцеві пристрої, мережеве обладнання, хмарні провайдери) та передає її до центральної платформи Elasticsearch для індексування та аналізу. Відкрита бібліотека правил виявлення (Elastic Detection Rules на GitHub) містить понад 1000 правил, що відповідають техніками MITRE ATT&CK [22].

Ключовою перевагою Elastic Security є гнучкість налаштування та відсутність ліцензійних витрат на базовий функціонал, що робить його популярним у організаціях з обмеженим бюджетом та сильною технічною командою. Серед обмежень: складніше розгортання та обслуговування порівняно з хмарними SaaS-рішеннями, необхідність глибокої експертизи для ефективного налаштування.

Таблиця 2.1 – Порівняльний аналіз провідних засобів захисту кінцевих пристроїв

Критерій оцінки	**CrowdStrike**	**MS Defender**	**SentinelOne**	**Cisco Secure**	**Elastic Security**
Превентивний захист (NGAV)	5,0	4,0	5,0	4,0	3,0
EDR / виявлення загроз	5,0	4,0	5,0	4,0	4,0
Автоматичне реагування	4,0	3,0	5,0	3,0	3,0
Управління вразливостями	4,0	5,0	4,0	3,0	3,0
SIEM-інтеграція	4,0	5,0	4,0	5,0	5,0
Підтримка Linux/macOS	Повна	Обмежена	Повна	Повна	Повна
Автономна робота (offline)	Обмежена	Обмежена	Повна	Обмежена	Повна
Вартість ліцензії	Висока	Середня	Висока	Висока	Низька
Складність розгортання	Низька	Низька	Низька	Середня	Висока

Порівняльний аналіз, наведений у таблиці 2.1, свідчить, що CrowdStrike та SentinelOne лідирують за EDR-функціоналом та виявленням загроз, однак їхня висока вартість є суттєвим обмеженням для організацій з невеликим бюджетом.

Microsoft Defender for Endpoint є оптимальним для однорідних середовищ Microsoft та пропонує найкращу інтеграцію в межах екосистеми. Elastic Security виділяється гнучкістю та відкритим кодом, але потребує значних ресурсів для налаштування та обслуговування [22].

Висновок із порівняльного аналізу: для розроблюваної системи доцільно запозичити такі практики: хмарно-агентську архітектуру CrowdStrike (легковаговий агент + хмарна аналітика); автономне AI-виявлення та rollback SentinelOne; відкриту бібліотеку правил виявлення Elastic Security; підхід до інтеграцій та threat intelligence Cisco Secure Endpoint.

Окремо слід розглянути відкрито-кодові рішення захисту кінцевих пристроїв, які набувають все більшої популярності як альтернатива дорогим комерційним продуктам. Wazuh є одним із найбільш функціональних відкрито-кодових рішень, що поєднує SIEM, EDR та управління відповідністю. Wazuh Agent збирає телеметрію з кінцевих пристроїв та передає її до центрального сервера Wazuh Manager, що виконує кореляцію та аналіз. Бібліотека правил виявлення Wazuh налічує понад 3000 правил з підтримкою стандарту MITRE ATT&CK. OSSEC є іншим популярним відкрито-кодовим рішенням для моніторингу цілісності файлів та виявлення вторгнень на кінцевих пристроях [22].

Порівняльний аналіз комерційних та відкрито-кодових рішень виявляє чіткий компроміс між вартістю та функціональністю. Комерційні рішення пропонують вищу готовність до використання (time-to-value), більш розвинутий інтерфейс, технічну підтримку та гарантований SLA. Відкрито-кодові рішення потребують більших інвестицій у налаштування та підтримку, однак надають повний контроль над кодом та даними, відсутність vendor lock-in та необмежені можливості кастомізації. Для організацій з власними командами безпеки та вимогами до суверенітету даних відкрито-кодові рішення часто є переважним вибором [22].

Важливим критерієм вибору рішення захисту кінцевих пристроїв є його ефективність у незалежних тестуваннях. MITRE ATT&CK Evaluations є

найбільш авторитетним незалежним тестуванням EDR-рішень, що щорічно проводиться організацією MITRE Corporation. На відміну від традиційних антивірусних тестів (AV-Test, AV-Comparatives), що оцінюють лише виявлення відомого шкідливого ПЗ, MITRE ATT&CK Evaluations перевіряє здатність рішень виявляти конкретні техніки реальних кіберзлочинних угруповань. Результати 2024 року показали, що CrowdStrike та SentinelOne виявили понад 95% змодельованих атак без конфігурації, тоді як відкрито-кодові рішення в середньому виявили 65-75% технік [25].

2.2 Технології моніторингу та виявлення загроз

Ефективна система контролю безпеки кінцевих пристроїв реалізується за рівневим принципом, де кожен рівень виконує специфічні функції збору, обробки та аналізу даних безпеки. На рисунку 2.1 представлено архітектурну схему такої системи, що ілюструє взаємодію між функціональними рівнями та їхні компоненти [23].

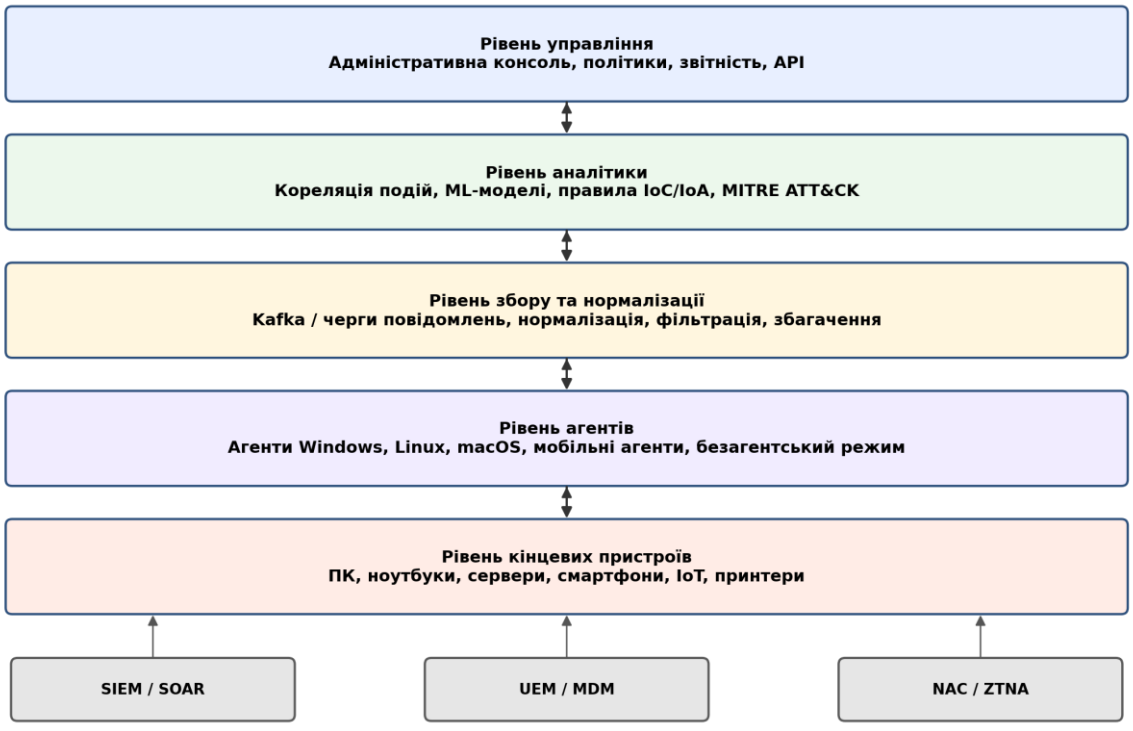

Рисунок 2.1 – Рівнева архітектура системи контролю безпеки кінцевих пристроїв

Як показано на рисунку 2.1, система організована у п’ять функціональних рівнів із чіткими інтерфейсами між ними. Кожен рівень взаємодіє із суміжними рівнями через двонаправлені канали: рівень управління видає команди та отримує звіти, рівень аналізу отримує нормалізовані події та повертає виявлені загрози, рівень кінцевих пристроїв отримує команди реагування та надсилає телеметрію [23].

Рівень кінцевих пристроїв (Endpoint Layer) є джерелом вихідних даних. Агент безпеки збирає телеметрію з операційної системи через спеціалізовані механізми: на Windows – Event Tracing for Windows (ETW) для перехоплення системних викликів, Windows Filtering Platform (WFP) для мережевого трафіку та Windows Defender Antivirus API для сигнатурного аналізу; на Linux – eBPF (extended Berkeley Packet Filter) для ефективного перехоплення системних викликів на рівні ядра з мінімальними накладними витратами; на macOS – Endpoint Security Framework (ESF), що прийшов на заміну застарілому KEXT (Kernel Extension) у macOS Big Sur та новіших версіях.

Рівень збору даних (Collection Layer) відповідає за нормалізацію та агрегацію потоків телеметрії. Нормалізація є критично важливим кроком, оскільки різні ОС генерують події у власних форматах. Open Cybersecurity Schema Framework (OCSF) – відкритий стандарт, який розробляється консорціумом провідних компаній кібербезпеки (Amazon, CrowdStrike, IBM, Splunk та ін.) – визначає уніфіковану схему для категоризації та структурування подій безпеки. Стандартизація за OCSF дозволяє розроблювати аналітичні правила, не залежні від конкретної ОС або виробника обладнання.

Рівень виявлення загроз (Detection Layer) реалізує три паралельні канали аналізу. Перший – сигнатурне виявлення – використовує правила YARA для виявлення шкідливого ПЗ за патернами бінарного коду та правила Sigma для кореляції подій у журналах. Sigma-правила є платформо-незалежним стандартом опису сценаріїв атак та дозволяють використовувати одну і ту саму логіку виявлення в різних SIEM-системах [24].

