Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

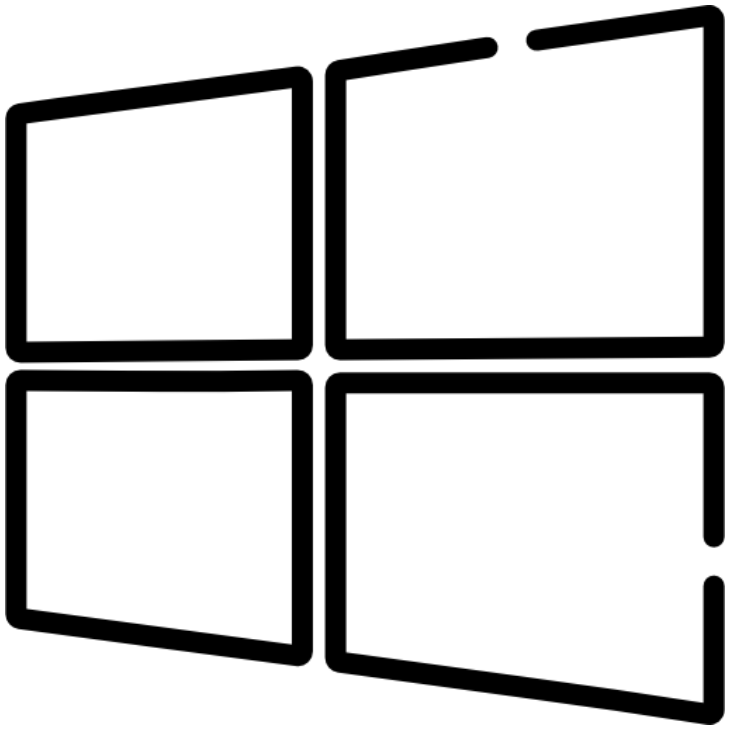
Защита информации

Безопасность операционной системы Windows 11

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

Windows 11 Security — Our Hacker-in-Chief Runs Attacks and Shows Solutions
https://www.youtube.com/watch?v=tg9QUrnVFho



Общие сведения о безопасности Windows 11

Общие сведения о безопасности Windows 11

- **Концепция проверки "Никому не доверяй**" явно применяется к рискам, создаваемым как устройствами, так и пользователями. Windows включает возможности аттестации работоспособности устройств и условного доступа , которые используются для предоставления доступа к корпоративным ресурсам.

Модель "Никому не доверяй"

- **Модель "Никому не доверяй"** основана на предположении, что сеть в пределах корпоративного брандмауэра небезопасна, а все запросы рассматриваются так, как если бы они поступали из открытой сети. Независимо от источника запроса и ресурсов, к которым он обращается, в рамках концепции "Никому не доверяй" исповедуется принцип "никогда не доверяй, всегда проверяй". Каждый запрос доступа предварительно проходит полную проверку подлинности, процедуру авторизации и шифрования. Для минимизации бокового смещения применяются принципы микросегментации и предоставления минимально необходимых прав. Для обнаружения аномалий и реагирования на них в режиме реального времени используются функциональные средства искусственного интеллекта и аналитики.

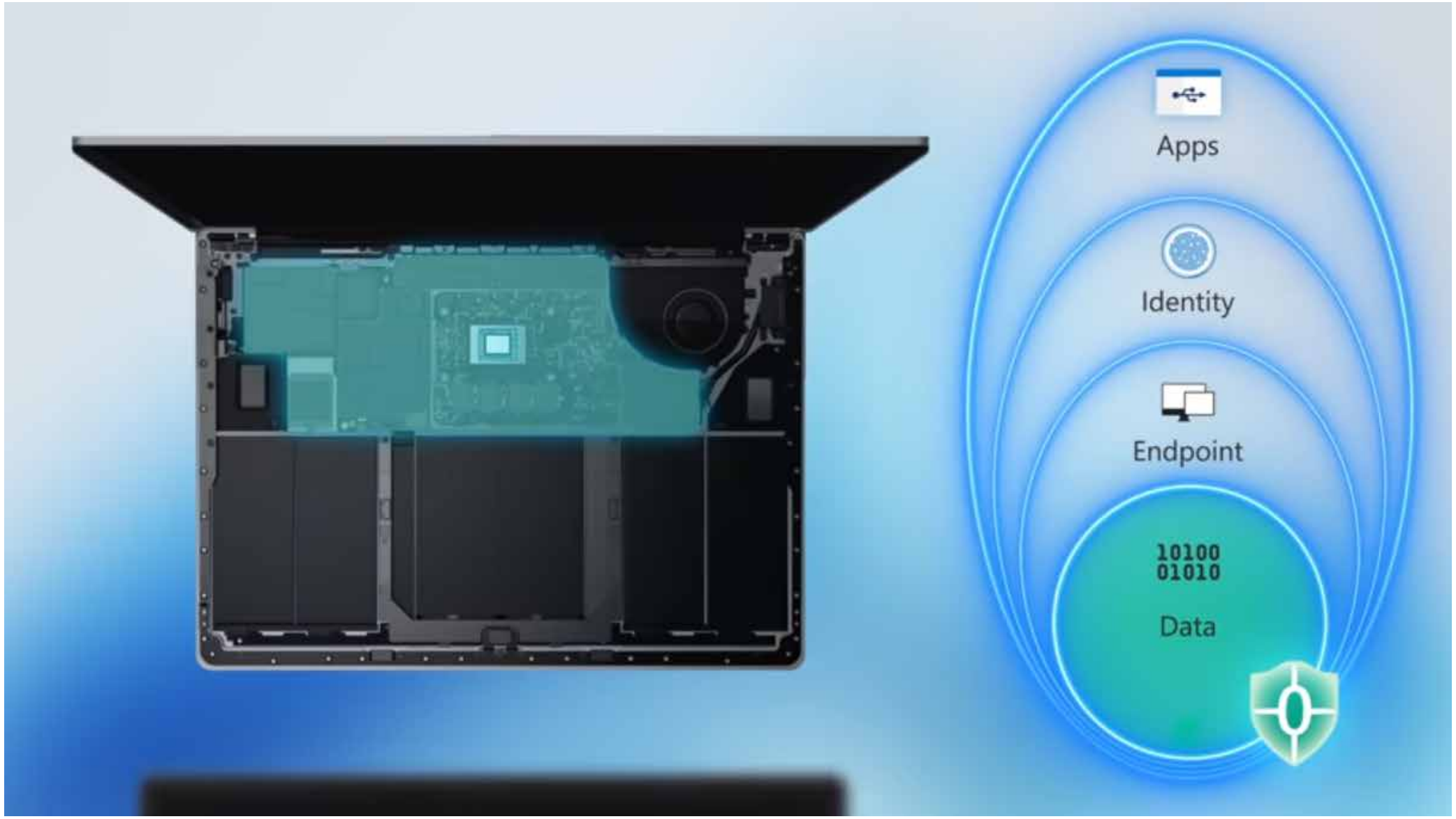
Модель безопасности “Никому не доверяй” (Zero Trust)

