МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет ім. В. Н. Каразіна

Факультет: **ННІ Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **122 Комп'ютерні науки**
Освітня програма: **Комп'ютерні науки та інформаційні технології в бізнесі**

Група: АК-21М **денна форма навчання**

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«ДОСЛІДЖЕННЯ ДЕСКТОПНИХ ОПЕРАЦІЙНИХ СИСТЕМ В АСПЕКТІ СИСТЕМНОГО АДМІНІСТРУВАННЯ З УРАХУВАННЯМ БЕЗПЕКИ»
ЗА НАКАЗОМ № 4601-5/3045 ВІД 25 ВЕРЕСНЯ 2024 РОКУ

здобувача вищої освіти **Пожарова Артема Георгійовича**

Робота допущена до захисту в ЕК

протокол кафедри ІТММ №4 від 30.11.2024

Завідувач кафедри ІТММ

к. п. н., доцент

_____**Н. І. Стяглик**

Науковий керівник

к. ф.- м. н., доцент

_____**Н. М. Чеканова**

м. Харків 2024 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут "Каразінський банківський інститут"
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти другий (магістерський)
Спеціальність 122 Комп'ютерні науки
Освітня програма Комп'ютерні науки

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ **Н. І. Стяглик**
Підпис ініціали прізвище

"25" вересня 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Пожарова Артема Георгійовича
(прізвище, ім'я, по батькові студента)

1. Тема роботи «Дослідження десктопних операційних систем в аспекті системного адміністрування з урахуванням безпеки»

Керівник роботи к. ф.-м. н., доцент Н. М. Чеканова

затверджено наказом по університету від "25" вересня 2024 року № 4601-5/3045

2. Строк подання студентом роботи 20 листопада 2024 року

3. Перелік питань, які потрібно розробити:
У розділі 1: Вибір операційних систем для порівняння. Провести класифікацію основних десктопних операційних систем (Chrome OS, macOS, Windows, Ubuntu). Оцінити ліцензії, ядро, інтерфейс, модель оновлення, призначення, ринкову частку. Аргументувати вибір операційних систем, які охоплюють різні типи ліцензування, безпеки, і цільових ринків.
У розділі 2: Порівняння захисту операційних систем від дій користувача. Дослідити архітектуру безпеки для Chrome OS, Windows, macOS, і Ubuntu. Оцінити методи захисту даних (наприклад, шифрування, захист від несанкціонованого доступу) та функціональність для забезпечення цілісності системи. Проаналізувати підходи до віртуалізації та контейнеризації

(наприклад, в Chrome OS) для ізоляції процесів і захисту даних.
У розділі 3: Продуктивність операційних систем. Провести тестування продуктивності ОС (Geekbench) для порівняння обчислювальних і графічних можливостей. Визначити методологію та параметри тестування. Зробити висновки щодо ефективності використання кожної ОС для різних обчислювальних завдань у корпоративному середовищі.
У розділі 4: Інтеграція операційних систем з корпоративним ПЗ Microsoft. Дослідити можливості інтеграції ОС із доменними технологіями (Active Directory, Entra ID). Проаналізувати сумісність з Microsoft 365, Adobe Creative Cloud та іншими корпоративними сервісами. Визначити особливості інтеграції кожної ОС з управлінськими і виробничими інструментами.
У розділі 5: Прогнозування майбутнього розвитку операційних систем. Дослідити майбутні тенденції та перспективи розвитку ОС з огляду на сучасні технічні вимоги. Проаналізувати стратегічні напрями кожної ОС (вплив хмарних технологій, штучного інтелекту, інтеграція із новими платформами). Сформулювати прогноз щодо найбільш перспективних ОС для різних галузей.
У розділі 6: Рекомендації щодо вибору ОС для корпоративних потреб. Визначити критерії вибору ОС залежно від специфіки діяльності організації. Розробити рекомендації для різних типів організацій з урахуванням аспектів безпеки, продуктивності, вартості. Сформулювати практичні поради щодо оптимізації корпоративної інфраструктури на базі обраних ОС.

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір теми дослідження.
2	Затвердження плану дослідження на кафедрі.
3	Проведення огляду літератури щодо десктопних операційних систем.
4	Вибір операційних систем для порівняння та обґрунтування вибору.
5	Дослідження аспектів безпеки обраних операційних систем.
6	Проведення тестування продуктивності ОС за допомогою Geekbench.
7	Аналіз результатів тестування та оцінка продуктивності для різних завдань.
8	Вивчення інтеграції ОС з корпоративним ПЗ Microsoft.
9	Прогнозування майбутніх тенденцій розвитку ОС.
10	Формулювання рекомендацій для корпоративного вибору ОС.
11	Підготовка та оформлення результатів дослідження.
12	Подання роботи на затвердження науковому керівнику.
13	Здача роботи на кафедру для допуску до захисту.
14	Захист кваліфікаційної магістерської роботи.

5. Дата видачі завдання 25 вересня 2024 року

Студент _____ А. Г. Пожаров
підпис ініціали, прізвище

Керівник роботи _____ Н. М. Чеканова
підпис ініціали, прізвище

РЕФЕРАТ
НА КВАЛІФІКАЦІЙНУ МАГІСТЕРСЬКУ РОБОТУ
«ДОСЛІДЖЕННЯ ДЕСКТОПНИХ ОПЕРАЦІЙНИХ СИСТЕМ В АСПЕКТІ СИСТЕМНОГО АДМІНІСТРУВАННЯ З УРАХУВАННЯМ БЕЗПЕКИ»
ПОЖАРОВА АРТЕМА ГЕОРГІЙОВИЧА

Кваліфікаційна магістерська робота містить 135 сторінки, 6 таблиць, список літератури з 47 найменувань.

Об2єктом дослідження є десктопні операційні системи (Chrome OS, macOS, Windows, Ubuntu), їх характеристики, особливості використання та інтеграції в корпоративному середовищі.

Предметом дослідження є порівняльний аналіз безпеки, продуктивності, та сумісності зазначених операційних систем у контексті системного адміністрування.

Мета кваліфікаційної магістерської роботи полягає у порівнянні особливостей захисту, продуктивності та зручності інтеграції операційних систем для подальшого вибору оптимальної ОС для корпоративного середовища.

Завданнями кваліфікаційної магістерської роботи є: Аналіз десктопних операційних систем у контексті їхньої безпеки та продуктивності. Оцінка систем безпеки, вбудованих механізмів захисту та методів шифрування у кожній з ОС. Порівняння продуктивності операційних систем на однаковому апаратному забезпеченні. Вивчення інтеграції з корпоративним ПЗ Microsoft (Active Directory, Microsoft Entra ID, Microsoft Intune тощо). Формулювання рекомендацій щодо вибору ОС для різних типів корпоративних середовищ.

Актуальність дослідження: питання вибору операційної системи набуває особливого значення в умовах зростання кіберзагроз і посилення вимог до захищеності даних. Розвиток корпоративних мереж потребує ефективних рішень з інтеграції ОС, які б забезпечили не тільки зручність адміністрування, а й безпеку та продуктивність для широкого спектру завдань.

За результатами дослідження: проведено аналіз чотирьох популярних операційних систем, оцінено їх переваги та недоліки у таких сферах: захист від дій користувачів, архітектура безпеки, можливості віртуалізації, продуктивність. Визначено переваги Chrome OS для середовищ з мінімальним втручанням користувача, переваги Windows у сфері інтеграції з корпоративними мережами, високий рівень безпеки macOS і гнучкість Ubuntu.

Практична новизна: розроблено рекомендації щодо вибору ОС для корпоративного середовища, що враховують безпеку, продуктивність та можливості інтеграції з корпоративним програмним забезпеченням. Результати можуть бути корисними для підприємств та організацій, які

мають високі вимоги до безпеки та продуктивності своїх систем.

Одержані результати можуть бути використані при виборі операційної системи для корпоративних середовищ, розробці політики безпеки та оптимізації адміністрування систем, враховуючи специфіку роботи та необхідний рівень захисту даних.

КЛЮЧОВІ СЛОВА: ОПЕРАЦІЙНА СИСТЕМА, БЕЗПЕКА, ПРОДУКТИВНІСТЬ, ІНТЕГРАЦІЯ, АДМІНІСТРУВАННЯ, CHROME OS, WINDOWS, MACOS, UBUNTU.

ABSTRACT
AT QUALIFICATION MASTER'S THESIS
«RESEARCH OF DESKTOP OPERATING SYSTEMS IN THE CONTEXT OF SYSTEM ADMINISTRATION WITH A FOCUS ON SECURITY»
ARTEM POZHAROV

The master's thesis contains 135 pages, 6 tables, and a list of references of 47 titles.

The object of the research is desktop operating systems (Chrome OS, macOS, Windows, Ubuntu), their characteristics, and the specifics of use and integration in a corporate environment.

The subject of the research is the comparative analysis of the security, performance, and compatibility of the specified operating systems within the context of system administration.

The purpose of this master's thesis is to compare the features of protection, performance, and ease of integration of operating systems to recommend the optimal OS for corporate use.

The tasks of the master's thesis are: Analyzing desktop operating systems in terms of security and performance. Assessing security systems, embedded security mechanisms, and encryption methods for each OS. Comparing OS performance on identical hardware. Studying integration with corporate Microsoft software (Active Directory, Microsoft Entra ID, Microsoft Intune, etc.). Formulating recommendations for OS selection across various types of corporate environments.

Relevance of the study: Choosing the right operating system is critical in an era of escalating cyber threats and heightened data security requirements. The development of corporate networks requires effective OS integration solutions that ensure not only ease of administration but also robust security and performance for a wide range of tasks.

According to the results of the research, an analysis of four popular operating systems was conducted, assessing their advantages and disadvantages in areas such as protection from user actions, security architecture, virtualization capabilities, and performance. The advantages of Chrome OS for environments requiring minimal user intervention, Windows for its integration with corporate networks, macOS for its high-security level, and Ubuntu for its flexibility were highlighted.

Practical novelty: Recommendations were developed for selecting an OS in a corporate environment, considering security, performance, and integration capabilities with corporate software. These results can be valuable for enterprises and organizations with high requirements for system security and performance.

The results obtained can be used when selecting an operating system for corporate environments, developing security policies, and optimizing system administration based on the specifics of each workplace and the required level of data protection.

KEYWORDS: OPERATING SYSTEM, SECURITY, PERFORMANCE, INTEGRATION, ADMINISTRATION, CHROME OS, WINDOWS, MACOS, UBUNTU.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ І ТЕРМІНІВ

ПЗ – програмне забезпечення

SAML (Security Assertion Markup Language) – XML-протокол для передачі аутентифікації.

SLA (Service Level Agreement) – угода між клієнтом і постачальником про рівень обслуговування.

GNU (GNU's Not Unix) – проект вільного ПЗ, основа для GNU/Linux.

PWA (Progressive Web Application) – веб-додаток з властивостями мобільних додатків.

DEP (Data Execution Prevention) – технологія захисту від небезпечного коду.

EFS (Encrypting File System) – шифрування файлів у Windows.

NTFS (New Technology File System) – файлова система Windows з журналюванням.

HKLM (HKEY_LOCAL_MACHINE) – реєстр Windows для системних налаштувань.

HKCU (HKEY_CURRENT_USER) – реєстр Windows для налаштувань користувача.

HKCR (HKEY_CLASSES_ROOT) – реєстр для асоціацій файлів у Windows.

HKU (HKEY_USERS) – реєстр для даних усіх користувачів.

HKCC (HKEY_CURRENT_CONFIG) – реєстр для поточного обладнання.

LDAP (Lightweight Directory Access Protocol) – протокол доступу до каталогів.

WSUS (Windows Server Update Services) – управління оновленнями Microsoft.

SCCM (System Center Configuration Manager) – управління IT-інфраструктурою.

LKM (Loadable Kernel Module) – модуль для розширення ядра Linux.

OS (Operating System) – операційна система.

GUI (Graphical User Interface) – графічний інтерфейс користувача.

LTS (Long Term Support) – довгострокова підтримка.

KVM (Kernel-based Virtual Machine) – віртуалізація на основі ядра.

MDM (Mobile Device Management) – управління мобільними пристроями.

SCCM (System Center Configuration Manager) – конфігураційне управління.

XNU (X is Not Unix) – ядро macOS.

RAM (Random Access Memory) – оперативна пам'ять.

SSD (Solid State Drive) – твердотільний накопичувач.

LTC (Long Term Candidate) – кандидат на довгострокову підтримку.

GPU (Graphics Processing Unit) – графічний процесор.

CPU (Central Processing Unit) – центральний процесор.

Vulkan – кросплатформний графічний API для високої продуктивності.

OpenCL – стандарт для паралельного програмування.

Metal – високопродуктивний графічний API Apple.

Touch Bar – сенсорна панель для керування на MacBook Pro.

Touchpad – сенсорна панель для навігації на ноутбуках.

Boot Camp – утиліта для встановлення Windows на Mac з Intel.

ВСТУП

Системне адміністрування операційних систем є важливою складовою забезпечення стабільної роботи корпоративної інфраструктури, особливо в умовах зростання цифровізації. Вибір операційної системи для робочих станцій впливає на безпеку, продуктивність, сумісність з корпоративним програмним забезпеченням, а також на зручність адміністрування та масштабованість інфраструктури.

Метою цієї роботи є порівняння чотирьох настільних операційних систем – Chrome OS, macOS, Windows та Ubuntu – з точки зору їхньої придатності для корпоративного середовища. Це дослідження охоплює такі критерії, як захист від некоректних дій користувачів, інтеграція з популярними корпоративними програмами (наприклад, Microsoft 365, PowerShell, Intune та Adobe Creative Cloud), а також сумісність з локальною інфраструктурою (Active Directory, Filewave). Крім того, ми оцінимо аспекти зручності використання, досліджуючи, як дизайн та інтерфейс кожної операційної системи впливають на продуктивність і задоволеність користувачів, що є важливими для мінімізації потреби в навчанні та зниження витрат на підтримку в корпоративних умовах.

Робота також охоплює тестування продуктивності обраних операційних систем на однаковому апаратному забезпеченні за допомогою тесту Geekbench. За результатами дослідження буде сформовано рекомендації щодо використання кожної з операційних систем у різних типах організацій з урахуванням їх потреб та вимог до безпеки.

Основна увага приділена дослідженню аспектів, що забезпечують безпеку корпоративних даних, мінімізацію ризиків від некоректних дій користувачів та захист від зовнішніх загроз. Це дозволить визначити найбільш підходящу операційну систему для різних корпоративних середовищ, зокрема для компаній з високими вимогами до інформаційної безпеки, сумісності з існуючою інфраструктурою та підтримки віддаленої

роботи.

РОЗДІЛ 1
ВИБІР ОС ДЛЯ ПОРІВНЯННЯ

1.1.Класифікація

Операційні системи можна класифікувати за різними параметрами, які визначають їхні характеристики та можливості використання:

Ліцензія: визначає, як поширюється і використовується ОС.

– Пропрієтарні ОС – розроблені конкретною компанією з обмеженнями на використання і модифікацію (наприклад, Windows, macOS);

– Вільні ОС – надають доступ до вихідного коду, дозволяючи змінювати і поширювати систему (наприклад, Ubuntu);

– Змішані ОС – поєднують елементи пропрієтарного та вільного коду (наприклад, Chrome OS).

Тип ядра: основний компонент ОС, який керує апаратними ресурсами і забезпечує роботу програм.

– Монолітні ядра – об'єднують всі функції в одному модулі, забезпечуючи високу продуктивність, але менш гнучкі (наприклад, Linux);

– Гібридні ядра – поєднують елементи монолітних і мікроядер для досягнення балансу між продуктивністю та стабільністю (наприклад, Windows, macOS);

– Мікроядра – мінімальний набір функцій, з додатковими службами в окремих модулях, що підвищує надійність, але може знизити продуктивність (наприклад, Google Fuchsia, GNU/Hurd та Minix).

Інтерфейс: спосіб взаємодії користувача з системою.

– Консольний інтерфейс – управління через текстові команди (наприклад, Ubuntu Server);

– Графічний інтерфейс (GUI) – взаємодія через візуальні елементи, такі як вікна та значки (усі ОС, що розглядаються).

Модель оновлення: як часто і яким чином випускаються оновлення.

– Довгострокова підтримка (LTS) – стабільні мінорні оновлення, що гарантують безпеку на тривалий термін без функціональних змін (наприклад, Ubuntu LTS, Chrome OS LTS, Windows LTSC та RHEL);

– Регулярні релізи – оновлення за встановленим графіком з новими функціями та виправленнями (усі стандартні версії ОС, що розглядаються);

– Постійне оновлення (Rolling Release) – постійні дрібні оновлення для забезпечення останніх версій програмного забезпечення (наприклад, Arch Linux).

Призначення: основна область застосування ОС.

– Десктопні ОС – для персональних комп'ютерів і ноутбуків;

– Серверні ОС – для серверів і мережевої інфраструктури;

– Мобільні ОС – для смартфонів і планшетів;

– Вбудовані ОС – для спеціалізованих пристроїв (наприклад, автомобілі чи побутова техніка).

1.2. Застосування класифікації

Для аналізу обрані Windows, macOS, Chrome OS та Ubuntu, які демонструють різні підходи в цих категоріях:

Windows

– Ліцензія: пропрієтарна;

– Тип ядра: гібридне (NT Kernel);

– Інтерфейс: графічний;

– Модель оновлення: регулярні релізи (щорічно) та LTS версії (LTSC, кожні три роки нова версія, підтримка старої виключно з баг-фіксами не менше 5 років);

– Призначення: десктопні та серверні середовища;

– Частка ринку: 71,47%.

macOS

– Ліцензія: пропрієтарна;

– Тип ядра: гібридне (XNU Kernel);

– Інтерфейс: графічний;

– Модель оновлення: нова версія macOS випускається щороку та підтримується протягом 3 років. Для кожного пристрою Mac: 5 років функціональних оновлень + 3 роки виправлень;

– Призначення: настільні комп'ютери та смартбуки (тобто компактні ноутбуки на мобільній платформі ARM);

– Частка ринку: 15,45%.

Chrome OS

– Ліцензія: змішана (на базі відкритого коду з пропрієтарними компонентами);

– Тип ядра: монолітне (Linux Kernel);

– Інтерфейс: графічний;

– Модель оновлення: S (Stable) – пристрої автоматично оновлюються до наступної стабільної версії кожного місяця; LTC (кандидат на довгострокову підтримку) – пристрої отримують функції LTS за 3 місяці до випуску версії на каналі LTS. Пристрої автоматично оновлюються до наступної версії LTC; LTS (довгострокова підтримка) – пристрої автоматично оновлюються до наступної версії LTS кожні 6 місяців. Хромбуки отримують поновлення протягом 10 років;

– Призначення: смартбуки та нетбуки (тобто компактні ноутбуки на мобільних чипах x86);

– Частка ринку: 1,73%.

Ubuntu

– Ліцензія: вільна;

– Тип ядра: монолітне (Linux Kernel);

– Інтерфейс: графічний із підтримкою консольного режиму;

– Модель оновлення: регулярні релізи випускаються восени та навесні

та підтримуються протягом 9 місяців. Основні та обмежені пакети підтримуються щонайменше 5 років у випусках з довгостроковою підтримкою (LTS), що виходять кожні два роки;

– Призначення: десктопні та серверні середовища;
– Частка ринку (разом з іншими дистрибутивами Linux): 4,55%.

1.3. Аргументація вибору

Ці чотири ОС були обрані завдяки їхній популярності, функціональності та різноманітним підходам. Windows і macOS є найпоширенішими пропрієтарними ОС для персональних комп'ютерів, що забезпечують велике охоплення як корпоративного, так і приватного ринків [1]. Chrome OS представляє сучасний підхід, орієнтований на хмарні обчислення і мобільні рішення, та показує зростаючий інтерес до змішаних моделей ліцензування. Ubuntu, як найпопулярніший дистрибутив GNU/Linux, надає альтернативу з відкритим вихідним кодом, популярну серед серверних і корпоративних користувачів.

Вибір цих операційних систем дозволяє охопити весь спектр сучасних рішень, враховуючи різні підходи до ліцензування, архітектури ядра, моделей оновлення та сфер застосування. Це дає можливість провести повний аналіз переваг і недоліків кожної системи у контексті використання в різних типах організацій з різними вимогами до безпеки, продуктивності та інтеграції з корпоративним програмним забезпеченням.

РОЗДІЛ 2
ПОРІВНЯННЯ ЗАХИСТУ ОПЕРАЦІЙНИХ СИСТЕМ ВІД ДІЙ КОРИСТУВАЧА

2.1. Огляд Chrome OS

Chrome OS – операційна система від Google, заснована на ядрі Linux і орієнтована на роботу з веб-додатками. Її інтерфейс подібний до традиційного робочого столу з панеллю завдань і підтримкою кількох вікон, що забезпечує користувачам інтуїтивне управління. Chrome OS побудована навколо веб-браузера Chrome і підтримує веб-орієнтовану екосистему додатків. Для виведення графіки система використовує стек Freon, з планами переходу на Wayland у майбутньому, а віконний менеджер Aura забезпечує зручну багатовіконну роботу.

Chrome OS доступна виключно на спеціалізованих пристроях Chromebook, але існує також версія для звичайних комп'ютерів – Chrome OS Flex, яка дозволяє встановлювати систему на старіші пристрої. Більшість вихідних кодів Chrome OS поширюються під вільною ліцензією Apache 2.0, що надає доступ до значної частини відкритого коду системи.

Вимоги до Chrome OS Flex

Chrome OS Flex розроблена для перетворення старих комп'ютерів та ноутбуків на функціональні пристрої, подібні до хромбуків. Однак для успішної установки необхідно враховувати специфічні апаратні вимоги та обмеження, що визначають сумісність з обладнанням.

Мінімальні системні вимоги:

– Процесор: Intel або AMD (ARM процесори наразі не підтримуються).

– Оперативна пам'ять (RAM): Мінімум 4 ГБ.

– Сховище: Мінімум 16 ГБ вільного простору на жорсткому диску або SSD.

– BIOS: Підтримка завантаження з USB (особливо важливо для

старіших пристроїв).

– Графіка: Інтегровані графічні процесори Intel або AMD. Графіка NVIDIA може працювати, але офіційна підтримка обмежена.

– USB-накопичувач: Необхідно мати флешку з мінімум 8 ГБ для створення інсталяційного носія.

Обмеження та непідтримувані функції:

– TPM (Trusted Platform Module): Хоча TPM не є обов'язковим для роботи Chrome OS Flex, відсутність цього модуля може обмежити деякі функції безпеки.

– Play Store: Android-додатки досі не працюють.

– Сенсорні екрани: Chrome OS Flex підтримує сенсорні екрани на певних сумісних моделях, але на всіх пристроях ця функція може працювати нестабільно.

– Камери та мікрофони: Деякі старі моделі можуть мати проблеми з роботою вбудованих камер та мікрофонів.

– Сканери відбитків пальців: Підтримка сканерів відбитків пальців, яка поширена на сучасних ноутбуках, не реалізована в Chrome OS Flex.

Рекомендовані вимоги для оптимальної роботи:

– Процесор: Для кращої продуктивності та роботи з інтенсивними веб-додатками рекомендується використовувати процесори Intel Core i3/i5/i7 або еквіваленти AMD Ryzen 3/5/7.

– Оперативна пам'ять: Оптимальним варіантом для багатозадачності є 8 ГБ оперативної пам'яті.

Офіційна підтримка пристроїв

Google підтримує офіційний список сертифікованих пристроїв для Chrome OS Flex. Цей список включає ноутбуки, десктопи та робочі станції, які були перевірені на сумісність з Chrome OS Flex. Деякі моделі можуть мати обмежену підтримку залежно від їхнього апаратного забезпечення, що варто враховувати під час вибору платформи для оновлення.

Завдяки цим вимогам Chrome OS Flex дозволяє перетворювати старі

пристрої на сучасні хромбуки, що важливо для оптимізації роботи в корпоративних та освітніх середовищах.

Архітектура безпеки

Безпека операційної системи є одним із ключових факторів при виборі платформи для корпоративного використання, особливо щодо захисту від випадкових або зловмисних дій користувачів. Chrome OS, розроблена Google, позиціонується як одна з найбільш захищених операційних систем "з коробки"[2]. У цьому розділі розглянемо переваги Chrome OS у контексті захисту від дій користувачів, порівнюючи її з іншими популярними операційними системами, такими як macOS, Windows і Ubuntu.

Chrome OS розроблена навколо концепції "нульової довіри" (Zero Trust), що означає, що жоден користувач або пристрій не довіряється автоматично. Кожен елемент системи перевіряється на безпеку під час кожної взаємодії, будь то завантаження файлів, використання програм або доступ до інтернет-ресурсів.

Chrome OS має унікальну функцію перевірки цілісності системи під час завантаження, відому як Verified Boot. Ця функція перевіряє прошивку і всі системні компоненти при кожному запуску пристрою. Якщо система виявляє будь-які зміни або пошкодження коду, Chrome OS автоматично повертається до попередньої перевіреної версії. Це запобігає завантаженню шкідливих програм, навіть якщо вони проникли в систему. Для порівняння, у Windows і macOS подібна перевірка не є настільки автоматизованою і може потребувати додаткових налаштувань і контролю з боку адміністратора.

Chrome OS побудована так, що не має користувачів з правами адміністратора. Це означає, що навіть досвідчені користувачі не мають доступу до системних драйверів, програм та налаштувань, які можуть потенційно скомпрометувати безпеку. Навіть у режимі розробника права користувача залишаються обмеженими, що знижує ризик виникнення вразливостей через неправильні дії або помилки адміністраторів.

Усі дані на пристроях Chrome OS шифруються за замовчуванням за

допомогою унікальних ключів шифрування для кожного користувача. Це забезпечує високий рівень конфіденційності, оскільки навіть у разі крадіжки або фізичного доступу до пристрою зловмисники не зможуть отримати доступ до даних без належних облікових даних. Дані гостьових користувачів видаляються одразу після завершення сесії, що робить Chrome OS ідеальною для використання на спільних пристроях. У Windows і macOS шифрування не завжди є стандартною функцією і може потребувати додаткової конфігурації.

Chrome OS активно використовує методи ізоляції (sandboxing) на рівні системи, додатків і браузера. Ізоляція гарантує, що кожен додаток, процес або вебсторінка працює в окремому середовищі, яке не може впливати на інші частини системи. Це запобігає поширенню зловмисного коду, навіть якщо користувач випадково відкрив небезпечний файл або відвідав заражений вебсайт. Вбудована функція "Безпечний перегляд" (Safe Browsing) у браузері Chrome автоматично захищає користувачів, ізолюючи кожну вебсторінку, щоб вона не могла впливати на інші вкладки чи програми на пристрої.

Chrome OS має меншу поверхню для атак через віддалений доступ завдяки використанню інноваційної системи захисту через брандмауер. Ця система перешкоджає зловмисникам використовувати протоколи виявлення сервісів для перенаправлення запитів і змушення систем до з'єднання з ресурсами під їх контролем. Крім того, Chromebook використовує чіп Google Secure Microcontroller (H1), який підтримує безліч функцій безпеки, включно із захистом ключів шифрування та локальних даних. Це ускладнює фізичний доступ до даних навіть у разі злому пристрою.

Вбудована консоль Chrome OS має обмежений функціонал порівняно з традиційними Unix shell середовищами. Chrome OS не підтримує абсолютну більшість команд UNIX shell, таких як sudo rm -rf /*. Це означає, що користувачі не можуть виконувати команди, які потребують привілейованого доступу або можуть впливати на критичні системні файли. Це забезпечує

додатковий рівень захисту від випадкових або зловмисних дій, оскільки запобігає виконанню команд, які можуть спричинити серйозні пошкодження операційної системи.

Команда sudo rm -rf /* в UNIX-подібних операційних системах є однією з найнебезпечніших. Вона виконує такі дії:

– sudo – запускає команду з правами суперкористувача (адміністратора).

– rm – команда для видалення файлів.

– -r – рекурсивно видаляє всі файли та каталоги.

– -f – форсує видалення, ігноруючи всі попередження і підтвердження.

– / – коренева директорія системи.

– * – вказує на всі файли та каталоги в поточній директорії.

При виконанні цієї команди в системі UNIX або Linux всі файли та каталоги в кореневій директорії (/) будуть видалені без можливості відновлення, що призведе до повної непрацездатності системи.

Команда отримала назву "Патч Барміна" через спробу інтернет-троля завуальовано знищити робочі станції UNIX, скориставшись такою зловмисною командою. Це не було жартом, а цілеспрямованою атакою, що зробило команду своєрідним еталоном для перевірки стійкості системи до руйнівних дій користувачів.

Віртуалізація

Chrome OS використовує віртуалізацію для додаткового захисту системи та користувацьких даних. Завдяки цим технологіям забезпечується високий рівень безпеки, дозволяючи виконувати додатки в ізольованих середовищах, що захищає основну систему від потенційних загроз. Розглянемо основні технології віртуалізації, що використовуються в Chrome OS, та супутню термінологію.

Контейнеризація – це форма віртуалізації на рівні операційної системи, де всі контейнери використовують спільне ядро ОС, але працюють в ізольованих середовищах.

– Переваги: низьке споживання ресурсів, швидкий запуск і виконання, легкість у розгортанні та масштабуванні.

– Недоліки: менша ізоляція, оскільки всі контейнери використовують спільне ядро ОС, вразливість до атак, що можуть вплинути на всю систему через спільне ядро.

