ТЕМА 9. ОПЕРАЦІЙНІ СИСТЕМИ

9.1 Архітектура операційних систем.
9.2. Процеси і потоки в операційних системах.
9.3. Керування пам’яттю в операційних системах.
9.4. Файлові системи.
9.5. Захисні механізми операційних систем (Unix, Windows Server 2022, Windows 10/11)

9.1. Архітектура операційних систем

Операційна система, скор. **ОС** (англ. *operating system, OS*) – комплекс взаємозалежних програм, призначених для управління ресурсами комп'ютера та організації взаємодії з користувачем.

У логічній структурі типової обчислювальної системи операційна система займає становище між пристроями з їхньою мікроархітектурою, машинною мовою і, можливо, власними (вбудованими) мікропрограмами (драйверами) – з одного боку – і прикладними програмами з іншого.

Розробникам програмного забезпечення операційна система дозволяє абстрагуватися від деталей реалізації та функціонування пристроїв, надаючи мінімально необхідний набір функцій (див. інтерфейс програмування додатків).

У більшості обчислювальних систем операційна система є основною, найбільш важливою (іноді й єдиною) частиною системного програмного забезпечення. З 1990-х років найбільш поширеними операційними системами є системи сімейства Windows, Unix і UNIX-подібні системи.

Функції

Основні функції:

– Виконання запитів програм (введення та виведення даних, запуск та зупинення інших програм, виділення та звільнення додаткової пам'яті та ін.).

– Завантаження програм на оперативну пам'ять та його виконання.

– Стандартизований доступ до периферійних пристроїв (пристрою введення-виведення).

– Управління оперативною пам'яттю (розподіл між процесами, організація віртуальної пам'яті).

– Керування доступом до даних на енергонезалежних носіях (таких як жорсткий диск, оптичні диски та ін), організованим у тій чи іншій файловій системі.

– Забезпечення інтерфейсу користувача.

– Збереження інформації про помилки системи.

Додаткові функції:

– Паралельне чи псевдопаралельне виконання завдань (багатозадачність).

– Ефективний розподіл ресурсів обчислювальної системи між процесами.

– Розмежування доступу різних процесів до ресурсів.

– Організація надійних обчислень (неможливість одного обчислювального процесу навмисно або помилково вплинути на обчислення в іншому процесі), заснована на розмежуванні доступу до ресурсів.

– Взаємодія між процесами: обмін даними, взаємна синхронізація.

– Захист самої системи, а також даних користувача та програм від дій користувачів (зловмисних або через незнання) або додатків.

– Розрахований на багато користувачів режим роботи і розмежування прав доступу (автентифікація, авторизація).

Поняття

Існують дві групи визначень операційної системи: «набір програм, керуючих обладнанням» та «набір програм, керуючих іншими програмами». Обидві вони мають свій точний технічний зміст, який пов'язаний із питанням, у яких випадках потрібна операційна система.

Є програми обчислювальної техніки, котрим операційні системи зайві. Наприклад, вбудовані мікрокомп'ютери, що містяться в багатьох побутових приладах, автомобілях (іноді по десятку в кожному), найпростіших стільникових телефонах, постійно виконують лише одну програму, що запускається після вмикання. Багато простих ігрових приставок – також спеціалізованих мікрокомп'ютерів – можуть обходитися без операційної системи, запускаючи при включенні програму, записану на вставленому в пристрій «картриджі» або компакт-диску.

Операційні системи потрібні:

– якщо потрібний універсальний механізм збереження даних;

– для надання програм системних бібліотек з підпрограмами, що часто використовуються;

– для розподілу повноважень;

– потрібна можливість імітації «одночасного» виконання кількох програм на одному комп'ютері;

– для керування процесами виконання окремих програм.

Таким чином, сучасні універсальні операційні системи можна охарактеризувати насамперед як:

– що використовують файлові системи (з універсальним механізмом доступу до даних),

– розраховані на багато користувачів (з поділом повноважень),

– багатозадачні (з розподілом часу).

Багатозадачність і розподіл повноважень вимагають певної ієрархії привілеїв компонентів у операційній системі. У складі операційної системи розрізняють три групи компонентів:

– ядро, що містить планувальник; драйвери пристроїв, які безпосередньо керують обладнанням; мережна підсистема; файлова система;

– системні бібліотеки;

– оболонка з утилітами.

Більшість програм, як системних (що входять до операційної системи), так і прикладних, виконуються в непривілейованому («користувальницькому»)

режимі роботи процесора і отримують доступ до обладнання (і, за необхідності, до інших ресурсів ядра, а також ресурсів інших програм) тільки за допомогою системних викликів. Ядро виконується у привілейованому режимі: саме в цьому сенсі кажуть, що система (точніше, її ядро) управляє обладнанням.

У визначенні складу операційної системи значення має критерій операційної цілісності (замкнутості): система має дозволяти повноцінно використовувати (включаючи модифікацію) свої компоненти. Тому до повного складу операційної системи включають і набір інструментальних засобів (від текстових редакторів до компіляторів, налагоджувачів та компонувальників).

Ядро

Ядро – центральна частина операційної системи, що управляє виконанням процесів, ресурсами обчислювальної системи та надає процесам координований доступ до цих ресурсів. Основними ресурсами є процесорний час, пам'ять та пристрої введення-виведення. Доступ до файлової системи та мережна взаємодія також можуть бути реалізовані лише на рівні ядра.

Як основний елемент операційної системи, ядро є найнижчим рівень абстракції для доступу додатків до ресурсів обчислювальної системи, необхідним для їх роботи. Як правило, ядро надає такий доступ виконуваним процесам відповідних додатків за рахунок використання механізмів міжпроцесної взаємодії та звернення до системних викликів ОС.

Описана завдання може відрізнятися залежно від типу архітектури ядра та її реалізації.

Об'єкти ядра ОС:

– процеси,
– файли,
– події,
– потоки,
– семафори,
– м'ютекси,
– канали,
– файли, що проецуються до пам’яті.

Типи архітектур ядер операційних систем

Монолітне ядро

Монолітне ядро надає багатий набір обладнання абстракції. Всі частини монолітного ядра працюють в одному адресному просторі. Це така схема операційної системи, коли всі компоненти її ядра є складовими частинами однієї програми, використовують загальні структури даних і взаємодіють друг з одним шляхом безпосереднього виклику процедур. Монолітне ядро – найстаріший спосіб організації операційних систем. Прикладом систем із монолітним ядром є більшість UNIX-систем.

– Переваги: Швидкість роботи, спрощена розробка модулів.

– Недоліки: Оскільки ядро працює в одному адресному просторі, збій в одному з компонентів може порушити працездатність усієї системи.

Приклади: Традиційні ядра UNIX (такі як BSD), Linux; ядро MS-DOS, ядро KolibriOS.

Деякі старі монолітні ядра, особливо систем класу UNIX / Linux, вимагали перекомпіляції за будь-якої зміни складу обладнання. Більшість сучасних ядер дозволяє під час роботи підвантажувати *модулі*, що виконують частину функцій ядра. У цьому випадку компоненти операційної системи є не самостійними модулями, а складовими частинами однієї великої програми, яка називається монолітним ядром (monolithic kernel), яке є набором процедур, кожна з яких може викликати кожну. Усі процедури працюють у привілейованому режимі.

Модульне ядро

Модульне ядро – сучасна, вдосконалена модифікація архітектури монолітних ядер операційних систем.

На відміну від «класичних» монолітних ядер, модульні ядра зазвичай не вимагають повної перекомпіляції ядра при зміні складу апаратного забезпечення комп'ютера. Натомість модульні ядра надають той чи інший механізм підвантаження модулів ядра, що підтримують те чи інше апаратне забезпечення (наприклад, драйверів). При цьому підвантаження модулів може бути як динамічною (виконуваної «на льоту», без перезавантаження ОС, у працюючій системі), так і статичної (виконується при перезавантаженні ОС після переконфігурування системи на завантаження тих чи інших модулів).

Приклади: OpenVMS;

Мікроядро

Мікроядро надає лише елементарні функції управління процесами та мінімальний набір абстракцій для роботи з обладнанням. Більша частина роботи здійснюється за допомогою спеціальних процесів користувача, званих *серверами*. Вирішальним критерієм «мікроядерності» є розміщення всіх або багатьох драйверів і модулів у сервісних процесах, іноді з явною неможливістю завантаження будь-яких модулів розширення у власне мікроядро, а також розробки таких розширень.

– Переваги: Стійкість до збоїв обладнання, помилок у компонентах системи. Основна перевага мікроядерної архітектури – високий рівень модульності ядра операційної системи. Це значно спрощує додавання до нього нових компонентів. У мікроядерній операційній системі можна, не перериваючи її роботи, завантажувати і вивантажувати нові драйвери, файлові системи і т.д. Компоненти ядра операційної системи нічим принципово не відрізняються від програм користувача, тому для їх налагодження можна застосовувати звичайні засоби. Мікроядерна архітектура підвищує надійність системи, оскільки помилка лише на рівні непривілейованої програми менш небезпечна, ніж відмова лише на рівні режиму ядра.

– Недоліки: Передача даних між процесами потребує накладних витрат.

Класичні мікроядра надають лише дуже невеликий набір низькорівневих примітивів, або системних викликів, що реалізують базові послуги операційної системи.

Сервісні процеси (в прийнятій у сімействі UNIX термінології – «демони ») активно використовуються в різних ОС для завдань типу запуску програм з

розкладу (UNIX і Windows NT), ведення журналів подій (UNIX і Windows NT), централізованої перевірки паролів і зберігання пароля поточного інтерактивного користувача у спеціально обмеженій області пам'яті (Windows NT). Тим не менш, не слід вважати ОС мікроядерними лише через використання такої архітектури.

Приклади: Symbian OS; Windows CE; Mach, що використовується в GNU/Hurd та Mac OS X; QNX; AIX; Minix; ChorusOS; AmigaOS; MorphOS.

Екзоядро

Екзоядро – ядро операційної системи, що надає лише функції для взаємодії між процесами, безпечного виділення та звільнення ресурсів. Передбачається, що API для прикладних програм надаватимуться зовнішніми по відношенню до ядра бібліотеками (звідки і назва архітектури).

Можливість доступу до пристроїв на рівні контролерів дозволить ефективніше вирішувати деякі завдання, які погано вписуються в рамки універсальної ОС, наприклад, реалізація СУБД матиме доступ до диска на рівні секторів диска, а не файлів та кластерів, що позитивно позначиться на швидкодії.

Наноядро

Наноядро – архітектура ядра операційної системи, в рамках якої вкрай спрощене та мінімалістичне ядро виконує лише одне завдання – обробку апаратних переривань, що генеруються пристроями комп'ютера. Після обробки переривань від апаратури наноядро посилає інформацію про результати обробки (наприклад, отримані з клавіатури символи) вищележачому програмному забезпеченню за допомогою того ж механізму переривань. Прикладом є KeyKOS – найперша ОС на наноядрі. Перша версія вийшла ще 1983 року.

Гібридне ядро

Гібридні ядра – це модифіковані мікроядра, що дозволяють прискорити роботу запускати «несуттєві» частини у просторі ядра. Приклад: ядра ОС Windows сімейства NT.

Комбінація різних підходів

Усі розглянуті підходи до побудови операційних систем мають свої переваги та недоліки. Найчастіше сучасні операційні системи використовують різні комбінації цих підходів. Так, наприклад, зараз ядро Linux є монолітною системою з окремими елементами модульного ядра. При компіляції ядра можна дозволити динамічне завантаження і вивантаження багатьох компонентів ядра – про модулів. У момент завантаження модуля його код завантажується лише на рівні системи та зв'язується з іншою частиною ядра. Всередині модуля можуть використовуватися будь-які функції, що експортуються ядром.

Існують варіанти ОС GNU, в яких замість монолітного ядра застосовується ядро Mach (таке ж, як у Hurd), а поверх нього працюють в просторі користувача ті ж самі процеси, які при використанні Linux були б частиною ядра. Іншим прикладом змішаного підходу може бути можливість запуску операційної системи з монолітним ядром під керуванням мікроядра. Так влаштовані 4.4 BSD і MkLinux, засновані на мікроядрі Mach. Мікроядро забезпечує управління віртуальною пам'яттю та роботу низькорівневих драйверів. Всі інші функції, зокрема взаємодія з прикладними програмами, здійснюються монолітним ядром.

Даний підхід сформувався в результаті спроб використовувати переваги мікроядерної архітектури, зберігаючи наскільки можна добре налагоджений код монолітного ядра.

Змішане ядро, в принципі, поєднує переваги монолітного ядра і мікроядра: здавалося б, мікроядро і монолітне ядро – крайності, а змішане – золота середина. У них можна додавати драйвера пристроїв двома методами: і всередину ядра, і в простір. Але практично концепція змішаного ядра часто підкреслює як переваги, а й недоліки обох типів ядер.

Приклади: Windows NT, DragonFly BSD.

9.2. Процеси і потоки в операційних системах

Процес є ідентифікованою абстракцією сукупності взаємопов'язаних системних ресурсів на основі окремого та незалежного віртуального адресного простору в контексті якої організується виконання потоків. Стандарт ISO 9000:2000 Definitions визначає процес як сукупність взаємопов'язаних та взаємодіючих дій, що перетворюють вхідні дані у вихідні.

Комп'ютерна програма як така – лише пасивна послідовність інструкцій. У той час як процес – безпосереднє виконання цих інструкцій.

Також, процесом називають програму, що виконується, і всі її елементи: адресний простір, глобальні змінні, регістри, стек, відкриті файли і так далі.

Представлення процесу

Зазвичай процес у обчислювальній системі представлений (також кажуть, «володіє») такими ресурсами:

- чином виконуваного машинного коду, асоційованого з програмою;
- пам'яттю (зазвичай деякою областю віртуальної пам'яті), яка включає:
  - виконуваний код;
  - вхідні та вихідні дані процесу;
  - стек викликів (для відстеження активних підпрограм);
  - купу для зберігання проміжних результатів обчислень, що генеруються під час виконання;
- дескрипторами ресурсів операційної системи, виділеними для процесу, наприклад, файл;
- файловими дескрипторами (в термінології ОС Unix) або «хендлами» (в термінології ОС Windows);
- атрибутами безпеки, такими як власник та набір повноважень процесу (допустимих операцій);
- станом процесора (контекстом), таким як:
  - вміст регістрів;
  - схема перетворення віртуальних адрес у фізичні;
  - і т.д.

Контекст поточного процесу вивантажується в пам'ять, коли перемикається на інший процес.

Операційна система зберігає більшу частину інформації про процеси в таблиці процесів.

У операційних системах, підтримують потоки виконання (нитки), потоки також мають власні ресурси. Зазвичай це лише стан процесора, хоча потоки можуть використовувати інші ресурси.

Для зниження ймовірності впливу процесів один на одного та ймовірності відмови системи (наприклад, взаємних блокувань або пробуксування) операційна система забезпечує ізоляцію процесів та виділяє необхідні їм ресурси. Також операційна система надає механізми для взаємодії процесів безпечними та передбачуваними способами.

Подання процесу у пам'яті

У цьому розділі розглянуто уявлення процесу в пам'яті операційної системи Linux та архітектури x86. Подібне уявлення мало відрізняється від багатьох інших багатозадачних операційних систем та архітектур. Наприклад в amd64, спадкоємці x86, стек викликів так само зростає зверху вниз, але розмір адресного простору збільшений до 2^{48} байт.

Linux використовує плоску модель пам'яті, і тому в даній архітектурі кожному процесу доступно 2^{32} байт пам'яті. Вся віртуальна пам'ять ділиться на простір користувача та простір ядра. Простір ядра займає один гігабайт пам'яті, починаючи з найстаршої адреси. Все інше простір, тобто три гігабайти відведено під простір користувача.

На схемі праворуч показано уявлення простору користувача будь-якого процесу. Простір ядра єдине всім процесів, оскільки у операційній системі може існувати лише один екземпляр ядра. Після запуску програми в оперативну пам'ять імпортуються команди процесора (машинний код) та ініціалізовані дані. Водночас у старші адреси імпортуються аргументи запуску та змінні оточення.

В області ініціалізованих даних зберігаються дані, доступні лише читання. Це може бути, наприклад, рядкові літерали.

У сфері неініціалізованих даних, як правило, зберігаються глобальні змінні.

Купа (heap) використовується виділення пам'яті під час роботи програми. У Linux для цього існує системний виклик mmap.

Область стека використовується для виклику процедур.

Також важливою деталлю є наявність випадкового відступу між стеком і верхньою областю, а також між областю ініціалізованих даних та купою. Робиться це з метою безпеки, наприклад, для запобігання вбудовуванню в стек інших функцій.

Бібліотеки, що динамічно підключаються, і відображення файлів розташовуються між стеком і купою.

Ієрархія процесів

У багатозадачних операційних системах з'явилася можливість працювати одночасно з кількома процесами. Операційні системи з витісняючою багатозадачністю дозволяли домогтися відчуття роботи кількох процесів одночасно. При цьому були потрібні засоби управління декількома процесами.

Unix

Unix – одна з перших багатозадачних ОС. Кожен процес має унікальний числовий ідентифікатор PID. Процеси в ній мають деревоподібну ієрархію, де коренем є процес init с PID 1. Новий процес можна створити системним викликом fork, він буде точною копією процесу батька. Будь-який процес крім init завжди має процес батька (атрибут PPID (англ. *Parent PID*)); процеси, батько яких завершив свою роботу, стають дочірніми процесами init.

Процеси також об'єднуються у **групи**. За керування ідентифікатором групи (PGID) відповідають системні виклики setpgidta getpgid. PGID дорівнює PID'у лідера групи. Процес нащадок успадковує групу батьків. Групи використовуються для керування завданнями.

Групи процесів об'єднуються у **сесії**. За створення нової сесії відповідає системний виклик setsid. Процеси з однієї групи не можуть належати різним сесіям. Тому лідер групи не може стати лідером сесії: під час створення сесії дочірній процес автоматично стає лідером сесії та лідером нової групи. Сесії використовують для відстеження всіх процесів, запущених після входу користувача.

Кожна сесія може мати не більше одного **керуючого терміналу**. Емулятор терміналу має дочірнім процесом оболонку команд (найчастіше bash або sh), яка перед запуском стає лідером нової сесії та встановлює собі керуючим термінал.

Створення процесу

Найпростішою операційній системі не потрібно створення нових процесів, оскільки в них працює одна-єдина програма, що запускається під час включення пристрою. У складніших системах треба створювати нові процеси. Зазвичай вони створюються:

– При запуску ОС (наприклад, коли відбувається ініціалізація драйверів пристроїв).

– З появою запиту створення процесу – відбувається у разі, коли працюючий процес виконує системний виклик.

Стан процесу

Процес, крім головного робочого стану, може бути в інших станах, наприклад очікування.

Linux

Процес в ОС Linux може бути в одному з наступних станів:

– **R –** *(running/runnable)* – процес виконується або чекає своєї черги виконуватися;

– **D** – безперервний сон – процес очікує певної події;

– **S** – сон, що переривається – процес очікує певної події або сигналу;

– **T** – зупинка – процес припинений, наприклад, відладчиком;

– **Z –** *(zombie)* – процес вже завершився, але ще не передав батьківському процесу свій код повернення.

Завершення процесу

Мінімум 2 етапи завершення:

1. Процес видаляється з усіх черг планування, тобто ОС більше не планує виділення будь-яких ресурсів процесу,

2. Збір статистики про спожиті процесом ресурси з подальшим видаленням його з пам'яті.

Причини завершення процесу:

– Звичайний вихід.
– Вихід за винятком чи помилкою.
– Недостатній обсяг пам'яті.
– Перевищення ліміту відведеного програмі часу.
– Вихід за межі відведеної області пам'яті
– Неправильна команда (дані програми інтерпретуються як інструкції для процесора).
– Помилка захисту (виконання непривілейованої команди).
– Завершення батьківського процесу.
– Помилка введення- виведення.
– Втручання оператора.

Потік виконання

Потік виконання (тред; від англ. *thread* – нитка) – Найменша одиниця обробки, виконання якої може бути призначене ядром операційної системи. Реалізація потоків виконання та процесів у різних операційних системах відрізняється один від одного, але в більшості випадків потік виконання знаходиться всередині процесу. Декілька потоків виконання можуть існувати в рамках того самого процесу і спільно використовувати ресурси, такі як пам'ять, тоді як процеси не поділяють цих ресурсів. Зокрема, потоки виконання поділяють послідовність інструкцій процесу (його код) та його *контекст* – значення змінних (регістрів процесора і стека викликів), які вони мають у будь-який момент часу.

Як аналогію потоки виконання процесу можна уподібнити кільком разом працюючим кухарям. Всі вони готують одну страву, читають ту саму кулінарну книгу з одним і тим самим рецептом і дотримуються його вказівок, причому не обов'язково всі вони читають на одній і тій же сторінці.

На одному процесорі *багатопотоковість* зазвичай відбувається шляхом тимчасового мультиплексування (як і у разі багатозадачності): процесор перемикається між різними потоками виконання. Це перемикання контексту зазвичай відбувається досить часто, щоб користувач сприймав виконання потоків чи завдань як одночасне. У багатопроцесорних і багатоядерних системах потоки чи завдання можуть реально виконуватися одночасно, у своїй кожен процесор чи ядро обробляє окремий потік чи завдання.

Багато сучасних операційних систем підтримують як тимчасові нарізки від планувальника процесів, і багатопроцесорні потоки виконання. Ядро операційної системи дозволяє програмістам управляти потоками виконання через інтерфейс системних викликів. Деякі реалізації ядра називають *потоком*

ядра, інші ж – *легковажним процесом* (англ. *light-weight process*, LWP), що є особливим типом потоку виконання ядра, який спільно використовує одні й ті ж стани і дані.

Програми можуть мати *користувальницький простір потоків виконання* при створенні потоків за допомогою таймерів, сигналів або іншими методами, що дозволяють перервати виконання та створити тимчасове нарізування для конкретної ситуації (Ad hoc).

Відміна від процесів

Потоки виконання відрізняються від традиційних процесів багатозадачної операційної системи тим, що:

– процеси, як правило, незалежні, тоді як потоки виконання існують як складові елементи процесів;

– процеси несуть значно більше інформації про стан, тоді як кілька потоків виконання всередині процесу спільно використовують інформацію про стан, а також пам'ять та інші обчислювальні ресурси;

– процеси мають окремі адресні простори, тоді як потоки виконання спільно використовують їх адресний простір;

– процеси взаємодіють лише через надані системою механізми зв'язків між процесами;

– перемикання контексту між потоками виконання в одному процесі, як правило, швидше, ніж перемикання контексту між процесами.

Такі системи, як Windows NT і OS/2, як кажуть, мають «дешеві» потоки виконання та «дорогі» процеси. В інших операційних системах різниця між потоками виконання і процесами не така велика, за винятком витрат на перемикання адресного простору, що передбачає використання буфера асоціативної трансляції.

Багатопотоковість

Багатопотоковість, як широко поширена модель програмування та виконання коду, дозволяє кільком потокам виконуватися в рамках одного процесу. Ці потоки виконання спільно використовують ресурси процесу, але можуть працювати самостійно. Багатопотокова модель програмування надає розробникам зручну абстракцію паралельного виконання. Однак, мабуть, найцікавіше застосування технології є в тому випадку, коли вона застосовується до одного *процесу*, що дозволяє його *паралельне виконання багатопроцесорної* системи.

Ця перевага багатопотокової програми дозволяє їй працювати швидше на комп'ютерних системах, які мають кілька процесорів, процесор з кількома ядрами або на кластері машин – через те, що потоки виконання програм природно піддаються дійсно паралельному виконанню процесів. У цьому випадку програмісту потрібно бути дуже обережним, щоб уникнути стану гонки та іншої неінтуітивної поведінки. Для того, щоб правильно маніпулювати даними, потоки виконання повинні часто проходити через рандеву процедуру, щоб обробляти дані в правильному порядку. Потокам виконання можуть також

знадобитися м'ютекси (які часто реалізуються з використанням семафорів), щоб запобігти одночасній зміні загальних даних або їх читання під час процесу зміни. Необережне використання таких примітивів може призвести до тупикової ситуації.

