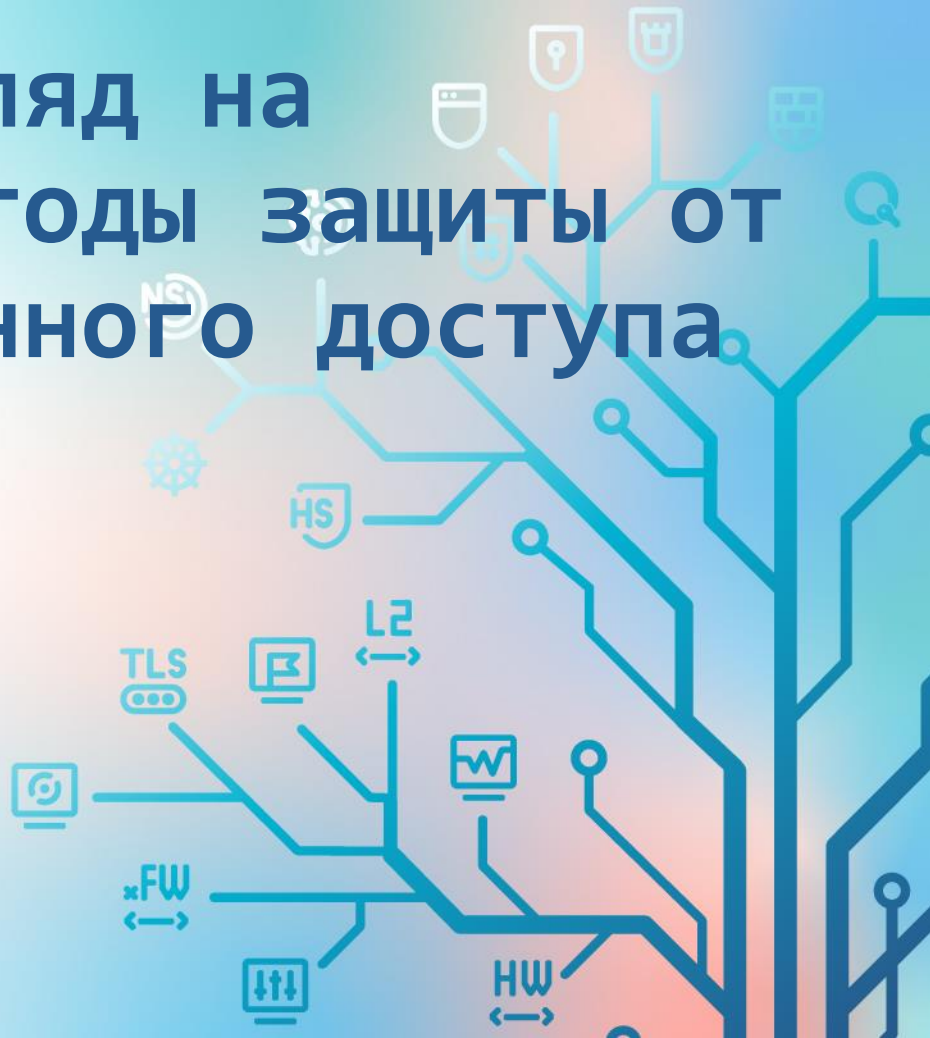
# Современный взгляд на классические методы защиты от несанкционированного доступа

**Иван Кадыков**
Руководитель направления

infotecs



# Потенциальный нарушитель

**«Классические» внутренние нарушители (инсайдеры)** - сотрудники, которые злоупотребляют своим законным доступом к конфиденциальным данным в корыстных целях

**Недовольные бывшие сотрудники** - которые хотят навредить своим работодателям

**Подкупленный сотрудник** – нанятый внешними компаниями для кражи, изменения или удаления конфиденциальных данных

**Безрассудные сотрудники** - тип инсайдеров, которые пренебрегают ИБ-политиками.

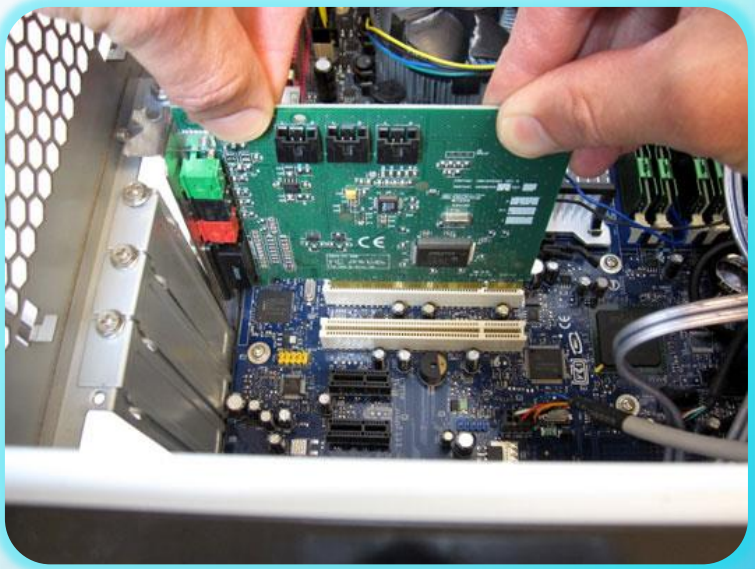
# Доверенная загрузка – первый и ключевой шаг к защите рабочих станций и серверов

