

**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

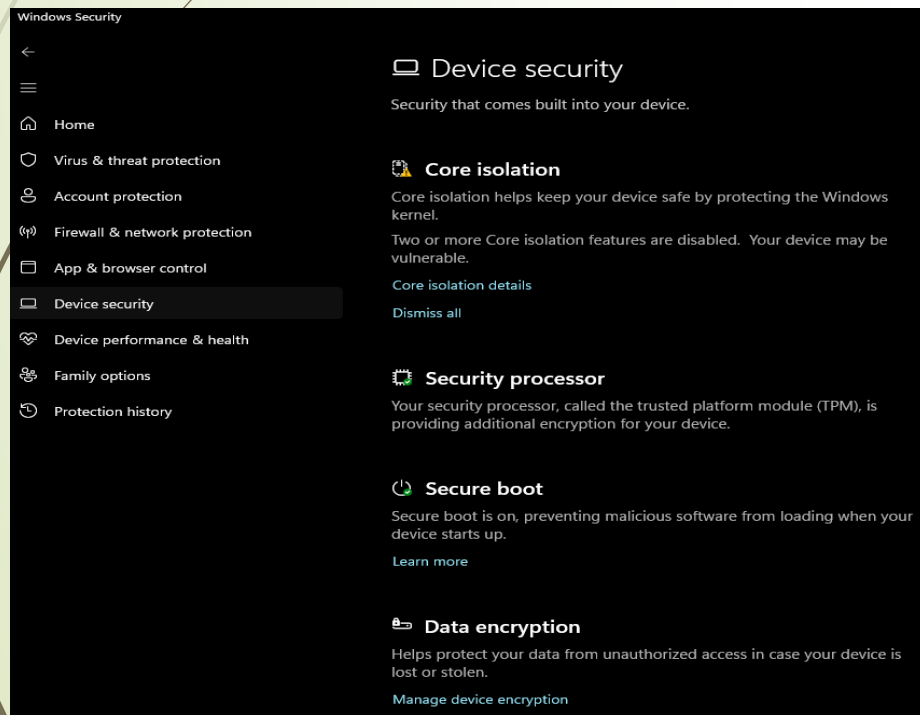
- Атаки через завантажувальний ланцюг
- Компрометація облікових даних
- Ransomware
- Експлойти нульового дня
- Соціальна інженерія
- Атаки на протоколи SMB, RDP



Апаратна безпека: UEFI, Secure Boot

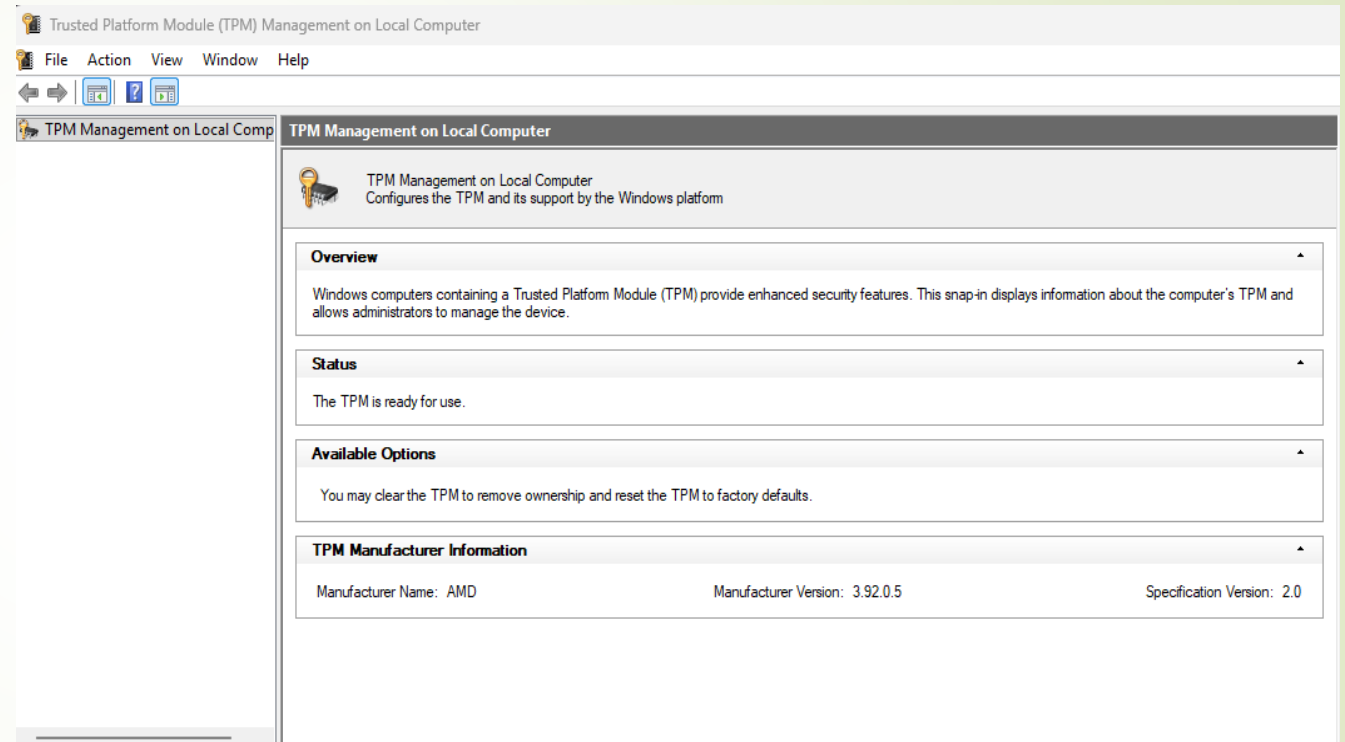
► Що забезпечують:

- 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

```
Administrator: Windows Powe... x + v
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\FastikFox> manage-bde -protectors -get C:
BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: [ ]
All Key Protectors
```

Operating system drive

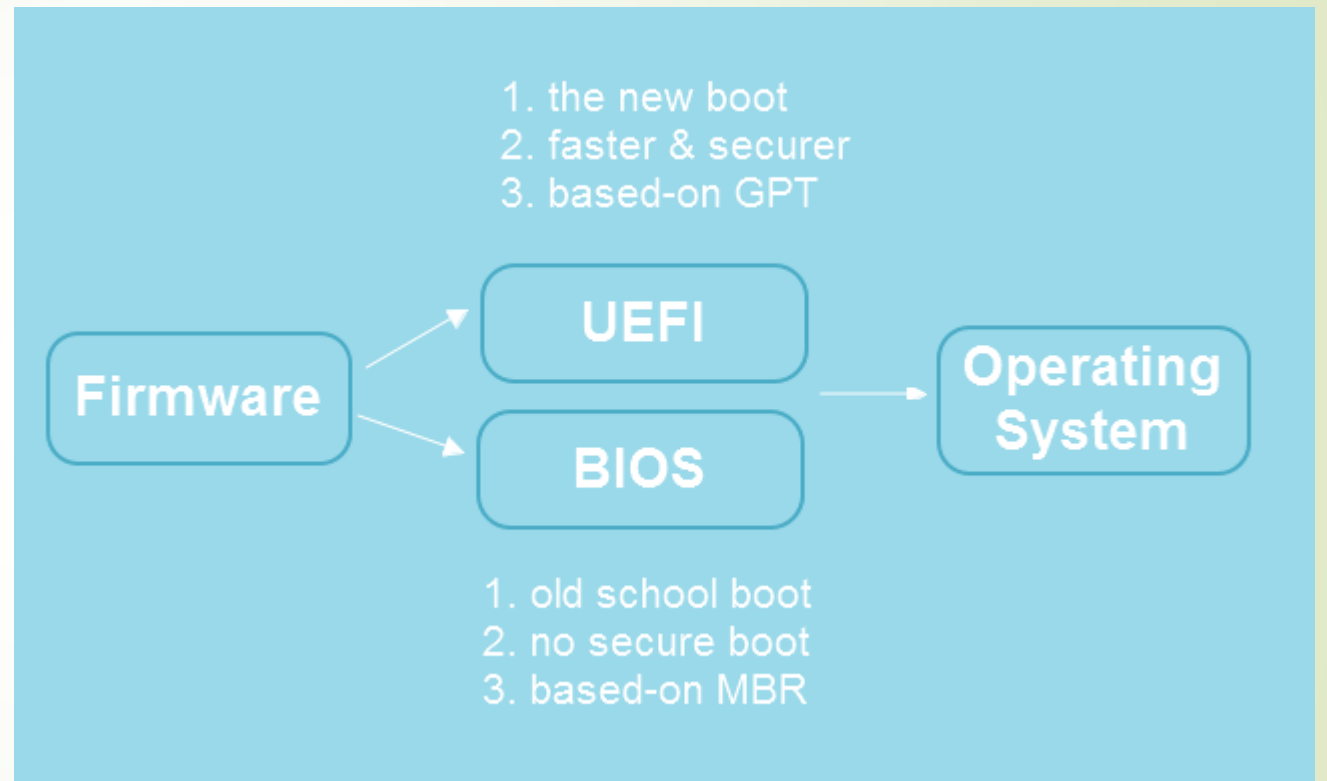
C: BitLocker Encrypting



- [Back up your recovery key](#)
- [Turn off BitLocker](#)

