КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ
Факультет автоматизації і інформаційних технологій
Кафедра кібербезпеки та комп'ютерної інженерії

Кваліфікаційна робота на тему:

«Інтегрований підхід до захисту та оптимізації Windows»

Студент групи БІКСм-24

Райський А.В.

Керівник:

к.т.н., Делембовський М.М.

2025 рік

Актуальність теми

Операційна система Windows домінує як у корпоративному середовищі, так і серед пересічних користувачів, що робить її ключовим об'єктом інтересу для кіберзлочинців. Щорічно зростає кількість атак, спрямованих саме на Windows-інфраструктури — від фішингу та програм-шифрувальників до експлойтів, що зловживають вразливостями ядра та служб.

Сучасні загрози вимагають **комплексного, інтегрованого підходу**, який поєднує апаратні механізми захисту (TPM, Secure Boot), системні інструменти (BitLocker, контроль служб, політики безпеки) та оптимізацію програмного середовища. Тільки поєднання цих рівнів дозволяє побудувати захищену, продуктивну та надійну Windows-платформу, здатну протистояти актуальним кіберзагрозам.

Інформація з сайту statcounter, на якому визначається популярність різних ОС

Мета та завдання

Метою роботи є формування цілісного підходу до підвищення рівня безпеки та продуктивності операційної системи Windows на основі поєднання апаратних та програмних механізмів.

Для досягнення цієї мети передбачено виконання таких завдань:
- проаналізувати вбудовані засоби захисту Windows (Secure Boot, TPM 2.0, BitLocker, UAC, групові політики);
- визначити ключові вразливості та ризики, характерні для сучасних систем на базі Windows;
- дослідити інструменти оптимізації продуктивності та зменшення навантаження ОС;
- розробити інтегровану модель взаємодії засобів захисту й оптимізації;
- реалізувати практичну апробацію моделі на реальній робочій станції та оцінити її ефективність.

НОВИЗНА

У роботі запропоновано цілісну методику інтегрованого підходу до захисту та оптимізації Windows, яка поєднує апаратні механізми (UEFI, Secure Boot, TPM 2.0), системні засоби безпеки (TPM 2.0, BitLocker) та інструменти оптимізації (служби, телеметрія, WinUtil). Уперше узгоджено й описано єдину модель, що охоплює весь цикл захисту — від моменту завантаження системи до роботи прикладного ПЗ — та дозволяє стандартизувати процеси підвищення безпеки й продуктивності Windows у персональних і корпоративних середовищах.

ПРАКТИЧНА ЦІННІСТЬ

Практична цінність полягає у можливості прямого застосування описаної моделі для налаштування реальних робочих станцій. Виконана конфігурація UEFI, TPM, Secure Boot і BitLocker, а також алгоритм оптимізації Windows можуть бути використані адміністраторами для підвищення стійкості систем до атак і поліпшення продуктивності. Представлені покрокові інструкції, скріншоти та експериментальні результати забезпечують можливість швидкого повторення методики у навчальних, корпоративних або сервісних умовах.

Об’єкт і предмет дослідження

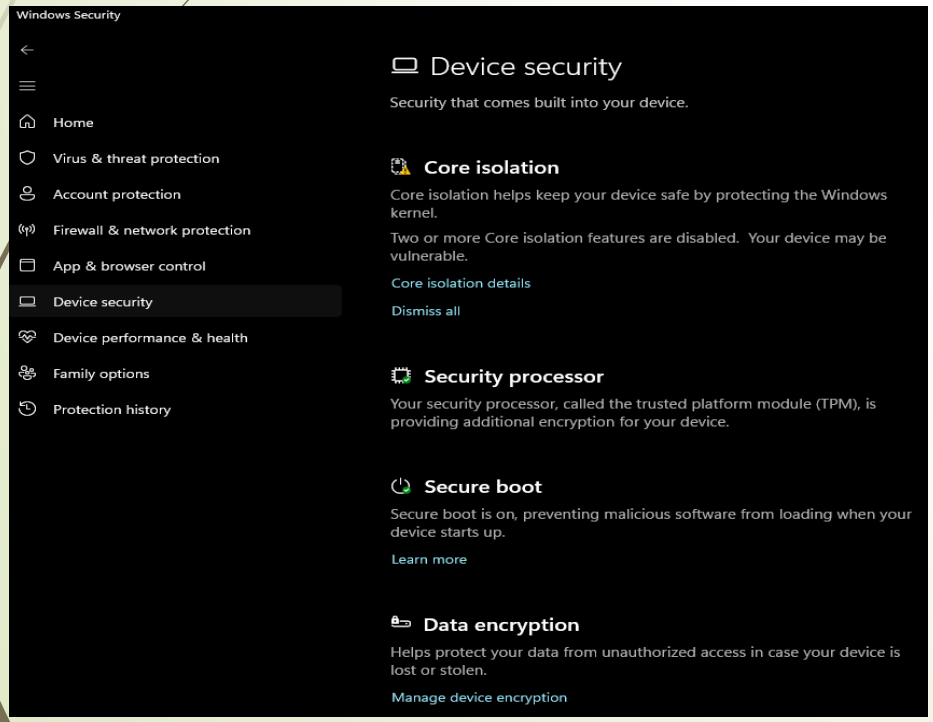
- **Об’єкт:** Інформаційна безпека та продуктивність операційної системи Windows.
- **Предмет:** Методи та засоби апаратного й програмного захисту Windows у поєднанні з оптимізаційними механізмами.

