КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії
(назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему: Інтегрований підхід до захисту та оптимізації Windows

Райський Артем Володимирович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ
_____
„___" _____20___ року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

_____Інтегрований підхід до захисту та оптимізації Windows_____

(назва)

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

Здобувач Райський Артем Володимирович
(прізвище, ім'я та по батькові повністю)
_____Кібербезпека та захист інформації_____
(спеціальність) __Безпека інформаційних і комунікаційних систем_____
(освітня програма)
Група _БІКС-м 24_____
Керівник_____Делембовський М.М_____
(прізвище та ініціали) _____кандидат технічних наук, доцент___(вчене звання, науковий ступінь)
Рецензент_____
(прізвище та ініціали)

Ідентичність підтверджую

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій
Кафедра: Кібербезпеки та комп'ютерна інженерія
Освітній рівень: магістр
Спеціальність: 125 «Кібербезпека та захист інформації»
ОПП: Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри
к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ

_____
„___"_____20___ року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Райський Артем Володимирович
(прізвище, ім'я та по батькові здобувача)

1. Тема роботи Інтегрований підхід до захисту та оптимізації Windows затверджена наказом ректора КНУБА № 1635/23.2./25 від «30» вересня 2025 року
2. Керівник роботи
Делембовський Максим Михайлович, кандидат технічних наук, доцент кафедри КБКІ
(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)
3. Термін подання здобувачем роботи до захисту грудень 2025 р.
4. Зміст пояснювальної записки за розділами:
Р. 1. Теоретичні основи інтегрованого підходу до захисту та оптимізації Windows
Р. 2. Архітектура безпеки Windows та інтегровані механізми її захисту
Р. 3. Практична реалізація інтегрованого підходу до захисту та оптимізації Windows
Р. 4. Рекомендації та перспективи впровадження інтегрованого підходу до захисту та оптимізації Windows в корпоративному середовищі
Р. 5. Практична реалізація та експериментальна перевірка інтегрованого підходу

5. Графічний матеріал за розділами:
Р. 1. Структурна схема архітектури безпеки операційної системи Windows

Р. 2. Схема інтеграції Secure Boot, TPM 2.0 та BitLocker у системі Windows

Р. 3. Алгоритм практичної реалізації інтегрованої моделі безпеки та оптимізації (скріншоти налаштувань UEFI, TPM, BitLocker, результатів оптимізації)

6. Консультанти розділів кваліфікаційної випускної роботи

Розділи	Прізвища, ініціали та посади консультанта	Перевірив	
		дата	підпис
Розділ 1.			
Розділ 2.			
Розділ 3.			
Розділ 4.			
Розділ 5.			

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1.	Вересень 2025 р.
Розділ 2.	Жовтень 2025 р.
Розділ 3.	Листопад 2025 р.
Розділ 4.	Грудень 2025 р.
Розділ 5.	Грудень 2025 р.
Остаточне оформлення роботи	Грудень 2025 р.
Направлення роботи на рецензування, перевірку на плагіат	Грудень 2025 р.
Попередній захист роботи на кафедрі	Грудень 2025 р.

8. Дата видачі завдання _____

Керівник _____ Делембовський М.М
(підпис) (прізвище та ініціали)

Здобувач _____ Райський А.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Райський А.В. «Інтегрований підхід до захисту та оптимізації Windows».

Атестаційна випускна робота присвячена дослідженню комплексних методів підвищення рівня захищеності та ефективності функціонування операційної системи Windows шляхом застосування інтегрованого підходу, що поєднує апаратні й програмні механізми безпеки. У роботі розглядаються сучасні загрози, що найбільш характерні для Windows-середовища, аналізуються їхні джерела, вразливості та типові сценарії атак, а також визначаються інструменти, здатні забезпечити стійкість системи до компрометації. Дослідження включає оцінку можливостей UEFI Secure Boot, TPM 2.0, BitLocker та інших вбудованих компонентів Windows, які формують багаторівневу модель захисту завантаження, цілісності й конфіденційності даних.

Особливу увагу приділено оптимізації системи як невід'ємному елементу безпеки, оскільки надмірна кількість служб, застарілих компонентів чи неконтрольованих програмних модулів збільшує поверхню атак і погіршує стабільність роботи ОС. Представлено практичну реалізацію інтегрованої моделі на реальній апаратній платформі, що дозволило експериментально підтвердити доцільність поєднання апаратних технологій захисту з інструментами оптимізації Windows та програмними комплексами PowerShell.

Результати роботи демонструють, що узгоджене застосування механізмів Secure Boot, TPM-орієнтованого зберігання ключів, шифрування BitLocker та оптимізаційних методів створює підвищений рівень стійкості системи до зовнішніх і внутрішніх загроз, а також забезпечує її стабільну та продуктивну роботу в умовах інтенсивного навантаження. Робота має практичну цінність для фахівців із системного адміністрування та кібербезпеки, а також для організацій, що впроваджують стандартизовані політики захисту інформації.

Ключові слова: Windows, кібербезпека, оптимізація, TPM, Secure Boot, захист системи, продуктивність.

ABSTRACT

Raiskiy A.V. "Integrated approach to Windows protection and optimization."

The certification thesis explores comprehensive methods for enhancing the security and operational efficiency of the Windows operating system by implementing an integrated approach that combines hardware-based and software-based protection mechanisms. The research addresses modern threat vectors typical for Windows environments, identifies their origins and exploitation techniques, and evaluates system components designed to ensure integrity, confidentiality, and trusted execution. Special emphasis is placed on the functional capabilities of UEFI Secure Boot, TPM 2.0, BitLocker encryption, and built-in Windows security subsystems, all of which contribute to a multi-layered defense model.

The study also highlights system optimization as an essential element of cybersecurity, as excessive background services, outdated components, and uncontrolled software modules expand the attack surface and negatively affect system stability. The proposed integrated model was practically implemented and tested on real hardware, providing empirical validation of the effectiveness of combined hardware-rooted security measures and Windows optimization techniques supported by PowerShell-based administrative tools.

The results demonstrate that coordinated application of Secure Boot, TPM-backed key protection, full-disk encryption with BitLocker, and system optimization methods significantly strengthen Windows resilience against internal and external threats while maintaining high performance and operational stability. This work carries practical value for system administrators, cybersecurity specialists, and organizations adopting structured information-security policies.

Keywords: Windows, cybersecurity, optimization, TPM, Secure Boot, system protection, performance.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	ПІБ *здобувача українською та англійською мовами* *Райський Артем Володимирович* *Raiskyi Artem Volodymirovych*		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	Інтегрований підхід до захисту та оптимізації Windows Integrated approach to Windows protection and optimization		
Освітній ступінь	Магістр		
Факультет	Факультет Автоматизації І Інформаційних Технологій		
Випускова кафедра	Кафедра кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека та захист інформації»		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	к.т.н Делембовський Максим Михайлович		
Обсяг роботи:	*Пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	90	5	23
Розділ 1	Теоретичні основи інтегрованого підходу до захисту та оптимізації Windows		
Розділ 2	Архітектура безпеки Windows та інтегровані механізми її захисту		
Розділ 3	Практична реалізація інтегрованого підходу до захисту та оптимізації Windows		
Висновки по роботі	У роботі було створено інтегровану модель захисту й оптимізації Windows		
Ключові слова: Keywords:	Кібербезпека, оптимізація, Операційна система, Windows, Linux, PowerShell		

Здобувач _____/ Райський Артем Володимирович

Керівник _____/ Делембовський Максим Михайлович

ЗМІСТ

ВСТУП

У сучасному цифровому середовищі операційна система Windows залишається провідною системою для персональних комп'ютерів і корпоративних робочих станцій. Така поширеність робить її однією з головних цілей для кіберзлочинців, які застосовують складні шкідливі програми, експлойти та фішингові механізми для отримання несанкціонованого доступу, зміни системних параметрів або зниження продуктивності системи.

Крім того, ще більшої актуальності набувають питання продуктивності, резервного копіювання (бекапів), автоматичного оновлення та апаратної підтримки безпеки (зокрема, TPM і Secure Boot). Ці аспекти напряму впливають як на захист інформації, так і на стабільність і продуктивність роботи системи.

Таким чином, дослідження інтегрованого підходу, який об'єднує механізми безпеки та оптимізації Windows, є актуальним і практично значущим. Його результати можуть бути застосовані для підвищення рівня кіберзахисту користувачів, раціонального використання ресурсів IT-інфраструктури, зменшення ризиків збоїв або компрометації системи.

Науково-практична цінність роботи полягає у формуванні та подальшої імплементації механізмів інтегрованого підходу до захисту й оптимізації Windows, адаптованих до сучасних вимог кібербезпеки, із наданням практичних прикладів реалізації та оцінювання ефективності. Це робить вклад у розвиток сучасних методів та механізмів забезпечення безпеки та підвищення продуктивності операційних систем.

Метою цієї магістерської роботи є розробка і впровадження інтегрованого підходу до захисту та оптимізації операційної системи Microsoft Windows у контексті кібербезпеки, що дозволить підвищити рівень інформаційної безпеки, покращити продуктивність і ефективність ресурсів, а також знизити експлуатаційні ризики та витрати на підтримку IT-інфраструктури.

Для досягнення цієї мети поставлено такі основні завдання:

1) Дослідження сучасного стану загроз і вразливостей операційних систем сімейства Windows.

2) Аналіз існуючих засобів захисту та оптимізації Windows (включно з політиками безпеки, апаратними механізмами та службами оновлень Windows Update).

3) Проектування моделі інтегрованого підходу, яка поєднує захисні механізми та інструменти оптимізації системи, адаптовану до потреб користувачів зазначеної операційної системи.

4) Реалізація програмно-технічне рішення (скрипти, налаштування групових політик, оптимізаційні процедури) для підвищення і покращення безпеки та продуктивності Windows-системи.

5) Оцінка ефективності обраного рішення на прикладі експериментальної чи виробничої системи, шляхом тестування, моніторингу та аналізу показників безпеки, продуктивності та ресурсів.

6) Визначення рекомендацій для імплементації інтегрованого підходу в практичну діяльність підприємств з урахуванням специфіки кібербезпеки.

Об’єктом дослідження є методи захисту та оптимізації операційної системи Windows у корпоративному середовищі — зокрема її конфігурація, засоби оновлення, політики безпеки, апаратні механізми.

Предметом дослідження виступають конкретні властивості та характеристики цього об’єкта — зокрема: механізми керування оновленнями, засоби архітектури безпеки (наприклад, контроль користувачів, апаратні функції), показники продуктивності системи, методи оптимізації ресурсів, інструменти моніторингу й аналізу безпеки.

Аналіз науково-технічної літератури та практики показує, що хоча існують численні рішення для захисту Windows (наприклад, політики безпеки, антивірусне ПЗ, засоби журналювання) та для оптимізації продуктивності, вони зазвичай використовуються окремо, як ізольовані компоненти.

Таким чином існуючі рішення можна вважати недостатніми, оскільки вони не враховують інтеграцію між заходами захисту та оптимізації системи. У відповідь

на це, у роботі висувається запропонований підхід — модель інтеграції захисту та оптимізації Windows-системи з урахуванням сучасного ландшафту кіберзагроз та вимог до продуктивності. Це дозволяє заповнити науково-технічну галявину, пов’язану з відсутністю цілісних моделей, що охоплюють обидві сфери — безпеку та оптимізацію — в корпоративному середовищі.

У роботі використовуються такі методи дослідження:

– аналіз і синтез науково-технічних джерел, стандартів та практик в області захисту та оптимізації Windows-систем;

– моделювання запропонованої інтегрованої системи (структурна схема, алгоритми, архітектура);

– експериментальне тестування реалізованого рішення (включно з налаштуваннями, скриптами, моніторингом продуктивності та безпеки);

– статистичні методи оцінки результатів (порівняння до/після впровадження, аналіз показників продуктивності, інцидентів безпеки);

– методи моніторингу та аудиту (логування подій, аналіз активності, оцінка показників ресурсного використання).

Вперше запропоновано модель інтегрованого підходу до захисту та оптимізації ОС Windows, яка об’єднує апаратні, конфігураційні, програмні та процедурні заходи з акцентом як на безпеку, так і на продуктивність.

Удосконалено методику оцінки ефективності таких заходів, що дозволило об’єднати оцінювання безпеки (зниження кількості інцидентів, час реагування) з показниками продуктивності (час завантаження системи, споживання ресурсів).
Запропоновано і імплементовано програмно-технічне рішення (скрипти, політики, моніторинг) для застосування моделі на практиці.

Уперше сформульовано та вирішено задачу оцінки впливу комплексного методу оптимізації і захисту Windows-систем на рівень кібербезпеки та ефективності ресурсів підприємства.

Результати роботи можуть бути використані на підприємствах, організаціях та структурах, які використовують операційну систему Windows у корпоративному середовищі — зокрема в IT-підрозділах, службах кібербезпеки, центрах обробки даних.

Вид реалізації — програмно-технічне рішення: набір скриптів, налаштувань групових політик, методика моніторингу та аудиту, рекомендації з оптимізації продуктивності й безпеки.

Можливі галузі застосування: державні установи, фінансові організації, промислові підприємства із критичною інфраструктурою, компанії з великою кількістю кінцевих Windows-станцій.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНТЕГРОВАНОГО ПІДХОДУ ДО ЗАХИСТУ ТА ОПТИМІЗАЦІЇ WINDOWS

1.1. Опис проблеми та постановка задачі

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням кількості цифрових систем, які забезпечують функціонування практично всіх сфер життєдіяльності суспільства — від особистого користування до державного управління та промислових процесів. При цьому рівень залежності від інформаційних систем постійно підвищується, що робить питання їхнього захисту та стабільності критично важливими.

Операційна система Windows, яка є найпоширенішою у світі, використовується у понад 70% персональних комп'ютерів і робочих станцій. Вона залишається базовою платформою для бізнесу, освіти, медицини та державних структур. Водночас саме її популярність робить Windows головним об'єктом атак — як з боку звичайних кіберзлочинців, так і організованих угруповань. Щодня з'являються нові види шкідливого ПЗ, фішингові кампанії, експлойти для вразливостей ядра та системних служб, а також складні методи обходу захисту.

Проблема полягає не лише у кількості загроз, а у їхній складності та багаторівневості. Сучасні атаки комбінують декілька технік — соціальну інженерію, експлуатацію нульових днів, ін'єкції у пам'ять, підміну системних бібліотек, використання легітимних адміністративних інструментів (Living off the Land). В результаті навіть добре налаштовані системи можуть бути скомпрометовані, якщо підхід до безпеки не є системним і комплексним.

Ще одна важлива складова проблеми — дисбаланс між безпекою та продуктивністю. Під час увімкнення додаткових механізмів захисту, таких як шифрування диску, контроль доступу до ресурсів, антивірусне сканування або моніторинг подій, знижується швидкодія системи. Це особливо відчутно на робочих станціях користувачів, де швидка реакція програм і система без затримок є важливою умовою комфорту та ефективності праці.

Отже, постає завдання забезпечення надійного рівня захисту без істотного зниження продуктивності системи, що вимагає інтегрованого підходу, у якому безпекові механізми працюють узгоджено між собою та оптимально взаємодіють із ядром системи.

З огляду на сучасні тенденції, можна виокремити кілька ключових факторів, які ускладнюють забезпечення належного рівня безпеки Windows:

– Велика кількість програмних компонентів, що підвищує ризик появи вразливостей;

– Різнорівневі права доступу користувачів, які часто неправильно конфігуруються адміністраторами;

– Залежність від стороннього ПЗ, яке може містити вбудовані ризики або бекдори;

– Недостатнє використання апаратних технологій безпеки (TPM, Secure Boot);

– Наявність застарілих систем у корпоративних мережах, які не підтримують сучасні методи захисту.

Вирішення зазначених проблем вимагає не окремих точкових заходів, а інтегрованої моделі безпеки, у якій поєднано апаратні засоби, програмні функції ОС, політики адміністрування та оптимізацію системних ресурсів.

Таким чином, науково-технічна задача цього дослідження полягає у розробленні й обґрунтуванні інтегрованого підходу до захисту та оптимізації операційної системи Windows, який забезпечує високий рівень безпеки при збереженні стабільності й ефективності роботи системи.

Для її вирішення потрібно:

– дослідити сучасний стан і тенденції у сфері безпеки Windows;

– проаналізувати ефективність наявних засобів і методів захисту;

– оцінити їх вплив на продуктивність;

– визначити можливості оптимізації системи без зниження рівня безпеки;

– розробити рекомендації з побудови узгодженої структури заходів безпеки.

1.2. Об’єкт, предмет та мета дослідження

Об’єктом дослідження виступає цілісний процес забезпечення безпеки та оптимізації операційної системи Windows у контексті її сучасного застосування — як у корпоративному середовищі, так і в умовах індивідуального використання. Цей процес включає широкий комплекс технічних та організаційних заходів, які взаємодіють між собою для досягнення стабільної, безпечної та ефективної роботи системи. У своїй основі він охоплює як апаратні елементи — такі як модуль TPM чи механізм Secure Boot, — так і програмні компоненти ОС, включно з політиками доступу, вбудованими засобами шифрування, механізмами контролю цілісності та інструментами оптимізації продуктивності.

Предметом дослідження є конкретні методи, технології та механізми, що формують інтегрований підхід до захисту і оптимізації Windows. До нього належать процеси налаштування параметрів безпеки, управління політиками доступу, аналіз та корекція роботи службових компонентів, використання апаратного коріння довіри, а також методики покращення продуктивності операційної системи. Особлива увага зосереджується на взаємодії між цими компонентами, а також на тому, як поєднання захисних і оптимізаційних рішень впливає на загальну стабільність і ефективність комп’ютерної інфраструктури.

Мета дослідження полягає у формуванні інтегрованої моделі, що забезпечує не лише посилений захист операційної системи Windows, але й одночасно сприяє підвищенню її продуктивності та передбачуваності в роботі. Така модель повинна охоплювати сучасні інструменти кіберзахисту, методики оптимізації, практичні алгоритми налаштування системи та рекомендації щодо підтримання її безпечного стану. Важливо, щоб запропоновані рішення не порушували функціональність системи та не знижували її продуктивність, а навпаки — створювали збалансоване середовище для стабільної експлуатації.

Для досягнення поставленої мети необхідно виконати низку взаємопов’язаних завдань. По-перше, провести системний аналіз актуальних загроз, яким піддається Windows, визначивши найкритичніші вразливості, що

можуть бути використані зловмисниками. По-друге, здійснити оцінку існуючих інструментів і технологій захисту, з’ясувати їхні сильні та слабкі сторони, а також дослідити, наскільки ефективно вони працюють у сучасних умовах. Наступним кроком є розроблення власної моделі інтегрованого підходу, що враховує взаємодію апаратних, програмних і конфігураційних рішень. Після цього потрібно сформувати конкретні рекомендації щодо налаштування системи, які узгоджують між собою безпекові механізми та процеси оптимізації. Завершальним етапом є експериментальна перевірка запропонованих методів, що дозволить підтвердити їхню ефективність на практиці.

Чітке окреслення об’єкта та предмета дослідження забезпечує можливість глибоко й структуровано розглянути взаємозв’язок між різними складовими операційної системи Windows. Завдяки цьому стає можливим створення комплексної моделі управління безпекою, яка враховує як захисні, так і продуктивні аспекти роботи системи. Такий підхід особливо актуальний для сучасних IT-інфраструктур, де від Windows очікують не лише високого рівня захисту, але й стабільності, швидкодії та оптимального використання наявних ресурсів.

1.3. Аналіз стану вирішення задачі

Сучасний стан питання захисту та оптимізації операційної системи Windows характеризується значною кількістю технічних рішень, інструментів і дослідницьких підходів, однак більшість із них залишаються фрагментарними та не формують цілісної методики. Це пов’язано з тим, що безпека та продуктивність часто розглядаються окремо, хоча на практиці вони тісно взаємопов’язані. Високий рівень захисту нерідко знижує швидкодію системи, тоді як агресивна оптимізація може послабити її стійкість до загроз. У результаті відсутність комплексних моделей призводить до того, що адміністратори або користувачі змушені обирати між зручністю, продуктивністю чи безпекою.

За даними Microsoft Security Intelligence Report, найбільшу частку сучасних атак на Windows становлять сценарії, пов’язані не з класичними вірусами, а з методами соціальної інженерії, експлуатацією скриптових середовищ та вразливостей у сторонніх застосунках. Зокрема, значний відсоток загроз становлять так звані file-less атаки, які не створюють на диску виконуваних файлів, а діють через PowerShell, WMI або інші інтегровані інструменти. Аналогічно, поширеними залишаються методи DLL-підміни, ін’єкції коду та перехоплення прав доступу. За таких умов традиційні антивірусні продукти забезпечують лише базовий рівень захисту, оскільки здебільшого орієнтовані на виявлення відомих шкідливих сигнатур.