Паравіртуалізація – метод, при якому віртуальні машини працюють на основі спеціального гіпервізора (наприклад, KVM у Chrome OS) і використовують модифіковану операційну систему, яка "знає" про своє віртуалізоване середовище.

– Переваги: краща продуктивність порівняно з повною віртуалізацією, висока ізоляція між віртуальними машинами і основною системою.

– Недоліки: потребує модифікації ОС, що може обмежувати сумісність із певними додатками або пристроями.

Повна віртуалізація – тип віртуалізації, в якому гіпервізор створює повноцінну віртуальну машину, що емулює апаратне забезпечення, необхідне для виконання операційної системи.

– Переваги: найвищий рівень ізоляції між віртуальними машинами та основною системою, можливість запускати будь-які ОС без модифікації.

– Недоліки: більше ресурсів, ніж контейнеризація або паравіртуалізація, можливе зниження продуктивності через накладні витрати на емуляцію апаратного забезпечення.

Crostini використовує паравіртуалізацію для запуску Linux-додатків. Віртуальна машина Termina містить контейнер з Debian GNU/Linux, що працює в ізольованому середовищі під керуванням гіпервізора KVM [4]. Це забезпечує захист основної системи Chrome OS навіть у разі загроз або атак у контейнері. У разі неполадок контейнер можна легко відтворити через налаштування Chrome OS.

Щоб забезпечити плавну інтеграцію Linux-додатків у графічне середовище Chrome OS, використовується Sommelier – реалізація Wayland, яка взаємодіє з віконним менеджером Aura. Sommelier виступає проміжною

ланкою, дозволяючи Linux-додаткам, які використовують Wayland або X11, відображатися в середовищі Chrome OS таким чином, що вони виглядають і функціонують подібно до рідних додатків Chrome OS. Це забезпечує кращу сумісність, безпеку і інтеграцію інтерфейсу.

Якщо команда sudo rm -rf /* виконується в середовищі контейнера Crostini на Chrome OS, її дія зазвичай обмежується даними та застосунками, що містяться всередині ізольованого Linux-середовища, залишаючи основну систему Chrome OS неушкодженою. У найгіршому випадку контейнер Crostini може стати непрацездатним; однак його можна швидко та легко відновити через налаштування Chrome OS, забезпечуючи мінімальне порушення роботи всієї системи.

Однак, якщо користувач надав Crostini доступ до каталогів Chrome OS через вбудований файловий менеджер, можуть бути порушені дані в цих спільних каталогах. У таких випадках, хоча основні файли операційної системи зазвичай захищені, втрата або пошкодження даних у спільних каталогах може вплинути на функціональність деяких застосунків або даних користувача, залежно від рівня наданого доступу.

Chrome OS не втрачає стабільності через подібні операції в межах Crostini завдяки своїй архітектурі, яка ізолює контейнерне середовище. Будь-яку втрату функціональності в контейнері можна вирішити шляхом скидання або перевстановлення середовища Crostini без потреби повного відновлення системи. Крім того, під час надання доступу до папок чи каталогів між Chrome OS та Crostini, Chrome OS виводить користувачеві попередження для підтвердження доступу, підкреслюючи ризики, пов’язані з наданням таких дозволів. Цей крок допомагає зменшити випадкову втрату даних, переконуючи користувача в усвідомленні потенційних наслідків.

Загалом, архітектура ізоляції Chrome OS та доступні варіанти відновлення для Crostini роблять її надійною системою, яка здатна витримувати такі помилки в межах контейнерів, зберігаючи стабільність основної системи.

ARC (Android Runtime for Chrome) раніше використовував контейнеризацію, що дозволяло запускати Android-додатки у контейнері на спільному ядрі з Chrome OS [5]. Проте це створювало певні ризики для безпеки, оскільки уразливості Android-додатків могли вплинути на інші частини системи.

ARCVM (Android Runtime for Chrome Virtual Machine) тепер використовує паравіртуалізацію, подібно до Crostini, що забезпечує кращу ізоляцію та безпеку [6]. Android-додатки працюють у віртуальній машині під керуванням KVM, ізольованій від основної системи Chrome OS.

Borealis – проект паравіртуалізації для запуску Steam-ігор на Linux в Chrome OS [7]. Використовує віртуальну машину на базі Ubuntu, яка підтримує апаратне прискорення відео та ігрові контролери, забезпечуючи високу продуктивність та безпеку під час гри.

Parallels Desktop для Chrome OS, використовуючи гіпервізор KVM для повної віртуалізації, дозволяє Chromebook пристроям запускати Windows-застосунки у безпечному, ізольованому середовищі віртуальної машини. Такий підхід підвищує стабільність і безпеку основної системи Chrome OS, проте ця послуга потребує підписки і доступна лише для високопродуктивних пристроїв на базі x86, не підтримуючи Chromebook з архітектурою ARM та Chrome OS Flex.

З середини 2020-х років розвиток оновлень Parallels Desktop для Chrome OS значно сповільнився, що викликало припущення, що Google може зосередити увагу на альтернативних рішеннях для запуску Windows-застосунків на Chromebook. Цю позицію підтверджує придбання Google компанії Cameyo, яка надає рішення для віртуалізації Windows-застосунків через браузер, дозволяючи користувачам отримувати доступ до програм Windows через активне інтернет-з’єднання. На відміну від локальної віртуалізації Parallels, підхід Cameyo значною мірою залежить від доступності та стабільності хмарних серверів Google Cameyo, що має наслідки для конфіденційності даних і надійності доступу.

Якщо Cameyo стане основним методом доступу до Windows-застосунків на Chrome OS, це може розширити підтримку для більшої кількості пристроїв, зокрема бюджетних Chromebook та пристроїв з ARM-процесорами. Однак такий перехід також означатиме зростаючу залежність від хмарної інфраструктури, що потенційно вплине на автономність управління даними та конфіденційність. Дані користувачів, що передаються через віртуалізацію Cameyo, проходитимуть через хмарні сервери Google, що породжує міркування щодо конфіденційності, оскільки обмінювані дані можуть підпадати під політику управління та безпеки даних Google. Користувачам у корпоративних середовищах варто оцінити, як ці зміни відповідають вимогам їхніх організацій до конфіденційності даних та відповідності нормам, особливо якщо мова йде про чутливу інформацію.

У цілому, хоча ARCVM, Crostini та Borealis використовують паравіртуалізаційні технології для підтримки високого рівня ізоляції між застосунками та основною системою, перехід до хмарної віртуалізації, як у випадку Cameyo, може додати нові міркування щодо конфіденційності та безпеки даних. Chrome OS залишається привабливим вибором для корпоративних користувачів, пропонуючи надійний захист і продуктивність, але нові підходи до віртуалізації підкреслюють важливість регулярного перегляду політик обміну даними та конфіденційності.

Висновки

Chrome OS має значні переваги у контексті захисту від дій користувачів, особливо щодо зниження ризику від випадкових або зловмисних дій. Її архітектура безпеки, включаючи функції перевірки завантаження (Verified Boot), шифрування даних, ізоляцію процесів, та захист від віддаленого доступу, робить її привабливим вибором для корпоративних клієнтів та організацій, які прагнуть мінімізувати ризики та підвищити рівень безпеки своїх систем.

Вбудовані механізми віртуалізації забезпечують додатковий рівень захисту, ізолюючи середовища запуску додатків від основної системи. Ці

можливості дозволяють уникнути поширення потенційних загроз і полегшують відновлення після інцидентів, зменшуючи можливі наслідки зловмисних дій або помилок користувачів.

Chrome OS є ідеальним рішенням для організацій, де безпека даних має критичне значення, а користувачі не мають високої технічної підготовки. Операційна система пропонує інноваційний підхід до безпеки, що включає автоматичні оновлення, контроль цілісності системи та мінімізацію прав користувачів, що робить її більш стійкою до сучасних загроз, ніж традиційні операційні системи, такі як Windows і macOS.

Таким чином, Chrome OS може бути рекомендована як оптимальне рішення для організацій, що прагнуть забезпечити надійний захист своїх систем і даних, мінімізуючи при цьому витрати на адміністрування та технічну підтримку.

2.2. Огляд macOS

macOS, розроблена компанією Apple спеціально для комп'ютерів Mac, вирізняється гібридним ядром XNU та зручним графічним інтерфейсом [8]. Ця операційна система стала популярним вибором серед користувачів, які цінують надійність, стабільність і простоту використання. З точки зору безпеки, macOS оснащена кількома шарами захисту, серед яких особливо виділяється технологія System Integrity Protection (SIP). Вона захищає системні файли та важливі налаштування від несанкціонованих змін, як з боку користувачів, так і від шкідливих програм.

Для забезпечення безпеки macOS використовує низку інноваційних рішень. System Integrity Protection (SIP) є ключовою функцією, яка обмежує доступ до критичних частин системи навіть для користувачів з адміністративними правами. SIP не дозволяє змінювати певні шляхи та файли, такі як /System, /usr (за винятком /usr/local), /bin, /sbin та інші важливі каталоги. Однак особисті дані користувача та файли, розташовані поза

межами цих захищених директорій, не підпадають під дію SIP.

Ще одним важливим елементом безпеки є Gatekeeper. Цей механізм перевіряє джерело завантажуваного програмного забезпечення, дозволяючи запускати лише ті програми, які підписані довіреними розробниками або отримали схвалення в App Store. Це значно зменшує ризик встановлення шкідливих програм.

Вбудовані антивірусні механізми, такі як XProtect та Malware Removal Tool (MRT), забезпечують виявлення та видалення відомих шкідливих програм. Вони регулярно оновлюються, щоб протидіяти новим загрозам і підтримувати безпеку системи на високому рівні.

Для захисту даних користувачів macOS пропонує FileVault – потужну функцію шифрування, яка захищає інформацію, зашифровуючи її на пристрої. Навіть у разі втрати або крадіжки пристрою, FileVault забезпечує збереження конфіденційної інформації в безпеці, роблячи її недоступною для неавторизованих користувачів і надаючи важливий захист для чутливих даних.

Apple також активно впроваджує концепцію перевикористання технологій між своїми пристроями, що дозволяє забезпечити високий рівень інтеграції та оптимізації як апаратних, так і програмних рішень. Це підхід, при якому інновації, створені для одного продукту, адаптуються та використовуються в інших, що значно покращує зручність і продуктивність для користувачів.

Одним із найкращих прикладів перевикористання технологій є інтеграція процесорів Apple Silicon серії M у пристрої Mac. Ці процесори базуються на архітектурі ARM, подібній до тієї, що використовується в iPhone та iPad. Завдяки цьому, Mac з процесорами серії M здатні запускати iOS-додатки без необхідності модифікацій, що відкриває нові можливості для користувачів і розробників. Однакове ядро операційної системи XNU та спільні бібліотеки й API, такі як Metal для графіки або Core ML для машинного навчання, забезпечують сумісність між різними типами

пристроїв, дозволяючи додаткам ефективно використовувати доступні апаратні ресурси.

Технології безпеки є ще однією важливою сферою перевикористання. Компонент Secure Enclave, вперше представлений в iPhone, зараз використовується й у Mac. Secure Enclave – це окремий модуль, який зберігає та обробляє чутливі дані, такі як біометричні дані для Touch ID або Face ID, у ізольованому середовищі, що забезпечує їх захист від потенційних загроз. Ця ізоляція гарантує, що навіть якщо основна система буде зламаною, дані, що обробляються Secure Enclave, залишаться недоступними.

Аналогічно, Touch ID, спочатку розроблений для iPhone, вже кілька років доступний на багатьох моделях MacBook, забезпечуючи зручний і безпечний метод аутентифікації користувачів та підтвердження дій, пов’язаних із безпекою. Повторне використання цієї технології підвищує рівень захисту та робить взаємодію з MacBook більш інтуїтивною і знайомою для користувачів, які звикли до інших пристроїв Apple.

Загалом, перевикористання технологій в екосистемі Apple дозволяє досягти значної інтеграції та спільності функцій. Це забезпечує безшовний досвід користувача, де пристрої відчуваються як частина єдиного цілого, взаємодіючи між собою та спрощуючи доступ до ресурсів та даних. Таке поєднання апаратних і програмних рішень допомагає створювати продукти, які гармонійно працюють разом, забезпечуючи користувачам високу продуктивність, безпеку та зручність.

Для додаткового захисту всі додатки, доступні в App Store для macOS, зобов'язані використовувати механізм App Sandbox. Ця "пісочниця" обмежує доступ додатків до системних ресурсів і даних, використовуючи систему контейнерів та налаштування прав доступу. Механізм визначає, які файли, мережеві ресурси та апаратні засоби можуть бути використані додатком, що значно знижує ризик використання вразливостей і обмежує потенційну шкоду від шкідливого коду. Наприклад, якщо iOS-додаток на macOS спробує отримати доступ до системних файлів або даних інших додатків, Sandbox

заблокує цю дію, захищаючи від можливих атак або витоків інформації.

Додатки, які не використовують Sandbox, мають повний доступ до файлової системи, мережевих з'єднань та інших ресурсів комп'ютера. Це дозволяє їм реалізовувати більш гнучкі функції, але також підвищує ризики для безпеки. Без використання Sandbox такі програми можуть змінювати системні файли, встановлювати шкідливе програмне забезпечення або збирати конфіденційну інформацію. Натомість додатки з Sandbox працюють в ізольованому середовищі, обмежуючи взаємодію з іншими частинами системи та даними, що робить систему більш захищеною.

Розглянемо ситуацію з виконанням команди sudo rm -rf /*, яка є однією з найбільш руйнівних в UNIX-подібних системах, включно з macOS. Виконання цієї команди видаляє всі незахищені файли та каталоги з кореневої директорії без можливості відновлення, що робить систему повністю непрацездатною.

На macOS така дія викликає ряд сповіщень, які вимагають дозволів на доступ до різних даних: жорсткого диска, контактів, фото тощо. Це пов'язано з вбудованими механізмами безпеки, які обмежують доступ додатків до приватних даних. Якщо користувач підтвердить всі запити, система продовжить видалення всіх незахищених директорій та файлів, які не захищені SIP. Можна спробувати виключити виведення цих сповіщень, перенаправивши їх у /dev/null, але це не уникне запиту на доступ до жорсткого диска.

У результаті виконання цієї команди призведе до неможливості доступу до всіх облікових записів на комп'ютері, оскільки вони не захищені SIP. Хоча система буде стабільно завантажуватися до екрана входу, введення правильного пароля не дозволить продовжити роботу.

Для виправлення ситуації на старих Mac з процесорами Intel необхідно використовувати комбінацію клавіш Cmd+R для входу в режим відновлення, який захищений SIP. У цьому режимі потрібно підключитися до Інтернету (наприклад, через Wi-Fi) і вибрати переустановку macOS.

На Mac з Apple Silicon процедура перевстановлення виглядає так:

1) Утримуйте кнопку живлення: Натисніть і утримуйте кнопку живлення на вашому Mac.

2) Перейдіть до екрана з параметрами завантаження: Продовжуйте утримувати кнопку живлення, поки ваш Mac не завантажить екран параметрів завантаження. Коли побачите опцію "Параметри" (Options), відпустіть кнопку живлення.

3) Виберіть "Параметри": Клацніть на "Параметри" (Options), а потім натисніть кнопку "Продовжити", яка з'явиться під нею.

4) Авторизація: Якщо вас попросять обрати користувача, пароль якого ви знаєте, оберіть його. Потім натисніть "Далі" і введіть пароль адміністратора, який цей користувач використовує для входу на Mac.

5) Початок перевстановлення: Дотримуйтесь інструкцій на екрані, щоб розпочати перевстановлення поточної версії macOS, яка була останньою встановленою на вашому комп'ютері.

Ця процедура не вимагає підключення до Інтернету, оскільки використовує копію macOS, що зберігається на вбудованому розділі відновлення.

Після перевстановлення система відновить свою функціональність. Можливо навіть використовувати ті ж облікові дані для входу в пошкоджені облікові записи, оскільки вони можуть бути розташовані в захищеній SIP директорії, наприклад, /var/db/dslocal/nodes/Default. Проте самі облікові записи будуть повністю порожніми, і їх потрібно буде налаштовувати заново.

Цікаво, що переустановка macOS може зберігати дані, налаштування та додатки [9]. Наприклад, якщо не вдається оновити macOS через помилку, можна скористатися переустановкою за допомогою USB-накопичувача з новішою версією ОС, і при цьому дані залишаться недоторканими. Це досягається завдяки розділенню диска на два томи: Macintosh HD (система) і Macintosh HD – Data (дані). Переустановка macOS перезаписує лише системний том, зберігаючи дані користувача, налаштування та додатки на

томі даних, якщо не обрано форматування всього диска.

Порівнюючи системи безпеки Chrome OS та macOS, можна відзначити різні підходи до забезпечення безпеки. Chrome OS, розроблена Google, застосовує концепцію "нульової довіри", де кожен елемент системи перевіряється на безпеку під час кожної взаємодії. Основні механізми захисту включають Verified Boot, шифрування даних та ізоляцію процесів через контейнери.

macOS, у свою чергу, забезпечує високий рівень безпеки завдяки вбудованим інструментам, таким як System Integrity Protection (SIP) та Gatekeeper. Як і Chrome OS на пристроях Chromebook, macOS є предустановленою операційною системою на комп'ютерах Mac, що означає, що користувачам не потрібно встановлювати додаткові драйвери – вони вже включені в систему. Драйвери в macOS захищені SIP, що запобігає їх пошкодженню або зміні користувачем. Вони розташовані у системній теці /System/Library/Extensions та мають захист від несанкціонованих змін.

Політика "нульової довіри" Chrome OS є більш автоматизованою та стійкою до помилок користувачів. Підхід Apple, натомість, передбачає більшу участь користувача у налаштуванні безпеки, але забезпечує надійний захист за допомогою комбінації апаратних і програмних заходів.

У підсумку, обидві операційні системи пропонують високий рівень безпеки, але їхні підходи відрізняються. Chrome OS підходить для середовищ, де потрібен автоматизований захист "з коробки", тоді як macOS вимагає більш ретельного налаштування та адміністрування для досягнення максимального рівня безпеки.

2.3. Огляд Windows

Операційна система (ОС) Windows є пропрієтарною платформою, розробленою компанією Microsoft, яка забезпечує основну взаємодію між апаратними компонентами комп'ютера та програмним забезпеченням. Вона

належить до гібридного типу ОС, поєднуючи в собі елементи монолітної та мікроядерної архітектури, що дозволяє оптимізувати продуктивність і забезпечити гнучкість у підтримці та розвитку системи.

Windows оснащена графічним інтерфейсом користувача (GUI), що робить її зрозумілою та зручною у використанні як для домашніх користувачів, так і в корпоративних середовищах. Вона підтримує багатозадачність, широкий спектр апаратного забезпечення, а також інтеграцію з численними сервісами Microsoft, такими як Microsoft 365, Azure та Microsoft Entra ID. Це робить Windows однією з найпопулярніших платформ для корпоративного використання завдяки високій сумісності з різноманітним програмним забезпеченням, розвиненій екосистемі розробників і надійній підтримці від Microsoft.

Операційна система Windows пропонує численні засоби безпеки, серед яких BitLocker, Microsoft Defender та Windows Hello (система біометричної автентифікації, що дозволяє входити в систему за допомогою відбитка пальця, розпізнавання обличчя або PIN-коду) [10]. Ці засоби забезпечують захист даних користувачів та запобігають кіберзагрозам. Завдяки цим функціям безпеки, а також інтеграції сучасних технологій, Windows залишається однією з найуніверсальніших та найпоширеніших операційних систем, яка постійно адаптується до нових викликів технологічного світу та потреб користувачів.

Сучасні операційні системи, зокрема Windows, впроваджують великий спектр технологій безпеки, що охоплюють захист на різних рівнях – від апаратного до програмного. Ці рішення спрямовані на захист ядра операційної системи, безпеку облікових записів користувачів та захист критично важливих ресурсів, забезпечуючи цілісність і стабільність роботи системи в умовах сучасних загроз.

Системи безпеки у Windows

Windows Defender System Guard – це комплекс технологій, спрямованих на захист системи на рівні ядра та забезпечення її цілісності.

Використовуючи апаратну верифікацію та безпеку на основі віртуалізації (VBS), System Guard запобігає атакам на ядро системи, таким як руткіти, і забезпечує захист від шкідливих дій, що можуть порушити роботу операційної системи. Ключові компоненти, такі як Secure Boot, Kernel Control Flow Guard (KCFG) та Memory Integrity, працюють разом, щоб гарантувати, що система завантажується і працює без втручання зловмисників.

Credential Guard, один із ключових компонентів цієї системи, використовує віртуалізацію на основі безпеки (VBS) для захисту облікових даних користувачів. Credential Guard ізолює ці дані в середовищі, недоступному для зловмисників, запобігаючи таким атакам, як "Pass-the-Hash", навіть якщо зловмисник має адміністративний доступ. Ця функція аналогічна до Apple Keychain у macOS, яка зберігає чутливі дані користувачів, такі як паролі та ключі шифрування, у зашифрованому середовищі, роблячи їх недоступними без автентифікації. Однак Credential Guard покладається на ізоляцію даних через віртуалізацію, тоді як Keychain використовує апаратне шифрування та інтеграцію з Secure Enclave для захисту інформації.

Процес захищеного завантаження (Trusted Boot) забезпечує перевірку цілісності кожного етапу завантаження Windows. Це гарантує, що на кожному етапі завантажується лише перевірене та безпечне програмне забезпечення. Компоненти Secure Boot, ELAM (Early Launch Anti-Malware) та Measured Boot працюють спільно, щоб захистити систему від руткітів та інших загроз ще до повного завантаження операційної системи.

BitLocker Drive Encryption дозволяє шифрувати диск, використовуючи алгоритми AES з 128- або 256-бітним ключем, забезпечуючи захист даних на диску від несанкціонованого доступу. Використання модуля TPM (Trusted Platform Module) для зберігання ключів шифрування підвищує безпеку, оскільки ключі зберігаються в апаратно захищеному середовищі. У порівнянні, на macOS функція FileVault надає аналогічні можливості шифрування дисків.

Для контролю запуску додатків Windows пропонує Windows Defender Application Control (WDAC) та AppLocker. WDAC дозволяє адміністраторам створювати політики, що обмежують запуск лише перевіреного програмного забезпечення, запобігаючи виконанню потенційно шкідливих програм. AppLocker доповнює цю функціональність, дозволяючи визначати, які додатки та скрипти можуть запускатися в системі, на основі сертифікатів, хешів або шляхів до файлів.

Контроль облікових записів користувачів (UAC) запобігає внесенню несанкціонованих змін до системи, вимагаючи підтвердження адміністратора для виконання дій, що можуть вплинути на безпеку або стабільність операційної системи.

Для запобігання використанню відомих вразливих драйверів Windows використовує Microsoft Vulnerable Driver Blocklist, яка блокує встановлення драйверів, що можуть бути використані зловмисниками для атак на ядро або зниження безпеки системи.

Windows Sandbox надає ізольоване середовище для безпечного запуску підозрілих програм. Використовуючи легковагову віртуалізацію на основі Hyper-V, Sandbox створює тимчасове середовище, яке видаляється після закриття, забезпечуючи, що жодні зміни не вплинуть на основну систему.

Запобігання виконанню даних (DEP) та Система шифрування файлів (EFS) забезпечують додаткові рівні безпеки. DEP запобігає виконанню коду з областей пам'яті, не призначених для цього, що перешкоджає атакам переповнення буфера. EFS дозволяє шифрувати окремі файли на рівні файлової системи NTFS, захищаючи їх від несанкціонованого доступу.

Захист ресурсів Windows (Windows Resource Protection) та TrustedInstaller працюють разом для забезпечення цілісності системних файлів та ключів реєстру. WRP використовує списки контролю доступу (ACL) для захисту критичних ресурсів, а TrustedInstaller контролює зміни до цих ресурсів, дозволяючи лише довіреним оновленням вносити зміни.

Нарешті, Менеджер безпеки облікових записів (SAM) зберігає дані

облікових записів користувачів, включаючи хеші паролів, у захищеній області реєстру. Це забезпечує, що доступ до цих даних має лише операційна система та авторизовані адміністратори, захищаючи облікові записи від несанкціонованого доступу.

Microsoft Defender: порівняння

Microsoft Defender for Endpoint (MDE) є еталонним засобом безпеки для Windows 11, оскільки він інтегрований безпосередньо в операційну систему, що забезпечує більш глибокий рівень контролю та доступу до системних ресурсів. Однак, версії для інших платформ – macOS, Ubuntu та Chrome OS – мають певні обмеження у порівнянні з версією для Windows. Нижче розглянемо ці обмеження та відмінності.

MDE на Windows 11 використовує всі наявні функції захисту, включаючи захист від загроз в реальному часі, контроль додатків, розширені можливості виявлення та реагування (EDR), аналіз безпеки на рівні ядра через System Guard, Credential Guard для ізоляції облікових даних, інтеграцію з BitLocker для шифрування, а також інші технології, специфічні для Windows, як-от Application Control (WDAC) та AppLocker.

Версія MDE для macOS підтримує захист від загроз в реальному часі, виявлення та реагування (EDR), але не має доступу до таких ключових технологій на кшталт Credential Guard, Application Control або шифрування через BitLocker на Windows. macOS також використовує власні вбудовані інструменти захисту, як-от Gatekeeper та XProtect, що працюють паралельно з MDE, але MDE не має таких глибоких привілеїв для управління ядром або мережевими ресурсами, як на Windows.

MDE на macOS покладається на системні API для моніторингу загроз і має обмеження щодо управління привілеями та мережевою активністю. Шифрування даних реалізується через FileVault, а не через BitLocker, що також зменшує можливості інтегрованого шифрування у контексті MDE.

На платформі Ubuntu MDE орієнтований здебільшого на серверну безпеку, забезпечуючи базові можливості моніторингу та виявлення загроз.

Однак, інтеграція з системними компонентами набагато менша у порівнянні з Windows, оскільки немає доступу до всіх функцій, таких як контролю додатків або шифрування на рівні системи. MDE на Linux (включаючи Ubuntu) забезпечує лише базові засоби виявлення шкідливого ПЗ та аналітику подій без додаткових можливостей контролю ядра або системного моніторингу.

Версія MDE для Chrome OS, яка доступна через Play Store, має значно обмежений функціонал, оскільки вона працює через середовище Android-додатків. Вона здебільшого орієнтована на захист кінцевих точок від загроз та забезпечує лише базові засоби виявлення шкідливого ПЗ. Оскільки Chrome OS сама по собі має інші засоби безпеки, такі як автоматичні оновлення та ізоляція середовища для додатків (sandboxing), MDE не має доступу до більш глибоких компонентів операційної системи, таких як ядро чи контроль додатків.

Альтернативи Defender

На додаток до Microsoft Defender for Endpoint, існують декілька кросплатформних рішень для забезпечення всебічного захисту на різних операційних системах:

– CrowdStrike Falcon: Надає розширений захист кінцевих точок для платформ Windows, macOS та Linux, з потужними можливостями Endpoint Detection and Response (EDR) та моніторингом у реальному часі.

– Sophos Intercept X: Забезпечує ефективний захист кінцевих точок з підтримкою різних платформ та централізованим управлінням, що гарантує узгоджені політики безпеки на різних операційних системах.

– SentinelOne: Пропонує повнофункціональне рішення для безпеки на Windows, включаючи автоматизовану функцію відновлення, яка може повернути систему до стану перед інфекцією. Однак на macOS і Linux деякі розширені функції можуть бути обмежені, що потенційно впливає на глибину захисту та можливості автоматизованого усунення загроз на цих платформах.

Варто зазначити, що, хоча ці альтернативи забезпечують надійний захист для різних платформ, їх інтеграція з хмарними сервісами Microsoft відрізняється. Для організацій, які активно використовують Microsoft 365, Azure або Microsoft Entra ID, безшовна інтеграція, що пропонує Microsoft Defender for Endpoint, може стати значною перевагою, забезпечуючи узгоджене управління безпекою та спрощуючи операції в межах екосистеми Microsoft.

Хмарне управління пристроями Defender

Microsoft Defender for Endpoint використовує потужну хмарну платформу для управління та моніторингу захисту на різних пристроях. Хмарне управління забезпечує централізований моніторинг загроз, автоматизацію реагування та інтеграцію з іншими хмарними рішеннями Microsoft. Для різних операційних систем хмарне управління пристроями через Defender є однаковим з точки зору базових можливостей моніторингу. Однак через обмежені можливості доступу до системних ресурсів (особливо на macOS та Chrome OS), деякі функції автоматизації та реагування можуть бути менш ефективними або обмеженими.

Висновок: хоча Microsoft Defender for Endpoint на інших платформах (macOS, Ubuntu, Chrome OS) надає базові можливості для виявлення загроз і моніторингу, він значно поступається версії для Windows у глибині інтеграції та рівні контролю над системними компонентами. Для повноцінного захисту на інших платформах можуть бути потрібні додаткові або альтернативні рішення безпеки.

Роль реєстру у Windows

Реєстр Windows є важливим елементом операційної системи, що вимагає ретельного захисту. Це централізована база даних, яка зберігає конфігураційні налаштування як системи, так і встановлених програм. Реєстр містить інформацію про апаратне забезпечення, драйвери, системні параметри, користувацькі профілі, а також інші ключові налаштування, що забезпечують роботу Windows та програмного забезпечення. Він виконує

важливу роль у забезпеченні узгодженості та цілісності конфігурацій, надаючи єдине місце для зберігання налаштувань.