Основні загрози для Windows

- Атаки через завантажувальний ланцюг
- Компрометація облікових даних
- Ransomware
- Експлойти нульового дня
- Соціальна інженерія
- Атаки на протоколи SMB, RDP

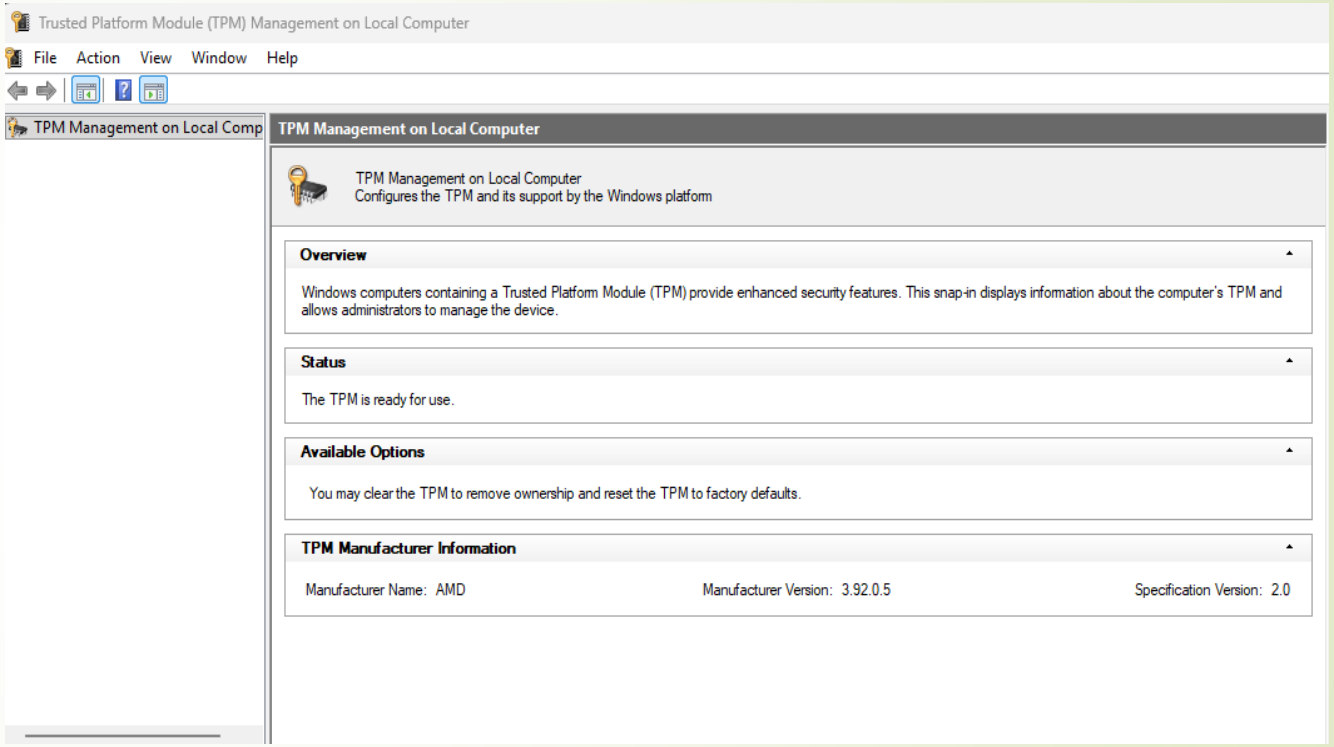
Апаратна безпека: UEFI, Secure Boot

- **Що забезпечують:**
- Захист від модифікації завантажувача
- Верифікація цифрових підписів
- Неможливість запуску непідписаного коду
- Створення кореня довіри для TPM та BitLocker



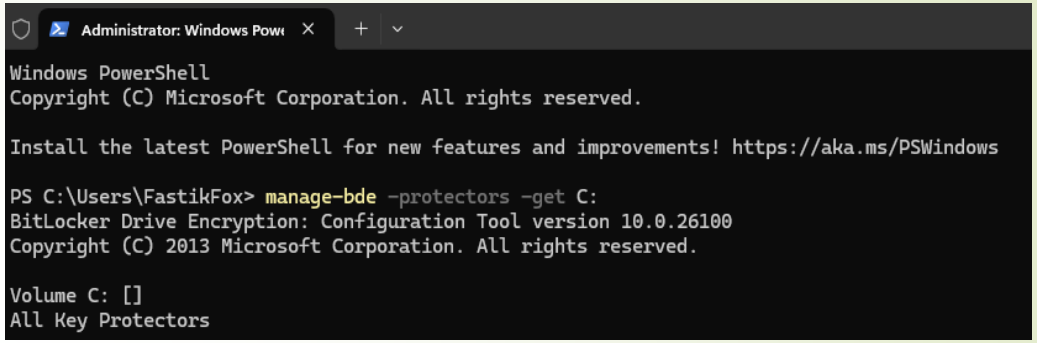
Trusted Platform Module 2.0

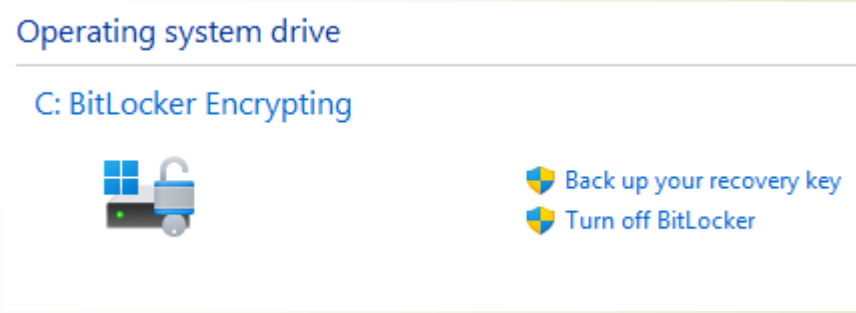
- Апаратний модуль зберігання ключів
- Використовує криптографію RSA/ECC та SHA-256
- Підтримує вимірювання цілісності (PCR)
- Необхідний для BitLocker, Windows Hello