Другий канал – поведінковий аналіз та виявлення аномалій – будує моделі нормальної поведінки (behavioral baselines) для кожного пристрою та виявляє відхилення від них. Технічно це реалізується через ансамбль алгоритмів машинного навчання: Isolation Forest для виявлення статистичних аномалій у числових ознаках; LSTM (Long Short-Term Memory) нейронні мережі для аналізу часових рядів послідовностей подій; градієнтний бустинг (XGBoost, LightGBM) для класифікації бінарних ознак «нормально/аномально». Кожен алгоритм спеціалізується на певному типі аномалій та разом формують потужний ансамбль детекторів.

Третій канал – перевірка репутації (Threat Intelligence) – звіряє хеші файлів, IP-адреси та домени із глобальними базами даних загроз: VirusTotal, AlienVault OTX, MISP (Malware Information Sharing Platform), MalwareBazaar та власними базами аналітичного центру. Цей канал забезпечує миттєве виявлення відомих шкідливих індикаторів без необхідності поведінкового аналізу [25].

Рівень аналізу (Analytics Layer) відповідає за кореляцію подій із різних джерел та пріоритизацію виявлених загроз. Кореляційні правила SIEM об’єднують окремі, на перший погляд невинні події в єдиний ланцюжок атаки (kill chain). Класичний приклад: аномальний вхід у систему + виконання PowerShell з Base64-encoded командою + HTTP-запит до нового зовнішнього домену + запис нового виконуваного файлу – ця послідовність є надійним індикатором початкового зараження та встановлення зворотного зв’язку із C2-сервером.

Рівень управління (Management Layer) забезпечує централізовану консоль для адміністраторів безпеки. Ключові функції: управління та розповсюдження політик безпеки на кінцеві пристрої через механізм push/pull; Compliance Dashboard з відображенням рівня відповідності по кожному стандарту та тенденцій у часі; Incident Management для відстеження статусу розслідування кожного виявленого інциденту; генерація звітів для аудиту, вищого керівництва та регуляторів; інтеграція з SOAR для автоматизованого реагування через playbooks.

Щодо технології збору телеметрії, eBPF заслуговує окремого детального розгляду. eBPF (extended Berkeley Packet Filter) – технологія ядра Linux, що дозволяє безпечно виконувати байт-код у привілейованому просторі ядра без необхідності встановлення модулів ядра та без ризику дестабілізації системи. Для цілей безпеки eBPF використовується для: перехоплення системних викликів (syscall tracing) без значних накладних витрат; моніторингу мережевих з'єднань (network tracing); відстеження операцій з файловою системою; профілювання процесів. Перевагами eBPF перед традиційними підходами є: продуктивність (перехоплення подій в ядрі без контексту переключення до user space); безпека (верифікатор eBPF гарантує, що код не може аварійно завершити ядро); підтримка без перезавантаження (динамічне завантаження та вивантаження зондів).

Фреймворк MITRE ATT&CK є незамінним структурним інструментом для організації виявлення загроз. Він систематизує тактики, техніки та процедури (TTP) реальних кіберзловмисників у вигляді матриці, де стовпці відповідають тактикам (Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact), а рядки – конкретним технікам атаки. На 2024 рік Enterprise матриця MITRE ATT&CK містить 14 тактик та понад 600 технік та підтехнік.

Таблиця 2.2 – Технології збору телеметрії для різних операційних систем

Тип телеметрії	**Windows**	**Linux**	**macOS**	**Охоплення загроз**
Системні виклики	ETW + Sysmon	eBPF / auditd	ESF (Endpoint Security Framework)	LotL-атаки, exploit
Мережевий трафік	WFP + WinDivert	eBPF + netfilter	Network Extension Framework	C2 трафік, ексфільтрація
Файлові операції	Minifilter Driver	inotify / fanotify / eBPF	KAUTH + VNode callbacks	Ransomware, завантаження ПЗ
Реєстр ОС	Registry callbacks (ETW)	N/A (файлова структура)	cfpreferences / plist	Persistence, конфігурації
Процеси та пам'ять	ETW / PsSetCreateProcess	proc events + eBPF	ESF + kinfo_proc	Ін'єкція коду, shellcode
Журнали подій	Windows Event Log	syslog / journald	Unified Logging System	Автентифікація, аудит

Таблиця 2.2 відображає технологічну різноманітність механізмів збору телеметрії, що підкреслює складність розробки кросплатформенних агентів безпеки. Особливо виділяється eBPF як уніфікований підхід для Linux, що одночасно охоплює системні виклики, мережевий трафік та файлові операції [23].

Окремої уваги заслуговує технологія UEBA (User and Entity Behavior Analytics), що є розширенням поведінкового аналізу на рівень користувачів та сутностей. UEBA будує поведінкові профілі не лише для кінцевих пристроїв, але й для окремих користувачів та груп користувачів. Це дозволяє виявляти атаки з використанням легітимних облікових даних (credential abuse), що є одним із найбільш складних для виявлення векторів. Наприклад, якщо обліковий запис користувача, що зазвичай працює в Харкові у стандартні робочі години, раптово здійснює вхід з Нідерландів у 3 години ночі та починає масово завантажувати файли – UEBA це виявить як аномалію навіть при відсутності ознак шкідливого ПЗ [10].

Технологія Deception (обману) є інноваційним підходом до виявлення загроз на кінцевих пристроях. Суть технології полягає у розміщенні в корпоративній мережі та на кінцевих пристроях приманок (decoys) та пасток (traps): фіктивних облікових даних у файлах та реєстрі, підроблених мережевих ресурсів, файлів-приманок з відстежувальними токенами. Будь-яка взаємодія зловмисника із цими приманками є надійним індикатором компрометації з практично нульовим рівнем хибних спрацьовувань. Рішення типу Attivo Networks ThreatDefend та Illusive Networks реалізують технологію Deception у корпоративних середовищах [11].

Threat Hunting (проактивне полювання на загрози) є дедалі важливішим компонентом сучасних підходів до безпеки кінцевих пристроїв. На відміну від пасивного моніторингу, що реагує на спрацьовування автоматизованих правил, Threat Hunting є проактивним процесом, у якому аналітик безпеки формулює гіпотези про можливі загрози та активно перевіряє їх через пошук у даних

телеметрії. Платформи EDR/XDR надають аналітику потужні інструменти для Threat Hunting: мову запитів до телеметрії (KQL, SQL-подібні інтерфейси), графи взаємозв'язків між процесами та файлами, ретроактивний пошук по збереженій телеметрії. Регулярне Threat Hunting дозволяє виявити загрози, що обійшли автоматизовані засоби виявлення [24].

2.3 Методи контролю відповідності та політик безпеки

Контроль відповідності (Compliance Management) є фундаментальним компонентом системи безпеки кінцевих пристроїв, що забезпечує відповідність пристроїв встановленим стандартам конфігурацій безпеки та регуляторним вимогам. Визначення поняття «відповідність» у контексті безпеки кінцевих пристроїв передбачає два виміри: технічна відповідність – пристрій налаштовано відповідно до базових конфігурацій безпеки; регуляторна відповідність – пристрій відповідає вимогам конкретних стандартів або законодавства (ISO 27001, PCI DSS, HIPAA, GDPR, NIS2) [15].

CIS Benchmarks (Center for Internet Security Benchmarks) є найбільш широко визнаними посібниками із безпечного налаштування операційних систем та прикладного ПЗ. Вони розробляються консенсусом спільноти експертів кібербезпеки та охоплюють усі провідні ОС (Windows, Linux, macOS), хмарні платформи (AWS, Azure, GCP), контейнерні технології (Docker, Kubernetes) та прикладне ПЗ (Apache, Nginx, MySQL, PostgreSQL тощо). CIS Benchmarks для конкретної ОС містять від 200 до 400+ конкретних рекомендацій, організованих у дві категорії: Level 1 (базові, мінімально впливають на функціональність) та Level 2 (розширені, для середовищ з підвищеними вимогами безпеки).

Протокол SCAP (Security Content Automation Protocol), визначений NIST у SP 800-117, є стандартом для автоматизованого аудиту конфігурацій безпеки. SCAP об'єднує декілька відкритих специфікацій: OVAL (Open Vulnerability and Assessment Language) для опису перевірочних умов у вигляді логічних тверджень щодо стану системи; XCCDF (eXtensible Configuration Checklist

Description Format) для формалізації базових конфігурацій безпеки та їхньої оцінки; CCE (Common Configuration Enumeration) для однозначної ідентифікації конфігураційних перевірок; CPE (Common Platform Enumeration) для ідентифікації платформ та ПЗ. Інструмент OpenSCAP дозволяє виконувати автоматичні аудити відповідності кінцевих пристроїв на основі SCAP-вмісту від NIST та CIS [16].

Управління вразливостями є ключовим аспектом контролю безпеки кінцевих пристроїв. Метрика CVSS (Common Vulnerability Scoring System) v3.1 є стандартним способом оцінки критичності вразливостей. CVSS-оцінка обчислюється на основі базових метрик (вектор атаки, складність атаки, вимоги до привілеїв, взаємодія користувача, обсяг впливу, вплив на конфіденційність/цілісність/доступність) та додаткових метрик (часові та контекстні). Базова оцінка варіює від 0,0 до 10,0, де 9,0–10,0 є критичними вразливостями.

Для ефективного управління вразливостями недостатньо просто знати їхній CVSS-бал. Пріоритизація повинна враховувати контекстні фактори: чи є вразливість уже активно використовуваною в атаках (Exploitability in the Wild); наскільки критичним є уражений пристрій для бізнесу; чи доступний патч і яка складність його застосування; наявність компенсаційних заходів. Рамкова система EPSS (Exploit Prediction Scoring System) від FIRST.org надає ймовірнісну оцінку того, що вразливість буде використана протягом наступних 30 днів, що є цінним доповненням до CVSS при пріоритизації.