Іншим використанням багатопотоковості, що застосовується навіть для однопроцесорних систем, є можливість застосування реагування на введення даних. В однопотокових програмах, якщо основний потік виконання заблокований виконанням тривалого завдання, вся програма може опинитися в замороженому стані. Переміщаючи такі тривалі завдання до *робочого потоку*, який виконується паралельно з основним потоком, стає можливим для додатків продовжувати реагувати на дії користувача під час виконання завдань у фоновому режимі. З іншого боку, в більшості випадків багатопотоковість – не єдиний спосіб зберегти чутливість програми. Те саме може бути досягнуто через асинхронне введення-виведення або сигнали в UNIX.

Операційні системи планують виконання потоків одним із двох способів:

1. *Пріоритетна багатопотоковість*, взагалі кажучи, вважається більш досконалим підходом, оскільки вона дозволяє операційній системі визначити, коли має відбуватися перемикання контексту. Недолік пріоритетної багатопотоковості полягає в тому, що система може зробити перемикання контексту в невідповідний час, що призводить до інверсії пріоритету та інших негативних ефектів, яких можна уникнути, застосовуючи кооперативну багатопотоковість.

2. *Кооперативна багатопотоковість* покладається самі потоки і цурається управління, якщо потоки виконання перебувають у точках зупинки. Це може створити проблеми, якщо потік виконання очікує на ресурс, поки він не стане доступним.

До кінця 1990-х процесори в настільних комп'ютерах не мали підтримки багатопотоковості, оскільки перемикання між потоками, як правило, відбувалося повільніше, ніж повне перемикання контексту процесу. Процесори у вбудовуваних системах, які мають більш високі вимоги до поведінки в реальному часі, можуть підтримувати багатопотоковість за рахунок зменшення часу на перемикання між потоками, можливо, шляхом розподілу виділених реєстрових файлів для кожного потоку виконання замість збереження/відновлення загального регістрового файлу. Наприкінці 1990-х ідея виконання інструкцій кількох потоків одночасно, відома як одночасна багатопотоковість, під назвою Hyper-Threading, досягла настільних комп'ютерів із процесором Intel Pentium 4. Потім вона була виключена з процесорів архітектури Intel Core та Core 2, але пізніше відновлена в архітектурі Core i7.

Критики багатопотоковості стверджують, що збільшення використання потоків має суттєві недоліки:

Хоча здається, що потоки виконання – це невеликий крок від послідовних обчислень, за суттю вони є величезним стрибком. Вони відмовляються від найбільш важливих та привабливих властивостей послідовних обчислень: зрозумілості, передбачуваності та детермінізму. Потоки виконання, як модель

обчислень, є недетермінованими, і зменшення цього недетермінізму стає завданням програміста.

Процеси, потоки виконання ядра, користувальницькі потоки та файбери

Процес є «найважчою» одиницею планування ядра. Власні ресурси для процесу виділяються операційною системою. Ресурси включають пам'ять, дескриптори файлів, роз'єми, дескриптори пристроїв та вікна. Процеси використовують адресний простір і файли ресурсів в режимі розподілу часу тільки через явні методи, такі як успадкування дескрипторів файлів і сегментів пам'яті, що розділяється. Процеси, як правило, попередньо перетворені на багатозадачний спосіб виконання.

Потоки виконання ядра належать до «легких» одиниць планування ядра. Усередині кожного процесу існує принаймні один потік виконання ядра. Якщо у процесі можуть існувати кілька потоків виконання ядра, всі вони спільно використовують загальну пам'ять і файл ресурсів. Якщо процес виконання планувальника операційної системи є пріоритетним, то потоки виконання ядра теж пріоритетно багатозадачними. Потоки виконання ядра немає власних ресурсів, крім стека викликів, копії регістрів процесора, включаючи лічильник команді локальну пам'ять потоку виконання (якщо вона є). Ядро може призначити по одному потоку виконання для кожного логічного ядра системи (оскільки кожен процесор поділяє сам себе на кілька логічних ядер, якщо він підтримує багатопотоковість, або підтримує лише одне логічне ядро на кожне фізичне ядро, якщо не підтримує багатопотоковість), а може виконувати свопінг заблокованих потоків виконання. Однак потоки виконання ядра вимагають набагато більше часу, ніж потрібно на свопінг потоків користувача виконання.

Потоки виконання іноді реалізуються в користувальницькому просторі бібліотек, в цьому випадку вони називаються *користувальницькими потоками виконання*. Ядро не знає про них, так що вони управляються і плануються в просторі користувача. У деяких реалізаціях *користувальницькі потоки виконання* ґрунтуються на кількох верхніх *потоках виконання ядра*, щоб використовувати переваги багатопроцесорних машин (моделі M: N). Під терміном «потік виконання» за умовчанням (без кваліфікатора «ядра» або «користувач») мається на увазі «потік виконання ядра». Користувальницькі потоки виконання, реалізовані за допомогою віртуальних машин, називають також «зеленими потоками виконання». Користувальницькі потоки виконання, як правило, можна швидко створювати, і ними легко керувати, але вони не можуть використовувати переваги багатопотоковості та багатопроцесорності. Вони можуть блокуватися, якщо всі пов'язані з ним потоки виконання ядра зайняті, навіть якщо деякі потоки користувача готові до запуску.

Файбери є ще більш «легкими» блоками планування, що належать до кооперативної багатозадачності: виконуваний файбер повинен явно «поступитися» право іншим файберам на виконання, що робить їх реалізацію набагато легше, ніж реалізацію потоків виконання ядра або потоків користувача. Файбери можуть бути заплановані для запуску в будь-якому потоці виконання

всередині процесу. Це дозволяє додаткам отримати підвищення продуктивності за рахунок управління плануванням самого себе, замість покладатися на планувальник ядра (який може бути не налаштований на таке застосування). Паралельні середовища програмування, такі як OpenMP, зазвичай реалізують свої завдання за допомогою файберів.

Проблеми потоків виконання та файберів

Паралелізм та структури даних

Потоки виконання одного і того ж процесу спільно використовують один і той же адресний простір. Це дозволяє одночасно виконуваним кодам бути щільно пов'язаними та зручно обмінюватися даними без накладних витрат та складності міжпроцесної взаємодії. При спільному доступі декількох потоків навіть до простих структур даних виникає небезпека виникнення стану гонки в тому випадку, якщо для оновлення даних потрібно більше однієї інструкції процесора: два потоки виконання можуть спробувати одночасно оновити структури даних і отримати в результаті дані, стан яких відрізняється від очікуваного. Помилки, спричинені станом гонки, буває дуже важко відтворити та ізолювати.

Щоб уникнути цього, прикладні програмні інтерфейси (API) потоків виконання пропонують примітиви синхронізації, такі як м'ютекси для блокування структур даних від одночасного доступу. На однопроцесорних системах потік виконання, який звернувся до заблокованого м'ютексу, повинен зупинити роботу і, отже, ініціювати перемикання контексту. На багатопроцесорних системах потік виконання може замість опитування м'ютексу зробити захоплення спінлока. Обидва способи можуть знижувати продуктивність і змушувати процесор в SMP-системах конкурувати за шину пам'яті, особливо якщо рівень модульності блокувань занадто високий.

Введення-виведення та планування

Реалізація користувацьких потоків виконання та файберів, як правило, проводиться повністю в користувальницькому просторі. В результаті переключення контексту між потоками користувача і файберами в одному і тому ж процесі дуже ефективно, оскільки взагалі не вимагає ніякої взаємодії з ядром. Переключення контексту проводиться локально шляхом збереження регістрів процесора, що використовуються працюючим потоком користувача або файбером, і потім завантаженням регістрів, необхідних для нового виконання. Оскільки планування відбувається в просторі користувача, політика планування може бути легко адаптована до вимог конкретної програми.

Однак використання блокувань системних викликів для потоків користувача (на відміну від потоків виконання ядра) і файберів має свої проблеми. Якщо потік користувача або файбер виконує системний виклик, інші потоки виконання та файбери процесу не можуть працювати до завершення цієї обробки. Типовий приклад такої проблеми пов'язаний із виконанням операцій введення-виведення. Більшість програм розраховані на синхронне виконання введення-виводу. При ініціації введення-виведення робиться системний виклик, і він не повертається до його завершення. У проміжку весь процес блокується

ядром і не може виконуватися, позбавляючи можливості роботи інші потоки користувачів і файбери цього процесу.

Загальним рішенням цієї проблеми є забезпечення окремого API для введення-виведення, який реалізує синхронний інтерфейс з використанням внутрішнього неблокуючого введення-виводу, і запуск іншого потоку користувача або файбера на час обробки введення-виведення. Подібні рішення можуть бути передбачені для системних викликів, що блокують. Крім того, програма може бути написана так, щоб уникнути використання синхронного введення-виводу або інших блокуючих системних викликів.

У SunOS 4.x реалізовані так звані легковажні процеси або LWP. У NetBSD 2.x+ та DragonFly BSD реалізовані LWP як потоки виконання ядра (модель 1:1). У SunOS 5.2 і до SunOS 5.8, а також в NetBSD 2 і до NetBSD 4 реалізована дворівнева модель, що використовує один або кілька потоків користувача для кожного потік виконання ядра (модель M:N). У SunOS 5.9 та наступних версіях, а також у NetBSD 5 ліквідовано підтримку користувацьких потоків виконання, відбулося повернення до моделі 1:1. У FreeBSD 5 реалізовано модель M:N. У FreeBSD 6 підтримуються обидві моделі: 1:1 та M:N, і користувач може вибрати, яку з них він використовуватиме в даній програмі, використовуючи /etc/libmap.conf. У FreeBSD починаючи з версії 7 модель 1:1 стала використовуватися за умовчанням, а FreeBSD 8 і наступних версіях модель M:N не підтримується зовсім.

Використання потоків виконання ядра спрощує код користувача, переміщуючи деякі з найскладніших аспектів багатопотокового в ядро. Від програми не потрібно планування потоків виконання та явних захоплень процесора. Код користувача може бути записаний у звичному процедурному стилі, включаючи виклики блокуючого API без позбавлення доступу до процесора інших потоків виконання. Тим не менш, потоки виконання ядра можуть викликати перемикання контексту між потоками виконання в будь-який час і тим самим наразити на небезпеку появи помилок гонки і одночасності, які могли б не виникати. На SMP-системах це ще більше посилюється, оскільки потоки виконання ядра можуть у сенсі виконуватися одночасно різних процесорах.

Моделі

1:1 (потоки виконання лише на рівні ядра)

Потоки виконання, створені користувачем моделі 1-1, відповідають диспетчованим сутностям ядра. Це найпростіший варіант реалізації потоковості. У Windows API цей підхід використовувався з самого початку. У Linux звичайна бібліотека C реалізує цей підхід (через бібліотеку потоків POSIX, а більш старших версіях через Linux Threads). Такий самий підхід використовується ОС Solaris, NetBSD та FreeBSD.

N:1 (потоки виконання рівня користувача)

У моделі N:1 передбачається, що це потоки виконання рівня користувача відображаються на єдину плановану сутність рівня ядра, і нічого не знає склад прикладних потоків виконання. При такому підході перемикання контексту

може бути зроблено дуже швидко, і, крім того, він може бути реалізований навіть на простих ядрах, які не підтримують багатопотоковість. Однак, одним із головних недоліків його є те, що в ньому не можна отримати жодної вигоди з апаратного прискорення на багатопотокових процесорах або багатопроцесорних комп'ютерах, тому що тільки один потік виконання може бути запланований на будь-який момент часу. Ця модель використовується у GNU Portable Threads.

M:N (змішана потоковість)

У моделі M:N кілька M прикладних потоків виконання відображаються на деяке число N сутностей ядра або «віртуальних процесорів». Модель є компромісною між моделлю рівня ядра («1:1») та моделлю рівня користувача («N:1»). Взагалі кажучи, «M:N» потоковість системи є більш складною для реалізації, ніж ядро або потоки користувача виконання, оскільки зміна коду як для ядра, так і для користувальницького простору не потрібно. У M:N реалізації бібліотека потоків відповідає за планування потоків користувача виконання на наявних планованих сутностях. У цьому переключення контексту потоків робиться дуже швидко, оскільки модель дозволяє уникнути системних викликів. Тим не менш, збільшується складність та ймовірність інверсії пріоритетів,

9.3. Керування пам’яттю в операційних системах

З поняттям керування пам’яттю в ОС пов'язані такі технології:
– Функції керування пам'яттю в ОС.
– Типи адрес.
– Методи розподілу пам'яті в ОС.
– Принцип кешування даних у ОС.

Функції керування пам'яттю в ОС

Операційна система вирішує такі завдання:
– Відстеження вільної та зайнятої пам'яті.
– Виділення та звільнення пам'яті за запитами процесів.
– Забезпечує налаштування адрес.
– Підтримка механізму віртуальної пам'яті.

Типи адрес

Для ідентифікації змінних та команд використовуються:
– символьні імена (мітки);
– віртуальні адреси;
– фізичні адреси.

Символьні імена

Символьні імена надає користувач під час написання програми.

Віртуальні адреси

Віртуальні адреси виробляє компілятор. Оскільки відомо, у якому місці оперативної пам'яті буде завантажена програма, то компілятор надає змінним і командам віртуальні (умовні) адреси, зазвичай вважаючи за умовчанням, що

програма буде розміщена, починаючи з нульової адреси. Сукупність віртуальних адрес процесу називається **віртуальним адресним простором**. Кожен процес має власний віртуальний адресний простір.

Фізичні адреси

Фізичні адреси відповідають номерам осередків оперативної пам'яті, де насправді розташовані або будуть розташовані змінні та команди. Перехід від віртуальних адрес до фізичних може здійснюватися двома способами.

У першому випадку заміну віртуальних адрес на фізичні робить спеціальна системна програма – завантажувач, що переміщає. Переміщаючий завантажувач на підставі наявних у нього вихідних даних про початкову адресу фізичної пам'яті, в яку належить завантажувати програму, та інформації, наданої компілятором про адресно-залежні константи програми, виконує завантаження програми, поєднуючи її із заміною віртуальних адрес фізичними.

Другий спосіб полягає в тому, що програма завантажується в пам'ять у незміненому вигляді у віртуальних адресах, при цьому операційна система фіксує зміщення дійсного розташування програмного коду щодо адресного віртуального простору. Під час виконання програми при кожному зверненні до оперативної пам'яті виконується перетворення віртуальної адреси на фізичну.

Другий спосіб є більш гнучким, він допускає переміщення програми під час її виконання, в той час як завантажувач, що переміщає, жорстко прив'язує програму до спочатку виділеної їй ділянці пам'яті. Разом про те використання переміщуючого завантажувача зменшує накладні витрати, оскільки перетворення кожної віртуальної адреси відбувається лише один раз під час завантаження, тоді як у другому випадку – щоразу під час звернення за цією адресою.

Іноді (зазвичай у спеціалізованих системах) заздалегідь точно відомо, в якій області оперативної пам'яті виконуватиметься програма, і компілятор видає код, що виконується, відразу у фізичних адресах.

Методи розподілу пам'яті в ОС

Виділяють такі методи розподілу пам'яті:

Методи розподілу пам'яті без використання дискового простору

Розподіл пам'яті фіксованими розділами

Підсистема керування пам’яттю у разі виконує такі задачи:

– порівнюючи розмір програми, що надійшла виконання, і вільних розділів, вибирає відповідний розділ;

– здійснює завантаження програми та налаштування адрес.

Переваги:

– із загальною чергою – простота;

– с окремими чергами – більша продуктивність.

Недоліки:

– Неефективне розподілення пам'яті (великі незаповнені фрагменти).

– Розмір програми може бути більшим за розмір розділу.

– Перед запуском можна розділити розділи.

Розподіл пам'яті розділами змінної величини

З непереміщуваними розділами

ОС створює під кожну задачу розділ необхідного розміру, коли завдання завершується, розділ звільняється.

Переваги:

– Знімається необхідність організації черг.

– Більше шансів одержати пам'ять потрібного розміру.

– Економічніше.

Недоліки:

– Фрагментація (вільний блок пам'яті виявляється розрізаний) – не будь-яка програма може бути запущена.

З розділами, що переміщаються

Фрагментація стиснення (переміщення): при кожному звільненні пам'яті розділи зміщуються у бік старших (молодших) адрес.

Перевага: немає фрагментації.

Недолік: зниження продуктивності.

Способи упорядкування адрес

Виділяють такі способи упорядкування адрес:

– Налаштування адрес, коли програма запущена (завантажувач, що переміщається).

– Динамічне перетворення віртуальних адрес на фізичні.

Способи боротьби із фрагментацією

У певні моменти часу відбувається стиск у бік молодших адрес. ОС послідовно переглядає зайняті програмами блоки, знаходить розрив і зміщує адресу. Ця схема ефективна у разі динамічного перетворення; якщо використовується завантажувач, що переміщається, то відбувається повний перерахунок адрес, який є дуже ресурсомістким.

Методи розподілу пам'яті з використання дискового простору

Метод оверлєєв

Був використаний та реалізований в ОС MS DOS. Програміст розбиває додаток на кілька частин (оверлєїв), що вміщуються у доступну пам'ять (640 кб). Спочатку відбувається завантаження 0-го оверлея, потім він вивантажується і завантажується перший, і так далі. Програма міститься на диску, активний оверлей – в оперативній пам'яті, а всі механізми забезпечуються програмістом. Механізм потребує ретельного проектування програм.

Сторінковий розподіл віртуальної пам'яті

Адресний простір процесу поділяється на сторінки фіксованих розділів. Фізична пам'ять у системі теж ділиться на сторінки, аналогічні віртуальній пам'яті. До кожного процесу ОС створює службову структуру – таблицю сторінок (дає однозначне відображення віртуальних сторінок у фізичні).

При активізації чергового процесу спеціальний регістр процесора завантажується адресу таблиці сторінок даного процесу.

При кожному зверненні до пам'яті читання з таблиці сторінок інформації про віртуальну сторінку, до якої відбулося звернення. Якщо ця віртуальна

сторінка знаходиться в оперативній пам'яті, то виконується перетворення віртуальної адреси на фізичну. Якщо потрібна віртуальна сторінка в даний момент вивантажена на диск, то відбувається так зване сторінкове переривання. Процес, що виконується, переводиться в стан очікування, і активізується інший процес з черги готових. Паралельно програма обробки переривання сторінок знаходить на диску необхідну віртуальну сторінку і намагається завантажити її в оперативну пам'ять. Якщо у пам'яті є вільна фізична сторінка, то завантаження виконується негайно, якщо ж вільних сторінок немає, вирішується питання, яку сторінку слід вивантажити з оперативної пам'яті.

Прапори

Види прапорів:

– час обробки;
– було звернення чи ні;
– ознака сторінок, що не вивантажуються;
– частота використання.

Розглянемо механізм перетворення віртуальної адреси у фізичну при сторінковій організації пам'яті.

Віртуальна адреса при сторінковому розподілі може бути представлена у вигляді пари (p, s), де p – номер віртуальної сторінки процесу (нумерація сторінок починається з 0), а s – усунення в межах віртуальної сторінки. Враховуючи, що розмір сторінки дорівнює 2 ступеня до, зсув s може бути отримано простим відділенням k молодших розрядів в двійковій запису віртуальної адреси. Старші розряди, що залишилися, є двійковим записом номера сторінки p.

При кожному зверненні до оперативної пам'яті апаратними засобами виконуються такі дії:

– на підставі початкової адреси таблиці сторінок, номера віртуальної сторінки та довжини запису в таблиці сторінок визначається адреса потрібного запису в таблиці,
– із цього запису витягується номер фізичної сторінки
– до номера фізичної сторінки приєднується зміщення.

Таблицю сторінок прагнуть розміщувати в "швидких" пристроях, що запам'ятовують. Це може бути, наприклад, набір спеціальних регістрів або пам'ять, що використовує зменшення часу доступу асоціативний пошук і кешування даних.

Сторінковий розподіл пам'яті може бути реалізований у спрощеному варіанті, без вивантаження сторінок на диск. І тут всі віртуальні сторінки всіх процесів постійно перебувають у оперативної пам'яті. Такий варіант сторінкової організації хоч і не надає користувачеві віртуальної пам'яті, але виключає фрагментацію.

Переваги:

– немає фрагментації
– пам'ять використовується оптимально
– механізм не вимагає жодних дій з боку програми

– швидке перетворення віртуальних адрес у фізичні.

Недоліки:

– при малих сторінках високі витрати при зберіганні таблиці сторінок

– немає можливості вказати тип інформації, що міститься, тому не можна встановити права доступу.

Сегментний розподіл пам'яті

Віртуальний адресний простір процесу ділиться на сегменти, розмір яких визначається програмістом з урахуванням змістового значення інформації, що міститься в них. Окремий сегмент може бути підпрограмою, масивом даних і т.п. Іноді сегментація програми виконується за замовчуванням компілятором.

При завантаженні процесу частина сегментів поміщається в оперативну пам'ять (при цьому для кожного з цих сегментів операційна система підшукує потрібну ділянку вільної пам'яті), а частина сегментів розміщується в дисковій пам'яті. Сегменти однієї програми можуть займати в оперативній пам'яті безмежні ділянки. Під час завантаження система створює таблицю сегментів процесу (аналогічну таблиці сторінок), в якій для кожного сегмента вказується початкова фізична адреса сегмента в оперативній пам'яті, розмір сегмента, правила доступу, ознака модифікації, ознака звернення до даного сегменту за останній інтервал часу та інша інформація. Якщо віртуальні адресні простори кількох процесів включають один і той же сегмент, то в таблицях сегментів цих процесів робляться посилання на ту саму ділянку оперативної пам'яті,

Система з сегментної організацією функціонує аналогічно системі зі сторінковою організацією: іноді відбуваються переривання, пов'язані з відсутністю необхідних сегментів у пам'яті, за необхідності звільнення пам'яті деякі сегменти вивантажуються, при кожному зверненні до оперативної пам'яті виконується перетворення віртуального адреси на фізичний. Крім того, при зверненні до пам'яті перевіряється, чи доступ доступного типу до даного сегменту.

Віртуальна адреса при сегментної організації пам'яті може бути представлена парою (g, s), де g – номер сегмента, а s – усунення в сегменті. Фізична адреса виходить шляхом додавання початкової фізичної адреси сегмента, знайденого в таблиці сегментів за номером g, і зміщення s.

Недоліком цього методу розподілу пам'яті є фрагментація лише на рівні сегментів і повільніше проти сторінковою організацією перетворення адреси.

Сегментно-сторінкова організація поділу пам'яті

Даний метод є комбінацією сторінкового та сегментного розподілу пам'яті і, внаслідок цього, поєднує в собі переваги обох підходів. Віртуальний простір процесу ділиться на сегменти, а кожен сегмент ділиться на віртуальні сторінки, які нумеруються в межах сегмента. Оперативна пам'ять поділяється на фізичні сторінки. Завантаження процесу виконується операційною системою посторінково, при цьому частина сторінок розміщується в оперативній пам'яті, частина на диску. Для кожного сегмента створюється своя таблиця сторінок, структура якої повністю збігається зі структурою таблиці сторінок, що використовується при розподілі сторінок. Для кожного процесу створюється

таблиця сегментів, де вказуються адреси таблиць сторінок всім сегментів даного процесу.

Переваги: цей механізм підтримується процесорами, тому працює швидше.

Недолік: великі обсяги таблиць.

Принцип кешування даних у ОС

Кеш-пам'ять – це спосіб організації спільного функціонування двох типів пристроїв, що відрізняються часом доступу і вартістю зберігання даних, який дозволяє зменшити середній час доступу до даних за рахунок динамічного копіювання в "швидкий" запам’ятовуючий пристрій (ЗП) найбільш часто використовуваної інформації з "повільного" ЗП.

Кеш-пам'яттю часто називають не тільки спосіб організації роботи двох типів пристроїв, що запам'ятовують, але і один з пристроїв – "швидке" ЗП. Воно коштує дорожче і зазвичай має порівняно невеликий обсяг. Важливо, що механізм кеш-пам'яті є прозорим для користувача, який не повинен повідомляти жодної інформації про інтенсивність використання даних і не повинен брати участь у переміщенні даних із ЗП одного типу в ЗП іншого типу, все це робиться автоматично системними засобами.

У системах, оснащених кеш-пам'яттю, кожен запит до оперативної пам'яті виконується відповідно до наступного алгоритму:

– Проглядається вміст кеш-пам'яті з метою визначення, чи не знаходяться потрібні дані в кеш-пам'яті; кеш-пам'ять не є адресованою, тому пошук потрібних даних здійснюється за вмістом – значенням поля "адреса в оперативній пам'яті", взятому із запиту.