BitLocker

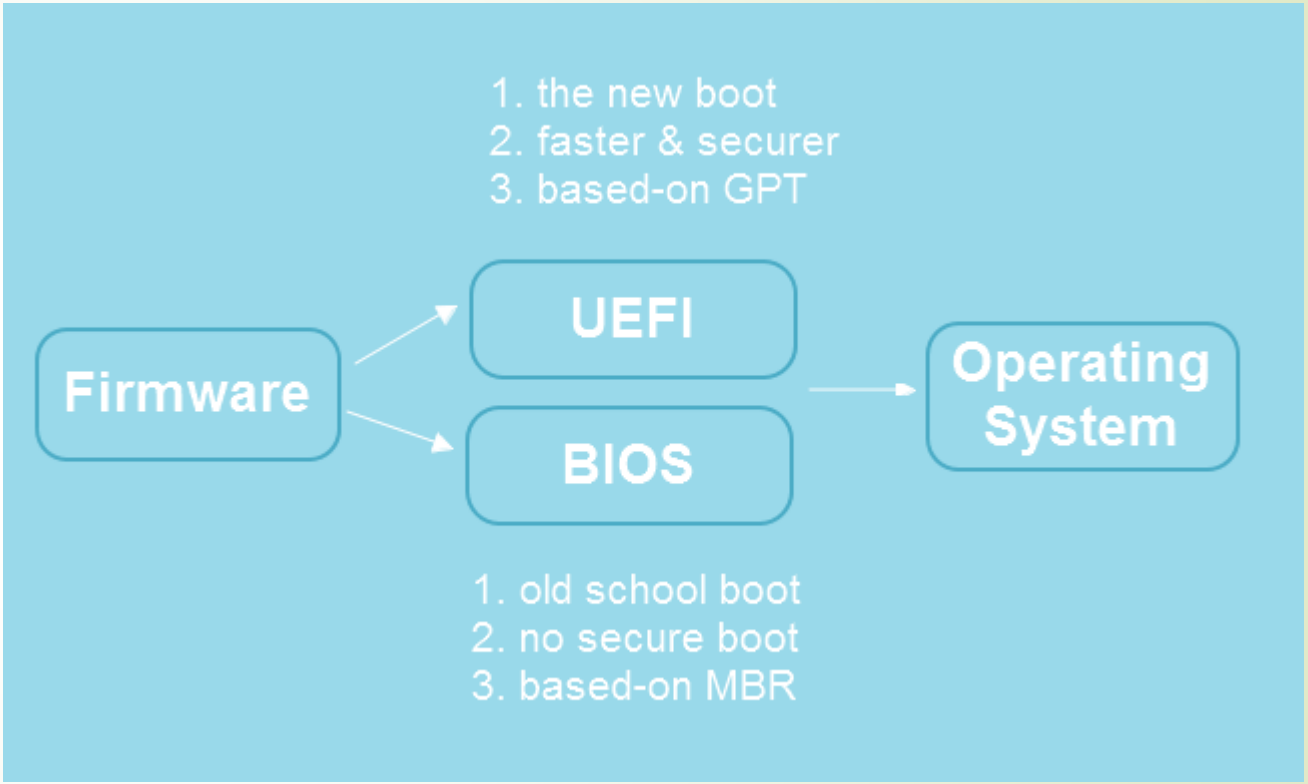
- **Переваги:**
- Автоматичний захист системного диска
- Інтеграція з TPM
- Шифрування XTS-AES
- Захист від викрадення даних
- **Скріншоти:**
- manage-bde -status
- BitLocker Enabled





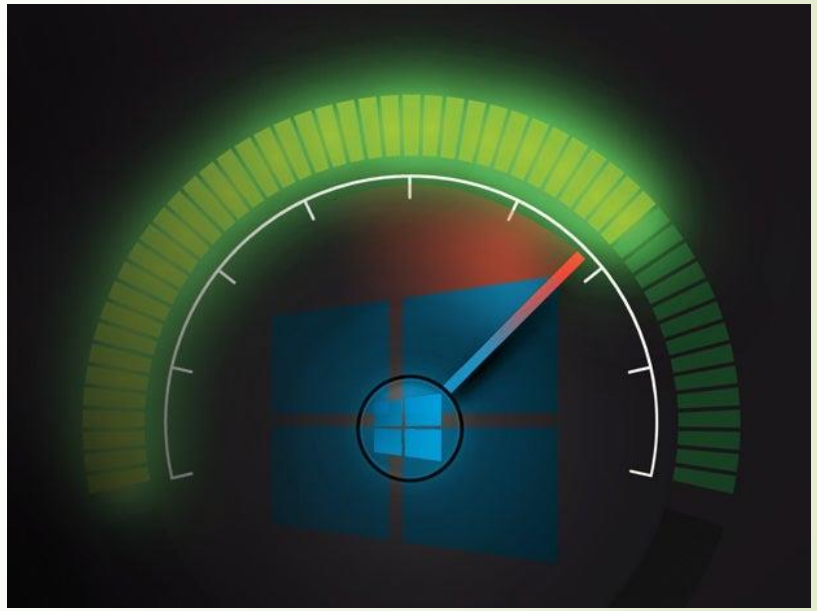
UEFI проти Legacy BIOS

- **UEFI забезпечує:**
- більшу безпеку;
- підтримку Secure Boot;
- кращу структуризацію завантаження;
- необхідність для Windows 11.