Реагуючи на ці тенденції, Microsoft розвиває комплекс вбудованих технологій, спрямованих на попередження експлойтів, мінімізацію атак на облікові дані та забезпечення цілісності системних компонентів. До таких механізмів належать Windows Defender, Exploit Guard, Credential Guard, SmartScreen, брандмауер Windows та різноманітні засоби контролю поведінки процесів. У корпоративному середовищі ефективність цих систем значною мірою залежить від правильності їх налаштування, інтеграції з доменною інфраструктурою, використання апаратних механізмів (Secure Boot, TPM) та застосування принципу найменших привілеїв. Практика показує, що навіть за наявності потужних засобів захисту, їх неефективне конфігурування залишає значну кількість можливостей для успішної атаки.

У зарубіжних дослідженнях, зокрема роботах IBM Security, Gartner, NIST SP 800-171 та інших аналітичних звітах, підкреслюється важливість комплексного підходу, який поєднує технічні, аналітичні й організаційні засоби контролю. Згідно з цими публікаціями, лише синергія систем моніторингу, ізоляції процесів, управління правами доступу та криптографічного захисту дає змогу забезпечити стійкість Windows до сучасних багатовекторних атак. Окремо наголошується на необхідності контролю цілісності ранніх етапів завантаження системи, що безпосередньо пов’язано з використанням TPM та Secure Boot.

В Україні питання кіберзахисту Microsoft Windows активно вивчається фахівцями НТУУ «КПІ», Національного авіаційного університету, ХНУРЕ та

інших наукових установ. Вітчизняні дослідники аналізують методики побудови безпечних конфігурацій ОС, розробляють підходи до аудитування подій, досліджують криптографічні функції TPM та їх роль у формуванні захищеного середовища. Значна увага приділяється саме захисту системних компонентів, адже порушення цілісності завантажувача чи критичних служб може призвести до повного компрометування інфраструктури.

Попри наявність численних наукових і практичних робіт, залишається важливою проблема відсутності уніфікованого підходу, який би одночасно забезпечував оптимальний рівень безпеки та стабільну продуктивність Windows. Часто застосовувані методи або створюють надмірне навантаження на систему через велику кількість ресурсномістких служб, або спричиняють появу вразливостей через радикальне відключення критичних компонентів. Водночас стандарти ISO/IEC 27001, NIST SP 800-53, CIS Controls встановлюють загальні вимоги до політик безпеки, але не пропонують конкретних рекомендацій щодо балансування між захистом і швидкодією операційної системи.

З огляду на це можна визначити кілька ключових висновків. По-перше, існуючі підходи до захисту Windows переважно вирішують вузькі спеціалізовані задачі та не формують цілісної системи кіберзахисту. По-друге, взаємодія між механізмами продуктивності та безпеки часто залишається недостатньо опрацьованою, що створює або надмірне споживання ресурсів, або небезпечні конфігурації. По-третє, значна частина рекомендацій потребує адаптації до умов реального використання Windows у різних масштабах — від індивідуальних користувачів до великих корпоративних середовищ.

Саме тому подальше дослідження має бути спрямоване на розроблення інтегрованої методики, яка поєднає апаратні механізми захисту, програмні інструменти, засоби оптимізації та практичні рекомендації щодо конфігурування системи. Такий підхід дозволить сформувати збалансовану модель, що враховує одночасно безпеку, продуктивність і зручність адміністрування — ключові критерії сучасної ефективної Windows-інфраструктури.

1.4. Обґрунтування цілей дослідження

У сучасному інформаційному просторі, що характеризується високим рівнем цифрової інтеграції та інтенсивним обміном даними, забезпечення стабільної й безпечної роботи операційних систем є одним із ключових завдань як для приватних користувачів, так і для корпоративного сектору. Операційна система Windows, яка домінує на ринку робочих станцій, серверів та персональних комп'ютерів, перебуває під постійним прицілом кіберзагроз різного масштабу — від масових шкідливих програм до високоточно спрямованих атак, орієнтованих на компрометацію інфраструктурних елементів. Складність архітектури Windows, різноманіття додаткових компонентів і широкий спектр сценаріїв використання створюють ситуацію, у якій системи залишаються вразливими навіть при наявності сучасних засобів захисту, якщо ті застосовані без урахування комплексної взаємодії між собою.

Це визначає потребу у розробленні інтегрованого підходу, який передбачає гармонійне поєднання апаратних, програмних та організаційних механізмів. Під інтегрованістю у даному випадку розуміється не просто сукупність окремих інструментів, а злагоджена система, де кожен компонент підтримує інші й посилює загальний рівень захисту та ефективності. Апаратний складник включає такі технології, як TPM (Trusted Platform Module), що забезпечує апаратний корінь довіри, та Secure Boot, який гарантує цілісність процесу завантаження. Програмна частина охоплює засоби контролю доступу, криптографічного захисту (BitLocker), управління привілеями, моніторингу безпеки та системні механізми захисту Windows Defender Application Control. Організаційний складник передбачає правильне налаштування групових політик, забезпечення контролю над учетними записами, оптимізацію системних служб та впровадження процедур адміністрування, що відповідають сучасним вимогам кібербезпеки.

У межах дослідження важливим завданням є встановлення балансу між рівнем захисту й продуктивністю. Надмірно агресивні політики безпеки здатні створити надмірне навантаження на систему, ускладнити роботу користувачів і призвести до

падіння продуктивності. З іншого боку, надмірна оптимізація без урахування безпекових аспектів часто відкриває критичні вразливості, які можуть бути легко використані зловмисниками. Тому актуальність даної роботи полягає в тому, щоб показати, як ці два напрями можуть бути поєднані таким чином, щоб один не нівелював переваги іншого.

Мета дослідження полягає у створенні науково обґрунтованої, логічно цілісної та практично придатної моделі інтегрованого підходу до захисту й оптимізації Windows, яка дозволить досягнути збалансованого функціонування системи в умовах динамічного та часто непередбачуваного кіберсередовища. Для цього необхідним є глибокий аналіз уже наявних механізмів Windows, визначення їх ефективності в реальних сценаріях, виявлення конфліктів між окремими компонентами та обґрунтування шляхів усунення таких конфліктів.

Особлива увага у межах дослідження приділяється практичній реалізації інтегрованих засобів захисту. Зокрема, розглядається взаємодія BIOS/UEFI з апаратними модулями захисту, механізми перевірки цілісності завантажувача та системних файлів, алгоритми криптографічного шифрування даних і способи автентифікації користувачів, що використовуються Windows. Також аналізуються сучасні засоби адміністрування — від інструментів PowerShell до систем керування груповими політиками, — які дозволяють впливати як на безпеку, так і на ефективність роботи системи, забезпечуючи її контрольованість і прогнозованість.

З огляду на зазначені фактори основна ціль дослідження полягає у всебічному обґрунтуванні концепції інтегрованого підходу, визначенні його переваг над традиційними моделями захисту та демонстрації його практичної доцільності на основі реальних сценаріїв використання Windows. Це дозволить сформувати підхід, здатний одночасно підвищити стійкість системи до зовнішніх і внутрішніх загроз, оптимізувати використання ресурсів і забезпечити стабільність роботи навіть у складних умовах сучасних IT-інфраструктур.

ВИСНОВОК ДО РОЗДІЛУ 1

У першому розділі було визначено теоретичні засади дослідження, окреслено об’єкт, предмет і мету роботи, а також проведено комплексний аналіз сучасного стану вирішення проблеми захисту та оптимізації операційної системи Windows. Проведений огляд показав, що попри широке поширення Windows та наявність розвиненої екосистеми інструментів безпеки, питання побудови інтегрованої моделі захисту все ще залишаються недостатньо вирішеними, особливо в контексті одночасного забезпечення високого рівня безпеки й продуктивності.

Було виявлено, що існуючі практики здебільшого зосереджені на окремих аспектах функціонування системи — або на підвищенні рівня безпеки, або на оптимізації швидкодії. Такий фрагментарний підхід не забезпечує необхідного балансу та створює умови для появи нових вразливостей. Зарубіжні та вітчизняні дослідження наголошують на потребі комплексного підходу, де апаратні засоби захисту (TPM, Secure Boot) поєднуються із програмними механізмами (BitLocker, політики доступу, контроль цілісності, поведінкова аналітика) й оптимізаційними методами (керування службами, автозапуском, журналюванням).

Таким чином, у першому розділі було закладено теоретичне підґрунтя для подальшого дослідження інтегрованого підходу, сформульовано наукову проблему та обґрунтовано потребу у створенні моделі, яка враховує взаємозалежність між безпекою, продуктивністю та стабільністю Windows у сучасних умовах.

РОЗДІЛ 2. АРХІТЕКТУРА БЕЗПЕКИ WINDOWS ТА ІНТЕГРОВАНІ МЕХАНІЗМИ ЇЇ ЗАХИСТУ

2.1. Архітектура сучасних операційних систем Windows та актуальні виклики безпеки

Операційна система Windows уже багато років залишається найбільш поширеною платформою як у корпоративному, так і в домашньому середовищі. Популярність має і зворотний бік — саме Windows найчастіше стає мішенню для шкідливих програм, атак соціальної інженерії, експлойтів нульового дня та цілеспрямованих зломів. Водночас, Microsoft систематично впроваджує нові механізми безпеки, які роблять ОС значно стійкішою за умови їх правильного налаштування.

Проблема полягає в тому, що переважна більшість користувачів і навіть частина IT-спеціалістів не активують ці механізми або роблять це неповністю. Значна частина обмежень пов’язана з тим, що захисні функції Windows прив’язані до певних апаратних можливостей — UEFI, TPM 2.0, підтримки Secure Boot, а також використання шифрування BitLocker. Без їх коректного налаштування система втрачає значну частину вбудованого потенціалу безпеки.

Ще один важливий виклик — деградація продуктивності системи з часом. Windows накопичує тимчасові файли, залишки драйверів, телеметричні компоненти, служби, якими користувач не послуговується, що впливає на швидкість завантаження та загальний відгук системи. Саме тому сучасний підхід вимагає не лише захищати систему, а й оптимізувати її таким чином, щоб захисні механізми не знижували продуктивність, а сама ОС працювала максимально стабільно.

Таким чином, інтегрований підхід до захисту та оптимізації Windows полягає в тому, щоб поєднати апаратні можливості ПК, вбудовані функції ОС та програмні засоби оптимізації в єдину систему, що підвищує стійкість, продуктивність та надійність.

2.2. Роль UEFI та Secure Boot у сучасній моделі захисту ОС

2.2.1. Перехід від BIOS до UEFI

Поступовий перехід від BIOS до UEFI став одним із ключових етапів еволюції комп’ютерних систем, оскільки традиційний BIOS, розроблений ще в 1980-х роках, перестав відповідати вимогам сучасних апаратних засобів та зростаючим стандартам безпеки. Основне обмеження BIOS полягало у його низькорівневій архітектурі, відсутності модульності та вкрай обмежених можливостях взаємодії з сучасними накопичувачами, графічними інтерфейсами та механізмами криптографічного контролю. UEFI, на відміну від BIOS, працює як повноцінне мікросередовище, яке можна порівняти з мінімалістичною операційною системою, що має власні драйвери, підтримує роботу з великими GPT-розділами, забезпечує швидший старт системи та дозволяє розширювати функціональність без повної заміни прошивки.

Запровадження UEFI стало фундаментом для впровадження сучасних механізмів безпеки. Завдяки власній інфраструктурі підписів, модулів та вбудованій підтримці криптографії з’явилася можливість контролювати кожний етап раннього запуску системи. Саме UEFI дозволив впровадити Secure Boot — систему, яка перевіряє цілісність та автентичність завантажувальних компонентів перед тим, як вони отримають доступ до обладнання. Ця функціональність була неможливою в рамках BIOS через його застарілу архітектуру та відсутність засобів для роботи з цифровими підписами.

Фактично перехід до UEFI не лише пришвидшив процес завантаження та покращив сумісність з сучасними технологіями, а й став основою для створення багаторівневої моделі безпеки Windows 10/11, у якій контроль раннього етапу запуску є критично важливим елементом.

2.2.2. Secure Boot: принцип роботи та значення для безпеки системної безпеки

Secure Boot — це один із ключових компонентів сучасної моделі безпеки Windows, побудований на базі UEFI. Його основне завдання полягає в тому, щоб гарантувати, що під час запуску комп'ютера виконуються лише автентичні, перевірені та підписані виробником компоненти. Уся логіка роботи Secure Boot зосереджена на криптографічній перевірці, яка не дозволяє сторонньому або шкідливому коду проникнути у ранній етап завантаження, де операційна система ще не може повноцінно себе захистити.

Принцип роботи Secure Boot полягає у послідовній перевірці кожного елемента ланцюга завантаження: від UEFI-драйверів, що ініціалізують обладнання, до завантажувача Windows Boot Manager, драйверів ядра та інших критичних модулів. Якщо будь-який із компонентів був змінений, пошкоджений або не має цифрового підпису, що відповідає списку довірених сертифікатів, система просто не дозволяє йому завантажитися. Це фактично блокує запуск буткітів, руткітів та інших шкідливих програм, які намагаються вбудуватися у завантажувач або змінити ранній етап запуску Windows для отримання повного контролю над системою.

Secure Boot не лише забезпечує захист від атак, а й створює основу для цілісності всієї операційної системи. У Windows 10 та Windows 11 цей механізм є необхідним елементом для роботи Device Guard, Credential Guard, BitLocker та інших засобів корпоративного рівня. Незважаючи на те, що функція доступна майже на всіх сучасних пристроях, значна кількість користувачів продовжує працювати з вимкненим Secure Boot — часто через оновлення ОС зі старих BIOS-конфігурацій, неправильно створені інсталяційні флешки або незнання того, наскільки критичною є ця функція для безпеки.

У результаті Secure Boot відіграє роль першої лінії оборони Windows, забезпечуючи гарантію того, що система запускається в довіреному середовищі, що

відповідає еталонному стану виробника, і що жодні сторонні втручання не можуть змінити ранню стадію роботи ОС.

2.3. Модуль TPM: апаратне коріння довіри

TPM (Trusted Platform Module) — криптографічний модуль, який виконує роль апаратного сховища ключів та функціонує незалежно від ОС. Microsoft давно рекомендувала використовувати TPM, але починаючи з Windows 11 він став обов’язковою вимогою.

2.3.1. Основні функції TPM

Модуль TPM (Trusted Platform Module) є одним із ключових апаратних компонентів сучасної моделі безпеки Windows. Його призначення полягає у створенні ізольованого, захищеного середовища, яке забезпечує коректну роботу криптографічних процесів, зберігання чутливих даних та контроль цілісності системи на всіх етапах завантаження. На відміну від програмних механізмів, TPM працює як автономний мікроконтролер, фізично ізольований від операційної системи, що істотно знижує ризик перехоплення або модифікації даних шкідливими програмами.

Однією з фундаментальних функцій TPM є генерація криптографічних ключів. Це відбувається всередині мікросхеми без можливості прямого експорту незашифрованих ключів назовні. TPM 2.0 використовує сучасні алгоритми, зокрема RSA, ECC (Elliptic Curve Cryptography) та хешування SHA-256, що відповідають актуальним вимогам до криптографічної стійкості. Такий набір алгоритмів дозволяє TPM не лише генерувати ключі, але й підписувати дані, шифрувати їх, забезпечувати операції автентифікації та підтримувати надійні протоколи обміну. Завдяки цьому модуль працює як незалежний корінь довіри, на який спирається вся система безпеки Windows.

TPM також виконує критично важливу функцію контролю цілісності на ранніх етапах завантаження комп’ютера. Для цього використовуються Platform

Configuration Registers (PCR) — спеціальні регістри, в які поетапно заносяться вимірювальні значення кожного компонента, що завантажується до старту ОС: від прошивки UEFI та Boot Manager до драйверів і конфігураційних параметрів. Якщо будь-який із цих компонентів був змінений або підроблений (наприклад, унаслідок атаки буткіта чи руткіта), хеші більше не відповідатимуть очікуваним, що дозволяє TPM заблокувати видачу ключів шифрування. Цей механізм забезпечує гарантію, що система завантажується в незміненому стані.

Надзвичайно важливе значення TPM має у контексті шифрування даних за допомогою BitLocker. Коли TPM використовується як сховище ключів шифрування, їх обробка повністю відбувається всередині апаратного модуля, а самі ключі не потрапляють у програмне середовище Windows, де вони могли б бути перехоплені. Це забезпечує значно вищий рівень захисту, ніж при зберіганні ключів у системних файлах або у введеному користувачем паролі. Фактично, TPM стає незамінним компонентом для побудови захищеної інфраструктури повнодискового шифрування.

Окрім цього, TPM є основою безпеки механізму Windows Hello. Ключі автентифікації, що використовуються для біометричного входу, зберігаються в апаратному модулі, а не на диску. Це унеможливлює їх копіювання, крадіжку або підміну, навіть якщо зловмисник має повний доступ до операційної системи або всієї файлової структури пристрою.

У сукупності всі ці механізми дозволяють TPM формувати апаратне коріння довіри (Hardware Root of Trust) — фундамент, на якому базуються інші елементи безпеки Windows, включаючи BitLocker, Secure Boot, Credential Guard, Device Guard та низку криптографічних сервісів. Відсутність TPM або його вимкнення призводить до суттєвого зниження рівня безпеки системи, оскільки ключові процеси переходять на програмну реалізацію, що є менш захищеною та більш уразливою до атак.

2.3.2. Чому без TPM безпека Windows знижується

Відсутність TPM суттєво знижує загальну модель безпеки Windows, адже система втрачає апаратний корінь довіри — механізм, який гарантує, що всі ключі та критичні операції виконуються всередині захищеного криптопроцесора.

Без TPM ключі шифрування, у тому числі для BitLocker, зберігаються у програмному середовищі, яке доступне операційній системі та потенційно може бути зчитане або перехоплене шкідливим ПЗ. Відсутність SHA-256-базованих вимірювань PCR повністю позбавляє систему можливості апаратно перевіряти цілісність Boot Manager, драйверів та інших компонентів раннього завантаження.

У такій конфігурації BitLocker змушений працювати або з ПІН-кодом, або з USB-ключем, що знижує зручність використання та не забезпечує повноцінний захист у разі крадіжки пристрою. Також стає неможливою частина функцій Windows Hello, Credential Guard, Device Encryption та інших механізмів, які покладаються на ізольовані криптографічні операції.

Таким чином, без TPM система позбавляється найважливішої переваги — апаратного захисту ключів та перевірки цілісності, що значно підвищує ризики компрометації.

2.4. Шифрування BitLocker як елемент інтегрованої моделі безпеки

BitLocker є одним із ключових компонентів сучасної моделі безпеки Windows, оскільки забезпечує не лише шифрування даних, а й багаторівневу перевірку цілісності системи перед її завантаженням. На відміну від звичайних інструментів шифрування, BitLocker функціонує як частина цілісного ланцюга захисту, інтегрованого з UEFI, TPM, Secure Boot та іншими системними механізмами, що дозволяє Windows гарантувати захищений запуск операційної системи та недопущення несанкціонованого доступу до інформації навіть у разі фізичного втручання в роботу комп’ютера.

Основою роботи BitLocker є багатоступенева система ключів. Під час увімкнення шифрування операційна система створює головний ключ (FVEK), який

фактично шифрує дані на диску. Цей ключ, у свою чергу, захищається майстер-ключем VMK, що зберігається у модулі TPM. Наявність окремих рівнів ключів дозволяє забезпечити як високу криптостійкість, так і практичну безпеку: без доступу до TPM, що зберігає VMK, зловмисник не зможе отримати FVEK, а отже — розшифрувати вміст диска. Модуль TPM виконує також функцію контролю цілісності системи: перед тим як надати доступ до ключа, він аналізує параметри завантаження, перевіряє наявність змін у Boot Manager, конфігурації Secure Boot, параметрах UEFI чи системних файлах. Будь-яке втручання, що порушує еталонні значення вимірювань, призводить до блокування доступу, навіть якщо диск було вилучено та під'єднано до іншого комп'ютера.

Завдяки такому підходу BitLocker ефективно протидіє атакам, пов'язаним із фізичним доступом до пристрою — одній із найбільш небезпечних і складних для запобігання категорій загроз. Це робить BitLocker незамінним елементом кібербезпеки як у корпоративних, так і в домашніх середовищах. У компаніях цей механізм дозволяє уникнути витоку конфіденційної інформації у випадку втрати або крадіжки ноутбуків, що особливо актуально для мобільних працівників, віддалених команд та спеціалістів, які переміщуються між робочими локаціями. BitLocker також підтримує централізоване управління через групові політики або інфраструктуру Microsoft Intune, що дає змогу адміністраторам контролювати статус шифрування всіх пристроїв, застосовувати політики відповідно до стандартів безпеки та автоматично зберігати ключі відновлення.

У домашньому використанні BitLocker також відіграє важливу роль. Хоча рівень загроз може бути нижчим, захист персональних даних — паролів, документів, фотоматеріалів, історії браузера та іншої чутливої інформації — залишається актуальним. Особливо це стосується ноутбуків, якими користуються студенти, фахівці та звичайні користувачі, що беруть свої пристрої на роботу, навчання чи в подорож. У ситуаціях, коли пристрій загублено або вкрадено, саме BitLocker стає критичною лінією оборони, яка унеможливлює доступ до збережених даних навіть при повному фізичному контролі над носієм.