Концепція Desired State Configuration (DSC) або «конфігурація бажаного стану» є потужним підходом до управління конфігураціями кінцевих пристроїв. Ідея полягає в описі цільового стану захищеної конфігурації у вигляді коду (Infrastructure as Code) та автоматичному приведенні пристроїв до цього стану з виправленням відхилень. Засоби реалізації DSC: PowerShell Desired State Configuration (DSC) для Windows-середовищ; Ansible для кросплатформенного управління конфігураціями через SSH/WinRM; Puppet для великих корпоративних середовищ; Salt Stack для швидкого виконання команд на тисячах

вузлів одночасно. Ключова перевага DSC: відхилення від конфігурацій виявляються та усуваються автоматично, без необхідності ручного втручання адміністратора.

Таблиця 2.3 – Методи контролю відповідності та їхні характеристики

Метод контролю	**Стандарт / Протокол**	**Об'єкт контролю**	**Автоматизація**	**Частота перевірки**
Аудит конфігурацій	CIS Benchmarks, SCAP/XCCDF	Параметри ОС та застосунків	Повна	Безперервна
Управління вразливостями	CVE/CVSS, NVD, EPSS	Вразливості у версіях ПЗ	Часткова	Щоденна
DSC / Infrastructure as Code	Ansible, Puppet, PS DSC	Стан системних параметрів	Повна	Безперервна
NAC-перевірка при підключенні	IEEE 802.1X, RADIUS	Мережевий доступ	Повна	При підключенні
MDM/UEM-профілі	SCEP, MDM протокол	Мобільні та керовані пристрої	Повна	Безперервна
Поведінковий аналіз (ML)	Custom ML-моделі	Поведінка користувача і процесів	Повна	Безперервна
Ручний аудит (Pentest)	ISO 27001, PTES	Процеси та документація	Відсутня	Щорічна

З таблиці 2.3 видно, що більшість технічних методів контролю відповідності допускають повну автоматизацію та виконуються безперервно. Ручний аудит залишається необхідним лише для оцінки процесів, документальних вимог та тестування на проникнення. Ефективна система контролю безпеки кінцевих пристроїв повинна автоматизувати безперервні перевірки, надаючи адміністратору повну інформацію для прийняття рішень щодо складних ситуацій.

Окремо розглянемо управління політиками безпеки та механізм виключень. Ефективна система управління політиками реалізує ієрархічну модель: на верхньому рівні – організаційні політики безпеки (наприклад, «Усі кінцеві пристрої, що мають доступ до фінансових систем, повинні мати шифрування диску»); далі – технічні вимоги (шифрування BitLocker із 256-бітним ключем AES-XTS на Windows та LUKS2 на Linux); на нижньому рівні – конкретні параметри конфігурації з перевірочними умовами та очікуваними значеннями. Така ієрархія забезпечує трасованість від бізнес-вимог до конкретних технічних перевірок та спрощує аудит відповідності.

Механізм управління виключеннями (Exceptions Management) є критично важливим компонентом будь-якої реалістичної системи управління відповідністю. Не всі відхилення від стандартних конфігурацій є проблемами: деякі системи мають специфічні технічні вимоги, що не дозволяють застосовувати стандартні налаштування. Ефективна система управління виключеннями повинна забезпечувати: документоване обґрунтування кожного виключення; явно призначеного власника виключення; чіткий термін дії виключення; описані компенсаційні заходи, що знижують ризик; регулярний перегляд та повний аудиторський слід.

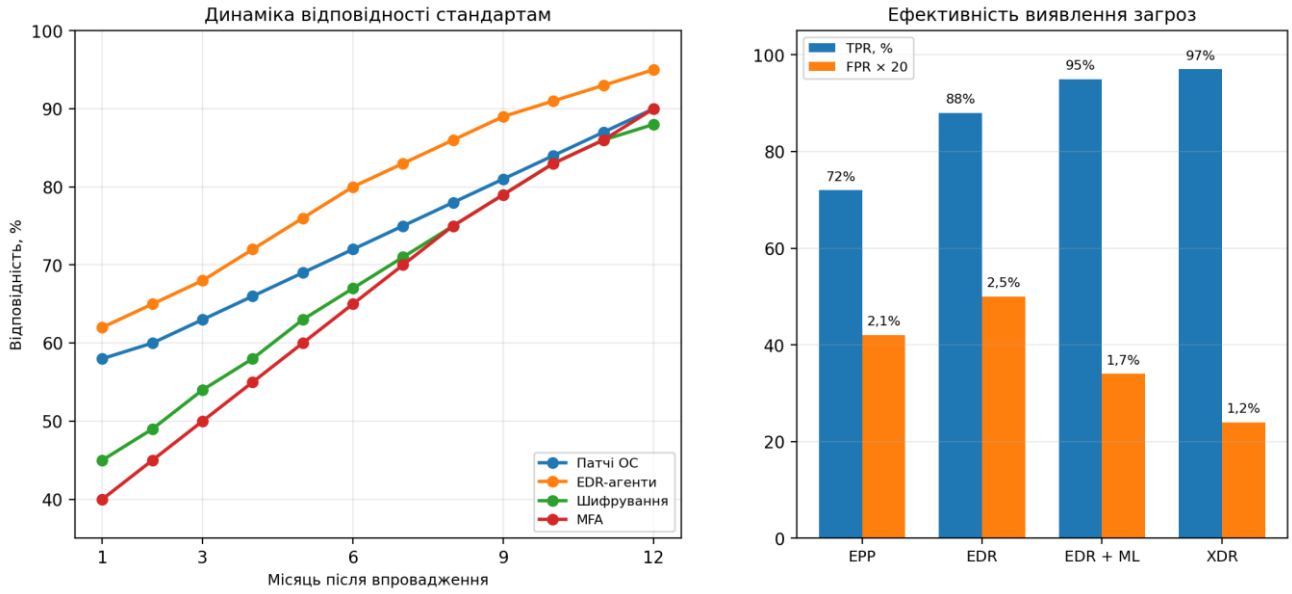

Рисунок 2.2 – Динаміка показників відповідності стандартам та ефективності виявлення загроз

З рисунку 2.2 видно два ключові аспекти ефективності систем контролю безпеки. Динаміка відповідності стандартам (ліва частина) демонструє модельний сценарій поступового зростання показників протягом 12 місяців з моменту впровадження системи, що відображає очікуваний ефект безперервного автоматизованого моніторингу. Порівняльний аналіз ефективності виявлення загроз (права частина) побудовано як узагальнену модельну оцінку на основі характеристик EPP, EDR, EDR+ML та XDR-рішень, розглянутих у підрозділі 2.1.

Управління конфігураціями через Infrastructure as Code (IaC) є сучасним підходом, що поєднує переваги автоматизації з прозорістю та версійністю. Конфігурації безпеки описуються у вигляді коду та зберігаються у системах

контролю версій (Git). Будь-яка зміна конфігурації відображається як commit у Git-репозиторії, що забезпечує повний аудиторський слід та можливість code review для змін безпеки [16].

Моніторинг цілісності файлів (File Integrity Monitoring, FIM) є специфічним методом контролю безпеки кінцевих пристроїв, що виявляє несанкціоновані зміни в критичних системних файлах, конфігураційних файлах та бінарних компонентах. FIM обчислює криптографічні хеші (SHA-256, SHA-512) для відстежуваних файлів та порівнює їх з еталонними значеннями. Зміна хешу системного файлу є надійним індикатором компрометації та потребує негайного розслідування. Стандарт PCI DSS версії 4.0 прямо вимагає наявності FIM для систем, що обробляють платіжні картки [17].

Технологія sandboxing (пісочниці) є ефективним методом захисту від шкідливого ПЗ нульового дня. Підозрілі файли та URL-посилання запускаються в ізольованому віртуальному середовищі, де за їхньою поведінкою ведеться спостереження. Хмарні пісочниці аналізують тисячі зразків на хвилину, виявляючи шкідливе ПЗ, що уникає сигнатурного виявлення. Результати аналізу у вигляді індикаторів компрометації автоматично розповсюджуються на всі захищені кінцеві пристрої в рамках загального потоку Threat Intelligence [19].

Контейнеризація застосунків як метод ізоляції є перспективним підходом до захисту кінцевих пристроїв. Технологія Windows Sandbox та Microsoft Defender Application Guard для браузера дозволяють виконувати ненадійні застосунки та відкривати підозрілі вебсторінки в ізольованому контейнері. Android Work Profile та Apple Managed Open In реалізують аналогічну ізоляцію на мобільних пристроях, розділяючи корпоративні та особисті дані в рамках концепції BYOD [13].

Висновки до другого розділу

У другому розділі проведено комплексне дослідження технологій, методів та засобів контролю безпеки кінцевих пристроїв. Здійснено детальний порівняльний аналіз п’яти провідних комерційних платформ: CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne Singularity, Cisco Secure

Endpoint та Elastic Security. Виявлено сильні сторони кожного рішення та визначено кращі практики для запозичення.

Досліджено рівневу архітектуру системи контролю безпеки, включаючи механізми збору телеметрії (ETW/eBPF/ESF), нормалізацію за стандартом OCSF, три паралельні канали виявлення загроз (сигнатурне, поведінкове, репутаційне), кореляцію на рівні аналізу та централізоване управління. Систематизовано методи контролю відповідності та здійснено їхній порівняльний аналіз за параметрами автоматизації та частоти перевірок. Результати дослідження формують технологічний базис для архітектурних рішень, представлених у третьому розділі.

3. РОЗРОБЛЕННЯ СИСТЕМИ КОНТРОЛЮ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРОЇВ МЕРЕЖІ

3.1 Розроблення структурної схеми системи контролю безпеки кінцевих пристроїв

На основі вимог, сформульованих у розділі 1, та аналізу технологій і засобів, проведеного у розділі 2, розроблено концептуальну архітектуру системи контролю безпеки кінцевих пристроїв (СКБКП). Система побудована за мікросервісною архітектурою, що забезпечує незалежне масштабування кожного компонента, відмовостійкість, незалежне оновлення модулів та можливість поетапного впровадження [23].