- Модель безопасности "Никому не доверяй" предоставляет нужным пользователям правильный доступ в нужное время.
- Эта **модель безопасности основана на трех принципах:**

- **Снижение риска путем явной проверки точек данных**, таких как удостоверение пользователя, местонахождение и работоспособность устройства, для каждого запроса на доступ без исключения.
- После проверки пользователям и устройствам **предоставляется доступ только к необходимым ресурсам в течение нужного количества времени**.
- **Использование непрерывной аналитики для обнаружения угроз** и улучшения защиты.

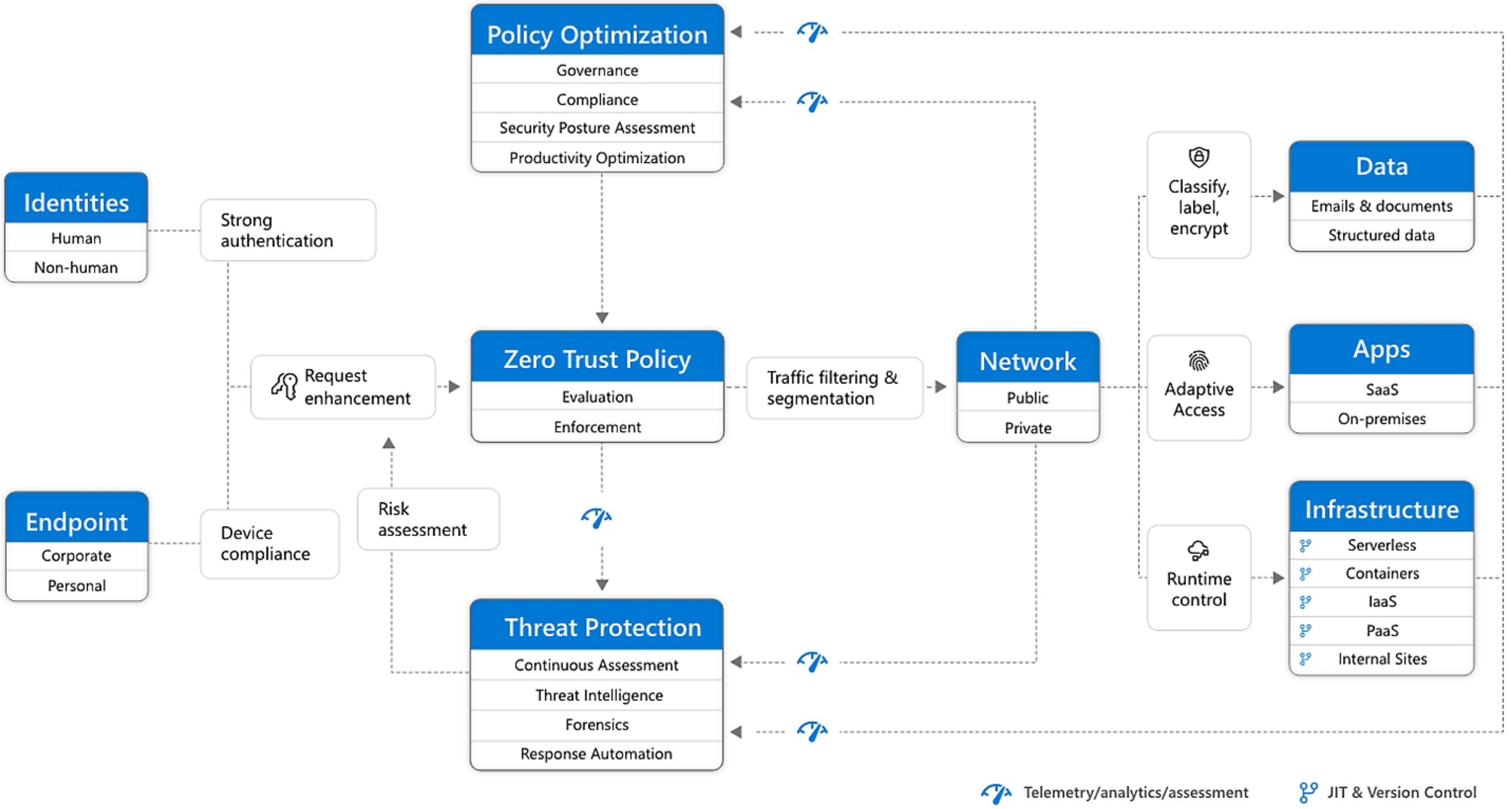
- В Windows 11 явная проверка по принципу "Никому не доверяй" применяется к рискам, связанным как устройствами, так и людьми. Windows 11 обеспечивает безопасность от микросхемы до облака