На відміну від Windows, в UNIX-подібних системах (наприклад, Ubuntu, macOS, Chrome OS) концепція реєстру відсутня. Замість єдиної централізованої бази даних, ці системи використовують набір окремих текстових файлів для збереження налаштувань. Системні налаштування зберігаються зазвичай у директорії /etc, тоді як користувацькі налаштування знаходяться у відповідних домашніх каталогах.

Цей підхід має свої переваги. Текстові файли легко редагувати, зберігати резервні копії або керувати ними через системи контролю версій. Крім того, розподілена структура конфігураційних файлів дозволяє уникнути єдиного пункту відмови. Якщо один з конфігураційних файлів пошкоджений, це впливає лише на конкретний компонент, а не на всю систему. Таким чином, UNIX-подібні системи забезпечують гнучкість, модульність і стабільність, відповідаючи своїй філософії відкритості та надійності.

Команда reg delete та її наслідки. Команда reg delete призначена для видалення розділів реєстру, включаючи всі основні гілки (HKLM, HKCU, HKCR, HKU, HKCC). Видалення цих ключів робить Windows невідновлюваною, оскільки реєстр є центральною базою даних, яка містить усі критично важливі налаштування операційної системи, драйверів і програм. Повне видалення ключів реєстру руйнує структуру Windows на глибокому рівні, що робить її неможливою для завантаження або відновлення.

Чому видалення реєстру є критичним? Реєстр Windows можна порівняти з "мозком" операційної системи – він містить дані про всі налаштування та конфігурації, включаючи параметри завантаження, драйвери, служби, налаштування безпеки та шляхи до виконуваних файлів. Видалення ключів реєстру руйнує всю цю конфігурацію, що робить систему непрацездатною [12]. При видаленні реєстру користувач втрачає саму систему, оскільки без реєстру операційна система не може завантажитися чи

функціонувати. Однак, дані користувача, що зберігаються на диску, можуть залишитися недоторканими і бути відновленими, навіть якщо система більше не працює.

Наприклад, за допомогою завантажувального USB-накопичувача або Live CD ви можете отримати доступ до диска і скопіювати особисті файли на інший носій. Якщо диск зашифровано за допомогою BitLocker, для цього буде потрібен ключ відновлення, який можна зберігати окремо (наприклад, в обліковому записі Microsoft або на USB-носії).

Для порівняння, команда del C:\ /s /q /f (так званий "патч Барміна" для Windows) видаляє всі файли на системному диску, включаючи файли операційної системи, програми та дані користувача. У цьому випадку користувач втрачає всі дані, зокрема файли операційної системи та особисті дані, проте базова структура системи може зберегтися. Це означає, що ОС все ще можна відновити за допомогою інструментів, таких як Windows Recovery або завантажувальний диск. Наприклад, на деяких пристроях після видалення файлів з диска все ще можна відновити облікові записи користувачів або встановити нову копію операційної системи.

Таким чином, видалення реєстру знищує критично важливі дані конфігурації, необхідні для завантаження та функціонування операційної системи, що робить відновлення без повного перевстановлення неможливим. Однак дані користувача можуть все ж бути відновлені за допомогою спеціалізованих інструментів для відновлення даних. Поширеними засобами для таких цілей є EaseUS Data Recovery Wizard, Recuva і Disk Drill, які можуть сканувати жорсткий диск на наявність відновлюваних файлів навіть після серйозного пошкодження системи. Крім того, функції Windows, такі як Відновлення системи та Резервне копіювання й відновлення, можуть бути корисними, якщо раніше були налаштовані резервні копії, що дозволяє відновити файли користувача або знімки системи.

З іншого боку, видалення файлів з системного диска зазвичай призводить до втрати даних, але може все ж дозволити відновлення системи.

У таких випадках середовище відновлення Windows (WinRE) може допомогти відновити деякі системні файли або дозволити скидання операційної системи, зберігаючи дані користувача, залежно від рівня пошкоджень. Завантажувальні USB-накопичувачі або диски відновлення, створені до інциденту, також можуть допомогти відновити критично важливі системні файли без повного перевстановлення.

Ці інструменти та методи можуть бути безцінними для зменшення втрати даних і відновлення функціональності після значних змін у системі або випадкових видалень.

Огляд WSL

Однак, сучасні версії Windows починаючи з 10 при своїй унікальній архітектурі з реєстром мають програмну сумісність з GNU/Linux!

Windows Subsystem for Linux (WSL) – це функція в операційній системі Windows, яка дозволяє запускати нативне ядро Linux безпосередньо на Windows без необхідності використання віртуальних машин або двох окремих систем. WSL забезпечує можливість виконання Linux-додатків, скриптів та команд безпосередньо в середовищі Windows, надаючи доступ до файлової системи, мережевих ресурсів та інших компонентів Windows.

Основною перевагою WSL є інтеграція Linux середовища з Windows, що дозволяє розробникам, адміністраторам та іншим користувачам працювати з інструментами Linux і Windows одночасно, використовуючи єдиний робочий процес. Це значно полегшує завдання, що вимагають обробки даних у Linux або використання специфічного програмного забезпечення, розробленого для цієї платформи, у звичайному робочому середовищі Windows.

WSL підтримує встановлення різних дистрибутивів Linux, таких як Ubuntu, Debian, Fedora, SUSE, та інші, що дозволяє користувачам вибирати середовище, яке найбільше відповідає їхнім потребам. За допомогою WSL можна виконувати більшість команд, доступних у Linux, включаючи запуск Bash скриптів, компіляцію коду, роботу з пакетними менеджерами та

налаштування серверних служб.

З появою WSL 2 було запроваджено повноцінне ядро Linux, яке працює у віртуальній машині на базі Microsoft Hyper-V. Це значно покращило продуктивність файлової системи, підтримку системних викликів та сумісність з програмами Linux. Завдяки цьому, WSL 2 забезпечує високий рівень інтеграції Linux із середовищем Windows, що робить його зручним інструментом для щоденного використання.

Нова функція WSL 2 також включає можливість запуску графічних Linux-додатків (GUI) безпосередньо на Windows, як нативних додатків, завдяки інтеграції з віконним менеджером Windows через протокол віддаленого робочого столу (RDP). Це дозволяє Linux-програмам відображатися і функціонувати в Windows як звичайні додатки, включаючи підтримку апаратного прискорення графіки. Користувачі можуть запускати додатки для обробки зображень, текстових редакторів, веб-браузерів тощо, які створені для Linux, без потреби в додаткових налаштуваннях.

Для забезпечення такої графічної інтеграції WSL 2 використовує протокол Wayland, сучасний протокол дисплея для Linux, який замінює застарілий X11, що можна було встановити в першій ітерації WSL. Wayland забезпечує більш швидке, безпечне та ефективне відображення графічного інтерфейсу, завдяки чому графічні додатки Linux можуть працювати з меншою затримкою і кращою підтримкою нових функцій. Подібно до Crostini в Chrome OS, де також використовується протокол Wayland, це дозволяє реалізувати більш плавний та інтегрований користувацький досвід.

Таким чином, WSL надає користувачам Windows зручний інструмент для інтеграції можливостей Linux у їхній щоденний робочий процес, забезпечуючи при цьому високу продуктивність, гнучкість та розширені можливості для роботи з графічними додатками.

Результати виконання команди sudo rm -rf / у Windows Subsystem for Linux (WSL) та порівняння з Crostini на Chrome OS. Windows Subsystem for Linux (WSL) є потужним інструментом, що дозволяє користувачам запускати

Linux-додатки та виконувати команди Linux безпосередньо на Windows [11]. Однак виконання певних деструктивних команд, таких як sudo rm -rf /* (відомий також як "патч Барміна"), може мати серйозні наслідки для операційної системи.

Виконання sudo rm -rf / як звичайний користувач. Коли ви запускаєте WSL як звичайний користувач і виконуєте команду sudo rm -rf /*, ваш обліковий запис Windows продовжує функціонувати, але всі незахищені дані, що знаходяться у вашій домашній директорії, видаляються. Це може спричинити пошкодження системних файлів WSL та порушити роботу додатків, встановлених у середовищі Linux. Наприклад, виконання команди sfc /scannow у Windows може виявити пошкоджені системні файли, які не можуть бути відновлені. Спроби перевстановлення WSL призводять до помилок через невірний системний шлях, а App Installer також може відмовитися працювати. У цьому випадку простіше видалити та створити новий обліковий запис Windows, оскільки основна операційна система залишається непошкодженою.

Виконання sudo rm -rf / як адміністратор. Якщо ви запускаєте WSL з правами адміністратора і виконуєте команду sudo rm -rf /* або навіть rm -rf /* (оскільки шкода завдається адміністратором Windows, а не суперкористувачем UNIX), ситуація значно погіршується. Критичні файли Windows можуть бути пошкоджені або видалені, що призводить до серйозних збоїв у роботі системи. У такому випадку система може перестати завантажуватися, показуючи "синій екран смерті" з помилкою CRITICAL_SERVICE_FAILED. Спроби відновлення з хмарної або локальної копії Windows зазвичай не дають результату, оскільки критичні компоненти ОС залишаються пошкодженими.

Чому вдалося скинути налаштування Windows після виконання del C:\ /s /q /f, але не після sudo rm -rf / у WSL? Команда del C:\ /s /q /f, виконана з правами адміністратора в Windows, намагається видалити всі файли на диску C:, однак багато критичних системних файлів захищені системними

механізмами, такими як Windows File Protection (WFP) або TrustedInstaller. Ці механізми запобігають видаленню системних файлів, забезпечуючи можливість відновлення системи до початкового стану.

На відміну від цього, команда sudo rm -rf /*, виконана з правами адміністратора Windows у середовищі WSL, може призвести до пошкодження критичних файлів Windows, оскільки WSL має прямий доступ до файлової системи Windows. При цьому команда обходить захисні механізми, властиві самій Windows, оскільки вона виконується в контексті Linux. У результаті пошкодження стає настільки серйозним, що операційну систему неможливо відновити звичайними методами, і потрібна повна перевстановлення з USB-носія.

Вразливість до програм-вимагачів

Ця вразливість виходить за межі випадкового виконання руйнівних команд і включає навмисні атаки шкідливих програм, особливо програм-вимагачів, які можуть зашифрувати або видалити файли на вашій системі. Програми-вимагачі часто імітують ефекти руйнівних команд, таких як `rm -rf` або `del`, підкреслюючи високу вразливість систем, де важливі дані зберігаються локально. Крім того, дані, синхронізовані з хмарними сервісами, такими як OneDrive, SharePoint або файлові сервери, також можуть бути під загрозою, оскільки програми-вимагачі на локальному пристрої можуть передавати зашифровані файли до хмари через синхронізацію.

Одним із основних захистів від програм-вимагачів у хмарних середовищах є версіювання файлів у таких сервісах, як SharePoint і OneDrive, що дозволяє зберігати попередні версії файлів. Ця функція дає змогу користувачам повернутися до останньої неінфікованої версії у разі атаки. Однак відновлення великої кількості даних із попередніх версій може бути трудомістким і витратним за часом, особливо якщо програма-вимагач уразила багато файлів у різних розташуваннях.

Крім того, складні програми-вимагачі можуть цілеспрямовано

атакувати хмарне сховище, потенційно обходячи захист через версіювання. Деякі варіанти видаляють або перезаписують попередні версії файлів, виснажуючи історію версій хмарного сервісу й залишаючи лише зашифровані копії. У SharePoint і OneDrive адміністратори можуть встановлювати обмеження на кількість збережених версій (наприклад, утримувати певну кількість версій для кожного файлу), але цей захист може бути недостатнім, якщо атаки тривають і видаляють або жорстко видаляють старі версії, роблячи їх невідновлюваними.

Для посилення захисту організації можуть реалізувати офлайн-резервні копії та холодне зберігання, до яких програми-вимагачі не мають доступу. Регулярні резервні копії, що зберігаються поза основним мережевим середовищем, допоможуть забезпечити цілісність даних і швидке відновлення навіть у випадку, якщо версіювання в хмарі та онлайн-резервні копії будуть скомпрометовані.

Важливість резервного копіювання хмарних сервісів.

Ця ситуація підкреслює необхідність резервного копіювання даних навіть для хмарних сервісів, таких як OneDrive, SharePoint та файлові сервери. Якщо зловмисне ПЗ зашифрує або видалить файли, синхронізація може призвести до втрати доступу до цих даних і в хмарі. Це особливо актуально на корпоративному рівні, де втрата критично важливих даних може завдати серйозних збитків.

Компанії повинні впроваджувати політики регулярного резервного копіювання для файлів, що зберігаються в хмарних сховищах або синхронізовані через локальні файлові сервери. Резервні копії повинні зберігатися в окремих, ізольованих середовищах, щоб захистити їх від шкідливого впливу або компрометації основної системи через викупне ПЗ.

У середовищі Crostini на Chrome OS, яке також дозволяє запускати Linux-додатки, ситуація дещо інша. Crostini використовує контейнеризацію для ізоляції середовища Linux від основної операційної системи. Якщо ви виконуєте команду sudo rm -rf /* у Crostini, вона пошкоджує лише файли і

дані, які знаходяться всередині контейнера, не зачіпаючи при цьому основну Chrome OS [3]. Контейнер Crostini можна легко видалити та створити новий через налаштування Chrome OS, тому такі пошкодження є відносно безпечними і легко усуваються.

Проте, якщо користувач вручну надав спільний доступ до папки у файловому менеджері Chrome OS з Crostini, наслідки для цієї папки будуть такими ж сумними, як і при виконанні команди на системі Windows: дані можуть бути видалені або пошкоджені. Однак, навіть за таких умов, система Chrome OS залишиться непошкодженою, оскільки шкідливі дії не можуть вплинути на основну операційну систему.

У випадку WSL на Windows, хоча WSL також є віртуалізованим середовищем, він має доступ до файлової системи Windows, і шкідливі команди можуть пошкодити не лише середовище WSL, а й основну операційну систему. Таким чином, наслідки виконання команди sudo rm -rf /* у WSL значно серйозніші, ніж у Crostini на Chrome OS, де основна система залишається захищеною від змін у контейнері.

Windows 10X

Windows 10X була амбітною спробою Microsoft створити сучасну операційну систему для конкуренції з Chrome OS, засновану на Windows Core OS. Її метою було вирішити недоліки класичної Windows, включно з проблемами безпеки реєстру та загальним захистом системи.

Контейнеризація та захист системи

Windows 10X впровадила принцип контейнеризації для забезпечення безпеки та стабільності. Програми Win32 запускалися в спільній віртуальній машині, яка ізолювала їх від системних компонентів, тим самим знижуючи ризик негативного впливу на операційну систему. Сучасні UWP-додатки (Universal Windows Platform) працювали в ізольованих контейнерах, що забезпечувало вищий рівень захисту. UWP-додатки упаковуються у формат APPX, який гарантує правильне встановлення та ізоляцію додатків, зменшуючи ризики для системи.

APPX – це формат пакунків для UWP-додатків, який дозволяє зберігати програму разом із її залежностями в одному файлі. APPX гарантує, що додатки будуть встановлюватися у захищених контейнерах, забезпечуючи ізоляцію та підвищену безпеку. Проте APPX більше підходить для UWP-додатків і має обмеження при роботі з класичними Win32-додатками.

Для запуску класичних Win32-додатків у Windows 10X використовувався формат MSIX, який є більш універсальним і дозволяє пакувати як Win32, так і UWP-додатки. MSIX забезпечує ізоляцію додатків разом із усіма їхніми залежностями, що підвищує контроль над їх впливом на систему. Також MSIX підтримує легке оновлення додатків та можливість відкоту до попередньої версії, що робить його більш гнучким для використання в корпоративному середовищі. Це продовження формату APPX, яке спрощує управління додатками.

Контейнеризація Windows 10X допомагала запобігти шкідливим діям, наприклад, видаленню критичних системних файлів. Такі дії впливали лише на відповідний контейнер, що мінімізувало можливість шкоди для всієї системи. Важливо зазначити, що Win32-додатки у Windows 10X не запускалися безпосередньо на системі, а через ізольовану віртуальну машину. Це забезпечувало додатковий рівень безпеки, але могло впливати на продуктивність і сумісність додатків. Цей підхід був подібний до ізоляційної моделі Chrome OS для Linux-додатків.

Відокремлення системних і користувацьких даних
Однією з ключових особливостей Windows 10X було відокремлення системних файлів від користувацьких даних, що сприяло більш швидкому і безпечному процесу оновлення. Системні оновлення не впливали на користувацькі файли, що дозволяло уникати втрати даних і значно скоротити час встановлення оновлень. Це також зробило процес оновлення більш плавним та зменшило ризики під час проведення апгрейдів.

Переваги та причини провалу. Windows 10X обіцяла стабільнішу, швидшу та безпечнішу роботу, де користувачам не потрібно було

турбуватися про встановлення драйверів, що можна порівняти з простотою Chromebook і Mac [13]. Проте реалізація Windows 10X зіткнулася з серйозними труднощами.

Однією з головних проблем була складність сумісності Win32-додатків. Вони не могли працювати безпосередньо на Windows 10X, а потребували використання віртуалізованого середовища (контейнерів або віртуальних машин), яке ізолювало їх від основної системи. Це значно обмежувало продуктивність і швидкість роботи багатьох класичних додатків, що робило їх менш ефективними в порівнянні з роботою на традиційній Windows.

Інша проблема полягала в нестачі апаратних пристроїв, здатних повноцінно працювати з цією операційною системою. Windows 10X була розроблена для нових типів пристроїв з подвійними екранами та складними форм-факторами, як, наприклад, Surface Neo. Однак такі пристрої не були широко представлені на ринку, що обмежило можливості поширення Windows 10X. Вона не змогла знайти широкого застосування на традиційних ноутбуках та планшетах, оскільки її функціонал був орієнтований на нові форм-фактори.

Для повноцінного розкриття потенціалу Windows 10X потрібні були сучасні пристрої, оптимізовані для контейнеризації, оскільки ОС значною мірою покладалася на ізоляцію додатків для забезпечення безпеки. Але через відсутність таких пристроїв користувачі могли відчути зниження продуктивності під час роботи з Win32-додатками та іншими ресурсомісткими завданнями.

Таким чином, основними причинами провалу Windows 10X стали проблеми з продуктивністю Win32-додатків через контейнеризацію та нестача сучасних апаратних пристроїв, здатних підтримувати цю нову ОС на належному рівні.

Хоча Windows 10X не була випущена на ринок, багато її інноваційних ідей перейшли до Windows 11. Оновлений дизайн Windows 11 значною

мірою черпав натхнення з Windows 10X, зробивши інтерфейс сучаснішим і мінімалістичним. Нижче наведені конкретні нововведення, які були запозичені з Windows 10X і впроваджені в Windows 11:

1) Оновлений дизайн і інтерфейс:

– Меню «Пуск» стало простішим, без "живих плиток", з організованим розташуванням додатків та рекомендацій.

– Панель задач тепер має центроване розташування значків, що робить інтерфейс більш симетричним.

– Закруглені кути вікон додають м'якості та сучасного вигляду системі.

2) Центр повідомлень та швидкі налаштування:

– Об’єднані швидкі налаштування і центр повідомлень створюють зручний доступ до головних функцій, нагадуючи мобільний інтерфейс, як у Windows 10X.

3) Оптимізація під сенсорні пристрої:

– Покращення для сенсорного управління, зокрема зручні жести для навігації та адаптивний режим для роботи на планшетах.

4) Snap Layouts і Snap Groups:

– Функції Snap Layouts і Snap Groups полегшують організацію вікон і багатозадачність, що є розвитком ідей, закладених у Windows 10X.

5) Новий провідник та системні застосунки:

– Провідник отримав сучасний вигляд із простішим інтерфейсом, полегшуючи навігацію.

6) Фокус на безпеці та простоті:

– Більш ізольована система з покращеною безпекою, яка частково реалізує ідеї Windows 10X щодо ізоляції системних компонентів.

7) Інтеграція з Microsoft Teams:

– Чат Microsoft Teams інтегрований прямо на панель задач, полегшуючи комунікацію, як це планувалося в Windows 10X.

Таким чином, ідеї Windows 10X стали фундаментом для багатьох

покращень у Windows 11, підвищивши загальний рівень зручності, функціональності та безпеки для користувачів.

Порівняння з macOS та Chrome OS

Операційна система Windows є однією з найпопулярніших і найбільш використовуваних платформ у світі, що робить її важливою мішенню для кіберзлочинців. Microsoft інвестує значні ресурси в забезпечення безпеки Windows, впроваджуючи багатошарові механізми захисту, такі як Microsoft Defender Antivirus, BitLocker, Windows Defender System Guard, а також функції безпеки, що базуються на віртуалізації (VBS). Однак, незважаючи на ці досягнення, Windows має кілька вразливих місць, які відрізняють її від macOS і Chrome OS.

Переваги Windows у сфері безпеки полягають у її здатності інтегрувати передові технології, такі як віртуалізація, контроль облікових записів (UAC), шифрування дисків (BitLocker) та захист програм (Microsoft Defender Application Control). Ці функції забезпечують багатошаровий захист від сучасних загроз, таких як зловмисне ПЗ та атаки нульового дня. Крім того, Windows забезпечує велику гнучкість і підтримку широкого спектра апаратних платформ і корпоративного програмного забезпечення, що є ключовим чинником для багатьох організацій.

Втім, Windows стикається з рядом викликів, яких немає у macOS і Chrome OS. Основні з них пов'язані з сумісністю драйверів, широкою підтримкою різноманітного обладнання та необхідністю забезпечувати зворотну сумісність із більш ранніми версіями програмного забезпечення. Це призводить до складнощів у забезпеченні стабільності та безпеки системи, особливо в корпоративному середовищі, де використовуються різні моделі пристроїв одночасно. Крім того, вразливість Windows до шкідливих дій, таких як виконання команд на кшталт del C:\ /s /q /f або деструктивних команд у середовищах, як-от реєстр Windows чи Windows Subsystem for Linux (WSL), може призвести до серйозних пошкоджень операційної системи, що ускладнює її відновлення.

На відміну від Windows, macOS та Chrome OS побудовані з акцентом на обмежену кількість апаратних конфігурацій і використовують обмеженіші, але більш контрольовані середовища. Windows повинна забезпечувати підтримку максимальної сумісності з усіма типами апаратних та програмних компонентів, що значно збільшує поверхню атаки і вимагає постійного моніторингу та оновлення системи безпеки.

Таким чином, безпека Windows є потужною та багатошаровою, але залежить від великої кількості змінних, таких як сумісність драйверів, різноманітність апаратних конфігурацій та потреба у підтримці старих версій програмного забезпечення.

Ці фактори, хоча й роблять Windows універсальною та гнучкою платформою, також підвищують ризики, пов'язані з безпекою, порівняно з більш закритими та контрольованими екосистемами, такими як macOS та Chrome OS.

2.4. Огляд Ubuntu

Я вирішив дослідити, як операційна система Ubuntu захищає себе від дій користувача. Ubuntu – це безкоштовна операційна система з відкритим вихідним кодом, заснована на дистрибутиві Debian, розроблена компанією Canonical у співпраці з відкритою спільнотою. Її назва походить від африканського філософського поняття "убунту", що означає "людяність" або "я існую, бо існуємо ми". Вперше випущена у 2004 році, Ubuntu швидко стала однією з найпопулярніших операційних систем на базі GNU/Linux, пропонуючи простоту встановлення, регулярні оновлення та активну підтримку спільноти.

Архітектурно Ubuntu використовує монолітне ядро Linux, яке забезпечує управління основними функціями операційної системи: управління пам'яттю, процесами, файловими системами та пристроями введення-виведення. Хоча ядро є монолітним, Linux підтримує динамічне завантаження модулів (LKM), що надає йому певну гнучкість для розширення функціональності без перезавантаження системи.

Це відрізняє Ubuntu від Windows, яка використовує гібридне ядро NT, що поєднує елементи як монолітної, так і мікроядерної архітектур. Це забезпечує баланс між продуктивністю та модульністю, дозволяючи ядру NT підтримувати високу гнучкість і безпеку системи.

macOS базується на ядрі XNU, яке поєднує в собі два підходи: мікроядро Mach, що відповідає за низькорівневі операції (управління пам'яттю, процесами тощо), і модулі BSD, які реалізують функціональність на вищому рівні, зокрема підтримку файлових систем та мереж. Поєднання цих двох підходів дозволяє macOS зберігати гнучкість і продуктивність, характерні для традиційних UNIX-систем.

Chrome OS, також заснована на ядрі Linux, але зосереджується на забезпеченні максимальної безпеки та простоти використання. Chrome OS обмежує користувацький простір і активно використовує контейнеризацію та

технології ізоляції додатків (sandboxing), що значно зменшує ризики втручання користувача в системні процеси та підвищує захист.

Ubuntu дотримується філософії відкритого коду та свободи користувача. На відміну від Windows і macOS, де користувачі мають обмежені можливості змінювати системне середовище, Ubuntu дозволяє практично повністю налаштовувати систему відповідно до власних потреб. Chrome OS, хоча й базується на ядрі Linux, вводить суворі обмеження з метою забезпечення простоти використання та безпеки, але ці обмеження також знижують можливості налаштування системи.

Існує кілька основних версій Ubuntu, які використовують різні графічні оболонки [14]. Ubuntu Desktop із середовищем GNOME стала основною починаючи з версії 17.10, після відмови від Unity. Kubuntu використовує середовище KDE Plasma, Xubuntu – легке середовище XFCE для старіших комп'ютерів, Lubuntu – LXQt, Ubuntu MATE – середовище MATE, яке базується на старій версії GNOME 2, Ubuntu Budgie – середовище Budgie тощо. Також є серверні версії Ubuntu, які не включають графічного середовища і призначені для адміністрування через командний рядок.

Спочатку Ubuntu використовувала GNOME 2 як основне графічне середовище. У 2010 році компанія Canonical вирішила розробити власну оболонку Unity, щоб запропонувати більш інтегрований та сучасний інтерфейс. Проте Unity не отримала широкої підтримки спільноти, і в 2017 році Canonical оголосила про повернення до GNOME з версії 17.10. Сучасні версії Ubuntu використовують GNOME 3+ з деякими власними модифікаціями для покращення користувацького досвіду.

Ubuntu використовує дві основні технології для встановлення програмного забезпечення: apt (Advanced Package Tool) та snap. Apt – це класичний пакетний менеджер, який дозволяє встановлювати пакети з репозиторіїв, забезпечує контроль залежностей та автоматичне оновлення. Він є гнучким та надійним, але пакети apt залежать від загальної системи, що може призводити до проблем із сумісністю. Snap – це новий формат пакетів,

розроблений Canonical, який дозволяє пакувати додатки разом з усіма залежностями в один контейнер. Це забезпечує сумісність між різними версіями Ubuntu і навіть іншими дистрибутивами, але збільшує розмір пакетів та використання ресурсів. Snap-пакети часто працюють повільніше через додатковий рівень ізоляції.

Ubuntu Core Desktop

Ubuntu Core Desktop - новий експериментальний варіант Ubuntu, який використовує виключно snap-пакети для всіх програм і системних компонентів. Це спроба Canonical відійти від традиційної Debian-моделі управління пакетами. Такий підхід покращує безпеку та стабільність, ізолюючи додатки один від одного, але також викликає критику за відхід від відкритості та гнучкості, які є основою філософії Linux.

Ubuntu Core спочатку розроблявся у 2014 році як повністю контейнеризована платформа для Інтернету речей (IoT) [17]. Кожен компонент системи знаходиться у безпечному середовищі, що дозволяє виконувати автоматичні оновлення та відновлення без втручання користувача. Вона має мінімальний розмір і підходить для роботи в умовах, де важливі безпека і надійність.

Незмінна операційна система – це система, яку не можна змінити під час роботи. Вона має властивості атомарних оновлень, передбачуваності та ізоляції додатків. Такий підхід підвищує безпеку, стабільність, можливість відтворення системи та спрощує управління. Недоліками є знижена гнучкість, обмежена сумісність з деякими програмами та підвищені вимоги до зберігання даних.

Ubuntu Core використовує підхід контейнеризації, схожий на той, що застосовується в Chrome OS, Fedora Silverblue, openSUSE MicroOS та інших дистрибутивах. Замість того щоб розглядати всю операційну систему як один незмінний об'єкт, Ubuntu Core розділяє її на окремі компоненти. Це знижує навантаження на систему та дозволяє оновлювати компоненти без перезавантаження.

Для доставки оновлень Ubuntu Core використовує механізм каналів (стабільний, кандидат, бета, крайній), що дозволяє користувачам обирати рівень ризику. Це забезпечує гнучкість і можливість швидкого відновлення системи у разі проблем.

Хоча Ubuntu Core з незмінною основою може значно підвищити безпеку та стабільність для розробників і звичайних користувачів, такий рівень стабільності приходить із жертвами для тих, хто потребує відкритості і контролю над системою.

Безпека Ubuntu

Ubuntu має ряд технологій для захисту від помилкових дій користувачів. AppArmor - система мандатного контролю доступу, яка обмежує доступ до ресурсів для кожного процесу на основі профілів. Ufw (Uncomplicated Firewall) – простий у налаштуванні брандмауер для захисту системи від мережевих атак [16]. SELinux (Security-Enhanced Linux) використовується в деяких конфігураціях Ubuntu замість AppArmor, пропонуючи додатковий рівень контролю безпеки [15]. Однак Ubuntu не має таких жорстких обмежень, як macOS з SIP (System Integrity Protection) або Chrome OS з відсутністю повних прав адміністратора. Це надає користувачам більше свободи, але вимагає більшої обережності при роботі з системою.