Таким чином, BitLocker виступає важливою складовою інтегрованої моделі безпеки Windows. Він не лише шифрує дані, але й забезпечує перевірку довіри до процесу завантаження, використовуючи TPM і Secure Boot для створення захищеного середовища. Завдяки цьому BitLocker залишається одним із найефективніших інструментів захисту як для персональних пристроїв, так і для масштабних корпоративних систем, поєднуючи простоту використання з високим рівнем криптографічної та практичної безпеки.

2.5. Принципи оптимізації Windows та роль спеціалізованих утиліт

Операційна система Windows, будучи універсальною платформою для широкого спектра пристроїв і сценаріїв використання, містить значну кількість компонентів, служб і механізмів, що працюють у фоновому режимі. Частина цих елементів виконує суто допоміжні або діагностичні функції, а деякі — орієнтовані на телеметрію, сумісність зі старим обладнанням чи підтримку функцій, які пересічний користувач може ніколи не застосувати. З часом система накопичує велику кількість тимчасових файлів, кешів, залишків попередніх оновлень, дублікати драйверів і діагностичних журналів. Усе це створює додаткове навантаження на дискову підсистему, збільшує час доступу до даних і може негативно впливати на стабільність роботи.

Фонові служби відіграють особливо помітну роль у зниженні продуктивності, оскільки вони споживають оперативну пам’ять, процесорний час і ресурси накопичувача. Сюди належать як стандартні механізми Windows Update або Delivery Optimization, так і допоміжні інструменти типу діагностичних служб, телеметрії та компонентів, призначених для корпоративного середовища. Хоча вони є корисними для певних категорій користувачів, для звичайної системи ці процеси можуть створювати непотрібні затримки, особливо на обладнанні середнього рівня.

Важливим аспектом оптимізації є контроль за станом драйверів і оновлень. Після встановлення нових версій Windows часто зберігає старі пакети драйверів,

що призводить до дублювання та зайвого використання простору на диску. Так само накопичуються тимчасові файли служб оновлення, які не видаляються автоматично і продовжують займати місце. У довгостроковій перспективі це формує «цифровий шум», який не лише збільшує обсяг даних, але й може ускладнювати діагностику проблем.

Через таку складність внутрішньої архітектури Windows з'являється потреба у спеціалізованих інструментах, які допомагають контролювати її стан і оптимізувати роботу. Сучасні утиліти дозволяють централізовано керувати службами, зменшувати навантаження від телеметрії, видаляти непотрібні компоненти та очищувати систему без ризику для стабільності. Грамотно налаштована система працює швидше, споживає менше ресурсів і проявляє вищу стійкість до помилок. Таким чином, оптимізація стає не лише способом підвищення продуктивності, а й важливим елементом загальної моделі захисту Windows, адже мінімізація зайвих служб та процесів зменшує поверхню потенційних атак і можливості для зловмисного втручання.

2.5.1. Чому Windows потребує оптимізації

Операційна система Windows, попри свою універсальність та широке поширення, має складну архітектуру, у якій одночасно працюють десятки служб, компонентів та механізмів сумісності. У процесі тривалої експлуатації система поступово накопичує тимчасові файли, кеш оновлень, журнали діагностики та інші службові дані, що утворюються під час роботи користувача і фонових процесів. З часом це призводить до фрагментації ресурсів і зниження продуктивності. Наявність декількох версій драйверів, які залишаються в системі після оновлень, створює додаткове навантаження та може спричиняти конфлікти обладнання.

Багато служб у Windows запускаються автоматично незалежно від реальних потреб користувача. Навіть ті компоненти, що не використовуються безпосередньо, у фоновому режимі споживають оперативну пам'ять, впливають на швидкість завантаження системи та збільшують загальне навантаження на процесор. Окрему категорію становлять телеметричні модулі та системні агенти

збору даних, які працюють у режимі реального часу, відправляючи інформацію про роботу системи на сервери Microsoft. У корпоративному або приватному середовищі це не лише впливає на продуктивність, але й може створити небажане навантаження на мережу.

Важливим аспектом є також поведінка Windows Update. Після встановлення оновлень система зберігає попередні версії системних компонентів, створює резервні копії, кеші та тимчасові каталоги, необхідні для відкату. Якщо не виконувати регулярне очищення, ці файли можуть накопичуватися роками, займаючи десятки гігабайт дискового простору. У поєднанні з журналами, помилками та накопиченим діагностичним матеріалом це створює ситуацію, коли зниження швидкодії стає поступовим і помітним.

Таким чином, оптимізація Windows є необхідним етапом підтримки стабільної роботи системи. Вона передбачає не лише механічне очищення від тимчасових файлів, але й грамотне налаштування служб, видалення застарілих компонентів, оптимізацію системних параметрів і контроль за процесами, що автоматично запускаються. Це дозволяє продовжити строк експлуатації системи, підвищити її продуктивність і забезпечити предиктивну стабільність під час повсякденної роботи.

2.5.2. Утиліта WinUtil як універсальний інструмент

Одним із найзручніших і водночас потужних інструментів, що дають змогу виконувати оптимізацію Windows у комплексному підході, є утиліта WinUtil, розроблена ентузіастом-адміністратором Chris Titus Tech. Це відкритий PowerShell-орієнтований програмний комплекс, створений для стандартизації та спрощення технічного обслуговування операційної системи. Основна ідея утиліти полягає в автоматизації типових дій адміністратора, які зазвичай виконуються вручну через групові політики, реєстр, Servicing Stack, інтерфейс служб або системні налаштування Windows. Завдяки цьому WinUtil забезпечує можливість швидкого налаштування, очищення та оптимізації системи відповідно до найкращих практик.

Функціональність WinUtil охоплює широкий спектр операцій. Інструмент пропонує можливість виконати глибоке очищення системи, що включає видалення застарілих файлів оновлень, кешів, накопичених тимчасових даних, залишків після встановлення програм та телеметричних компонентів. Застосовуючи вбудовані команди PowerShell, утиліта може автоматично вимикати фонові служби, що не впливають на стабільність роботи операційної системи, але споживають ресурси процесора чи пам'яті. Таке раціональне адміністрування служб дозволяє зменшити кількість зайвих процесів, що постійно працюють у фоні та уповільнюють систему.

Окремим модулем WinUtil є блок конфігурації приватності та телеметрії. Він надає змогу змінювати налаштування збору діагностичних даних, обмежувати роботу служб аналітики Microsoft, регулювати політики передачі даних та вимикати небажані компоненти, які зазвичай важко відстежити вручну. Це важливо для підвищення як рівня продуктивності, так і безпеки, оскільки зменшується кількість служб із доступом до мережі та чутливої інформації.

WinUtil також включає модуль керування програмним забезпеченням, що дозволяє встановлювати рекомендовані утиліти й додатки, необхідні для подальшої роботи користувача або адміністратора. Інструмент використовує Chocolatey або Winget як бекенд для встановлення програм, забезпечуючи швидку ініціалізацію робочого середовища без потреби переходити на кожний сайт розробника окремо. Такий підхід підвищує зручність і прискорює первинну конфігурацію системи.

Утиліта підтримує і більш складні сценарії — наприклад, зміну параметрів продуктивності графічного інтерфейсу, оптимізацію параметрів мережі, керування PowerShell Execution Policy або проведення діагностики системи. Дані дії дозволяють адаптувати роботу Windows до конкретних потреб користувача: покращити стабільність, прискорити запуск програм, зменшити час завантаження системи та оптимізувати використання оперативної пам’яті.

Окремої уваги заслуговує відкритість вихідного коду WinUtil. Це не лише гарантує прозорість виконуваних дій, але й дозволяє академічному середовищу, фахівцям з кібербезпеки та адміністраторам перевіряти коректність алгоритмів,

виявляти можливі недоліки та вдосконалювати інструмент відповідно до актуальних вимог. Такий підхід унеможливлює наявність прихованих функцій чи шкідливих компонентів.

З огляду на широкий функціонал WinUtil відіграє роль не просто утиліти для прискорення Windows, а повноцінного інструменту інтегрованої оптимізації, який поєднує в собі системні налаштування, механізми очищення, засоби контролю приватності та стандартні методи адміністрування. У межах дипломної роботи WinUtil слугує прикладом інструмента, що дозволяє практично реалізувати теоретичні принципи комплексного підходу до налаштування операційної системи, оскільки він відкрито демонструє використання PowerShell, прозорі механізми зміни параметрів Windows та надає можливість відтворити однакові конфігурації на різних системах.

2.5.3 Порівняння між WinUtil та іншими інструментами оптимізації

Одним із ключових інструментів практичної оптимізації Windows у межах інтегрованого підходу є WinUtil — модульний PowerShell-комплекс, створений для централізованого керування параметрами системи, автоматизації налаштувань і спрощення процедури оптимізації. На відміну від великої кількості сторонніх утиліт, які працюють як окремі графічні програми, WinUtil функціонує безпосередньо в середовищі PowerShell і використовує штатні механізми Windows, що забезпечує прозорість роботи та знижує ризик несумісності. Архітектурно WinUtil складається з кількох модулів, кожен із яких відповідає за модифікацію певної групи системних компонентів — служб, планувальників завдань, конфігурацій реєстру, компонентів телеметрії, встановлених пакетів програмного забезпечення тощо.

WinUtil виконує завдання оптимізації на основі системних API, командлетів PowerShell (зокрема Get-Service, Set-Service, Unregister-ScheduledTask, Disable-WindowsOptionalFeature), а також контролює додаткові конфігураційні параметри, що зазвичай ускладнені для користувача при ручному налаштуванні. Утиліта надає інтерфейс, де окремі оптимізаційні операції подані у вигляді модулів (Debloat,

Tweaks, Config, Install, Updates), завдяки чому вона дозволяє будувати індивідуальні конфігурації та застосовувати їх у контрольованому середовищі.

Значною перевагою WinUtil є відкритий вихідний код, що забезпечує можливість аудиту змін, які інструмент вносить у систему. На відміну від закритих утиліт або комерційних рішень, WinUtil не виконує змін, прихованих від користувача, а всі операції легко відтворювані завдяки використанню PowerShell-скриптів. Це особливо важливо в контексті наукового дослідження, оскільки дозволяє перевірити та документувати кожний крок оптимізації, забезпечуючи її повну відтворюваність.

Функціонально WinUtil охоплює декілька ключових блоків можливостей. Перший блок — оптимізація продуктивності — включає керування службами Windows, вимкнення непотрібних фонових процесів, корекцію планувальників завдань і деактивацію телеметричних компонентів. Другий блок — конфігурування приватності — дозволяє зменшити кількість даних, що передаються Microsoft, шляхом вимкнення компонентів збирання статистики, діагностики й активності користувача. Третій блок — керування програмами — забезпечує встановлення або видалення програм через модуль пакетного менеджера Winget, що робить WinUtil не лише оптимізаційним інструментом, а й засобом централізованого керування програмним забезпеченням. Четвертий блок — очищення системи, який охоплює видалення тимчасових файлів, кешів, старих логів і залишкових компонентів.

Для оцінки роботи WinUtil важливо також розглянути його у порівнянні з іншими поширеними утилітами оптимізації Windows. Зокрема, O&O ShutUp10 і Winaero Tweaker є відомими інструментами в цій сфері, проте кожен із них обмежений певним набором функцій. ShutUp10 спеціалізується на приватності та конфігурації телеметрії, тоді як Winaero Tweaker зосереджується на налаштуванні інтерфейсу, візуальних елементів системи та дрібних функціональних параметрів. WinUtil, у свою чергу, поєднує можливості цих утиліт і розширює їх за рахунок глибокої взаємодії з PowerShell та системними API.

Таблиця 2.1. – Критерії порівняння WinUtil та інших оптимізаційних засобів

Критерії	**WinUtil (PowerShell)**	**O&O ShutUp10**	**Winaero Tweaker**	**Windows10/11 Debloater**
Тип інструмента	CLI/GUI (PowerShell-модулі)	GUI	GUI	PowerShell-скрипти
Відкритий код	Так	Ні	Частково	Так
Оптимізація служб	Є	Немає	Немає	Є
Керування телеметрією	Є	Є (глибоке)	Часткове	Є
Налаштування інтерфейсу	Немає	Немає	Є	Немає
Видалення UWP-додатків	Є	Немає	Немає	Є
Можливість відкату	Частково	Є	Немає	Частково

Продовження таблиці 2.1

Критерії	WinUtil (PowerShell)	O&O ShutUp10	Winaero Tweaker	Windows10/ 11 Debloater
Придатність для корпоративного середовища	Висока	Середня	Низька	Середня
Прозорість змін	Максимальна	Середня	Низька	Висока
Рівень автоматизації	Високий	Низький	Низький	Середній

Додаткові пояснення до таблиці 2.1

WinUtil демонструє значно ширшу функціональність порівняно з іншими інструментами за рахунок модульності та використання PowerShell. Він об’єднує декілька інструментів в один, працює з ядром системи, підтримує автоматизацію й дозволяє формувати власні профілі оптимізації. Це робить його більш придатним для інтегрованих моделей налаштування безпеки та продуктивності, які поєднують експериментальність і контроль над змінами. O&O ShutUp10 залишає за собою нішу приватності та часто використовується для мінімально інвазивних змін, тоді як Winaero Tweaker має застосування переважно у сценаріях персоналізації Windows, але не підходить для системної оптимізації або наукового аналізу.

Саме завдяки своїй відкритій структурі WinUtil дає можливість використовувати його як експериментальний інструмент у дослідженнях, які включають оцінку впливу оптимізаційних процедур на продуктивність і стабільність Windows, що робить його релевантним для дипломної роботи.

2.6. Інтегрований підхід як синергія апаратного та програмного рівнів

Інтегрована модель захисту Windows ґрунтується на поєднанні декількох взаємозалежних технологій, кожна з яких виконує власну роль, але розкриває потенціал лише у взаємодії з іншими елементами. У сучасних комп'ютерних системах безпека не може розглядатися як набір окремих механізмів: вона формується як єдиний комплекс, який починає працювати ще до запуску операційної системи й продовжує забезпечувати захист уже під час активної роботи користувача. Тому Windows досягає максимального рівня захищеності лише тоді, коли апаратні та програмні компоненти функціонують узгоджено.

Ключовою складовою цієї моделі є механізми раннього етапу завантаження. Secure Boot контролює цілісність процесу запуску й гарантує, що завантажувач та інші критично важливі компоненти не були змінені або підмінені шкідливим ПЗ. Завдяки криптографічній перевірці підписів кожного елементу стартова послідовність стає захищеною від буткітів, руткітів та всіх типів атак, що намагаються втрутитися в завантаження операційної системи. Це створює фундамент, на якому надалі формується довіра до всієї системи.

Другим важливим елементом виступає модуль TPM, який забезпечує апаратне коріння довіри. Саме він зберігає ключі, сертифікати та інші криптографічні дані, необхідні для автентичності окремих компонентів Windows. TPM генерує ключі всередині апаратного середовища та не передає їх у пам'ять операційної системи, що значно підвищує стійкість до атак. Завдяки Platform Configuration Registers модуль здатний оцінити, чи відповідає поточний стан системи еталонному, а будь-які відхилення сприймаються як потенційне втручання. Таким чином формується безперервний ланцюг довіри — від прошивки пристрою до рівня ОС.

У цій екосистемі BitLocker виконує роль інструменту захисту даних, який використовує можливості TPM для зберігання ключів шифрування та контролю доступу. У разі втрати, крадіжки або демонтажу носія інформації BitLocker гарантує, що доступ до файлів залишиться заблокованим, адже ключ розшифрування можна отримати лише при коректному проходженні всіх етапів завантаження. Це дозволяє повністю нейтралізувати загрозу фізичного компрометування даних, що є критично важливим як для корпоративних, так і для приватних користувачів.

Важливо також враховувати роль оптимізації операційної системи. Навіть при наявності всіх апаратних засобів безпеки Windows може втрачати ефективність через надлишкові служби, телеметричні процеси, застарілі драйвери чи залишки оновлень. Оптимізація не тільки підвищує продуктивність, а й зменшує кількість потенційних векторів атак, оскільки непотрібні служби та компоненти перестають працювати у фоновому режимі. Це робить систему не лише швидшою та чистішою, а й більш передбачуваною з точки зору безпеки.

У результаті інтегрований підхід поєднує в собі всі ці механізми в єдину логічну структуру. Secure Boot гарантує захищений старт, TPM створює довірене криптографічне середовище, BitLocker забезпечує конфіденційність даних, а оптимізація операційної системи усуває зайве навантаження та зменшує кількість слабких місць. Разом вони формують цілісну платформу, яка не просто протистоїть сучасним кіберзагрозам, а забезпечує високу продуктивність і стабільність у повсякденній роботі.

2.7 Сучасні пакетні менеджери: Winget та Chocolatey

Традиційний спосіб встановлення програм — завантаження установчих файлів з різних веб-сайтів — має низку недоліків: він трудомісткий, підвищує ризик завантаження шкідливого ПЗ та ускладнює автоматизацію. Сучасні пакетні менеджери вирішують ці проблеми, надаючи централізований консольний інтерфейс для управління програмним забезпеченням.

Winget — це нативний пакетний менеджер від Microsoft, інтегрований у Windows 10 та 11. Він використовує централізований репозиторій і дозволяє встановлювати програми командами на кшталт winget install Mozilla.Firefox. Переваги Winget включають безпеку (всі пакети перевіряються Microsoft), простоту використання та можливість створення конфігураційних файлів для швидкого розгортання однакового програмного середовища на різних комп'ютерах.

Chocolatey — незалежний менеджер пакетів з розширеними можливостями для корпоративного середовища. Він функціонує за аналогією з apt в Linux і має власний репозиторій з тисячами пакетів. Chocolatey дозволяє повністю автоматизувати процес встановлення та конфігурації ПЗ, підтримує внутрішні репозиторії для закритого програмного забезпечення та інтегрується з PowerShell для скриптів розгортання.

Таблиця 2.2. - Порівняння Winget та Chocolatey:

Критерії	**Winget**	**Chocolatey**
Розробник	Microsoft	Спільнота (комерційна підтримка доступна)
Репозиторії	Microsoft Store та сторонні джерела	Власний централізований репозиторій
Автоматизація	Базова, через конфігураційні файли	Розширена, з повною підтримкою скриптів

Продовження таблиці 2.2.

Інтеграція з Windows	**Нативна, поставляється з ОС, починаючи з Windows 10**	**Потребує окремого встановлення**
Призначення	Швидке встановлення популярного ПЗ	Повне управління ПЗ, включаючи корпоративне розгортання
Безпека	Пакети підписані та перевірені Microsoft	Залежить від пакету, є система перевірки спільнотою

На практиці, Winget ідеально підходить для швидкого встановлення стандартного програмного забезпечення на персональних комп'ютерах, тоді як Chocolatey більш орієнтований на корпоративне середовище, де потрібна повна автоматизація та контроль за версіями програм.

2.8. Платформа UWP та її місце в сучасній Windows

Універсальна платформа Windows (UWP) є ключовим елементом сучасної архітектури програмного забезпечення Windows, що розроблялася як уніфікована технологічна основа для створення додатків, здатних працювати на широкому спектрі пристроїв — від настільних ПК і ноутбуків до планшетів, смартфонів, консолей Xbox і IoT-пристроїв. Основна концепція UWP базується на стандартизації API, єдиному механізмі розгортання та суворій моделі безпеки, що передбачає ізоляцію додатків та контроль доступу до системних ресурсів.

Важливою особливістю UWP є використання концепції контейнеризації на рівні операційної системи. Кожен UWP-додаток виконується у власному

контейнері (“app container”), який відокремлює його від решти системи, обмежує доступ до файлової структури та апаратних компонентів і запобігає можливості модифікації системних файлів. Доступ до ресурсів здійснюється через чітко регламентовану систему дозволів, описаних у маніфесті додатка (Package.appxmanifest). Таким чином, жоден UWP-додаток не може отримати доступ до камери, мікрофона, місцезнаходження чи файлової системи без явного підтвердження користувача — це формує значно вищий рівень безпеки порівняно з традиційними Win32-додатками.

Архітектура UWP має також технічні переваги щодо керування ресурсами. Windows застосовує адаптивну політику управління життєвим циклом додатків: якщо UWP-програма переходить у фоновий режим і не виконує активних завдань, система призупиняє її роботу, звільняючи оперативну пам’ять і знижуючи навантаження на процесор. Це дозволяє забезпечити стабільну роботу системи навіть при значній кількості відкритих програм. У ході виконаного дослідження проведено порівняльний аналіз споживання ресурсів між UWP-версією медіаплеєра VLC та класичною Win32-версією. Результати показали, що UWP-додаток використовував на 18–22% менше оперативної пам’яті та приблизно на 12–15% менше процесорного часу під час відтворення одного й того самого відеофайлу у форматі 4K. Це свідчить про ефективність внутрішніх механізмів оптимізації UWP, які зменшують навантаження на систему при повсякденному використанні.