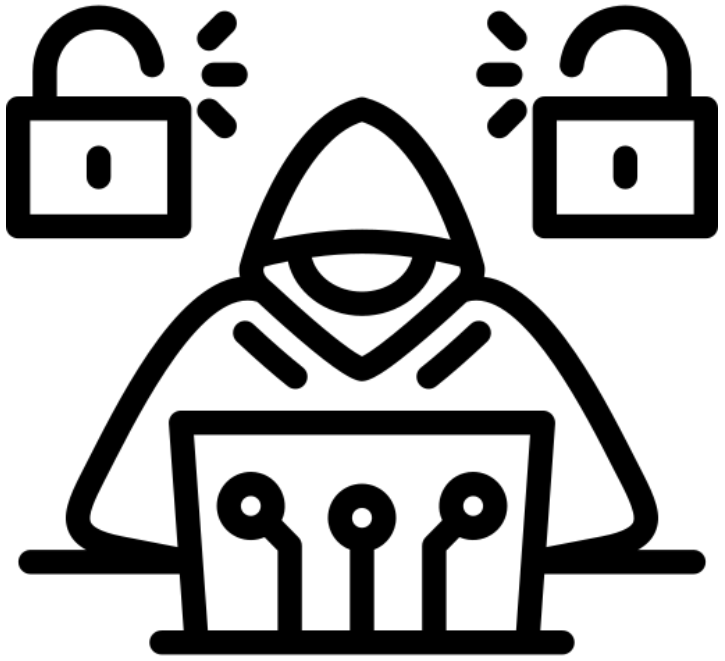
Zero Trust



Принципы «Никому не доверяй»

- **Проверка явным образом.** Всегда выполняйте проверку подлинности и авторизацию на основе всех доступных точек данных, включая удостоверение пользователя, расположение, работоспособности устройства, службу или рабочую нагрузку, классификацию данных и мониторинг аномалий.
- **Используйте доступ с минимальными привилегиями.** Ограничьте доступ пользователей с помощью JIT и достаточного доступа, адаптивных политик на основе рисков и защиты данных, чтобы защитить данные и поддерживать производительность
- **Предположим, что нарушение.** Предотвратить получение доступа злоумышленниками, чтобы свести к минимуму потенциальный ущерб для данных и систем. Защита привилегированных ролей, проверка сквозного шифрования, использование аналитики для получения видимости и обнаружение угроз для улучшения защиты


Policy Optimization
Governance
Compliance
Security Posture Assessment
Productivity Optimization
Identities
Human
Non-human
Strong authentication
Request enhancement
Zero Trust Policy
Evaluation
Enforcement
Traffic filtering & segmentation
Network
Public
Private
Classify, label, encrypt
Data
Emails & documents
Structured data
Adaptive Access
Apps
SaaS
On-premises
Endpoint
Corporate
Personal
Device compliance
Risk assessment
Runtime control
Infrastructure
Serverless
Containers
IaaS
PaaS
Internal Sites
Threat Protection
Continuous Assessment
Threat Intelligence
Forensics
Response Automation
Telemetry/analytics/assessment
JIT & Version Control



Защита от киберпреступников

Безопасность операционной системы Windows 11

- Безопасность и конфиденциальность зависят от операционной системы, защищающей систему и сведения с момента запуска, обеспечивая основную защиту от микросхемы до облака. Windows 11 — это самая безопасная Windows с широкими возможностями действий защиты, разработанными для обеспечения безопасности. Это включает встроенное расширенное шифрование и защиту данных, надежную сетевую и системную безопасность, а также интеллектуальные средства защиты от постоянно развивающихся угроз.

Безопасность системы

Безопасная загрузка и надежная загрузка

- Безопасная загрузка и доверенная загрузка помогают предотвратить загрузку вредоносных программ и поврежденных компонентов при запуске устройства.

- Безопасная загрузка начинается с начальной защиты при загрузке, а затем запускается процесс доверенной загрузки. Вместе безопасная загрузка и доверенная загрузка помогают обеспечить безопасную и надежную загрузку системы.