Якщо в Ubuntu виконати команду sudo rm -rf /*, це призведе до видалення всіх файлів та директорій з кореневого каталогу, фактично знищуючи всю систему. Файли, що були відкриті на момент виконання команди і не були закриті процесами, можуть залишитися в оперативній пам'яті, але після перезавантаження вони будуть втрачені. Усі файли операційної системи, включаючи ядро, драйвери, конфігураційні файли та встановлене програмне забезпечення, будуть видалені, і система стане непридатною для роботи.

На відміну від Ubuntu, де такі дії можуть призвести до повної втрати працездатності системи, інші операційні системи мають вбудовані механізми захисту. Windows з WPF (Windows Protected Folders) обмежує доступ до

критичних системних файлів, macOS використовує SIP для захисту системних компонентів, а Chrome OS взагалі не надає повних прав адміністратора користувачеві, що робить такі команди неможливими.

Ubuntu не має вбудованого інструменту для скидання налаштувань до заводських, оскільки вона орієнтована на досвідчених користувачів, які можуть самостійно встановлювати та налаштовувати систему. Це дозволяє повністю контролювати середовище, але вимагає знань та досвіду для вирішення можливих проблем.

Гнучкість Ubuntu

Однією з найбільших переваг Ubuntu є можливість запуску системи в режимі Live CD, що дозволяє завантажити операційну систему з USB або CD без її встановлення на комп'ютер. Це дає змогу перевірити сумісність обладнання, виконати діагностику і навіть відновити файли з жорсткого диска в разі проблем з встановленою операційною системою.

Крім того, як і в Chrome OS або macOS, драйвери для більшості пристроїв автоматично встановлюються під час встановлення Ubuntu. Це спрощує процес встановлення в порівнянні з Windows, де часто потрібно завантажувати драйвери вручну. Ubuntu підтримує роботу на більшості апаратних конфігурацій, але, як і будь-яка інша універсальна операційна система, може мати проблеми з певним обладнанням або їх комбінаціями, які не сертифіковані під Linux.

Ubuntu – це справжня композиція відкритих технологій з усього світу, і користувачі мають можливість кастомізувати систему під себе. Вони можуть змінити графічне середовище (GNOME, KDE, XFCE, LXQt, MATE, Budgie тощо), замінити постачальника оновлень, встановити різні програми, змінити ядро Linux, налаштувати командний рядок, замінити завантажувач та систему ініціалізації.

Користувачі можуть кастомізувати вже зібрану Ubuntu за допомогою інструментів, таких як Cubic. Під капотом Cubic запускає середовище chroot, де можна змінювати файлову систему Ubuntu, додавати або видаляти пакети,

змінювати конфігурації та створювати новий завантажувальний образ. Наприклад, індійський школяр Рудра Сарасват повернув таким чином оточення Unity в Ubuntu замість стандартного GNOME, і Ubuntu Unity стала офіційним різновидом операційної системи від Canonical. Використовуючи власні скрипти, розробники Linux Mint замінили пакетний менеджер Snap на контрольований спільнотою вільного програмного забезпечення Flatpak та перейшли на використання своєї десктопної оболонки Cinnamon. Це дозволяє створити повністю налаштований дистрибутив, готовий до встановлення або використання в режимі Live CD. Для цього потрібні лише базові знання високорівневих мов, таких як Bash, а в особливо складних випадках – Python. Для внесення змін до Chrome OS потрібно мати детальні знання її архітектури і значно більше ресурсів, таких як потужний сервер для перекомпіляції коду.

На завершення, Ubuntu надає користувачам неймовірну гнучкість і свободу, але вимагає більшої відповідальності та обережності в роботі з системою. Це ідеальний вибір для тих, хто бажає повного контролю над своїм комп’ютером і не боїться експериментувати.

РОЗДІЛ 3
ПРОДУКТИВНІСТЬ ОПЕРАЦІЙНИХ СИСТЕМ

3.1. Вступ та методологія тестування

Продуктивність операційної системи безпосередньо впливає на її доступність, що є ключовим елементом інформаційної безпеки, як зазначено в тріаді конфіденційність, цілісність, доступність (CIA). Низька продуктивність може створити загрози безпеці, такі як простої системи або перебої в роботі, що може зробити її вразливою до атак або ускладнити своєчасне реагування на загрози.

Крім того, висока продуктивність зменшує ризики, пов'язані з людським фактором, оскільки збої та затримки можуть спричинити помилки користувачів. Наприклад, неправильні дії або несанкціоноване втручання можуть виникати через спроби оперативного усунення проблем. Це особливо актуально в критичних середовищах, де стабільність системи має вирішальне значення.

Тривале функціонування системи на межі її можливостей також може спричинити зношення обладнання, що загрожує доступності та стабільності. Отже, оптимізація продуктивності сприяє стабільності роботи та захищеності системи в цілому, і недооцінка цього фактору може мати серйозні наслідки.

Чим швидше система виконує завдання, навіть з підвищеним використанням ресурсів, тим менше часу вона навантажує ці ресурси. Це знижує загальне енергоспоживання і зменшує ризик зношення обладнання.

Мета дослідження. Ми поставили за мету протестувати продуктивність різних операційних систем: Crostini (у Chrome OS Flex), Ubuntu, macOS та Windows Subsystem for Linux 2 (WSL 2). Для отримання комплексної оцінки продуктивності ми обрали як процесорні тести, так і тести вбудованої відеокарти.

Вибір інструменту для тестування. Для проведення тестів я обрав

Geekbench, одну з найпопулярніших та найрозвинутіших програм для такого типу тестування. Вибір Geekbench обумовлений його здатністю забезпечити стандартизовані та повторювані результати, що охоплюють широкий спектр завдань, від базових обчислень до складних графічних операцій. Крім того, Geekbench підтримує багатоплатформність, що дозволяє коректно порівнювати результати між різними операційними системами.

Методологія тестування.

- Чисте середовище: Для забезпечення максимальної чистоти експерименту, я встановлював офіційні образи кожної операційної системи на повністю відформатований жорсткий диск. Це дозволяло уникнути впливу стороннього програмного забезпечення та залишкових даних від попередніх встановлень.
- Один запуск тесту: Кожен тест у Geekbench я запускав один раз для кожної операційної системи. Geekbench автоматично виконує серію підтестів у рамках одного запуску, що дозволяє отримати усереднений результат без необхідності додаткових повторів.
- Контроль умов тестування: Під час проведення тестів я стежив за тим, щоб на системі не працювали інші ресурсоємні процеси. Були встановлені останні оновлення ОС, вимкнені хмарні сервіси синхронізації та інші додатки, які могли б вплинути на результати.
- Обробка можливих відхилень: Якщо під час тестування я спостерігав би значні відхилення або аномалії в результатах (що могло б вказувати на збої чи сторонній вплив), я би повторили тестування для підтвердження результатів. Проте в цьому випадку результати були стабільними та не вимагали додаткових повторів.

Чому я не виконував кілька запусків? Geekbench спроектований таким чином, що один запуск тесту містить множинні підзадачі, результати яких усереднюються для отримання фінального балу. Це зменшує вплив випадкових коливань продуктивності та забезпечує достовірність даних. Тому я вважав достатнім виконувати по одному запуску для кожної системи.

Дотримуючись описаної методології, я отримав надійні та порівнювані результати продуктивності для кожної операційної системи. Це дозволило мені зробити обґрунтовані висновки щодо їх ефективності та впливу на інформаційну безпеку через призму доступності та стабільності роботи.

3.2. Метрики продуктивності

File Compression – тестує здатність процесора стискати файли.
Navigation – оцінює швидкість навігації в інтерфейсі.
HTML5 Browser – продуктивність рендерингу веб-сторінок.
Clang – швидкість компіляції за допомогою Clang.
Object Detection – розпізнавання об'єктів на зображеннях.
Structure from Motion – обчислення 3D-структур з відео.
Background Blur – здатність розмивати фон.
Face Detection – розпізнавання облич на зображеннях.
Horizon Detection – виявлення горизонтів на зображеннях.
Edge Detection – виявлення контурів об'єктів.
Gaussian Blur – застосування гауссового розмиття.
Feature Matching – співставлення особливостей між зображеннями.
Stereo Matching – співставлення стереозображень для 3D-сцен.
Particle Physics – обчислення фізики частинок.
Ray Tracer – рендеринг із трасуванням променів.
PDF Renderer – рендеринг PDF-документів.
Text Processing – обробка великих обсягів тексту.
Photo Library – продуктивність у роботі з бібліотеками фото.
Asset Compression – стиск мультимедійних активів.
Object Remover – видалення об'єктів із зображень.
HDR – обробка зображень із високим динамічним діапазоном.
Photo Filter – застосування фільтрів до зображень.
FPS (Frames Per Second) – кількість кадрів за секунду для плавної анімації.

Bare Metal – архітектура безпосередньо на фізичному обладнанні.

Single-Core – обробка даних одним ядром.

Multi-Core – обробка даних кількома ядрами для паралельних задач.

3.3. Підготовка середовища до тестування

Тестування проводилося на MacBook Pro (13 дюймів, середина 2018 року) з процесором Intel Core i7-8559U, 16 ГБ оперативної пам'яті DDR3 SDRAM та інтегрованою графікою Intel Iris Plus Graphics 655. Ця конфігурація використовувалася для оцінки загальної продуктивності системи в різних сценаріях обробки даних та графіки.

Сумісність обладнання:

- macOS: ідеальна підтримка обладнання “з коробки”.
- Windows 10 22H2 (через Boot Camp): Сумісність обладнання зберігалася на високому рівні. Однак, тачбар має фіксовані віртуальні кнопки F і вже не настільки інтерактивний як на macOS.
- Windows 11 24H2: Для оновлення Intel MacBook з Boot Camp-версії Windows 10 до Windows 11, оскільки пряма установка Windows 11 не рекомендується через проблеми з клавіатурою, Touch Bar і тачпадом “з коробки”, я скористався скриптом MediaCreationTool.bat. Основною особливістю цього рішення є можливість динамічного відключення перевірки на наявність TPM (Trusted Platform Module), що необхідно, адже MacBook офіційно несумісний з Windows 11 через відсутність цього модуля. Під час використання скрипта TPM-перевірка відключається за допомогою модифікації параметрів установки безпосередньо в процесі оновлення. Це дозволяє обійти апаратні обмеження та інсталювати операційну систему на пристрої, що не відповідає мінімальним вимогам Windows 11. Варто зазначити, що мій MacBook має достатньо оперативної пам’яті, SSD та процесор Intel 8-го покоління, що дозволяє йому стабільно працювати на Windows 11,

незважаючи на відсутність TPM. Після оновлення клавіатура, Touch Bar і тачпад все одно не працювали після виходу з режиму гібернації. Для реініціалізації обладнання доводилося перезавантажувати комп'ютер. Для усунення цієї проблеми я встановив відповідні драйвери з Інтернету, після чого клавіатура і тачпад почали працювати належним чином. Однак Touch Bar продовжував періодично давати збої після виходу з режиму гібернації, що вимагало подальшого втручання. Незважаючи на ці труднощі, решта компонентів системи працюють стабільно, що дозволяє використовувати Windows 11 на MacBook з належною продуктивністю.

– Ubuntu: Touch Bar та Touchpad не працювали взагалі, що вимагало використання зовнішніх пристроїв введення. Також клавіатура не працювала, що додатково ускладнювало використання системи. Довелося використовувати зовнішню клавіатуру та мишу.

Проблеми з установкою Chrome OS Flex. Спроби встановити Chrome OS Flex на MacBook Pro 2018 виявилися невдалими. Це відповідає офіційній документації, яка зазначає, що пристрої Mac з Touch Bar, чипом безпеки T2 або процесором Apple Silicon не підтримуються і можуть мати серйозні помилки, навіть якщо вони працюють. Однак проблеми із встановленням на більш застарілі Mac на базі процесорів Intel не повинні виникати.

3.4. Аналіз результатів тестів Geekbench

Нещодавно ми провели серію тестів за допомогою Geekbench 6.3, щоб оцінити продуктивність різних операційних систем на однаковому апаратному забезпеченні. Тестувалися Windows 11 24H2, macOS 15, Ubuntu 24.04 (на голому залізі) та Ubuntu 24.04 у середовищі WSL 2.

Результати тестів показують, що вибір операційної системи може суттєво вплинути на продуктивність у різних задачах. Windows 11 демонструє сильні сторони у багатоядерних та фізичних обчисленнях. macOS

завдяки Metal API лідирує у графічних задачах та обробці зображень. Ubuntu на голому залізі показує конкурентну продуктивність у багатьох тестах, особливо у веб-рендерингу та компіляції коду, що робить її відмінним вибором для розробників та користувачів, які цінують відкриті системи.

WSL 2, хоча і відстає в графічних метриках, демонструє гідну продуктивність у процесорних задачах, що робить її корисною для розробників, які працюють у Windows, але потребують Linux-середовища.

CPU-тести Windows, Ubuntu, WSL 2 та macOS

Таблиця 3.4

Порівняння процесорної Geekbench-продуктивності ОС на пристрої Apple

Метрика	Windows 11 24H2	Ubuntu 24.04 WSL2	Ubuntu 24.04 Bare Metal	macOS 15
1	2	3	4	5
Single-Core	1517	1503	1527	1458
Multi-Core	4934	4687	4876	4755
File Compression (Single-Core)	1444 (207.3 МБ/сек)	1136 (163.2 МБ/сек)	1413 (202.9 МБ/сек)	1376 (197.7 МБ/сек)
File Compression (Multi-Core)	3607 (518.0 МБ/сек)	3091 (443.8 МБ/сек)	3367 (483.5 МБ/сек)	3454 (496.0 МБ/сек)
Navigation (Single-Core)	1705 (10.3 маршрутів/сек)	1494 (9.00 маршрутів/сек)	1670 (10.1 маршрутів/сек)	1538 (9.27 маршрутів/сек)
Navigation (Multi-Core)	7680 (46.3 маршрутів/сек)	7193 (43.3 маршрутів/сек)	7091 (42.7 маршрутів/сек)	7101 (42.8 маршрутів/сек)
HTML5 Browser (Single-Core)	1593 (32.6 стор./сек)	1698 (34.8 стор./сек)	1721 (35.2 стор./сек)	1494 (30.6 стор./сек)
HTML5 Browser (Multi-Core)	5900 (120.8 стор./сек)	5782 (118.4 стор./сек)	6106 (125.0 стор./сек)	5525 (113.1 стор./сек)
PDF Renderer (Single-Core)	1626 (37.5 Мпікселів/сек)	1677 (38.7 Мпікселів/сек)	1605 (37.0 Мпікселів/сек)	1646 (38.0 Мпікселів/сек)

Продовження таблиці 3.4

1	2	3	4	5
PDF Renderer (Multi-Core)	6719 (155.0 Мпікселів/сек)	6015 (138.7 Мпікселів/сек)	6078 (140.2 Мпікселів/сек)	6151 (141.9 Мпікселів/сек)
Photo Library (Single-Core)	1313 (17.8 зобр./сек)	1232 (16.7 зобр./сек)	1248 (16.9 зобр./сек)	1264 (17.1 зобр./сек)
Photo Library (Multi-Core)	4490 (60.9 зобр./сек)	4410 (59.8 зобр./сек)	4508 (61.2 зобр./сек)	4580 (62.2 зобр./сек)
Clang (Single-Core)	1726 (8.50 Клінiй/сек)	1893 (9.32 Клінiй/сек)	1906 (9.39 Клінiй/сек)	1708 (8.41 Клінiй/сек)
Clang (Multi-Core)	5722 (28.2 Клінiй/сек)	5555 (27.4 Клінiй/сек)	5961 (29.4 Клінiй/сек)	5507 (27.1 Клінiй/сек)
Text Processing (Single-Core)	1493 (119.5 стор./сек)	1549 (124.0 стор./сек)	1519 (121.6 стор./сек)	1469 (117.6 стор./сек)
Text Processing (Multi-Core)	1800 (144.1 стор./сек)	1763 (141.2 стор./сек)	1807 (144.7 стор./сек)	1671 (133.9 стор./сек)
Asset Compression (Single-Core)	1455 (45.1 МБ/сек)	1515 (47.0 МБ/сек)	1515 (46.9 МБ/сек)	1499 (46.4 МБ/сек)
Asset Compression (Multi-Core)	6065 (187.9 МБ/сек)	6453 (199.9 МБ/сек)	6102 (189.1 МБ/сек)	5440 (168.6 МБ/сек)
Object Detection (Single-Core)	717 (21.5 зобр./сек)	712 (21.3 зобр./сек)	707 (21.1 зобр./сек)	721 (21.6 зобр./сек)
Object Detection (Multi-Core)	2261 (67.7 зобр./сек)	2188 (65.5 зобр./сек)	2200 (65.8 зобр./сек)	2149 (64.3 зобр./сек)
Background Blur (Single-Core)	2210 (9.15 зобр./сек)	2293 (9.49 зобр./сек)	2271 (9.40 зобр./сек)	2223 (9.20 зобр./сек)
Background Blur (Multi-Core)	5953 (24.6 зобр./сек)	4749 (19.7 зобр./сек)	6127 (25.4 зобр./сек)	5916 (24.5 зобр./сек)
Horizon Detection (Single-Core)	1987 (61.8 Мпікселів/сек)	2056 (64.0 Мпікселів/сек)	2006 (62.4 Мпікселів/сек)	1986 (61.8 Мпікселів/сек)

Продовження таблиці 3.4

1	2	3	4	5
Horizon Detection (Multi-Core)	8023 (249.7 Мпікселів/сек)	6672 (207.6 Мпікселів/сек)	7744 (241.0 Мпікселів/сек)	7974 (248.1 Мпікселів/сек)
Object Remover (Single-Core)	1363 (104.8 Мпікселів/сек)	1263 (97.1 Мпікселів/сек)	1274 (97.9 Мпікселів/сек)	1089 (83.7 Мпікселів/сек)
Object Remover (Multi-Core)	5360 (412.1 Мпікселів/сек)	4630 (356.0 Мпікселів/сек)	5054 (388.5 Мпікселів/сек)	5133 (394.7 Мпікселів/сек)
HDR (Single-Core)	1611 (47.3 Мпікселів/сек)	1619 (47.5 Мпікселів/сек)	1606 (47.1 Мпікселів/сек)	1560 (45.8 Мпікселів/сек)
HDR (Multi-Core)	5415 (158.9 Мпікселів/сек)	5255 (154.2 Мпікселів/сек)	5055 (148.3 Мпікселів/сек)	5369 (157.5 Мпікселів/сек)
Photo Filter (Single-Core)	1869 (18.5 зобр./сек)	1834 (18.2 зобр./сек)	1659 (16.5 зобр./сек)	1518 (15.1 зобр./сек)
Photo Filter (Multi-Core)	4943 (49.0 зобр./сек)	4998 (49.6 зобр./сек)	4998 (49.6 зобр./сек)	4777 (47.4 зобр./сек)
Ray Tracer (Single-Core)	1404 (1.36 Мпікселів/сек)	1442 (1.40 Мпікселів/сек)	1518 (1.47 Мпікселів/сек)	1402 (1.36 Мпікселів/сек)
Ray Tracer (Multi-Core)	6455 (6.25 Мпікселів/сек)	6750 (6.53 Мпікселів/сек)	7183 (6.95 Мпікселів/сек)	6672 (6.46 Мпікселів/сек)
Structure from Motion (Single-Core)	1843 (58.3 Кпікселів/сек)	1951 (61.8 Кпікселів/сек)	1912 (60.6 Кпікселів/сек)	1835 (58.1 Кпікселів/сек)
Structure from Motion (Multi-Core)	5999 (189.9 Кпікселів/сек)	6431 (203.6 Кпікселів/сек)	6304 (199.6 Кпікселів/сек)	6544 (207.2 Кпікселів/сек)

Ubuntu 24.04 на «голому залізі» показала найвищу продуктивність в однопотокових задачах, набравши 1527 балів – на 0,7% більше, ніж у Windows 11, і на 4,7% вище, ніж у macOS 15. Цікаво, що Ubuntu у WSL 2 відстала лише на 1,6%, що свідчить про високу ефективність паравіртуалізації. У багатопотокових тестах Windows 11 стала лідером з 4934 балами, випередивши Ubuntu на 1,2% і macOS на 3,8%. WSL 2 відстала на 5%, але показала конкурентну продуктивність у багатозадачних

середовищах.

У компресії файлів Windows 11 лідирує в однопотоковому режимі з 1444 балами (207,3 Мегабайт/сек), а Ubuntu на «голому залізі» відстала лише на 2,1%. У багатопотоковому режимі Windows зберегла перевагу з 3607 балами, але різниця з macOS 15 і Ubuntu була незначною. WSL 2 відставала, що можна пояснити обмеженнями віртуалізації. У навігаційних завданнях Windows 11 лідирує з 1705 балами, а Ubuntu відстала лише на 2%. В багатопотокових навігаційних тестах Windows теж була попереду, а WSL 2 продемонструвала конкурентоспроможність, підтверджуючи ефективність віртуалізованого середовища.

В тестах рендерингу HTML5 браузер Ubuntu на «голому залізі» випередила Windows на 8%, а WSL 2 також обійшла Windows, підкреслюючи ефективність Ubuntu у веб-завданнях. У багатопотоковому режимі Ubuntu утримала першість. В тестах PDF-рендерингу WSL 2 лідирувала з результатом, що випередив Windows і macOS. У багатопотоковому режимі Windows перевершила суперників, показавши високі показники обробки PDF-файлів.

У тестах бібліотеки зображень Windows 11 очолила список, тоді як macOS лідирувала в багатопотоковому режимі, перевершуючи Ubuntu і Windows. В компіляції коду Ubuntu показала найвищу продуктивність як в однопотоковому, так і в багатопотоковому режимах. В обробці тексту WSL 2 лідирувала, залишивши позаду Ubuntu та Windows в однопотокових задачах, а в багатопотокових – Ubuntu досягла найвищого результату.

WSL 2 показала високі результати у компресії активів в однопотоковому режимі, тоді як у багатопотоковому режимі також стала лідером, випередивши Ubuntu і Windows. В задачах комп'ютерного зору macOS мала незначну перевагу, а в багатопотокових тестах Windows лідирувала з невеликим відривом від Ubuntu і WSL 2. У тестах розмиття фону WSL 2 показала найкращий результат в однопотоковому режимі, а в багатопотоковому режимі лідером була Ubuntu.

Тест на виявлення горизонту показав перевагу WSL 2 в однопотоковому режимі, тоді як Windows лідирувала в багатопотоковому. У видаленні об'єктів Windows 11 очолила однопотоковий режим, а в багатопотоковому знову стала лідером, обігнавши macOS та Ubuntu. В тестах HDR-обробки WSL 2 була кращою в однопотоковому режимі, а Windows 11 лідирувала в багатопотоковому. У застосуванні фотофільтрів Windows 11 мала найвищий результат в однопотокових задачах, а WSL 2 та Ubuntu розділили перше місце в багатопотокових.

У рейтрейсингу Ubuntu продемонструвала найвищу продуктивність, особливо в багатопотоковому режимі, де значно випередила інших. В задачах 3D-реконструкції WSL 2 показала найкращий результат в однопотоковому режимі, тоді як macOS лідирувала в багатопотоковому.

GPU-тести Windows, Ubuntu, WSL 2 та macOS

Таблиця 3.5

Порівняння графічної Geekbench-продуктивності ОС на пристрої Apple

Метріка	Windows 11 24H2 Vulkan	Windows 11 24H2 OpenCL	macOS 15 Metal	macOS 15 OpenCL	Ubuntu 24.04 Vulkan Bare Metal	Ubuntu 24.04 Vulkan WSL
1	2	3	4	5	6	7
Оцінка	8951	8033	10114	7588	7175	221
Background Blur	3978 16.5 зобр./сек	3844 15.9 зобр./сек	4272 17.7 зобр./сек	3424 14.2 зобр./сек	4541 18.8 зобр./сек	96 0.40 зобр./сек
Face Detection	2592 8.46 зобр./сек	3445 11.2 зобр./сек	4281 14.0 зобр./сек	2884 9.42 зобр./сек	2709 8.84 зобр./сек	69 0.23 зобр./сек
Horizon Detection	12709 395.5 Мегапікселів/сек	7393 230.1 Мегапікселів/сек	9882 307.5 Мегапікселів/сек	10245 318.8 Мегапіксекслів/сек	9640 300.0 Мегапікселів/сек	446 13.9 Мегапікселів/сек
Edge Detection	10532 390.7 Мегапікселів/сек	9821 364.3 Мегапікселів/сек	11041 409.6 Мегапікселів/сек	10174 377.4 Мегапікселів/сек	10964 406.7 Мегапікселів/сек	505 18.7 Мегапікселів/сек

Продовження таблиці 3.5

1	2	3	4	5	6	7
Gaussian Blur	10482 456.7 Мегапікселів/сек	6316 275.2 Мегапікселів/сек	12580 548.1 Мегапікселів/сек	6126 266.9 Мегапікселів/сек	5888 256.6 Мегапікселів/сек	242 10.6 Мегапікселів/сек
Feature Matching	2939 115.8 Мегапікс./сек	2780 109.6 Мегапікс./сек	4020 158.5 Мегапікс./сек	2895 114.1 Мегапікс./сек	1503 59.2 Мегапікс./сек	63 2.47 Мегапікс./сек
Stereo Matching	32470 30.9 Гігапікс./сек	34518 32.8 Гігапікс./сек	42531 40.4 Гігапікс./сек	24629 23.4 Гігапікс./сек	34095 32.4 Гігапікс./сек	674 641.1 Мегапікс./сек
Particle Physics	29855 1314.0 FPS	29751 1309.4 FPS	25503 1122.4 FPS	24447 1075.9 FPS	17899 787.8 FPS	368 16.2 FPS

У задачі розмиття фону перше місце зайняла Ubuntu на «голому залізі» з API Vulkan, досягнувши 4541 бала (18,8 зобр./сек), що перевершує macOS 15 з Metal на 6,3% та Windows 11 з Vulkan на 14,1%. Такий результат підкреслює ефективність використання Vulkan API на платформі Linux у завданнях обробки зображень.

У розпізнаванні облич лідером виявилася macOS 15 з Metal, отримавши 4281 бал (14,0 зобр./сек), що значно перевищує показники Windows 11 з OpenCL (3445 балів, 11,2 зобр./сек) і Ubuntu на «голому залізі» (2709 балів, 8,84 зобр./сек), демонструючи високий рівень оптимізації Metal API для таких задач.

Windows 11 з Vulkan показала найвищий результат у виявленні горизонту, набравши 12709 балів (395,5 Мегапікс./сек), що на 28,6% більше за macOS 15 з OpenCL та на 31,8% більше за Ubuntu на «голому залізі». Така перевага, ймовірно, пояснюється специфічними оптимізаціями драйверів Windows для графічних операцій на основі Vulkan.

У тесті на виявлення країв macOS 15 з Metal трохи перевершила Ubuntu на «голому залізі» з результатами 11041 та 10964 бали відповідно, де різниця між macOS і Windows (Vulkan) склала лише 4,8% (Windows набрала 10532

бали).

В задачах розмиття за Гаусом лідерство належить macOS 15 з Metal, яка набрала 12580 балів (548,1 Мегапікс./сек), перевершивши Windows 11 з Vulkan на 20% та Ubuntu на «голому залізі» на значні 113,7%, що підтверджує ефективність Metal API у подібних графічних задачах.

У співставленні ознак macOS 15 з Metal обігнала Windows 11 з Vulkan на 36,7%, набравши 4020 балів (158,5 Мегапікс./сек) проти 2939 балів у Windows, тоді як Ubuntu на «голому залізі» відстала від Windows на 48,9%, що свідчить про потребу в додаткових оптимізаціях Vulkan на Linux.

У тесті стерео-відповідності лідером стала macOS 15 з Metal з результатом 42531 бал (40,4 Гігапікс./сек). Ubuntu на «голому залізі» випередила Windows 11 з Vulkan на 5%, досягнувши 34095 балів (32,4 Гігапікс./сек) проти 32470 балів у Windows, що демонструє конкурентоспроможність Ubuntu у цій категорії.

У симуляції частинок Windows 11 з Vulkan стала беззаперечним лідером, набравши 29855 балів (1314,0 FPS), що на 17,1% перевищує результат macOS 15 з Metal. Ubuntu на «голому залізі» відстала на 29,8%, можливо, через кращу оптимізацію драйверів Windows для фізичних розрахунків.

Тестування на HP Pavilion Laptop 15-eh1xxx: детальний порівняльний аналіз усіх метрик. Через обмеження на встановлення Chrome OS Flex на MacBook, додаткове тестування було проведено на ноутбуці HP Pavilion Laptop 15-eh1xxx з процесором AMD Ryzen 7 5700U (8 ядер, 16 потоків), інтегрованою графікою AMD Radeon RX Vega 8 та 8 ГБ оперативної пам’яті. Метою тесту було порівняти продуктивність Debian GNU/Linux 12 на «голому залізі» з оточенням GNOME та у віртуальному середовищі Crostini на Chrome OS Flex.

Для запуску тестів на Chrome OS довелося виконати додаткові кроки: надати файлам тестів необхідні дозволи командою chmod +rwx та встановити пакет vulkan-tools для проходження тестів GPU, незважаючи на відсутність

підтримки апаратного прискорення графіки.

Одним із можливих рішень могло б бути використання кастомного контейнера з підтримкою Vulkan, як-от Arch Linux, подібного до Borealis (Steam Beta для Chrome OS). Однак цей метод є складним, не підтримується офіційно та не є доступним «з коробки», тому нижче наведено результати стандартного контейнера Crostini та Debian на «голому залізі».