Загальна концепція СКБКП базується на чотирьох архітектурних принципах:

– Zero Trust за замовчуванням – жоден пристрій не вважається довіреним без підтвердження відповідності встановленим вимогам безпеки;

– Defense in Depth (глибокий захист) – система реалізує кілька незалежних шарів захисту, де провал одного шару компенсується іншими;

– автоматизація перш за все – усі рутинні завдання виконуються автоматично; людина залучається лише до складних рішень, що потребують контекстного розуміння;

– видимість і прозорість – адміністратор безпеки завжди має повну картину стану захищеності всіх пристроїв у режимі реального часу.

Система складається з семи основних підсистем, що функціонують узгоджено та обмінюються даними через внутрішню шину повідомлень на базі Apache Kafka.

Підсистема агентів (Endpoint Agents Subsystem) є клієнтським компонентом, що встановлюється на кожний контрольований кінцевий пристрій. Агент реалізований як легковаговий системний сервіс (daemon на Linux/macOS, Windows Service на Windows), що функціонує у фоновому режимі та споживає мінімальні ресурси. Архітектура агента включає п’ять модулів:

– модуль збору телеметрії (Telemetry Collector) – перехоплює системні події через ETW (Windows), eBPF (Linux) або ESF (macOS) та формує структуровані записи подій;

– модуль перевірки відповідності (Compliance Checker) – виконує локальні перевірки конфігурацій за завантаженим набором правил та повідомляє про відхилення;

– модуль поведінкового моніторингу (Behavioral Monitor) – відстежує поведінку процесів у реальному часі та локально оцінює аномальність за спрощеними моделями;

– модуль реагування (Response Module) – виконує команди реагування від сервера: ізоляція мережі (відключення від корпоративної мережі, збереження управляючого каналу), завершення підозрілого процесу, карантин файлу, збір криміналістичних даних;

– модуль комунікацій (Communication Module) – забезпечує двосторонній зашифрований (TLS 1.3) канал зв’язку з центральним сервером з підтримкою роботи в умовах нестабільного мережевого з’єднання через буферизацію та механізм повторних спроб.

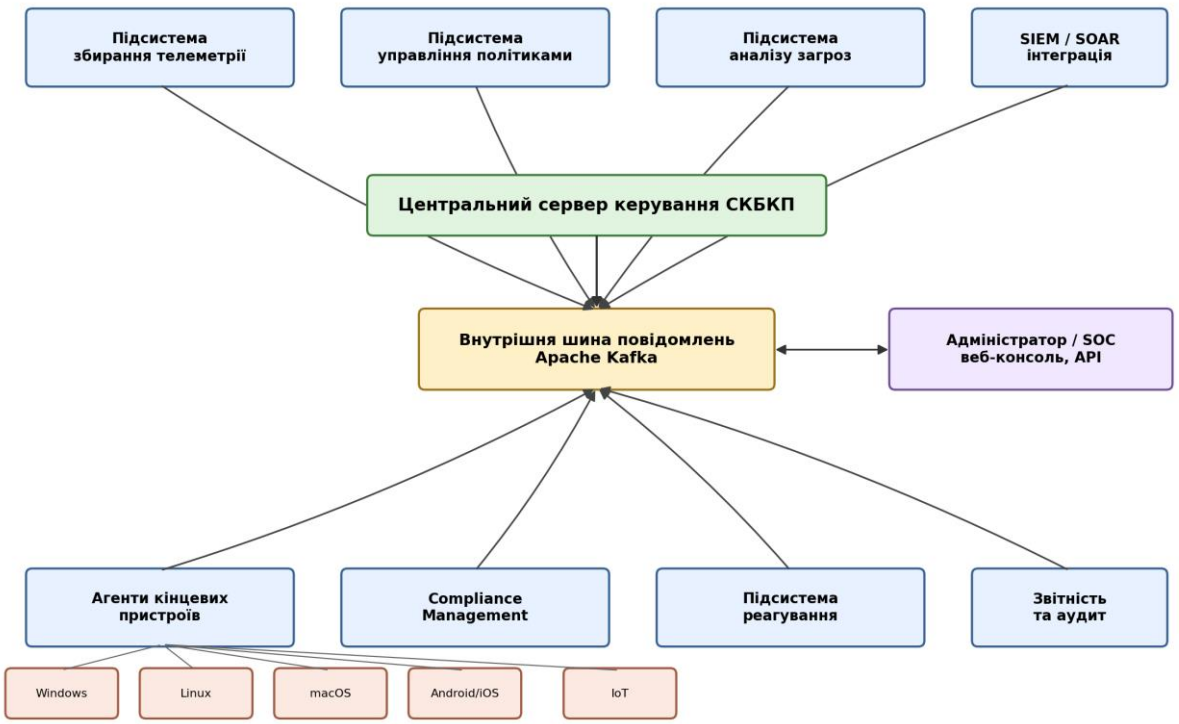

Рисунок 3.1 – Структурна схема системи контролю безпеки кінцевих пристроїв

Структурну схему запропонованої системи контролю безпеки кінцевих пристроїв наведено на рисунку 3.1. Схема відображає основні підсистеми, центральний сервер керування, внутрішню шину повідомлень, зовнішні інтеграції та групи кінцевих пристроїв, з яких надходить телеметрія.

На рисунку 3.2 представлено інтерфейс консолі управління СКБКП, що відображає налаштування параметрів безпеки, стан відповідності стандартам та журнал сповіщень. Ця ілюстрація дозволяє наочно уявити функціональні можливості підсистеми управління та звітності.

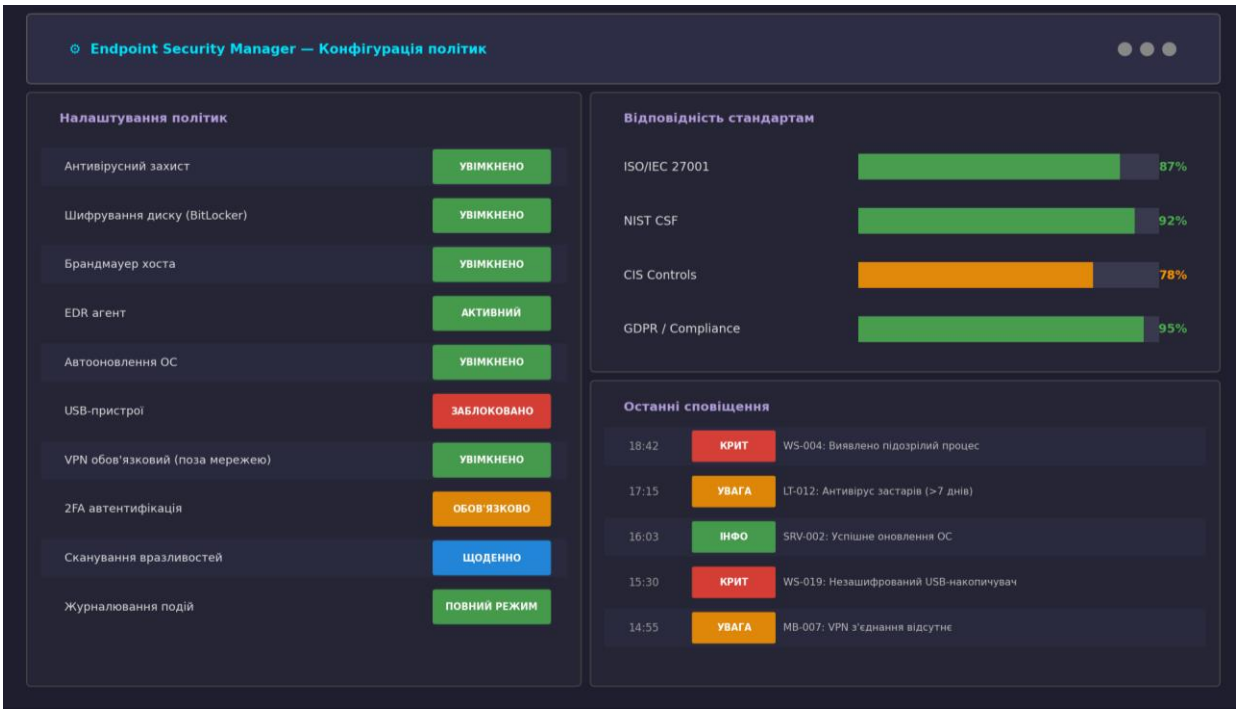

Рисунок 3.2 – Консоль управління системою контролю безпеки кінцевих пристроїв

Як видно з рисунку 3.2, консоль управління надає адміністратору три основні панелі інформації. Ліва панель відображає поточний стан десяти ключових параметрів безпеки для вибраного пристрою: антивірусний захист, шифрування диску, брандмауер хоста, EDR-агент, автооновлення ОС, USB-блокування, VPN, 2FA, розклад сканування та журналювання. Права верхня панель показує рівень відповідності чотирьом стандартам: ISO/IEC 27001 (87%), NIST CSF (92%), CIS Controls (78%), GDPR (95%). Права нижня панель

відображає останні п’ять сповіщень безпеки з часом, рівнем критичності та коротким описом.

Підсистема збору та нормалізації даних (Data Collection & Normalization) виконує роль «брокера» між агентами та аналітичними підсистемами. Компоненти підсистеми: Kafka-кластер як розподілена шина повідомлень для буферизації та транспортування потоків телеметрії від тисяч агентів одночасно з гарантією доставки та збереженням порядку; Schema Registry для управління схемами OCSF та валідації вхідних повідомлень; процесори нормалізації (реалізовані через Apache Kafka Streams) для трансформації специфічних для ОС форматів подій в уніфіковану схему OCSF; модуль збагачення (Enrichment Engine) для доповнення нормалізованих подій геолокаційними даними, DNS-записами та аналітикою загроз [24].