Измеряемая загрузка

- Измеряемая загрузка измеряет все важные параметры кода и конфигурации во время загрузки Windows. К ним относятся: микропрограммы, диспетчер загрузки, гипервизор, ядро, защищенное ядро и операционная система. Измеренная загрузка сохраняет измерения в TPM на компьютере и делает их доступными в журнале, который можно протестировать удаленно, чтобы проверить состояние загрузки клиента.

- Функция измеряемой загрузки предоставляет программное обеспечение для защиты от вредоносных программ с доверенным (устойчивым к спуфингам и незаконному изменению) журнала всех загрузочных компонентов, которые были запущены до этого. Антивредоносная программа может использовать журнал, чтобы определить, являются ли компоненты, которые работали до этого, надежными или они заражены вредоносными программами. Программное обеспечение для защиты от вредоносных программ на локальном компьютере может отправить журнал на удаленный сервер для оценки. Удаленный сервер может инициировать действия по исправлению, взаимодействуя с программным обеспечением на клиенте или с помощью отдельных механизмов, в зависимости от ситуации.

Служба аттестации работоспособности устройств

- Процесс проверки работоспособности устройства с Windows поддерживает модель нулевого доверия, смещающую фокус со статических сетевых периметров на пользователей и ресурсы. Процесс аттестации подтверждает, что устройство, встроенное ПО и процесс загрузки находятся в хорошем состоянии и не были изменены, прежде чем они смогут получить доступ к корпоративным ресурсам. Определения сделаны с помощью данных, хранящихся в TPM, который обеспечивает безопасный корень доверия. Эти сведения отправляются в службу подтверждения, например, в Azure Attestation, чтобы убедиться, что устройство находится в доверенном состоянии. Затем средство MDM, например Microsoft Intune проверяет работоспособности устройства и соединяет эти сведения с идентификатором Microsoft Entra для условного доступа.

Параметры политики безопасности Windows и аудит

- Корпорация Майкрософт предоставляет надежный набор политик параметров безопасности, которые ИТ-администраторы могут использовать для защиты устройств с Windows и других ресурсов в своей организации.

Назначенный доступ (режим киоска)

- Некоторые настольные устройства на предприятии служат специальной цели. Например, компьютер в "вестибюле", который клиенты используют для работы с каталогом продукции. Или компьютер, отображающий визуальное содержимое в виде цифрового знака. Клиент Windows предлагает два разных закрытых интерфейса для общего или специализированного использования: киоск с одним приложением, в котором одно приложение универсальной платформы Windows (UWP) работает в полноэкранном режиме над экраном блокировки, или киоск с несколькими приложениями, на котором работает одно или несколько приложений. приложения с рабочего стола.

- Конфигурации киоска основаны на назначенном доступе, функции Windows, которая позволяет администратору управлять работой пользователя, ограничивая точки входа приложения, доступные пользователю.

Защита от вирусов и угроз

Антивирусная программа в Microsoft Defender

- Антивирусная программа в Microsoft Defender — это решение для защиты, включенное во все версии Windows. С момента загрузки Windows антивирусная программа в Microsoft Defender постоянно отслеживает вредоносные программы, вирусы и угрозы безопасности. Обновления скачиваются автоматически для обеспечения безопасности устройства и защиты его от угроз. Антивирусная программа в Microsoft Defender включает антивирусную защиту в реальном времени, основанную на поведении, и эвристику.

- Сочетание постоянного сканирования содержимого, отслеживания поведения файлов и процессов и других эвристик эффективно предотвращает угрозы безопасности. антивирусная программа Microsoft Defender постоянно проверяет наличие вредоносных программ и угроз, а также обнаруживает и блокирует потенциально нежелательные приложения (PUA), которые считаются приложениями, которые негативно влияют на ваше устройство, но не считаются вредоносными программами.

Защита локального администратора безопасности (LSA)

- В Windows есть несколько важных процессов для проверки удостоверения пользователя. Проверки включают локальный центр безопасности (LSA), отвечающий за проверку подлинности пользователей и проверку входа в систему Windows. LSA обрабатывает маркеры и учетные данные, такие как пароли, используемые для единого входа в учетную запись Microsoft и службы Azure. Для обеспечения защиты этих учетных данных дополнительная защита LSA позволяет загружать только доверенный подписанный код и обеспечивает надежную защиту от кражи учетных данных.

- Защита LSA включена по умолчанию на новых корпоративных устройствах с Windows 11 с добавленной поддержкой блокировки, отличной от UEFI, и управления политиками через MDM и групповую политику.

Сокращение направлений атак (ASR)

- Правила сокращения направлений атак (ASR) помогают предотвратить поведение программного обеспечения, которое часто используется для взлома устройства или сети. Сокращая число направлений атак, можно снизить уровень общей уязвимости организации.

- Администраторы могут настроить определенные правила ASR, чтобы помочь блокировать определенные действия, такие как запуск исполняемых файлов и сценариев, пытающихся скачать или запустить файлы, запуск запутанных или иным образом подозрительных сценариев, выполнение действий, которые приложения обычно не инициируют при повседневной работе.

Параметры защиты от несанкционированного доступа для MDE

- Защита от несанкционированного доступа — это возможность Microsoft Defender для конечной точки, помогающая защитить определенные параметры безопасности, такие как защита от вирусов и угроз, от отключения или изменения. Во время некоторых видов кибератак злоумышленники пытаются отключить функции безопасности на устройствах. Отключение функций безопасности обеспечивает злоумышленникам более простой доступ к данным, возможность устанавливать вредоносные программы, а также возможность использовать данные, удостоверения и устройства. Защита от несанкционированного доступа обеспечивает защиту от подобных действий.