За результатами тестів CPU, продуктивність Crostini наближається до нативного Debian з відставанням 3–7%. У однопотокових задачах відставання було меншим, ніж у багатопотокових, де досягало до 18%.

Щодо GPU, Crostini продемонстрував значне відставання в межах 94–99% у графічних тестах, що робить його непридатним для ресурсомістких графічних задач.

CPU-тести Debian Single-Core

Таблиця 3.6

Порівняння однопотокової процесорної Geekbench-продуктивності Debian на пристрої HP

Метрика	Debian 11 (Bare Metal)	Debian 11 на Crostini	Відставання Crostini (%)
1	2	3	4
Загальний бал	1708	1648	-3,5%
File Compression	1783 (256.0 Мегабайт/сек)	1670 (239.8 Мегабайт/сек)	-6,3%
Navigation	1799 (10.8 маршрути/сек)	1620 (9.76 маршрути/сек)	-9,9%
HTML5 Browser	1612 (33.0 стор./сек)	1577 (32.3 стор./сек)	-2,2%
PDF Renderer	1707 (39.4 Мегапікс./сек)	1714 (39.5 Мегапікс./сек)	+0,4%
Photo Library	1552 (21.1 зобр./сек)	1534 (20.8 зобр./сек)	-1,2%
Clang	1863 (9.18 Кілоряд/сек)	1826 (8.99 Кілоряд/сек)	-2,0%
Text Processing	1569 (125.6 стор./сек)	1562 (125.1	-0,4%

		стор./сек)	

Продовження таблиці 3.6

1	2	3	4
Asset Compression	1856 (57.5 Мегабайт/сек)	1845 (57.2 Мегабайт/сек)	-0,6%
Object Detection	927 (27.7 зобр./сек)	900 (26.9 зобр./сек)	-2,9%
Background Blur	2390 (9.89 зобр./сек)	2336 (9.67 зобр./сек)	-2,3%
Horizon Detection	2369 (73.7 Мегапікс./сек)	2300 (71.6 Мегапікс./сек)	-2,9%
Object Remover	1362 (104.7 Мегапікс./сек)	1240 (95.3 Мегапікс./сек)	-9,0%
HDR	1749 (51.3 Мегапікс./сек)	1652 (48.5 Мегапікс./сек)	-5,5%
Photo Filter	2038 (20.2 зобр./сек)	1839 (18.2 зобр./сек)	-9,8%
Ray Tracer	1804 (1.75 Мегапікс./сек)	1787 (1.73 Мегапікс./сек)	-0,9%
Structure from Motion	1987 (62.9 Кілопікс./сек)	1955 (61.9 Кілопікс./сек)	-1,6%

Аналіз: У більшості однопотокових метрик Crostini відстає від нативного Debian на 2-6%, що є незначним відставанням. Тест PDF Renderer навіть показав невелике покращення в Crostini (+0,4%).

CPU-тести Debian Multi-Core

Таблиця 3.7

Порівняння багатопотокової процесорної Geekbench-продуктивності Debian на пристрої HP

Метрика	Debian 11 (Bare Metal)	Debian 11 на Crostini	Відставання Crostini (%)
1	2	3	4
Загальний бал	7068	6561	-7,2%

File Compression	3656 (525.0 Мегабайт/сек)	3464 (497.5 Мегабайт/сек)	-5,3%

Продовження таблиці 3.7

1	2	3	4
Navigation	9013 (54.3 маршрут/сек)	7352 (44.3 маршрут/сек)	-18,4%
HTML5 Browser	7286 (149.2 pages/сек)	6787 (138.9 pages/сек)	-6,9%
PDF Renderer	9651 (222.6 Мегапікс./сек)	9305 (214.6 Мегапікс./сек)	-3,6%
Photo Library	8245 (111.9 зобр./сек)	7968 (108.1 зобр./сек)	-3,4%
Clang	12016 (59.2 Кілоряд/сек)	10968 (54.0 Кілоряд/сек)	-8,7%
Text Processing	1877 (150.3 pages/сек)	1641 (131.4 pages/сек)	-12,6%
Asset Compression	13242 (410.3 Мегабайт/сек)	13015 (403.3 Мегабайт/сек)	-1,7%
Object Detection	3150 (94.3 зобр./сек)	3066 (91.8 зобр./сек)	-2,7%
Background Blur	7710 (31.9 зобр./сек)	7587 (31.4 зобр./сек)	-1,6%
Horizon Detection	10182 (316.8 Мегапікс./сек)	9713 (302.2 Мегапікс./сек)	-4,6%
Object Remover	7701 (592.1 Мегапікс./сек)	6387 (491.0 Мегапікс./сек)	-17,0%
HDR	7256 (212.9 Мегапікс./сек)	6745 (197.9 Мегапікс./сек)	-7,0%
Photo Filter	5032 (49.9 зобр./сек)	4352 (43.2 зобр./сек)	-13,5%
Ray Tracer	15871 (15.4 Мегапікс./сек)	15541 (15.0 Мегапікс./сек)	-2,1%
Structure from Motion	9187 (290.9 Кілопікс./сек)	8864 (280.7 Кілопікс./сек)	-3,5%

Аналіз: У багатопотокових задачах відставання Crostini дещо більше, особливо в метриках Navigation (-18,4%) та Object Remover (-17,0%). Це може бути пов'язано з особливостями віртуалізації та розподілу ресурсів між ядрами.

GPU Тести Debian: Vulkan Продуктивність

Таблиця 3.8

Порівняння графічної Geekbench-продуктивності Debian на пристрої HP

Метрика	Debian 11 (Bare Metal)	Debian 11 на Crostini	Відставання Crostini (%)
Загальний бал	17149	337	-98%
Background Blur	8401 (34.8 зобр./сек)	131 (0.54 зобр./сек)	-98,4%
Face Detection	5031 (16.4 зобр./сек)	79 (0.26 зобр./сек)	-98,4%
Horizon Detection	15125 (470.7 Мегапікс./сек)	769 (23.9 Мегапікс./сек)	-94,9%
Edge Detection	20794 (771.4 Мегапікс./сек)	912 (33.8 Мегапікс./сек)	-95,6%
Gaussian Blur	24956 (1.09 Гігапікс./сек)	392 (17.1 Мегапікс./сек)	-98,4%
Feature Matching	5665 (223.3 Мегапікс./сек)	102 (4.01 Мегапікс./сек)	-98,2%
Stereo Matching	62990 (59.9 Гігапікс./сек)	1023 (972.8 Мегапікс./сек)	-98,4%
Particle Physics	63200 (2781.5 FPS)	566 (24.9 FPS)	-99,1%

Аналіз: GPU продуктивність у Crostini значно відстає від нативного середовища, з відставанням у 94-99% у всіх метриках. Це обумовлено відсутністю апаратного прискорення графіки у віртуальному середовищі Crostini.

Рекомендації:

– Процесорні задачі: Crostini та WSL можна використовувати для Linux-середовищ з мінімальним впливом на продуктивність.

– Графічні задачі: Віртуалізація призводить до підвищеного енергоспоживання та нагрівання, тому краще використовувати нативні системи, такі як Debian або Ubuntu, для забезпечення максимальної ефективності.

Порівняння операційних систем:

– macOS виявляється беззаперечним переможцем завдяки найвищій загальній продуктивності, особливо у графічних задачах, завдяки використанню Metal API.

– Windows 11 демонструє чудові результати у тестах на процесорну продуктивність (CPU).

– Ubuntu 24.04 є відмінною відкритою альтернативою на "голому залізі".

– Chrome OS Flex підходить для легких завдань, але обмежена через відсутність графічного прискорення.

Важливі зауваження: Apple вже перейшла на власні пропрієтарні чипи Apple Silicon, що незабаром призведе до завершення функціональних оновлень для Mac на базі Intel. Microsoft не планує адаптувати Windows під нову платформу Apple, зосереджуючи співпрацю з Qualcomm, Intel та AMD. Chrome OS Flex підтримує лише процесори Intel та AMD. Ubuntu потенційно може бути адаптована під нові Mac, але з певною затримкою.

У найближчі роки доведеться порівнювати не лише операційні системи, а й цілі програмно-апаратні комплекси.

Посилання на результати тестів

1) Windows 11 24H2 GPU (Vulkan): https://browser.geekbench.com/v6/compute/2796634

2) Windows 11 24H2 GPU (OpenCL): https://browser.geekbench.com/v6/compute/2785078

3) macOS 15 GPU (Metal): https://browser.geekbench.com/v6/compute/2796702

4) macOS 15 GPU (OpenCL): https://browser.geekbench.com/v6/compute/2765709

5) Ubuntu 24.04 Bare Metal GPU (Vulkan): https://browser.geekbench.com/v6/compute/2799882

6) Windows 11 24H2 WSL 2 GPU (Vulkan): https://browser.geekbench.com/v6/compute/2792812

7) Windows 11 24H2 CPU: https://browser.geekbench.com/v6/cpu/7861464

8) macOS 15 CPU: https://browser.geekbench.com/v6/cpu/7802217

9) Ubuntu 24.04 Bare Metal CPU: https://browser.geekbench.com/v6/cpu/7903554

10) Ubuntu 24.04 WSL 2 CPU: https://browser.geekbench.com/v6/cpu/7895199

11) HP Pavilion Debian 11 Bare Metal CPU: https://browser.geekbench.com/v6/cpu/7917798

12) HP Pavilion Debian 11 Bare Metal GPU: https://browser.geekbench.com/v6/compute/2805058

13) HP Pavilion Debian 11 на Chrome OS Flex CPU: https://browser.geekbench.com/v6/cpu/7918495

14) HP Pavilion Debian 11 на Chrome OS Flex GPU: https://browser.geekbench.com/v6/compute/2805845

РОЗДІЛ 4
ІНТЕГРАЦІЯ ОС З КОРПОРАТИВНИМ ПЗ

4.1. Інтеграція Windows з доменними технологіями Microsoft

У сучасному корпоративному світі інформаційні технології стали основою всіх бізнес-процесів. Ефективна робота корпоративних доменних структур дозволяє централізовано керувати пристроями, користувачами та доступом до ресурсів. Інтеграція операційної системи Windows з корпоративними доменами є важливим елементом ефективного управління IT-інфраструктурою.

Active Directory (AD) та Microsoft Entra ID (раніше відомий під назвою Azure Active Directory) стали де-факто стандартами в корпоративному середовищі. Завдяки глибокій інтеграції з Windows, вони надають широкі можливості управління безпекою та підтримують гібридні рішення, які поєднують переваги локальної інфраструктури та хмарних технологій.

Розглянемо локальні, гібридні та хмарні сценарії інтеграції з використанням Active Directory та Microsoft Entra ID, а також технології управління пристроями, такі як Microsoft Intune. Проаналізуємо переваги та недоліки кожного підходу та надамо рекомендації щодо вибору оптимального варіанту для бізнесу.

Active Directory

Active Directory (AD) – це служба каталогів Microsoft, яка використовується для управління користувачами, пристроями та ресурсами в корпоративній мережі. Вона дозволяє централізовано адмініструвати доступ до систем, забезпечуючи автентифікацію та авторизацію користувачів і пристроїв. Традиційно AD використовується в локальних корпоративних мережах і є важливим компонентом екосистеми Windows, надаючи організаціям надійні інструменти для управління інфраструктурою.

Переваги використання AD очевидні. Організації можуть мінімізувати

ризики, пов'язані з довірою до хмарних провайдерів, оскільки всі дані залишаються всередині корпоративної мережі. Це дозволяє повністю контролювати дані та знижує ризики, пов'язані із законодавством інших країн щодо їх зберігання та обробки. Крім того, AD надає IT-адміністраторам широкі можливості налаштування конфігурацій, політик безпеки та інтеграції з іншими локальними системами.

Однак є і недоліки. Налаштування та адміністрування AD вимагає глибоких знань. Складність початкової настройки, встановлення контролерів домену, створення організаційних одиниць, налаштування групових політик (GPO) та встановлення довірчих відносин між доменами потребують досвіду та часу. Наприклад, помилка в налаштуванні реплікації між контролерами домену може призвести до збоїв в автентифікації користувачів.

Також неправильна міграція профілю користувача з одного домену на інший може призвести до неможливості подальшого оновлення комп'ютера з Windows 10 на 11. У результаті профіль доведеться перенести в іншу папку, потім виконати оновлення, створити новий профіль з тими ж даними користувача та перенести вміст старого профілю в новий. Однак цей спосіб є дуже ризикованим і вимагає як попередньої підготовки, так і тестування всіх компонентів після маніпуляцій.

Пристрої на Windows 11 можуть інтегруватися з AD через налаштування, що дозволяє організаціям централізовано керувати доступом до ресурсів. Для цього необхідно приєднати пристрій до домену та налаштувати групові політики для управління пристроєм. Така інтеграція забезпечує високий рівень безпеки та спрощує адміністрування багатьох пристроїв у мережі.

Entra ID

Microsoft Entra ID – це хмарна служба каталогів Microsoft, яка забезпечує управління ідентифікацією та доступом користувачів до ресурсів у хмарному середовищі Microsoft Azure. Вона інтегрується з хмарними додатками і сервісами, такими як Microsoft 365 та Teams, підтримуючи

функції єдиної автентифікації (SSO), умовного доступа (CA) і багатофакторної автентифікації (MFA) для підвищення рівня безпеки.

Microsoft Entra ID має суттєві відмінності від традиційної Active Directory. Якщо AD призначена для локальних мереж і управління ресурсами в корпоративній інфраструктурі, то Microsoft Entra ID є повністю хмарним рішенням, що забезпечує доступ до хмарних додатків. Це робить його ідеальним для компаній, які активно використовують хмарні технології.

Використання Microsoft Entra ID у поєднанні з Windows 11 без необхідності локальної Active Directory пропонує ряд переваг. Адміністрування здійснюється віддалено через зручний веб-інтерфейс, що дозволяє керувати пристроями та користувачами з будь-якої точки з інтернетом. Швидкість розгортання значно вища, оскільки немає потреби в налаштуванні локальних серверів та інфраструктури. Крім того, зменшується навантаження на підтримку, оскільки немає необхідності в обслуговуванні та оновленні локальних серверів, включаючи встановлення патчів і оновлень безпеки. Це знижує загальні витрати на обслуговування інфраструктури та дозволяє IT-персоналу зосередитися на більш стратегічних завданнях.

Однак існують і певні недоліки. Залежність від хмарних сервісів Microsoft означає, що будь-які збої в їх роботі можуть негативно впливати на бізнес-процеси. Можливості налаштування в Microsoft Entra ID можуть бути обмежені в порівнянні з локальним Active Directory (AD). Наприклад, встановлення мінімальної довжини пароля більше 8 символів недоступне, якщо синхронізація з локальним Active Directory не ввімкнена через Azure AD Connect. Це обмеження може створювати потенційні ризики безпеки для організацій, які прагнуть запровадити жорсткіші політики щодо паролів.

Підхід Microsoft до безпеки паролів наголошує на коротших паролях у поєднанні з надійними практиками безпеки, такими як багатофакторна аутентифікація (MFA) та умовний доступ (CA). Microsoft виступає за коротші, унікальні паролі, які легше запам’ятати, у поєднанні з MFA як додатковим рівнем захисту. З MFA користувачі зобов'язані підтвердити свою

особу за допомогою додаткового методу – наприклад, мобільного пристрою або електронної пошти – що значно знижує ризик несанкціонованого доступу лише завдяки скомпрометованим паролям.

Крім того, політики умовного доступу Microsoft надають розширений контроль безпеки, динамічно застосовуючи умови доступу на основі таких факторів, як місцезнаходження користувача, стан пристрою та рівень ризику. Така багаторівнева стратегія безпеки дозволяє організаціям зменшувати ризики навіть із коротшими паролями, вимагаючи MFA та застосовуючи обмеження доступу згідно з попередньо визначеними критеріями безпеки.

Інтегруючи ці механізми, Microsoft прагне збалансувати безпеку та зручність використання, зменшуючи залежність від складних вимог до паролів і одночасно підвищуючи загальний захист. Однак деякі організації можуть все ж таки віддавати перевагу гнучкості локального Active Directory для налаштування політик паролів понад встановлені значення Microsoft, залежно від їхніх унікальних вимог безпеки та регуляторних стандартів.

Ще одним суттєвим недоліком є обмежені можливості резервного копіювання в Microsoft Entra ID. На ринку немає комерційних продуктів, які б дозволяли повноцінно резервувати дані Entra ID, а відновлення в інше (власне) середовище неможливе через специфіку Entra ID. У разі необхідності відновлення даних, це доведеться робити вручну, що може бути трудомістким і ризикованим процесом. Практичний досвід показує, що відсутність автоматизованих рішень для резервного копіювання і відновлення може стати серйозною проблемою для організацій, які покладаються на Microsoft Entra ID як на основний засіб управління ідентифікацією.

Крім того, використання хмарних сервісів створює певні регулятивні ризики. Зберігання даних у хмарі вимагає дотримання законодавства країн, де розташовані дата-центри Azure, а також законів країни компанії, що використовує ці сервіси. Це може ускладнити питання відповідності нормативним вимогам і вимагати додаткових зусиль для забезпечення

юридичної чистоти операцій.

Підключення пристрою до Entra ID (Azure AD Join) дозволяє приєднати ваш пристрій безпосередньо до Entra ID. Для цього необхідно підготувати обліковий запис користувача в Entra ID з необхідними правами, а потім через налаштування Windows 11 приєднати пристрій до хмарного домену.

Гібридне підключення

Гібридна інтеграція дозволяє поєднати пристрої, керовані локальною Active Directory, з хмарною службою Microsoft Entra ID. Це рішення надає організаціям переваги обох світів: локальну автономність і контроль, а також можливості хмарних сервісів і мобільності.

Windows 11 підтримує гібридне підключення, що дозволяє користувачам автентифікуватися як у локальних мережах, так і в хмарі, забезпечуючи безперервний робочий процес незалежно від місцезнаходження пристрою або користувача. Це є однією з ключових особливостей Windows, що вигідно відрізняє її від інших операційних систем, таких як Chrome OS, Ubuntu чи macOS, завдяки можливості інтеграції локальних та хмарних ресурсів.

Переваги гібридного підключення включають інтеграцію локальної та хмарної інфраструктури, єдину автентифікацію (SSO), централізоване управління та безпеку, віддалений доступ та мобільність, а також поступовий перехід до хмарних технологій. Однак є і недоліки: складність налаштування та управління, залежність від стабільності мережевого з'єднання, збільшення витрат на підтримку, можливі конфлікти політик безпеки та регулятивні й юридичні складнощі.

Для налаштування гібридного приєднання необхідно встановити на сервері Azure AD Connect для синхронізації об'єктів з локальної Active Directory в Entra ID, налаштувати групові політики для автоматичного приєднання пристроїв до Entra ID та забезпечити доступ до необхідних інтернет-ресурсів Azure AD.

Microsoft Intune

Microsoft Intune – це хмарна служба управління пристроями та додатками, що забезпечує централізоване налаштування, моніторинг і управління пристроями на різних платформах. Основною перевагою є інтеграція з екосистемою Microsoft, зокрема Microsoft Entra ID, що дозволяє ефективно керувати пристроями, додатками та політиками безпеки.

Переваги Microsoft Intune для Windows 11 включають інтеграцію з екосистемою Microsoft, використання Windows Autopilot для автоматичного налаштування нових пристроїв, централізоване управління оновленнями та мережевими профілями, а також єдину платформу управління.

Для підключення Windows 11 до Intune необхідно зареєструвати пристрій в Microsoft Entra ID, підключити його до Intune через налаштування Windows або за допомогою додатка Company Portal із Microsoft Store, а потім застосувати політики та профілі, налаштовані адміністратором Intune.

SCCM

Microsoft System Center Configuration Manager (SCCM) – це локальний інструмент управління пристроями, що забезпечує повний контроль над інфраструктурою. Це робить його ідеальним вибором для середовищ з високими вимогами до безпеки. Основні відмінності між Microsoft Intune та SCCM полягають у типі інфраструктури: Intune базується на хмарних технологіях, тоді як SCCM – на локальних серверах. Intune забезпечує кросплатформене управління, в той час як SCCM більш орієнтований на пристрої Windows. Також можлива гібридна інтеграція SCCM з Intune, що дозволяє отримати переваги обох рішень. Однак варто зазначити, що SCCM є складнішим у налаштуванні, що потребує більше часу та ресурсів для початкової конфігурації та підтримки.

Для підключення пристрою до SCCM необхідно виконати кілька кроків: підготувати Windows-сервер для роботи з SCCM, налаштувати клієнт SCCM на кожному пристрої, перевірити підключення пристрою до сервера SCCM та забезпечити виконання політик, а також розгортання програм через

Software Center.

Цей підхід дозволяє забезпечити ефективне управління пристроями, їх відповідність політикам безпеки, а також спрощене розгортання необхідного програмного забезпечення на рівні компанії.

Висновок: Інтеграція Windows з корпоративними сервісами надає значні переваги завдяки гнучкості, розширеним можливостям управління та глибокій інтеграції в екосистему Microsoft. Windows дозволяє організаціям обирати локальні, хмарні або гібридні рішення, адаптовані до їхніх потреб. Гібридний підхід є особливо корисним для тих, хто прагне використовувати хмарні сервіси, зберігаючи при цьому контроль над критично важливими даними та забезпечуючи відповідність регуляторним вимогам.

Крім того, популярність Windows і його усталена екосистема спрощують пошук партнерів для інтеграції та ресурсів підтримки. Організації можуть покладатися не лише на широку мережу партнерів, сертифікованих Microsoft, але й на потужну підтримку від самої Microsoft і активної спільноти. Ця розвинена екосистема підтримки полегшує вирішення проблем, інтеграцію та налаштування, дозволяючи бізнесу оптимізувати свої системи за допомогою експертних порад.

При виборі відповідного рішення важливо враховувати не лише технічні аспекти, а й регуляторні, правові та операційні чинники. Наприклад, обмеження у можливостях резервного копіювання в Microsoft Entra ID можуть бути критичними для деяких організацій. Вимоги до безпеки, такі як впровадження суворих політик щодо паролів, також потребують уважного розгляду.

Гнучкість платформи Windows дозволяє бізнесу керувати IT-інфраструктурою у відповідності до своїх стратегічних цілей, підтримуючи ефективність, безпеку та конкурентоспроможність. Вибір між Active Directory, Microsoft Entra ID або комбінацією обох залежить від конкретних потреб і пріоритетів організації.

4.2. Інтеграція macOS з доменними технологіями Microsoft

Інтеграція операційних систем у корпоративне середовище є важливою складовою для забезпечення безпеки, управління пристроями та ефективної роботи користувачів. У порівнянні з Windows, яка добре інтегрується з інфраструктурою Microsoft, macOS має свої особливості та виклики в контексті інтеграції з доменними рішеннями, як-от Active Directory та Microsoft Entra ID. У цій статті буде розглянуто основні аспекти інтеграції macOS з доменними технологіями Microsoft, а також функціонал таких рішень, як Xcreds від Twocanoes Software, Apple Business Manager (ABM) та Mobile Device Management (MDM).

Active Directory

macOS підтримує інтеграцію з Active Directory через вбудований інструмент Directory Utility. Це дозволяє користувачам macOS автентифікуватися через доменні облікові записи та отримувати доступ до корпоративних ресурсів, що є стандартною практикою в багатьох організаціях, які використовують Windows. Однак ця інтеграція має деякі обмеження:

- Обмежена підтримка групових політик (GPO): Windows дозволяє адміністраторам централізовано керувати користувачами і пристроями через GPO, що спрощує впровадження політик безпеки. macOS не має повноцінної підтримки GPO, і для адміністраторів це означає необхідність використовувати додаткові рішення, як-от Mobile Device Management (MDM). Хоча GPO є важливою складовою управління Windows, управління macOS через MDM може бути не настільки гнучким або глибоким.
- Синхронізація паролів: Одна з найбільших проблем при інтеграції macOS з Active Directory – це синхронізація паролів. Якщо пароль змінюється в Active Directory, macOS не завжди коректно оновлює ці дані, що може спричинити проблеми з автентифікацією або

блокуванням доступу. Однак, це можна вирішити за допомогою додаткових інструментів, таких як Xcreds.

- Продуктивність підключення: Інтеграція через Directory Utility іноді може призводити до затримок при доступі до мережевих ресурсів через повільне виконання LDAP-запитів. Це може бути помітно при роботі в корпоративних мережах із великим обсягом даних.

Попри ці проблеми, інтеграція macOS з Active Directory все ще використовується багатьма організаціями через його широку підтримку на рівні Microsoft інфраструктури, але вона вимагає додаткових налаштувань та рішень для повноцінної роботи.

Entra ID

Microsoft Entra ID (колишній Azure Active Directory) є хмарним сервісом для управління ідентифікацією і є основою для багатьох корпоративних середовищ, які використовують Microsoft 365. Інтеграція macOS з Microsoft Entra ID можлива через кілька інструментів, проте вона також має свої особливості та обмеження:

- Company Portal: macOS можна підключити до Microsoft Entra ID через додаток Company Portal [20]. Це дозволяє користувачам отримувати доступ до хмарних ресурсів і забезпечує базове управління пристроями. Однак у порівнянні з Windows функціональність інтеграції є менш гнучкою, зокрема у сфері управління доступом до локальних ресурсів та керування пристроями.
- Primary Sign-On (PSSO): У новіших версіях macOS Microsoft почала тестувати функцію PSSO, що дозволяє приєднувати нові пристрої до Entra ID під час першого запуску (Out of Box Experience). Проте функціональність все ще перебуває на стадії прев’ю і не може забезпечити повноцінної інтеграції для великих корпоративних середовищ.

Отже, хоча Microsoft Entra ID забезпечує базову інтеграцію macOS з хмарними рішеннями Microsoft, його функціональність ще не досягає рівня,

який є доступним для пристроїв на Windows.

Xcreds

Xcreds від Twocanoes Software є відкритим інструментом для синхронізації локальних облікових записів macOS з Microsoft Entra ID та Active Directory. Це рішення було прийняте багатьма організаціями через його здатність вирішувати основні проблеми інтеграції macOS з хмарними сервісами [21].

– Синхронізація облікових даних: Xcreds автоматично синхронізує паролі між macOS та Entra ID або Active Directory. Це вирішує одну з основних проблем, з якими стикаються користувачі, – невідповідність паролів у локальних облікових записах і хмарних системах. Після зміни пароля в Microsoft Entra ID, Xcreds автоматично оновлює облікові дані на macOS, забезпечуючи безперебійну роботу користувачів без необхідності подальших маніпуляцій.

Однак є кілька додаткових кроків, які можуть ускладнити процес для кінцевих користувачів. Наприклад, спочатку потрібно залогінитися у macOS для розблокування шифрованого диска FileVault. Після цього користувач повинен увійти в Microsoft Entra ID через веб-інтерфейс у вікні Xcreds, використовуючи ті самі облікові дані. Це додатковий крок може бути незрозумілим для деяких користувачів і потребує детального пояснення з боку адміністратора.

– Особливості синхронізації та додаткові вікна: Після входу в Microsoft Entra ID через Xcreds може з'явитися додаткове вікно з вимогою ввести облікові дані Microsoft для синхронізації локальних облікових записів з хмарою. Це вікно можна просто закрити, оскільки воно не впливає на роботу системи. Хоча це додає непотрібний крок у процес авторизації, він не призводить до критичних збоїв і є лише незначною незручністю.
– Багатофакторна автентифікація (MFA): Xcreds підтримує MFA, що важливо для організацій, які потребують додаткового рівня безпеки. Це дозволяє інтегрувати macOS в середовище з високими вимогами до

безпеки.

Xcreds дозволяє організаціям інтегрувати macOS з Microsoft Entra ID, забезпечуючи значну гнучкість і безпеку. Хоча його функціональність не відповідає рівню нативної підтримки Microsoft технологій на Windows, він популярний серед організацій завдяки відкритості та активній підтримці спільноти.

Однак пошук кваліфікованого партнера, який має експертизу в середовищах Microsoft і macOS, може бути складним завданням, оскільки більшість партнерів Microsoft Solutions мають обмежений або взагалі відсутній досвід роботи з macOS. Ця нестача може вимагати додаткового часу та ресурсів для організацій, що шукають кваліфіковану підтримку в інтеграції macOS з Microsoft Entra ID, і потенційно змусить їх покладатися на спеціалізованих консультантів або менші компанії, обізнані з кросплатформенними середовищами.

Apple Silicon

Перехід на процесори Apple Silicon приніс значні зміни в архітектурі macOS, що вплинуло на адміністрування пристроїв. Apple Silicon покращує безпеку завдяки своїм апаратним можливостям, таким як Secure Enclave та шифрування на рівні апаратури.

- Безпека: Apple Silicon підвищує рівень безпеки, обмежуючи можливості стороннього втручання та покращуючи захист від атак на рівні апаратури. Це змінює підходи до управління пристроями, адже багато традиційних методів адміністрування вимагають адаптації до нових вимог.
- Обмеження для адміністраторів: Зміни в архітектурі також означають, що адміністратори повинні шукати нові підходи до управління пристроями, адже деякі старі методи (наприклад, повне управління через Active Directory) стають менш ефективними або застарілими.

ABM, MDM та їх інтеграція з Intune

Apple пропонує два важливі інструменти для управління своїми

пристроями в корпоративному середовищі: Apple Business Manager (ABM) та Mobile Device Management (MDM). Ці рішення працюють разом для забезпечення централізованого контролю та налаштування пристроїв, але кожен з них виконує свої специфічні функції.