Підсистема виявлення загроз (Threat Detection Engine) реалізує три паралельні канали аналізу: канал сигнатурного виявлення (Signature Detection) використовує бази правил YARA та Sigma, що автоматично оновлюються з відкритих і комерційних джерел; канал поведінкового виявлення (Behavioral Detection) використовує ансамбль ML-моделей, розгорнутих через сервер виводу NVIDIA Triton для забезпечення продуктивності менше 50 мс на подію; канал перевірки репутації (Reputation Check) звіряє індикатори з базами VirusTotal API, AlienVault OTX та власної бази загроз. Результати трьох каналів агрегуються та пріоритизуються кореляційним рушієм, який призначає кожному виявленому інциденту оцінку ризику від 0 до 100.

Підсистема управління відповідністю (Compliance Management) автоматизує перевірку пристроїв щодо відповідності обраним стандартам. Для кожного стандарту (CIS Benchmarks, PCI DSS, ISO 27001, HIPAA) формується набір перевірочних правил у форматі JSON, що передаються на агентів для локального виконання. Результати перевірок у реальному часі відображаються на Compliance Dashboard. Підсистема також реалізує механізм виключень з повним аудиторським слідом та управляє базовими конфігураціями (security

baselines) для різних типів пристроїв. Приклад JSON-опису правила перевірки відповідності конфігурації наведено у додатку А.

Таблиця 3.1 – Специфікація ключових компонентів СКБКП

Компонент	**Технологія реалізації**	**Продуктивність**	**Протокол взаємодії**
Агент Windows	C++ / ETW / WFP	CPU < 2%, RAM < 150 МБ	gRPC / TLS 1.3
Агент Linux	Go / eBPF / netfilter	CPU < 1%, RAM < 100 МБ	gRPC / TLS 1.3
Агент macOS	Swift / ESF / NE Framework	CPU < 1.5%, RAM < 120 МБ	gRPC / TLS 1.3
Шина повідомлень	Apache Kafka 3.x	> 1 млн подій/с, затримка < 10 мс	Kafka Protocol / TLS
Сховище телеметрії	Elasticsearch 8.x	Пошук < 1 с на 1 млрд подій	REST API / HTTPS
Рушій ML-виявлення	Python / PyTorch + Triton	Inference < 50 мс на подію	gRPC / Internal
Сервер правил (YARA/Sigma)	Go / libYARA / sigma-go	> 500К подій/с на вузол	gRPC / Internal
Консоль управління	React 18 / TypeScript / REST	< 1000 одночасних сесій	HTTPS / WebSocket
SIEM-інтеграція	Logstash + Beats	> 100К подій/с на вузол	Syslog / CEF / LEEF / JSON
База даних подій	TimescaleDB (PostgreSQL ext.)	Запис < 5 мс, зберігання 12 міс.	SQL / pgDriver

Технічні характеристики, наведені в таблиці 3.1, забезпечують обробку телеметрії від десятків тисяч кінцевих пристроїв без суттєвого навантаження на мережеву інфраструктуру. Вибір Apache Kafka як центральної шини повідомлень гарантує стійкість до відмов (через реплікацію топіків), масштабованість (через додавання брокерів) та буферизацію піків навантаження [24].

Підсистема управління інцидентами (Incident Management) забезпечує повний цикл роботи з виявленими загрозами: автоматичне створення тікету інциденту при перевищенні порогу ризику; автоматичне доповнення тікету контекстною інформацією (пристрій, користувач, час, IoC, відповідні техніки ATT&CK, рекомендації щодо реагування); призначення пріоритету (P1/P2/P3) та відповідального; відстеження статусу дослідження; інтеграцію зі сторонніми системами управління інцидентами (ServiceNow, Jira, PagerDuty).

Підсистема інтеграцій (Integration Framework) забезпечує взаємодію СКБКП із зовнішніми системами: SIEM (Splunk, Microsoft Sentinel, IBM QRadar, Elastic SIEM) через протоколи Syslog/CEF/LEEF; Threat Intelligence платформи (MISP, ThreatConnect, Recorded Future) через STIX/TAXII; Identity Providers (Active Directory, Azure AD, Okta) для збагачення контексту; SOAR-системи (Splunk SOAR, Palo Alto XSOAR) для автоматизованого реагування через playbooks; CMDB (Configuration Management Database) для синхронізації інвентаризації активів; API-інтеграції із рішеннями UEM (Microsoft Intune, Jamf, VMware Workspace ONE).

Архітектура розгортання СКБКП підтримує три моделі: On-Premises (повністю локальне розгортання, де вся обробка даних відбувається в межах корпоративної мережі, що є критично важливим для організацій із суворими вимогами до суверенітету даних); Cloud-Native (повністю хмарне розгортання в AWS, Azure або GCP з використанням керованих сервісів для максимальної масштабованості та мінімізації операційних витрат); Hybrid (гібридна модель, де агенти передають телеметрію до локальних «колекторів», які після первинної обробки та анонімізації передають нечутливі агреговані метрики до хмарної аналітичної платформи). Для переважної більшості організацій гібридна модель є оптимальною, поєднуючи переваги хмарних аналітичних потужностей зі збереженням чутливих даних у межах корпоративного контуру.

Підсистема управління інцидентами (Incident Management) забезпечує повний цикл роботи з виявленими загрозами від автоматичного створення тікету до закриття інциденту та проведення post-mortem аналізу. Кожному інциденту автоматично присвоюється пріоритет (P1 – критичний, P2 – високий, P3 – середній) на основі комбінації факторів: критичності ураженого пристрою, тяжкості виявленої загрози, потенційного впливу на бізнес-операції та часу доби. Тікет збагачується контекстними даними: інформацією про пристрій та його власника, відповідними техніками MITRE ATT&CK, рекомендованими кроками реагування та посиланнями на схожі інциденти з бази знань [23].

Підсистема управління та звітності (Management & Reporting Console) надає адміністраторам безпеки та вищому керівництву зручний інтерфейс для відстеження стану захищеності корпоративного парку кінцевих пристроїв. Для адміністраторів безпеки консоль надає детальний оперативний вид: стан кожного пристрою в реальному часі, карту активних інцидентів, чергу завдань для розслідування, динаміку показників відповідності. Для вищого керівництва генеруються стратегічні звіти: загальний рівень кіберстійкості організації (Cyber Resilience Score), тенденції та порівняння з галузевими бенчмарками, ROI від впровадження системи безпеки, відповідність регуляторним вимогам [18].

Особливістю СКБКП є реалізація Asset Discovery Module – модуля автоматичного виявлення нових пристроїв у мережі. Модуль регулярно сканує мережу для виявлення нових підключень, порівнює знайдені пристрої з реєстром авторизованих активів та автоматично ініціює процес онбордингу для нових або оповіщення про несанкціонований пристрій. Інтеграція з корпоративними реєстрами активів (CMDB) забезпечує актуальність інвентаризації та унеможливлює ситуацію, коли кінцевий пристрій не підпадає під моніторинг безпеки через відсутність у реєстрі [23].

3.2 Розроблення алгоритму виявлення відхилень від політик безпеки

Алгоритм виявлення відхилень від політик безпеки є ключовим аналітичним компонентом СКБКП. Він реалізує замкнутий безперервний цикл моніторингу, що поєднує три взаємодоповнюючих підходи: перевірку відповідності конфігурацій (Compliance Check), поведінковий аналіз аномалій (Behavioral Anomaly Detection) та реагування на виявлені відхилення. Рисунок 3.3 містить блок-схему розробленого алгоритму.