Контролируемый доступ к папкам

- Ценные сведения в определенных папках можно защитить, управляя доступом приложений к определенным папкам. Только доверенные приложения могут получить доступ к защищенным папкам, указанным при настройке контролируемого доступа к папкам. Часто используемые папки, например используемые для документов, изображений, скачиваний, обычно включаются в список управляемых папок. Управляемый доступ к папкам работает со списком доверенных приложений. Приложения, включенные в список доверенных программ, работают должным образом. Приложения, которые не включены в список доверенных, не могут вносить какие-либо изменения в файлы в защищенных папках.

- Управляемый доступ к папкам обеспечивает защиту ценных данных от вредоносных приложений и угроз, таких как программы-шантажисты.

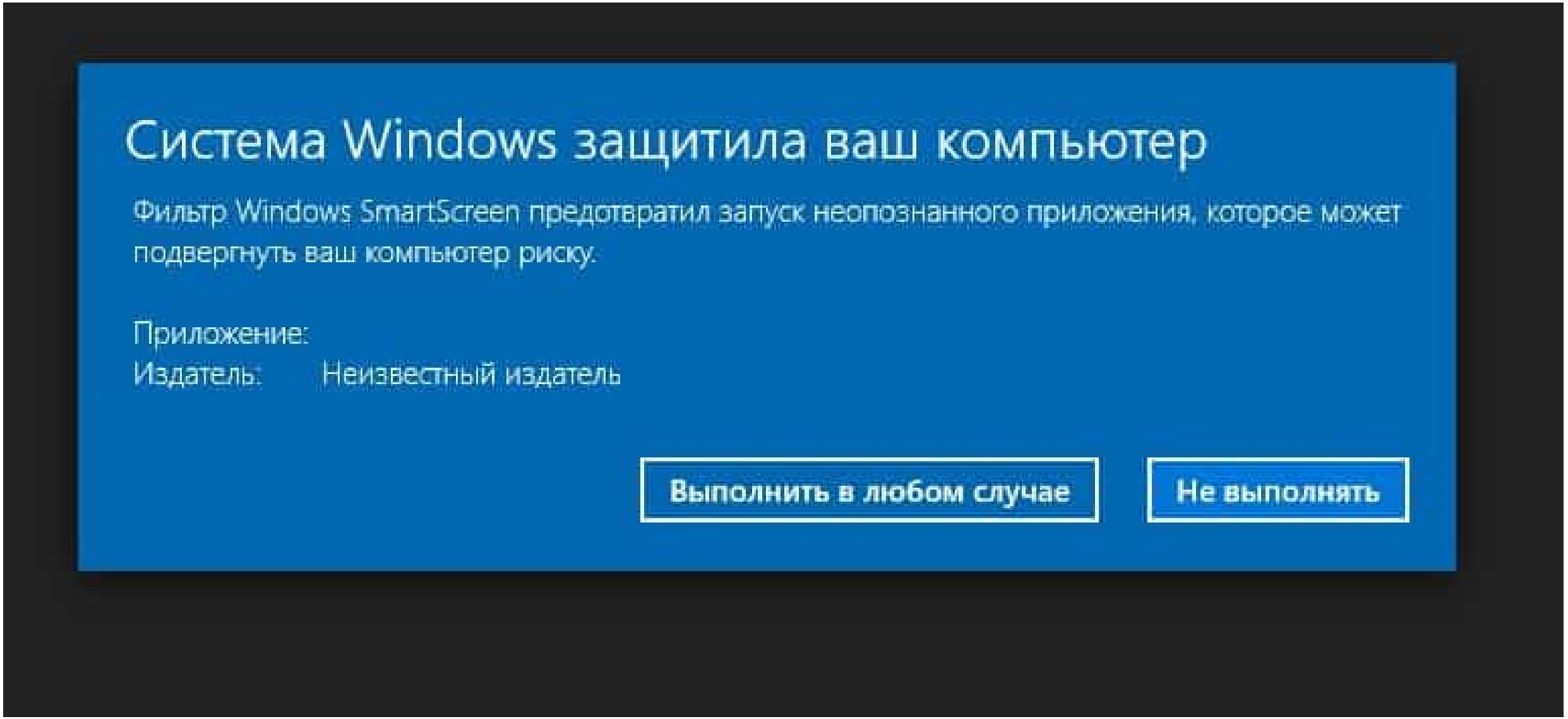
Защита от эксплойтов

- Защита от эксплойтов автоматически применяет несколько методов защиты от эксплойтов к процессам и приложениям операционной системы. Защита от эксплойтов лучше всего работает с Microsoft Defender для конечной точки, предоставляющей организациям подробные отчеты о событиях и блокировках защиты от эксплойтов в рамках типичных сценариев исследования предупреждений. Защиту от эксплойтов можно включить на отдельном устройстве, а затем использовать MDM или групповую политику для распространения файла конфигурации на несколько устройств. При обнаружении меры защиты на устройстве появится уведомление из центра уведомлений. Вы можете настроить уведомления, указав сведения о компании и контактные данные. Можно также включать правила по отдельности, чтобы настроить методы, отслеживаемые этой функцией.