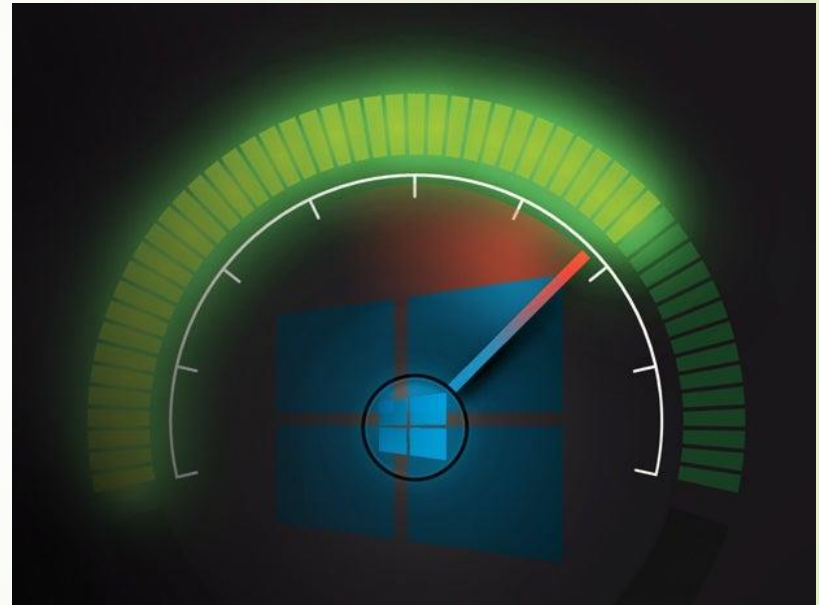
UEFI проти Legacy BIOS

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



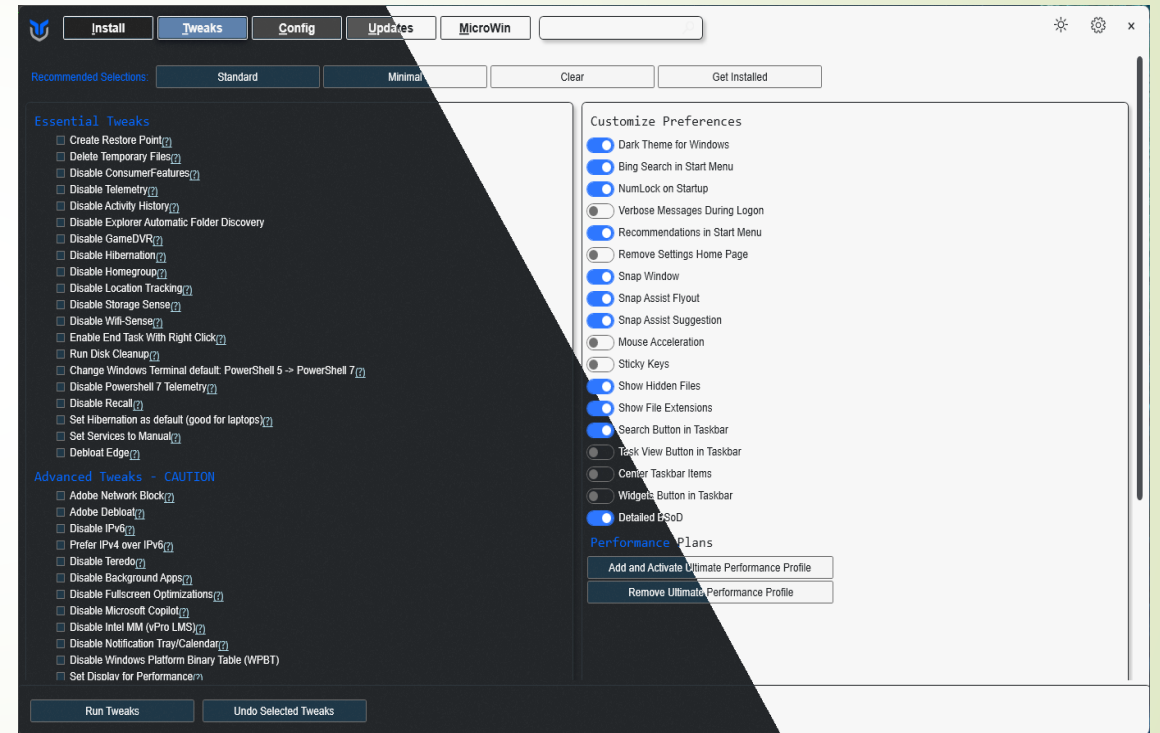
Оптимізація ОС Windows

- 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...	