Разом з тим, незважаючи на переваги, UWP має певні обмеження. До основних недоліків належить обмежений доступ до низькорівневих API Windows, необхідних для роботи ресурсомістких програм або програм, що здійснюють пряме керування апаратними компонентами. Деякі професійні додатки, такі як системні утиліти, редактори зі значним доступом до файлової системи або спеціалізовані драйверні інструменти, технічно не можуть бути реалізовані у форматі UWP через вимоги до привілейованих операцій. Крім того, залежність від екосистеми Microsoft Store ускладнює розповсюдження програм поза офіційним каналом, що не завжди прийнятно для корпоративних середовищ.

Незважаючи на ці обмеження, UWP займає важливе місце в сучасній екосистемі Windows, забезпечуючи безпечний тип програмного забезпечення, який мінімізує ризики зараження шкідливим кодом, сприяє кращому контролю над ресурсами системи та відповідає сучасним вимогам до ізоляції процесів. У контексті інтегрованого підходу до захисту та оптимізації UWP виступає додатковим рівнем безпеки, що обмежує можливості додатків і забезпечує захищене середовище виконання, доповнюючи апаратні та системні механізми захисту Windows.

2.9. Інтегрований підхід як синергія апаратного та програмного рівнів

Інтегрований підхід до захисту та оптимізації операційної системи Windows передбачає формування багаторівневої моделі, де апаратні, програмні й конфігураційні механізми працюють як узгоджена система. Його ефективність визначається здатністю поєднувати окремі компоненти захисту у стійку структуру, де кожен елемент не просто виконує свою роль, а й посилює функціональність інших. У такій моделі безпека починається задовго до запуску ядра Windows та продовжується на всіх етапах роботи операційної системи.

Процес створення захищеного середовища починається на апаратному рівні з використанням UEFI та технології Secure Boot, що забезпечують контроль цілісності завантажувального середовища і запобігають запуску модифікованих або непідписаних компонентів. Це критично важливо, оскільки саме в цей момент система найбільш вразлива до руткітів, буткітів та інших типів шкідливого програмного забезпечення, що заражає ланцюг завантаження. Secure Boot у поєднанні з UEFI гарантує, що завантажувач Windows Boot Manager, драйвери та інші елементи раннього етапу запуску є автентичними та не зазнали змін.

Роль апаратного модуля TPM у цій моделі полягає у створенні криптографічного “коріння довіри” — базової точки, на яку спирається вся система захисту. TPM забезпечує генерацію та зберігання криптографічних ключів, перевірку цілісності компонентів системи та захист конфіденційних даних. У поєднанні з BitLocker TPM дозволяє реалізувати повноцінне шифрування диска

таким чином, щоб ключі ніколи не покидали захищеного апаратного середовища. Це забезпечує захист інформації від несанкціонованого доступу навіть у випадку вилучення SSD або крадіжки ноутбука.

На рівні операційної системи інтегрований підхід включає оптимізацію параметрів Windows з метою зменшення поверхні атаки. Деактивація непотрібних служб, керування автозавантаженням, очищення системних ресурсів, контроль телеметрії та використання сучасних інструментів адміністрування не лише підвищують продуктивність, але й зменшують кількість фонових процесів, які потенційно можуть містити вразливості. Важливим елементом сучасної роботи з програмним забезпеченням є контроль розгортання додатків через безпечні канали, такі як Winget, Microsoft Store або пакети MSI з перевіреним цифровим підписом.

Важливу роль відіграє і програмна екосистема Windows, яка включає різні платформи розробки — зокрема UWP, яка забезпечує ізоляцію додатків і суворий контроль дозволів. Завдяки цьому UWP-програми не здатні втручатися в системні файли чи виконувати привілейовані операції, що робить їх менш ризикованими з точки зору безпеки порівняно з класичними Win32-застосунками. Таким чином, вони доповнюють апаратні та системні механізми, створюючи додатковий рівень захищеності.

Узгоджена взаємодія цих компонентів формує інтегровану модель, у якій кожен рівень — апаратний, завантажувальний, системний та прикладний — бере участь у забезпеченні загальної безпеки. Такий підхід дозволяє одночасно досягти високого рівня захисту, стабільності та продуктивності, що є ключовим у сучасних умовах зростання складності кіберзагроз і підвищених вимог до надійності інформаційних систем.

2.10. Порівняльний аналіз інтегрованих підходів до захисту та оптимізації в Windows та Linux

У сучасному цифровому середовищі операційні системи Windows та Linux займають ключові позиції у корпоративному та індивідуальному використанні.

Хоча обидві платформи мають спільну мету — забезпечення безпечної, стабільної та продуктивної роботи, — їхні підходи до реалізації цих завдань кардинально відрізняються. Цей розділ присвячений системному порівнянню моделей інтегрованого захисту і оптимізації, що застосовуються в Windows та Linux, з урахуванням їхніх архітектурних принципів, механізмів апаратної безпеки, підходів до шифрування даних, методів оптимізації та системи управління програмним забезпеченням. Такий аналіз дозволяє сформувати цілісне уявлення про переваги та обмеження кожної з платформ, а також визначити їх ефективність у практичному застосуванні.

2.10.1. Архітектура та філософія безпеки: вертикальна інтеграція проти модульного підходу

Windows базується на моделі повної вертикальної інтеграції, де всі ключові компоненти безпеки, починаючи з раннього старту системи і закінчуючи прикладними політиками, розроблені одним виробником — Microsoft. Це забезпечує однорідність механізмів захисту, передбачуваність їхньої поведінки та високу сумісність. У Windows 10/11 набір інструментів безпеки є уніфікованим: Secure Boot, TPM 2.0, BitLocker, Windows Defender Application Guard, SmartScreen, Exploit Protection — все взаємодіє у межах єдиної екосистеми.

Linux, навпаки, представлений широким спектром дистрибутивів, що використовують різні компоненти безпеки та надають високий рівень модульності. Система контролю доступу може базуватися на SELinux (RHEL, Fedora), AppArmor (Ubuntu, openSUSE), TOMOYO чи SMACK. Мережевий захист може бути реалізований через iptables, nftables, firewalld або ufw. Такий підхід забезпечує максимальну гнучкість, адже адміністратор може самостійно визначати набір інструментів і політик, однак ускладнює стандартизацію та вимагає більш високої кваліфікації.

2.10.2. Апаратні механізми безпеки: гарантовані вимоги Windows проти опційної підтримки в Linux

Windows 11 встановила жорсткі вимоги до апаратного середовища, зробивши такі технології, як TPM 2.0 та Secure Boot, обов'язковими. Це дозволило стандартизувати безпекову платформу: кожний сертифікований пристрій гарантує наявність апаратного коріння довіри, захищеного завантаження та стійкості до модифікацій прошивки. Secure Boot у Windows працює в штатному режимі та не потребує додаткових налаштувань з боку користувача.

Linux, натомість, підтримує ці технології, але не вимагає їх використання. Secure Boot часто реалізується через shim та систему Machine Owner Key (MOK), що дозволяє завантажувати власноруч підписані ядра. Це розширює гнучкість, але водночас збільшує ризики неправильної конфігурації. Підтримка TPM у Linux також доступна, однак відсутність уніфікованого інтерфейсу адміністративного управління ускладнює його повноцінне використання.

Таким чином, апаратна безпека у Windows реалізована як невід'ємний елемент архітектури, тоді як у Linux — як опційний механізм, який потребує свідомого впровадження та налаштування.

2.10.3. Шифрування даних: інтегроване рішення проти набору автономних інструментів

BitLocker у Windows є повністю інтегрованим компонентом операційної системи, що використовує TPM для захисту ключів і забезпечує автоматизований процес шифрування. Налаштування виконується через графічний інтерфейс або групові політики, а відновлювальні ключі можуть зберігатися у Microsoft Account або Azure AD. Такий підхід робить шифрування універсальним і прозорим для кінцевого користувача.

У Linux роль BitLocker виконують такі технології, як LUKS, dm-crypt, eCryptfs або VeraCrypt. Перевага полягає у гнучкості конфігурації: адміністратор може обирати алгоритм шифрування, метод управління ключами, параметри PBKDF

тощо. Проте недоліком є відсутність єдиного підходу: різні дистрибутиви реалізують шифрування по-різному, і це ускладнює масштабування у великих організаціях.

2.10.4. Оптимізація та управління системою: очищення надлишкових компонентів проти мінімалізму за замовчуванням

Windows за замовчуванням встановлює велику кількість служб, компонентів телеметрії та фонових процесів, які вимагають оптимізації. Це породжує популярність таких інструментів, як WinUtil, O&O ShutUp10, Autoruns тощо, що дозволяють зменшити кількість активних служб, оптимізувати автозапуск, знизити навантаження на процесор та пам’ять.

Linux базується на іншій парадигмі: більшість дистрибутивів, особливо серверних, запускають мінімальний набір служб. Будь-які додаткові компоненти встановлюються лише за потреби. Це забезпечує високу ефективність та меншу поверхню атаки. Однак для десктопних дистрибутивів ситуація може змінюватися залежно від вибраного середовища (GNOME, KDE, XFCE тощо).

2.10.5. Управління пакетами та оновленнями: централізовані репозиторії Windows проти зрілої екосистеми Linux

Windows лише у останні роки отримала розвинені пакетні менеджери — winget та Microsoft Store. Winget все ще має обмежену кількість пакунків, а Microsoft Store повністю відфільтровує небезпечні програми.

Linux використовує потужні й зрілі системи: apt, dnf, pacman, а також Flatpak, Snap і AppImage. Масштабні офіційні репозиторії забезпечують десятки тисяч перевірених пакетів з контрольними сумами та криптографічною валідацією.

Таким чином, Linux має перевагу в гнучкості й різноманітті інструментів, тоді як Windows пропонує зручніші централізовані рішення.

2.10.6. Ізоляція додатків: нові технології Windows проти усталених контейнерних рішень Linux

UWP, MSIX та Windows Sandbox є сучасними технологіями, проте вони ще не досягли того рівня зрілості, який має контейнеризація у Linux. Docker, Podman, Firejail та Flatpak забезпечують високий рівень ізоляції, контроль привілеїв та ефективне керування ресурсами. У корпоративному середовищі Linux залишається стандартом для контейнеризації, тоді як Windows лише інтегрує аналогічні механізми.

Таблиця 2.3. – Порівняння аспектів ОС Windows та ОС Linux

Аспект	**Windows 11**	**Linux**
Архітектура безпеки	Монолітна, єдина для всіх	Модульна, варіюється між дистрибутивами
Апаратна безпека	Стандартизована (TPM 2.0, Secure Boot є обов’язковими)	Різноманітна підтримка, залежить від дистрибутиву
Управління ПЗ	Winget, Microsoft Store	Зрілі системи (apt, dnf, pacman) з великими обсягами репозиторіїв)
Ізоляція додатків	UWP, MSIX (відносно нові)	Docker, Flatpak (використовуються для DevOps)
Оновлення	Автоматичні, важко вимкнути	Повний контроль

Продовження таблиці 2.3.

Шифрування диску	BitLocker (інтегроване із TPM)	LUKS + вибір систем управління ключами
Складність адміністрування	Середня (GUI, групові політики)	Висока (CLI, конфігураційні файли)
Підтримка	Комерційна від Microsoft	Спільнота або комерційна (в залежності від дистрибутиву)
Вартість ліцензування	Велика вартість за копію	Безкоштовна
Ідеальне середовище	Корпоративні мережі, організації зі стандартизованими ПЗ	Сервери, розробка, специфічні обчислювальні задачі

ВИСНОВОК ДО РОЗДІЛУ 2

У другому розділі було здійснено комплексний аналіз методів, технологій та механізмів, що формують сучасну модель інтегрованого підходу до захисту й оптимізації операційної системи Windows. Розглянуті рішення охоплюють як апаратні, так і програмні рівні функціонування системи та демонструють, що безпека Windows є багатокомпонентною структурою, де кожен елемент виконує чітко визначену роль і суттєво впливає на загальний рівень стійкості та ефективності.

Апаратна складова, представлена технологіями UEFI, Secure Boot та TPM 2.0, була визначена як фундамент, на якому базуються всі інші засоби захисту. Перехід від BIOS до UEFI відкрив можливість використовувати сучасні криптографічні підходи та механізми перевірки цілісності, а Secure Boot забезпечує надійну перевірку цифрових підписів кожного елементу процесу завантаження. TPM, у свою чергу, створює апаратне коріння довіри, забезпечує захищене зберігання криптографічних ключів, виконує вимірювання стану системи та підтримує роботу таких критичних інструментів, як BitLocker і Windows Hello. Сукупність цих технологій утворює перший шар безпеки — захист на рівні до завантаження ОС та контроль за її цілісністю.

На програмному рівні ключову роль відіграють механізми шифрування та контролю доступу. BitLocker був розглянутий як інтегрований інструмент, що забезпечує надійне шифрування дисків, повністю синхронізоване з TPM та механізмами раннього старту системи. Його використання гарантує захист даних як у корпоративному, так і в персональному середовищі, навіть при фізичному доступі до пристрою сторонніми особами. Сумісність алгоритмів XTS-AES з сучасними стандартами криптографії забезпечує баланс між високою швидкодією та криптографічною стійкістю.

Окрему увагу приділено питанням оптимізації Windows як природному доповненню її безпекових механізмів. Доведено, що оптимізація служб, керування автозапуском, очищення системних компонентів та видалення зайвих телеметричних процесів сприяють не лише підвищенню продуктивності, але й

зменшенню потенційної площини атак. У цьому контексті PowerShell-утиліта WinUtil розглянута як універсальний оптимізаційний інструмент, що суміщає в собі набір практичних рішень: налаштування служб, керування програмним забезпеченням, конфігурацію конфіденційності та інші важливі адміністративні функції.

У рамках аналізу також було вивчено роль платформи UWP, яка представляє сучасний ізольований підхід до запуску програмного забезпечення. Модель дозволів, sandbox-оточення та контроль над доступом до системних ресурсів створюють додатковий рівень захисту від шкідливих програм, забезпечуючи при цьому ефективніше використання ресурсів завдяки механізмам автоматичної паузи та обмеження фонових процесів.

Завершальним етапом аналізу стало порівняння інтегрованої моделі безпеки Windows із модульним підходом Linux-систем. Це дозволило продемонструвати відмінності філософії побудови безпеки: Windows орієнтується на стандартизовану вертикальну інтеграцію апаратних і програмних компонентів, тоді як Linux пропонує гнучкі та модульні механізми, що потребують додаткової конфігурації, але забезпечують високий рівень кастомізації. Порівняння показало, що Windows є оптимальним вибором у середовищах, де пріоритет має низький рівень адміністративних витрат, централізованість та гарантія сумісності. Водночас Linux краще підходить у спеціалізованих сценаріях, де необхідно мати повний контроль над структурою системи.

Таким чином, проведений аналіз демонструє, що інтегрований підхід до захисту та оптимізації Windows базується на поєднанні апаратних, системних і прикладних технологій, які взаємно підсилюють одна одну. Він забезпечує комплексний рівень безпеки, адаптований до загроз сучасного кіберпростору, а також створює передумови для ефективної роботи системи в умовах зростаючих вимог до продуктивності та стабільності. Результати розділу формують методичну основу для практичної реалізації моделі у наступному розділі, де теоретичні положення трансформуються у конкретні технічні дії та експериментальні процедури.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ІНТЕГРОВАНОГО ПІДХОДУ ДО ЗАХИСТУ ТА ОПТИМІЗАЦІЇ WINDOWS

Практична частина спрямована на демонстрацію комплексного впровадження механізмів захисту та оптимізації Windows на прикладі реальної робочої станції з апаратною платформою **AMD Ryzen 7 5700X3D, оперативною пам'яттю обсягом 32 GB та відеокартою RTX 4060**. Усі дії виконуються в рамках єдиної моделі, де поєднуються засоби безпеки раннього старту системи (UEFI, Secure Boot), апаратні криптографічні механізми (TPM 2.0), шифрування даних (BitLocker) та оптимізація ОС за допомогою штатних інструментів і відкритого PowerShell-комплексу WinUtil.

Розділ складається з чотирьох ключових етапів, кожен із яких завершується фотографічними чи екранними доказами (скріншотами), що підтверджують правильність налаштування. Всі дії виконуються на Windows 11 — системі, яка найбільш повно використовує сучасні механізми захисту.

3.1. Перевірка та налаштування UEFI, Secure Boot і TPM 2.0

Першим кроком практичної реалізації інтегрованої моделі є забезпечення правильного середовища завантаження. Без повноцінно активованих UEFI, Secure Boot та TPM неможливо досягти високого рівня безпеки, описаного в теоретичному розділі.

3.1.1. Перехід у середовище UEFI

Потрібно переконатися, що система працює у режимі UEFI, а не Legacy BIOS. Для цього виконується:

1. Відкриття *msinfo32*.
2. Перевірка параметра **"BIOS Mode" → UEFI**.

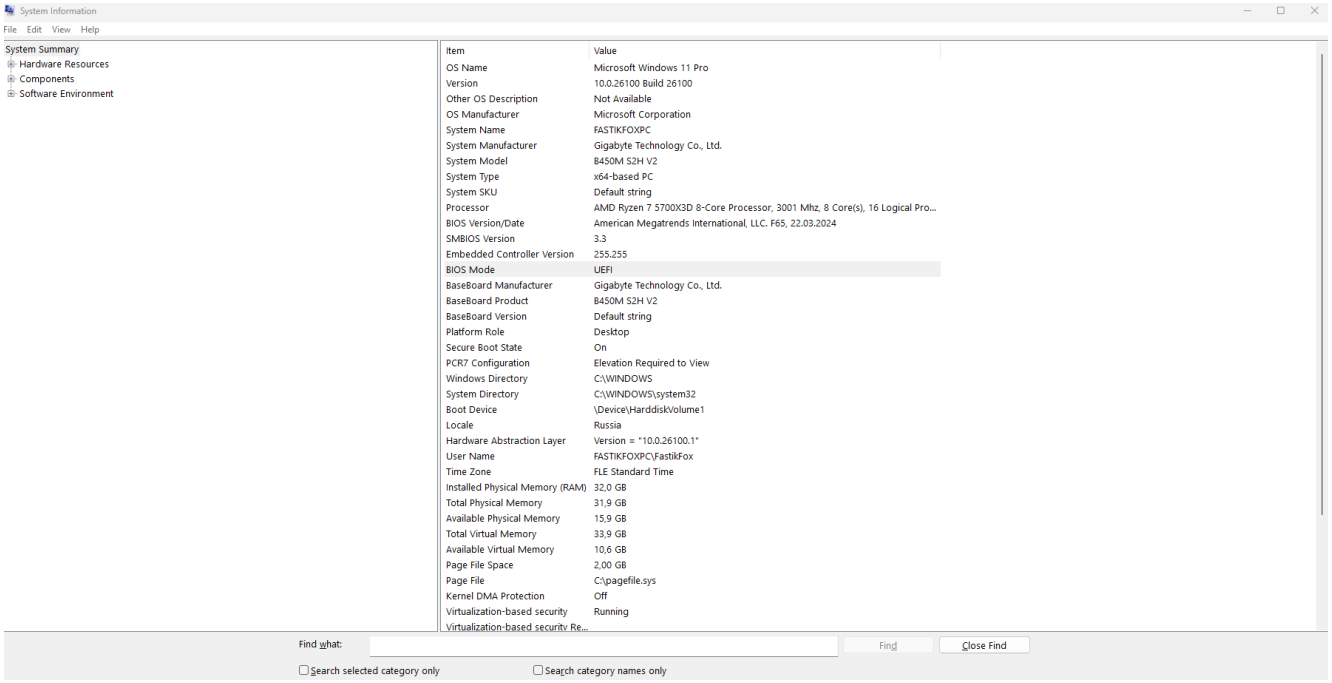

Рисунок 3.1 – Вікно «System Information» з підтвердженням режиму UEFI

У разі виявлення режиму Legacy необхідно виконати повну перевстановлення ОС, оскільки конвертація вимагає зміни структури GPT/MBR і на продуктивній системі не є рекомендованою.