– Якщо дані виявляються в кеш-пам'яті, вони зчитуються з неї, і результат передається в процесор.

– Якщо потрібних даних немає, вони разом зі своєю адресою копіюються з оперативної пам'яті в кеш-пам'ять, і результат виконання запиту передається в процесор. При копіюванні даних може виявитися, що в кеш-пам'яті немає вільного місця, тоді вибираються дані, до яких в останній період було найменше звернень, для витіснення з кеш-пам'яті. Якщо дані, що витісняються, були модифіковані за час знаходження в кеш-пам'яті, то вони переписуються в оперативну пам'ять. Якщо ці дані були модифіковані, їх місце у кеш-пам'яті оголошується вільним.

На практиці в кеш-пам'ять зчитується не один елемент даних, до якого відбулося звернення, а цілий блок даних, це збільшує ймовірність так званого "попадання в кеш", тобто знаходження потрібних даних у кеш-пам'яті.

9.4. Файлові системи

Файлова система (англ. *file system*) – порядок, що визначає спосіб організації, зберігання та іменування даних на носіях інформації в комп'ютерах, а також в іншому електронному обладнанні: цифрових фотоапаратах, мобільних телефонах і т. п. Файлова система визначає формат вмісту та спосіб фізичного зберігання інформації, яку прийнято групувати як файлів. Конкретна файлова система визначає розмір імен файлів (і каталогів), максимальний можливий розмір файлу та розділу, набір атрибутів файлу. Деякі файлові системи надають сервісні можливості, наприклад розмежування доступу або шифрування файлів.

Файлова система пов'язує носій інформації з одного боку та API доступу до файлів – з іншого. Коли прикладна програма звертається до файлу, вона не має жодного уявлення про те, яким чином розташована інформація в конкретному файлі, так само як і про те, на якому фізичному типі носія (CD, жорсткому диску, магнітній стрічці, блоці флеш-пам'яті або іншому) він записаний. Все, що знає програма – це ім'я файлу, його розмір та атрибути. Ці дані вона одержує від драйвера файлової системи. Саме файлова система встановлює, де і як буде записано файл на фізичному носії (наприклад, жорсткому диску).

З погляду операційної системи (ОС), весь диск є набором кластерів (як правило, розміром 512 байт і більше). Драйвери файлової системи організують кластери у файли та каталоги (реально є файлами, що містять список файлів у цьому каталозі). Ці ж драйвери відстежують, які з кластерів нині використовуються, які вільні, які позначені як несправні.

Однак файлова система не обов'язково безпосередньо пов'язана з фізичним носієм інформації. Існують віртуальні файлові системи, а також мережні файлові системи, які є лише способом доступу до файлів, що знаходяться на віддаленому комп'ютері.

Основні функції файлових систем

Основними функціями файлової системи є:

– розміщення та впорядкування на носії даних у вигляді файлів;
– визначення максимально підтримуваного обсягу даних носії інформації;
– створення, читання та видалення файлів;
– призначення та зміна атрибутів файлів (розмір, час створення та зміни, власник та творець файлу, доступний тільки для читання, прихований файл, тимчасовий файл, архівний, виконуваний, максимальна довжина імені файлу тощо);
– визначення структури файлу;
– пошук файлів;
– організація каталогів для логічного організації файлів;
– захист файлів під час системного збою;
– захист файлів від несанкціонованого доступу та зміни їхнього вмісту.

Класифікація файлових систем

За призначенням файлові системи можна класифікувати на нижченаведені категорії.

– Для носіїв з довільним доступом (наприклад, жорсткий диск): FAT32, HPFS, ext2 та ін. Оскільки доступ до дисків у кілька разів повільніше, ніж доступ до оперативної пам'яті, для збільшення продуктивності в багатьох файлових системах застосовується асинхронний запис змін на диск. Для цього застосовується або журналювання, наприклад, в ext3, ReiserFS, JFS, NTFS, XFS, або механізм soft updates та ін. Журналювання поширене в Linux, застосовується в NTFS. Soft updates – у BSD-системах.

– Для носіїв з послідовним доступом (наприклад, магнітні стрічки): QIC та ін.

– Для оптичних носіїв – CD і DVD: ISO9660, HFS, UDF та ін.

– Віртуальні файлові системи: AEFS та ін.

– Мережеві файлові системи: NFS, CIFS, SSHFS, GmailFS та ін.

– Для флеш-пам'яті: YAFFS, ExtremeFFS, exFAT.

– Дещо випадають із загальної класифікації спеціалізовані файлові системи: ZFS (власне файловою системою є лише частина ZFS), VMware VMFS (т.з. кластерна файлова система, яка призначена для зберігання інших файлових систем) та ін.

Завдання файлової системи

Основні функції будь-якої файлової системи націлені на вирішення наступних завдань:

– найменування файлів;

– програмний інтерфейс роботи з файлами для програм;

– відображення логічної моделі файлової системи на фізичну організацію сховища даних;

– організація стійкості файлової системи до збоїв живлення, помилок апаратних та програмних засобів;

– зміст параметрів файлу, необхідні правильної його взаємодії коїться з іншими об'єктами системи (ядро, докладання тощо.).

У розрахованих на багато користувачів системах з'являється ще одне завдання: захист файлів одного користувача від несанкціонованого доступу іншого користувача, а також забезпечення спільної роботи з файлами, наприклад, при відкритті файлу одним з користувачів, для інших цей же файл тимчасово буде доступний в режимі «тільки читання».

Файлова система (ФС) дозволяє оперувати не нулями та одиницями, а більш зручними та зрозумілими об'єктами – файлами. Для зручності роботи з файлами використовуються їх символьні ідентифікатори – імена. Сам вміст файлів записано в *кластери* (*clusters*) – дрібні одиниці даних, якими оперує файлова система, розмір їх кратний 512 байтам (512 байт – розмір сектора жорсткого диска, мінімальної одиниці даних, яка зчитується з диска або записується на диск). Для організації інформації крім імені файлу використовуються також каталоги (або папки), як абстракція, що дозволяє

групувати файли за певним критерієм. За своєю суттю каталог – це файл, що містить інформацію про вкладені в нього каталоги і файли.

Вся інформація про файли зберігається в спеціальних областях розділу (томи) – файлових довідниках. Структура цих довідників залежить від типу файлової системи. Довідник файлів дозволяє асоціювати числові ідентифікатори файлів та додаткову інформацію про них (дата зміни, права доступу, ім'я тощо) з безпосереднім вмістом файлу, що зберігається в іншій області розділу (томи).

На жорстких дисках комп'ютерів під керуванням систем сімейства Windows використовуються два типи файлових систем: **FAT** (FAT16 та FAT32) та **NTFS**.

9.5. Захисні механізми операційних систем

Захист ОС сімейства Unix

Захист ОС сімейства Unix у загальному випадку базується на трьох основних механізмах:

– ідентифікації та автентифікації користувача при вході до системи;

– розмежування прав доступу до файлової системи, в основі якої лежить реалізація дискреційної моделі доступу;

– аудит, тобто. реєстрація подій.

При цьому відзначимо, що для різних клонів ОС сімейства Unix можливості механізмів захисту можуть незначно відрізнятися, однак розглядатимемо ОС Unix у загальному випадку, без урахування деяких незначних особливостей окремих ОС цього сімейства.

Побудова файлової системи та розмежування доступу до файлових об'єктів має особливості, властиві цьому сімейству ОС. Розглянемо стисло ці особливості. Усі дискові накопичувачі (томи) поєднуються в єдину ***віртуальну файлову систему*** шляхом операції монтування тома. При цьому вміст тома проектується на вибраний каталог файлової системи. Елементами файлової системи є також всі пристрої, що підключаються до комп'ютера, що захищається (монтуються до файлової системи). Тому розмежування доступу до них здійснюється через файлову систему.

Кожен файловий об'єкт має індексний дескриптор, у якому зберігається інформація про розмежування доступу до цього файлового об'єкта. Права доступу поділяються на три категорії: доступ для власника, доступ для групи та доступ для інших користувачів. У кожній категорії визначаються права на читання, запис та виконання (у разі каталогу – перегляд).

Користувач має унікальні символьний ідентифікатор (ім'я) та числовий ідентифікатор (UID). Символьний ідентифікатор пред'являється користувачем під час входу до системи, числової використовується операційною системою визначення прав користувача у системі (доступ до файлів тощо.).

Принципові недоліки захисних механізмів ОС сімейства Unix

Розглянемо у випадку недоліки реалізації системи захисту ОС сімейства Unix у частині невиконання вимог захисту конфіденційної інформації, безпосередньо пов'язані з можливістю НСД до інформації.

Спочатку відзначимо, що у ОС сімейства Unix, внаслідок реалізованої нею концепції адміністрування (не централізована), неможливо забезпечити замкнутість (чи цілісність) програмного середовища. Це пов'язано з неможливістю встановлення атрибуту "виконання" на каталог (для каталогу цей атрибут обмежує можливість "огляду" вмісту каталогу). Тому при розмежуванні адміністратором доступу користувачів до каталогів, користувач, як "власник" створюваного ним файлу, може занести у свій каталог файл, що виконується і, як його "власник", встановити на файл атрибут "виконання", після чого запустити записану ним програму. Ця проблема безпосередньо пов'язана з концепцією захисту інформації, що реалізується в ОС.

Не повному обсязі реалізується дискреційна модель доступу, зокрема, що неспроможні розмежовуватися права доступу користувача "root" (UID = 0), тобто. даний суб'єкт доступу виключається із схеми управління доступом до ресурсів. Відповідно всі процеси, що їм запускаються, мають необмежений доступ до ресурсів, що захищаються. З цим недоліком системи захисту пов'язано безліч атак, зокрема:

– несанкціоноване одержання прав root;

– запуск з правами root власного виконуваного файлу (локально чи віддалено впровадженого), причому несанкціонована програма отримує повний доступом до ресурсів і т.д.

Крім того, в ОС сімейства Unix неможливо вбудованими засобами гарантовано видаляти залишкову інформацію. Для цього у системі абсолютно відсутні відповідні механізми.

Слід зазначити, більшість ОС даного сімейства не мають можливості контролю цілісності файлової системи, тобто. не містять відповідних інтегрованих засобів. У разі додатковими утилітами то, можливо реалізований контроль конфігураційних файлів ОС за розкладом у той час, як найважливішою можливістю даного механізму вважатимуться контроль цілісності програм (додатків) їх запуском, контроль файлів даних користувача тощо.

Щодо реєстрації (аудиту), то в ОС сімейства Unix не забезпечується реєстрація видачі документів на "тверду копію", а також деякі інші вимоги до реєстрації подій.

Якщо ж трактувати вимоги до управління доступом у загальному випадку, то при захисті комп'ютера у складі ЛОМ необхідно управління доступом до вузлів мережі. Однак вбудованими засобами захисту деяких ОС сімейства Unix управління доступом до вузлів не реалізується.

З наведеного аналізу видно, що багато механізмів, необхідних з погляду виконання формалізованих вимог, більшістю ОС сімейства Unix не реалізується в принципі, або реалізується лише частково.

Механізми безпеки Windows Server 2022

Безпека була в центрі уваги в останніх збірках **Windows**, як і у випадку з **Windows Server 2022**. Він поєднує можливості безпеки для **Windows Server**, а також підтримує багаторівневу безпеку для активізації механізму активного захисту від просунутих загроз і атак. Ось дві ключові функції безпеки, які ви можете очікувати в **Windows Server 2022**:

– Безпечне підключення.
– Сервер із захищеним ядром.

Безпечне підключення

Безпечне (Secure) підключення є обов'язковим та дуже необхідним для серверів, особливо в сучасному світі, де щодня відбуваються нові кібератаки. Щоб забезпечити встановлення безпечних з'єднань, у **Windows Server 2022** реалізовані такі функції:

HTTPS і TLS 1.3 включені в Windows Server 2022 за замовчуванням. (HTTPS and TLS 1.3 є в Windows Server 2022 заборонено.) Остання версія протоколу безпеки Інтернету – **Transport Layer Security** (**TLS**) 1.3. Він забезпечує безпечний канал зв'язку між двома кінцевими точками за рахунок шифрування даних. Тепер, увімкнувши **HTTPS** (HTPPS) і **TLS 1.3** у **Windows Server 2022**, він гарантує, що дані клієнтів, підключених до сервера, захищені. Від старих криптографічних механізмів відмовляються та використовуються нові алгоритми безпеки.

Безпечний DNS (Secure DNS) – ще одна гарна розширена функція, що забезпечує безпечне підключення. **DNS-over-HTTPS** (**DoH**) тепер підтримується **DNS-клієнтом** (DNS Client) у **Windows Server 2022**. **DoH шифрує** (DoH) DNS – (DNS) запити з використанням протоколу **HTTPS** та зберігає конфіденційність трафіку, що ще більше підвищує безпеку. Крім того, за його допомогою можна запобігти підслуховуванню.

Для шифрування та підпису **Server Message Block** (**SMB) у** (SMB) **Windows Server** тепер підтримуються **криптографічні набори AES-256-GCM та AES-256-CCM** (AES-256-GCM and AES-256-CCM cryptographic suites). **Надійне** (Strong) шифрування є потребою у обчисленнях, оскільки зловмисники продовжують знаходити нові способи злому алгоритмів безпеки. Використання пакетів **AES-256-GCM** та **AES-256-CCM** забезпечує більш високий рівень шифрування. Тим не менш, **AES-128** для сумісності з попередніми версіями, як і раніше, підтримується.

Для **загальних томів кластера** (Cluster Shared Volumes) (**CSV**) та рівня **шини сховища** (Storage Bus Layer) (**SBL**) буде жорстке та покращене шифрування та підписання внутрішньовузлових з'єднань сховища, що підтримуються відмовостійкими кластерами **Windows Server.** В основному це означає, що користувачі тепер можуть шифрувати або підписувати обмін даними між сходом і заходом усередині кластера за допомогою **Storage Spaces Direct**.

У **Windows Server 2022 Datacenter**: Azure Edition та підтримуваних клієнтах **Windows підтримується** (Windows) **SMB через QUIC на додаток до TLS 1.3** (SMB over QUIC in addition to TLS 1.3). Це гарантує, що користувачі та програми мають безпечний доступ до даних із прикордонних файлових серверів.

Крім того, більше немає необхідності в **VPN** для мобільних та віддалених користувачів, щоб отримати доступ до своїх файлових серверів через **SMB**, перебуваючи у **Windows**.

Захищений основний сервер

Захищене основне обслуговування забезпечує додатковий рівень захисту від нових загроз та викликів. Він заснований на трьох основних параметрах, які полягають у наступному:

– Спрощена безпека.
– Розширений захист.
– Превентивний захист.

Спрощена безпека (Simplified Security)

Не буде жодних труднощів у налаштуванні функцій безпеки захищених основних серверів. Ви можете легко налаштувати **Windows Server** з **Центру адміністрування Windows** (Windows Admin Center).

Розширений захист (Advanced Protection)

Оскільки захищені базові сервери повністю використовують апаратне забезпечення, вбудоване ПЗ та можливості операційної системи, забезпечується покращений захист від поточних та майбутніх загроз. Він має широкий підхід у областях, які включають:

– **Апаратний корінь довіри** (Hardware root-of-trust): Trusted Platform Module 2.0 (**TPM 2.0**) забезпечує використання захищених основних серверів. Він забезпечує апаратний корінь довіри, який підвищує рівень безпеки, що забезпечується такими можливостями, як **BitLocker**.

– **Захист вбудованого програмного забезпечення:** (Firmware Protection:) Оскільки вбудоване програмне забезпечення працює з вищими привілеями і пов'язане з безліччю вразливостей безпеки, поліпшення захисту вбудованого програмного забезпечення є потребою години. Такі функції, як **технологія Dynamic Root (DRTM)**, **захист** DMA і **системи із захищеним ядром, можуть забезпечити захист вбудованого ПЗ.** (DMA)

– **Безпека на основі віртуалізації (VBS):** (Virtualization-based security (VBS)) **VBS** та цілісність коду на основі гіпервізора (**HVCI**) підтримуються захищеними центральними серверами.

Превентивний захист (Preventative Defense)

Захищені головні сервери активно захищають систему від зловмисників.

Механізми безпеки Windows 10/11

Безпека Windows створена на основі принципів «Нікому не довіряй» для захисту даних і доступу їх будь-якого місця. Забезпечує безпеку та ефективність вашої роботи.

Механізми безпеки Windows 10/11 включають у себе наступні розділи:

"Нікому не довіряй» та Windows

Апаратна безпека

– Довірений платформний модуль.

– Захист від вбудованого програмного забезпечення System Guard у Захиснику Windows.

– Безпечний запуск System Guard у Захиснику Windows та захист SMM.

– Захист цілісності коду на основі віртуалізації.

– Захист DMA для ядра.

Безпека операційної системи

– Безпека системи.

– Шифрування та захист даних.

– Базові параметри безпеки Windows.

– Посібник з віртуальних приватних мереж.

– Брандмауер Windows Defender.

– Захист від вірусів та погроз.

Безпека додатків

– Управління програмами та захист на основі віртуалізації.

– Управління додатком.

– Application Guard.

– Пісочниця Windows.

– Фільтр SmartScreen у Microsoft Defender.

– S/MIME для Windows.

Безпека користувача та захищене посвідчення

– Windows Hello для бізнесу.

– Захист від крадіжки облікових даних у Windows.

– Захист облікових даних домену.

– Credential Guard у Захиснику Windows.

– Втрачені та забуті паролі.

– Управління доступом.

– Смарт-картки.

Хмарні служби

– Управління мобільними пристроями.

– Azure Active Directory.

– Ваш обліковий запис Майкрософт.

– OneDrive.

– Сімейна безпека.

Основи безпеки

– Життєвий цикл розробки захищених програм (Майкрософт).

– Програма Microsoft Bug Bounty.

– Загальні критерії сертифікації.

– Перевірка на відповідність стандарту FIPS 140.

Елементи управління конфіденційністю

Розглянемо усі ці елементи більш детально.

Нульова довіра та працездатність пристроїв Windows

Організаціям потрібна модель безпеки, яка ефективніше адаптується до складності сучасного робочого середовища. IT-адміністраторам необхідно використовувати гібридне робоче місце, одночасно захищаючи людей, пристрої, програми та дані скрізь, де вони знаходяться. Реалізація моделі «Нікому не довіряй» для забезпечення безпеки допомагає усунути сучасні складні середовища.

Принципи нульової довіри:

– **Явним чином перевірте.** Завжди виконувати автентифікацію та авторизацію на основі всіх доступних точок даних, включаючи посвідчення користувача, розташування, працездатність пристрою, службу або робоче навантаження, класифікацію даних та моніторинг аномалій.

– **Використовуйте найменш привілейований доступ**. Обмеживши доступ користувачів за допомогою JIT-доступу та JIT-доступу, адаптивних політик на основі ризиків та захисту даних для захисту даних та підтримки продуктивності.

– **Припустимо, що порушення безпеки**. Запобігайте отриманню доступу зловмисниками, щоб звести до мінімуму потенційні збитки даним та системам. Захист привілейованих ролей, перевірка наскрізного шифрування, використання аналітики для отримання видимості та виявлення загроз для підвищення захисту.

Концепція перевірки «**Нікому не** довіряй» явно застосовується до ризиків, які є як пристроями, так і користувачами. Windows забезпечує **атестацію** працездатності пристроїв та **можливості** умовного доступу, які використовуються для надання доступу до корпоративних ресурсів.

Умовний доступ оцінює сигнали ідентифікації, щоб переконатися, що користувачі є користувачами, які вони говорять, перш ніж їм буде надано доступ до корпоративних ресурсів.

Windows 11 підтримує атестацію працездатності пристроїв, допомагаючи переконатися, що пристрої перебувають у працездатному стані та не були змінені. Ця можливість допомагає користувачам отримувати доступ до корпоративних ресурсів незалежно від того, чи знаходяться вони в офісі, вдома чи у дорозі.

Атестація допомагає перевірити посвідчення та стан важливих компонентів, а також переконатися, що пристрій, вбудоване програмне забезпечення та процес завантаження не були змінені. Відомості про вбудоване програмне забезпечення, процес завантаження та програмне забезпечення використовуються для перевірки стану безпеки пристрою. Ці дані криптографічно зберігаються в модулі довіреної платформи (TPM) для спільної обробки даних системи безпеки. Після атестації пристрою йому може бути надано доступ до ресурсів.

Атестація працездатності пристроїв у Windows

Під час завантаження може виникнути багато ризиків безпеки, оскільки цей процес може бути найбільш привілейованим компонентом усієї системи.

Процес перевірки використовує віддалену атестацію як безпечний канал для визначення та подання працездатності пристрою. Віддалена атестація визначає:

– Якщо пристрій може бути довіреним.

– Правильність завантаження операційної системи.

– Якщо в операційній системі увімкнено правильний набір функцій безпеки.

Ці визначення виконуються за допомогою захищеного кореня довіри за допомогою довіреного платформного модуля (TPM). Пристрої можуть підтвердити, що TPM увімкнено і що пристрій не було незаконно змінено.

Windows включає безліч функцій безпеки, які допомагають захистити користувачів від шкідливих програм та атак. Однак довіра до компонентів безпеки Windows може бути досягнута лише в тому випадку, якщо платформа завантажується належним чином і не була змінена. Windows використовує безпечне завантаження UEFI, антишкідливе програмне забезпечення раннього запуску (ELAM), динамічний корінь довіри для вимірювань (DRTM), довірене завантаження та інші низькорівневі функції безпеки обладнання та вбудованого програмного забезпечення. Коли комп'ютер увімкнеться до запуску захисту від шкідливих програм, Windows підтримуватиме відповідну конфігурацію обладнання, щоб забезпечити безпеку. Вимірювана та довіреназавантаження, реалізована завантажувачами та BIOS, перевіряє та криптографічно записує кожен крок завантаження у ланцюжку. Ці події прив'язані до співпроцесора безпеки (TPM), який виступає як корінь довіри. Віддалена атестація – це механізм, за допомогою якого служба зчитує та перевіряє ці події для надання перевіряється, ненаправлено та незаконно змінено стійкий звіт. Дистанційна атестація є довіреним аудитором завантаження системи, що дозволяє певним сутностям довіряти пристрою.

Нижче наведено зведення дій щодо атестації та нульової довіри на стороні пристрою.

1. На кожному етапі процесу завантаження, наприклад завантаження файлу, оновлення спеціальних змінних тощо, такі відомості, як ґеші файлів і підпис, вимірюються в PRS TPM. Вимірювання прив'язані специфікацією довіреної групи обчислень (TCG), яка визначає, які події можуть бути записані, та формат кожної події.

2. Після завантаження Windows атестатор або модуль, що перевіряється, запитує у довіреного платформного модуля отримання вимірювань, що зберігаються в регістрі конфігурації платформи (PCR) разом з журналом TCG. Вимірювання в обох компонентах формують свідчення атестації, яке потім відправляється в службу атестації.

3. Довірений платформний модуль перевіряється за допомогою ключів або криптографічних матеріалів, доступних у наборі мікросхем із службою сертифікатів Azure.

4. Потім ці відомості надсилаються до служби атестації у хмарі, щоб переконатися, що пристрій є безпечним. Microsoft Endpoint Manger інтегрується з Microsoft Атестація Azure для комплексного аналізу працездатності пристрою та підключення цієї інформації до умовного доступу до Azure Active Directory.

Ця інтеграція є ключем до рішень «Нікому не довіряй", які допомагають прив'язати довіру до ненадійних пристроїв.

5. Служба атестації виконує такі завдання:

– Перевірте цілісність свідчення. Ця перевірка виконується шляхом перевірки PRS, які відповідають значенням, які перераховуються шляхом відтворення журналу TCG.

– Переконайтеся, що TPM має дійсний ключ посвідчення атестації, виданий перевіркою TPM.

– Переконайтеся, що функції безпеки знаходяться в очікуваному стані.

– Служба атестації повертає звіт про атестацію, що містить відомості про функції безпеки на основі політики, налаштованої у службі атестації.

– Потім пристрій надсилає звіт у хмару Microsoft Endpoint Manager для оцінки надійності платформи відповідно до правил відповідності пристроїв, налаштованих адміністратором.