ed category only Search category names only

System > Storage > Storage Sense

Cleanup of temporary files

Keep Windows running smoothly by automatically cleaning up temporary system and app files

Automatic User content cleanup

On

Storage Sense runs based on the frequency you choose here. We cleaned up 5,79 GB of space in the past month. Last run: 08.12.2025 3:59.

Configure cleanup schedules

Run Storage Sense

Every month

Delete files in my recycle bin if they have been there for over:

14 days

Delete files in my Downloads folder if they haven't been opened for more than:

Never (default)

Run Storage Sense now ✓

Done! We were able to free up 5,79 GB of disk space.

Практична частина: BitLocker

```
Administrator: Windows Powe x + v
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows


PS C:\Users\FastikFox> manage-bde -protectors -get C:
BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: [ ]
All Key Protectors
```

Operating system drive

C: BitLocker Encrypting



 Back up your recovery key

 Turn off BitLocker

← BitLocker Drive Encryption (C:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might still contain retrievable info.

Encrypt used disk space only (faster and best for new PCs and drives)

Encrypt entire drive (slower but best for PCs and drives already in use)

Next Cancel

```
Administrator: Windows Powe x + v
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\FastikFox> manage-bde -protectors -get C:
BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: [ ]
All Key Protectors

TPM:
ID: {F99F3581-3E80-42F9-BE2C-7CFA1A54CF40}
PCR Validation Profile:
7, 11
(Uses Secure Boot for integrity validation)

Numerical Password:
ID: {5FC0BEFB-876A-4DFA-AFE7-73D84CF05DF4}
Password:
414634-596409-150282-302412-214423-025223-380600-686279
Backup type:
Saved to file

PS C:\Users\FastikFox>
```

Практична частина: WinUtil

```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

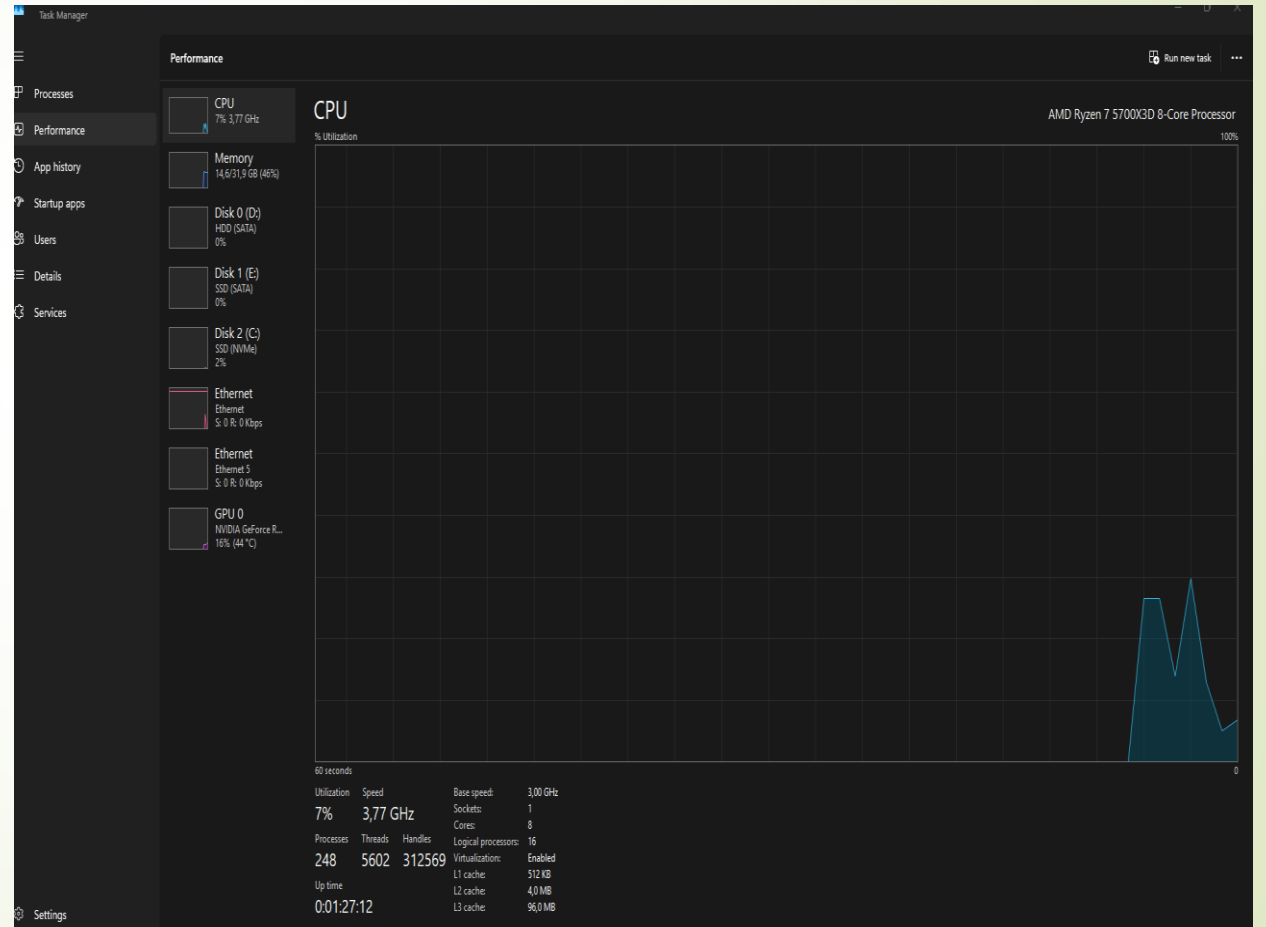
PS C:\Users\FastikFox> irm https://christitus.com/win | iex
```