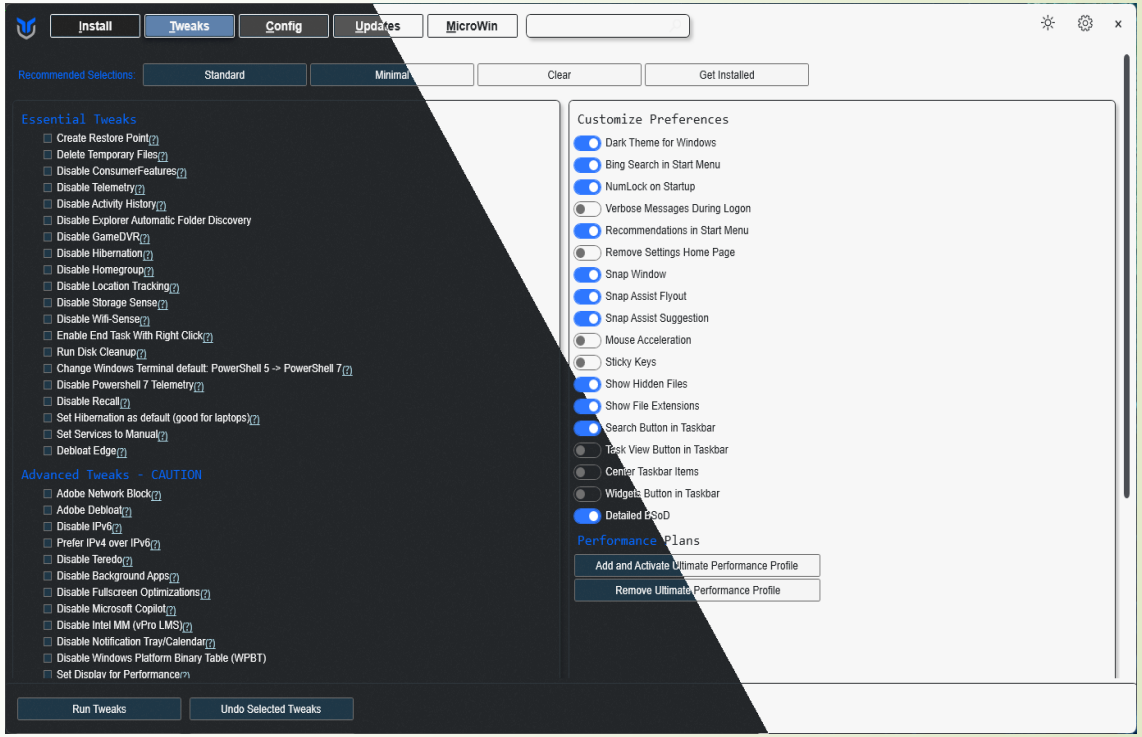
Оптимізація ОС Windows

- Розглядається:
- Відключення непотрібних служб
- Керування автозавантаженням
- Оптимізація телеметрії
- Очищення системи
- Вимкнення непотрібних компонентів Windows Feature Set