– Умовний доступ разом зі станом відповідності пристроїв вирішує дозволити або заборонити доступ.

Апаратна безпека Windows

Сучасні загрози вимагають сучасної безпеки з надійним узгодженням між апаратною безпекою та методами безпеки програмного забезпечення для захисту користувачів, даних та пристроїв. Тільки операційна система не може захиститися від широкого спектру засобів та методів, які зловмисники використовують для компрометації комп'ютера у його кремнієвих системах. Всередині зловмисників може бути важко виявити зловмисників, які можуть бути залучені до декількох шкідливих дій, від крадіжки важливих даних до запису адрес електронної пошти та інших конфіденційних відомостей. Ці нові загрози спричинять обчислювальні апаратні засоби, які захищені до самого ядра, включаючи апаратні мікросхеми та процесори. Корпорація Майкрософт та наші партнери, у тому числі виробники мікросхем та пристроїв.

Заходи безпеки	**Функції & можливості**
Довірений платформний модуль (TPM)	Довірений платформний модуль (TPM) призначений для надання апаратних функцій безпеки та запобігання небажаним незаконним змінам. TPM надають переваги безпеці та конфіденційності для системного обладнання, власників платформ та користувачів. Мікросхема довіреного платформного модуля – це захищений криптографічний процесор, який допомагає виконувати такі дії, як створення, зберігання та обмеження використання криптографічних ключів. Багато TPM включають кілька фізичних механізмів безпеки, щоб запобігти незаконній зміні та запобіганню незаконної зміни шкідливим програмним забезпеченням функцій безпеки довіреного платформного модуля.

Кореневий каталог довіри на основі обладнання з System Guard у Захиснику Windows	Для захисту критично важливих ресурсів, таких як автентифікація Windows, маркери єдиного входу, Windows Hello і модуль віртуальної довіреної платформи, вбудоване ПЗ та обладнання системи повинні бути надійними. System Guard у Windows Defender допомагає захистити та підтримувати цілісність системи в міру її запуску та перевірки того, чи дійсно цілісність системи була збережена за допомогою локальної та віддаленої атестації.
Увімкнення функції захисту цілісності коду на основі віртуалізації	HVCI – це функція безпеки на основі віртуалізації (VBS), доступна у Windows. У Windows безпеки пристроїв HVCI називається цілісністю пам'яті. HVCI і VBS покращують модель загроз Windows забезпечують надійніший захист від шкідливих програм, які намагаються використовувати Windows ядра. VBS використовує гіпервізор Windows для створення ізольованого віртуального середовища, яке стає коренем довіри операційної системи, яка передбачає, що ядро може бути скомпрометоване. HVCI – це критично важливий компонент, який захищає та захищає це віртуальне середовище, запускаючи в ньому цілісність коду в режимі ядра та обмежуючи виділення пам'яті ядра, яке може використовуватися для компрометації системи.
Захист прямого доступу до пам'яті ядра (DMA)	Пристрої гарячого модуля PCIe, такі як Thunderbolt, USB4 і CFexpress, дозволяють користувачам підключати нові класи зовнішніх периферійних пристроїв, включаючи графічні карти або інші пристрої PCI, до своїх комп'ютерів з інтерфейсом, ідентичним USB. Так як порти гарячого модуля PCI, що підключається, є зовнішніми і легко доступні, комп'ютери піддаються атакам прямого доступу до пам'яті (DMA). Захист доступу до пам'яті (також відомий як захист DMA ядра) захищає комп'ютери від атак DMA на диску, що використовують пристрої гарячого модуля PCIe, що підключається, обмеживши ці зовнішні периферійні пристрої можливістю безпосередньо копіювати пам'ять, коли користувач заблокує свій комп'ютер.

Комп'ютери із захищеними ядрами	Корпорація Майкрософт тісно співпрацює з партнерами OEM та постачальниками кремнієвого обладнання для створення захищених ядер комп'ютерів з глибоко інтегрованим обладнанням, вбудованим програмним забезпеченням та програмним забезпеченням для забезпечення підвищеної безпеки пристроїв, посвідчень та даних. Захищені основні комп'ютери забезпечують захист від складних атак і забезпечують підвищену впевненість при обробці критично важливих даних у деяких найбільш чутливих до цих галузях, таких як медичні працівники, які обробляють медичні записи та інші персональні дані (PII), комерційні ролі, які обробляють високий рівень впливу на бізнес та високо конфіденційні дані, такі як фінансовий контролер з даними про прибуток. Додаткові відомості прозахищені комп'ютери з ядрами.

Довірений платформний модуль

Технологія довірених платформних модулів (TPM) призначена для надання апаратних функцій, пов'язаних із безпекою. Мікросхема TPM – це надійний криптографічний процесор, який дозволяє створювати, зберігати та обмежувати використання криптографічних ключів. Детальний опис див. у наступних розділах.

Розділ	Опис
Огляд довіреного платформного модуля	Огляд довіреного платформного модуля (TPM) та його використання у Windows для керування доступом та автентифікації.
Основи TPM	Загальні відомості про роботу довіреного платформного модуля із ключами шифрування. Тут також описуються технології, які працюють з TPM, наприклад, віртуальні смарт-карти на основі TPM.
Параметри групової політики довіреного платформного модуля	Тут розглядаються служби TPM, якими централізовано можна керувати за допомогою параметрів групової політики:
Резервне копіювання даних відновлення TPM в AD DS	Опис резервного копіювання даних довіреного платформного модуля комп'ютера в доменних службах Active Directory (лише для Windows 10, версія 1511 та 1507).

Виправлення неполадок довіреного платформного модуля (TPM)	Опис дій, які можна виконати в оснастці TPM, TPM.msc: перегляд стану TPM, усунення проблем ініціалізації TPM та видалення ключів з TPM. Крім того, для TPM 1.2 та Windows 10 версії 1507 або 1511 або Windows 11 описується, як увімкнути або вимкнути TPM.
Загальні відомості про банки PCR на пристроях TPM 2.0	Загальні відомості про те, що відбувається під час перемикання банків PCR на пристроях TPM 2.0.
Рекомендації щодо довіреного платформного модуля	Розглядаються аспекти TPM, такі як різниця між TPM 1.2 та 2.0, та функції Windows, для яких потрібно або рекомендується використовувати TPM.

Захисник Windows System Guard: як апаратний корінь довіри допомагає захистити Windows 10

Щоб захистити критично важливі ресурси, такі як Windows стек автентифікації, однотонні маркери, біометричний стек Windows Hello і модуль віртуальної надійної платформи, необхідно довіряти прошивці та обладнанню системи.

Захисник Windows System Guard реорганізує існуючі Windows 10 функції цілісності системи під одним дахом і визначає наступний набір інвестицій у Windows безпеки. Він призначений для забезпечення цих гарантій безпеки:

– Захист та збереження цілісності системи у міру її початку.

– Перевірка того, що цілісність системи дійсно підтримується за допомогою локальної та віддаленої перевірки.

Підтримка цілісності системи у міру її початку

Статичний корінь довіри для вимірювання (SRTM)

З Windows 7 одним із засобів, які зловмисники будуть використовувати для виявлення і ухилятися від виявлення, є установка в системі так часто іменованого як bootkit або rootkit. Це шкідливе програмне забезпечення почнеться Windows запуску або під час процесу завантаження, що дозволить йому почати з найвищого рівня привілеїв.

З Windows 10 на сучасному обладнанні (тобто Windows 8 сертифіковано або більше) корінь довіри на основі обладнання допомагає переконатися, що несанкціоноване прошивка або програмне забезпечення (наприклад, bootkit) може розпочатися до завантаження Windows завантажувача. Ця коренева довіра на основі обладнання походить від функції Безпечного завантаження пристрою, яка є частиною єдиного extensible інтерфейсу прошивки (UEFI). Цей метод вимірювання статичних ранніх компонентів завантаження UEFI називається статичним коренем довіри вимірювання (SRTM).

Так як існують тисячі постачальників ПК, які виробляють багато моделей з різними версіями UEFI BIOS, при завантаженні стає неймовірно велика кількість вимірів SRTM. Для встановлення довіри тут існують два методи: або підтримувати список відомих «поганих» вимірів SRTM (також відомих як блок-

лист), або список відомих «хороших» вимірів SRTM (також відомий як список дозвільних даних).

Кожен варіант має недолік:

– Список відомих «поганих» вимірювань SRTM дозволяє хакеру змінити лише 1 біт у компоненті, щоб створити новий ґеш SRTM, який необхідно перерахувати. Це означає, що потік SRTM за своєю суттю є крихким – незначна зміна може призвести до недійсних для всього ланцюжка довіри.

– Список відомих «хороших» вимірювань SRTM вимагає, щоб кожен новий вимір комбінації BIOS/PC був ретельно доданий, що є повільним. Крім того, виправлення помилки для коду UEFI може зайняти багато часу для розробки, складання, повторної перевірки, перевірки та переробки.

Безпечний запуск – динамічний корінь довіри для вимірювання (DRTM)

Захисник Windows System Guard Secure Launch, вперше представлений у Windows 10 версії 1809, спрямований на усунення цих проблем за допомогою технології, відомої як динамічний корінь довіри для вимірювання (DRTM). DRTM дозволяє системі вільно завантажитися в ненаглядовий код спочатку, але незабаром після запуску системи в надійний стан, взявши під контроль всі процесори і змусивши їх вниз по відомому та виміряному шляху коду. Це дозволяє ненадійним раннім кодом UEFI завантажити систему, але потім безпечно перейти в надійний та виміряний стан.

Secure Launch спрощує управління вимірами SRTM, оскільки код запуску тепер не пов'язаний із певною конфігурацією обладнання. Це означає, що кількість допустимих вимірювань коду невелика, а майбутні оновлення можна розгорнути ширше та швидше.

Захист режиму керування системою (SMM)

Режим управління системою (SMM) – це режим ЦП спеціального призначення в мікроконтролерах x86, який обробляє управління живленням, конфігурацію обладнання, моніторинг теплового середовища та все інше, що виробник вважає за корисне. Щоразу, коли запитується одна з цих системних операцій, під час виконання викликається не переривання, що маскується (SMI), який виконує SMM-код, встановлений BIOS. SMM-код виконується на найвищому рівні привілеїв та невидимий для ОС, що робить його привабливою метою для шкідливих дій. Навіть якщо для пізнього запуску використовується system Guard Secure Launch, SMM-код потенційно може отримати доступ до пам'яті гіпервізора та змінити гіпервізор.

Для захисту від цього використовуються два методи:

– Захист підкачки для запобігання неналежного доступу до коду та даних.

– Спостереження та аттестація обладнання SMM.

Захист від пагінгу може бути реалізований для блокування певних таблиць коду для читання тільки для запобігання фальсифікації. Це запобігає доступу до пам'яті, яка не була призначена.

Функція обробника SMI з апаратним забезпеченням, відома як обробник SMI, може відстежувати SMM і не отримувати доступу до будь-якої частини адресного простору, на яку вона не повинна.

Захист SMM побудований на основі технології Secure Launch і потребує її функціонування. У майбутньому Windows 10 також буде вимірювати поведінку обробника SMI і засвідчити, що жодна пам'ять, що належить ОС, не була підроблена.

Перевірка цілісності платформи після Windows (час запуску)

Хоча Захисник Windows System Guard надає розширені засоби захисту, які допоможуть захистити та зберегти цілісність платформи під час завантаження та під час запуску, реальність така, що ми повинні застосувати ментальність «припустити порушення» навіть для наших найскладніших технологій безпеки. Ми можемо довіряти, що технології успішно роблять свою роботу, але нам також потрібна можливість переконатися, що вони успішно досягають своєї мети. Для цілісності платформи ми можемо просто довіряти платформі, яка потенційно може бути скомпрометована, щоб самостійно підтвердити її стан безпеки. Так Захисник Windows System Guard включає низку технологій, які дозволяють віддалено аналізувати цілісність пристрою.

Як Windows 10 чоботи, ряд вимірів цілісності Захисник Windows System Guard за допомогою довіреного модуля платформи 2.0 (TPM 2.0). System Guard Secure Launch не підтримує попередні версії TPM, наприклад TPM 1.2. Цей процес та дані ізольовані від Windows, щоб гарантувати, що дані вимірювань не схильні до типу фальсифікації, які можуть статися, якщо платформа була скомпрометована. Тут вимірювання можна використовувати для визначення цілісності прошивки пристрою, стану конфігурації обладнання та компонентів Windows, пов'язаних із завантаженням.

Після роботи системи Захисник Windows system Guard підписує та запечатує ці вимірювання за допомогою TPM. За запитом, система керування, наприклад Intune або Microsoft Endpoint Configuration Manager, може придбати їх для віддаленого аналізу. Якщо Windows Defender system Guard вказує, що пристрій не вистачає цілісності, система керування може прийняти ряд дій, наприклад заборонити пристрою доступ до ресурсів.

Безпечний запуск System Guard та захист SMM

У цьому розділі пояснюється, як налаштувати захист системного безпечного запуску та режиму керування системою (SMM) для підвищення безпеки під час запуску Windows 10 та Windows 11 пристроїв. Наведені нижче відомості представлені з погляду клієнта.

Увімкнення безпечного запуску System Guard

Ви можете увімкнути безпечний запуск System Guard за допомогою будь-якого з наступних параметрів:

- Управління мобільними пристроями (MDM).
- Групова політика.
- Безпека Windows програми.
- Реєстр.

Управління мобільними пристроями

Безпечний запуск System Guard можна налаштувати для мобільних Керування пристроями (MDM) за допомогою DeviceGuard у постачальника служб конфігурації політики DeviceGuard/ConfigureSystemGuardLaunch.

Групова політика

1. Натисніть кнопку « >« і виберіть «Змінити групову політику".

2. Натисніть кнопку «Адміністративні > шаблони конфігурації комп'ютера > «. Система > Device Guard > увімкне > конфігурацію безпечного запуску на основі віртуалізації.

Безпека Windows програми

Натисніть кнопку start > Установки > Update & Security > Безпека Windows > Open Безпека Windows > Device security > Core isolation > Firmware protection.

Реєстр

1. Відкрийте редактор реєстру.

2. Клацніть HKEY_LOCAL_MACHINE > system > CurrentControlSet > Control > DeviceGuard > Scenarios.

3. Клацніть правою кнопкою миші «Сценарії створення > ключа > « і наведіть ім'я нового ключа SystemGuard.****

4. Клацніть правою кнопкою миші systemGuard > New > DWORD (32-розрядне) значення та наведіть ім'я нового параметра DWORD Enabled.

5. Двічі клацніть «Увімкнено «, змініть значення на 1 і натисніть кнопку «ОК".

Перевірка налаштування та виконання безпечного запуску System Guard

Щоб переконатися, що безпечний запуск запущено, використовуйте інформацію про систему (MSInfo32). Натисніть **кнопку «** Пуск «**, знайдіть** Відомості про систему та перегляньте **розділ «** Запущені служби безпеки на основі віртуалізації» та «Настроєні служби безпеки на **основі віртуалізації"**.

Увімкнення функції захисту цілісності коду на основі віртуалізації (HVCI)

У цьому розділі описано різні способи увімкнення цілісності коду із захистом гіпервізора (HVCI) Windows 10 і Windows 11. Деякі програми, включаючи драйвери пристроїв, можуть бути несумісні з HVCI. Така несумісність може призвести до збою пристроїв або програмного забезпечення, а в окремих випадках може призвести до синього екрана. Такі проблеми можуть виникати після активації служби HVCI або безпосередньо під час активації служби. Якщо ці проблеми виникають, див. інструкції з усунення несправностей.

Так як у ньому використовується управління виконанням на основі *режиму,* HVCI краще працює з процесорами Intel Kaby Lake або AMD Zen 2 та пізнішими версіями. Процесори без MBEC покладатимуться на емуляцію цієї функції, звану обмеженим користувальницьким режимом, *яка* більш впливає на продуктивність.

Функції HVCI

– HVCI захищає зміну растрового зображення Control Flow Guard (CFG).

– HVCI також гарантує, що інші довірені процеси, такі як Credential Guard отримали дійсний сертифікат.

– Сучасні драйвери пристроїв повинні мати сертифікат EV (розширена перевірка) і підтримувати HVCI.

Увімкнення HVCI у Windows 10 та Windows 11

Щоб увімкнути HVCI на Windows 10 та Windows 11 із допоміжним обладнанням на підприємстві, використовуйте будь-який з наступних варіантів:

– Безпека Windows програми.

– Microsoft Intune (або іншого постачальника MDM).

– Групова політика.

– Microsoft Endpoint Configuration Manager.

– Реєстр.

Безпека Windows програми

HVCI **** > позначена як **** цілісність пам'яті в програмі Безпека Windows, і доступ до неї можна отримати за допомогою оновлення параметрів & Security > Безпека Windows > Device security > Core isolation details > Memory integrity.

Увімкнення HVCI за допомогою Intune

Щоб увімкнути Intune, необхідно використовувати вузол цілісності коду в постачальнику служб конфігурації AppLocker.

Включення HVCI за допомогою групової політики

1. Щоб змінити існуючий об'єкт групової політики або створити новий об'єкт групової політики, використовуйте групову політику редактора (gpedit.msc).

2. Перейдіть до адміністративних > шаблонів конфігурації комп'ютера > System > Device Guard.

3. Двічі клацніть «Включити безпеку на основі віртуалізації".

4. Клацніть « Увімкнено» і в розділі «Захист цілісності коду на основі віртуалізації» виберіть «Увімкнено з блокуванням UEFI **", щоб переконатися, що HVCI не можна відключити віддалено, або виберіть «Увімкнено без блокування UEFI".

5. Натисніть кнопку « ОК", щоб закрити редактор.

Щоб застосувати нову політику на комп'ютері, приєднаному до домену, перезапустіть або запустіть gpupdate /forceкомандний рядок з підвищеними привілеями.

Використання розділів реєстру для увімкнення захисту цілісності коду на основі віртуалізації

Встановіть наступні значення розділів реєстру, щоб увімкнути HVCI. Ці ключі надають такий самий набір параметрів конфігурації, що і групова політика.

Захист DMA для ядра

У Windows 10 версії 1803 корпорація Майкрософт представила нову функцію під назвою «Захист DMA ядра» для захисту комп'ютерів від атак прямого доступу до пам'яті (DMA) за допомогою пристроїв гарячого модуля PCI, що підключається до зовнішніх портів PCIe (наприклад, портів Thunderbolt™ CFexpress). У Windows 10 версії 1903 корпорація Майкрософт розширює підтримку захисту DMA ядра, щоб охопити внутрішні порти PCIe (наприклад, слоти M.2).

Атаки DMA на диску можуть призвести до розкриття конфіденційної інформації на комп'ютері або навіть впровадження шкідливих програм, які дозволяють зловмисникам обійти екран блокування або керувати комп'ютерами віддалено.

Ця функція не захищає від атак DMA за допомогою 1394/FireWire, PCMCIA, CardBus, ExpressCard тощо.

Фон

Пристрої PCI підтримують DMA, що дозволяє їм зчитувати та записувати системну пам'ять у міру потреби, не залучаючи системний процесор до цих операцій. Можливість DMA – це те, що робить пристрої PCI найбільш високовиробними пристроями, доступними на сьогоднішній день. Ці пристрої історично існували лише у корпусі ПК, підключених як картка чи припайних до плати. Для доступу до цих пристроїв користувачеві потрібно було вимкнути живлення системи та дизассемблювати корпус.

В даний час це більше не працює з портами PCIe гарячого модуля (наприклад, Thunderbolt™ і CFexpress).

Порти pcIe з гарячим модулем, що підключається, такі як технологія Thunderbolt™, надали сучасні комп'ютери з розширюваністю, яка раніше була недоступна для комп'ютерів. Він дозволяє користувачам підключати нові класи зовнішніх периферійних пристроїв, таких як графічні карти або інші пристрої PCI, до своїх комп'ютерів за допомогою гарячого модуля, що підключається, ідентичного USB. Наявність зовнішніх і легко доступних портів гарячого модуля PCI, що підключається, робить комп'ютери вразливими до атак DMA на дисках.

Атаки DMA на диску – це атаки, які відбуваються, коли власник системи відсутній і зазвичай займає менше 10 хвилин з простими і модеративними засобами атак (доступним, готовим обладнанням та програмним забезпеченням), які не потребують дизассемблювання комп'ютера. Простим прикладом може бути те, що власник комп'ютера залишає комп'ютер для швидкої кавоварки, а в перерві зловмисник підключається до USB-пристрою та покрокову передачу всіх секретів на комп'ютері або впроваджує шкідливу програму, яка дозволяє йому віддалено керувати комп'ютером.

Захист Windows від атак на диски DMA

Windows використовує системну одиницю керування пам’яттю вводу-виводу (IOMMU) для блокування запуску та виконання DMA зовнішніми периферійними пристроями, якщо драйвери цих периферійних пристроїв не підтримують ізоляцію пам'яті (наприклад, DMA-remapping). Периферійні пристрої із сумісними драйверами DMA Remapping автоматично

перераховуються, запускаються і можуть виконувати DMA у призначених ним областях пам'яті.

За замовчуванням периферійні пристрої з несумісними драйверами DMA remapping блокуватимуть запуск та виконання DMA доти, доки авторизований користувач не увійде до системи або не розблокує екран. IT-адміністратори можуть змінювати стандартну поведінку, яка застосовується до пристроїв з несумісними драйверами DMA RemaPping, за допомогою політик MDM DmaGuard.

Взаємодія з користувачем

За замовчуванням периферійні пристрої з драйверами пристроїв, сумісними з DMA, автоматично перераховуватимуться та запускатимуться. Периферійні пристрої з несумісними драйверами перенаправлення DMA будуть заблоковані, якщо периферійний пристрій був підключений до входу авторизованого користувача або під час блокування екрана. Після розблокування системи ос запускає периферійний драйвер, і периферійний пристрій працюватиме у звичайному режимі до перезавантаження системи або вимкнення периферійного пристрою. Периферійний пристрій продовжить працювати у звичайному режимі, якщо користувач заблокує екран або вийдіть із системи.

Сумісність системи

Для захисту від Ядра DMA потрібна нова підтримка вбудованого UEFI. Ця підтримка очікується тільки в системах, що недавно з'явилися, на базі Intel з Windows 10 версії 1803 (не для всіх систем). Безпека на основі віртуалізації (VBS) не потрібна.

Щоб дізнатися, чи підтримує система захисту DMA ядра, перевірте настільний додаток System Information (MSINFO32). Системи, випущені до Windows 10 версії 1803, не підтримують захист DMA ядра, але можуть використовувати інші заходи щодо усунення атак DMA, як описано у статті про лічильники BitLocker.

Безпека операційної системи Windows

Безпека та конфіденційність залежать від операційної системи, яка захищає систему та інформацію з моменту її запуску, забезпечуючи основний захист від мікросхеми у хмару. Windows 11 є найбільш безпечним Windows з великими заходами безпеки, призначеними для забезпечення безпеки. До цих заходів відносяться вбудоване розширене шифрування і захист даних, надійна безпека мережі та системи, а також інтелектуальні заходи захисту від загрози, що постійно змінюється.

Заходи безпеки	Функції та можливості
Безпечне завантаження та довірене завантаження	Безпечне завантаження та довірене завантаження допомагають запобігти завантаженню шкідливих програм та пошкоджених компонентів у Windows пристрою. Безпечне завантаження починається з початкового захисту під час завантаження, а потім довірене завантаження вибирає процес. Водночас безпечне завантаження та довірене завантаження допомагають забезпечити безпечне завантаження системи Windows.
Управління криптографією та сертифікатами	Шифрування використовує код для перетворення даних, щоб конкретний одержувач зчитую їх за допомогою ключа. Шифрування забезпечує конфіденційність, щоб ніхто, крім передбачуваного одержувача, не зчитування даних, цілісність, щоб забезпечити захист даних від незаконної зміни, та автентифікацію, яка перевіряє посвідчення для забезпечення безпеки обміну даними.
Безпека Windows програми	Вбудований Windows безпеки, знайдений у параметрах, дозволяє швидко переглянути стан безпеки та працездатність пристрою. Ці аналітичні відомості допомагають виявити проблеми та вжити заходів для захисту.
Шифрування та захист даних	Де конфіденційні дані не зберігаються, вони повинні бути захищені від несанкціонованого доступу, як шляхом крадіжки фізичного пристрою, так і з шкідливих додатків. Windows надійні рішення захисту неактивних даних, які забезпечують захист від зловмисників.
BitLocker	Шифрування диска BitLocker – це функція захисту даних, яка інтегрується в операційну систему та запобігає загрозі розкрадання даних або розкриття інформації на втрачених, вкрадених або неправильно виведених з експлуатації комп'ютерах. BitLocker забезпечує максимальний захист при використанні довіреного платформного модуля (TPM) версії 1.2 або вище.