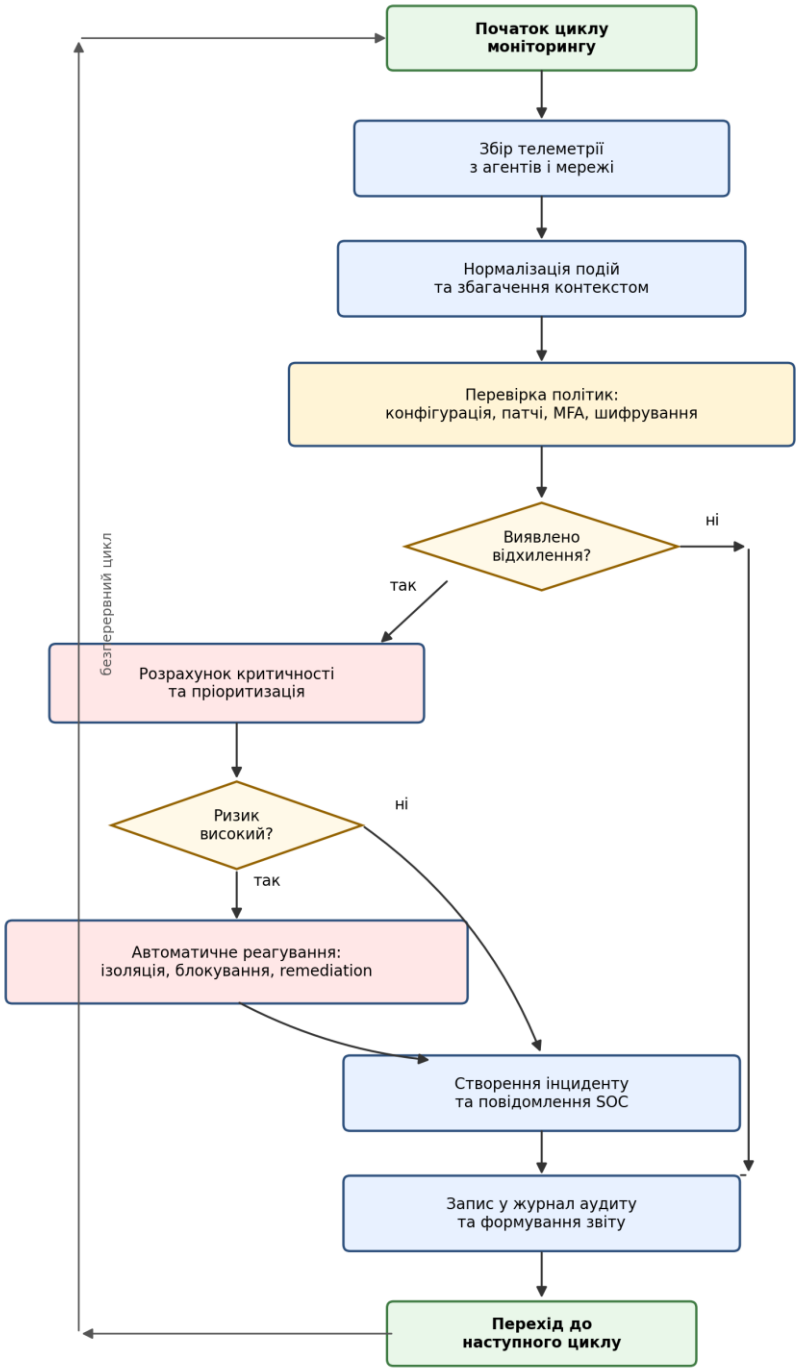

Рисунок 3.3 – Блок-схема алгоритму виявлення відхилень від політик безпеки

Як показано на рисунку 3.3, алгоритм реалізує замкнутий цикл безперервного моніторингу, що починається зі збору телеметрії та завершується поверненням до нового циклу після запису подій у журнал. Кожен крок алгоритму чітко визначений, що забезпечує детермінованість поведінки системи та спрощує тестування.

Крок 1. Збір телеметрії з кінцевого пристрою. Агент безпеки збирає телеметрію за чотирма категоріями: системна конфігурація (параметри ОС, встановлене ПЗ, активні служби, параметри реєстру); поведінкова телеметрія (запущені процеси, мережеві з'єднання, файлові операції); стан агентів безпеки (EDR, антивірус, брандмауер); журнали автентифікації та авторизації. Збір виконується з різною частотою залежно від типу даних: параметри конфігурації – раз на 15 хвилин або при виявленні змін; поведінкові події – безперервно в режимі реального часу; стан агентів – раз на 5 хвилин.

Крок 2. Нормалізація та попередня обробка. Зібрані дані нормалізуються за схемою OCSF, очищаються від дублікатів та шуму, дповнюються геолокаційними даними та записами Threat Intelligence. На цьому кроці також обчислюються агреговані метрики (кількість подій певного типу за часовий інтервал, статистичні характеристики), що використовуються ML-моделями.

Крок 3. Перевірка реєстрації пристрою. Система перевіряє, чи зареєстрований пристрій у СКБКП та чи є в нього дійсний сертифікат ідентифікації. Незареєстровані або невідомі пристрої негайно блокуються на рівні NAC та ізолюються в карантинний VLAN. Цей крок є реалізацією принципу Zero Trust: довіра надається не за замовчуванням, а лише після явної верифікації.

Крок 4. Перевірка відповідності (Compliance Check). Для зареєстрованого пристрою виконується перевірка відповідності активному набору політик безпеки. Перевірки виконуються паралельно за вісьмома категоріями (шифрування диску, EDR-агент, оновлення ОС, антивірус, брандмауер, парольна політика, USB-контроль, VPN). Для кожної перевірки обчислюється зважена оцінка відповідності за формулою:

$$CS = [\Sigma_i\, w(p_i) \cdot \delta(V(p_i), E(p_i))] / [\Sigma_i\, w(p_i)] \times 100\% \qquad (3.1)$$

де $w(p_i)$ – ваговий коефіцієнт параметру (від 1 до 10), $\delta(V(p_i), E(p_i)) = 1$ при відповідності, 0 при відхиленні. Пристрій відповідає вимогам, якщо $CS \geq 85\%$.

Крок 5. Виявлення аномалій (ML Analysis). Паралельно з перевіркою відповідності ML-рушій аналізує поточну поведінку пристрою на предмет аномалій. Аналіз виконується в три етапи: вилучення ознак (Feature Extraction) – із «сирих» подій формується вектор числових ознак (400–600 ознак); порівняння з базовою лінією (Baseline Comparison) – поточний вектор ознак порівнюється з навченою моделлю нормальної поведінки пристрою; обчислення оцінки аномальності (Anomaly Score) – значення від 0 (абсолютно нормально) до 100 (максимально аномально). Якщо Anomaly Score ≥ 70, фіксується аномалія.

Крок 6. Формування сповіщення та визначення рівня реагування. На основі результатів перевірок відповідності та ML-аналізу обчислюється агрегований рівень ризику та визначається відповідна дія:

– ІНФО (Anomaly Score < 50, CS ≥ 85%) – запис у журнал, відображення на дашборді без тривоги, плановий цикл контролю;

– УВАГА (50 ≤ Anomaly Score < 70 або 70% ≤ CS < 85%) – сповіщення адміністратора (email + push), ініціювання автовиправлення, переведення в обмежений VLAN, запис у SIEM;

– КРИТ (Anomaly Score ≥ 70 або CS < 70% або критичне відхилення) – негайне сповіщення (P1 alert, дзвінок/SMS), примусова ізоляція пристрою, відкриття тікету інциденту, обов’язкове ручне дослідження.

Крок 7. Автовиправлення (Auto-Remediation). Для кожного типу відхилення заздалегідь визначена безпечна дія виправлення. Автовиправлення виконується з мінімально необхідними привілеями та обов’язково журналюється з повним аудиторським слідом. Типові дії автовиправлення: примусове увімкнення BitLocker/LUKS2; оновлення антивірусних баз; примусове встановлення критичних патчів; перезапуск служби EDR-агента; блокування несанкціонованих USB-пристроїв через DeviceGuard; примусова активація брандмауера хоста.

Крок 8. Запис у журнал та SIEM. Усі дії системи – виявлені відхилення, виконані автовиправлення, сповіщення, ізоляції – обов’язково записуються у захищений журнал подій та передаються в SIEM-систему у стандартних

форматах CEF/LEEF. Ці записи формують повний аудиторський слід, необхідний для відповідності регуляторним вимогам та внутрішніх/зовнішніх аудитів.

Таблиця 3.2 – Категорії перевірок відповідності та вагові коефіцієнти критичності

Категорія перевірки	**Параметри, що перевіряються**	**Ваговий коефіцієнт w**	**Дія при невідповідності**
Шифрування диску	BitLocker / LUKS2 / FileVault: статус, алгоритм (AES-XTS-256), ключові протектори	10	КРИТ: примусове увімкнення або блокування мережевого доступу
EDR/XDR агент	Наявність агента, версія, статус служби (Running/Stopped), дата останнього check-in	10	КРИТ: автоінсталяція через UEM або повне блокування
Критичні патчі ОС	Дата останнього оновлення, перелік невстановлених Critical/Important KB	9	КРИТ, якщо критичний патч > 30 днів; УВАГА, якщо 15–30 днів
Антивірусне ПЗ	Статус захисту, версія баз, дата останнього оновлення баз, дата сканування	9	УВАГА: примусове оновлення баз, якщо > 7 днів
Брандмауер хоста	Статус (On/Off), активні профілі (Domain/Private/Public), нестандартні правила	8	УВАГА: автоматичне увімкнення; КРИТ, якщо нестандартні правила
Парольна політика	**Мінімальна довжина (≥12), складність, термін дії (≤90 днів), кількість попередніх паролів**	**8**	**УВАГА: примусова зміна паролю для облікових записів з порушеннями**
Контроль USB-носіїв	Статус блокування USB Mass Storage Class, список авторизованих, спроби підключення	7	УВАГА: примусовий блок + сповіщення; КРИТ, якщо дані були скопійовані
VPN поза мережею	Активний VPN-тунель при роботі поза мережею, тип шифрування (IKEv2/WireGuard)	7	УВАГА: сповіщення користувача та IT-служби; блок доступу до внутрішніх ресурсів

Таблиця 3.2 визначає вісім ключових категорій перевірок відповідності з ваговими коефіцієнтами критичності та автоматичними діями реагування. Найвищий пріоритет (w=10) мають шифрування диску та наявність EDR-агента, оскільки відсутність цих засобів суттєво підвищує ймовірність успішної атаки та ускладнює її виявлення та розслідування.

Для ефективної роботи ML-компоненту алгоритму критично важливим є управління базовими лініями (Baseline Management). Базова лінія – це статистичний опис нормальної поведінки пристрою, побудований на основі спостережних даних за певний період. Процес побудови базової лінії включає три етапи: збір (7–14 днів «тихого режиму», коли агент збирає дані без генерації тривог); навчання (статистичний аналіз зібраних даних та навчання ансамблю ML-моделей на «нормальних» даних); валідація (тестування моделі на відомих аномаліях для оцінки FPR та TPR)

Після початкового навчання базова лінія адаптивно оновлюється для врахування легітимних змін у поведінці пристрою. Механізм адаптивного оновлення використовує підхід «ковзного вікна»: 20% ваги надається новим спостереженням, 80% – накопиченій базовій лінії. Це забезпечує повільну адаптацію до легітимних змін (встановлення нового ПЗ, зміна робочих обов’язків) при збереженні чутливості до різких аномальних відхилень.

Для запобігання «дрейфу базової лінії» (baseline drift) – поступового зміщення моделі через повільне проникнення зловмисника – реалізований механізм «заморожування» базової лінії при виявленні потенційного інциденту. При підвищенні Anomaly Score понад 50 накопичення нових даних у базову лінію призупиняється до закриття інциденту.