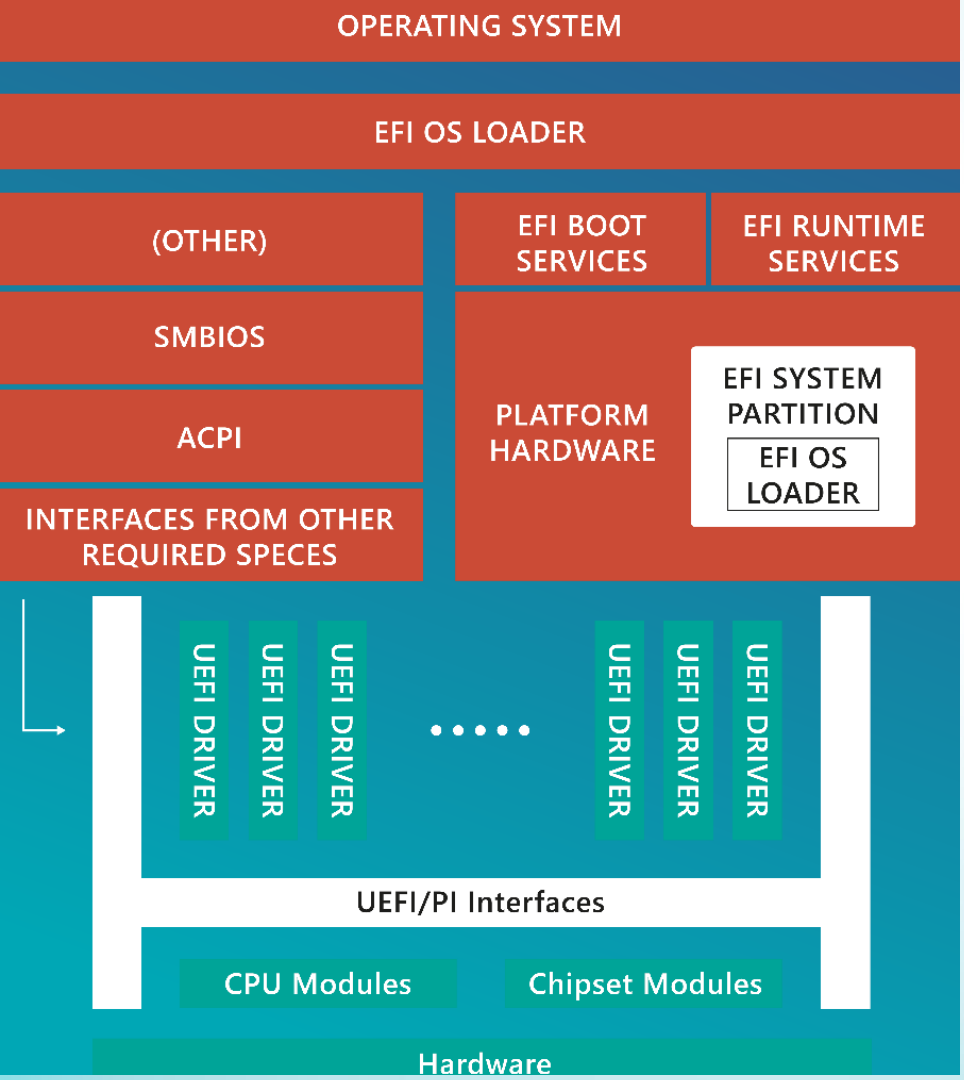
Все средства защиты установленные в ОС бессильны если:

- Любой пользователь может включить компьютер
- Получить доступ к UEFI BIOS
- Загрузить любую ОС с внешнего носителя

# Доверенная загрузка – «Старая школа»

| | |
|---|---|
| Ключевая задача | • Защита от внутренних нарушителей |
| Механизмы защиты | • Идентификация и аутентификация<br>• Контроль целостности программной среды<br>• Передача управления доверенному загрузчику |
| Исполнение | • Аппаратно-программное |






# Всё развивается и меняется

- На смену Legacy BIOS пришёл UEFI BIOS
- UEFI BIOS – «небольшая ОС»
- В UEFI BIOS можно загружать и выполнять произвольный код

# Доверенная загрузка – «Новая школа»

| | |
|---|---|
| Ключевая задача | • Защита от внутренних нарушителей<br>• Защита от внешних нарушителей<br>• Защита платформы от стороннего воздействия в процессе «цепочки поставки» |
| Механизмы защиты | • Идентификация и аутентификация<br>• Контроль целостности программной среды<br>• Передача управления доверенному загрузчику и контроль SecureBoot<br>• Защита UEFI BIOS от попадания стороннего кода<br>• Контроль и блокировка специфичных для UEFI объектов (NVRAM-переменные, ACPI-таблиц WPBT, Контроль программных SMI, прямая запись на HDD из BIOS) |
| Исполнение | • Программное |

# ViPNet SafeBoot 3

**Новое поколение высокотехнологичного программного модуля доверенной загрузки (ПМДЗ).**

Предназначен для создания точки доверия к платформе и её компонентам, а также к загружаемой операционной системе.