Зашифрований жорсткий диск	Зашифрований жорсткий диск використовує швидке шифрування, що надається шифруванням диска BitLocker, для підвищення безпеки даних та управління ними. Шляхом передачі криптографічних операцій на обладнання функція «Зашифрований жорсткий диск» підвищує продуктивність BitLocker та знижує споживання ресурсів ЦП та електроенергії. Завдяки тому, що функція зашифрованих жорстких дисків швидко шифрує дані, пристрої організації можуть розширювати розгортання BitLocker з мінімальним впливом на продуктивність.
Базові показники безпеки	Базові параметри безпеки – це група рекомендованих корпорацією Майкрософт параметрів конфігурації, щоб пояснити їх вплив на безпеку. Ці параметри ґрунтуються на відгуках фахівців із забезпечення безпеки Microsoft, груп розвитку продуктів, партнерів та клієнтів. Базові показники безпеки включені до набору засобів забезпечення відповідності вимогам безпеки, який можна завантажити з Центру завантаження Майкрософт.
Віртуальна приватна мережа	Віртуальні приватні мережі (VPN) – це з'єднання точки в приватній або загальнодоступній мережі, наприклад, в Інтернеті. VPN-клієнт використовує спеціальні протоколи на основі TCP/IP або UDP, які називають протоколами тунелювання для віртуального виклику віртуального порту VPN-сервера.
Брандмауер Windows Defender	Брандмауер Захисника Windows – це брандмауер вузла з відстеженням стану, який допомагає захистити пристрій, дозволяючи створювати правила, які визначають, який мережевий трафік може входити на пристрій з мережі та який мережевий трафік пристрій може надсилати до мережі. брандмауер Windows Defender також підтримує протокол IPsec, який можна використовувати для запиту автентифікації з будь-якого пристрою, який намагається зв'язатися з пристроєм.

Антивірусна програма & захист від шкідливих програм	Антивірусна програма в Microsoft Defender включена у всі версії Windows 10, Windows Server 2016 і пізніших версій, а також Windows 11. Якщо у вас встановлена та включена інша антивірусна програма, антивірусна програма в Microsoft Defender автоматично відключається. Якщо видалити іншу програму, антивірусна програма в Microsoft Defender знову буде увімкнено. З моменту завантаження Windows антивірусна програма в Microsoft Defender постійно відстежує шкідливі програми, віруси та загрози безпеці. Оновлення завантажуються автоматично, щоб захистити пристрій від загроз. антивірусна програма в Microsoft Defender постійно перевіряє наявність шкідливих програм та загроз, а також виявляє та блокує потенційно небажані програми (додатки, які можуть негативно вплинути на пристрій, навіть якщо вони не вважаються шкідливими). Антивірусна програма в Microsoft Defender інтегрується з хмарним захистом, який забезпечує практично миттєве виявлення та блокування нових та нових загроз.
Правила скорочення напрямів атак	Ваші області атаки – це місця та способи, якими ви схильні до кібератаків. Правила зменшення вразливої зони вбудовані в Windows та Windows Server для запобігання та блокування певних дій, які часто використовуються для компрометації пристрою або мережі. Така поведінка може включати запуск скриптів або виконуваних файлів, які намагаються завантажити або запустити інші файли, запускати підозрілі скрипти або виконувати інші дії, які програми зазвичай не ініціюють під час звичайної роботи. Ви можете налаштувати правила зменшення вразливої зони для захисту від ризикованих дій.

Захист від незаконної зміни	Під час кібер атак (наприклад, спроб програм-шантажистів) зловмисники намагаються відключити функції безпеки, такі як антивірусний захист на цільових пристроях. Зловмисники хотіли б вимкнути функції безпеки, щоб спростити доступ до даних користувача, встановити шкідливі програми або іншим чином скористатися даними, посвідченнями та пристроями користувача, не побоюючись блокування. Захист від незаконної зміни допомагає запобігти таким діям. При захисті від незаконної зміни шкідливі програми не можуть виконувати такі дії, як: – відключення захисту від вірусів і загроз – відключення захисту в режимі реального часу – відключення моніторингу поведінки – відключення антивірусної програми (наприклад, IOffice Antivirus (IOAV)) – відключення хмарного захисту; – видалення оновлень аналітики безпеки.
Захист мережі	Захист мережі у Windows допомагає запобігти доступу користувачів до небезпечних IP-адрес і доменів, на яких можуть бути розміщені атаки фішингу, експлойти та інший шкідливий вміст в Інтернеті. Захист мережі є частиною скорочення напрямків атак та допомагає забезпечити додатковий рівень захисту для користувача. За допомогою служб на основі репутації захист мережі блокує доступ до потенційно шкідливих доменів та IP-адрес на основі низької репутації. У корпоративних середовищах захист мережі найкраще працює з Microsoft Defender для кінцевої точки, яка надає докладні звіти про події захисту в рамках більших сценаріїв дослідження.
Контрольований доступ до папок	За допомогою керованого доступу до папок можна захистити цінну інформацію у певних папках, керуючи доступом додатків до певних папок. Тільки довірені програми можуть отримати доступ до захищених папок, заданих при налаштуванні керованого доступу до папок. Як правило, до списку керованих папок включаються папки, що часто використовуються, наприклад для документів, зображень, файлів, що завантажуються. Керований доступ до папок допомагає захистити цінні дані від шкідливих програм та загроз, таких як програми-шантажисти.

Захист від експлойтів	Захист від експлойтів, доступний у Windows 10 версії 1709 і пізніших, автоматично застосовує кілька методів усунення експлойтів до процесів та додатків операційної системи. Захист від експлойтів найкраще працює з Microsoft Defender для кінцевої точки, яка надає організаціям докладні звіти про події та блоки захисту від експлойтів у рамках типових сценаріїв дослідження оповіщень. Ви можете увімкнути захист від експлойтів на окремому пристрої, а потім використовувати групова політика для поширення файлу XML на кілька пристроїв одночасно. Якщо ви знайдете захист на пристрої, з'явиться повідомлення із центру сповіщень. Ви можете налаштувати повідомлення, вказавши відомості про компанію та контактні дані. Ви також можете включити правила окремо, щоб налаштувати методи, які відстежуються компонентами.
Microsoft Defender для кінцевої точки	Windows E5 отримують переваги від Microsoft Defender для кінцевої точки, корпоративної виявлення та нейтралізація атак на кінцеві точки, яка допомагає корпоративним командам безпеки виявляти, досліджувати та реагувати на складні загрози. Завдяки докладним даними про події та аналітичні відомості про атаки Defender для кінцевої точки дозволяє групі безпеки дослідити інциденти та ефективно та ефективно виконувати дії з виправлення. Defender для кінцевої точки також є частиною Microsoft 365 Defender, єдиного корпоративного набору засобів захисту до та після порушення безпеки, що спочатку координує виявлення, запобігання, дослідження та реагування на них між кінцевими точками, посвідченнями, електронною поштою та додатками для забезпечення інтегрованого захисту від складних атак.

Безпечне завантаження та довірене завантаження

Безпечне завантаження та довірене завантаження допомагають запобігти завантаженню шкідливих програм та пошкоджених компонентів при Windows 11 пристрою. Безпечне завантаження починається з початкового захисту під час завантаження, а потім довірене завантаження вибирає процес. Водночас безпечне завантаження та довірене завантаження допомагають забезпечити безпечне завантаження Windows 11 системи.

Безпечне завантаження

Першим кроком у захисті операційної системи є забезпечення безпечного завантаження після безпечного завершення початкових послідовностей завантаження обладнання та вбудованого програмного забезпечення. Безпечне завантаження забезпечує безпечний та надійний шлях із UEFI через послідовність надійного завантаження ядра Windows. Атаки шкідливих програм на послідовність завантаження Windows блокуються підтвердженнями застосування підписів у всій послідовності завантаження між середовищами UEFI, завантажувачем, ядром та додатками.

Коли комп'ютер починає процес завантаження, він спочатку перевіряє, чи підписано вбудоване програмне забезпечення цифровим підписом, що знижує ризик використання кореневих наборів вбудованого програмного забезпечення. Потім безпечне завантаження перевіряє весь код, що виконується до операційної системи, і перевіряє цифровий підпис завантажувача ОС, щоб переконатися, що вона є довіреною політикою безпечного завантаження і не була змінена.

Надійне завантаження

Довірене завантаження вибирає процес, який розпочався із безпечного завантаження. Завантажувач Windows перевіряє цифровий підпис ядра Windows перед завантаженням. Ядро Windows, у свою чергу, перевіряє всі інші компоненти процесу запуску Windows, у тому числі драйвери завантаження, файли запуску та драйвер антишкідливих програм для раннього запуску антишкідливих програм (ELAM). Якщо якийсь із цих файлів було змінено, завантажувач виявляє проблему та відхиляє завантаження пошкодженого компонента. Незаконна зміна або шкідливі програми в послідовності завантаження Windows блокуються підтвердженням застосування сигнатур між середовищами UEFI, завантажувачем, ядром та програмами.

Часто Windows може автоматично відновити пошкоджений компонент, відновлюючи цілісність Windows і дозволяючи Windows 11 нормально запускатися.

Шифрування та захист даних у Windows клієнті

Коли люди переміщуються разом зі своїми комп'ютерами та пристроями, їхня конфіденційна інформація передається разом з ними. Де конфіденційні дані не зберігаються, вони повинні бути захищені від несанкціонованого доступу, як шляхом крадіжки фізичного пристрою, так і з шкідливих додатків. Функції шифрування та захисту даних включають:

– Зашифрований жорсткий диск.
– BitLocker.

Зашифрований жорсткий диск

Зашифрований жорсткий диск використовує швидке шифрування, що надається шифруванням диска BitLocker, для підвищення безпеки даних та управління ними. Розвантаживши криптографічні операції на обладнання, зашифровані жорсткі диски збільшують продуктивність BitLocker та знижують завантаження ЦП та енергоспоживання. Оскільки зашифровані жорсткі диски

швидко шифрують дані, корпоративні пристрої можуть розширювати розгортання BitLocker із мінімальним впливом на продуктивність.

Зашифровані жорсткі диски надають такі можливості:

– Підвищена продуктивність: обладнання шифрування, інтегроване в контролер диска, дозволяє працювати з повною швидкістю передачі даних без зниження продуктивності.

– Надійна безпека на основі обладнання: шифрування завжди увімкнено, а ключі шифрування ніколи не залишають жорсткий диск. Перевірка автентифікації користувача виконується диском до його розблокування незалежно від операційної системи.

– Простота використання: шифрування є прозорим для користувача, і користувачеві не потрібно його увімкнути. Зашифровані жорсткі диски легко видаляються за допомогою локального ключа шифрування. не потрібно повторно шифрувати дані на диску.

– Низька вартість володіння: нова інфраструктура не потрібна для керування ключами шифрування, оскільки BitLocker використовує існуючу інфраструктуру для збереження відомостей про відновлення. Пристрій працює ефективніше, оскільки цикли процесора не потрібно використовувати для процесу шифрування.

Зашифровані жорсткі диски – це новий клас жорстких дисків, які самозашифруються на апаратному рівні та дозволяють повністю шифрувати обладнання на диску.

BitLocker

Шифрування диска BitLocker – це функція захисту даних, яка інтегрується в операційну систему та запобігає загрозі розкрадання даних або розкриття інформації на втрачених, вкрадених або неправильно виведених з експлуатації комп'ютерах.

BitLocker забезпечує шифрування операційної системи, фіксованих даних та знімних дисків даних за допомогою таких технологій, як апаратний інтерфейс тестування безпеки (HSTI), сучасний резервний сервер, безпечне завантаження UEFI та TPM.

Windows постійно покращує захист даних, покращуючи наявні параметри та надаючи нові стратегії.

Базові показники безпеки

Використання базових параметрів безпеки у вашій організації

Корпорація Майкрософт призначена для надання клієнтам безпечних операційних систем, таких як Windows та Windows Server, та безпечних програм, таких як програми Microsoft 365 для підприємств та Microsoft Edge. Крім гарантії безпеки своїх продуктів, Microsoft також дозволяє точно керувати середовищем за допомогою різних можливостей конфігурації.

Незважаючи на те, що в Windows і Windows Server реалізовані вбудовані засоби безпеки, багатьом організаціям все ж таки потрібен ретельніший контроль над конфігураціями безпеки. Для орієнтації в різних елементах управління

організаціям потрібні рекомендації щодо налаштування різних функцій безпеки. Microsoft надає такі рекомендації як базові параметри безпеки.

Рекомендується відмовитися від самостійного створення конфігурацій на користь розгортання поширених і ретельно протестованих стандартних конфігурацій, наприклад, базових параметрів безпеки Microsoft. Ця стандартна у галузі конфігурація допомагає підвищити гнучкість та знизити витрати.

Для отримання додаткових відомостей див. наступний запис блогу: «Використання добре відомих і перевірених рішень".

Що таке базові параметри безпеки?

Кожна організація стикається з загрозами безпеці. Однак типи загроз безпеці, які є найважливішими для однієї організації, можуть відрізнятися від інших. Наприклад, компанія електронної комерції може зосередитись на захисті своїх веб-додатків з виходом в Інтернет, а госпітал може зосередитися на захисті конфіденційної інформації про пацієнтів. Всі ці організації об'єднує одне: їм необхідно забезпечити безпеку своїх програм та пристроїв. Пристрої повинні відповідати стандартам (або базовим параметрам) безпеки, які визначаються організацією.

Базові показники безпеки – це група рекомендованих корпорацією Майкрософт параметрів конфігурації, яка пояснює їх вплив на безпеку. Ці параметри ґрунтуються на відгуках фахівців із забезпечення безпеки Microsoft, груп розвитку продуктів, партнерів та клієнтів.

Навіщо потрібні базові параметри безпеки?

Базові параметри безпеки надають користувачам важливі переваги, оскільки поєднують глибокі знання фахівців Microsoft, її партнерів і клієнтів.

Наприклад, існує більше 3000 параметрів групової політики для Windows 10, які не включають більше 1800 параметрів Internet Explorer 11. З цих 4800 параметрів лише деякі пов'язані з безпекою. Хоча Microsoft надає комплексні рекомендації щодо різних функцій безпеки, вивчення кожної з них може тривати багато часу. Вам доведеться самостійно визначити вплив кожного параметра на безпеку. Потім, як і раніше, необхідно визначити відповідне значення для кожного параметра.

У сучасних організаціях середовище загроз безпеки постійно розвивається, і IT-фахівці та розробники політик повинні стежити за загрозами безпеки та вносити необхідні зміни до параметрів безпеки для усунення цих загроз. Щоб прискорити розгортання та спростити керування продуктами Майкрософт, корпорація Майкрософт надає клієнтам базові показники безпеки, доступні в форматах, що споживаються, таких як резервне копіювання об'єктів групової політики.

Базові принципи

Наші рекомендації відповідають спрощеному та ефективному підходу до базових визначень. В основі цього підходу, за суттю, є:

– Базові показники призначені для добре керованих організацій з підтримкою безпеки, в яких стандартні кінцеві користувачі не мають прав адміністратора.

– Базовий план застосовує параметр лише в тому випадку, якщо він усуває загрозу безпеці та не викликає операційних проблем, які гірші, ніж ризики, які вони усувають.

– Базовий план застосовує значення за замовчуванням тільки в тому випадку, якщо авторизований користувач може задати небезпечний стан:

- Якщо користувач без права адміністратора може встановити небезпечний стан, встановіть значення за замовчуванням.
- Якщо для налаштування небезпечного стану потрібні права адміністратора, примусіть значення за замовчуванням лише в тому випадку, якщо неправильно сформований адміністратор в іншому випадку вибере неправильний вибір.

Як використовувати базові параметри безпеки?

Базові параметри безпеки можна використовувати таким чином:

– для забезпечення відповідності параметрам конфігурації користувачів та пристроїв;

– для налаштування параметрів конфігурації. Наприклад, можна використовувати групову політику, Microsoft Endpoint Configuration Manager або Microsoft Intune для налаштування пристрою з параметрами, вказаними в базовому плані.

Де можна отримати базові параметри безпеки?

Існує кілька способів отримання та використання базових показників безпеки:

1. Ви можете завантажити базові параметри безпеки з Центру завантаження Майкрософт. Ця сторінка завантаження призначена для набору засобів забезпечення відповідності вимогам безпеки (SCT), який включає засоби, які можуть допомогти адміністраторам управляти базовими показниками на додаток до базових показників безпеки. SCT також включає засоби управління базовими показниками безпеки. Ви також можете одержати підтримку базових показників безпеки.

2. Базові показники безпеки управління мобільними пристроями (MDM) функції, такі як базові показники безпеки на основі групової політики Майкрософт, можуть легко інтегрувати ці базові показники в існуючий засіб управління MDM.

3. Базові показники безпеки MDM можна легко налаштувати в Microsoft Endpoint Manager на пристроях під керуванням Windows 10 та Windows 11. Додаткові відомості див. у списку параметрів у базовому плані безпеки MDM Windows 10/11 у Intune.

Технічний посібник з VPN Для Windows

У цьому посібнику наведено покрокові інструкції щодо прийняття рішень для Windows 10 або Windows 11 клієнтів у корпоративному рішенні VPN та налаштуванні розгортання. Цей посібник посилається на постачальника служб конфігурації (CSP) VPNv2 і містить інструкції з налаштування керування мобільними пристроями (MDM) за допомогою Microsoft Intune та шаблону профілю VPN для Windows 10 та Windows 11.

Розділ	Опис
Типи підключень VPN	Виберіть VPN-клієнт та протокол тунелювання.
Рішення про маршрутизацію для VPN	Виберіть конфігурацію з розділенням тунелю або примусовим використанням тунелю.
Параметри автентифікації для VPN	Виберіть метод автентифікації EAP.
VPN та умовний доступ	Використовуйте оцінку політики Azure Active Directory для налаштування політик доступу для підключення VPN.
Дозвіл імен VPN	Визначте, як працюватиме роздільна здатність імен.
Параметри профілю VPN, що автоматично ініціюються.	Налаштуйте профіль VPN, щоб автоматично встановлювати підключення залежно від програми або імені, включати режим «Завжди увімкнено» та не активувати VPN у довірених мережах.
Функції безпеки VPN	Налаштування фільтрації трафіку, підключення профілю VPN до Windows Information Protection (WIP) тощо.
Параметри профілю VPN	Об'єднайте параметри в один профіль VPN за допомогою XML.

Брандмауер Windows Defender з розширеною безпекою

У цьому розділі наведено огляд функцій брандмауера Windows Defender (WFS) та протоколу IPsec.

Загальні відомості про брандмауер Windows Defender з розширеною безпекою

Брандмауер Захисника Windows у Windows 8, Windows 7, Windows Vista, Windows Server 2012, Windows Server 2008 та Windows Server 2008 R2 – це брандмауер вузла з відстеженням стану, який допомагає захистити пристрій, дозволяючи створювати правила, що визначають, який мережевий трафік може входити на пристрій із мережі та який мережевий трафік. пристрій може надсилатися до мережі. брандмауер Windows Defender також підтримує протокол IPsec, який можна використовувати для запиту автентифікації з будь-якого пристрою, який намагається зв'язатися з пристроєм. Якщо потрібна автентифікація, пристрої, які не можуть бути автентифіковані як довірені пристрої, не можуть взаємодіяти з пристроєм. За допомогою IPsec можна також вимагати шифрування певного мережевого трафіку,

Оснащення брандмауера Windows Defender MMC розширеної безпеки є більш гнучким і надає набагато більше функціональних можливостей, ніж користувальницький інтерфейс брандмауера Windows Defender на панелі керування. Обидва інтерфейси взаємодіють із однаковими базовими службами, але забезпечують різні рівні контролю над цими службами. Хоча програма брандмауер Windows Defender панель керування може захистити один пристрій у домашній середовищі, вона не надає достатньо централізованих функцій

управління або безпеки для захисту більш складного мережевого трафіку в типовому корпоративному середовищі.

Опис компонента

брандмауер Windows Update з розширеною безпекою є важливою частиною багаторівневої моделі безпеки. Забезпечуючи двонаправлену фільтрацію мережевого трафіку на основі вузла для пристрою, брандмауер Windows Defender блокує несанкціонований мережевий трафік, що входить до локального пристрою або виходить з нього. брандмауер Windows Defender також працює зі службою «Повідомлення про мережу", щоб вона використовувала параметри безпеки, які відповідають типам мереж, до яких підключено пристрій. брандмауер Windows Defender конфігурації IPsec інтегровані в одну консоль керування (MMC) з іменем брандмауер Windows Defender, тому брандмауер Windows Defender також є важливою частиною мережі. стратегії ізоляції.

Практичне застосування

Щоб вирішити проблеми з безпекою мережі, брандмауер Windows Defender надає такі переваги:

– **Знижує ризик погроз безпеки мережі.** брандмауер Windows Defender зменшує поверхню атаки пристрою, надаючи додатковий рівень для моделі глибинного захисту. Зменшення поверхні атаки пристрою підвищує керованість та знижує ймовірність успішної атаки.

– **Захищає конфіденційні дані та інтелектуальну власність.** Завдяки інтеграції з IPsec брандмауер Windows Defender надає простий спосіб примусового забезпечення наскрізного мережного зв'язку з автентифікацією. Він надає масштабований багаторівневий доступ до довірених мережних ресурсів, допомагаючи забезпечити цілісність даних та за бажанням допомагаючи захистити конфіденційність даних.

– **Розширює цінність наявних інвестицій.** Так брандмауер Windows Defender є брандмауером на основі вузла, який входить в операційну систему, іншого обладнання або програмного забезпечення не потрібно. Брандмауер Windows Defender також призначений для доповнення існуючих рішень для безпеки мережі, що не стосуються Майкрософт, за допомогою задокументованих програмних інтерфейсів (API).

Захист від вірусів та погроз

Захист від вірусів та погроз призначений для виявлення та блокування нових і виникаючих загроз. Завдяки хмарному та машинному навчанню антивірусна програма Microsoft Defender допоможе зупинити атаки в режимі реального часу.

– Автоматична служба пісочниці.
– Моніторинг поведінки.
– Захист на основі хмари.
– Машинне навчання.
– Захист URL-адрес.

Безпека додатків Windows

Кіберзлочинні регулярно отримують доступ до цінних даних шляхом злому додатків. Це може бути атака шляхом впровадження коду, коли зловмисники вставляють шкідливий код, який може змінювати дані або навіть знищувати його. Можливо, у програмі налаштована неправильна конфігурація безпеки, тому зловмисники можуть відчинити двері. Крім того, важливі відомості про клієнтів та корпоративні дані можуть залишити конфіденційні дані недоступними. Windows захищає цінні дані за допомогою рівнів безпеки програм.

Заходи безпеки	Функції та можливості
Керування програмами у програмі Windows Defender	Керування програмами – це один з найбільш ефективних елементів керування безпекою, які запобігають запуску небажаного або шкідливого коду. Він переходить від моделі довіри додатків, де передбачається, що весь код є надійним, модель, в якій програми повинні отримати довіру для виконання.
Application Guard в Microsoft Defender	Application Guard використовує апаратну ізоляцію на основі мікросхем для ізоляції недовірених веб-сайтів та ненадійних Office-файлів, безперешкодного запуску ненадійних веб-сайтів та файлів в ізольованому контейнері на основі Hyper-V, окремо від операційної системи робочого столу, та гарантує, що все, що відбувається у контейнері, залишається ізольованим від робочого столу.
Пісочниця Windows	Пісочниця Windows надає компактне середовище робочих столів для безпечного запуску програм в ізоляції. Програмне забезпечення, встановлене всередині середовища Пісочниці Windows, ізольовано від решти системи і працює незалежно від головного комп'ютера. Пісочниця є тимчасовою. При її закритті все програмне забезпечення, що знаходиться в ній, всі файли і дані про стан видаляються. При кожному відкритті програми ви отримуєте новий екземпляр пісочниці.
Безпека електронної пошти	Завдяки Windows безпеки електронної пошти S/MIME користувачі можуть шифрувати вихідні повідомлення та вкладення, щоб їх могли читати лише отримувачі з цифровою ідентифікацією (ідентифікатором), також званим сертифікатом. Користувачі можуть цифрово підписати повідомлення, яке перевіряє посвідчення відправника та гарантує, що повідомлення не було змінено.