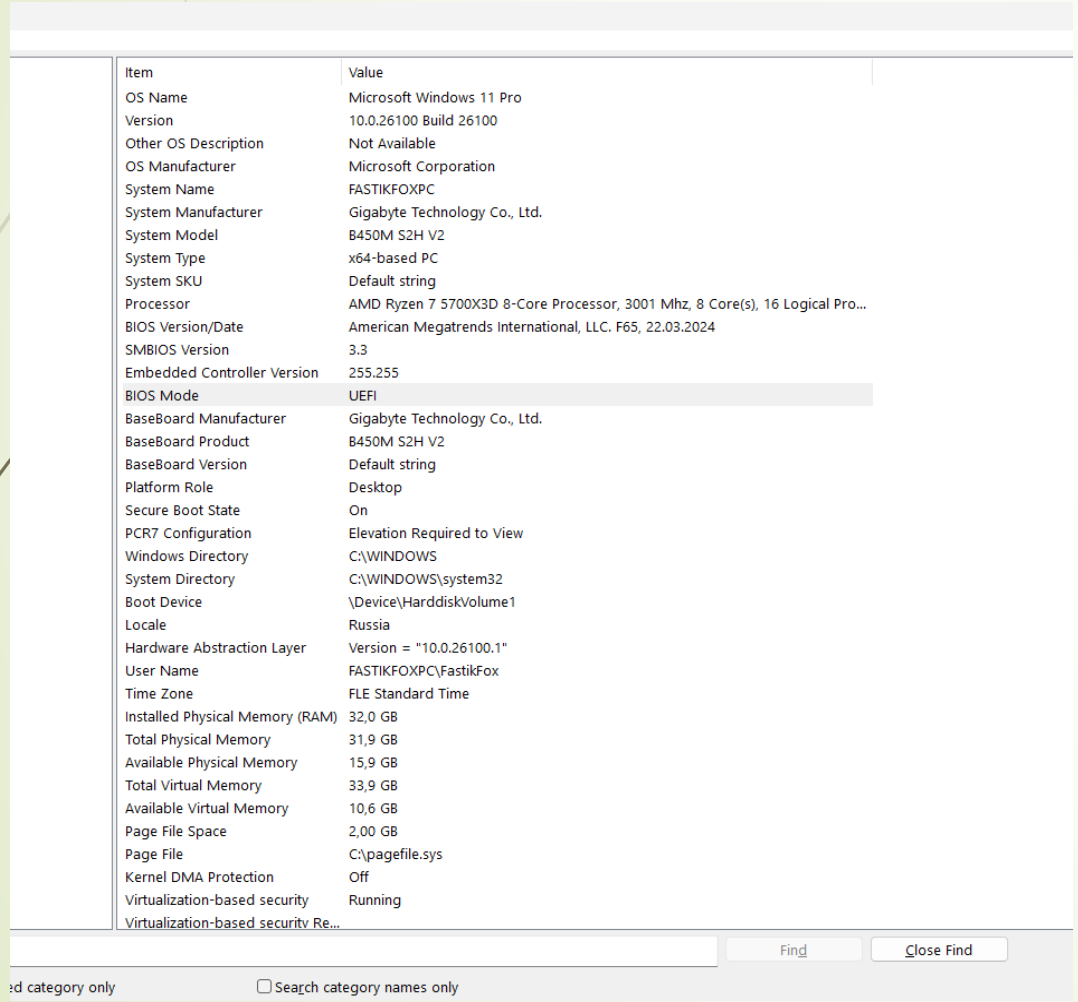


WinUtil як інструмент оптимізації Windows

- WinUtil дозволяє:
- Повну автоматизацію оптимізації
- Вимкнення телеметрії
- Очищення тимчасових файлів
- Оптимізацію служб
- Встановлення корисного ПЗ
- Усунення зайвих компонентів



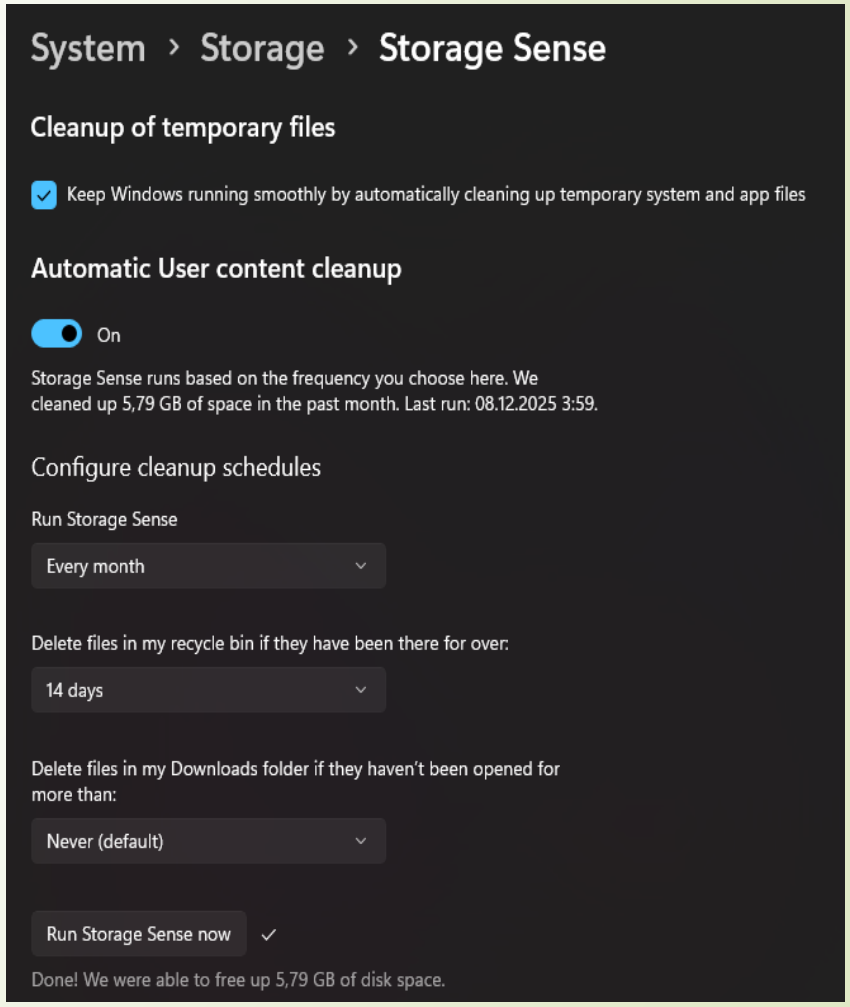
Практична частина: Підготовка системи



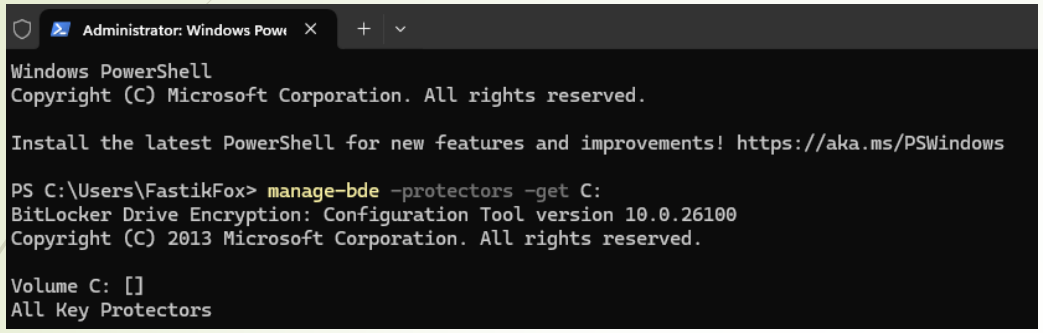
Item	Value
OS Name	Microsoft Windows 11 Pro
Version	10.0.26100 Build 26100
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	FASTIKFOXPC
System Manufacturer	Gigabyte Technology Co., Ltd.
System Model	B450M S2H V2
System Type	x64-based PC
System SKU	Default string
Processor	AMD Ryzen 7 5700X3D 8-Core Processor, 3001 Mhz, 8 Core(s), 16 Logical Pro...
BIOS Version/Date	American Megatrends International, LLC. F65, 22.03.2024
SMBIOS Version	3.3
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	Gigabyte Technology Co., Ltd.
BaseBoard Product	B450M S2H V2
BaseBoard Version	Default string
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	Russia
Hardware Abstraction Layer	Version = "10.0.26100.1"
User Name	FASTIKFOXPC\FastikFox
Time Zone	FLE Standard Time
Installed Physical Memory (RAM)	32,0 GB
Total Physical Memory	31,9 GB
Available Physical Memory	15,9 GB
Total Virtual Memory	33,9 GB
Available Virtual Memory	10,6 GB
Page File Space	2,00 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Running
Virtualization-based security Re...	