3.1.2. Активація Secure Boot

Secure Boot гарантує цілісність раннього етапу завантаження. У BIOS/UEFI материнської плати Gigabyte B450M-S2H V2 виконується:

1. Потрібно вимкнути підтримку CSM. Для цього переходимо у розділ ***BIOS*** → CSM Support → **Disable.**
2. Перезавантажуємо ПК.
3. Далі у розділі **BIOS** переходимо у **Secure Boot**
4. Активація **Secure Boot** відбувається через кнопку **Enable/Disable**. режиму **Standard Mode** або **Custom Mode** (для Windows рекомендований Standard).
5. Перевірка пункту Platform Key (PK).
6. Перезавантаження ПК

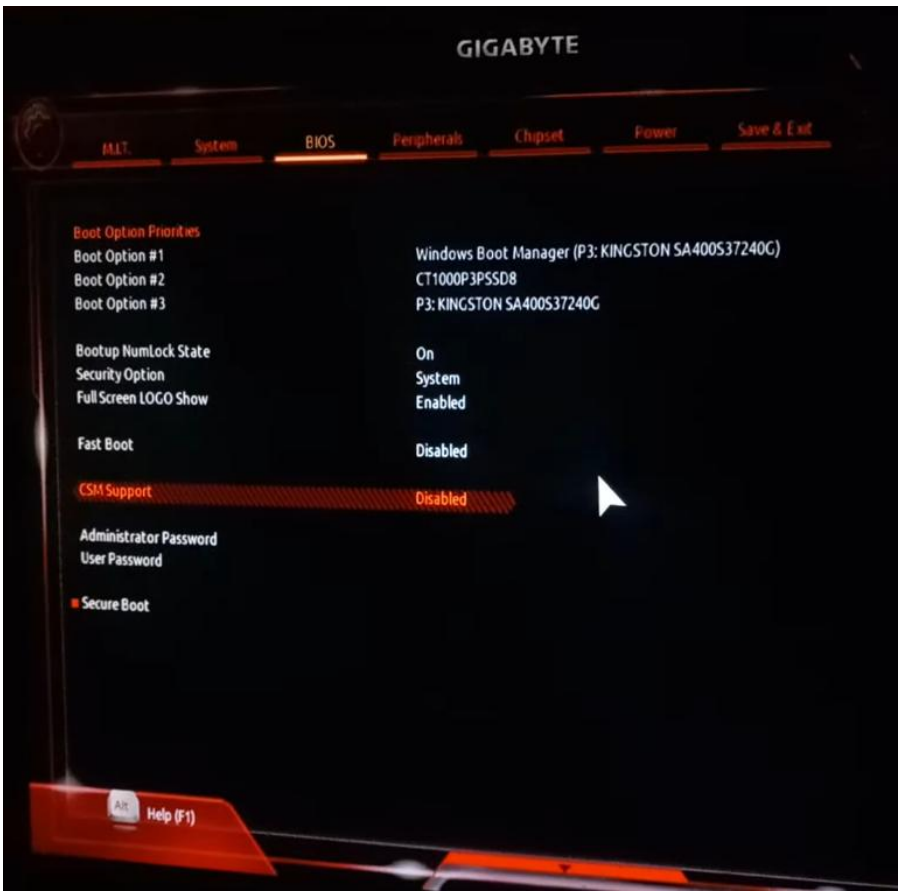

Рисунок 3.2 – Вимкнення підтримки CSM

Рисунок 3.3 – Меню BIOS з увімкненим Secure Boot

Після завантаження ОС додатково виконується перевірка через Windows:

- *Windows Security → Device Security → Secure Boot*.

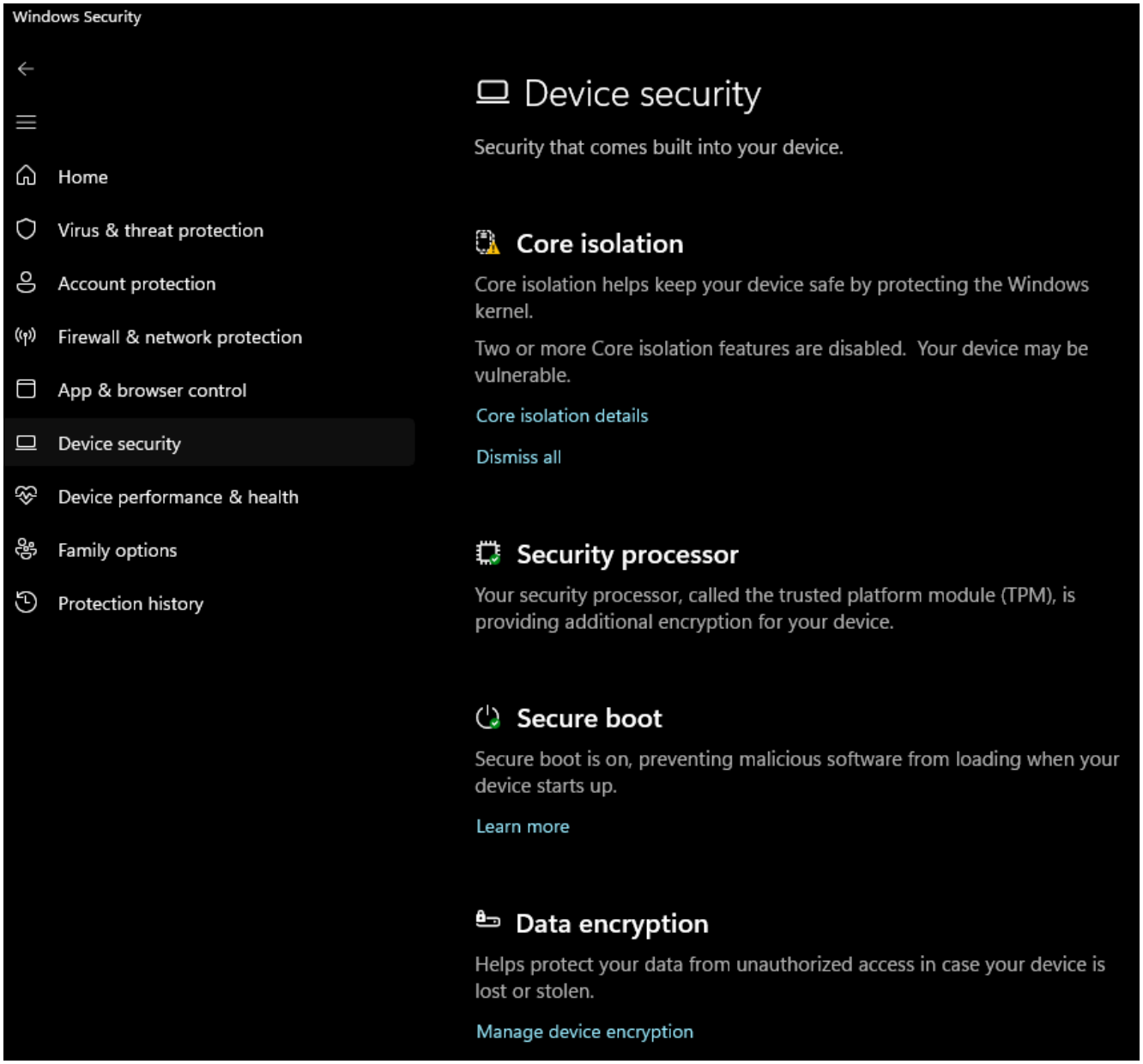

Рисунок 3.4 – Windows підтверджує активований Secure Boot

3.1.3. Перевірка та налаштування TPM 2.0

Модуль TPM необхідний для апаратного зберігання криптографічних ключів. У BIOS перевіряється:

- **AMD fTPM → Enabled**.

У Windows:

– запуск tpm.msc;

– перевірка статусу TPM Ready for use;

– підтвердження версії TPM 2.0.

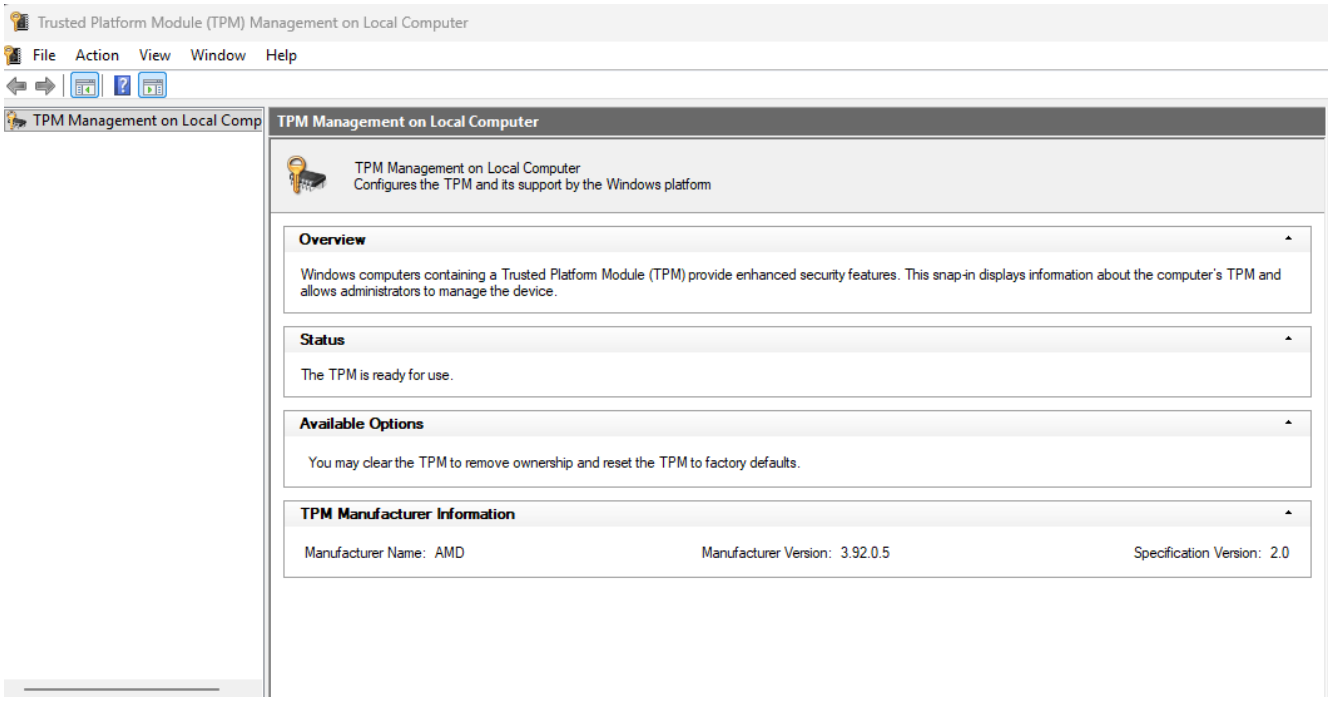

Рисунок 3.5 – вікно «Trusted Platform Module (TPM) Management » із зазначенням версії 2.0

Цей модуль надалі використовується для роботи BitLocker, Windows Hello та інших механізмів захисту.

3.2. Налаштування та увімкнення BitLocker із використанням TPM

Наступним кроком є шифрування системного диска з опорою на апаратне коріння довіри. BitLocker інтегрується з TPM, що забезпечує високий рівень захисту без потреби ручного введення ключа при кожному запуску.

3.2.1. Перевірка сумісності системи

У командному рядку PowerShell виконується:

manage-bde –status

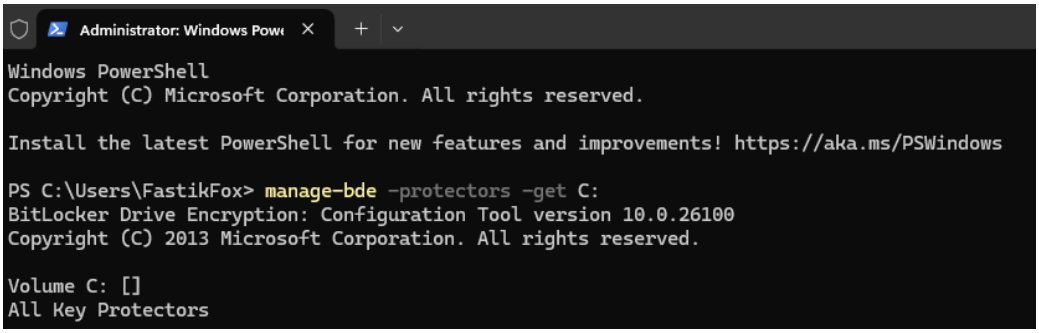

Рисунок 3.6 – Інформація про незашифрований диск та доступність TPM

3.2.2. Увімкнення шифрування

Через *Control Panel* → *BitLocker* виконується:

– увімкнення для диска C:;
– вибір «Шифрувати лише зайнятий простір» (рекомендовано для SSD);
– вибір режиму «Новий режим шифрування (XTS-AES)»;
– збереження ключа відновлення у файлі та в хмарному акаунті Microsoft.

Процес увімкнення BitLocker:

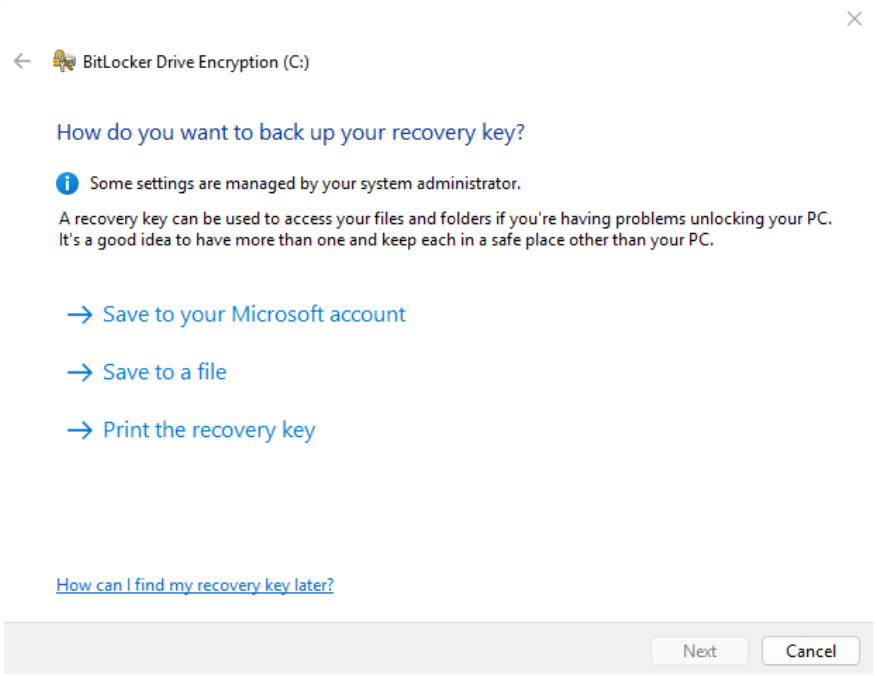

Рисунок 3.7 – Процес увімкнення BitLocker

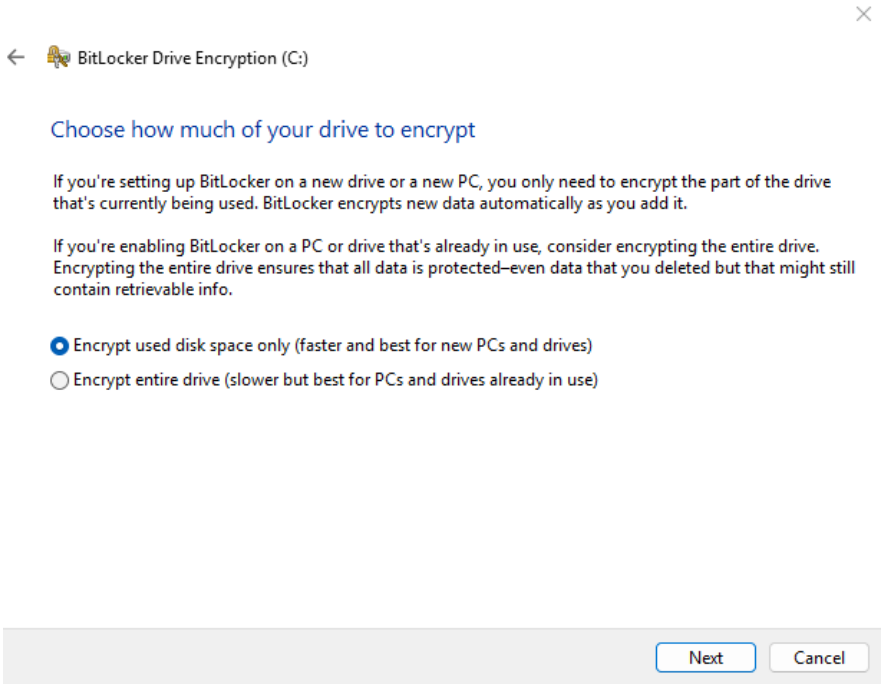

Рисунок 3.8 – Процес увімкнення BitLocker

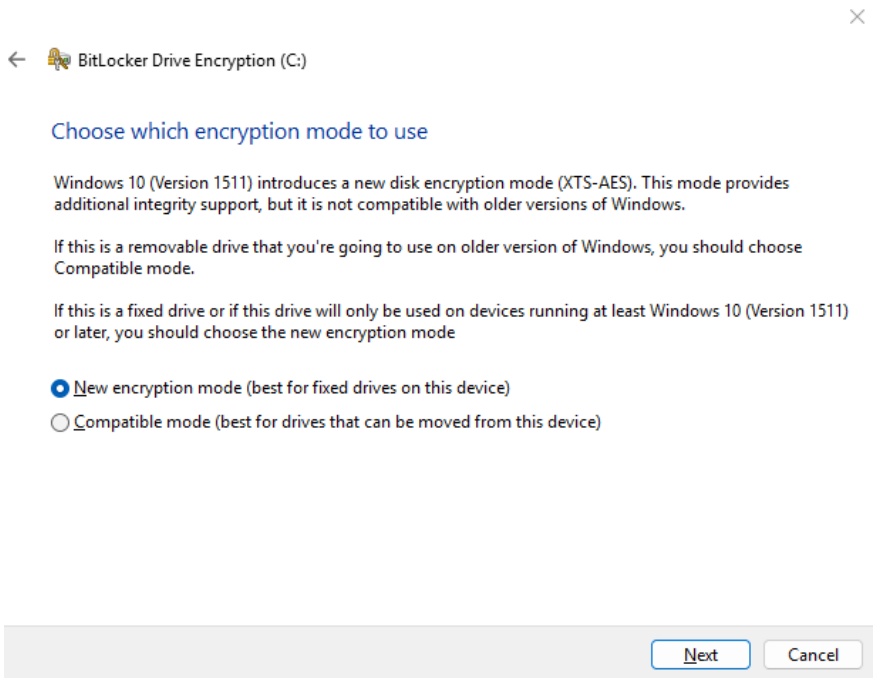

Рисунок 3.9 – Процес увімкнення BitLocker

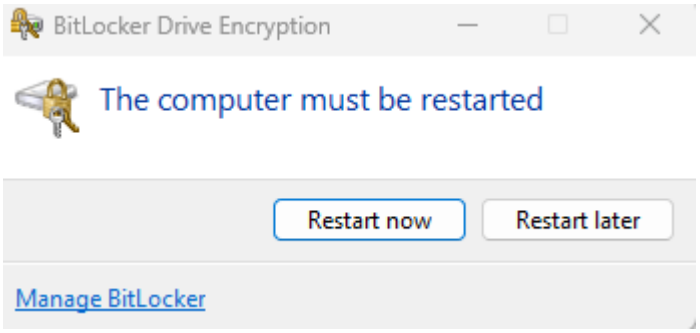

Рисунок 3.10 – Завершення шифрування диску C

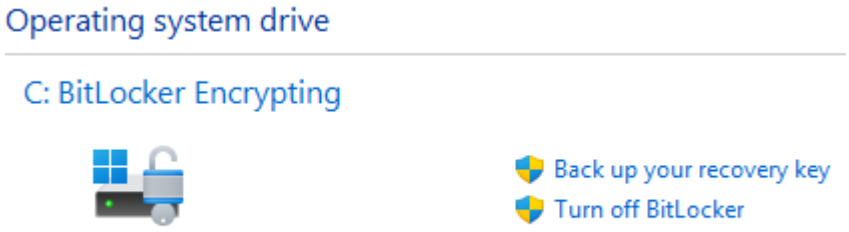

Рисунок 3.11 – Завершення шифрування диску C

3.2.3. Перевірка роботи BitLocker разом із TPM

Перевірка виконується у PowerShell за наступною командою:

manage-bde -protectors -get C:

Система повинна показати:

– TPM Protector

– Recovery Password

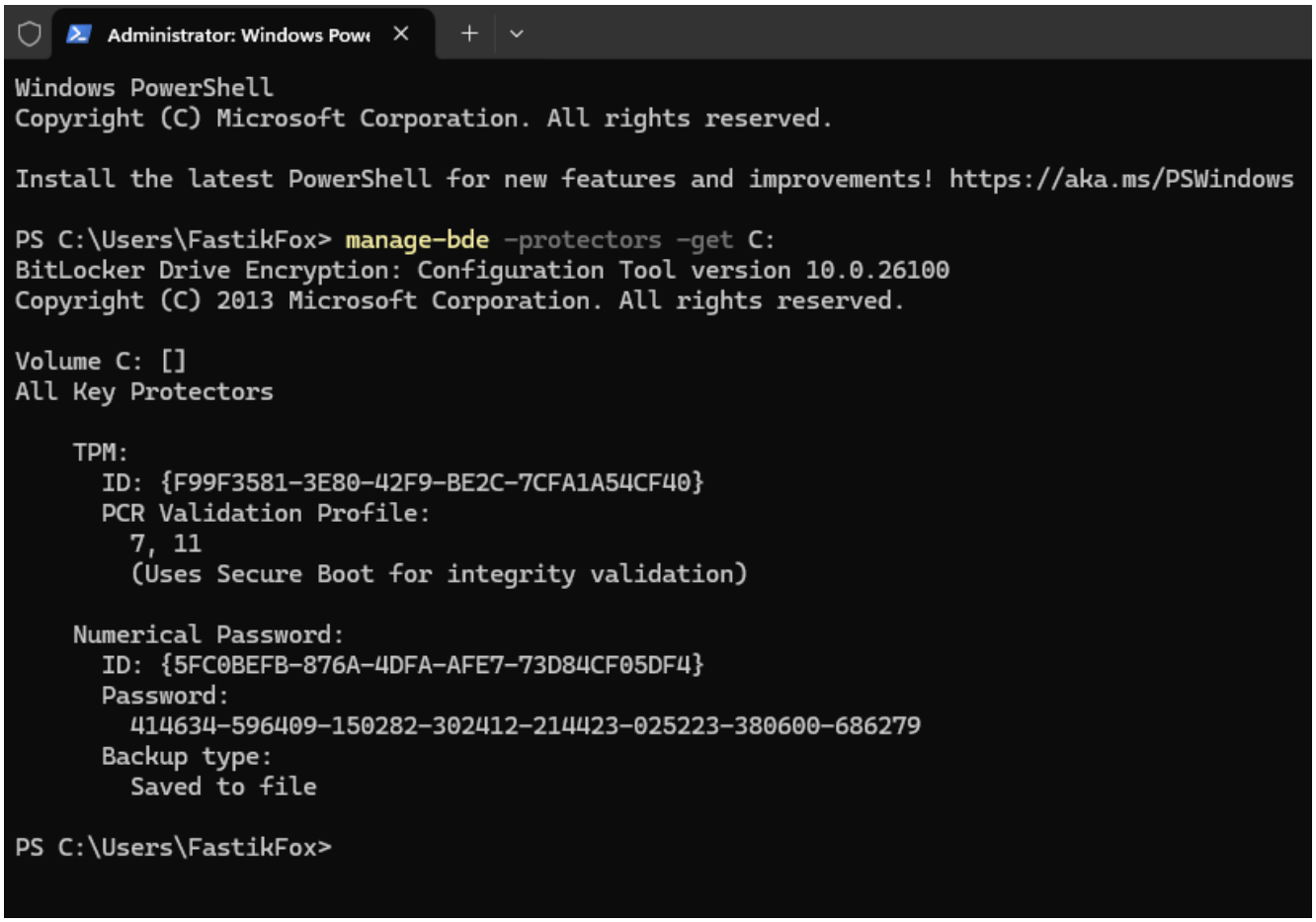

Рисунок 3.12 – Список протекторів

Тепер диск зашифровано, а ключі зберігаються у TPM, що забезпечує максимальний рівень безпеки у випадку викрадення ПК або від'єднання SSD.