Фільтр SmartScreen у Microsoft Defender	Фільтр SmartScreen у Microsoft Defender захищає від фішингових та шкідливих веб-сайтів та програм, а також від скачування потенційно небезпечних файлів.

Управління програмами у Windows Defender та захист цілісності коду на основі віртуалізації

Windows 10 включає набір технологій обладнання та ОС, які при спільному налаштуванні дозволяють підприємствам «блокувати» Windows 10 системи, щоб вони більшою мірою поводяться як мобільні пристрої. У цій конфігурації Захисник Windows application Control (WDAC) використовується для обмеження пристроїв на запуск лише затверджених програм, в той час як операційна система захищена від атак на пам'ять ядра за допомогою цілісності коду, захищеного гіпервізором (HVCI).

Політики WDAC та HVCI – це потужні засоби захисту, які можна використовувати окремо. Однак, якщо ці дві технології налаштовані для спільної роботи, вони мають надійний захист для Windows 10 пристроїв.

Використання Захисник Windows керування програмами для обмеження пристроїв лише авторизованими програмами має такі переваги в порівнянні з іншими рішеннями:

1. Політика WDAC застосовується до самого ядру Windows, і вона набирає чинності на ранніх етапах послідовності завантаження перед виконанням багатьох інших кодів ОС і до запуску традиційних антивірусних рішень.

2. WDAC дозволяє задати політику керування додатками для коду, який виконується в режимі користувача, драйверів обладнання та програмного забезпечення в режимі ядра, а також навіть коду, який виконується як частина Windows.

3. Клієнти можуть захистити політику WDAC навіть від незаконної зміни локального адміністратора, підписавши політику цифровим підписом. Для зміни підписаної політики потрібні права адміністратора та доступ до процесу цифрового підписування організації. Через це зловмиснику, зокрема користувачеві, якому вдалося отримати права адміністратора, важко змінити політику WDAC.

4. Ви можете захистити весь механізм примусового застосування WDAC за допомогою HVCI. Навіть якщо вразливість існує у коді режиму ядра, HVCI значно знижує ймовірність того, що зловмисник може успішно використовувати її. Це важливо, тому що зловмисник, який скомпрометує ядро, зазвичай може відключити більшість системних захисту, включаючи ті, які застосовуються WDAC або будь-яким іншим рішенням для керування програмами.

Керування програмами для Windows

Щодня створюються тисячі нових шкідливих файлів, тому використання традиційних методів, таких як антивірусні програми-визначення шкідливого коду на основі сигнатур з його подальшим усуненням-не забезпечує достатнього захисту від нових атак.

У більшості організацій інформація є найбільш цінним ресурсом, і дуже важливо переконатися, що доступом до цієї інформації мають лише затверджені користувачі. Однак, якщо користувач запускає процес, цей процес має той самий рівень доступу до даних, що й у користувача. В результаті конфіденційні відомості можуть бути легко видалені або передані за межі організації, якщо користувач навмисно або випадково запускає шкідливе ПЗ.

Керування програмами може допомогти усунути такі загрози безпеці, обмеживши програми, які можуть запускати користувачі, і код, що виконується в System Core (ядро). Політики керування програмами також можуть блокувати непідписані скрипти та msis та обмежувати Windows PowerShell для виконання в обмеженому мовному режимі.

Управління додатками – це ключова лінія захисту для захисту підприємств з урахуванням сучасних загроз, яка має перевагу в порівнянні з традиційними антивірусними рішеннями. Зокрема, керування додатками переходить від моделі довіри додатків, де всі додатки вважаються надійними, тоді як додатки повинні отримати довіру для запуску. Багато організацій, такі як Australian Signals Directorate, розуміють важливість управління програмами і часто називають управління програмами одним з найбільш ефективних способів усунення загрози виконуваних файлових шкідливих програм (.exe,.dll і т.д.).

Windows 10 і Windows 11 включають дві технології, які можна використовувати для керування програмами в залежності від конкретних сценаріїв та вимог вашої організації:

– Захисник Windows керування програмами (WDAC).
– AppLocker.

Огляд Application Guard у Microsoft Defender

Application Guard у Microsoft Defender (Application Guard) призначена для запобігання старим і новим атакам, щоб підтримувати продуктивність співробітників. За допомогою нашого унікального підходу до ізоляції обладнання наша мета полягає в тому, щоб знищити книгу відтворення, що використовується зловмисниками через те, що сучасні методи атаки застаріли.

Для Microsoft Edge application Guard допомагає ізолювати сайти, які не захищені корпоративними даними, захищаючи вашу компанію під час перегляду співробітниками Інтернету. Як адміністратор підприємства, ви визначаєте, які веб-сайти, хмарні ресурси та внутрішні мережі можна вважати довіреними. Усі елементи, які відсутні у списку, розцінюються як ненадійні. Якщо працівник відправляється на непорушний сайт через Microsoft Edge або Internet Explorer, Microsoft Edge відкриває сайт в ізольованому контейнері з Hyper-V увімкненою підтримкою.

Для Microsoft Office application Guard допомагає запобігти доступу до довірених ресурсів файлів Word, PowerPoint Excel і Excel. Application Guard відкриває ненав'язані файли в ізольованому Hyper-V із включеною підтримкою. Ізольований контейнер Hyper-V окремо від хост-операційної системи. Це ізолювання контейнера означає, що якщо непорушений сайт чи файл виявиться шкідливим, хост-пристрій захищений, а зловмисник не може отримати дані

підприємства. Ця концепція передбачає роботу ізольованого контейнера в анонімному режимі, тому зловмисник зможе отримати корпоративні облікові дані вашого співробітника.

Пісочниця Windows

Пісочниця Windows надає компактне середовище робочих столів для безпечного запуску програм в ізоляції. Програмне забезпечення, встановлене всередині Пісочниці Windows, ізольовано від решти системи і працює незалежно від головного комп'ютера.

Пісочниця є тимчасовою. При її закритті все програмне забезпечення, що знаходиться в ній, всі файли і дані про стан видаляються. При кожному відкритті програми ви отримуєте новий екземпляр пісочниці. Зверніть увагу, що починаючи з Windows 11 (складання 22509) ваші дані будуть зберігатися під час перезапуску, ініційованого з віртуалізованого середовища. Це зручно для встановлення програм, яким потрібне перезавантаження ОС.

Програмне забезпечення та програми, встановлені на головному комп'ютері, не є безпосередньо доступними у пісочниці. Якщо в середовищі Пісочниці Windows потрібні певні програми, їх необхідно явно встановити в цьому середовищі.

Пісочниця Windows має такі властивості:

– Це частина Windows: все, що потрібно для цієї функції, входить до операційних систем Windows 10 Pro та Windows 10 Корпоративна. Немає необхідності завантажувати VHD.

– Чиста система: під час кожного запуску Пісочниці Windows створюється новий екземпляр Windows.

– Одноразовість: на пристрої не зберігаються жодні дані. Коли користувач закриває цю програму, всі дані видаляються.

– Безпека: для ізоляції ядра використовується апаратна віртуалізація. Гіпервізор Майкрософт виконує окреме ядро, яке відокремлює Пісочницю Windows від комп'ютера.

– Ефективність: використовується інтегрований планувальник ядра, інтелектуальне керування пам'яттю та віртуальний ГП.

Налаштування S/MIME для Windows

S/MIME забезпечує додатковий рівень безпеки для пошти, що надсилається та отримує обліковий запис Exchange ActiveSync (EAS). S/MIME дозволяє користувачам шифрувати вихідні повідомлення та вкладення, щоб тільки передбачувані одержувачі, які мають цифрову ідентифікацію (ID), також відому як сертифікат, могли їх читати. Користувачі можуть створювати цифрові підписи для повідомлень, що забезпечує одержувачам можливість перевірити посвідчення відправника та переконатися в тому, що повідомлення не було несанкціоновано змінено.

Шифрування повідомлень

Користувачі можуть надсилати зашифровані повідомлення контактам у своїй організації та за її межами за наявності сертифікатів шифрування. Однак

користувачі, які використовують програму Mail for Windows, можуть зчитувати зашифровані повідомлення лише в тому випадку, якщо повідомлення отримано в обліковому записі Exchange і у них є відповідні ключі розшифровки.

Зашифровані повідомлення можуть прочитати лише отримувачі, які мають сертифікат. При спробі надіслати зашифроване повідомлення одержувачам, чий сертифікат шифрування недоступний, програма перед відправкою запропонує видалити одержувачам.

Цифрові підписи

Цифровий підпис повідомлення показує одержувачу, що повідомлення не було піддано несанкціонованій зміні та перевіряє посвідчення відправника. Отримувачі можуть перевірити цифровий підпис лише за умови використання клієнта електронної пошти з підтримкою S/MIME.

Шифрування та підписання окремих повідомлень

1. Під час створення повідомлення виберіть вкладку стрічки Параметри. На телефоні можна отримати доступ до параметрів, натиснувши багатокрапку (...).

2. Щоб підписати це повідомлення за допомогою цифрового підпису або зашифрувати його, використовуйте піктограми Підписати та Шифрувати відповідно.

Читання підписаних або зашифрованих повідомлень

Коли ви отримуєте зашифроване повідомлення, поштова програма перевіряє, чи є на вашому комп'ютері сертифікат. Якщо сертифікат доступний, під час відкриття повідомлення буде розшифровано. Якщо сертифікат зберігається на смарт-карті, вам буде запропоновано вставити смарт-картку, щоб прочитати повідомлення. Для доступу до сертифіката на смарт-картці також може знадобитися ПІН-код.

Встановлення сертифікатів із отриманого повідомлення

При отриманні підписаного повідомлення ел. пошти програма надає можливість встановлення на пристрій відповідного сертифіката шифрування, якщо такий сертифікат доступний. Цей сертифікат надалі можна використовувати для надсилання зашифрованої електронної пошти цій людині.

1. Відкрийте підписане повідомлення.

2. Торкніться піктограми цифрового підпису в області читання або натисніть.

3. Торкніться Встановити.

Windows посвідчення та конфіденційності

Зловмисники щодня запускають мільйони атак із паролями. Слабкі паролі, розпилення паролів та фішинг є точкою входу для багатьох атак. Знаючи, що потрібний користувач має доступ до правильного пристрою та потрібні дані, дуже важливо забезпечити безпеку та безпеку вашого бізнесу, сім'ї та себе. Windows Hello, Windows Hello для бізнесу та Credential Guard дозволяють клієнтам перейти на багатофакторну автентифікацію без пароля (MFA). MFA може знизити ризик компрометації в організаціях.

Можливості безпеки	Опис
Захист посвідчення користувача за допомогою Windows Hello	Windows Hello та Windows Hello для бізнесу замінити автентифікацію на основі пароля більш надійною моделлю автентифікації для входу на пристрій за допомогою секретного коду (ПІН-коду) або іншої біометричної автентифікації. Ця автентифікація на основі PIN-коду або біометричних даних дійсна лише на пристрої, на якому вона зареєстрована, і не може використовуватися на іншому пристрої. Додаткові відомості: Windows Hello для бізнесу
Credential Guard у Windows Defender та Remote Credential Guard	Credential Guard у Windows Defender допомагає захистити системи від методів крадіжки облікових даних (pass-the-hash або pass-the-ticket), а також допомагає запобігти доступу шкідливих програм до секретів системи, навіть якщо процес виконується з правами адміністратора. Захисник Windows Remote Credential Guard допомагає захистити облікові дані через підключення до віддаленого робочого стола шляхом перенаправлення запитів Kerberos назад на пристрій, що запитує підключення. Він також дає можливість єдиного входу для сеансів віддаленого робочого столу. Додаткові відомості: захист похідних облікових даних домену за допомогою програми Credential Guard у Захиснику Windows та захист облікових даних віддаленого робочого стола за допомогою Windows Remote Credential Guard
Альянс FIDO	Протоколи, визначені в Fast Identity Online (FIDO), стають відкритим стандартом для забезпечення надійної автентифікації, яка допомагає запобігти фішингу, а також зрозумілі і з урахуванням конфіденційності. Windows 11 підтримує вхід пристрою за допомогою ключів безпеки FIDO 2, а також Microsoft Edge або іншими сучасними браузерами підтримує використання захищених облікових даних на основі FIDO для захисту облікових записів користувачів. Докладніше про FIDO Alliance.

Microsoft Authenticator	Microsoft Authenticator є ідеальним компаньйоном для забезпечення безпеки за допомогою Windows 11. Це дозволяє легко і безпечно виконувати входи для всіх облікових записів в Інтернеті за допомогою багатофакторної автентифікації, входу на телефон без пароля або автозаповнення паролів. Крім того, у вас є додаткові параметри керування обліковими записами корпорації Майкрософт для особистих, робочих або навчальних облікових записів. Microsoft Authenticator можна використовувати для налаштування багатофакторної автентифікації для користувачів. Додаткові відомості: увімкнення входу без пароля за допомогою програми Microsoft Authenticator.
Смарт-картки	Смарт-картки – це стійкі до незаконного злому переносні пристрої зберігання, які можуть підвищити безпеку завдань у Windows, таких як автентифікація клієнтів, код підписування, захист електронної пошти та вхід за допомогою облікових записів Windows домену. Додаткові відомості про смарт-картки.
Контроль доступу	Керування доступом – це процес авторизації користувачів, груп та комп'ютерів для доступу до об'єктів та ресурсів у мережі або комп'ютері. Комп'ютери можуть керувати використанням системних та мережевих ресурсів за допомогою взаємопов'язаних механізмів автентифікації та авторизації. Додаткова інформація: контроль доступу.

Windows Hello для бізнесу

У Windows 10 Windows Hello для бізнесу замінює паролі суворою двофакторною автентифікацією на пристроях. У процесі автентифікації використовується новий тип облікових даних користувача, прив'язаних до пристрою, включаючи біометричні дані або ПІН-код.

Вхід із використанням біометричних даних

Windows Hello забезпечує надійну комплексну біометричну автентифікацію на основі розпізнавання облич або відбитків пальців. У Windows Hello використовується поєднання з особливих інфрачервоних (ІЧ)-камер та програмного забезпечення, що підвищує точність та захищає від спуфінгу. Провідні виробники обладнання постачають пристрої із вбудованими камерами, сумісними із Windows Hello. Обладнання для читання відбитків пальців можна використовувати або додавати на пристрої, на яких його немає. На пристроях, які підтримують Windows Hello, простий біометричний жест розблокує облікові дані користувачів.

– **Розпізнавання особи**. Це тип біометричної автентифікації, коли використовуються спеціальні камери, що зчитують дані в ІЧ-діапазоні, що дозволяє надійно відрізнити фотографію або відскановане зображення від живої

людини. Деякі виробники постачають зовнішні камери, в які вбудована така можливість, і більшість виробників ноутбуків також вбудовують цю функцію у свої пристрої.

– **Розпізнавання відбитків пальців**. Це тип біометричної автентифікації, коли використовується ємнісний датчик, скануючий відбитки пальців. Сканери відбитків пальців були доступні для комп'ютерів Windows протягом багатьох років, але поточне покоління датчиків є більш надійним і менш схильні до помилок. Більшість існуючих засобів читання відбитків пальців працюють Windows 10 і Windows 11, незалежно від того, чи вони зовнішні або інтегровані в ноутбуки або USB-клавіатури.

Біометричні дані, що використовуються для реалізації Windows Hello, надійно зберігаються у Windows лише на локальному пристрої. Біометричні дані не переміщуються та ніколи не відправляються на зовнішні пристрої або сервери. Так, Windows Hello дані біометричної ідентифікації зберігаються тільки на пристрої, немає єдиної точки збору, яку зловмисник може скомпрометувати для крадіжки біометричних даних. Для отримання додаткових відомостей про біометричну автентифікацію з Windows Hello для бізнесу див. Windows Hello біометричних даних на підприємстві.

Захист від крадіжки облікових даних у Windows

У цьому розділі пояснюється, як відбуваються атаки з крадіжкою облікових даних, а також стратегії та засоби протидії, які можна реалізувати для їх усунення на наступних етапах безпеки:

– Визначення ресурсомістких ресурсів із високою цінністю.
– Захист від відомих та невідомих погроз.
– Виявлення атак pass-the-hash та пов'язаних з ними атак.
– Реагування на підозрілі дії.
– Відновлення після пролому.

Атаки, які викрадають облікові дані

Дізнайтеся про різні типи атак, які використовуються для крадіжки облікових даних, і про фактори, які можуть призвести до ризику вашої організації. До типів атак належать:

– Передача ґешу.
– Kerberos передає квиток.
– Квиток Kerberos Golden Ticket та silver.
– Клавіатурні шпигуни.
– Сучасна дошка.

Стратегії захисту облікових даних

Ця частина посібника допоможе вам зрозуміти налаштування зловмисника з вказівкою того, як розставити пріоритети для високопріоритетних облікових записів та комп'ютерів. Ви дізнаєтесь, як створити архітектуру захисту від крадіжки облікових даних:

– Створення моделі зберігання для привілеїв облікового запису.
– Посилення захисту та обмеження адміністративних вузлів.
– Переконайтеся, що реалізовані конфігурації безпеки та рекомендації.

Технічні контрзаходи для крадіжки облікових даних

Цілі та очікувані результати розглядаються для кожного з цих лічильників:

– Використання Windows 10 Credential Guard.

– Обмеження та захист облікових записів домену з високим рівнем привілеїв.

– Обмеження та захист локальних облікових записів із правами адміністратора.

– Обмеження вхідного мережевого трафіку.

Також розглядаються багато інших контрзаходів, такі як використання Microsoft Passport та Windows Hello або багатофакторна автентифікація.

Виявлення атак з обліковими даними

У цих розділах описано, як виявити використання вкрадених облікових даних і як збирати події комп'ютера для виявлення крадіжки облікових даних.

Реагування на підозрілі дії

Ознайомтеся з рекомендаціями корпорації Майкрософт щодо реагування на інциденти, включаючи відновлення контролю скомпрометованих облікових записів, вивчення атак та відновлення пролому.

Захист витягнутих облікових даних домену за допомогою Credential Guard у Захиснику Windows

Вперше компонент Credential Guard у Windows Defender з'явився в Windows 10 Корпоративна та Windows Server 2016. Для захисту секретів він використовує засіб забезпечення безпеки на основі віртуалізації, щоб тільки привілейоване системне ПЗ могло отримувати доступ до цих даних. Несанкціонований доступ до секретів може призвести до атак, спрямованих на крадіжку облікових даних, наприклад Pass-the-Hash або Pass-The-Ticket. Credential Guard у Захиснику Windows запобігає цим атакам, захищаючи ґеш-коди паролів NTLM, квитки Kerberos Ticket Granting та облікові дані, що зберігаються в додатках як облікові дані домену.

Credential Guard у Windows Defender забезпечує перелічені нижче функції та рішення:

– **Апаратний захист** У NTLM, Kerberos та диспетчері облікових даних для захисту облікових даних використовуються функції забезпечення безпеки платформи, включаючи безпечне завантаження та віртуалізацію.

– **Засіб забезпечення безпеки на основі віртуалізації**. Облікові дані, витягнуті з Windows NTLM і Kerberos, та інші секрети виконуються в захищеному середовищі, яке ізольовано від операційної системи, що використовується.

– **Покращений захист від цілеспрямованих стійких загроз** Якщо для захисту облікових даних домену диспетчера облікових даних, а також облікових даних, вилучених з NTLM і Kerberos, використовується за допомогою засобу безпеки на основі віртуалізації, блокуються методи та засоби крадіжок облікових даних, які використовуються в багатьох цілеспрямованих атаках. Шкідливі програми, що працюють в операційній системі з правами адміністратора, не можуть отримати доступ до секретів, захищених за допомогою засобу безпеки

на основі віртуалізації. Хоча Credential Guard у Windows Defender є потужним засобом усунення загроз, постійні атаки збереженої загрози, швидше за все, будуть перемикання на нові методи атак, і вам також слід впровадити інші стратегії безпеки та архітектури.

Політика технічної підтримки для втрачених або забутих паролів

Облікові записи Майкрософт, операційна система Windows та інші продукти Microsoft містять паролі для захисту інформації. У цій статті наведено деякі параметри, які можна використовувати для скидання або відновлення пароля, якщо ви забули його. Якщо ці параметри не працюють, інженери служби підтримки Майкрософт не можуть допомогти вам отримати або обійти втрачений або забутий пароль.

Скидання пароля для облікового запису домену

Якщо ви втратите або забудете пароль для облікового запису домену, зверніться до IT-адміністратора або служби технічної підтримки. Щоб отримати додаткові відомості, див. Зміна або скидання пароля Windows.

Скидання пароля для облікового запису Майкрософт

Якщо ви втратите або забудете пароль для облікового запису Майкрософт, використовуйте майстер відновлення облікового запису.

Цей майстер просить ваші перевірки безпеки. Якщо ви забули свої перевірки безпеки або більше не маєте до них доступу, виберіть, що я **їх більше не має**. Після вибору цього параметра заповніть форму команди облікового запису Майкрософт. Вкажіть якнайбільше відомостей у цій формі. Команда облікових записів Майкрософт перевіряє відомості, які ви надаєте, щоб визначити, чи є власником облікового запису. Це остаточне рішення. Корпорація Майкрософт не впливає на вибір команди.

Скидання пароля для локального облікового запису на пристрої Windows

Локальні облікові записи на пристрої включають обліковий запис адміністратора пристрою.

Скидання пароля BIOS обладнання

Якщо ви втратите або забудете пароль для BIOS обладнання пристрою, зверніться за допомогою та підтримкою до виробника пристрою. Якщо ви дійсно зверталися до виробника через Інтернет, обов'язково відвідайте веб-сайт виробника, а не веб-сайт стороннього виробника.

Скидання пароля для окремого файлу

Деякі програми дозволяють захистити окремі файли паролем. Якщо ви втратите або забудете такий пароль, ви можете використовувати цю програму тільки для скидання або відновлення. Інженери служби підтримки Майкрософт не можуть допомогти вам скинути, вийняти або обійти такі паролі.

Використання сторонніх засобів введення паролів

Деякі сторонні компанії мають можливість обійти паролі, які були застосовані до файлів та функцій, які використовуються програмами Майкрософт. З юридичних причин ми не можемо рекомендувати чи

підтримувати будь-яку з цих компаній. Якщо вам потрібна допомога в обході або скиданні пароля, ви можете знайти та звернутися за допомогою до третьої сторони. Однак ви використовуєте такі сторонні продукти та служби на свій ризик.

Огляд керування доступом

У цьому розділі для IT-фахівців описується керування доступом у Windows, яке є процесом авторизації користувачів, груп та комп'ютерів для доступу до об'єктів у мережі або на комп'ютері. Основними поняттями, які є управління доступом, є дозволи, володіння об'єктами, наслідування дозволів, права користувача та аудит об'єктів.

Опис компонента

Комп'ютери з підтримуваною версією Windows можуть керувати використанням системних та мережевих ресурсів за допомогою взаємопов'язаних механізмів автентифікації та авторизації. Після автентифікації користувача операційна система Windows використовує вбудовані технології авторизації та контролю доступу для реалізації другого етапу захисту ресурсів: визначення того, чи користувач, що пройшов перевірку автентичності, правильні дозволи на доступ до ресурсу.

Загальні ресурси доступні користувачам та групам, крім власника ресурсу, та їх необхідно захистити від несанкціонованого використання. У моделі керування доступом користувачі та групи (також звані суб'єктами безпеки) представлені унікальними ідентифікаторами безпеки (SID). Їм призначаються права та дозволи, які повідомляють операційній системі, що може робити кожен користувач та група. Кожен ресурс має власника, який надає дозволи суб'єктам безпеки. Під час перевірки контролю доступу ці дозволи перевіряються, щоб визначити, які суб'єкти безпеки можуть отримати доступ до ресурсу та як вони можуть отримати доступ до нього.