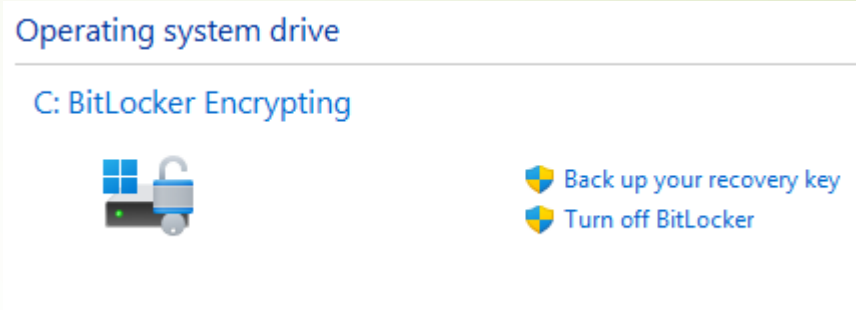
Find Close Find

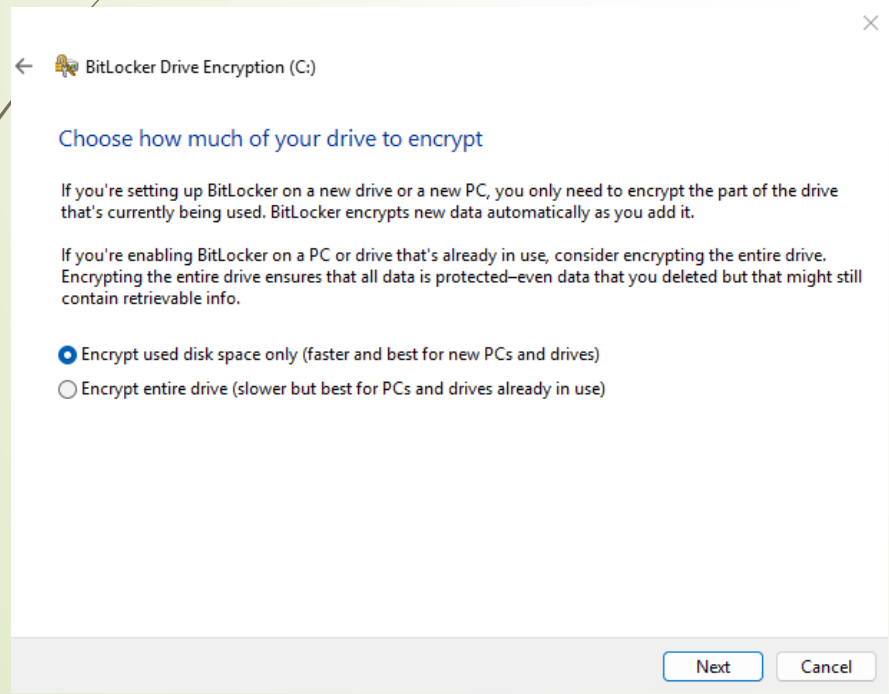
ed category only Search category names only