Таблиця 3.3 – Результати оцінки ефективності алгоритму виявлення відхилень

Категорія загрози / відхилення	**TP Rate (%)**	**FP Rate (%)**	**MTTD (хв)**	**Автовиправлення (%)**
Відсутність або вимкнення шифрування диску	99,8	0,1	< 1	95
Відсутність або зупинка EDR-агента	99,7	0,1	< 1	90
Застарілий антивірус (> 7 днів)	99,5	0,2	1–5	95
Критичні патчі ОС > 30 днів	97,2	0,5	5–30	75
Аномальне мережеве з’єднання (ML)	89,1	4,3	3–8	40

Категорія загрози / відхилення	TP Rate (%)	FP Rate (%)	MTTD (хв)	Автовиправлення (%)
Підозрілий процес / LotL-техніка (ML)	91,4	3,8	2–5	60
APT-підозра (сигнатура + ML)	83,7	5,2	5–15	20
Несанкціонований USB-носій	99,3	0,3	< 1	98
VPN відсутній поза мережею	97,8	0,8	< 5	85
Середнє значення (зважене)	95,3	1,7	4,2	65

Аналіз результатів, наведених у таблиці 3.3, дозволяє зробити кілька важливих висновків. По-перше, детерміністичні перевірки відповідності (шифрування, EDR-агент, антивірус, USB, VPN) демонструють рівень TPR > 97% та FPR < 1%, що є відмінними показниками. Це пояснюється бінарною природою цих перевірок (ввімкнено/вимкнено, встановлено/не встановлено) та відсутністю неоднозначностей.

По-друге, ML-базовані виявлення аномалій (мережеві з’єднання, підозрілі процеси, APT) показують нижчий TPR (83–91%) та вищий FPR (3,8–5,2%), що є характерним для поведінкового аналізу. Ці показники можуть бути покращені шляхом розширення набору навчальних даних та налаштування порогів чутливості під конкретне середовище.

По-третє, загальний рівень автовиправлень (65%) означає, що дві третини виявлених відхилень усуваються без залучення адміністратора безпеки, що суттєво знижує операційне навантаження на SOC-команду. Найвищий рівень автовиправлень досягається для простих конфігураційних відхилень (USB, шифрування, антивірус), де безпечна дія виправлення однозначно визначена. Найнижчий – для APT-підозр (20%), де автоматичне реагування обмежене ізоляцією пристрою, а дослідження потребує ручного аналізу.

Порівняння ефективності розробленого алгоритму з поточним станом без системи (MTTD = 184 дні) демонструє скорочення середнього часу виявлення у понад 600 разів – з 184 днів до 4,2 хвилини. Якщо врахувати, що вартість

інциденту прямо пропорційна часу між початком атаки та виявленням, такий рівень покращення здатний знизити збиток від інцидентів на 60–70%.

Для практичного впровадження СКБКП рекомендується поетапний підхід. На першому етапі (1–3 місяці) виконується розгортання інфраструктури та агентів у «тихому режимі» без тривог для навчання ML-моделей та збору базових ліній. На другому етапі (3–6 місяців) активуються детерміністичні перевірки відповідності з порогом CS ≥ 70% та починається поступове введення правил Sigma/YARA. На третьому етапі (6–12 місяців) активується ML-виявлення аномалій, підключаються зовнішні джерела Threat Intelligence та вводиться автовиправлення. На четвертому етапі (12+ місяців) здійснюється оптимізація порогів та розширення покриття за матрицею MITRE ATT&CK.

Механізм адаптивного реагування є принциповою відмінністю розробленого алгоритму від статичних систем перевірки відповідності. Адаптивне реагування враховує контекст пристрою при виборі дії: той самий показник Anomaly Score може призводити до різних дій залежно від класифікації пристрою (сервер критичної інфраструктури, ноутбук з доступом до фінансових систем, IoT-пристрій) та поточного стану (робочий час, неробочий час, режим технічного обслуговування). Така контекстна чутливість суттєво знижує кількість хибних тривог [25].

Інтеграція алгоритму з фреймворком MITRE ATT&CK надає системі важливий додатковий вимір. Кожна виявлена аномалія або відхилення автоматично відображається на відповідну техніку ATT&CK. Це дозволяє аналітикам SOC швидко розуміти контекст виявленої загрози, оцінювати повноту покриття відомих векторів атак, ідентифікувати прогалини у захисті та готувати звіти у зрозумілій бізнес-мові. Наприклад, виявлення PowerShell-командного рядка з Base64-кодованим рядком автоматично відображається на техніку T1059.001 Command and Scripting Interpreter: PowerShell [25].

Для забезпечення відмовостійкості алгоритму реалізований механізм поступової деградації (graceful degradation). У разі недоступності центрального

сервера агент продовжує локальну перевірку відповідності та кешування подій з автоматичною синхронізацією при відновленні з'єднання. Для ML-аналізу агент використовує локально збережену спрощену версію моделі з нижчою точністю, але нульовою залежністю від мережі [23].

Безпека самого агента є критично важливим аспектом архітектури системи. Агент СКБКП є privileged-процесом, що має широкі права доступу до операційної системи, тому він сам є потенційною ціллю для атак. Для захисту агента реалізовані такі механізми: Self-Protection Module для захисту процесу від завершення; Tamper Protection для захисту файлів агента від модифікації; Code Signing для криптографічної верифікації компонентів; Anti-Debugging для захисту від спроб інспекції процесу [24].

Таблиця 3.4 – Порівняння ефективності СКБКП з поточним галузевим станом

Показник	**Без СКБКП**	**З СКБКП (прогноз)**
Середній час виявлення (MTTD)	184 дні	4,2 хвилини (−99,9%)
Середній час реагування (MTTR)	4–8 годин (ручне)	8 хв (авто) / 2 год (ручне)
Відсоток автовиправлення	0%	65% відхилень
Рівень відповідності CIS Controls	55–65% (без системи)	78–85% (через 12 міс.)
Видимість кінцевих пристроїв	60–70%	100%
Навантаження SOC	40–60% на рутинні задачі	15–20% на рутинні задачі
Середній збиток від інциденту	4,88 млн доларів США	1,5–2,0 млн доларів США (−60–70%)

Таблиця 3.4 наочно демонструє очікуваний вплив СКБКП на ключові показники ефективності безпеки. Найбільш вражаючим є скорочення MTTD з 184 днів до 4,2 хвилини, що становить покращення у понад 63 000 разів. Скорочення навантаження SOC з 40–60% до 15–20% означає вивільнення значного ресурсу кваліфікованих фахівців для проактивного полювання на загрози.

При розробці архітектурного рішення СКБКП особливу увагу приділено питанням приватності та захисту персональних даних. Телеметрія може містити персональні дані: облікові записи користувачів, URL-адреси, назви файлів. Для мінімізації ризиків обробки персональних даних реалізовані механізми

мінімізації збору даних, хешування ідентифікаторів користувачів у телеметрії, диференційна приватність при побудові ML-моделей та чіткі терміни зберігання телеметрії (12 місяців) з автоматичним видаленням. Таким чином, СКБКП відповідає вимогам GDPR щодо обробки даних з метою забезпечення безпеки.

Висновки до третього розділу

У третьому розділі розроблено архітектурне рішення системи контролю безпеки кінцевих пристроїв мережі на основі мікросервісної архітектури. Система складається з семи взаємопов'язаних підсистем: агентів, збору та нормалізації даних, виявлення загроз, управління відповідністю, управління інцидентами, управління та звітності, інтеграцій. Специфіковано 11 ключових компонентів системи із зазначенням технологій реалізації, характеристик продуктивності та протоколів взаємодії.

Розроблено формалізований восьмикроковий алгоритм виявлення відхилень від політик безпеки, що реалізує замкнутий цикл моніторингу та поєднує детерміністичну перевірку відповідності конфігурацій (8 категорій із ваговими коефіцієнтами) з поведінковим ML-аналізом. Алгоритм реалізує три рівні реагування: ІНФО, УВАГА та КРИТ.

Оцінка ефективності на основі дев'яти категорій загроз та відхилень показала: середній TPR = 95,3%, середній FPR = 1,7%, MTTD = 4,2 хвилини. Порівняно з поточним галузевим показником MTTD = 184 дні це означає скорочення часу виявлення у понад 600 разів. Рівень автоматичного виправлення відхилень становить 65%, що суттєво знижує операційне навантаження на SOC-команду.

ВИСНОВКИ

У кваліфікаційній роботі виконано комплексне дослідження проблематики безпеки кінцевих пристроїв корпоративних мереж та розроблено систему контролю безпеки кінцевих пристроїв (СКБКП). За результатами роботи можна зробити такі висновки.

1. Аналіз сучасного стану безпеки кінцевих пристроїв підтвердив критичну важливість проблеми: 71% кіберінцидентів у 2024 році пов'язані з кінцевими вузлами, середній час виявлення загрози складає 184 дні, а середня вартість одного інциденту досягла 4,88 мільйона доларів США. Виявлено вісім системних проблем, що обумовлюють неефективність існуючих підходів до захисту.

2. Дослідження підходів до захисту кінцевих пристроїв систематизувало шість концепцій (EPP, EDR, XDR, NAC, UEM, ZTNA) та підтвердило, що максимальний рівень захисту досягається лише при їхній комплексній інтеграції. Жоден підхід окремо не забезпечує вичерпного захисту від усього спектра сучасних загроз.

3. Порівняльний аналіз п'яти провідних комерційних рішень (CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne Singularity, Cisco Secure Endpoint, Elastic Security) виявив їхні сильні сторони та обмеження. Визначено кращі практики для запозичення у розроблюваній системі.

4. Дослідження технологій збору телеметрії показало суттєву технологічну різноманітність механізмів (ETW/eBPF/ESF) та підкреслило необхідність нормалізації за відкритим стандартом OCSF. Розроблено порівняльну характеристику методів контролю відповідності за параметрами автоматизації та частоти перевірок.

5. Розроблено структурну схему СКБКП на основі мікросервісної архітектури із семи підсистем. Специфіковано 11 ключових компонентів системи. Система підтримує три моделі розгортання (On-Premises, Cloud-Native, Hybrid) та забезпечує масштабованість від 100 до 100 000+ кінцевих пристроїв.