Суб'єкти безпеки виконують дії (включаючи читання, запис, зміну або повний контроль) з об'єктами. До об'єктів належать файли, папки, принтери, розділи реєстру та доменні служби Active Directory (AD DS). Загальні ресурси використовують списки керування доступом (ACL) для призначення дозволів. Це дозволяє диспетчерам ресурсів застосовувати керування доступом такими способами:

– Заборона доступу неавторизованих користувачів та груп.

– Встановлення чітко визначених обмежень на доступ, наданий авторизованим користувачам та групам.

Власники об'єктів зазвичай надають дозволи групам безпеки, а не окремим користувачам. Користувачі та комп'ютери, додані до існуючих груп, передбачають дозволи цієї групи. Якщо об'єкт (наприклад, папка) може містити інші об'єкти (наприклад, вкладені папки та файли), він називається контейнером. В ієрархії об'єктів зв'язок між контейнером та його вмістом виражається посиланням на контейнер як батьківський. Об'єкт у контейнері називається дочірнім, і дочірній елемент успадковує параметри керування доступом

батьківського елемента. Власники об'єктів часто визначають дозвіл для об'єктів контейнерів, а не окремих дочірніх об'єктів, щоб спростити керування доступом.

Цей набір містить:

- Огляд динамічного контролю доступу.
- Ідентифікатори безпеки.
- Суб'єкти безпеки:
  - Локальні облікові записи.
  - Облікові записи Active Directory.
  - Облікові записи Майкрософт.
  - Облікові записи служби.
  - Групи безпеки Active Directory.

Практичне застосування

Адміністратори, які використовують підтримувану версію Windows, можуть уточнити програму та керування доступом до об'єктів та суб'єктів, щоб забезпечити наступну безпеку:

– Захистіть більшу кількість та різноманітність мережних ресурсів від неправильного використання.

– Підготовка користувачів до доступу до ресурсів відповідно до політик організації та вимог їх завдань.

– Надання користувачам доступу до ресурсів із різних пристроїв у різних розташуваннях.

– Регулярно оновлюйте доступ користувачів до ресурсів у міру зміни політик організації чи зміни завдань користувачів.

– З урахуванням зростаючого числа сценаріїв використання (таких як доступ з віддалених розташування або швидко розширюється безліч пристроїв, таких як планшетні комп'ютери і мобільні телефони).

– Виявляйте та усувайте проблеми з доступом, коли допустимі користувачі не можуть отримати доступ до ресурсів, необхідних для виконання своїх завдань.

Дозволи

Дозволи визначають тип доступу, який надається користувачеві або групі для об'єкта або властивості об'єкта. Наприклад, групі Finance можна надати дозволи на читання та запис файлу з ім'ям Payroll.dat.

За допомогою інтерфейсу керування доступом можна встановити дозволи NTFS для таких об'єктів, як файли, об'єкти Active Directory, об'єкти реєстру або системні об'єкти, такі як процеси. Дозволи можуть бути надані будь-якому користувачеві, групі чи комп'ютеру. Рекомендується призначати дозволи групам, оскільки це підвищує продуктивність системи під час перевірки доступу до об'єкта.

Для будь-якого об'єкта можна надати дозволи на:

– Групи, користувачі та інші об'єкти з ідентифікаторами безпеки у домені.

– Групи та користувачі в цьому домені та всі довірені домени.

– Локальні групи та користувачі на комп'ютері, де знаходиться об'єкт.

Дозволи, підключені до об'єкта, залежать від типу об'єкта. Наприклад, дозволи, які можна вкласти у файл, відрізняються від дозволів, які можна

вкласти

до розділу реєстру. Однак, деякі дозволи є спільними для більшості типів об'єктів. Нижче наведено поширені дозволи.

– Прочитайте.
– Змінити.
– Зміна власника.
– Видалити.

Під час встановлення дозволів вказується рівень доступу для груп та користувачів. Наприклад, можна дозволити одному користувачу зчитувати вміст файлу, дозволити іншому користувачеві вносити зміни до файлу та заборонити іншим користувачам доступ до файлу. Ви можете задати аналогічні дозволи на принтерах, щоб певні користувачі могли налаштовувати принтер, а інші користувачі могли лише друкувати.

Якщо потрібно змінити дозволи для файлу, можна запустити провідник Windows, клацнути правою кнопкою миші ім'я файлу та натиснути кнопку «**Властивості"**. На **вкладці «** Безпека» можна змінити дозволи для файлу. Щоб отримати додаткові відомості, див. Управління роздільною здатністю.

Володіння об'єктами

Власник призначається об'єкту під час його створення. За замовчуванням власником об'єкта є власник. Незалежно від дозволу об'єкта, власник об'єкта завжди може змінити дозволи. Щоб отримати додаткові відомості, див. Управління володінням об'єктом.

Наслідування дозволів

Спадкування дозволяє адміністраторам легко призначати дозволи та керувати ними. Ця функція автоматично призводить до того, що об'єкти в контейнері успадковують всі дозволи цього контейнера. Наприклад, файли в папці успадковують роздільну здатність папки. Наслідуються лише дозволи, позначені для наслідування.

Права користувача

Права користувача надають певні привілеї та права входу користувачам та групам у обчислювальному середовищі. Адміністратори можуть призначати певні права на облікові записи груп або окремі облікові записи користувачів. Ці права дозволяють користувачам виконувати певні дії, такі як вхід до системи в інтерактивному режимі або резервне копіювання файлів та каталогів.

Права користувача відрізняються від дозволів, оскільки права користувача застосовуються до облікових записів користувачів, а дозволи пов'язані з об'єктами. Хоча права користувачів можуть застосовуватися до окремих облікових записів користувачів, права користувачів найкраще адмініструвати на основі облікового запису групи. У інтерфейсі керування доступом користувача не підтримується надання прав користувача. Однак призначення прав користувача можна адмініструвати за допомогою **локальних параметрів безпеки**.

Для отримання додаткових відомостей про права користувачів див. розділ «Призначення прав користувача".

Аудит об'єктів

З правами адміністратора можна виконувати аудит успішного чи невдалого доступу користувачів до об'єктів. Ви можете вибрати, який об'єкт має доступ до аудиту, за допомогою інтерфейсу управління доступом, але спочатку необхідно включити політику **** аудиту, вибравши «Аудит доступу до об'єкта» в розділі «Локальні політики» в локальних параметрах безпеки. Потім ці події, пов'язані з безпекою, можна переглянути в журналі безпеки Перегляд подій.

Технічний довідник смарт-карт

Що таке смарт-картки?

Смарт-картки – це стійкі до незаконного злому переносні пристрої зберігання, які можуть підвищити безпеку таких завдань, як перевірка справжності клієнтів, підписування коду, захист електронної пошти та вхід за допомогою облікового запису домену Windows.

Смарт-картки надають:

– Захищене від незаконної зміни сховище для захисту закритих ключів та інших форм персональних даних.

– Ізоляція критично важливих для безпеки обчислень, які включають автентифікацію, цифрові підписи та обмін ключами з інших частин комп'ютера. Ці обчислення виконуються на смарт-картці.

– Перенесення облікових даних та іншої конфіденційної інформації між комп'ютерами на роботі, вдома або в дорозі.

Смарт-картки можна використовувати лише для входу до облікових записів домену, а не для локальних облікових записів. При використанні пароля для інтерактивного входу в обліковий запис домену Windows використовує протокол Kerberos версії 5 (v5) для автентифікації. Якщо ви використовуєте смарт-карту, операційна система використовує автентифікацію Kerberos версії 5 з сертифікатами X.509 v3.

Віртуальні смарт-картки з'явилися у Windows Server 2012 та Windows 8, щоб усунути необхідність у фізичній смарт-картці, засобі читання смарт-карток та пов'язаному адмініструванні цього обладнання. Відомості про віртуальні смарт-карти див. у розділі «Загальні відомості про віртуальні смарт-картки".

Windows та хмарна безпека

Сучасні співробітники мають більшу свободу і мобільність, ніж будь-коли раніше. Зі збільшенням впровадження корпоративної хмари, збільшенням використання особистих додатків та збільшенням використання сторонніх додатків ризик уразливості даних є найвищим. Увімкнення Zero-Trust захисту Windows 11 працює з хмарними службами Майкрософт. Windows та хмарні служби допомагають організаціям посилити інфраструктуру безпеки в декількох хмарах, захистити гібридні хмарні робочі навантаження та захистити конфіденційну інформацію, контролюючи доступ та усуваючи загрози.

Windows 11 включає хмарні служби, перелічені в наступній таблиці:

Тип служби	Опис
Управління мобільними пристроями (MDM) та Microsoft Endpoint Manager	Windows 11 підтримує MDM, рішення для управління підприємством, допомагаючи керувати політиками безпеки та бізнес-додатками вашої організації. MDM дозволяє групі безпеки керувати пристроями, не порушуючи конфіденційність користувачів на власних пристроях. Сервери сторонніх розробників можна використовувати для керування Windows 11 за допомогою стандартних галузевих протоколів.
Обліковий запис Майкрософт	Коли користувачі додають обліковий запис Microsoft у Windows 11, вони можуть переносити Windows, Microsoft Edge, Xbox, вибрані веб-сторінки, файли, фотографії та ін. на своїх пристроях. Обліковий запис Microsoft дозволяє користувачам керувати всім в одному місці. Вони можуть зберігати вкладки у своїх підписках та журналі замовлень, впорядковувати цифрове життя сім'ї, оновлювати параметри конфіденційності та безпеки, відстежувати працездатність та безпеку своїх пристроїв та навіть отримувати винагороди.
OneDrive	OneDrive – це інтернет-сховище для файлів, фотографій та даних. OneDrive забезпечує додаткову безпеку, резервне копіювання та відновлення важливих файлів та фотографій. За допомогою особистих та бізнес-рішень користувачі можуть використовувати OneDrive для зберігання та захисту файлів у хмарі, дозволяючи користувачам працювати на ноутбуках, настільних комп'ютерах та мобільних пристроях. Якщо пристрій втрачено або викрадено, користувачі можуть швидко відновити всі важливі файли, фотографії та дані. Особистий OneDrive також забезпечує захист найбільш конфіденційних файлів без втрати зручності доступу будь-де. Файли захищені за допомогою автентифікації, але легко доступні користувачам на їхніх пристроях. Дізнайтеся, як налаштувати Особистий сейф. У разі атаки програми-шантажиста OneDrive можливість відновлення. Якщо ви налаштуєте резервне копіювання в OneDrive, у вас буде більше можливостей для усунення та відновлення після атаки програми-шантажиста.

Доступ до Azure Active Directory	Microsoft Azure Active Directory (Azure AD) – це повне хмарне рішення для керування посвідченнями та каталогами, забезпечення доступу до програм та захисту посвідчень від загроз безпеки. Використовуючи Azure AD, ви можете керувати посвідченнями та захищати посвідчення для співробітників, партнерів та клієнтів для доступу до потрібних програм та служб. Windows 11 з Azure Active Directory забезпечує безпечний доступ, керування посвідченнями та єдиний вхід до програм та служб з будь-якого місця.

Управління мобільними пристроями

Дізнайтеся, як реєструвати пристрої Windows та керувати політиками безпеки компанії та бізнес-програмами.

Azure Active Directory

Захищений адаптивний доступ

Захистіть доступ до ресурсів і даних завдяки надійній автентифікації та політиці адаптивного доступу на основі ризиків, не впливаючи на роботу користувачів.

Зручна взаємодія з користувачем

Забезпечте простий і швидкий вхід у своє багатохмарне середовище, щоб підвищити продуктивність користувачів, а також зменшити витрати часу на керування паролями.

Комплексне керування ідентичностями

Керуйте ідентичностями й забезпечуйте доступ до локальних і хмарних програм у центральному розташуванні, щоб покращити видимість та контроль.

Спрощене керування ідентичностями

Ефективно керуйте доступом до програм і даних усіх користувачів та адміністраторів за допомогою автоматичних засобів керування ідентичностями, щоб гарантувати доступ лише авторизованим користувачам.

Облікові записи Майкрософт

Сайти, служби, властивості та комп'ютери Майкрософт, які працюють у Windows 10, можуть використовувати обліковий запис Майкрософт як засіб ідентифікації користувача. Раніше обліковий запис Майкрософт називався Windows Live ID. Він містить секрети, що визначаються користувачем, і складається з унікальної адреси електронної пошти та пароля.

Коли користувач входить за допомогою облікового запису Майкрософт, пристрій підключено до служб хмар. Багато параметрів, переваг та програм користувача можна спільно використовувати на різних пристроях.

Як працює обліковий запис Майкрософт

Обліковий запис Microsoft дозволяє користувачам входити на веб-сайти, які підтримують цю службу, за допомогою одного набору облікових даних.

Облікові дані користувачів перевіряються сервером автентифікації облікового запису Майкрософт, пов'язаним із веб-сайтом. Microsoft Store є прикладом зв'язку. Коли нові користувачі входять на веб-сайти, для яких можна використовувати облікові записи Майкрософт, вони надсилаються на найближчий сервер автентифікації, який запитує ім'я користувача та пароль. Windows використовує постачальник підтримки безпеки Schannel для відкриття підключення tls/SSL для цієї функції. Користувачі можуть використовувати диспетчер облікових даних для зберігання облікових даних.

Коли користувачі входять на веб-сайти, для яких дозволено використовувати обліковий запис Майкрософт, на своїх комп'ютерах встановлюється обмежений за часом файл cookie, який включає потрійний тег зашифрованого ідентифікатора DES. Цей зашифрований тег ідентифікатора був узгоджений між сервером автентифікації та веб-сайтом. Цей тег ідентифікатора надсилається на веб-сайт, і веб-сайт встановить ще один обмежений зашифрований HTTP-файл cookie на комп'ютері користувача. Якщо ці файли cookie дійсні, користувачам не потрібно вказати ім'я користувача та пароль. Якщо користувач активно виходить з облікового запису Microsoft, ці файли cookie видаляються.

Створення облікових записів Майкрософт

Щоб запобігти шахрайству, система Майкрософт перевіряє IP-адресу під час створення облікового запису користувачем. Користувач, який намагається створити кілька облікових записів Майкрософт з однаковою IP-адресою, зупиняється. Облікові записи Майкрософт не призначені для створення пакетів, наприклад, для групи користувачів домену у вашій організації.

Існує два способи створення облікового запису Майкрософт:

– **Використовуйте існуючу адресу електронної пошти**. Користувачі можуть використовувати дійсні адреси електронної пошти для реєстрації облікових записів корпорації Майкрософт. Служба перетворює адресу електронної пошти запитувача на обліковий запис Майкрософт. Користувачі також можуть вибирати свої особисті паролі.

– **Зареєструйтесь, щоб отримати адресу електронної пошти Майкрософт**. Користувачі можуть зареєструватися для отримання облікового запису електронної пошти за допомогою служб веб-пошти Майкрософт. Цей обліковий запис можна використовувати для входу на веб-сайти, які включені для використання облікових записів корпорації Майкрософт.

Захист інформації про обліковий запис Майкрософт

Облікові дані шифруються двічі. Перше шифрування ґрунтується на паролі облікового запису. Облікові дані шифруються знову під час їх надсилання через Інтернет. Збережені дані недоступні для інших служб Майкрософт або інших служб.

– **Необхідний надійний пароль**. Не можна використовувати порожні паролі. Щоб отримати додаткові відомості, див. розділ Як забезпечити безпеку та безпеку облікового запису Майкрософт.

– **Потрібне додаткове підтвердження особистості**. Перш ніж отримати доступ до інформації та параметрів профілю користувача на другому

підтримуваному комп'ютері Windows вперше, необхідно встановити довіру для цього пристрою, надавши додаткове підтвердження особи. Це можна зробити, надавши Windows код, який надсилається на номер мобільного телефону або дотримуючись інструкцій, надісланих на альтернативну адресу електронної пошти, вказану користувачем у параметрах облікового запису.

– **Усі дані профілю користувача шифруються на клієнті перед передачею в хмару**. За замовчуванням дані користувача не переміщуються бездротовою широкою мережею (WWAN), таким чином захищаючи дані профілю. Усі дані та параметри, що залишають пристрій, передаються через протокол TLS/SSL.

Відомості про безпеку облікового запису Майкрософт

Користувачі можуть додавати відомості про безпеку до облікових записів Майкрософт через інтерфейс **облікових записів** на комп'ютерах під керуванням підтримуваних версій Windows. Ця функція дозволяє користувачеві оновлювати інформацію про безпеку, надані під час створення облікових записів. Ці відомості про безпеку включають альтернативну адресу електронної пошти або номер телефону, тому якщо пароль скомпрометований або забутий, можна надіслати код перевірки для перевірки їхньої особи. Користувачі можуть використовувати свої облікові записи Майкрософт для зберігання корпоративних даних в особистому програмі OneDrive або поштовій програмі, тому власнику облікового запису безпечно зберігати ці відомості про безпеку в актуальному стані.

Обліковий запис Майкрософт для підприємства

Хоча обліковий запис Майкрософт призначений для обслуговування споживачів, ви можете знайти ситуації, коли користувачі домену можуть скористатися своїм особистим обліковим записом Майкрософт у вашій організації. У цьому списку описані деякі переваги.

– **Завантажте програми Microsoft Store**. Якщо ваше підприємство вирішить розповсюджувати програмне забезпечення через Microsoft Store, користувачі можуть використовувати свої облікові записи Майкрософт для завантаження та використання на п'яти пристроях з будь-якою версією Windows 10, Windows 8.1, Windows 8 або Windows RT.

– **Єдиний вхід**. Користувачі можуть використовувати облікові дані облікового запису Microsoft для входу на пристрої під керуванням Windows 10, Windows 8.1, Windows 8 або Windows RT. При цьому Windows працює з програмою Microsoft Store, щоб забезпечити для них можливості, що пройшли автентифікацію. Користувачі можуть зв'язати обліковий запис Майкрософт з обліковими даними для входу до програм або веб-сайтів Microsoft Store, щоб ці облікові дані переміщувалися на всіх пристроях із підтримуваними версіями.

– **Синхронізація персоналізованих параметрів**. Користувачі можуть зв'язати параметри операційної системи, які найчастіше використовуються, з обліковим записом Майкрософт. Ці параметри доступні щоразу, коли користувач входить з цим обліковим записом на будь-якому пристрої під керуванням підтримуваної версії Windows і підключений до хмари. Після входу

користувача пристрій автоматично намагається отримати параметри користувача з хмари та застосувати їх до пристрою.

– **Синхронізація програм**. Програми Microsoft Store можуть зберігати настройки користувача, щоб ці параметри були доступні для будь-якого пристрою. Як і у випадку з параметрами операційної системи, ці параметри програми для конкретних користувачів доступні при кожному вході користувача з тим же обліковим записом Майкрософт на будь-якому пристрої, на якому запущено підтримувану версію Windows і підключено до хмари. Після входу користувача цей пристрій автоматично завантажує настройки з хмари та застосовує їх під час встановлення програми.

– **Інтегровані служби соціальних мереж**. Контактні дані та статус друзів та партнерів користувачів автоматично залишаються актуальними на таких сайтах, як Hotmail, Outlook, Facebook, Twitter та LinkedIn. Користувачі також можуть отримувати доступ до фотографій, документів та інших файлів з таких сайтів, як OneDrive, Facebook та Flickr.

Керування обліковим записом Майкрософт у домені

Залежно від IT-моделей та бізнес-моделей, використання облікових записів Майкрософт у вашій організації може ускладнювати або надавати рішення. Перш ніж дозволити використання цих типів облікових записів в організації, слід враховувати такі рекомендації:

– Обмеження використання облікового запису Майкрософт.
– Налаштування підключених облікових записів.
– Підготовка облікових записів Майкрософт в організації.
– Аудит дій облікового запису.
– Виконання скидання пароля.
– Обмеження встановлення та використання додатків.

Обмеження використання облікового запису Майкрософт

Наступні параметри групової політики допомагають керувати використанням облікових записів Майкрософт в організації:

– Блокування автентифікації користувача облікового запису Майкрософт для всіх споживачів.
– Облікові записи: блокування облікових записів Майкрософт.

Блокування автентифікації користувача облікового запису Майкрософт для всіх споживачів

Цей параметр визначає, чи користувачі можуть надавати облікові записи Майкрософт для автентифікації для програм або служб.

Якщо цей параметр увімкнено, всі програми та служби на пристрої заборонено використовувати облікові записи Майкрософт для автентифікації. Це стосується як існуючих користувачів пристрою, так і нових користувачів, які можуть бути додані.

Однак будь-яка програма або служба, що вже пройшли автентифікацію користувача, не будуть порушені включенням цього параметра до закінчення терміну дії кеша автентифікації. Рекомендовано увімкнути цей параметр перед тим, як будь-який користувач увійде на пристрій, щоб запобігти появі кешованих маркерів.

Якщо цей параметр вимкнено або не налаштовано, програми та служби можуть використовувати облікові записи Майкрософт для автентифікації. Цей **параметр вимкнено за** замовчуванням.

Цей параметр не впливає на можливість входу користувачів на пристрої за допомогою облікових записів Майкрософт або надання облікових записів Майкрософт через браузер для перевірки автентичності за допомогою веб-застосунків.

Шлях до цього параметра: Конфігурація комп'ютера\Адміністративні шаблони\Компоненти Windows\обліковий запис Майкрософт.

Облікові записи: блокування облікових записів Майкрософт

Цей параметр забороняє використання програми «**Параметри** « для додавання облікового запису Майкрософт для автентифікації єдиного входу для служб Майкрософт та деяких фонових служб або використання облікового запису Майкрософт для єдиного входу до інших програм або служб.

Якщо цей параметр увімкнено, існує два варіанти5

– **Користувачі не можуть додавати облікові записи Майкрософт**. Існуючі підключені облікові записи, як і раніше, можуть входити на пристрій (і відображатися на екрані входу). Однак користувачі не можуть використовувати програму «**Параметри»** для додавання нових підключених облікових записів або підключення локальних облікових записів до облікових записів Майкрософт.

– **Користувачі не можуть додавати або виконувати вхід за допомогою облікових записів Майкрософт**. Користувачі не можуть додавати нові підключені облікові записи (або підключати локальні облікові записи до облікових записів корпорації Майкрософт) або використовувати існуючі підключені облікові записи за допомогою **параметрів**.

Цей параметр не впливає на додавання облікового запису Microsoft для автентифікації програми. Наприклад, якщо цей параметр увімкнено, користувач, як і раніше, може надати обліковий запис Майкрософт для автентифікації за допомогою програми **Пошта**, але користувач не може використовувати обліковий запис Майкрософт для автентифікації єдиного входу для інших програм або служб (іншими словами, користувачеві буде запропоновано пройти автентифікацію для інших програм або служб).

Цей параметр **не визначено** за замовчуванням.

Шлях до цього параметра: Конфігурація комп'ютера\Параметри Windows\Параметри безпеки\Локальні політики\Параметри безпеки.

Налаштування підключених облікових записів

Користувачі можуть підключити обліковий запис Майкрософт до свого облікового запису домену та синхронізувати установки та налаштування між ними. Це дозволяє користувачам переглядати той самий фон робочого стола, параметри програми, журнал браузера та вибране, а також інші параметри облікового запису Майкрософт на інших пристроях.

Користувачі можуть вимкнути обліковий запис Майкрософт від облікового запису домену в будь-який час таким чином: у **параметрах комп'ютера** торкніться або клацніть **Користувачі**, торкніться або натисніть кнопку «**Вимкнути** «, а потім натисніть кнопку «**Готово** «.

Підготовка облікових записів Майкрософт в організації

Облікові записи Майкрософт – це приватні облікові записи користувачів. Корпорація Майкрософт не надає жодних методів підготовки облікових записів Майкрософт для підприємства. Підприємства повинні використовувати облікові записи домену.

Аудит дій облікового запису

Оскільки облікові записи Майкрософт знаходяться в Інтернеті, Windows не має механізму аудиту їх використання, доки обліковий запис не буде пов'язаний з обліковим записом домену. Але цей зв'язок не обмежує користувача від вимкнення облікового запису або від'єднання від домену. Неможливо перевірити активність облікових записів, які не пов'язані з вашим доменом.

Виконання скидання пароля

Тільки власник облікового запису Microsoft може змінити пароль. Паролі можна змінити на порталі входу до облікового запису Майкрософт.