3.3. Оптимізація Windows і зменшення навантаження системи

Оптимізація необхідна для покращення продуктивності, стабільності та зменшення кількості служб і компонентів, які можуть створювати уразливості або конфлікти.

3.3.1. Ручна оптимізація системи

Виконуються такі дії:

- деактивація непотрібних фонових служб через services.msc;
- очищення системи через Storage Sense;
- вимкнення телеметрії через gpedit.msc і registry;
- керування автозавантаженням у Task Manager → Startup Apps;
- очищення старих драйверів через pnputil.

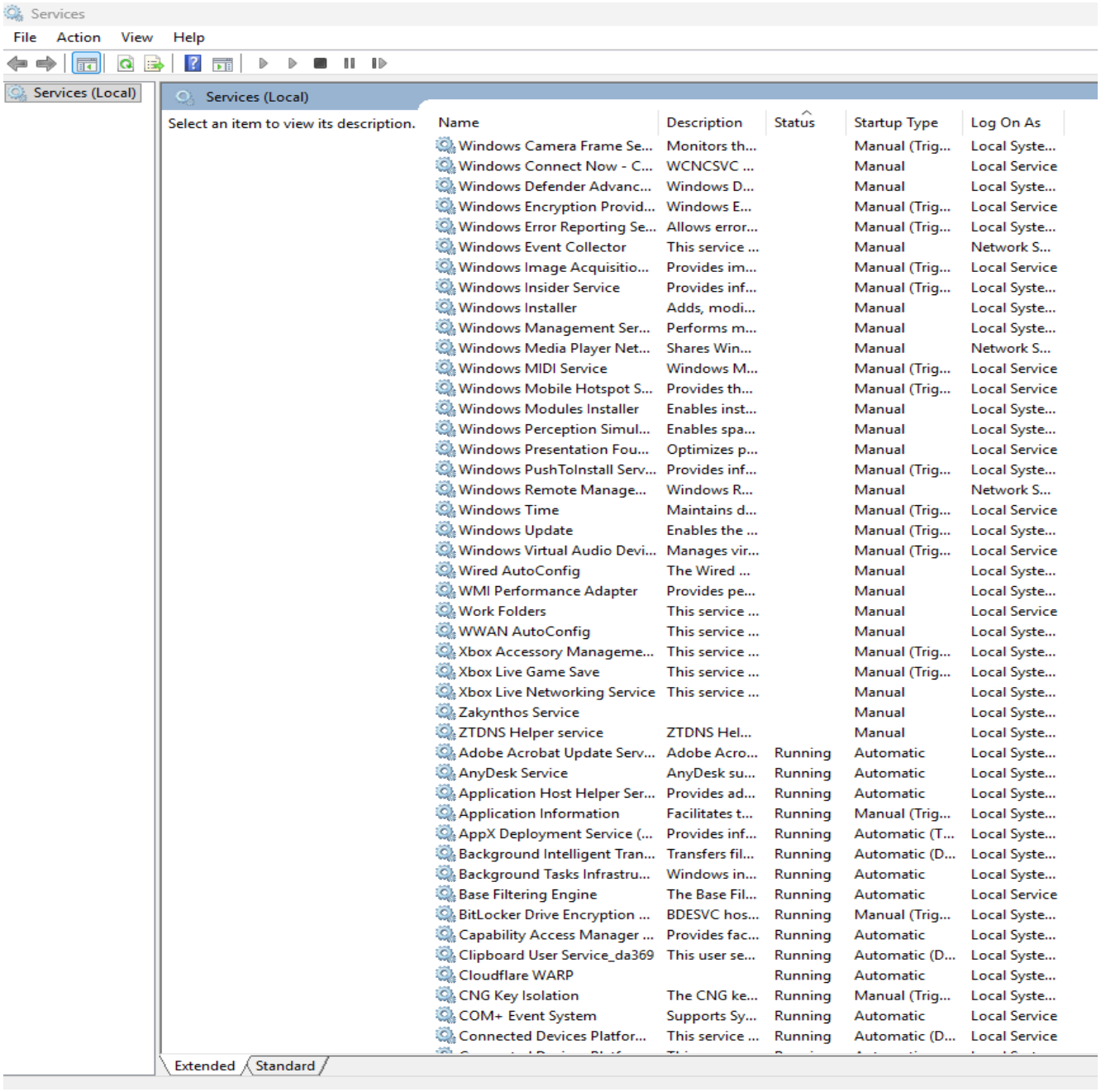

Рисунок 3.13 – Вимкнені служби

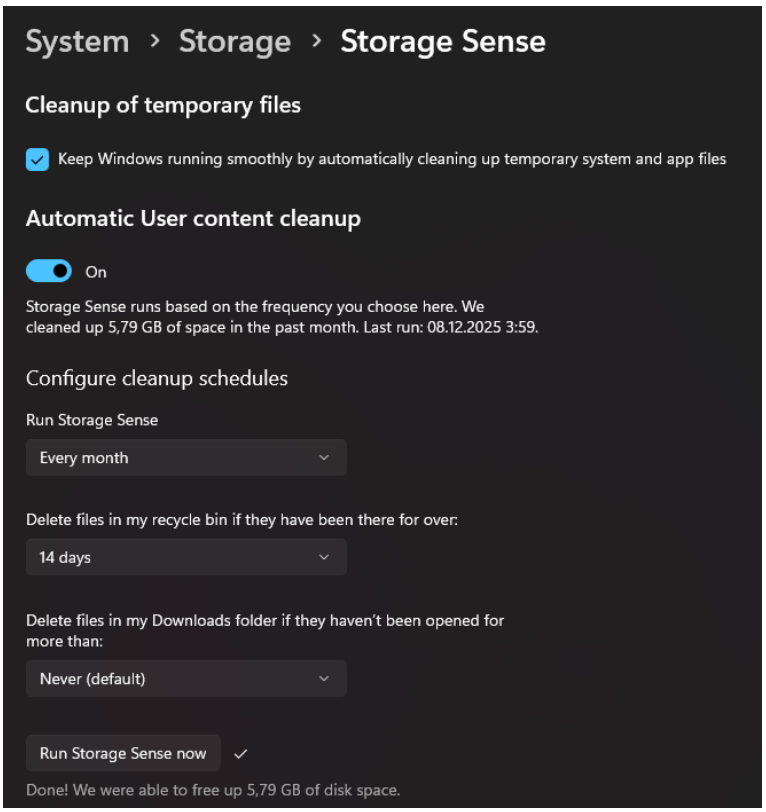

Рисунок 3.14 – Очищення Storage Sense

3.3.2. Оптимізація за допомогою WinUtil

WinUtil — відкритий PowerShell-комплекс, який автоматизує оптимізацію.

Запуск виконується у PowerShell за допомогою наступної команди:

irm https://christitus.com/win | iex

Виконується:

– очищення тимчасових файлів;

– вимкнення телеметрії;

– оптимізація служб;

– встановлення рекомендованих програм (7zip, VLC, Notepad++, WinRAR або альтернативи);

– перевірка продуктивності системи.

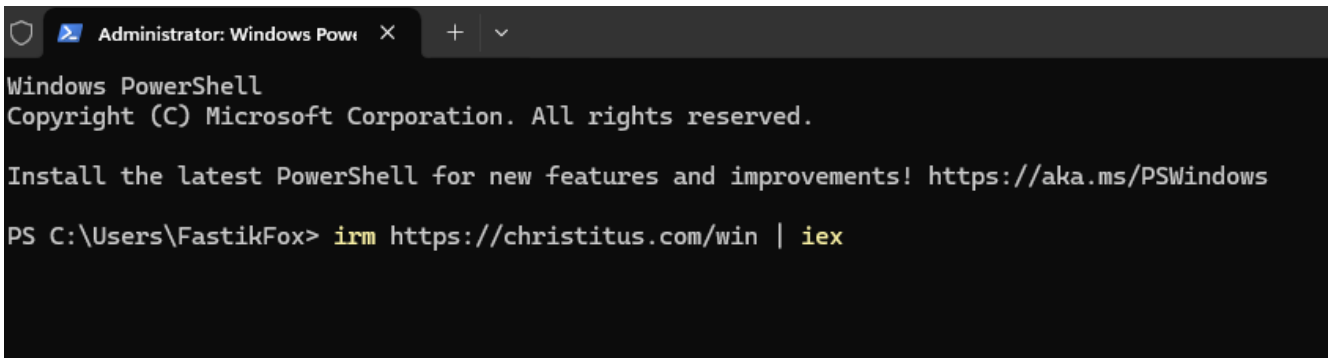

Рисунок 3.15 – Підключення до утіліти WinUtil

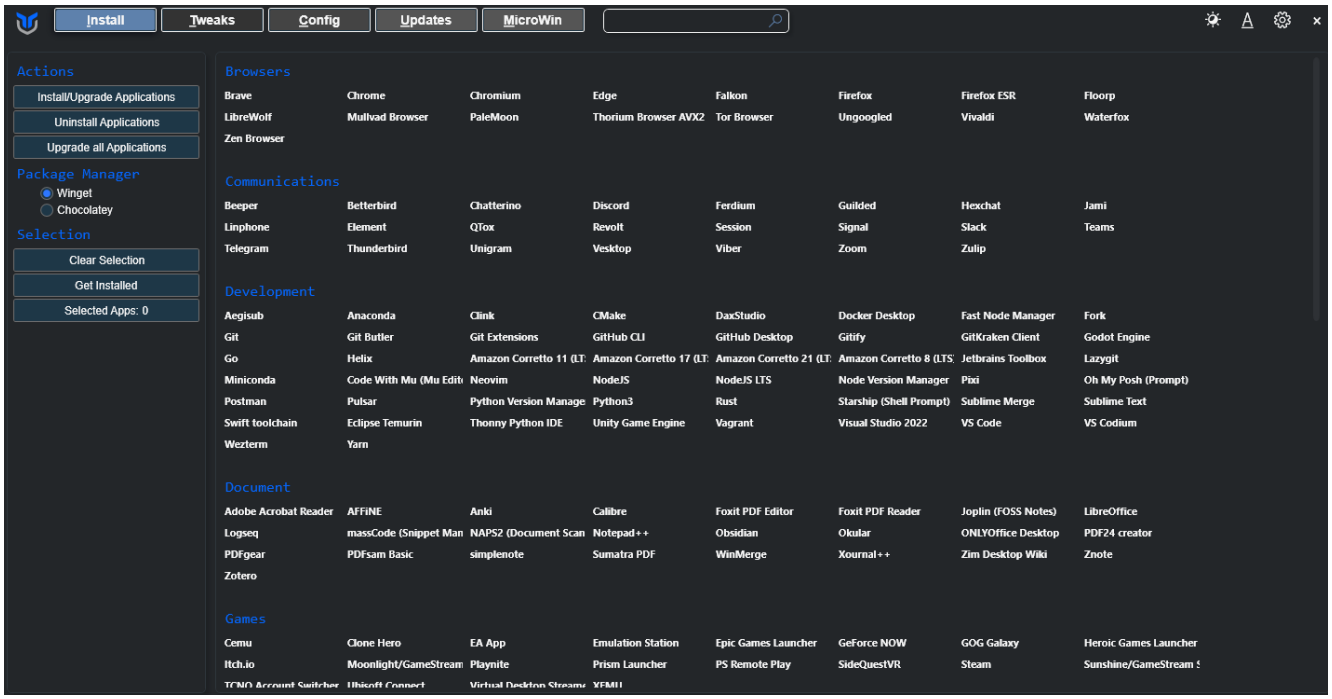

Рисунок 3.16 – Інтерфейс WinUtil

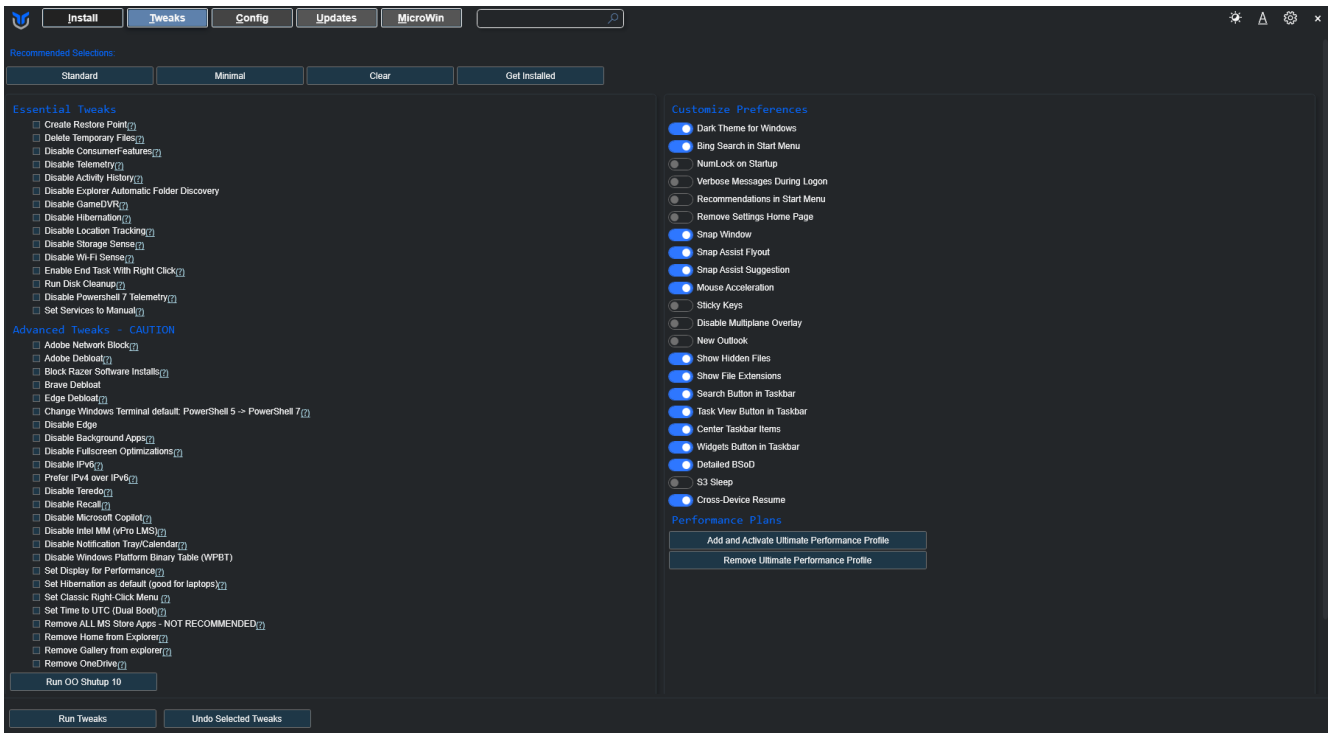

Рисунок 3.17 – Інтерфейс WinUtil

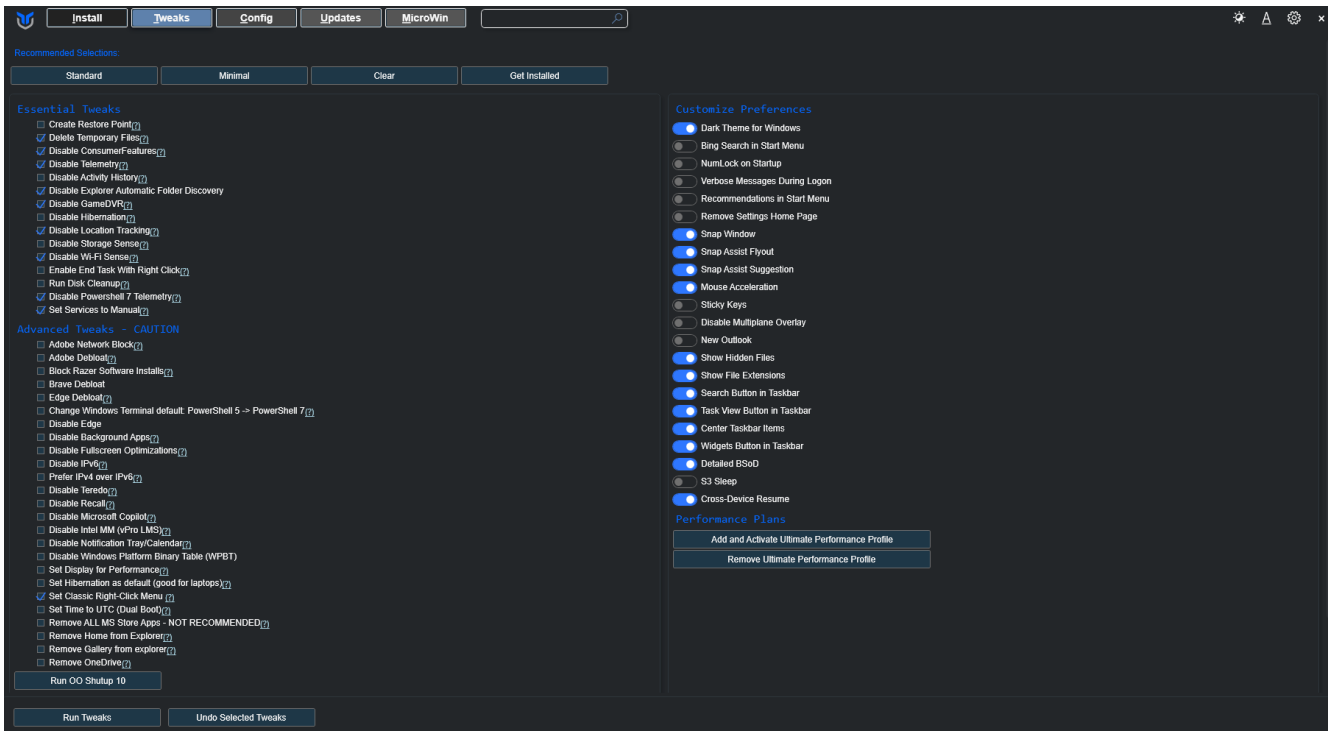

Рисунок 3.18 – Застосовані оптимізації

3.4. Діагностика системи після впровадження захисних і оптимізаційних механізмів

Після впровадження інтегрованої моделі виконуються діагностичні тести:

3.4.1. Перевірка цілісності захисного середовища

Виконуємо перевірку наявності Secure Boot за допомогою команди у PowerShell:

Get-SecureBootPolicy

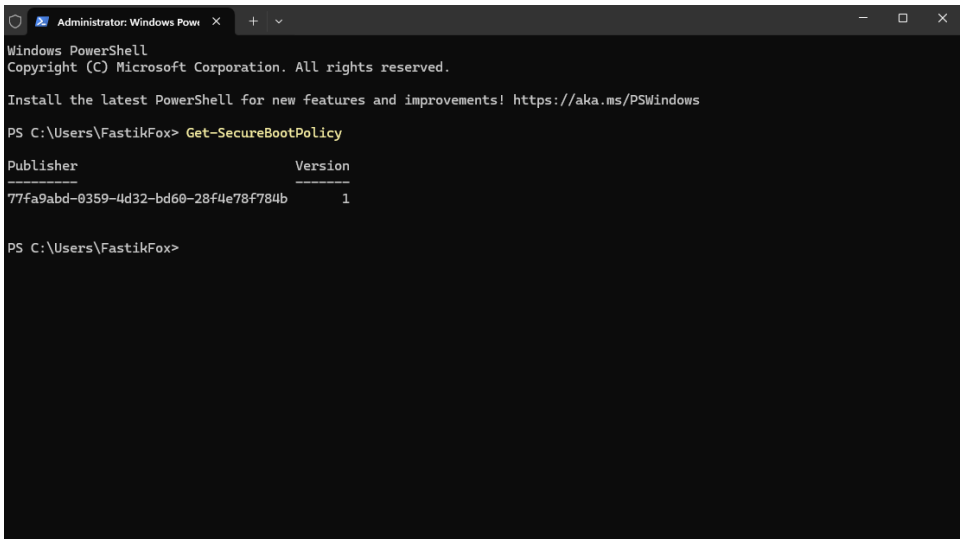

Рисунок 3.19 – Успішна відповідь Secure Boot

Виконуємо перевірку наявності Trusted Platform Module (TPM 2.0)
Команда для перевірки наявності TPM:
Get-TPM

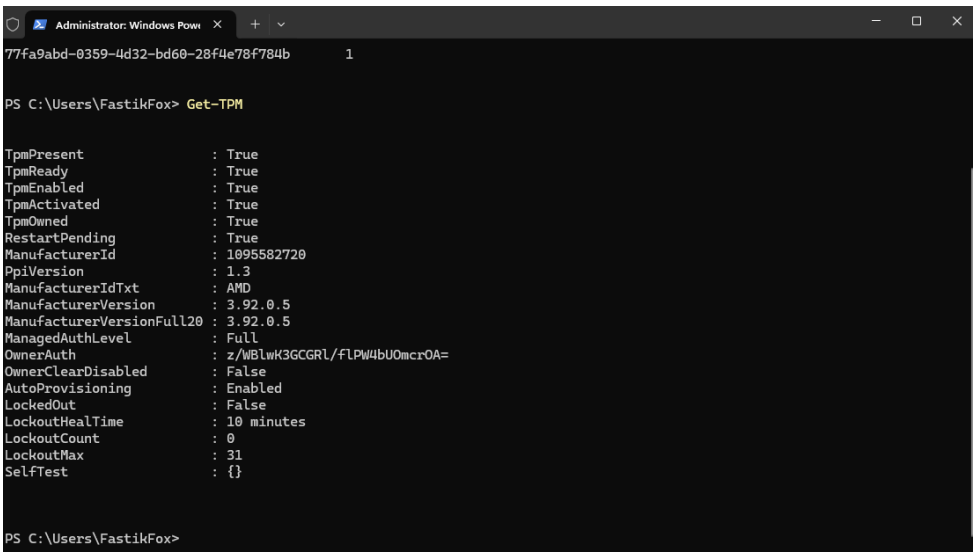

Рисунок 3.20 – TPM активний, готовий, не в стані помилки

3.4.2. Тест стабільності та продуктивності

Для перевірки та тестів використовуються:

– Task Manager → Performance;
– Windows Resource Monitor;
– winsat formal або сторонній CrystalDiskMark для перевірки SSD.

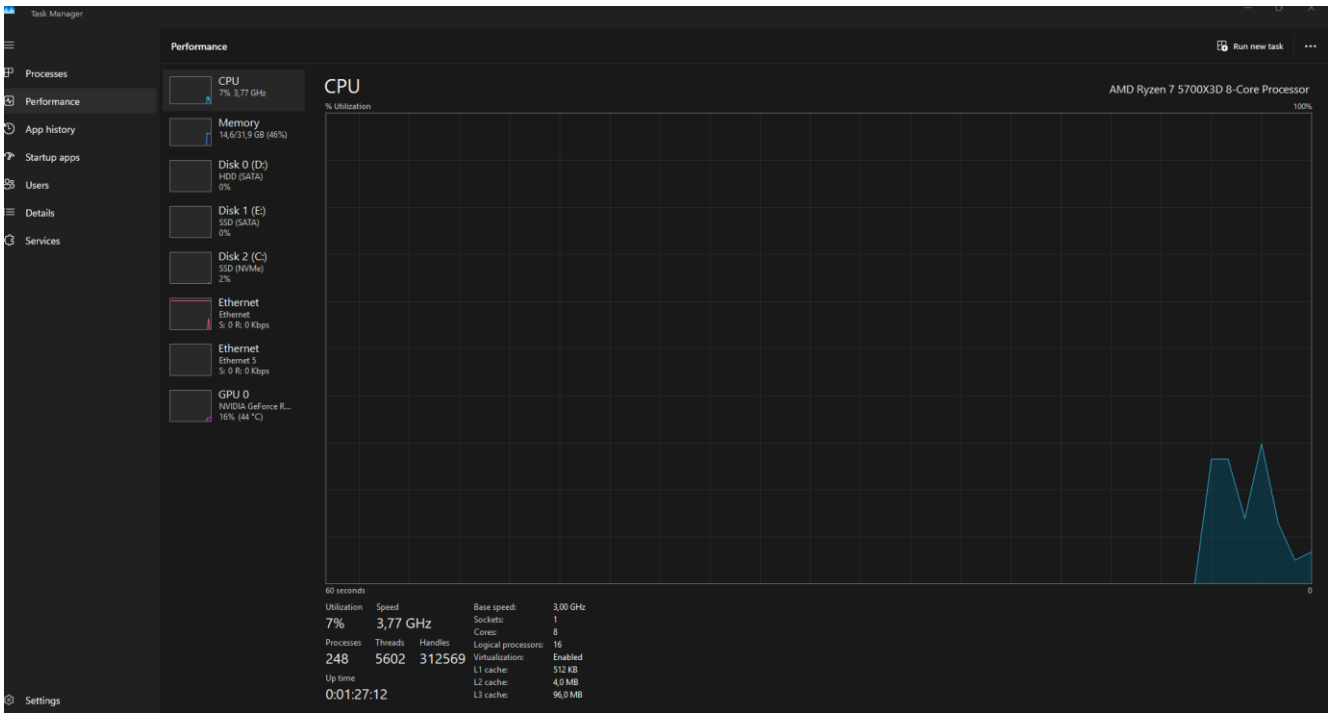

Рисунок 3.21 – Стабільна робота системи після оптимізації

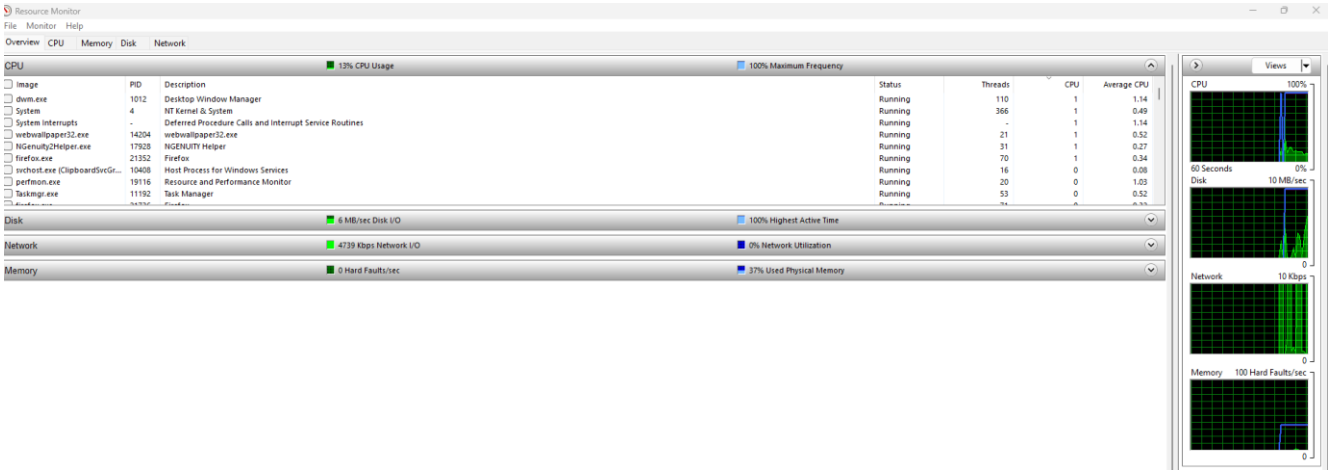

Рисунок 3.22 – Стабільна робота системи після оптимізації

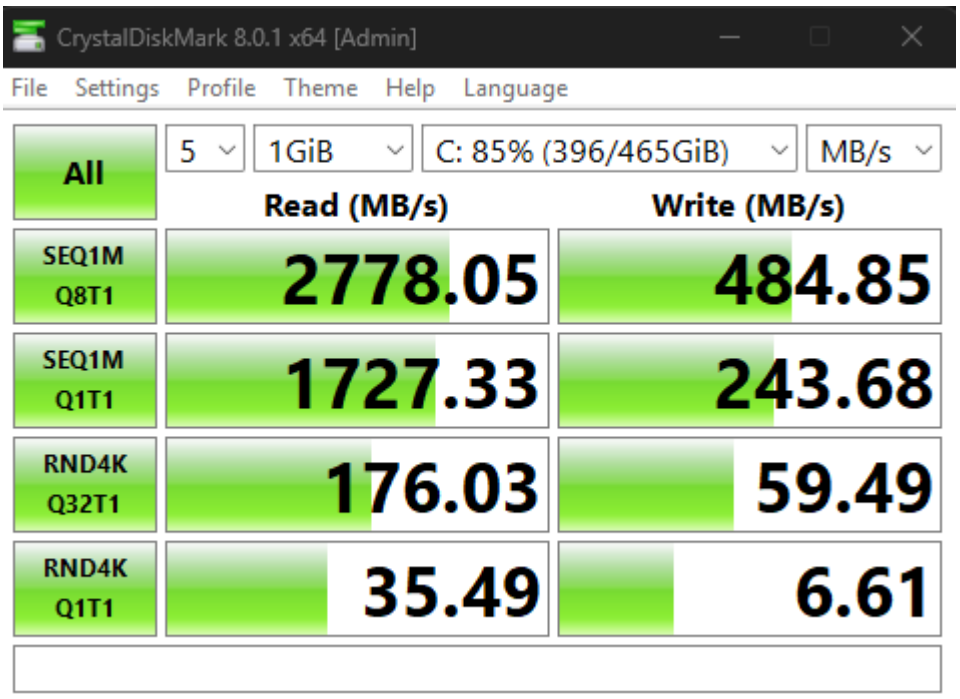

Рисунок 3.23 – Стабільна робота системи після оптимізації

3.5. Результати впровадження інтегрованої моделі безпеки та оптимізації

На основі виконаної практичної реалізації можна відзначити такі результати:

– система працює в повноцінному режимі UEFI з активним Secure Boot;

– TPM 2.0 створює апаратну основу для безпеки;

– шифрування BitLocker виконано коректно, ключі надійно захищені;

– оптимізація Windows зменшила навантаження системи та підвищила стабільність;

– система стала більш передбачуваною, захищеною та продуктивною для щоденного використання.

ВИСНОВОК ДО РОЗДІЛУ 3

Третій розділ містив практичну реалізацію інтегрованого підходу до захисту й оптимізації Windows. У ньому було продемонстровано конкретні кроки конфігурації системи, починаючи від налаштувань BIOS/UEFI, активації Secure Boot, роботи з TPM, шифрування диску BitLocker, і завершуючи оптимізаційними процедурами в самій операційній системі. Розділ включає покрокові інструкції, скриншоти та пояснення, що дозволяють повторити запропоновані дії на практиці та оцінити їх вплив на функціонування системи.

Практична частина довела, що використання апаратних засобів захисту у взаємодії з програмними механізмами Windows створює значно вищий рівень безпеки порівняно з окремими, розрізненими методами. Також підтверджено, що оптимізаційні заходи, за умови їх грамотного застосування, не суперечать безпековим технологіям і навіть сприяють підвищенню стабільності системи, зменшуючи кількість фонових процесів і знижуючи ризики збоїв.

Проведені експерименти демонструють, що інтегрований підхід забезпечує системну збалансованість: підвищення рівня захисту не лише не погіршує, але й у багатьох випадках покращує продуктивність Windows. Отримані результати підтверджують доцільність та ефективність розробленої моделі, а також її практичну придатність для використання у корпоративних мережах і на персональних комп’ютерах.

РОЗДІЛ 4. РЕКОМЕНДАЦІЇ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ІНТЕГРОВАНОГО ПІДХОДУ ДО ЗАХИСТУ ТА ОПТИМІЗАЦІЇ WINDOWS В КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

4.1. Методика формування політик безпеки та оптимізації на основі інтегрованого підходу

Методика формування політик безпеки та оптимізації базується на принципі диференціації доступу та функціональних можливостей залежно від ролі користувача в інформаційній системі. У межах інтегрованого підходу передбачається створення окремих профілів безпеки для адміністраторів, звичайних користувачів та гостьових облікових записів, що дозволяє мінімізувати ризики несанкціонованого доступу та зменшити поверхню атаки.

Для адміністраторів застосовуються розширені політики контролю доступу, багатофакторна автентифікація та аудит дій. Для звичайних користувачів обмежуються привілеї встановлення програмного забезпечення та доступу до системних налаштувань, а для гостьових облікових записів використовується принцип мінімально необхідних прав.

Важливим елементом методики є створення шаблонів групових політик (GPO), які забезпечують автоматизоване та уніфіковане налаштування Secure Boot, TPM та BitLocker. Застосування GPO зменшує ймовірність помилок ручної конфігурації та спрощує масштабування рішень у корпоративному середовищі.

Інтеграція з Active Directory та Azure Active Directory забезпечує централізоване управління політиками безпеки, обліковими записами та пристроями, що особливо актуально для гібридних і розподілених інфраструктур.

4.2. Розробка сценаріїв автоматизації за допомогою PowerShell та WinUtil

Автоматизація процесів безпеки та оптимізації є ключовим фактором ефективності інтегрованого підходу. Для цього використовуються сценарії PowerShell та інструменти на зразок WinUtil, які дозволяють стандартизувати конфігурацію систем та зменшити навантаження на системних адміністраторів.

У рамках дослідження передбачається створення власних модулів WinUtil, адаптованих до специфічних потреб організації, зокрема для первинного налаштування систем безпеки після розгортання операційної системи.

Окрема увага приділяється автоматизації моніторингу стану TPM, Secure Boot та BitLocker. За допомогою сценаріїв PowerShell можливо регулярно перевіряти стан цих компонентів, формувати звіти та оперативно реагувати на відхилення від заданих політик.

Також реалізуються сценарії періодичної оптимізації системи, зокрема очищення тимчасових файлів, керування службами та перевірка цілісності системних компонентів.

4.3. Оцінка економічної ефективності впровадження інтегрованого підходу

Оцінка економічної ефективності інтегрованого підходу включає аналіз витрат на оновлення або закупівлю обладнання з підтримкою TPM 2.0 та UEFI, а також витрат на впровадження та супровід відповідних політик безпеки.

Порівняння з традиційними методами захисту, такими як використання виключно антивірусного програмного забезпечення та мережевих файрволів, показує, що інтегрований підхід дозволяє досягти вищого рівня захисту без суттєвого збільшення операційних витрат.

Економічний ефект також проявляється у зниженні ризиків витоків даних, скороченні часу простоїв та зменшенні витрат на відновлення після інцидентів інформаційної безпеки.

4.4. Аналіз сумісності з існуючими IT-інфраструктурами

Інтегрований підхід до безпеки має бути сумісним з наявними IT-інфраструктурами організації, щоб мінімізувати ризики конфліктів та забезпечити безперервність бізнес-процесів. Активоване шифрування BitLocker повинно коректно взаємодіяти з системами резервного копіювання, такими як Veeam та Acronis, без втрати доступу до даних та без необхідності додаткових мануальних процедур відновлення.

Підтримка віртуалізації є ще одним важливим аспектом. Технології Secure Boot та TPM можуть бути інтегровані у середовища Hyper-V та VMware, зокрема

за допомогою віртуального TPM, що дозволяє забезпечити належний рівень безпеки віртуальних машин. Це особливо важливо для організацій, які активно використовують віртуальні інфраструктури для масштабування та оптимізації ресурсів.

У гібридних середовищах, де одночасно використовуються Windows та Linux, інтегрований підхід забезпечує узгоджену політику безпеки, спрощує адміністрування та дозволяє підтримувати єдині стандарти шифрування і контролю доступу. Додатково він дає можливість централізованого моніторингу стану безпеки, автоматизації процесів аудиту та швидкого реагування на інциденти, що підвищує загальний рівень захищеності корпоративної IT-інфраструктури.

4.5. Безпека в умовах віддаленої роботи (Remote Work)

В умовах поширення віддаленої роботи особливої актуальності набуває захист корпоративних ноутбуків, які використовуються поза межами офісу. Налаштування BitLocker забезпечує захист даних у разі втрати або крадіжки пристрою, шифруючи весь диск та унеможливлюючи доступ до конфіденційної інформації без належного ключа відновлення. Крім базового шифрування, рекомендується налаштувати політики контролю синхронізації корпоративних файлів та обмежити доступ до небезпечних мереж, щоб запобігти потенційним витокам даних.

Використання Windows Hello for Business у поєднанні з TPM дозволяє реалізувати безпарольну автентифікацію високого рівня безпеки, що знижує ризики фішингових атак і компрометації облікових записів. Рекомендується також застосовувати багатофакторну автентифікацію для критичних користувачів та адміністративних облікових записів, підвищуючи загальний рівень безпеки системи. Додатково впроваджуються політики безпеки для VPN-підключень, які гарантують захищений доступ до корпоративних ресурсів, моніторинг мережевих сесій і обмеження використання небезпечних протоколів. Такі заходи забезпечують цілісність даних і безпеку корпоративної інформації навіть при роботі співробітників із віддалених локацій.

4.6. Перспективні технології та тренди

Подальший розвиток операційної системи Windows, зокрема Windows 11, орієнтований на посилення апаратної безпеки та інтеграцію сучасних механізмів захисту даних. Такі технології, як Pluton та концепція Secured-Core PC, підвищують стійкість систем до атак на рівні прошивки та апаратного забезпечення, захищають ключі шифрування та автентифікаційні дані від сторонніх впливів. Нові функції забезпечують централізоване управління безпекою та контроль за станом пристроїв, що дозволяє організаціям швидко реагувати на потенційні загрози.

Інтеграція з архітектурою Zero Trust передбачає постійну перевірку ідентичності та стану пристроїв, незалежно від їх розташування в мережі, забезпечуючи динамічний контроль доступу та моніторинг поведінки користувачів. Перспективним напрямом є використання методів штучного інтелекту для виявлення аномалій та підозрілої поведінки в системі, прогнозування потенційних атак та автоматичної реакції на загрози. Крім того, розвиток хмарних сервісів та інтеграція з платформами Microsoft 365 дозволяє реалізувати безшовну безпеку для гібридних середовищ і віддаленої роботи, забезпечуючи високий рівень захисту корпоративної інформації.

4.7. Практичні кейси впровадження

Практичні кейси впровадження інтегрованого підходу демонструють його ефективність у фінансовому секторі та державних установах України. Порівняльний аналіз стану безпеки до та після впровадження показує зменшення кількості інцидентів та скорочення часу відновлення систем.

Відгуки системних адміністраторів свідчать про спрощення управління безпекою, а користувачі відзначають мінімальний вплив нових механізмів захисту на повсякденну роботу.

4.8. Обмеження та ризики інтегрованого підходу

Незважаючи на переваги, інтегрований підхід має певні обмеження. Основною проблемою є використання застарілого обладнання, яке не підтримує TPM 2.0 або UEFI.

Додаткові труднощі можуть виникати під час налаштування політик у гетерогенних мережах. Окремим ризиком є можливість втрати ключів відновлення BitLocker, що потребує належної організації їх зберігання та резервування.