Фильтр SmartScreen в Microsoft Defender

- Фильтр SmartScreen в Microsoft Defender защищает от фишинговых и вредоносных веб-сайтов и приложений, а также от скачивания потенциально вредоносных файлов.
- Для расширенной защиты от фишинга SmartScreen также оповещает пользователей, когда они вводят свои учетные данные в потенциально опасном расположении. ИТ-специалисты могут настроить отображение уведомлений с помощью MDM или групповой политики.
- По умолчанию защита работает в режиме аудита, предоставляя ИТ-администраторам полное управление принятием решений по созданию и применению политик.

Фильтр SmartScreen **в** Microsoft Defender



Microsoft Defender **для конечной точки**

- Microsoft Defender для конечной точки — это корпоративное решение для обеспечения безопасности конечных точек, помогающее группам безопасности обнаруживать, исследовать и реагировать на сложные угрозы. Организации могут использовать обширные данные о событиях и сведения об атаках, предоставляемые Defender для конечной точки, для исследования инцидентов. Defender для конечной точки объединяет следующие элементы, чтобы предоставить более полную картину инцидентов безопасности: поведенческие датчики конечных точек, облачную аналитику безопасности, аналитику угроз и широкие возможности реагирования.

Сетевая безопасность

Безопасность на уровне транспорта (TLS)

- **Протокол TLS — это криптографический протокол, предназначенный для обеспечения безопасности связи по сети.**
- TLS 1.3 — это последняя версия протокола, включенная по умолчанию в Windows 11.
- В этой версии устранены устаревшие криптографические алгоритмы, повышена безопасность по сравнению с прежними версиями, и она направлена на шифрование как можно большей части рукопожатия TLS. Рукопожатие обеспечивает более высокий уровень эффективности с меньшей дистанцией кругового пути на подключение в среднем и поддерживает только пять наборов шифров, обеспечивающих идеальную секретность перенаправления и меньший операционный риск.

Безопасность системы доменных имен (DNS)

- Начиная с Windows 11, DNS-клиент Windows поддерживает dns через HTTPS (DoH), зашифрованный протокол DNS. Это позволяет администраторам гарантировать, что их устройства защищают DNS-запросы от злоумышленников по пути, будь то пассивные наблюдатели, регистрирующих поведение браузера, или активные злоумышленники, пытающиеся перенаправить клиенты на вредоносные сайты.

- В модели "никому не доверяй", в которой нет доверия, размещенного на границе сети, требуется безопасное подключение к сопоставителью доверенных имен.

Соединение Bluetooth и защита подключения

- Число Bluetooth-устройств, подключенных к Windows, продолжает расти. Windows поддерживает все стандартные протоколы соединения Bluetooth, включая классические соединения и соединения LE Secure, безопасное простое соединение, а также классическое и устаревшее соединение LE. Windows также реализует конфиденциальность LE, располагаясь на узле. Обновления Windows помогают пользователям оставаться в курсе проблем с функциями безопасности ОС и драйверов в соответствии с bluetooth Special Interest Group (SIG), стандартными отчетами об уязвимостях и проблемами, выходящими за рамки основных отраслевых стандартов Bluetooth. Корпорация Майкрософт настоятельно рекомендует пользователям следить за непрерывным обновлением микропрограмм и программного обеспечения их аксессуаров Bluetooth.

Безопасность Wi-Fi

- Wi-Fi защищенный доступ (WPA) — это программа сертификации безопасности, предназначенная для защиты беспроводных сетей. WPA3 — это последняя версия сертификации, обеспечивающая более безопасный и надежный метод подключения по сравнению с WPA2 и более ранними протоколами безопасности. Windows поддерживает три режима WPA3: персональный WPA3 с протоколом Hash-to-Element (H2E), WPA3 Enterprise и WPA3 Enterprise 192-bit Suite B.

- Windows 11 также поддерживает WPA3 Enterprise, определенный WFA, включающий расширенную проверку сертификата сервера и TLS 1.3 для проверки подлинности с использованием проверки подлинности EAP-TLS.

Opportunistic Wireless Encryption (OWE)

- Opportunistic Wireless Encryption (OWE) — это технология, позволяющая беспроводным устройствам устанавливать зашифрованные соединения с общедоступными точками доступа Wi-Fi.

Брандмауэр Windows

- Брандмауэр Windows обеспечивает двусторонняя фильтрацию сетевого трафика на основе узла, блокируя несанкционированный трафик, поступающий на локальное устройство или из него, в зависимости от типов сетей, к которым подключено устройство. Брандмауэр Windows уменьшает число направлений атак устройства с помощью правил, ограничивающих или разрешающих трафик по многим свойствам, таким как IP-адреса, порты или пути к программам. Уменьшение поверхности атаки устройства повышает управляемость и снижает вероятность успешной атаки.

- Благодаря интеграции с протоколом безопасности Интернета (IPsec) брандмауэр Windows предоставляет простой способ обеспечить сквозную сетевую связь с проверкой подлинности. Он предоставляет масштабируемый многоуровневый доступ к доверенным сетевым ресурсам, помогая обеспечить целостность данных и при желании помогая защитить конфиденциальность данных. Брандмауэр Windows — это брандмауэр на основе узла, который входит в состав операционной системы. Дополнительное оборудование или программное обеспечение не требуется. Брандмауэр Windows также предназначен для дополнения существующих решений сетевой безопасности сторонних производителей с помощью документированного интерфейса прикладного программирования (API).