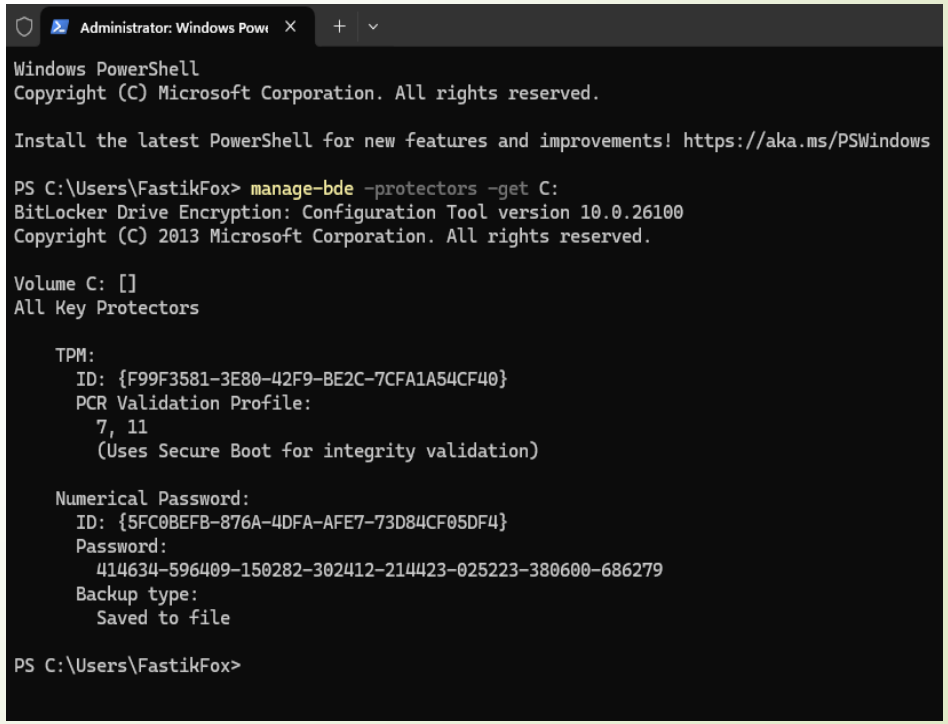


Практична частина: BitLocker

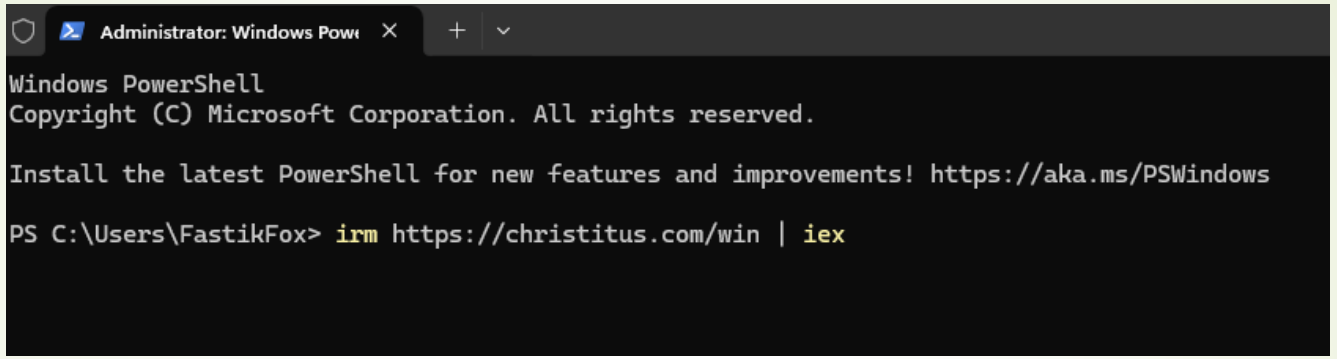


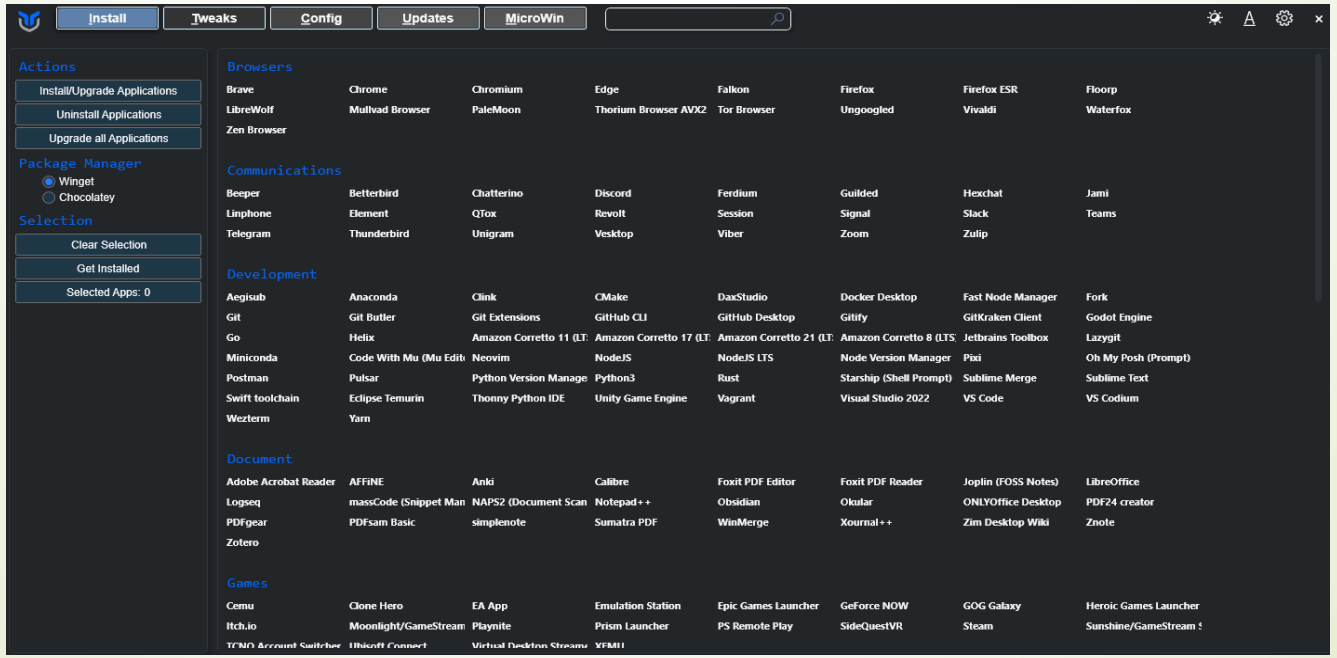






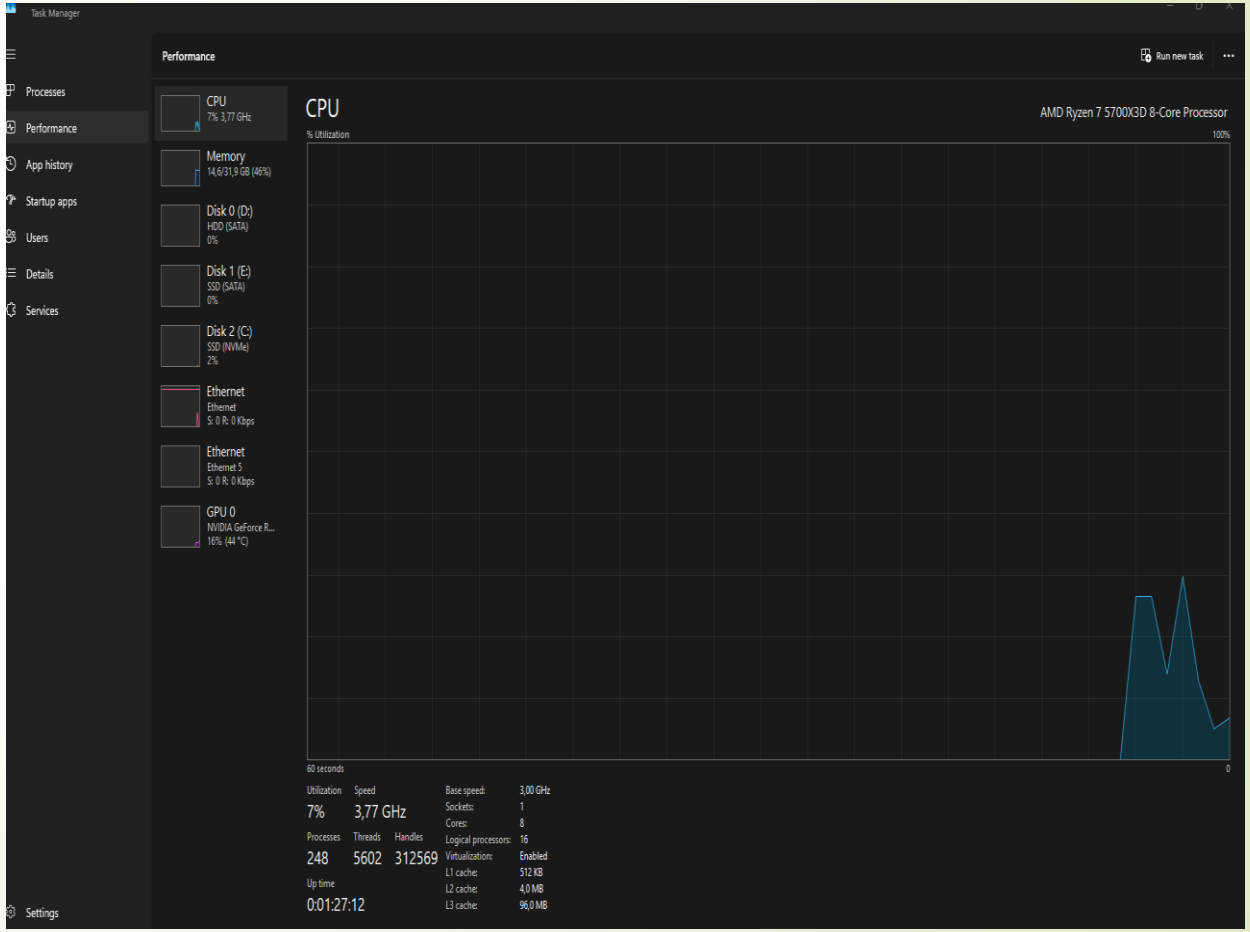
Практична частина: WinUtil





Результати практичної частини

- Результати впровадження:
- Підвищення стабільності
- Зменшення фонових процесів
- Зростання продуктивності
- Максимальний рівень апаратного захисту
- Зменшення ризику компрометації системи



Висновки та перспективи розвитку

Основні результати роботи:

- Проаналізовано структуру безпеки Windows
- Досліджено можливості TPM, Secure Boot, BitLocker
- Розроблено інтегровану модель захисту
- Проведено оптимізацію ОС у практичному середовищі
- Підтверджено ефективність моделі тестуванням

Перспективи розвитку:

- Використання Defender Application Control
- Впровадження Zero Trust моделі
- Автоматизація застосованих налаштувань через PowerShell-скрипти
- Інтеграція з Active Directory

Інформація щодо публікацій

- **III МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ “НОВІТНІ ТЕХНОЛОГІЧНІ ТЕНДЕНЦІЇ СМАРТ ІНДУСТРІЇ ТА ІНТЕРНЕТУ РЕЧЕЙ”**
- АНАЛІЗ ТЕХНОЛОГІЙ ДИСТАНЦІЙОГО КЕРУВАННЯ ЖИВЛЕННЯМ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ (сторінка 100)

Експериментальна база та джерела практичної реалізації

Практична частина роботи базується на аналізі офіційної технічної документації, наукових публікацій та галузевих рекомендацій щодо безпеки Windows.

У процесі реалізації використано:

- офіційну документацію Microsoft щодо Secure Boot, TPM 2.0 та BitLocker;
- рекомендації NIST (SP 800-53, SP 800-171) щодо захисту інформаційних систем;
- матеріали CIS Benchmarks для Windows;
- аналітичні звіти щодо загроз Windows-платформ;
- експериментальну перевірку налаштувань на реальній робочій станції з фіксацією результатів (скріншоти, команди PowerShell).

Microsoft Learn – learn.microsoft.com
NIST Cybersecurity Framework – nist.gov
CIS Benchmarks – cisecurity.org

Дякую за увагу!