- Apple Business Manager (ABM): ABM – це веб-платформа для централізованої реєстрації та управління пристроями Apple. Вона дозволяє автоматично додавати нові пристрої до MDM-системи, а також керувати ліцензіями на додатки та обліковими записами користувачів. ABM надає можливість компаніям централізовано реєструвати пристрої в організації, що спрощує їх подальше налаштування та адміністрування за допомогою MDM.
- Mobile Device Management (MDM): MDM використовується для безпосереднього управління пристроями, включаючи налаштування безпеки, політики доступу, оновлення програмного забезпечення та моніторинг. Адміністратори можуть централізовано керувати пристроями на macOS, iOS, iPadOS та tvOS. Однак, функціональність MDM іноді може бути обмеженою порівняно з рішеннями, такими як Microsoft Intune в поєднанні з MS Windows.

Інтеграція ABM з Microsoft Intune

Нещодавні зміни дозволили тісну інтеграцію Apple Business Manager з Microsoft Intune, що відкриває нові можливості для управління пристроями Apple у корпоративному середовищі. Microsoft Intune – це хмарне рішення для управління мобільними пристроями, яке надає розширені можливості управління та безпеки для різних платформ, включаючи macOS та iOS.

Кооперація між ABM та Intune дозволяє компаніям використовувати ABM для централізованої реєстрації пристроїв, після чого ці пристрої автоматично підключаються до Intune для подальшого управління. Це спрощує процес налаштування нових пристроїв та забезпечує гнучкість у налаштуванні політик безпеки та доступу.

Основні переваги інтеграції ABM та Intune:

- Автоматична реєстрація пристроїв: Нові пристрої Apple можуть автоматично реєструватися в Intune через ABM, що усуває необхідність ручного налаштування кожного пристрою.
- Гнучке управління безпекою: Intune дозволяє застосовувати розширені політики безпеки, зокрема багатофакторну автентифікацію (MFA), політики управління додатками та шифрування даних.
- Управління у змішаних середовищах: Intune надає можливість централізовано керувати пристроями з різними операційними системами, що є важливим для компаній, які використовують як Windows, так і Apple.

Завдяки інтеграції Apple Business Manager з Intune організації отримують можливість більш ефективно управляти пристроями Apple разом з іншими платформами. Використання ABM разом із MDM та Intune дозволяє компаніям автоматизувати процеси реєстрації пристроїв, впроваджувати політики безпеки та підтримувати високий рівень контролю над пристроями на різних операційних системах.

Ця інтеграція дає можливість поєднувати зручність централізованого керування пристроями Apple через ABM з потужними інструментами безпеки та управління Intune, що робить цей підхід оптимальним для організацій із змішаними середовищами.

Висновок: Інтеграція macOS та інших пристроїв Apple у корпоративне середовище має свої переваги й виклики, особливо у порівнянні з Windows. Apple Business Manager та Mobile Device Management надають базові можливості для централізованого управління пристроями. Однак інтеграція з Microsoft Intune суттєво розширює ці можливості, особливо у змішаних середовищах, де використовуються як пристрої Apple, так і Windows. Завдяки автоматичній реєстрації пристроїв через ABM та розширеним політикам безпеки Intune, компанії можуть досягти більш високого рівня контролю та ефективності управління.

Крім того, інтеграція macOS з Microsoft Entra ID забезпечує базовий

рівень доступу до хмарних сервісів Microsoft, але має свої обмеження, зокрема в частині керування локальними ресурсами та автентифікації. Інструменти, такі як Xcreds, допомагають вирішити проблеми синхронізації облікових даних і підтримують багатофакторну автентифікацію, що робить інтеграцію більш надійною та безпечною.

Для організацій, що прагнуть зменшити залежність від Active Directory і перейти до сучасних хмарних технологій, інтеграція macOS з Microsoft Entra ID та використання Xcreds можуть стати ефективним рішенням. У поєднанні з ABM та Intune, це забезпечує високу гнучкість, безпеку та можливість централізованого управління всіма пристроями в організації.

4.3. Інтеграція Ubuntu 24.04 з доменними технологіями Microsoft

Останнім часом Canonical активно розширює можливості інтеграції Ubuntu з інфраструктурою Microsoft, включаючи Active Directory (AD), Entra ID (колишній Azure AD), і Microsoft Intune. Реліз Ubuntu 24.04 приносить нові інструменти, такі як AuthD для аутентифікації через хмарні платформи та інтеграція з Microsoft Entra ID, а також вдосконалені механізми роботи з Active Directory через System Security Services Daemon (SSSD) та ADSys. У цьому розділі розглянемо технічні аспекти цієї інтеграції та порівняємо її з рівнем інтеграції Windows 11 та macOS.

Active Directory

Інтеграція Ubuntu 24.04 з Active Directory базується на двох основних компонентах: SSSD та ADSys. SSSD використовується для базової аутентифікації користувачів і забезпечує підтримку LDAP (Lightweight Directory Access Protocol – це протокол для доступу і управління інформацією в каталогах, таких як бази даних користувачів та ресурсів) та Kerberos (протокол автентифікації, який використовує квитки для безпечної ідентифікації користувачів у мережі), тоді як ADSys розширює можливості управління через Group Policy Objects (GPO) і надає підтримку управління

сертифікатами, проксі-налаштуваннями та мережевими сховищами.

Windows 11 має нативну інтеграцію з Active Directory і Microsoft Entra ID, що дозволяє максимально ефективно використовувати всі функції цих платформ. Це включає можливості управління пристроями, політики безпеки та інтеграцію з іншими продуктами Microsoft. macOS, своєю чергою, також підтримує інтеграцію з Active Directory, але її можливості обмежені в порівнянні з Windows, особливо в частині управління через GPO [18].

Ubuntu, за допомогою ADSys, забезпечує схожу на macOS інтеграцію з AD, дозволяючи користувачам аутентифікуватися за допомогою корпоративних облікових записів та застосовувати певні політики. Проте рівень контролю, який надає ADSys через GPO, все ще поступається рішенню, яке пропонує Windows 11 [23].

Entra ID

Ubuntu 24.04 пропонує новий підхід до інтеграції з хмарними сервісами Microsoft через AuthD, який замінив попередній aad-auth. AuthD дозволяє здійснювати аутентифікацію через Entra ID (Azure AD) та OpenID Connect-провайдерів, що розширює можливості управління ідентифікацією в хмарі [22].

Інсталяція AuthD на Ubuntu 24.04 досить проста і включає встановлення самого AuthD та Entra ID брокера через Snap. Після цього користувачі можуть налаштовувати Ubuntu для аутентифікації через Entra ID, використовуючи механізми OAuth2 (протокол авторизації, що дозволяє додаткам отримувати обмежений доступ до ресурсів користувачів без передачі їх паролів) та OpenID Connect (розширення OAuth2, яке додає функції автентифікації, дозволяючи підтвердити особу користувача).

Windows 11 має вбудовану підтримку Entra ID, що забезпечує максимальну інтеграцію з сервісами Microsoft, включаючи Single Sign-On (SSO) та повне управління пристроями [19]. macOS, хоча і підтримує Azure AD через зовнішні програми, пропонує меншу функціональність у порівнянні з Windows.

Ubuntu ж через AuthD наближається до Windows за рівнем інтеграції з Entra ID, забезпечуючи подібну функціональність з точки зору аутентифікації та авторизації. Однак, деякі аспекти управління пристроями, такі як повне управління політиками безпеки, можуть бути складнішими в реалізації на Ubuntu.

Intune

Управління пристроями Ubuntu через Microsoft Intune значно обмежене у порівнянні з Windows і macOS. Microsoft Intune підтримує Ubuntu як корпоративний пристрій, але можливості управління на цьому рівні є обмеженими порівняно з повною інтеграцією Windows і macOS [24].

На Windows 11, Intune надає повний контроль над налаштуваннями безпеки, установкою програмного забезпечення, оновленнями системи і управлінням політиками. macOS, хоч і поступається Windows в інтеграції, також пропонує широкий спектр можливостей управління через Intune. В обох випадках користувачі отримують безперервне управління через єдиний портал.

На Ubuntu, Intune може бути використаний для основного управління, але не забезпечує тієї ж глибини інтеграції. Ubuntu не підтримує повноцінну установку політик Intune і оновлень системи, що обмежує можливості корпоративного управління.

Корпоративні рішення від Canonical

Canonical пропонує декілька рішень, розроблених для інтеграції Ubuntu в корпоративні середовища з акцентом на безпеку, управління та безперервну інтеграцію з корпоративними системами.

ADSys від Canonical спрощує інтеграцію Ubuntu з Microsoft Active Directory, забезпечуючи ключові корпоративні функції, такі як підтримка об’єктів групових політик (GPO), управління сертифікатами та виконання скриптів, пов’язаних з політиками AD. Це дозволяє адміністраторам IT застосовувати політики та забезпечувати налаштування на Ubuntu-системах подібно до Windows, полегшуючи роль Ubuntu в середовищі з різними ОС.

Ubuntu Pro призначений для підвищення рівня безпеки та стабільності для корпоративних користувачів. Він пропонує посилене управління безпекою, надаючи критичні та високопріоритетні оновлення для всієї екосистеми Ubuntu, включаючи пакунки з основного та додаткового сховищ. Основні можливості включають:

- Extended Security Maintenance (ESM): Ubuntu Pro надає довготривалу підтримку з критичними оновленнями до 10 років, усуваючи вразливості, які інакше могли б залишитися без уваги в непідтримуваних пакунках.
- Відповідність та сертифікації: Ubuntu Pro відповідає стандартам відповідності індустрії, таким як CIS і FIPS, що задовольняє жорсткі вимоги до безпеки в регульованих галузях.
- Пріоритетна підтримка та SLA: Canonical забезпечує технічну підтримку з угодами про рівень обслуговування (SLA) для допомоги з усуненням проблем, наданням кращих практик та підтримкою стабільності корпоративних розгортань.

Landscape є комплексним рішенням Canonical для управління великими розгортаннями Ubuntu, що служить альтернативою Microsoft Intune для систем Ubuntu. Landscape дозволяє адміністраторам ефективно моніторити, оновлювати та налаштовувати великі парки пристроїв на Ubuntu. Landscape пропонує кілька варіантів розгортання, забезпечуючи організаціям гнучкість у виборі оптимальної конфігурації для їхніх операційних потреб та інфраструктурних переваг [47]:

- Landscape SaaS (Програмне забезпечення як послуга): Це повністю хмарний сервіс, керований Canonical, який усуває потребу в обслуговуванні серверного програмного забезпечення на місці. Використовуючи Landscape SaaS, організації отримують переваги централізованого управління без складності в обслуговуванні серверної інфраструктури, дозволяючи адміністраторам зосередитися на операційних завданнях, поки Canonical займається інфраструктурою та

оновленнями.

- Self-Hosted Landscape: Ця версія Landscape дозволяє організаціям встановлювати та керувати платформою у власній інфраструктурі. Вона може бути розгорнута на локальних серверах для максимального контролю або в хмарних середовищах, таких як AWS, Azure або будь-яка інша сумісна хмарна інфраструктура. Цей варіант забезпечує настроюване налаштування, що підходить для організацій, які потребують більшого контролю над даними, параметрами безпеки або регуляторною відповідністю.
- Managed Landscape: Managed Landscape надає експертизу та контроль Canonical над розгортанням Landscape у будь-якому середовищі. Організації можуть використовувати платформу Landscape на обраній інфраструктурі – будь то локальна чи хмарна, а Canonical буде здійснювати управління, моніторинг та оновлення. Цей варіант поєднує переваги самостійного розгортання з технічною підтримкою Canonical, надаючи організаціям операційну гнучкість без необхідності самостійного обслуговування.

Ці варіанти розгортання пропонують баланс між зручністю та контролем, дозволяючи компаніям обрати оптимальну конфігурацію на основі їхніх специфічних вимог, таких як зменшення навантаження на обслуговування, відповідність жорстким стандартам безпеки або контроль над інфраструктурою.

Інтеграція Ubuntu 24.04 з доменними технологіями Microsoft продовжує розвиватися, наближаючись за рівнем підтримки до Windows 11, особливо в частині аутентифікації через Entra ID. Однак, деякі аспекти, такі як повне управління пристроями через Microsoft Intune та GPO, ще не досягають рівня, що надається Windows 11. Попри це, завдяки таким інструментам, як AuthD і ADSys, Ubuntu залишається конкурентоспроможним вибором для організацій, які використовують інфраструктуру Microsoft.

4.4. Інтеграція ChromeOS з доменними технологіями Microsoft

Active Directory

Інтеграція Microsoft Active Directory (AD) з Chrome OS наразі більше не підтримується. Починаючи з версії ChromeOS 110, неможливо виконати вхід або реєстрацію пристроїв у режимі AD. Компанії, що раніше використовували AD, тепер повинні перейти до хмарного управління через Google Workspace або Cloud Identity. Це кардинально відрізняється від платформ, таких як Windows або Ubuntu, де інтеграція з AD залишається основним компонентом управління ідентифікацією та доступом користувачів.

Для Chrome OS рекомендовано використовувати альтернативні підходи, такі як Google Cloud Directory Sync або використання SAML для єдиного входу (SSO), щоб забезпечити доступ до ресурсів організації [25]. Важливою особливістю є також підтримка Kerberos для доступу до внутрішніх ресурсів.

Entra ID

Chrome OS підтримує інтеграцію з Microsoft Entra ID (колишній Azure AD) за допомогою SAML для налаштування єдиного входу та синхронізації користувачів [26]. Ця інтеграція дозволяє користувачам входити в систему за допомогою облікових даних Microsoft Entra ID замість облікового запису Google. Порівняно з Windows, який має нативну інтеграцію з Entra ID, Chrome OS обмежений необхідністю використання SAML та сторонніх механізмів для управління користувачами та пристроями.

На відміну від Windows та macOS, де інтеграція з Entra ID нативна, Chrome OS значною мірою залежить від Google SSO та інших хмарних рішень для забезпечення єдиного входу. У випадку Ubuntu, також можливе налаштування через SAML, але ці рішення не такі нативні, як у Windows, який може працювати з Entra ID "із коробки".

Intune

До недавнього часу Chrome OS можна було частково керувати через Microsoft Intune, використовуючи політики захисту застосунків для Android-додатків та політики умовного доступу Azure AD [27]. Однак, завдяки недавнім оновленням, Microsoft Intune для Chrome OS запровадив можливість синхронізувати інформацію про пристрої Chrome OS в Microsoft Endpoint Manager. Ця функція дозволяє виконувати базові віддалені дії (перезавантаження, видалення даних, блокування загубленого пристрою), але MDM-управління не підтримується нативно, як для Windows, macOS або iOS [28].

Обмеження

Chrome OS, хоча і має високий рівень інтеграції з хмарними сервісами, залишається обмеженою через невідключну залежність від хмарних сервісів Google. Це може бути критичним обмеженням для організацій, що працюють із чутливими даними або обслуговують критичну інфраструктуру, яка вимагає автономних рішень без доступу до зовнішніх хмарних сервісів. Наприклад, у таких сценаріях використання Windows або Ubuntu, які можуть бути конфігуровані для локальної роботи без доступу до хмари, можуть бути більш привабливими варіантами.

Альтернативи від Google

Google надає власні аналоги рішень від Microsoft для управління ідентифікацією та пристроями:

1) Google Cloud Identity є аналогом Active Directory та Entra ID. Він дозволяє керувати ідентифікацією користувачів та доступом до ресурсів Google та сторонніх сервісів.
2) Google Workspace Admin Console використовується для управління пристроями та користувачами. Вона дозволяє адмініструвати політики пристроїв Chrome OS, керувати оновленнями та забезпечувати доступ до ресурсів.
3) Google Endpoint Management забезпечує базове управління пристроями, проте воно не настільки просунуте, як Microsoft Intune, особливо щодо

нативного управління пристроями, такими як Windows або iOS.

Переваги екосистеми Google

Основною перевагою екосистеми Google є простота налаштування та використання пристроїв Chrome OS. Хромбуки готові до роботи з коробки, що значно спрощує процес впровадження для кінцевих користувачів. Крім того, синхронізація з Google Workspace забезпечує легке управління пристроями через хмару. Інтеграція з Microsoft Entra ID також дозволяє об'єднувати облікові записи для єдиного входу, що робить цю платформу зручною для організацій, що вже використовують Microsoft 365.

Проте, порівняно з Windows та macOS, які можуть працювати як у локальних мережах, так і в хмарі, Chrome OS значною мірою залежить від хмарної інфраструктури, що робить її менш гнучкою для організацій з жорсткими вимогами до безпеки та конфіденційності.

Інтеграція Chrome OS з рішеннями Microsoft має як переваги, так і недоліки. Вона забезпечує просте та ефективне управління через Google Workspace, проте обмежена у порівнянні з Windows або macOS, які мають ширші можливості нативного управління через Entra ID та Intune. Для організацій, які покладаються на хмарні рішення, Chrome OS може бути зручним вибором, однак для критичних інфраструктур краще звернути увагу на більш гнучкі платформи, такі як Windows або Ubuntu.

4.5. Операційні системи без Інтернету: порівняння можливостей

У сучасному світі операційні системи значною мірою орієнтовані на використання Інтернету, але іноді виникає потреба використовувати комп'ютер без підключення до мережі. Це може бути необхідно в умовах роботи на закритих об'єктах державної важливості, де Інтернет заборонений з міркувань безпеки, або в місцях з обмеженим доступом до мережі. У таких ситуаціях важливо розуміти, наскільки добре різні ОС справляються з роботою в офлайн-режимі. Ми порівняємо Windows, macOS, Ubuntu і Chrome

OS з точки зору можливості використання локальних облікових записів, установки оновлень без Інтернету та загальної працездатності без мережевого підключення.

Windows

Локальні акаунти

Windows, починаючи з версії 10, значно акцентує увагу на використанні Microsoft Account для синхронізації даних, роботи з хмарними сервісами тощо. Проте існує можливість створення локального облікового запису після завершення налаштування або за допомогою обхідних методів.

У Windows 11 цей процес став складнішим, особливо у версії Home, де підключення до Інтернету та використання облікового запису Microsoft є обов'язковим під час початкового налаштування. Проте існують способи обійти цю вимогу:

1. Комбінація клавіш Shift + F10 і команда oobe\bypassnro:
   На етапі, коли система вимагає увійти в Microsoft Account:
   - Натисніть Shift + F10 (або Shift + Fn + F10 на ноутбуках із активованими функціональними клавішами), щоб відкрити командний рядок.
   - У командному рядку введіть oobe\bypassnro і натисніть Enter.
   - Система перезапуститься, і з'явиться можливість пропустити підключення до Інтернету та створити локальний обліковий запис.
2. Використання неправдивих даних:
   Якщо підключення до Інтернету неможливо вимкнути, можна ввести фіктивний e-mail (наприклад, fake@fake.com) і будь-який пароль. Після невдалої спроби з'явиться можливість продовжити налаштування без облікового запису Microsoft.

У версії Pro створення локального облікового запису є простішим і доступним без зазначених обхідних шляхів. На етапі налаштування з'являється варіант підключення до локального домену (аналогічно

підключенню до корпоративної мережі), який дозволяє створити локальний обліковий запис. Хоча цей варіант виглядає як корпоративна функція, він дозволяє обійти вимогу щодо використання Microsoft Account.

Оновлення офлайн

Установити оновлення Windows без Інтернету можна, але це потребує певної підготовки. Оновлення можна завантажити на інший комп'ютер (де є підключення до Інтернету) через утиліти, такі як WSUS Offline або використання каталогу оновлень Microsoft. Однак сам процес може бути дещо складним для недосвідчених користувачів. Майкрософт активно просуває свої сервіси онлайн-оновлень і визнає WSUS застарілим методом.

Функціональність офлайн

Windows загалом добре працює в офлайн-режимі, більшість локальних застосунків та інструментів функціонують без підключення до мережі. Однак деякі функції, що залежать від хмари, такі як Microsoft Store, синхронізація файлів OneDrive та інші хмарні сервіси, будуть недоступні без інтернету. Застосунки Microsoft Office, такі як Word, Excel та PowerPoint, можуть працювати в офлайн-режимі, хоча для активації або періодичної аутентифікації ліцензій часто потрібен вхід у систему. Для користувачів Microsoft 365 (раніше Office 365) необхідний періодичний доступ до інтернету для підтвердження статусу підписки. Якщо застосунки Office використовуються офлайн протягом тривалого періоду, користувачі можуть зіткнутися з обмеженнями або нагадуваннями про необхідність підключення до інтернету для оновлення ліцензії.

Для організацій, які потребують більш надійної роботи в офлайн-режимі, доступна версія Microsoft Office LTSC (Long-Term Servicing Channel). Ця версія Office розроблена для сценаріїв, де регулярний доступ до інтернету може бути недоступний, наприклад, у захищених середовищах. Версії LTSC ліцензуються на кожен пристрій і не потребують частого підключення до інтернету для перевірки ліцензії, що робить їх стабільним вибором для організацій, які надають пріоритет надійності роботи в офлайні.

Проте вони не містять деяких функцій, інтегрованих із хмарою, і частих оновлень, які є у Microsoft 365, оскільки LTSC орієнтована на стабільність, а не на розширення функцій.

macOS. Локальні акаунти

macOS, подібно до Windows, пропонує можливість використовувати обліковий запис iCloud для синхронізації та доступу до хмарних сервісів. Проте, під час встановлення ви можете обрати створення локального облікового запису без прив'язки до iCloud. Після цього користувач зможе користуватися системою без необхідності постійного підключення до Інтернету.

Оновлення офлайн (до macOS 10.15)

Для версій macOS до 10.15 (Catalina) Apple надає можливість завантажувати окремі пакети оновлень безпосередньо з офіційного сайту. Ці оновлення можна зберігати і встановлювати без Інтернету. Такий підхід є зручним для користувачів, які мають обмежений доступ до мережі, або для тих, хто керує великою кількістю пристроїв. Посилання для завантаження оновлень: https://support.apple.com/downloads/macos.

Оновлення офлайн (macOS 11+)

Для macOS 11 (Big Sur) та новіших версій Apple відійшла від окремих пакетів оновлень, замінивши їх повними інсталяторами системи. Ці інсталятори можна завантажити, зберегти офлайн та використовувати для повних оновлень системи. Однак навіть при використанні повного інсталятора (наприклад, Install macOS Monterey.app) може знадобитися доступ до інтернету під час встановлення для завантаження прошивки або даних, специфічних для конкретного пристрою, які не включені в основний інсталятор. Крім того, менші, термінові оновлення безпеки та патчі можуть не бути повністю включені в ці офлайн-інсталятори та можуть вимагати підключення до інтернету для застосування.

Apple періодично випускає критичні виправлення безпеки поза звичайним циклом оновлень, і зазвичай вони застосовуються автоматично у

фоновому режимі, коли система підключена до мережі. Для організацій, які надають пріоритет офлайн-середовищам, така залежність від інтернету для певних оновлень безпеки може створювати труднощі, оскільки не всі оновлення безпеки доступні у вигляді окремих пакетів.

Створення завантажувальної USB-версії

Для створення завантажувального USB-диска можна використовувати команду createinstallmedia з інсталятором, що завантажений у папку /Applications. Але, як і в попередньому випадку, навіть при використанні такого USB-диска, інсталяція може потребувати Інтернету для отримання мікропрограм та інших важливих даних.

Функціональність офлайн

macOS добре працює в офлайн-режимі, і більшість застосунків – таких як пакет iWork (Pages, Numbers, Keynote), Finder, текстові редактори та інші локальні інструменти – функціонують без проблем без підключення до інтернету. Однак деякі функції, що залежать від хмари, такі як синхронізація з iCloud, iCloud Drive та App Store, будуть недоступні в офлайн-режимі. Для користувачів, які запускають Microsoft Office на macOS, такі програми, як Word, Excel та PowerPoint, зазвичай працюють в офлайн-режимі, хоча вони можуть періодично просити користувача увійти в обліковий запис для активації або перевірки ліцензій. Для передплатників Microsoft 365 потрібен періодичний доступ до інтернету для оновлення статусу ліцензії, оскільки тривале використання в офлайн-режимі може викликати нагадування про підключення.

Користувачі версії Office LTSC (Long-Term Servicing Channel) на macOS отримують стабільніший досвід роботи в офлайні, оскільки ця версія розроблена для сценаріїв з обмеженим доступом до інтернету і не вимагає частих перевірок ліцензії в мережі. Проте, як і у випадку з Windows, версії LTSC не мають регулярних хмарних оновлень та додавання функцій, зосереджуючись натомість на стабільності та надійності в офлайн-режимі.

Ubuntu

Локальні акаунти

В Ubuntu (і більшості інших дистрибутивів GNU/Linux) локальні облікові записи є стандартним варіантом. Під час установки системи створюється локальний користувач, і для роботи з системою не потрібні облікові записи в хмарних сервісах. Це робить Ubuntu одним із найкращих варіантів для використання в офлайн-режимі.

Оновлення офлайн

Для встановлення оновлень без Інтернету в Ubuntu також можливо використовувати офлайн-репозиторії або завантажувати пакети на іншому комп'ютері, а потім переносити їх через USB-накопичувачі. Крім того, існує утиліта APTonCD, яка дозволяє створювати резервні копії встановлених програм і оновлень для їх відновлення на іншій системі без доступу до Інтернету. Більш того, організація може зробити форк/свою модифікацію Ubuntu для корпоративних потреб, завдяки вільній природі цього дистрибутиву.

Функціональність офлайн

Ubuntu і більшість додатків для Linux чудово працюють без Інтернету. Офісні пакети, редактори зображень, текстові редактори та інші локальні додатки не потребують постійного підключення до мережі. Щоправда, деякі специфічні програми, як-от браузери з веб-сервісами, втратять частину своїх функцій.

Chrome OS

Локальні акаунти відсутні

Chrome OS – це операційна система, яка спочатку була створена з урахуванням хмарних технологій і тісно пов'язана з обліковим записом Google. Хоча є обмежена можливість використовувати "гостьовий режим", повноцінна робота передбачає підключення до Google-сервісів. Можливість створення повноцінного локального облікового запису в Chrome OS відсутня.

Оновлення офлайн

Chrome OS практично не підтримує офлайн-оновлення. Усі оновлення

виконуються через Інтернет, і відсутність доступу до мережі ускладнює отримання нових версій системи чи безпекових патчів.

Функціональність офлайн

Chrome OS значною мірою залежить від Інтернету. Хоча деякі функції (наприклад, робота з Google Docs або завантаженими веб-додатками) можуть бути доступні офлайн, загальна функціональність значно обмежується при відсутності підключення. Ця ОС найкраще підходить для користувачів, які постійно перебувають в мережі.

Таким чином, якщо вам потрібна операційна система для роботи без Інтернету, найкращим вибором стануть Windows або Ubuntu, оскільки всі вони підтримують локальні облікові записи та дозволяють оновлення офлайн (хоча в кожній системі це зробити по-різному складно). Для версій macOS 11+ (Big Sur та новіших) навіть при наявності повного інсталятора потрібен Інтернет для отримання мікропрограм та інших специфічних для пристрою даних.

Ubuntu має найбільшу гнучкість і автономність, коли справа доходить до використання в повністю офлайн-середовищі. Натомість Chrome OS є найбільш залежною від Інтернету і не пропонує такої ж гнучкості, як інші системи, для офлайн-роботи, тому її використання без мережі є обмеженим.

4.6. FileWave

FileWave – це уніфіковане рішення для управління кінцевими точками (UEM), яке забезпечує централізоване управління пристроями та програмним забезпеченням у середовищах Windows, macOS, iOS, iPadOS, Android та Chrome OS. FileWave дозволяє автоматизувати завдання управління пристроями, такі як розгортання програм, управління оновленнями, налаштування політик безпеки, а також відстеження активності користувачів і пристроїв. Основна мета FileWave полягає в спрощенні процесу адміністрування великих IT-інфраструктур, де використовується

різноманітне обладнання, зменшуючи кількість ручних дій.

Порівняння інтеграції на різних ОС

FileWave надає глибоку інтеграцію з операційною системою Windows, забезпечуючи повний контроль над пристроями. Вона дозволяє встановлювати і управляти програмами, політиками безпеки, налаштуваннями оновлень і шифруванням за допомогою таких функцій, як Windows Configuration Manager та підтримка PowerShell-скриптів. Також доступні інструменти для автоматизації масових завдань, зокрема інсталяція пакетів програмного забезпечення і оновлень Windows на віддалених пристроях.

FileWave також підтримує інтеграцію з macOS, де рішення показує себе ефективним для управління політиками безпеки, шифруванням за допомогою FileVault, та розгортанням програмного забезпечення на пристроях Apple. FileWave може працювати з налаштуваннями профілів конфігурації для macOS, підтримуючи такі функції, як налаштування MDM (Mobile Device Management), централізоване керування політиками доступу і безпеки.

Хоча Chrome OS також підтримується FileWave, інтеграція тут не настільки глибока, як з Windows чи macOS. FileWave дозволяє виконувати базові дії, такі як управління додатками та інвентаризація пристроїв Chrome OS. Також підтримується синхронізація з Google Admin Console для автоматизованого управління пристроями, але інтеграція є менш гнучкою порівняно з рішеннями для інших платформ [29].

FileWave не підтримує інтеграцію з дистрибутивами Linux, такими як Ubuntu. Це є одним з ключових обмежень платформи, оскільки GNU/Linux стає все популярнішим серед організацій, що використовують open-source інфраструктуру. Відсутність підтримки Linux означає, що адміністратори не можуть централізовано керувати пристроями на основі Ubuntu через FileWave.