Виртуальная частная сеть (VPN)

- Клиентская платформа Windows VPN включает встроенные протоколы VPN, поддержку конфигурации, общий пользовательский интерфейс VPN и поддержку программирования для пользовательских протоколов VPN. VPN-приложения доступны в Microsoft Store для корпоративных и для потребительских VPN, включая приложения для самых популярных корпоративных VPN-шлюзов.

- В Windows 11 наиболее часто используемые элементы управления VPN интегрированы прямо в панель быстрых действий. На панели быстрых действий пользователи могут видеть состояние VPN, запускать и останавливать VPN-туннели, а также получать доступ к приложению "Параметры" для дополнительных элементов управления.

Always On **VPN (туннель устройства)**

- С помощью Always On VPN можно создать выделенный профиль VPN для устройства. В отличие от Пользовательского туннеля, который подключается только после входа пользователя на устройство, Device Tunnel позволяет VPN установить подключение до входа пользователя. И Device Tunnel, и User Tunnel работают независимо со своими профилями VPN, могут быть подключены одновременно и могут использовать различные методы проверки подлинности и другие параметры конфигурации VPN соответствующим образом.

Прямой доступ (DirectAccess)

- DirectAccess позволяет удаленным пользователям подключаться к сетевым ресурсам организации без необходимости использования традиционных подключений к виртуальной частной сети (VPN).

- Благодаря подключениям DirectAccess удаленные устройства всегда подключены к организации, и удаленным пользователям не нужно запускать и останавливать подключения.

Служба файлов SMB

- Шифрование SMB обеспечивает сквозное шифрование данных SMB и защищает данные от прослушивания во внутренних сетях. В Windows 11 протокол SMB содержит значительные обновления безопасности, включая 256-битное шифрование AES, ускоренную подпись SMB, сетевое шифрование с удаленным доступом к памяти каталогов (RDMA) и SMB через QUIC для ненадежных сетей. В Windows 11 представлены криптографические наборы AES-256-GCM и AES-256-CCM для шифрования SMB 3.1.1. Администраторы Windows могут разрешить использование более продвинутой системы безопасности или продолжать использовать более совместимое и безопасное шифрование AES-128.

SMB Direct

- SMB Direct (SMB через удаленный прямой доступ к памяти) — это протокол хранилища, обеспечивающий прямую передачу данных из памяти в память между устройством и хранилищем с минимальной загрузкой ЦП при использовании стандартных сетевых адаптеров с поддержкой RDMA.

- SMB Direct поддерживает шифрование, и теперь вы можете работать так же безопасно, как и с традиционным TCP, и с производительностью RDMA. Ранее включение шифрования SMB отключало прямое размещение данных, делая RDMA таким же медленным, как TCP. Теперь данные шифруются перед размещением, что приводит к относительно незначительному снижению производительности при добавлении конфиденциальности пакетов AES-128 и AES-256.

Шифрование и защита данных

Управление BitLocker

- BitLocker CSP позволяет решению MDM, такому как Microsoft Intune, управлять функциями шифрования BitLocker на устройствах Windows. Сюда входят тома ОС, фиксированные диски и извлекаемое хранилище, а также управление ключами восстановления в Microsoft Entra id.