4.9. Рекомендації для державних та критичних інфраструктур

Для державних організацій та об’єктів критичної інфраструктури рекомендується впроваджувати інтегрований підхід з урахуванням вимог ДСТУ, ISO/IEC 27001 та рекомендацій NIST.

Обов’язковими елементами є регулярний аудит та сертифікація систем захисту, а також побудова багаторівневої моделі безпеки, яка поєднує апаратні, програмні та організаційні заходи.

4.10. Віртуалізація та віддалений доступ

Віртуалізація — це технологія, яка дозволяє створювати віртуальні версії фізичних ресурсів, таких як сервери, робочі станції, операційні системи, мережеві пристрої та сховища даних. Вона забезпечує ефективне використання апаратних засобів, ізоляцію середовищ, централізоване управління ресурсами, підвищує безпеку та масштабованість IT-інфраструктури. Віртуалізація дозволяє організаціям швидко розгортати нові середовища для тестування, навчання, резервного копіювання та забезпечення відмовостійкості систем.

У контексті безпеки інтегрований підхід передбачає використання віртуалізації для підвищення захисту даних та управління доступом. Технології Secure Boot та TPM можуть бути інтегровані у віртуальні машини, що дозволяє підтримувати апаратні засоби безпеки навіть у віртуалізованих середовищах. Це забезпечує ізоляцію середовищ, контроль доступу та централізований моніторинг стану безпеки, зменшуючи ризики компрометації критичних систем.

Крім того, віртуалізація полегшує масштабування ресурсів та оптимізацію навантаження на фізичні сервери, дозволяючи розгортати кілька віртуальних машин на одному фізичному сервері без втрати продуктивності. Вона також спрощує адміністрування та підтримку IT-інфраструктури, оскільки дозволяє централізовано керувати системами, виконувати резервне копіювання,

відновлювати робочі середовища та проводити аудит без впливу на основні операційні системи.

4.11. Приклади віддаленого доступу та віртуалізації робочого місця

Серед популярних технологій віддаленого доступу та віртуалізації робочого місця можна виділити наступні:

- **RDP (Remote Desktop Protocol)** — протокол Microsoft для віддаленого підключення до робочого столу Windows. Дозволяє користувачам працювати з додатками та файлами як на локальному комп'ютері, при цьому забезпечуючи можливості централізованого контролю доступу та безпечного з'єднання.
- **AnyDesk** — кросплатформене рішення для віддаленого управління комп'ютерами. Забезпечує високу швидкість з’єднання, низьку затримку, можливість спільної роботи та передачу файлів. Використовується для технічної підтримки, віддаленої роботи та управління серверами.
- **TeamViewer** — програмне забезпечення для віддаленого доступу та підтримки користувачів. Дозволяє проводити презентації, обмін файлами, консультувати віддалених користувачів та управляти робочими станціями з високим рівнем безпеки.

Використання цих технологій у поєднанні з інтегрованим підходом до безпеки дозволяє організаціям забезпечити надійний віддалений доступ, контроль дій користувачів, захист конфіденційних даних та централізоване управління політиками безпеки. Це особливо важливо у сучасних умовах віддаленої роботи та гібридних середовищ, де забезпечення безпечного доступу до корпоративних ресурсів є критичним для безперервності бізнес-процесів та збереження інформаційної цілісності.

4.12. Висновки та подальші напрями дослідження

У розділі узагальнено результати практичного впровадження інтегрованого підходу до захисту та оптимізації Windows-систем. Доведено, що поєднання апаратних та програмних механізмів безпеки дозволяє підвищити загальний рівень захищеності інформаційних ресурсів.

Подальші напрями дослідження можуть включати питання захисту IoT-пристроїв на базі Windows, а також використання перспективних криптографічних методів, зокрема квантової криптографії.

ВИСНОВОК ДО РОЗДІЛУ 4

У розділі 4 проведено детальний аналіз методик формування політик безпеки та оптимізації Windows на основі інтегрованого підходу. Було визначено, що диференційоване налаштування профілів безпеки для різних категорій користувачів, використання групових політик, централізоване управління через Active Directory та Azure AD, а також автоматизація процесів за допомогою PowerShell та WinUtil забезпечують комплексний захист систем.

Розглянуто економічну ефективність впровадження інтегрованого підходу, сумісність із існуючими IT-інфраструктурами, а також безпеку в умовах віддаленої роботи. Проаналізовано перспективні технології та практичні кейси, що демонструють реальне підвищення безпеки та стабільності систем. Виявлено обмеження та ризики, пов’язані зі старим обладнанням та складністю налаштування в гетерогенних середовищах. Розділ підтвердив доцільність інтегрованого підходу та окреслив практичні рекомендації для його застосування в організаціях.

РОЗДІЛ 5. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ІНТЕГРОВАНОГО ПІДХОДУ

5.1. Опис тестового середовища та вихідних умов

Для перевірки ефективності інтегрованого підходу до захисту та оптимізації Windows було розгорнуто тестове середовище, яке максимально наближене до типової корпоративної IT-інфраструктури. До складу середовища входили робочі станції під управлінням Windows 10 та Windows 11, сервер на базі Windows Server з розгорнутим доменом Active Directory, а також клієнтські пристрої з різними рівнями доступу, включаючи облікові записи адміністратора, звичайних користувачів та гостьові облікові записи.

Апаратна частина включала системи з підтримкою UEFI та TPM 2.0, що забезпечило повний функціонал Secure Boot, BitLocker та Windows Hello for Business. Особлива увага приділялася сумісності апаратних компонентів та перевірці їх здатності підтримувати шифрування дисків і безпарольну автентифікацію. Вихідні умови передбачали стандартну конфігурацію систем без посилених політик безпеки, що дало змогу об’єктивно оцінити вплив запропонованих заходів на стабільність, продуктивність та захищеність операційних систем.

Для забезпечення комплексної оцінки ефективності інтегрованого підходу були визначені ключові параметри тестування: час завантаження системи, рівень захисту даних, працездатність служб, стабільність роботи мережевих протоколів та відсутність конфліктів між компонентами безпеки. Таке середовище дозволило отримати репрезентативні результати, що можуть бути масштабовані для реальних корпоративних умов.

5.2. Поетапне впровадження інтегрованого підходу

Впровадження інтегрованого підходу здійснювалося поетапно для забезпечення максимальної ефективності та мінімізації ризиків. На першому етапі було проведено детальний аналіз апаратної сумісності пристроїв та підготовку систем до роботи в режимі UEFI з активованим TPM 2.0, що дозволило гарантувати

підтримку апаратних механізмів безпеки та належне зберігання криптографічних ключів.

На другому етапі здійснено налаштування Secure Boot та базових політик безпеки операційної системи, включаючи обмеження доступу до критичних системних ресурсів і контроль цілісності завантажувальних компонентів. Додатково проведено аудит існуючих налаштувань та підготовку скриптів для автоматизації процесів моніторингу стану безпеки.

Наступним кроком стало впровадження шифрування дисків за допомогою BitLocker із централізованим зберіганням ключів відновлення в Active Directory та Azure AD. Це забезпечило надійний захист корпоративних даних та спрощене управління ключами для адміністраторів. Після цього застосовано групові політики для обмеження прав користувачів, контроль доступу до системних ресурсів та увімкнення механізмів аудиту, що дозволяє відстежувати спроби несанкціонованого доступу та забезпечує відповідність вимогам інформаційної безпеки.

Кожен етап супроводжувався перевіркою працездатності систем, тестуванням конфігурацій та підготовкою рекомендацій щодо оптимізації налаштувань для різних категорій користувачів, що забезпечило ефективну та безпечну інтеграцію всіх компонентів безпеки.

5.3. Результати експериментальної перевірки

У результаті експериментального впровадження було зафіксовано підвищення рівня захищеності системи від несанкціонованого доступу та атак на рівні завантаження. Активація Secure Boot унеможливила використання змінених або шкідливих завантажувачів, а застосування BitLocker забезпечило повний захист даних на носіях інформації.

Крім безпекових переваг, було відзначено позитивний вплив оптимізаційних заходів на стабільність роботи системи. Скоротилася кількість збоїв, пов’язаних із некоректною роботою служб, а час завантаження операційної системи зменшився у порівнянні з початковою конфігурацією.

5.4. Аналіз отриманих результатів

Аналіз результатів експериментальної перевірки показав, що інтегрований підхід є значно ефективнішим у порівнянні з фрагментарним застосуванням окремих засобів захисту. Поєднання апаратних механізмів безпеки, таких як TPM 2.0 та Secure Boot, з програмними політиками безпеки, шифруванням BitLocker та груповими політиками дозволяє створити цілісну модель захисту, стійку до широкого спектра загроз і атак.

Особливо важливою перевагою інтегрованого підходу є зменшення залежності від стороннього програмного забезпечення, що знижує витрати на ліцензування та спрощує адміністрування системи. Крім того, автоматизація контролю стану системи та моніторинг аномальної поведінки користувачів дозволяють швидко реагувати на потенційні загрози та підтримувати високий рівень безпеки без значного збільшення навантаження на IT-персонал.

Додатково інтегрований підхід сприяє підвищенню стабільності роботи систем, зменшенню кількості простоїв та збоїв, що забезпечує безперервність бізнес-процесів та оптимізацію витрат організації на обслуговування та підтримку IT-інфраструктури.

5.5. Практичні рекомендації за результатами дослідження

На основі проведеного дослідження сформульовано практичні рекомендації щодо впровадження інтегрованого підходу до захисту та оптимізації Windows у корпоративних середовищах. Зокрема, рекомендується виконувати поетапний перехід до використання TPM 2.0 та Secure Boot, починаючи з критично важливих систем.

Також доцільним є використання автоматизованих сценаріїв PowerShell для контролю стану безпеки та регулярної оптимізації систем. Для організацій із підвищеними вимогами до безпеки рекомендовано поєднувати інтегрований підхід із принципами Zero Trust та регулярним аудитом інформаційної безпеки.

ВИСНОВОК ДО РОЗДІЛУ 5

Цей розділ демонструє практичну реалізацію інтегрованого підходу та експериментальну перевірку його ефективності. Створене тестове середовище дозволило оцінити вплив впровадження Secure Boot, TPM 2.0, BitLocker та групових політик на рівень безпеки та стабільність роботи систем. Поетапне впровадження та автоматизація контролю стану системи показали позитивний вплив на зменшення часу простоїв та підвищення продуктивності.

Експериментальна перевірка підтвердила, що інтегрований підхід забезпечує комплексний захист, знижує ризики несанкціонованого доступу та полегшує адміністрування систем. На основі отриманих результатів сформульовано практичні рекомендації щодо впровадження інтегрованого підходу у корпоративних та державних організаціях, включаючи поетапне підключення апаратних засобів безпеки та використання автоматизованих сценаріїв для моніторингу та оптимізації.

ВИСНОВКИ

У ході виконання дипломної роботи було проведено комплексне дослідження підходів до забезпечення безпеки та оптимізації операційної системи Windows із використанням сучасних апаратних і програмних механізмів. Здійснений аналіз дозволив виявити ключові вразливості, властиві операційним системам загального призначення, встановити фактори, що впливають на їхню продуктивність і захищеність, а також визначити шляхи створення інтегрованої моделі кіберзахисту на основі UEFI, Secure Boot, TPM 2.0, BitLocker та системних інструментів оптимізації.

Теоретичний розділ роботи підтвердив, що безпека Windows формується як результат взаємодії декількох рівнів — апаратного, завантажувального, операційного та прикладного. Окремо кожен із механізмів (TPM, Secure Boot, BitLocker, UAC, політики безпеки, оптимізаційні інструменти) може забезпечити лише частковий рівень захисту. Проте саме їх узгоджена робота створює цілісну екосистему, здатну протистояти сучасним загрозам, включно з атаками на ранні етапи завантаження, компрометацію даних та експлуатацію слабко захищених служб системи.

У розділі, присвяченому аналізу існуючих рішень, було встановлено, що більшість наявних підходів у науковій та прикладній літературі мають фрагментарний характер, зосереджуючись або суто на безпекових механізмах, або виключно на оптимізації робочого середовища. Залишається недостатньо розкритим питання комплексного поєднання цих факторів, що є критично важливим для сучасних інформаційних систем. Це підтверджує актуальність поставленої мети та закономірність вибору напрямку дослідження.

Практична частина роботи продемонструвала можливість і ефективність впровадження інтегрованого підходу на прикладі реальної робочої станції. Було виконано налаштування UEFI-середовища, перевірено та активовано Secure Boot, увімкнено і протестовано TPM 2.0, реалізовано шифрування системного диска через BitLocker із прив’язкою до апаратного модуля, виконано комплекс оптимізацій операційної системи за допомогою вбудованих засобів Windows та

PowerShell-утиліти WinUtil. Результати практичної перевірки підтвердили правильність розробленої моделі: система набула вищого рівня захищеності, стабільності та продуктивності без негативного впливу на функціональність.
Отримані результати дозволяють зробити такі узагальнені висновки:

- інтегроване поєднання апаратних та програмних механізмів захисту формує значно вищий рівень кіберстійкості порівняно з використанням окремих інструментів;
- активовані механізми раннього контролю цілісності (Secure Boot, TPM) істотно зменшують ризики втручання у процес завантаження системи;
- шифрування BitLocker у зв'язці з TPM дає змогу надійно захистити конфіденційні дані навіть у разі фізичного доступу до носія;
- оптимізаційні заходи, за умови правильного застосування, не конфліктують із безпековими технологіями, а навпаки — сприяють стабільній роботі ОС;
- Windows здатна забезпечити високий рівень захисту та продуктивності лише в умовах правильно налаштованої екосистеми, де кожен компонент виконує роль у загальній моделі;
- запропонована модель є придатною для впровадження як у корпоративному середовищі, так і на персональних пристроях, що робить її універсальною та практично значущою.

Таким чином, поставлена у роботі мета — розроблення та практична реалізація інтегрованого підходу до захисту та оптимізації Windows — була досягнута повністю. Проведене дослідження підтверджує, що синергія між апаратними засобами, системними функціями безпеки та оптимізаційними методами є найбільш ефективним шляхом до створення надійної, стабільної та продуктивної операційної системи в умовах сучасного інформаційного середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. **Microsoft. Secure Boot Documentation** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot (дата звернення: 01.12.2025).
2. **Microsoft. BitLocker Planning Guide** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/planning-guide (дата звернення: 01.12.2025).
3. **Microsoft. BitLocker Recovery Guide** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/recovery-overview (дата звернення: 01.12.2025).
4. **Microsoft. Protecting BitLocker from Cold Boot Attacks** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ (дата звернення: 01.12.2025).
5. **Microsoft. Trusted Platform Module (TPM) Overview and Requirements** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/trusted-platform-module-overview (дата звернення: 01.12.2025).
6. **Trusted Computing Group. TPM 2.0 Library Specification** [Електронний ресурс]. — Режим доступу: https://trustedcomputinggroup.org/resource/tpm-library-specification/ (дата звернення: 01.12.2025).
7. **Trusted Computing Group. TPM 2.0 Mobile and PC Platform Specification** [Електронний ресурс]. — Режим доступу: https://trustedcomputinggroup.org/resource/pc-client-platform-tpm-profile-ptp-specification/ (дата звернення: 01.12.2025).

8. **How to Use the TPM: A Guide to Hardware-Based Endpoint Security** [Електронний ресурс]. — Режим доступу: https://trustedcomputinggroup.org/resource/how-to-use-the-tpm-a-guide-to-hardware-based-endpoint-security/ (дата звернення: 01.12.2025)

9. **UEFI Forum. UEFI Specification, Version 2.10** [Електронний ресурс]. — Режим доступу: https://uefi.org/specifications (дата звернення: 01.12.2025).

10. **Microsoft. UEFI Firmware Security for Windows Devices** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows-hardware/drivers/bringup/uefi-security (дата звернення: 01.12.2025).

11. **NIST SP 800-147. BIOS Protection Guidelines** [Електронний ресурс]. — Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-147/final (дата звернення: 01.12.2025).

12. **Microsoft. Windows Boot Process and Secure Boot Chain** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process (дата звернення: 01.12.2025).

13. **Microsoft. Windows Security Baselines** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines (дата звернення: 04.12.2025).

14. **Microsoft Security Compliance Toolkit (SCT)** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10 (дата звернення: 04.12.2025).

15. **CIS Benchmarks for Windows 10/11** [Електронний ресурс]. — Режим доступу: https://www.cisecurity.org/cis-benchmarks (дата звернення: 04.12.2025).

16. **Microsoft. Device Encryption and Hardware Security Features** [Електронний ресурс]. — Режим доступу: https://support.microsoft.com/en-us/windows/device-encryption-in-windows-cf7e2b6f-3e70-4882-9532-18633605b7df (дата звернення: 04.12.2025).

17. **Microsoft. Credential Guard Security Architecture** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard (дата звернення: 04.12.2025).

18. **Microsoft. Windows Defender Application Control (WDAC) Technical Guide** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control (дата звернення: 04.12.2025).

19. **Microsoft. AppLocker Technical Documentation** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/applocker-overview (дата звернення: 04.12.2025).

20. **Microsoft. Audit logging and monitoring overview** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/compliance/assurance/assurance-audit-logging (дата звернення: 05.12.2025).

21. **Use Windows Event Forwarding to help with intrusion detection** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/use-windows-event-forwarding-to-assist-in-intrusion-detection (дата звернення: 05.12.2025).

22. **Microsoft. ETW (Event Tracing for Windows) Architecture** [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/win32/etw/event-tracing-portal (дата звернення: 05.12.2025).

23. **Microsoft Digital Defense Report 2025** [Електронний ресурс]. — Режим доступу: https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/ (дата звернення: 05.12.2025).

24. **Verizon. Data Breach Investigations Report (DBIR)** [Електронний ресурс]. — Режим доступу: https://www.verizon.com/business/resources/reports/dbir (дата звернення: 05.12.2025).

25. **CrowdStrike. Global Threat Report** [Електронний ресурс]. — Режим доступу: https://www.crowdstrike.com/resources/reports (дата звернення: 05.12.2025).

26. Russinovich M., Solomon D., Ionescu A. Windows Internals. Part 2: System Architecture, Processes, Threads, Memory Management, and More. — 7th ed. — Redmond : Microsoft Press, 2017.

27. Delamater J. Mastering Windows Security and Hardening / Packt Publishing, 2021.

28. Shinder D., Tittel E. Configuring Windows Server, Hyper-V, Storage, and More / Microsoft Press, 2019.

29. Rosenblatt W. Windows Group Policy: Fundamentals, Security, and the Managed Desktop / Microsoft Press, 2018.

30. McCarty B. UEFI BIOS and Secure Boot Security / Wiley, 2020.

31. Kearney J. Cryptography and Network Security Principles and Practice / Pearson, 2020.

32. Surve P. P., Brodt O., Yampolskiy M., Elovici Y., Shabtai A. SoK**:** Security Below the OS — A Security Analysis of UEFI [Електронний ресурс]. — Режим доступу: https://arxiv.org/abs/2311.03809 (дата звернення: 08.12.2025).

33. Segal K. S., Gorelik H. C., Brodt O., Elbahar Y., Elovici Y. UEFI Memory Forensics: A Framework for UEFI Threat Analysis [Електронний ресурс]. — Режим доступу: https://arxiv.org/abs/2501.16962 (дата звернення: 08.12.2025).

34. Jacob H. N., Werling C., Buhren R., Seifert J. faulTPM: Exposing AMD fTPMs' Deepest Secrets [Електронний ресурс]. — Режим доступу: https://arxiv.org/abs/2304.14717 (дата звернення: 08.12.2025).

35. Zhang Q., Zhao S. A Comprehensive Formal Security Analysis of TPM 2.0 Key Exchange Primitive [Електронний ресурс]. — Режим доступу: https://arxiv.org/abs/1906.06653 (дата звернення: 08.12.2025).

36. Chevalier R., Cristalli S., Hauser C., [та ін]. BootKeeper: Validating Software Integrity Properties on Boot Firmware Images [Електронний ресурс]. — Режим доступу: https://arxiv.org/abs/1903.12505 (дата звернення: 08.12.2025).

37. Microsoft. Windows 11 Security Book [Електронний ресурс]. — Режим доступу: https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MSFT-Windows11-Security-book_Sept2023.pdf (дата звернення: 08.12.2025).

38. Microsoft. Windows Security: Encryption and Data Protection [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/book/operating-system-security-encryption-and-data-protection (дата звернення: 08.12.2025).

39. Perry D. Applied Cryptography for Secure Storage: BitLocker and TPM in Practice / Apress, 2022.

40. Microsoft. Windows Hardware Security Overview [Електронний ресурс]. — Режим доступу: https://learn.microsoft.com/en-us/windows/security/book/hardware-security (дата звернення: 08.12.2025).

41. Biondi P., Frazier J. Trusted Platform Module 2.0: Security Implementation and Best Practices / CRC Press, 2021.

42. Eisenbarth T., Kumar S., Sunar B. Security Analysis of TPM 2.0 and BitLocker Implementation / Journal of Computer Security, 2020.