Порівняння FileWave з Microsoft Intune

Microsoft Intune – це хмарне рішення для управління кінцевими точками, яке забезпечує інтеграцію з операційними системами Windows, macOS, iOS, Android і Chrome OS. Ось основні відмінності між FileWave та Intune:

1) Підтримка платформ:
   - Intune має ширшу підтримку платформ, зокрема Linux (хоча обмежену для інвентаризації та управління політиками). FileWave не підтримує Ubuntu або інші дистрибутиви Linux, що робить Intune кращим вибором для організацій з гетерогенним середовищем, включаючи пристрої Linux.
   - FileWave, в свою чергу, спеціалізується на управлінні macOS і Windows, забезпечуючи глибшу інтеграцію з цими платформами, зокрема з FileVault для macOS і PowerShell для Windows(macos).
2) Гнучкість та функціональність:
   - Intune пропонує більш інтегроване рішення для управління через Entra ID та Microsoft 365, що дозволяє централізовано керувати ідентифікацією, доступом і безпекою користувачів. Intune також підтримує інші Microsoft продукти, такі як Microsoft Defender, що надає додаткові переваги в сфері кібербезпеки.
   - FileWave дозволяє гнучко керувати програмним забезпеченням і пристроями, особливо на платформах macOS і Windows. Однак інтеграція з хмарними рішеннями та кібербезпекою не настільки глибока, як у Intune. FileWave орієнтована на гнучке управління з мінімальним хмарним впливом, що може бути перевагою для організацій з обмеженим доступом до хмари.
3) Хмарні сервіси:
   - Intune працює виключно як хмарне рішення і вимагає постійного інтернет-з’єднання для повноцінної роботи. Це може бути недоліком для організацій, які не мають стабільного доступу до хмари.

– FileWave, хоча і підтримує хмарні сервіси, може працювати більш автономно, з мінімальним підключенням до хмари, що підходить для організацій, які працюють в офлайн середовищах.

Найкраща інтеграція FileWave

Найбільш ефективно FileWave працює з операційними системами Windows та macOS [30, 31]. Глибока інтеграція з інструментами управління для цих платформ, такими як PowerShell для Windows і FileVault для macOS, робить FileWave оптимальним вибором для організацій, що мають переважно ці операційні системи. FileWave дозволяє повністю контролювати управління пристроями, надаючи інструменти для розгортання програм, управління політиками безпеки і контролю доступу.

У випадку Chrome OS, FileWave підтримує основні функції, але можливості управління значно обмежені в порівнянні з Windows і macOS. Відсутність підтримки для Linux робить його менш привабливим для організацій з інфраструктурою на базі вільних рішень.

4.7. Powershell

PowerShell – це потужний інструмент для автоматизації задач, який став кросплатформенним із випуском версії 6. Однак існують суттєві відмінності між тим, як PowerShell функціонує на Windows і інших платформах, таких як Ubuntu, Chrome OS (через Crostini), і macOS. У цьому розділі ми детально розглянемо, в чому саме Windows має перевагу, а які функції PowerShell стали доступними на всіх платформах.

Переваги PowerShell для Windows

– Глибока інтеграція з операційною системою: Windows PowerShell 5.1 побудована на основі .NET Framework, що дозволяє працювати з багатьма системними компонентами Windows, включно з реєстром, сервісами, WMI (Windows Management Instrumentation), EventLog, та іншими функціями, недоступними на інших платформах. Наприклад,

такі команди як Get-Service, Set-Service, Get-EventLog та багато інших працюють лише на Windows через специфіку архітектури Windows.

- Windows Management Framework та WSMan: Windows PowerShell підтримує WS-Management (WinRM), який використовується для віддаленого управління комп'ютерами у Windows. Ця технологія недоступна на інших платформах, хоча PowerShell 7 підтримує SSH для віддаленого доступу на всіх системах.
- Підтримка старих модулів та компонентів: Багато застарілих модулів, таких як CimCmdlets, ISE, PSWorkflow та інші, доступні лише у Windows PowerShell, оскільки вони залежать від специфічних компонентів Windows, які не підтримуються у .NET Core.
- Функції реєстру та локальних облікових записів: Робота з Windows Registry через команди на кшталт Get-ItemProperty або управління локальними обліковими записами (LocalAccounts) також є ексклюзивною можливістю Windows.
- Специфічні для Windows інструменти адміністрування: PowerShell на Windows підтримує адміністрування таких специфічних компонентів, як служби, реєстр, EventLog та інші через відповідні модулі Microsoft.PowerShell.Management і Microsoft.PowerShell.Diagnostics, що недоступні в інших операційних системах.

Кросплатформні можливості PowerShell

- PowerShell Core та .NET Core: PowerShell 7 побудована на основі .NET Core, що зробило її кросплатформною. Це дозволяє працювати на різних ОС, таких як macOS, Linux (включно з Ubuntu), і навіть на Chrome OS через віртуальне середовище Crostini [32]. Основні функціональні можливості PowerShell, такі як робота з файлами, об'єктами, функціями, умовними операціями та потоками, залишаються ідентичними на всіх платформах [33].
- SSH-ремоутинг: У той час як WSMan доступний тільки у Windows, PowerShell 7 додала підтримку SSH-ремоутингу, що дозволяє

використовувати віддалене управління і на macOS, і на Linux. Це суттєво спрощує кросплатформне управління.

- Модулі з підтримкою PowerShell 7: Модулі, такі як Az для роботи з Azure, Microsoft Graph SDK, і більшість основних модулів для управління, стають доступними на всіх платформах. PowerShell забезпечує підтримку більшості модулів через кросплатформенний .NET Core, що робить можливим виконання більшості скриптів, незалежно від платформи [35].
- Команди файлової системи: PowerShell на Linux і macOS адаптований до роботи з їх файловими системами. Наприклад, файли у Unix-подібних системах є чутливими до регістру, що впливає на роботу команд PowerShell. Також підтримується використання слешів / і \ як роздільників шляхів.
- Інтероперабельність з командами Unix: PowerShell на Linux і macOS підтримує нативні Unix-команди та усуває конфлікти з основними командами (наприклад, ls, cp, mv), щоб користувачі могли безперешкодно використовувати команди Unix у PowerShell [34].

Хоча PowerShell став потужним кросплатформенним інструментом, Windows залишається найсильнішою платформою для цього середовища через глибоку інтеграцію з системними компонентами і підтримку специфічних модулів. Проте, кросплатформені можливості PowerShell значно розширилися з виходом версії 7, що дозволяє використовувати більшість базових команд і модулів на всіх сучасних платформах, включаючи Linux і macOS [36].

4.8. Microsoft 365

Огляд

Microsoft 365 (раніше Office 365) – це комплексний хмарний сервіс від Microsoft, який включає набір офісних додатків, а також інструменти для

спільної роботи та зберігання даних у хмарі через OneDrive. Сервіс доступний на багатьох платформах, таких як Windows, macOS, Android та iOS, що дозволяє користувачам працювати з документами та даними на різних пристроях. Проте функціональність може змінюватись в залежності від операційної системи.

Короткий опис програм Microsoft 365

- Word – потужний текстовий процесор для створення, редагування та форматування документів. Підтримує макроси, шаблони, розширені інструменти перевірки правопису та спільну роботу над документами.
- Excel – популярна програма для роботи з електронними таблицями. Excel має інструменти для обробки великих обсягів даних, створення діаграм, використання функцій та формул, а також підтримує автоматизацію за допомогою макросів (VBA).
- PowerPoint – засіб для створення презентацій, який підтримує мультимедійні елементи, анімації та можливість спільної роботи над презентаціями.
- Outlook – клієнт електронної пошти з функціями управління контактами, календарем та завданнями. Відмінно інтегрується з іншими програмами Microsoft 365 для спрощення робочих процесів.
- OneDrive – хмарне сховище файлів, що дозволяє зберігати документи, синхронізувати їх між пристроями та ділитися ними з іншими користувачами.
- Teams – платформа для спілкування та співпраці, що підтримує відеоконференції, чат, обмін файлами і спільну роботу над документами.
- Access – система управління базами даних, яка дозволяє створювати та керувати реляційними базами даних (доступно лише на Windows).
- Publisher – інструмент для створення друкованих публікацій, таких як брошури, буклети та інші маркетингові матеріали (доступно лише на Windows).

– Visio – програма для створення схем, діаграм та технічних креслень, зокрема блок-схем і діаграм бізнес-процесів (доступно лише на Windows).

Microsoft 365 під Windows та macOS

Windows є основною платформою для Microsoft 365, на якій реалізовано повний функціонал офісних програм. Версія для Windows підтримує всі додатки Microsoft 365, включно зі спеціалізованими програмами, такими як Access, Visio та Publisher, які відсутні на macOS [41]. Крім того, Microsoft 365 для Windows пропонує широку підтримку макросів на Visual Basic (VBA), що дозволяє автоматизувати робочі процеси, зокрема в Excel. Це особливо корисно для корпоративних користувачів.

macOS, хоч і підтримує більшість основних програм, має деякі обмеження. Зокрема, відсутність Access, Visio та Publisher. Також деякі функції, як-от макроси в Excel, можуть працювати менш стабільно або взагалі не підтримуватись через різницю в системній архітектурі. Попри ці недоліки, Microsoft 365 для macOS забезпечує високий рівень інтеграції з системою Apple, що робить роботу з програмами більш нативною для користувачів Mac.

Ubuntu: обмеження та альтернативи

Microsoft 365 не має офіційної десктопної версії для Ubuntu або інших дистрибутивів Linux. Однак користувачі можуть працювати з веб-версією Microsoft 365 через браузер, що забезпечує базовий функціонал для редагування документів. Ця версія не підтримує складні функції, як-от макроси чи інтеграція з OneDrive на рівні файлової системи. Для повноцінного використання Microsoft 365 на Ubuntu, можна скористатися альтернативними технологіями, такими як Wine або Crossover, які дозволяють запускати Windows-додатки на Linux. Проте, стабільність і функціональність через ці інструменти не завжди є надійними, особливо в частині роботи з хмарними сервісами.

Найкращою безкоштовною та вбудованою альтернативою для Ubuntu є

LibreOffice – це повнофункціональний кросплатформений офісний пакет, який підтримує багато форматів файлів Microsoft Office [37]. До його складу входять такі програми: Writer (аналог Microsoft Word), Calc (аналог Microsoft Excel), Impress (аналог Microsoft PowerPoint), Draw (для векторної графіки, частково аналог Microsoft Visio), Base (аналог Microsoft Access) та Math (для створення математичних формул). Однак можуть виникати проблеми із синхронним спільним онлайн-редагуванням, сумісністю форматування та підтримкою макросів під час обробки складних документів, створених у Microsoft Office.

Chrome OS: браузер та Cameyo

Chrome OS також не має нативної підтримки десктопних додатків Microsoft 365, але хмарні можливості цієї операційної системи дозволяють працювати з офісними програмами через веб-версії. Програми Microsoft 365 доступні через браузер, що дозволяє редагувати документи, зберігати їх у хмарі та співпрацювати з іншими користувачами. Водночас, веб-версія не підтримує всі функції десктопних програм – наприклад, складні формули в Excel або розширені інструменти для роботи з мультимедіа в PowerPoint можуть бути недоступними.

Для розширення можливостей Chrome OS, можна використовувати платформу Cameyo – це рішення від Google дозволяє запускати повноцінні десктопні додатки Microsoft 365 через браузер, незалежно від операційної системи. Це може бути ефективним способом використання Microsoft 365 на пристроях з Chrome OS, але робота через тонкий клієнт вимагає стабільного інтернет-з'єднання і може мати обмеження в продуктивності [40].

Google Workspace та iWork

Google Workspace є прямим конкурентом Microsoft 365 у хмарному сегменті. Він включає такі додатки, як Google Docs, Sheets та Slides, які є аналогами Word, Excel і PowerPoint відповідно [39]. Основною перевагою Google Workspace є зручність спільної роботи в реальному часі та повна інтеграція з Google Drive та Chrome OS. Однак він має обмеження щодо

підтримки складних форматів документів Microsoft Office. Наприклад, Excel-файли з макросами або складними таблицями можуть некоректно відображатися в Google Sheets. Також функції офлайн-доступу обмежені, хоча можливі через кешування даних у браузері.

iWork – це набір офісних додатків від Apple, включно з Pages (аналог Word), Numbers (аналог Excel) і Keynote (аналог PowerPoint). Він оптимізований для пристроїв на macOS та iOS і надає зручний та інтуїтивний інтерфейс для користувачів Apple [38]. Однак, у порівнянні з Microsoft 365, iWork має обмежену підтримку файлів Microsoft Office, що може призводити до проблем з форматуванням і функціональністю, особливо під час роботи з великими таблицями або складними презентаціями.

Тобто, кожна операційна система має свої сильні сторони і обмеження для роботи з офісними програмами. Windows залишається найбільш функціональною платформою для Microsoft 365, забезпечуючи доступ до всіх додатків та функцій. macOS надає потужні інструменти для роботи з офісними документами, хоча й має певні обмеження щодо специфічних додатків і макросів. Ubuntu не має офіційної підтримки Microsoft 365, але може використовувати веб-версії або Wine/Crossover для запуску десктопних програм, хоча стабільність може бути під питанням. Chrome OS забезпечує доступ до офісних додатків через браузер або Cameyo, хоча продуктивність таких рішень залежить від швидкості інтернету.

Тому, для користувачів, які шукають найбільш універсальну платформу для роботи з Microsoft 365, Windows залишається оптимальним вибором, хоча він достатньо добре працює на macOS. Проте альтернативи, як-от Google Workspace, LibreOffice або Cameyo, забезпечують гнучкість і доступність для користувачів інших ОС.

4.9. Adobe Creative Cloud

Adobe Creative Cloud – це комплексний набір інструментів,

розроблений Adobe для підтримки потреб творчих фахівців, що охоплює графічний дизайн, відеомонтаж, веб-розробку, аудіообробку та інші види контенту. Платформа пропонує як десктопні, так і мобільні додатки, а також інтегровані хмарні сервіси, що дозволяють спільну роботу та доступ до проєктів з різних пристроїв. Нижче наведено детальний огляд продуктів Creative Cloud та порівняння можливостей на macOS, Windows, ChromeOS та Ubuntu.

Огляд

1) Photoshop – професійне програмне забезпечення для роботи з растровими зображеннями, що дозволяє виконувати комплексну обробку фотографій, створювати цифрове мистецтво та редагувати зображення для різних медіа. Photoshop забезпечує високу гнучкість і є стандартом у галузі редагування зображень.

2) Illustrator – передовий інструмент для роботи з векторною графікою. Використовується для створення логотипів, ілюстрацій, інфографіки та інших векторних графічних компонентів. Illustrator відрізняється високою точністю та можливостями створення масштабованих зображень.

3) InDesign – інструмент для створення друкованих та цифрових публікацій, таких як журнали, брошури, електронні книги. InDesign підтримує інструменти для точного компонування тексту та зображень, що дозволяє створювати публікації професійної якості.

4) Premiere Pro – професійний відеоредактор, що використовується для монтажу відео різної складності – від коротких кліпів до повнометражних фільмів. Premiere Pro підтримує багатокамерний монтаж, кольорову корекцію та інтеграцію з іншими програмами Creative Cloud.

5) After Effects – інструмент для створення візуальних ефектів та анімації. Використовується для генерації динамічної графіки, спецефектів і є основним компонентом у пост-продакшн обробці відео.

6) Lightroom – професійне рішення для обробки фотографій,

орієнтоване на управління великими колекціями зображень та корекцію кольорів. Lightroom також підтримує обробку RAW-файлів, що надає користувачам максимальну гнучкість у редагуванні.

7) Adobe XD – інструмент для створення прототипів і розробки інтерфейсів користувача. Використовується для інтерактивного проєктування мобільних додатків та вебсайтів, надаючи функціонал для спільної роботи з дизайнерами та розробниками.

8) Dreamweaver – редактор для веброзробки, що підтримує одночасну роботу з візуальними та кодовими інтерфейсами. Dreamweaver дозволяє швидко створювати вебсайти та вебдодатки з використанням сучасних технологій HTML, CSS та JavaScript.

9) Audition – професійний інструмент для аудіообробки, що дозволяє здійснювати багатодоріжковий монтаж, запис та покращення якості звуку. Audition широко використовується для створення подкастів, аудіовставок для відео та іншого контенту.

10) Animate – програмне забезпечення для створення анімацій та інтерактивного контенту. Особливо популярне для створення анімацій у форматі HTML5, а також для розробки інтерактивних вебелементів.

11) Adobe Acrobat Pro – інструмент для професійної роботи з PDF-документами, що дозволяє редагувати, підписувати, коментувати та ділитися документами. Можливість використання електронних підписів робить Acrobat Pro важливим інструментом для бізнесу та управління документацією.

12) Adobe Spark – зручний інструмент для створення графіки, вебсторінок та коротких відео для соціальних медіа. Spark дозволяє швидко створювати якісний контент навіть без досвіду в дизайні.

13) Adobe Fonts – бібліотека ліцензованих шрифтів, доступних через підписку Creative Cloud, що дозволяє використовувати високоякісні шрифти у будь-яких проєктах, зберігаючи стиль та індивідуальність.

Порівняння можливостей на macOS і Windows

Програми Adobe Creative Cloud функціонально подібні на платформах macOS і Windows, проте існують деякі ключові відмінності в оптимізації та інтеграції:

– macOS є традиційно оптимізованою платформою для творчих фахівців через тісну інтеграцію з апаратним забезпеченням Apple, що особливо актуально для завдань, пов'язаних з графікою і дисплеями Retina. Значна частина користувачів відзначає покращену стабільність та продуктивність програм Adobe на macOS, зокрема при роботі з відео високої роздільної здатності та складною графікою.

– Windows забезпечує ширший вибір апаратного забезпечення та є доступнішою для більшості користувачів. Creative Cloud додатки працюють на Windows з повноцінним функціоналом, однак деякі аспекти, такі як кольорова корекція чи продуктивність GPU, можуть залежати від характеристик конкретного комп'ютера.

– Деякі програми, як-от Adobe XD, спочатку були розроблені під macOS, що могло вплинути на оптимізацію під цю платформу. Тим не менш, сучасні версії забезпечують повноцінну підтримку обох систем.

Хмарні можливості на ChromeOS та Ubuntu

На платформах ChromeOS та Ubuntu нативна підтримка десктопних додатків Adobe Creative Cloud відсутня. Однак існує можливість доступу до певних продуктів через вебдодатки та хмарні сервіси:

– Adobe Spark доступний через браузер і може бути використаний для створення базового графічного та відео контенту на ChromeOS та Ubuntu.

– Adobe Lightroom має вебверсію, яка надає можливості для редагування фотографій онлайн, що дозволяє працювати з фотографіями без встановлення десктопних додатків.

– Adobe Photoshop також має вебверсію, доступну через Creative Cloud, що дозволяє виконувати базові функції редагування зображень безпосередньо в браузері. Це забезпечує зручний доступ для користувачів ChromeOS та Ubuntu без потреби у десктопній версії.

– Хмарне зберігання, Creative Cloud Libraries та інші інтегровані сервіси доступні через вебінтерфейс, що дозволяє синхронізувати проєкти між пристроями та платформами.

Повноцінне використання таких програм, як Photoshop або Premiere Pro, залишається недосяжним на цих платформах через відсутність десктопних версій та обмеження підтримки апаратного прискорення.

Запуск Adobe Creative Cloud через Wine/Crossover

Запуск додатків Adobe через Wine або Crossover на Linux (включаючи Ubuntu) або ChromeOS є складним і не завжди надійним. Деякі старіші версії програм, як-от Photoshop або Lightroom, можуть частково працювати, але більшість сучасних версій Creative Cloud вимагають використання специфічних API Windows, які не повністю підтримуються в цих емуляторах.

Можливі проблеми включають:

– Некоректне відображення інтерфейсу користувача, що ускладнює роботу з програмами.
– Обмеження підтримки апаратного прискорення (GPU), що є критичним для обробки відео та роботи з графікою високої роздільної здатності.
– Проблеми з ліцензуванням та оновленням, оскільки Creative Cloud регулярно перевіряє ліцензії через інтернет, що може викликати збої у використанні програм.

Кросплатформенні альтернативи

Для тих, хто шукає кросплатформенні інструменти для роботи на Windows, macOS, Linux та інших системах, існує низка альтернатив з відкритим вихідним кодом або безкоштовних аналогів:

– GIMP – безкоштовний редактор растрової графіки, що надає базовий функціонал для редагування зображень і може бути альтернативою для Photoshop. Незважаючи на менший набір функцій, GIMP задовольняє більшість потреб у базовій обробці фотографій.
– Krita – інструмент для цифрового малювання та редагування, особливо популярний серед художників і ілюстраторів. Krita надає потужний

набір інструментів для малювання, підтримуючи роботу на різних платформах.

- Inkscape – безкоштовний векторний редактор, що може бути альтернативою для Adobe Illustrator. Inkscape дозволяє створювати масштабовані графічні елементи та працювати з різними форматами файлів.
- Kdenlive – відеоредактор з відкритим вихідним кодом, який працює на Linux, Windows та macOS і може служити альтернативою Adobe Premiere Pro. Kdenlive підтримує багатодоріжковий монтаж та базову кольорову корекцію.
- Audacity – безкоштовний аудіоредактор, що може слугувати аналогом Adobe Audition. Audacity дозволяє записувати, монтувати та редагувати аудіо з підтримкою різних ефектів і фільтрів.
- Blender – потужне програмне забезпечення для 3D-моделювання, анімації та рендерингу, яке також містить функції для відеомонтажу та створення спецефектів, подібні до After Effects. Blender є безкоштовним і доступним на всіх основних платформах.

Висновок: Adobe Creative Cloud є провідним набором інструментів для творчих професіоналів, але його використання на платформах ChromeOS та Ubuntu має суттєві обмеження через відсутність нативної підтримки десктопних додатків. Проте, завдяки вебдодаткам та хмарним сервісам, користувачі можуть отримати обмежений доступ до деяких функцій. Крім того, існують альтернативні програми з відкритим вихідним кодом, які, хоча і поступаються у функціональності, можуть задовольнити базові потреби креативної роботи на цих платформах.

З огляду на наведене порівняння, macOS виявляється найбільш оптимальною операційною системою для роботи з Adobe Creative Cloud завдяки тісній інтеграції з апаратним забезпеченням, стабільності та продуктивності. Windows залишається універсальною та доступною платформою, яка також здатна забезпечити повноцінний досвід роботи з

продуктами Adobe, проте деякі оптимізаційні аспекти можуть варіюватися залежно від апаратної конфігурації. ChromeOS та Ubuntu не можуть повністю конкурувати через обмеження підтримки десктопних додатків, але завдяки веб-інструментам надають обмежену функціональність для базових потреб.

РОЗДІЛ 5.
ПРОГНОЗУВАННЯ МАЙБУТНЬОГО ДАНИХ ОС

5.1. ChromeOS

Операційна система ChromeOS від Google перебуває на порозі значних змін, які можуть докорінно змінити майбутнє цієї платформи. Враховуючи розвиток технологій та нові підходи компанії, ChromeOS може стати ще більш інтегрованою з Android, що відкриває нові можливості для користувачів. Ось основні зміни, на які варто звернути увагу.

Google вже тривалий час інтегрує елементи Android в ChromeOS, але найближчим часом ця інтеграція може досягти свого апогею. ChromeOS перетвориться на Android-орієнтовану дистрибуцію з оптимізованим для десктопа інтерфейсом [45]. Такий підхід не лише розширить функціонал системи, а й дозволить ефективніше використовувати Android-додатки на ноутбуках і планшетах.

Перехід на Android також відкриває шлях для глибшого впровадження технологій штучного інтелекту [46]. Однією з таких ключових функцій є Gemini AI, яка надасть користувачам можливість взаємодіяти з AI для виконання складних завдань. Наприклад, функція Help me write допомагає генерувати та покращувати текстові документи, а Magic Editor дозволяє швидко редагувати фотографії з використанням штучного інтелекту. Інші AI-інструменти, такі як Help me read, допоможуть користувачам отримувати резюме документів та вебсайтів, а також задавати додаткові запитання для глибшого розуміння контенту.

Google також працює над новою версією браузера Chrome для Android, яка буде підтримувати розширення, але ця функціональність буде доступною переважно для десктопних пристроїв, таких як Chromebook [44]. Впровадження підтримки розширень забезпечить користувачам досвід, максимально наближений до повноцінного браузера для ПК, що дозволить

використовувати інструменти, такі як блокувальники реклами та інші корисні додатки.

Проте варто зазначити, чому Google взагалі переписує Chrome. Річ у тім, що Chrome є невід'ємною частиною ChromeOS, і браузер фактично є першою лінією захисту від шкідливих веб-програм. Через це в браузерах частіше знаходять вразливості, і тому їх регулярно оновлюють. У випадку більшості операційних систем, браузер можна оновити окремо, перезавантаживши лише його. Але в ChromeOS, щоб застосувати патч для браузера, необхідно оновлювати всю систему. Якщо операційна система перестає підтримуватися, то браузер також залишається без оновлень безпеки, що є значним ризиком.

Водночас, в Android завдяки більш модульній архітектурі системи, такі компоненти, як браузер, можуть оновлюватися через Google Play без потреби оновлювати всю операційну систему. Ця тенденція до відокремлення компонентів системи в рамках проекту Treble зростає, і Google, ймовірно, піде аналогічним шляхом і для Chromebook. Це дозволить частіше та ефективніше оновлювати браузер без залежності від глобальних оновлень всієї системи.

Одним із важливих змін стане відмова від ARCVM (Android Runtime for Chrome Virtual Machine), що на даний момент використовується для запуску Android-додатків у середовищі ChromeOS. Перехід на нативну Android-архітектуру дозволить суттєво підвищити продуктивність та знизити навантаження на систему, оскільки зникне потреба у віртуалізації [43]. Це спростить взаємодію з Android-додатками і зробить роботу системи швидшою та стабільнішою.

Google активно просуває свої власні процесори Tensor, і, з огляду на інтеграцію між Android та ChromeOS, ймовірно, ці процесори будуть використані і в майбутніх пристроях Chromebook. Це дозволить краще оптимізувати апаратне та програмне забезпечення, створюючи більш потужну та продуктивну екосистему .

Хоча веб-додатки (PWA) залишаються важливою частиною екосистеми ChromeOS, вони мають певні обмеження, особливо у взаємодії з операційною системою та можливості роботи офлайн. Android-додатки заповнять ці прогалини, забезпечуючи автономність та приватність, яких бракує PWA. Таким чином, роль Android-додатків зростатиме, і вони стануть основним інструментом для виконання багатьох завдань .

Незважаючи на перехід до архітектури Android, ChromeOS продовжуватиме підтримувати застосунки Debian через проєкт Crostini, який переноситься на Android [42]. Це дозволить користувачам запускати Linux-застосунки на Chromebook, забезпечуючи більшу гнучкість і функціональність для розробників і досвідчених користувачів.

Висновок: Майбутнє ChromeOS виглядає захоплюючим, адже нові зміни обіцяють зробити операційну систему ще більш функціональною, модульною та адаптованою до потреб сучасних користувачів. Перехід на Android-архітектуру не лише підвищить продуктивність і спростить взаємодію з Android-додатками, але й відкриє нові можливості для впровадження інноваційних рішень на основі штучного інтелекту. Технологія Gemini AI стане центральним елементом цієї трансформації, допомагаючи користувачам ефективніше виконувати завдання за допомогою функцій, таких як Help me write та Magic Editor.

Інтеграція Android-додатків замінить складні рішення на базі ARCVM, що зменшить навантаження на систему і зробить її роботу швидшою та стабільнішою. Підтримка Debian-додатків через Crostini збереже гнучкість системи для користувачів, які потребують доступу до Linux-застосунків. Усі ці нововведення зроблять ChromeOS більш потужною, багатофункціональною і готовою до майбутнього, де штучний інтелект буде невід’ємною частиною повсякденного користування технологіями.

5.2. macOS

Майбутнє macOS виглядає набагато спокійнішим порівняно з тим, що пропонує ChromeOS від Google. Причина цього криється в різному підході компаній до своїх операційних систем. Apple, на відміну від Google, ніколи не розробляла дві абсолютно різні платформи, подібно до Android та ChromeOS. Замість цього вона з самого початку розвивала macOS на спільному стеку з iPadOS та iOS. Такий підхід дозволив Apple не лише уникнути проблем з інтеграцією різних екосистем, але й забезпечив природне зближення мобільних і десктопних платформ через перехід на власні ARM-чипи серії Apple Silicon .

Поява власних процесорів Apple Silicon, таких як M1, M2 і майбутні покоління, не тільки забезпечує вражаючу продуктивність і енергоефективність, але й зближує macOS, iOS та iPadOS у єдину екосистему. Це дозволяє користувачам відчувати зручний та плавний перехід між пристроями, використовуючи схожий набір додатків та функцій .

Фактично, більшість цілей, які Google намагається досягти через об’єднання ChromeOS та Android, Apple вже реалізувала. Універсальна платформа, яку Apple розвиває роками, вже охоплює всі аспекти використання: від мобільних пристроїв до десктопів, що робить екосистему Apple цілісною та стабільною .

Однак, на тлі цієї стабільності, Apple продовжує впроваджувати нові технології, серед яких – штучний інтелект. Представлена Apple Intelligence, система штучного інтелекту, яка використовує генеративні моделі для виконання завдань на основі персонального контексту. Ця система вже інтегрована у macOS, iPadOS та iOS і дозволяє переписувати, коригувати та резюмувати текст у різних додатках, таких як Mail, Pages та Notes .