6. Розроблено восьмикроковий алгоритм виявлення відхилень від політик безпеки, що інтегрує детерміністичну перевірку відповідності (8 категорій із ваговими коефіцієнтами від 7 до 10) та ML-аналіз поведінкових аномалій. Алгоритм реалізує три рівні реагування (ІНФО, УВАГА, КРИТ) та механізм автовиправлення для 65% виявлених відхилень.

7. Оцінка ефективності алгоритму показала: TPR = 95,3%, FPR = 1,7%, MTTD = 4,2 хвилини. Порівняно з поточним галузевим показником MTTD = 184 дні це означає скорочення часу виявлення у понад 600 разів та здатне знизити збиток від інцидентів на 60–70%.

8. Розроблена система повністю відповідає вимогам регуляторного середовища (NIS2, GDPR, ISO/IEC 27001) та може бути впроваджена в корпоративних середовищах різного профілю та масштабу за запропонованою чотирьохетапною схемою розгортання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ponemon Institute. 2024 State of Endpoint Security: Tracking the Evolution of Endpoint Threats / Ponemon Institute LLC. – Traverse City : Ponemon Institute, 2024. – 52 p.

2. ENISA. ENISA Threat Landscape 2024 / European Union Agency for Cybersecurity. – Heraklion : ENISA, 2024. – 118 p. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 10.06.2026).

3. Verizon. 2024 Data Breach Investigations Report / Verizon Communications Inc. – New York : Verizon Business, 2024. – 104 p. – URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 10.06.2026).

4. IBM Security. Cost of a Data Breach Report 2024 / IBM Corporation. – Armonk : IBM Corp., 2024. – 86 p. – URL: https://www.ibm.com/reports/data-breach (дата звернення: 10.06.2026).

5. Gartner. Market Guide for Endpoint Security, 2024 / Gartner Inc. – Stamford : Gartner, 2024. – 28 p.

6. Scarfone K. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security : NIST SP 800-46 Rev. 3 / K. Scarfone, M. Souppaya. – Gaithersburg : NIST, 2023. – 54 p.

7. Cisco. Cisco Annual Internet Report 2018–2023 White Paper / Cisco Systems Inc. – San Jose : Cisco, 2023. – 35 p.

8. Bhardwaj A. Evolution of Endpoint Security: From Antivirus to EDR and XDR / A. Bhardwaj, S. Goundar // International Journal of Advanced Computer Science and Applications. – 2023. – Vol. 14, No. 8. – P. 112–124.

9. Dang Q. T. Endpoint Protection Platforms: A Comprehensive Survey / Q. T. Dang, P. Le // IEEE Access. – 2024. – Vol. 12. – P. 28450–28468. – DOI: 10.1109/ACCESS.2024.3361912.

10. Bhatt P. Endpoint Detection and Response Architecture: Design Principles and Implementation / P. Bhatt // Journal of Cybersecurity and Privacy. – 2023. – Vol. 3, No. 2. – P. 290–314.

11. Alqahtani H. XDR: Extended Detection and Response – A Comprehensive Analysis / H. Alqahtani, G. Bhatt // Computers & Security. – 2024. – Vol. 138. – Art. 103649.

12. IEEE Std 802.1X-2020. IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control. – New York : IEEE, 2020. – 366 p.

13. Microsoft. Microsoft Intune: Unified Endpoint Management Documentation / Microsoft Corporation. – Redmond : Microsoft, 2024. – URL: https://learn.microsoft.com/en-us/mem/intune/ (дата звернення: 10.06.2026).

14. Scarfone K. Guide to a Secure Enterprise Network Landscape : NIST SP 800-215 / K. Scarfone, M. Souppaya. – Gaithersburg : NIST, 2022. – 42 p.

15. Rose S. Zero Trust Architecture : NIST Special Publication 800-207 / S. Rose, O. Borchert, S. Mitchell, S. Connelly. – Gaithersburg : NIST, 2020. – 60 p.

16. Waltermire D. The Technical Specification for the Security Content Automation Protocol (SCAP) : NIST SP 800-126 Rev. 3 / D. Waltermire, S. Quinn, H. Booth. – Gaithersburg : NIST, 2023. – 42 p.

17. European Parliament. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive). – Official Journal of the European Union, 2022. – L 333. – P. 80–152.

18. Scarfone K. Technical Guide to Information Security Testing and Assessment : NIST SP 800-115 / K. Scarfone, M. Souppaya, A. Cody, A. Orebaugh. – Gaithersburg : NIST, 2023. – 80 p.

19. CrowdStrike. Falcon Platform Technical Architecture Overview / CrowdStrike Holdings Inc. – Austin : CrowdStrike, 2024. – 24 p.

20. Microsoft. Microsoft Defender for Endpoint Documentation / Microsoft Corporation. – Redmond : Microsoft, 2024. – URL: https://learn.microsoft.com/en-us/defender-endpoint/ (дата звернення: 10.06.2026).

21. SentinelOne. Singularity Platform: Technical Architecture White Paper / SentinelOne Inc. – Mountain View : SentinelOne, 2024. – 32 p.

22. Elastic. Elastic Security: Open and Unified Security Platform Documentation / Elastic N.V. – San Francisco : Elastic, 2024. – URL: https://www.elastic.co/guide/en/security/current/ (дата звернення: 10.06.2026).

23. Newman S. Building Microservices: Designing Fine-Grained Systems. – 2nd ed. – Sebastopol : O'Reilly Media, 2021. – 616 p.

24. Grenier C. eBPF for Security Monitoring: From Theory to Practice / C. Grenier, F. Denis // ;login: The USENIX Magazine. – 2023. – Vol. 48, No. 2. – P. 16–25.

25. MITRE Corporation. MITRE ATT&CK Framework: Enterprise Matrix v14.1 / MITRE Corporation. – McLean : MITRE, 2024. – URL: https://attack.mitre.org/ (дата звернення: 10.06.2026).

26. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. – URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 10.06.2026).

27. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021 // База даних «Законодавство України» / Верховна Рада України. – URL: https://zakon.rada.gov.ua/go/447/2021 (дата звернення: 10.06.2026).

28. Річний аналітичний огляд: ключові події, тенденції та розвиток кібербезпеки України у 2024 році / Національний координаційний центр кібербезпеки при РНБО України. – Київ, 2025. – URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf (дата звернення: 10.06.2026).

29. Кібероперації рф: нові цілі, інструменти та групи. Аналітика хакерських атак проти України за І півріччя 2024 року / CERT-UA. – Київ :

Держспецзв’язку, 2024. – URL: https://cip.gov.ua/ua/news/cyber-operations-rf-h1-2024-report (дата звернення: 10.06.2026).

30. Михайлишин Д. А. Система моніторингу безпеки кінцевих пристроїв : кваліфікаційна робота / Д. А. Михайлишин ; кер. Н. Г. Яцків. – Тернопіль : ЗУНУ, 2022. – URL: https://dspace.wunu.edu.ua/bitstream/316497/46655/1/%D0%9C%D0%B8%D1%85%D0%B0%D0%B9%D0%BB%D0%B8%D1%88%D0%B8%D0%BD.pdf (дата звернення: 10.06.2026).

31. Журило О. Д. Огляд рішень з апаратної безпеки кінцевих пристроїв туманних обчислень у Інтернеті речей / О. Д. Журило, О. Ляшенко, К. Аветісова // Сучасний стан наукових досліджень та технологій в промисловості. – 2023. – № 1 (23). – С. 57–68. – DOI: 10.30837/ITSSI.2023.23.057.

ДОДАТКИ

Додаток А Приклад JSON-опису правил перевірки відповідності конфігурацій


```
{
 "policy_id": "WIN-BASELINE-CIS-2024-v2",
 "policy_name": "Базова конфігурація безпеки Windows (CIS Level 1)",
 "version": "2.4.1",
 "platform": "Windows",
 "effective_date": "2024-01-15",
 "review_date": "2024-07-15",
 "owner": "security-team@example.com",
 "checks": [
  {
   "check_id": "WIN-ENC-001",
   "cis_ref": "CIS-Win11-2.3.11.6",
   "description": "Шифрування системного диску BitLocker",
   "category": "ENCRYPTION",
   "weight": 10,
   "severity": "CRITICAL",
   "collection_method": "powershell",
   "command": "(Get-BitLockerVolume -MountPoint C:).ProtectionStatus",
   "expected_value": "On",
   "auto_remediation": {
    "enabled": true,
    "action": "Enable-BitLocker -MountPoint C: -EncryptionMethod XtsAes256",
    "requires_reboot": false,
```

```
      "timeout_minutes": 60
     }
    },
    {
     "check_id": "WIN-AV-001",
     "cis_ref": "CIS-Win11-18.9.47.4",
     "description": "Windows Defender або EDR-агент активний",
     "category": "ANTIVIRUS",
     "weight": 10,
     "severity": "CRITICAL",
     "collection_method": "registry",
     "registry_path": "HKLM:\\SOFTWARE\\Microsoft\\Windows Defender",
     "registry_value": "DisableAntiSpyware",
     "expected_value": 0,
     "auto_remediation": {
      "enabled": true,
      "action": "Set-MpPreference -DisableRealtimeMonitoring $false",
      "requires_reboot": false
     }
    },
    {
     "check_id": "WIN-FW-001",
     "description": "Брандмауер Windows активний у всіх профілях",
     "category": "FIREWALL",
     "weight": 8,
     "severity": "HIGH",
     "collection_method": "command",
     "command": "netsh advfirewall show allprofiles state",
     "expected_pattern": "State\\s+ON",
```

```
    "auto_remediation": {
      "enabled": true,
      "action": "Set-NetFirewallProfile -All -Enabled True"
    }
  }
 ]
}
```