Обмеження встановлення та використання додатків

В організації можна налаштувати політики керування програмами для регулювання установки та використання програм для облікових записів Майкрософт. Для отримання додаткових відомостей див. AppLocker та упаковані програми та правила інсталятора упакованих програм AppLocker.

OneDrive

Допомагає користувачам в організації зберігати, синхронізувати та обмінюватися файлами в Microsoft 365.

Параметри для сім'ї

У розділі **Параметри для сім'ї** містяться посилання на параметри та подальша інформація для батьків щодо комп'ютера з Windows 10. Він не призначений для корпоративних чи бізнес-середовищ. У Windows 10 версії 1709 цей розділ можна приховати від користувачів комп'ютера. Цей параметр може бути корисним, якщо ви не бажаєте, щоб співробітники вашої організації могли бачити або мати доступ до цього розділу.

Основи безпеки Windows

Корпорація Майкрософт прагне постійно інвестувати у покращення процесу розробки програмного забезпечення, створення програмного забезпечення з високим рівнем безпеки та відповідність вимогам безпеки. Корпорація Майкрософт впроваджує рекомендації щодо безпеки та конфіденційності на ранніх етапах життєвого циклу всіх процесів розробки програмного забезпечення. Ми створимо безпеку з нуля для ефективного захисту у середовищі загроз.

Наша надійна основа безпеки використовує життєвий цикл розробки помилок (SDL) Майкрософт, підтримку стандартів та сертифікатів безпеки продуктів, а також підписування коду Azure. В результаті ми покращуємо безпеку, створивши програмне забезпечення з меншою кількістю дефектів та вразливостей, а не застосовуючи оновлення після виявлення вразливостей.

Додаткові відомості про основи безпеки див. у наступній таблиці:

Концепція	Опис
Перевірка FIPS 140-2	Публікація 140-2 федерального стандарту обробки інформації (FIPS) є стандартом державних організацій США. FIPS засновано на розділі 5131 в Акті 1996 року про структуру управління інформаційними технологіями. Він визначає мінімальні вимоги безпеки для криптографічних модулів в IT-продуктах. Корпорація Майкрософт активно виконує зобов'язання щодо забезпечення відповідності вимогам стандарту FIPS 140-2, перевіряючи криптографічні модулі з моменту його першого створення у 2001 році.
Загальні критерії сертифікації	Корпорація Майкрософт підтримує програму сертифікації загальних критеріїв, гарантує, що продукти включають функції та функції, необхідні для відповідних профілів захисту загальних критеріїв, та завершує сертифікацію загальних критеріїв продуктів Microsoft Windows.
Життєвий цикл розробки захищених програм (Майкрософт)	Життєвий цикл розробки безпеки (SDL) – це процес забезпечення безпеки, орієнтований на розробку програмного забезпечення. SDL відіграє важливу роль у впровадженні безпеки та конфіденційності програмного забезпечення та мови та регіональних параметрів корпорації Майкрософт..
Програма Microsoft Bug Bounty	Якщо ви виявите вразливість у продукті, службі або пристрої Майкрософт, ми хочемо дізнатися від вас! Якщо звіт про вразливість впливає на продукт або службу в рамках однієї з наших програм, наведених нижче, ви можете отримати нагороду відповідно до опису програми.

Життєвий цикл розробки захищених програм (Майкрософт)

Життєвий цикл розробки безпеки (SDL) – це процес забезпечення безпеки, орієнтований на розробку програмного забезпечення. Починаючи з 2004 року, SDL є ініціативою корпорації Майкрософт та обов'язковою політикою, яка відіграє важливу роль у впровадженні безпеки та конфіденційності у програмне забезпечення та мову та регіональні параметри корпорації Майкрософт. Завдяки поєднанню цілісного та практичного підходу SDL покликаний зменшити кількість та серйозність уразливостей у програмному забезпеченні. SDL забезпечує безпеку та конфіденційність на всіх етапах процесу розробки.

Программа Microsoft Bug Bounty

Ви дослідник безпеки? Ви знайшли вразливість у продукті, службі або пристрої Майкрософт? Якщо так, то ми хочемо почути від вас!

Якщо звіт про вразливість впливає на продукт або службу, яка знаходиться в межах однієї з наших програм щедрості, ви можете отримати нагороду відповідно до описів програми.

Загальні критерії сертифікації

Корпорація Майкрософт прагне оптимізувати безпеку своїх продуктів та служб. У рамках цього зобов'язання корпорація Майкрософт підтримує програму сертифікації загальних критеріїв, гарантує, що продукти включають функції та функції, необхідні для відповідних профілів захисту загальних критеріїв, та завершує сертифікацію загальних критеріїв продуктів Microsoft Windows.

Перевірка FIPS 140-2

Огляд стандарту FIPS 140-2

Публікація 140-2 федерального стандарту обробки інформації (FIPS) є стандартом державних організацій США. FIPS засновано на розділі 5131 в Акті 1996 року про структуру управління інформаційними технологіями. Він визначає мінімальні вимоги безпеки для криптографічних модулів в IT-продуктах. Програма перевірки криптографічного модуля (CMVP) – це спільна робота Національного інституту стандартів та технологій США (NIST) та Центру кібербезпеки Канади (CCCS). Він перевіряє криптографічні модулі на відповідність вимогам безпеки для криптографічних модулів (частина FIPS 140-2) та пов'язаним стандартам шифрування FIPS. Вимоги до безпеки FIPS 140-2 охоплюють 11 областей, пов'язаних із проектуванням та реалізацією криптографічного модуля. Бібліотека інформаційних технологій NIST управляє пов'язаною програмою, яка перевіряє затверджені FIPS алгоритми шифрування в модулі.

Підхід корпорації Майкрософт до перевірки FIPS 140-2

Корпорація Майкрософт активно виконує зобов'язання щодо забезпечення відповідності вимогам стандарту FIPS 140-2, перевіряючи криптографічні модулі з моменту його першого створення у 2001 році. Корпорація Майкрософт перевіряє свої криптографічні модулі NIST CMVP, як описано вище. Ці криптографічні модулі використовують кілька продуктів Майкрософт, включаючи Windows 10, Windows Server та багато хмарних служб.

Використання Windows у затвердженому режимі роботи FIPS 140-2

Windows 10 і Windows Server можна налаштувати для роботи в затвердженому режимі FIPS 140-2, який зазвичай називають режимом FIPS. Якщо ви увімкнете режим FIPS, модулі бібліотеки примітивів шифрування (bcryptprimitives.dll) та бібліотеки примітивів шифрування режиму ядра (CNG.sys) будуть виконувати самообробку перед виконанням криптографічних операцій Windows. Ці самообслуговування виконуються відповідно до розділу 4.9 FIPS 140-2. Вони гарантують правильну роботу модулів.

Бібліотека криптографічних примітивів та бібліотека криптографічних примітивів режиму ядра є єдиними модулями, які торкнулися режиму FIPS. Режим FIPS не завадить Windows та його підсистемам з використанням алгоритмів шифрування, не перевірених FIPS. FIPS – це просто поради для програм або компонентів, відмінних від бібліотеки криптографічних примітивів та бібліотеки криптографічних примітивів режиму ядра.

У державних установах США, як і раніше, потрібен режим FIPS для державних пристроїв на Windows. Інші клієнти повинні самостійно вирішити, чи підходить для них режим FIPS. Існує безліч програм і протоколів, які використовують політику режиму FIPS, щоб визначити, які функції шифрування слід запускати. Клієнтам, які прагнуть дотримуватися стандарту FIPS 140-2, слід вивчити параметри конфігурації своїх програм та протоколів. Це дослідження допоможе переконатись, що їх можна налаштувати для використання перевіреного шифрування FIPS 140-2.

Windows та відповідність вимогам до конфіденційності:

Корпорація Майкрософт приділяє особливу увагу конфіденційності даних у всіх продуктах та послугах. Пропонуємо адміністраторам та відповідальним за дотримання законодавства ознайомитися з вимогами щодо захисту даних у Windows. Корпорація Майкрософт збирає дані під час взаємодії з користувачами пристроїв Windows. Ці відомості можуть містити персональні дані, які можуть бути використані для надання, захисту та покращення Windows, а також для забезпечення мережевих функцій. Ці відомості дозволяють адміністраторам та відповідальним за дотримання законодавства налагодити співпрацю, щоб краще забезпечувати конфіденційність персональних даних та дотримуватися пов'язаних з ними положень, таких як загальні вимоги до захисту даних (GDPR).

1. Прозорість збору даних у Windows

Прозорість є важливою частиною процесу збирання даних у Windows. Детальні відомості про функції та процеси, що використовуються для збору даних, доступні для користувачів та адміністраторів прямо у Windows як під час, так і після налаштування пристрою.

1.1. Процедура налаштування пристрою та підтримка багаторівневої прозорості

При настроюванні пристрою користувач може налаштувати конфіденційність. Ці параметри конфіденційності є ключем для визначення обсягу персональних даних, що збираються. По кожному параметру конфіденційності користувачеві надаються відомості про параметр разом із посиланнями на додаткову інформацію. Ця інформація пояснює, які дані збираються, як дані використовуються та як керувати параметром після завершення налаштування пристрою. Користувач також може ознайомитися із заявою про конфіденційність під час підключення до мережі на етапі налаштування. Короткий огляд параметрів конфіденційності наведено у статті Учасники програми попередньої оцінки Windows першими побачать новий макет екрана параметрів конфіденційності у Windows 10 – запис у блогах про Windows.

1.2 Контроль збору даних

Засіб перегляду діагностичних даних (DDV) – це програма Microsoft Store (доступна у Windows 10 починаючи з версії 1803 та Windows 11), що дозволяє користувачеві переглядати дані діагностики Windows, які збираються на пристрої з Windows і надсилаються до корпорації Майкрософт у режимі реального часу. DDV групує інформацію в прості категорії, що описують дані, що збираються. Адміністратор також може використовувати засіб перегляду діагностичних даних для модуля PowerShell для перегляду діагностичних даних, що збираються з пристрою, замість інтерфейсу користувача засобу перегляду діагностичних даних. Докладніші відомості див. у розділі Засіб перегляду діагностичних даних для PowerShell.

2. Управління збором даних у Windows

Можна керувати параметрами конфіденційності у Windows різними способами. Користувачі можуть змінити параметри конфіденційності, відкривши програму «Параметри» у Windows. Організація також може керувати параметрами конфіденційності за допомогою групової політики або управління мобільними пристроями (MDM). У наступних розділах наведено загальні відомості про те, як керувати параметрами конфіденційності, розглянутими раніше у цій статті.

2.1 Налаштування конфіденційності для користувачів

Якщо пристрій з Windows налаштований, користувач може керувати параметрами збору даних, відкривши програму «Параметри» у Windows. Адміністратори можуть керувати параметрами конфіденційності шляхом налаштування політики на пристрої (див. розділ 2.2 нижче). У цьому випадку користувач побачить оповіщення **Деякі параметри приховані або керуються організацією** під час переходу на сторінку «Параметри". У цьому випадку користувач може змінювати параметри лише відповідно до політик, встановлених адміністратором на пристрої.

2.2 Керування параметрами конфіденційності для адміністраторів

Адміністратори можуть налаштовувати конфіденційність та керувати ними в межах своєї організації за допомогою групової політики, параметрів керування мобільними пристроями (MDM) або параметрів реєстру Windows.

У таблиці нижче наведено загальні відомості про параметри конфіденційності, описані вище в цьому документі, з детальною інформацією про те, як можна налаштувати ці політики. У таблиці також наводиться інформація про значення за замовчуванням для кожного з цих параметрів конфіденційності на випадок, якщо ви не керуєте цим параметром за допомогою політики і не пропускаєте процедуру запуску при першому увімкненні комп'ютера (OOBE) під час налаштування пристрою. Якщо ви хочете мінімізувати збір даних, тут також наводяться рекомендовані значення для налаштування.

2.3 Посібник з налаштування конфігурації

У цьому розділі наводяться загальні відомості та посилання на докладніші відомості, а також інструкції для адміністраторів та відповідальних за дотримання законодавства. За допомогою цих інструкцій ви зможете керувати

настройками пристрою, щоб керувати цілями щодо відповідності вимогам вашої організації. Сюди включені відомості про налаштування пристрою та встановлення параметрів пристрою після завершення процедури налаштування, щоб звести до мінімуму обсяг даних, що збираються, і забезпечити конфіденційність у роботі користувачів з пристроєм.

2.3.1 Керування процесом налаштування пристрою

Розгортання Windows можна налаштувати за допомогою різних способів, які надають адміністратору можливості для керування, включаючи те, як пристрій налаштований, що увімкнено за замовчуванням, а також що користувач може змінювати пристрій після входу в систему.

Якщо ви хочете отримати можливість повністю контролювати та застосовувати обмеження до даних, що надсилаються до корпорації Майкрософт, можна використовувати Менеджер конфігурацій як рішення для розгортання. Диспетчер конфігурацій можна використовувати для розгортання налаштованого способу завантаження за допомогою різних методів розгортання. Можна додатково обмежити надсилання до корпорації Майкрософт будь-яких діагностичних даних, які стосуються диспетчера конфігурацій, відключивши цей параметр, як описано тут.

Крім того, адміністратори можуть також використовувати програму Windows Autopilot. Autopilot знижує загальне навантаження на розгортання, що дозволяє адміністраторам повністю налаштовувати запуск при першому включенні комп'ютера. Тим не менш, оскільки Windows Autopilot є хмарним рішенням, адміністратори повинні знати, що мінімальний набір ідентифікаторів пристроїв відправляється до корпорації Майкрософт під час початкового завантаження пристрою. Ця залежна від пристрою інформація використовується для ідентифікації пристрою, щоб він міг отримувати налаштовані адміністратором профіль та політики Autopilot.

2.3.2 Керування мережними функціями та основними службами Windows

Windows включає компоненти, які підключаються до Інтернету для надання розширених функцій та додаткових можливостей на основі служб. Ці компоненти називають мережевими функціями. Наприклад, антивірусна програма Microsoft Defender – це мережна функція, що забезпечує оновлений захист для підтримки безпеки пристроїв в організації.

Основні служби – це служби продукту, які підключаються до корпорації Майкрософт для забезпечення безпеки, своєчасного оновлення та належної роботи продукту. Наприклад, ліцензійна служба, яка підтверджує наявність дійсної ліцензії на використання Windows.

Основні служби та функції мережі Windows надають список найпоширеніших основних служб і мережевих функцій Windows.

Якщо Ви використовуєте мережну функцію, дані надсилаються в корпорацію Майкрософт і обробляються нею, щоб надати цю мережну функцію. Адміністратори можуть керувати тим, які дані надсилаються з їх організації до корпорації Майкрософт, налаштування параметрів, пов'язаних з можливостями, що надаються мережними функціями та основними службами Windows. Для

отримання додаткових відомостей див. розділ Керування з'єднаннями з операційної системи Windows до служб Майкрософт. У цій статті наведено різні методи, які можна використовувати для налаштування кожного параметра, вплив на функціональність, а також вказано, які версії Windows можна застосувати.

У статті Керування кінцевими точками підключення для Windows 11 Корпоративна список кінцевих точок, до яких мережеві функції Windows передають дані для останнього випуску Windows, а також описи будь-яких функцій, які можуть бути порушені обмеженням збору даних.

2.3.3 Базовий план обмеженої функціональності

Організації може знадобитися мінімізувати обсяг даних, надісланих у Microsoft або спільних з програмами Майкрософт, шляхом керування підключеннями та налаштування додаткових параметрів на своїх пристроях. Аналогічно Базовим параметрам безпеки Windows корпорація Майкрософт випустила обмежений базовий рівень функціональності, спрямований на налаштування параметрів для мінімізації даних, що надсилаються до Майкрософт. Проте застосування цих налаштувань може вплинути на функціональність пристрою. У статті Управління підключеннями від компонентів операційної системи Windows до служб Майкрософт викладаються докладні відомості про те, як застосувати базовий план, наводиться повний перелік параметрів, що входять до базового плану, а також розповідається про те, які функції торкнуться. Адміністратори, які не бажають застосовувати базовий план, також можуть знайти відомості про те, як налаштувати кожен параметр окремо, щоб знайти оптимальний баланс між надсиланням даних та впливом на необхідні для організації функції.

2.3.4 Діагностичні дані: керування повідомленнями про зміну рівня при вході

Починаючи з Windows 10, версія 1803 та Windows 11, якщо адміністратор змінив параметр збору діагностичних даних, користувачі будуть повідомлені про цю зміну при першому вході до пристрою. Наприклад, якщо ви налаштували пристрій на надсилання додаткових діагностичних даних, користувач отримає повідомлення під час наступного входу до пристрою. Ці оповіщення можна вимкнути за допомогою налаштування групової політики Конфігурація комп'ютера > Адміністративні шаблони > Компоненти Windows > Збір даних та попередні збирання > Налаштування повідомлень про зміну згоди на збір даних телеметрії або політики MDM ConfigureTelemetryOptInChangeNotification.

2.3.5 Діагностичні дані: керування вибором кінцевого користувача для зміни параметра

Windows 10 версії 1803 і пізніших версій та Windows 11 дозволяє користувачам змінювати рівень діагностичних даних на нижче значення, ніж задане адміністратором. Наприклад, якщо ви налаштували пристрій на надсилання необов'язкових діагностичних даних, користувач може змінити параметр так, щоб надсилалися лише обов'язкові діагностичні дані, відкривши програму «Параметри» у Windows і перейшовши до розділу Діагностика та відгуки. Адміністратори можуть обмежити можливість зміни цього параметра

користувачами, увімкнувши групову політику.Налаштування інтерфейсу згоди на збір даних телеметрії або політику MDM ConfigureTelemetryOptInSettingsUx.

2.3.6 Діагностичні дані: керування видаленням даних залежно від пристрою

У Windows 10 версії 1809 і пізніших версій і Windows 11 користувач може видалити діагностичні дані, зібрані на його пристрої, відкривши програму «Параметри» у Windows, перейшовши в розділ Діагностика та відгуки та натиснувши кнопку Видалити під заголовком Видалити діагностичні дані. Адміністратор також може видалити діагностичні дані з пристрою за допомогою командлета PowerShell Clear-WindowsDiagnosticData.

Адміністратор може вимкнути можливість користувача видаляти дані діагностики з пристрою, налаштувавши групову політику Конфігурація комп'ютера > Адміністративні шаблони > Компоненти Windows > Збір даних та попередні збирання > Вимкнути видалення діагностичних даних або політику MDM DisableDeviceDelete.

2.3.7 Діагностичні дані: увімкнення конфігурації обробника діагностичних даних Windows

Конфігурація обробника діагностичних даних Windows дозволяє IT-адміністраторам бути керуючими відповідно до Загального регламенту Європейського Союзу захисту даних (GDPR) для діагностичних даних Windows, зібраних з пристроїв з Windows, які приєднані до Azure Active Directory (AAD) і відповідають вимогам до конфігурації. Щоб отримати додаткові відомості, див. Увімкнення конфігурації процесора діагностичних даних Windows у статті Настроювання діагностичних відомостей Windows у вашій організації. Діагностичні дані Windows не включають дані, які обробляє корпорація Майкрософт у зв'язку з наданням можливостей, заснованих на службах.

Діагностичні дані Windows, зібрані з пристроїв, для яких увімкнена конфігурація процесора діагностичних даних Windows, можуть бути пов'язані з конкретним ідентифікатором користувача Azure Active Directory або ідентифікатором пристрою. Конфігурація обробника діагностичних даних Windows надає елементи керування, які допомагають відповідати на запити суб'єкта даних (DSR) для видалення діагностичних даних при закритті облікового запису користувача для певного ідентифікатора користувача Azure AD. Крім того, можна експортувати запити суб'єкта даних для діагностичних даних, пов'язаних з певним ідентифікатором користувача Azure AD. Щоб отримати додаткові відомості, див. Процес здійснення прав суб'єкта даних. Корпорація Майкрософт також забезпечить закриття облікового запису клієнта або тому, що ви вирішили закрити свій обліковий запис клієнта Azure або Azure AD, або тому що ви вирішили закрити обліковий запис клієнта Azure або Azure AD або тому, що ви вирішили, що більше не хочете бути контролером даних для діагностики даних Windows, але, як і раніше, хочете залишатися клієнтом Azure.

IT-адміністраторам, які включили конфігурацію обробника діагностичних даних Windows, рекомендується враховувати наступне:

– Обмежте можливість користувача входити до облікового запису Microsoft (MSA) за допомогою блокування групової політики облікового запису Майкрософт.

– Обмежте можливість користувача надсилати відгуки, оскільки будь-які відгуки або додаткові журнали, надіслані користувачем, не керуються параметром конфігурації процесора діагностичних даних Windows. Ви можете видалити програму «Центр відгуків» за допомогою PowerShell, а можливість надсилання відгуків у Microsoft Edge можна заблокувати за допомогою групової політики відгуків.

3. Процедура реалізації прав суб'єкта даних

У цьому розділі описано різні способи, які корпорація Майкрософт надає користувачам та адміністраторам для реалізації прав суб'єктів даних стосовно даних, зібраних на пристрої з Windows.

Для IT-адміністраторів, у яких є пристрої, які використовують конфігурацію процесора діагностичних даних Windows, див. Запити суб'єктів даних для GDPR та CCPA. В іншому випадку переходьте до розділів нижче.

3.1 Видалення

Користувачі можуть видалити дані на основі пристроїв, відкривши програму «Параметри» у Windows, перейшовши до розділу «Діагностика та відгуки» та натиснувши кнопку «Видалити» під заголовком «Видалити діагностичні дані». Адміністратори можуть також використовувати командлет PowerShell Clear-WindowsDiagnosticData.

3.2 Перегляд

Засіб перегляду діагностичних даних (DDV) надає можливість перегляду діагностичних даних, що збираються на пристрої Windows. Адміністратори також можуть використовувати командлет PowerShell Get-DiagnosticData.

3.3 Експорт

Засіб перегляду діагностичних даних (DDV) забезпечує можливість експорту діагностичних даних, отриманих під час роботи програми шляхом натискання кнопки «Експорт даних» у верхньому меню. Адміністратори можуть також використовувати сценарій командлета PowerShell Get-DiagnosticData.

3.4 Пристрої, підключені до облікового запису Майкрософт

Якщо користувачі входять до інтерфейсу Windows або програми на пристрої за допомогою облікового запису Майкрософт, вони можуть переглядати, видаляти та експортувати дані, пов'язані зі своїм обліковим записом Майкрософт, на Інформаційній панелі конфіденційності.

4. Передача даних через кордони

Корпорація Майкрософт виконує вимоги чинного законодавства щодо збору, використання та зберігання персональних даних, у тому числі щодо їх передачі через кордони.

5. Відомості про пов'язані продукти Windows

У розділах нижче наведено докладні відомості про те, як збираються та обробляються конфіденційні дані та у зв'язаних продуктах Windows.

5.1 Windows Server 2016 та пізніших версій

Windows Server використовує самі механізми, як і Windows 10 (і пізніших версій), для обробки персональних даних.

5.2 Surface Hub

Surface Hub є загальним пристроєм, який використовується в організації. Ідентифікатор пристрою, який збирається у складі діагностичних даних, не пов'язаний з користувачем. Для видалення діагностичних даних Windows, які надсилаються до корпорації Майкрософт щодо Surface Hub, можна використовувати засіб видалення діагностичних даних Surface Hub, доступний у Microsoft Store.

5.3 Аналітика комп'ютерів

Аналітика комп'ютерів – це набір рішень для порталу Azure, які надають широку інформацію про стан пристроїв у розгортанні. Аналітика комп'ютерів – це окрема від Windows пропозиція, яка залежить від увімкнення режиму мінімального збору даних на пристрої для роботи.

5.4 Комп'ютери, керовані Майкрософт

Комп'ютери, керовані Майкрософт (MMD), це служба, яка надає користувачам безпечні сучасні можливості та завжди забезпечує оновлення пристроїв з урахуванням останніх версій Windows Корпоративна, Office 365 професійний плюс і служб безпеки Microsoft.

5.5 Підтримка оновлень

Підтримка оновлень – це служба, яка дозволяє організаціям відстежувати оновлення безпеки, якості та функцій для випусків Windows Професійна, для освітніх закладів та Корпоративна, а також переглядати звіт про проблеми пристроїв та оновлень, пов'язані з відповідністю вимогам, які потребують уваги. Підтримка оновлень використовує діагностичні дані Windows для всіх звітів.