The screenshot shows the WinUtil application interface with a dark theme. The top navigation bar includes tabs for 'Install', 'Tweaks', 'Config', 'Updates', and 'MicroWin'. The main content area is organized into several categories:

- Actions:** Install/Upgrade Applications, Uninstall Applications, Upgrade all Applications.
- Package Manager:** Winget (selected), Chocolatey.
- Selection:** Clear Selection, Get Installed, Selected Apps: 0.
- Browsers:** Brave, Chrome, Chromium, Edge, Falkon, Firefox, Firefox ESR, Floorp, LibreWolf, Mullvad Browser, PaleMoon, Thorium Browser AVX2, Tor Browser, Ungoogled, Vivaldi, Waterfox, Zen Browser.
- Communications:** Beeper, Betterbird, Chatterino, Discord, Ferdium, Guilded, Hexchat, Jami, Linphone, Element, QTox, Revolt, Session, Signal, Slack, Teams, Telegram, Thunderbird, Unigram, Vesktop, Viber, Zoom, Zulip.
- Development:** Aegisub, Anaconda, Clink, CMake, DaxStudio, Docker Desktop, Fast Node Manager, Fork, Git, Git Butler, Git Extensions, GitHub CLI, GitHub Desktop, Gitify, GitKraken Client, Godot Engine, Go, Helix, Amazon Corretto 11 (LT), Amazon Corretto 17 (LT), Amazon Corretto 21 (LT), Amazon Corretto 8 (LTS), JetBrains Toolbox, Lazygit, Miniconda, Code With Mu (Mu Editor), Neovim, NodeJS, NodeJS LTS, Node Version Manager, Pixa, Oh My Posh (Prompt), Postman, Pulsar, Python Version Manager, Python3, Rust, Starship (Shell Prompt), Sublime Merge, Sublime Text, Swift toolchain, Eclipse Temurin, Thonny Python IDE, Unity Game Engine, Vagrant, Visual Studio 2022, VS Code, VS Codium, Wezterm, Yarn.
- Document:** Adobe Acrobat Reader, AFFINE, Anki, Calibre, Foxit PDF Editor, Foxit PDF Reader, Joplin (FOSS Notes), LibreOffice, Logseq, massCode (Snippet Manager), NAPS2 (Document Scanner), Notepad++, Obsidian, ONLYOffice Desktop, PDF24 creator, PDFgear, PDFsam Basic, simplenote, Sumatra PDF, WinMerge, Xournal++, Zim Desktop Wiki, Znote, Zotero.
- Games:** Cemu, Clone Hero, EA App, Emulation Station, Epic Games Launcher, GeForce NOW, GOG Galaxy, Heroic Games Launcher, Itch.io, Moonlight/GameStream, Playnite, Prism Launcher, PS Remote Play, SideQuestVR, Steam, Sunshine/GameStream, TFCM Account Switcher, Ubisoft Connect, Virtual Desktop Streamer, YFM1.

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!