Включение BitLocker

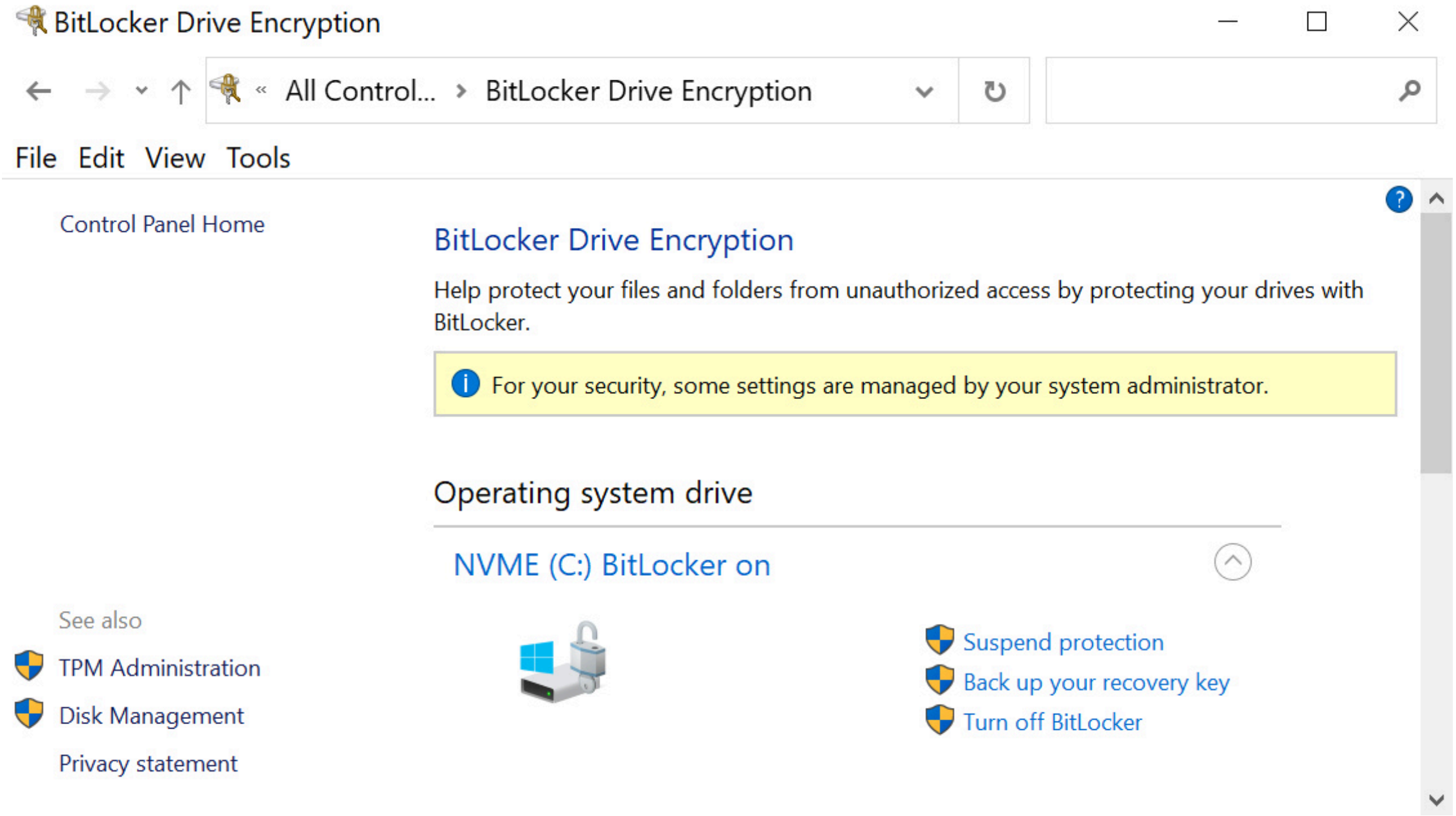
- **Шифрование диска BitLocker** — это функция защиты данных, которая интегрируется в операционную систему и предотвращает угрозы хищения данных или раскрытия информации на потерянных, украденных или неправильно выведенных из эксплуатации компьютерах. BitLocker использует алгоритм AES в режиме работы XTS или CBC с длиной ключа 128 или 256 бит для шифрования данных на томе. Облачное хранилище в Microsoft OneDrive или Azure можно использовать для сохранения содержимого ключа восстановления. BitLocker может управляться любым решением MDM, например Microsoft Intune, с помощью поставщика служб конфигурации (CSP).

- BitLocker обеспечивает шифрование для ОС, фиксированных данных и съемных дисков с данными, используя такие технологии, как интерфейс тестирования аппаратной безопасности (HSTI), современный режим ожидания, безопасная загрузка UEFI и TPM.

Зашифрованный жесткий диск

- Зашифрованные жесткие диски — это класс жестких дисков, которые самостоятельно шифруются на аппаратном уровне и обеспечивают полное аппаратное шифрование диска, будучи прозрачными для пользователя устройства. Эти диски объединяют преимущества безопасности и управления, предоставляемые BitLocker Drive Encryption, с мощностью дисков с самостоятельным шифрованием.

- Путем передачи криптографических операций в оборудование функция "Зашифрованный жесткий диск" повышает производительность BitLocker и снижает потребление ресурсов ЦП и электроэнергии. Поскольку зашифрованные жесткие диски быстро шифруют данные, развертывание BitLocker можно распространить на корпоративные устройства практически без влияния на производительность.


BitLocker Drive Encryption
All Control... › BitLocker Drive Encryption
File Edit View Tools
Control Panel Home
BitLocker Drive Encryption
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.
For your security, some settings are managed by your system administrator.
Operating system drive
NVME (C:) BitLocker on
Suspend protection
Back up your recovery key
Turn off BitLocker
See also
TPM Administration
Disk Management
Privacy statement

Шифрование персональных данных (PDE)

- Шифрование персональных данных (PDE) работает с BitLocker и Windows Hello для бизнеса для дополнительной защиты пользовательских документов и других файлов, в том числе когда устройство включено и заблокировано. Файлы шифруются автоматически и плавно, чтобы повысить безопасность пользователей, не прерывая их рабочий процесс.

- Windows Hello для бизнеса используется для защиты контейнера, в котором хранятся ключи шифрования, используемые PDE. При входе пользователя в систему контейнер проходит проверку подлинности, чтобы освободить ключи в контейнере для расшифровки содержимого пользователя.

Шифрование электронной почты (S/MIME)

- Шифрование электронной почты позволяет пользователям шифровать исходящие сообщения электронной почты и вложения, чтобы их могли прочитать только предполагаемые получатели с цифровым идентификатором (сертификатом). Пользователи могут подписать сообщение цифровой подписью, которое проверяет личность отправителя и подтверждает, что сообщение не было изменено. Зашифрованные сообщения могут быть отправлены пользователем другим пользователям в своей организации или внешним контактам, если у них есть соответствующие сертификаты шифрования.

Защита информации

Тема: Безопасность операционной системы Windows 11

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024