Крім того, завдяки технології Private Cloud Compute, обробка даних користувачів відбувається з високим рівнем конфіденційності, що відповідає високим стандартам безпеки, які Apple завжди ставить на перший план.

Apple Intelligence також пропонує нові можливості для створення зображень, керування фотографіями та спрощення рутинних завдань за допомогою глибокої інтеграції в операційні системи .

Ще однією важливою складовою майбутнього macOS є подальший розвиток технологій безпеки та мобільності, багато з яких впроваджуються завдяки тісній інтеграції з iPadOS та iOS. Наприклад, покращена інтеграція з iPhone дозволяє швидко переносити робочі процеси між пристроями, використовуючи загальні дані облікового запису та функціональні можливості iCloud. Такі інструменти, як Stage Manager і покращений багатозадачний інтерфейс, вже сьогодні демонструють, як Apple планує зробити свої пристрої більш зручними та продуктивними для користувачів .

Таким чином, хоча майбутнє macOS може здаватися менш інноваційним порівняно з експериментами Google, Apple вже реалізувала багато амбітних цілей щодо об’єднання своїх платформ. Тепер компанія зосереджується на розвитку штучного інтелекту, підвищенні рівня безпеки та мобільності, зберігаючи при цьому стабільність і цілісність своєї екосистеми.

5.3. Windows

На відміну від Google і Apple, Microsoft не вдалося втриматися на ринку мобільних пристроїв після невдач з Windows 10 Mobile та смартфонами Lumia. Це суттєво обмежило можливості компанії щодо інновацій, адже сьогодні більшість нововведень надходять з мобільних платформ на десктопи, а не навпаки. Однак Microsoft не втратила всі свої технологічні активи і, можливо, навіть зберегла частину команди з колишньої Nokia Mobile. Саме тому компанія продовжує активно розвивати потужні та енергоефективні пристрої на базі ARM-чипів в рамках ініціативи Copilot+ PC, яка має на меті забезпечити глибоку інтеграцію штучного інтелекту у Windows-пристрої .

Щоб вийти з тіні провалів на мобільному ринку, Microsoft запустила

Windows 11 як нову маркетингову стратегію, відмовившись від концепції універсальної операційної системи Windows 10 для мобільних і десктопних пристроїв. Проте основна проблема полягає в тому, що компанія не планує повністю відмовлятися від підтримки x86_64-архітектури (Intel та AMD), яка залишається основною для багатьох десктопів. Тому розробникам доведеться адаптувати свій софт для ARM-архітектури, що є викликом для компанії .

Як і Google з її проектом Treble, Microsoft прагне зробити компоненти Windows більш модульними. Наприклад, такі програми, як Paint, Edge та Notepad, тепер можна завантажити з Microsoft Store окремо, тоді як раніше вони були невіддільними частинами ОС. Це дозволяє оновлювати окремі компоненти системи без необхідності перезавантаження комп’ютера, що робить систему більш гнучкою та стабільною. Крім того, нові функції можуть приходити у вигляді накопичувальних оновлень, без необхідності глобальних апдейтів, які можуть ламати сумісність із обладнанням та програмами .

Ще одним нововведенням є Hotpatching, яке дозволяє встановлювати оновлення без необхідності перезавантаження системи, що є частиною планів Microsoft для Windows Server 2025. Це значно скорочує час простою та знижує навантаження на системи, що є ключовим для корпоративних користувачів .

Microsoft також активно розвиває інтеграцію з Linux, включаючи код зі свого гіпервізора Hyper-V, що використовується для віртуалізації. Проект WSL 2 (Windows Subsystem for Linux) продовжує розвиватися, що дозволяє запускати Linux-додатки безпосередньо в Windows. Microsoft також забезпечує інтеграцію Windows з мобільними пристроями на базі Android та iOS. Деякі чутки навіть припускають можливий перехід Windows на ядро Linux, хоча це виглядає малоймовірним на поточному етапі.

До того ж, Microsoft розвиває функціонал штучного інтелекту в рамках Copilot+ PCs, що включає нові можливості для підвищення продуктивності та безпеки. Однією з таких функцій є Recall, яка використовується для пошуку і

відновлення контенту, переглянутого на пристрої. Recall робить знімки активного екрана кожні кілька секунд і зберігає їх на локальному диску у зашифрованому вигляді. Це дозволяє користувачам швидко знаходити потрібний контент на основі текстових пошуків або за допомогою таймлайну, що дає змогу переглядати всі збережені знімки екрана .

Завдяки потужним можливостям нових процесорів на базі ARM, таких як Snapdragon X Elite та інших чипів, Recall може працювати з величезними обсягами даних, забезпечуючи високу швидкість пошуку. Microsoft інтегрує цю функцію з іншими AI-інструментами для покращення роботи з контентом, що стає ще одним важливим кроком на шляху до підвищення ефективності та зручності роботи на Windows .

Таким чином, хоча Windows і рухається у бік еволюційних змін, а не революційних, компанія активно інвестує в нові технології та намагається адаптувати свою операційну систему до сучасних потреб, зокрема через інтеграцію штучного інтелекту та покращену підтримку ARM-пристроїв.

5.4. Ubuntu

Майбутнє Ubuntu, швидше за все, залишатиметься досить передбачуваним і подібним до того, що ми бачимо у Windows, оскільки Canonical припинила розробку власної оболонки Unity, яка планувалася як універсальна для телефонів і десктопів, передавши її подальшу розробку спільноті. Це означає, що Canonical вирішила зосередитися на більш стабільних і широко використовуваних технологіях, таких як GNOME, яку компанія активно оптимізує. Раніше GNOME відзначався певною повільністю і нестабільністю анімацій, але завдяки патчам від Canonical, GNOME стає більш гладким і продуктивним, що є важливим для користувачів десктопних редакцій Ubuntu.

Однією з ключових сфер розвитку Ubuntu є інтеграція з Windows Subsystem for Linux (WSL). Ця система дозволяє запускати Ubuntu на

Windows, і Canonical продовжує її активно розвивати, забезпечуючи більш глибоку інтеграцію та стабільність для розробників, які працюють у гібридному середовищі. Це сприяє популяризації Ubuntu серед розробників, що використовують Windows для тестування і розробки програмного забезпечення.

Ще одним важливим напрямом є тісна інтеграція серверної версії Ubuntu з хмарними сервісами таких провайдерів, як Amazon, Google та Microsoft Azure. Canonical прагне забезпечити зручну і надійну підтримку хмарних рішень, що робить Ubuntu важливим гравцем у сфері корпоративних обчислень. Це дозволяє легко розгортати серверні рішення на основі Ubuntu в хмарі та управляти ними за допомогою хмарних платформ.

Snap залишається одним з важливих аспектів розвитку Ubuntu. Хоча технологія отримує як похвалу за універсальність, так і критику за швидкість, Canonical робить ставку на її розвиток, поступово роблячи snap-пакети швидшими і більш нативними. Вони спрощують процес оновлення програм і підтримки залежностей, особливо для LTS-випусків (Long Term Support), що важливо для корпоративних користувачів. Canonical, ймовірно, продовжить просувати Snap як головний інструмент для установки програмного забезпечення, поступово відмовляючись від класичних Debian-пакетів.

Що стосується ядра Linux, Canonical планує прискорити доставку нових версій ядра, впроваджуючи у бета-випуски реліз-кандидати, а не лише стабільні версії. Це дозволить користувачам швидше отримувати новітні функції та покращення безпеки, що критично важливо для сучасних корпоративних систем.

Попри те, що Canonical позиціонує Ubuntu як стабільний дистрибутив, орієнтований на користувачів і бізнес, компанія може поступово переглянути свою стратегію стосовно класичних Debian-пакетів. Ймовірно, спільнота та бізнес-користувачі будуть поступово підготовлені до більшого фокусу на універсальних Snap-пакетах, щоб уникнути проблем з залежностями в LTS-випусках та забезпечити легше підтримання сучасного програмного

забезпечення для всіх дистрибутивів.

В умовах глобальної політичної та економічної нестабільності, такої як санкційні війни та обмеження на використання певних технологій, Ubuntu є привабливим рішенням для організацій, які прагнуть незалежності від державної та корпоративної політики великих постачальників програмного забезпечення. Як дистрибутив із відкритим кодом, Ubuntu може бути розгалужений і налаштований для задоволення конкретних корпоративних потреб, забезпечуючи організаціям гнучкість та автономію. Якщо виникнуть технологічні чи юридичні труднощі з використанням вебсервісів Canonical, організації можуть перейти на локальні дзеркала або розробити власні рішення на основі форку Ubuntu.

Декілька організацій і урядів успішно адаптували Ubuntu або подібні дистрибутиви з відкритим кодом для своїх внутрішніх потреб. Наприклад:

– Жандармерія Франції: Цей підрозділ національних правоохоронних органів Франції перейшов на Ubuntu у 2008 році, створивши власну версію під назвою GendBuntu. Цей крок знизив залежність від пропрієтарного програмного забезпечення і дозволив зберегти контроль над IT-інфраструктурою, суттєво заощадивши кошти.

– Місто Мюнхен: Як один із перших урядових користувачів Linux, Мюнхен перейшов на LiMux, спеціально розроблену версію Linux на основі Ubuntu, з метою знизити витрати та отримати незалежність від великих постачальників ПЗ. Хоча місто згодом повернулося до пропрієтарного ПЗ, цей проєкт продемонстрував можливість адаптації Linux для потреб державного сектора.

– Китай: У відповідь на зростаючі побоювання щодо залежності від іноземних технологій Китай розробив Ubuntu Kylin, локалізовану та адаптовану версію Ubuntu, пристосовану до потреб урядових і корпоративних користувачів Китаю. Цей дистрибутив забезпечує сумісність з унікальною IT-інфраструктурою та регуляторними вимогами Китаю.

– Міністерство національної оборони Південної Кореї: Південна Корея

також вирішила перейти на системи з відкритим кодом, використовуючи Ubuntu як основу для зниження залежності від пропрієтарних платформ та вирішення питань кібербезпеки.

Ці приклади показують, як Ubuntu та інші дистрибутиви з відкритим кодом можуть бути адаптовані для задоволення конкретних потреб організацій, що діють у різних геополітичних умовах. Завдяки налаштуванню програмного забезпечення з відкритим кодом, ці установи отримують більшу автономію та контроль над своєю технологічною інфраструктурою, зменшуючи залежність від зовнішніх постачальників програмного забезпечення.

У майбутньому Ubuntu продовжуватиме залишатися стабільною компіляцією новітніх вільних технологій із відкритим кодом, зосередженою на розвитку таких ключових аспектів, як інтеграція з хмарними сервісами, вдосконалення GNOME, пришвидшення впровадження нових версій ядра Linux та поширення snap-пакетів. Canonical продовжить поступово скорочувати залежність від традиційних Debian-пакетів, щоб забезпечити легше оновлення та підтримку програмного забезпечення.

Проте в умовах зростаючої політичної та економічної напруженості, організації все частіше звертатимуть увагу на Ubuntu як на інструмент для забезпечення технологічної автономії. Це надає дистрибутиву додаткові шанси для поширення, особливо серед корпоративних користувачів, що шукають стабільності та контролю над своїми технологіями.

РОЗДІЛ 6
РЕКОМЕНДАЦІЇ ЩОДО ВИБОРУ ОС ДЛЯ РІЗНИХ ТИПІВ ОРГАНІЗАЦІЙ

На основі аналізу чотирьох операційних систем – Chrome OS, macOS, Windows та Ubuntu – варто зазначити, що кожна система має свої унікальні переваги та недоліки залежно від потреб різних типів організацій.

1) Chrome OS:

– Переваги: Chrome OS вирізняється високим рівнем безпеки "з коробки" завдяки архітектурі, побудованій навколо концепції "нульової довіри". Відсутність прав адміністратора, ізоляція процесів (sandboxing) та автоматичні оновлення роблять її ідеальною для освітніх установ, благодійних організацій та підприємств, де співробітники не мають глибоких технічних знань. Вона також підходить для організацій, які прагнуть мінімізувати витрати на технічну підтримку та адміністрування.

– Недоліки: Хмарозалежність Chrome OS обмежує її використання в середовищах з високими вимогами до автономності, таких як стратегічні підприємства чи критична інфраструктура. Відсутність широкої підтримки корпоративного ПЗ також обмежує її вживання у великих ентерпрайзах. Chrome OS встановлюється на спеціалізовані фірмові пристрої, що забезпечує сумісність із апаратними функціями. Водночас вона не підтримує офлайн-аккаунти та не дозволяє оновлюватися з інших джерел, що обмежує її автономність. Хоча вихідний код багатьох компонентів відкритий, базова система залишається дуже залежною від хмарних сервісів Google, тому можливий лише теоретичний форк. Однак є обґрунтовані сподівання, що міграція ChromeOS на платформу Android забезпечить більш нативну інтеграцію із сервісами Microsoft 365, Intune, FileWave, а також можливість використовувати облікові записи, незалежні від Google. Про це свідчить досвід експлуатації планшетів і смартфонів на Android.

2) macOS:

– Переваги: Високий рівень продуктивності, інтеграція з

апаратним забезпеченням та просунуті технології безпеки, такі як SIP (System Integrity Protection), роблять macOS ідеальним рішенням для інноваційних стартапів, креативних індустрій та компаній, що активно використовують технології Apple. macOS підходить для підприємств, що шукають баланс між продуктивністю, безпекою та сумісністю з корпоративним ПЗ, наприклад, через підтримку Adobe Creative Cloud.

– Недоліки: macOS може бути дорогим варіантом для малих і середніх підприємств через високу вартість обладнання Apple, що обмежує її використання в бюджетних організаціях. Важливо відзначити, що macOS, як і Chrome OS, встановлюється на фірмових пристроях, що забезпечує повну підтримку всіх апаратних функцій. Apple Silicon є лідером серед енергоефективних ноутбуків, що робить macOS ідеальним вибором для користувачів, які цінують тривалий час автономної роботи. Для оновлень macOS вимагає підключення до серверів Apple, що впливає на її автономність від хмарних сервісів.

3) Windows:

– Переваги: Windows – це найпопулярніша корпоративна ОС завдяки підтримці широкого спектра програмного забезпечення, таких як Microsoft 365, Intune та Active Directory. Вона підходить для великих підприємств і державного сектору, де важлива інтеграція з корпоративною інфраструктурою та потужні інструменти адміністрування.

– Недоліки: Незважаючи на підтримку корпоративного ПЗ, Windows є вразливішою до кіберзагроз порівняно з macOS та ChromeOS і потребує більшого налаштування безпеки з боку адміністратора. Це може створювати додаткові витрати на технічне обслуговування для малих та середніх підприємств. Крім того, Windows активно просуває хмарні сервіси Microsoft, такі як Entra ID, Intune, Microsoft 365 та цифрову активацію ліцензії, що робить систему залежнішою від хмари, ніж Ubuntu.

Хоча Microsoft поки не відмовляється від «застарілих» компонентів, таких як Microsoft Office LTSC, Microsoft System Center Configuration

Manager, офлайн-оновлення через Windows Server Update Services та KMS-активація Windows через локальний Windows-сервер, хмарні сервіси залишаються домінуючими. Більше того, Microsoft активно просуває концепцію тонкого клієнта Windows 365 Link, який відтворює операційну систему Windows 11 з потужного хмарного сервісу Azure.

Таке рішення дозволяє користувачам використовувати ресурси хмарної версії Windows, яка виконується на серверах Azure, тоді як локальні пристрої працюють як "тонкі клієнти". Ключовими перевагами таких пристроїв є: швидке розгортання, оновлення, та відновлення до заводських налаштувань; централізоване адміністрування через Entra ID та Intune; висока продуктивність, оскільки основні обчислювальні операції виконуються на потужних серверах Azure. Проте існують і певні обмеження.

Однією з головних проблем є залежність від стабільного та швидкого інтернет-з’єднання: у разі втрати зв’язку доступ до робочого середовища стає неможливим. Крім того, використання Windows 365 створює сильну залежність від екосистеми Microsoft, що може бути недоліком для компаній, які прагнуть більшої автономії.

4) Ubuntu:

– Переваги: Ubuntu є безкоштовним та відкритим рішенням, що підходить для організацій з обмеженими бюджетами. Вона забезпечує високу гнучкість та незалежність від хмарних сервісів, що робить її ідеальним вибором для підприємств з критично важливими завданнями, таких як стратегічні підприємства або ті, що обслуговують критичну інфраструктуру. Ubuntu також підходить для розробників та технічних стартапів, які цінують відкритий код і адаптивність ОС.

– Недоліки: Відсутність прямої підтримки популярного корпоративного ПЗ, такого як Microsoft Office, може обмежити її використання в традиційних офісах. Водночас Ubuntu надає велику свободу конфігурації, що робить її легкою до пошкодження у разі необережного поводження з рут-правами, навіть простіше, ніж Windows. Проте Ubuntu є

більш незалежною від хмари, ніж інші ОС, і залишається найбільш гнучкою для підприємств, що шукають політичну та технологічну автономність.

Висновки щодо збалансованості: Найбільш збалансованими системами є macOS та Windows (по 8 балів), оскільки вони мають міцні позиції як у безпеці, так і в продуктивності та сумісності з корпоративним ПЗ. Однак, macOS краще підходить для креативних і технологічних компаній, а Windows – для великих корпоративних середовищ.

Системи розташовані в таблиці за принципом п'єдесталу на олімпіаді. Чим менше балів, тим система краще.

Таблиця 6.1.

Олімпіадне порівняння різних ОС

ОС	Хмаронезалежність	Продуктивність	Корпоративне ПЗ	Безпека	Підсумковий бал
ChromeOS	4	4	4	1	13
macOS	3	1	2	2	8
Windows	2	2	1	3	8
Ubuntu	1	3	3	4	11

Ідеальна операційна система майбутнього – це поєднання найкращих властивостей існуючих ОС. Вона повинна поєднувати тісну інтеграцію з обладнанням, що забезпечує максимальну продуктивність і ефективність, як це демонструє macOS.

Окрім цього, система має володіти захистом від помилкових дій користувачів та простотою управління, подібними до Chrome OS, що дозволяє мінімізувати ризики від некоректного використання та спрощує адміністрування великих інфраструктур.

Не менш важливим аспектом є підтримка потужних корпоративних технологій і широка сумісність з інфраструктурними рішеннями, як у Windows, що дозволить інтегрувати систему в будь-яке корпоративне

середовище, незалежно від розміру чи складності. Водночас, система має залишатися гнучкою та незалежною, як це демонструє Ubuntu, надаючи можливість модифікацій та незалежність від закритих вендорів, забезпечуючи політичну та технологічну автономність.

Підвищення стандартів безпеки, гнучкості та інтеграції є важливим вектором для майбутнього розвитку операційних систем. Створення такої ідеальної ОС потребує нових підходів до взаємодії з апаратним забезпеченням, впровадження інноваційних механізмів захисту, розвитку автоматизованих рішень для адміністрування та підтримки корпоративного ПЗ. Така система стала б еталоном не лише для комерційного сектору, але й для критично важливих інфраструктур, державного управління та інноваційних технологічних стартапів.

Цей синтез найкращих практик і технологій приведе до створення нового покоління операційних систем, які зможуть підняти стандарти на новий рівень, забезпечивши не лише зручність і безпеку, але й адаптивність та довготривалу стійкість. Це стане основою для розвитку майбутніх інформаційних екосистем, де автономність, прозорість і потужність будуть ключовими вимогами.

Тому вивчення й удосконалення таких систем є важливим кроком до побудови надійної цифрової інфраструктури, яка відповідатиме вимогам часу та забезпечуватиме стабільність, безпеку та прогрес для всіх сфер людської діяльності.

ВИСНОВОК

У ході виконання магістерської роботи було досліджено особливості настільних операційних систем у контексті системного адміністрування та безпеки, що є ключовими аспектами для їх використання в корпоративному середовищі. Зокрема, виконано наступне:

1. Аналіз обраних операційних систем: Проведено порівняльний аналіз чотирьох операційних систем — Chrome OS, macOS, Windows та Ubuntu, — що дозволило визначити їх переваги та недоліки з точки зору безпеки, продуктивності, зручності використання та інтеграції з корпоративними сервісами.

2. Порівняння систем захисту: Вивчено архітектуру безпеки кожної з операційних систем. Визначено, що Chrome OS забезпечує найвищий рівень автоматизованого захисту «з коробки», macOS вирізняється високою стабільністю та інтеграцією апаратних і програмних рішень, а Windows пропонує широку сумісність і функціональність для корпоративного середовища. Ubuntu забезпечує гнучкість і можливості налаштування для специфічних потреб.

3. Тестування продуктивності: Проведено тестування обчислювальних і графічних можливостей операційних систем на однаковому апаратному забезпеченні, що дозволило оцінити їхню ефективність для різних завдань.

4. Інтеграція з корпоративними системами: Вивчено можливості інтеграції кожної операційної системи з корпоративним програмним забезпеченням, зокрема Microsoft 365, Active Directory, та іншими сервісами, які є важливими для забезпечення злагодженої роботи організацій.

5. Прогнозування розвитку: Проаналізовано сучасні тенденції в розвитку операційних систем, зокрема вплив хмарних технологій, штучного інтелекту та мобільних платформ, що дозволило сформулювати прогноз щодо перспектив їх використання у корпоративному середовищі.

6. Рекомендації: На основі проведеного аналізу розроблено рекомендації щодо вибору операційної системи для корпоративних середовищ, враховуючи специфіку їхньої діяльності, потребу у високій продуктивності, безпеці та сумісності з існуючою інфраструктурою.

Результати роботи можуть бути використані для оптимізації вибору операційних систем у різних типах організацій, а також для розробки політик безпеки, що враховують сучасні загрози. Практична новизна дослідження полягає у розробці рекомендацій, які допоможуть організаціям ефективніше використовувати ресурси, підвищувати рівень захищеності даних і знижувати витрати на адміністрування.

Отримані результати можуть бути корисними для підприємств, які прагнуть інтегрувати сучасні технології у свою діяльність, забезпечуючи високий рівень захисту та стабільності своєї інформаційної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Statcounter Global Stats. Операційні системи: Частка ринку в усьому світі [Електронний ресурс]. – Режим доступу: https://gs.statcounter.com (дата звернення: вересень 2024).

2. Найбезпечніша ОС з коробки [Електронний ресурс]. – Режим доступу: https://services.google.com/fh/files/misc/chromeos-the-most-secure-os-out-of-the-box.pdf.

3. SunTimes. Патч Барміна може пошкодити UEFI [Електронний ресурс]. – Режим доступу: https://suntimes.com.ua/didzhytal/patch-barmina-mozhe-poshkoditi-uefi.html.

4. Linux на Chrome OS [Електронний ресурс]. – Режим доступу: https://chromeos.dev/en/linux.

5. Android-додатки на Chrome OS [Електронний ресурс]. – Режим доступу: https://chromeos.dev/en/android.

6. Покращення продуктивності за допомогою нових функцій керування ресурсами ARC [Електронний ресурс]. – Режим доступу: https://chromeos.dev/en/posts/improving-performance-with-new-arc-resource-management-features.

7. Steam для Chromebook (бета) [Електронний ресурс]. – Режим доступу: https://support.google.com/chromebook/answer/14220699?hl=en.

8. macOS – Безпека – Apple [Електронний ресурс]. – Режим доступу: https://www.apple.com/macos/security/.

9. Як перевстановити macOS [Електронний ресурс]. – Режим доступу: https://support.apple.com/en-us/102655.

10. Документація з безпеки Windows [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/windows/security/.

11. Документація Windows Subsystem for Linux [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/windows/wsl/.

12. Реєстр – додатки Win32 | Microsoft Learn [Електронний ресурс]. –

Режим доступу: https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry.

13. Огляд Windows 10X: концепція, архітектура, інтерфейс [Електронний ресурс]. – Режим доступу: https://root-nation.com/ua/articles-ua/windows-ua/ua-oglyad-microsoft-windows-10x/.

14. Варіанти Ubuntu [Електронний ресурс]. – Режим доступу: https://ubuntu.com/desktop/flavours.

15. AppArmor | Ubuntu [Електронний ресурс]. – Режим доступу: https://ubuntu.com/server/docs/apparmor.

16. UFW – Wiki допомоги спільноти [Електронний ресурс]. – Режим доступу: https://help.ubuntu.com/community/UFW.

17. Ubuntu як незмінний настільний Linux | Ubuntu [Електронний ресурс]. – Режим доступу: https://ubuntu.com/blog/ubuntu-core-an-immutable-linux-desktop.

18. Інтеграція Active Directory за допомогою Directory Utility на Mac [Електронний ресурс]. – Режим доступу: https://support.apple.com/guide/directory-utility/integrate-active-directory-diru39a25fa2/mac.

19. Підключення нового пристрою Windows до Microsoft Entra під час первинного налаштування [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/entra/identity/devices/device-join-out-of-box.

20. Підключення пристрою Mac до Microsoft Entra ID через Company Portal (попередній перегляд) [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/entra/identity/devices/device-join-microsoft-entra-company-portal.

21. Посібник адміністратора XCreds [Електронний ресурс]. – Режим доступу: https://twocanoes.com/knowledge-base/xcreds-admin-guide/.

22. Використання AuthD з Entra ID на Ubuntu 24.04 [Електронний ресурс]. – Режим доступу: https://www.linkedin.com/pulse/using-authd-entra-id-ubuntu-2404-don-fountain-z31oe/.

23. Як інтегрувати Ubuntu Desktop з Active Directory [Електронний ресурс]. – Режим доступу: https://ubuntu.com/engage/microsoft-active-directory.

24. Реєстрація пристрою Linux в Intune [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/mem/intune/user-help/enroll-device-linux.

25. Як перенести пристрої в Chrome Management [Електронний ресурс]. – Режим доступу: https://support.google.com/chrome/a/answer/7497916.

26. Налаштування єдиного входу та реєстрації користувачів між Microsoft Entra ID та ChromeOS [Електронний ресурс]. – Режим доступу: https://support.google.com/chrome/a/answer/12103994.

27. Як налаштувати умовний доступ для ChromeOS з Microsoft Entra ID [Електронний ресурс]. – Режим доступу: https://support.google.com/chrome/a/answer/13530707.

28. Дослідження підтримки Intune для ChromeOS [Електронний ресурс]. – Режим доступу: https://joymalya.com/exploring-intune-chrome-os-support/.

29. Chrome OS | База знань FileWave [Електронний ресурс]. – Режим доступу: https://kb.filewave.com/books/chromeos.

30. Microsoft Windows | База знань FileWave [Електронний ресурс]. – Режим доступу: https://kb.filewave.com/books/chromeos.

31. macOS | База знань FileWave [Електронний ресурс]. – Режим доступу: https://kb.filewave.com/books/macos.

32. Перехід з Windows PowerShell 5.1 на PowerShell 7 [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/powershell/scripting/whats-new/migrating-from-windows-powershell-51-to-powershell-7.

33. Відмінності між Windows PowerShell 5.1 і PowerShell 7.x [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/powershell/scripting/whats-new/differences-from-windows-powershell.

34. Відмінності PowerShell на платформах, відмінних від Windows

[Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/powershell/scripting/whats-new/unix-support.

35. Історія випуску модулів і командлетів [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/powershell/scripting/whats-new/cmdlet-versions.

36. Сумісність модулів PowerShell 7 [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/powershell/scripting/whats-new/module-compatibility.

37. Порівняння функцій: LibreOffice та Microsoft Office [Електронний ресурс]. – Режим доступу: https://wiki.documentfoundation.org/Feature_Comparison:LibreOffice-_Microsoft_Office.

38. iWork – Apple [Електронний ресурс]. – Режим доступу: https://www.apple.com/iwork/.

39. Google Workspace: безпечні онлайн-інструменти для продуктивності та співпраці [Електронний ресурс]. – Режим доступу: https://workspace.google.com/.

40. Cameyo: Віртуалізація застосунків | Доставка віртуальних застосунків [Електронний ресурс]. – Режим доступу: https://cameyo.com/.

41. Microsoft 365 [Електронний ресурс]. – Режим доступу: https://www.office.com/.

42. Google готується дозволити запуск Linux-додатків на Android, подібно до Chrome OS [Електронний ресурс]. – Режим доступу: https://www.androidauthority.com/android-linux-terminal-app-3489887/.

43. Віртуальна машина Linux ARCVM займає всю оперативну пам’ять і процесор на Chromebook з ТІЛЬКИ БАЗОВИМИ ДОДАТКАМИ [Електронний ресурс]. – Режим доступу: https://support.google.com/chromebook/thread/246040605/linux-arcvm-virtual-machine-takes-up-all-the-ram-and-cpu-on-a-chromebook-with-only-default-apps.

44. Google тестує нову версію Chrome для Android із підтримкою

розширень [Електронний ресурс]. – Режим доступу: https://www.androidauthority.com/desktop-chrome-android-extensions-3488455.

45. Google нарешті приймає Android для настільних комп'ютерів, і я в захваті [Електронний ресурс]. – Режим доступу: https://www.howtogeek.com/google-is-finally-embracing-android-desktops-and-im-stoked/.

46. Побудова швидшого, розумнішого досвіду Chromebook з використанням найкращих технологій Google [Електронний ресурс]. – Режим доступу: https://blog.chromium.org/2024/06/building-faster-smarter-chromebook.html.

47. Порівняння редакцій Landscape [Електронний ресурс]. – Режим доступу: https://ubuntu.com/landscape/pricing.