Ключевыми задачами продукта являются разграничение доступа к платформе, защита UEFI BIOS, контроль неизменности и защита компонентов ПК, а также организация доверенной загрузки штатной операционной системы.

# Доверие и защита платформы

- Защита UEFI BIOS
  - защиту BIOS от перезаписи, чтения и от изменений EFI-переменных
  - защита после S3 - защита при выходе из спящего режима
  - Блокировка обновлений UEFI BIOS
  - Фильтрация и контроль программных SMI
- Защита от malware
  - Блокировка ACPI WPBT, защита системных таблиц
  - Защита дисков от записи
  - Блокировка UEFI Option Rom
- Эмуляция NVRAM

# Использование СЗИ от НСД для решения современных задач информационной безопасности

# ViPNet SafePoint

**ViPNet SafePoint – сертифицированный программный комплекс защиты информации от несанкционированного доступа уровня ядра операционной системы (ОС).**

ViPNet SafePoint устанавливается на рабочие станции и сервера в целях обеспечения мандатного и дискреционного разграничения доступа пользователей к критически важной информации и подключаемым устройствам.

# Ключевой набор функциональности для СЗИ от НСД

- Идентификация и аутентификация пользователей
- Дискреционная модель доступа (контроль доступа к файлам, реестру, процессам, службам)
- Замкнутая программная среда
- Контроль целостности
- Контроль времени работы
- Контроль подключения съемных носителей
- Мандатный контроль доступа

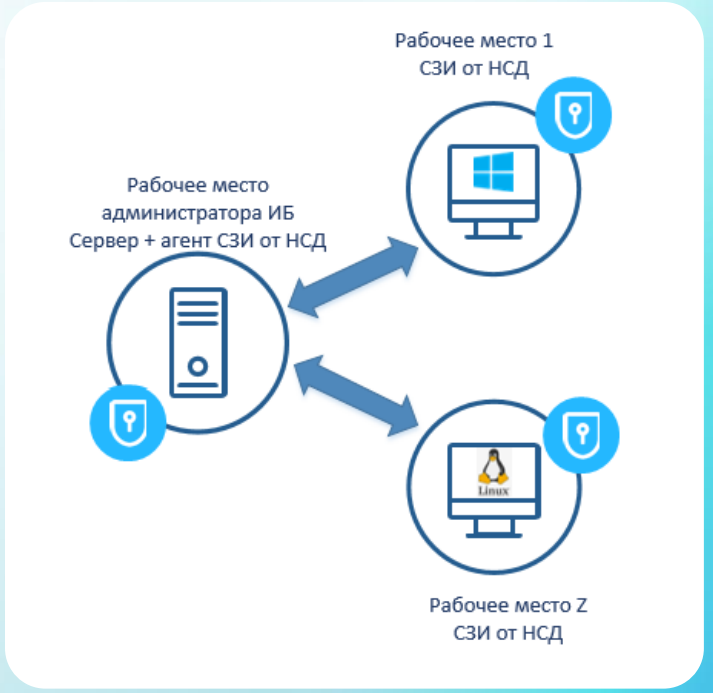
# Управление привилегированными пользователями

В СЗИ от НСД – реализована защита и контроль непосредственно на хостах.

Субъекта доступа формируется из трёх сущностей

- исходный идентификатор пользователя SID
- эффективный идентификатор пользователя (контекст безопасности (маркер-token) процесса при доступе )
- «полнопутевое» имя процесса (имя исполняемого файла процесса)

*PIM/PAM/PUM – контролируют подключение привилегированными пользователями к целевым системам и их работу только в соответствующих сессиях



# Защита от появления и исполнения зловредных программ

За счёт функции «Контроль доступа к файлам» можно создать политику:

- Файлы с расширением *.exe, *.bat, *.js и т.д. может создавать только администратор

За счёт функции «Контроль доступа к объектам реестра» можно создать политику:

- Доступ к настройке служб в реестре ОС разрешен только администратору (HKLM\SYSTEM*ControlSet*\services*)

ViPNet SafePoint предотвращает такие попытки для пользователя с фиксацией информации в журнале аудита

# Защита от действий «неопытного» пользователя

Запрет запуск приложений, скриптов из писем (защита от фишинговых атак по почте). Переход по нежелательным ссылкам

Как реализовать:

- запрет запуска, приложений из почтового клиента Outlook (кроме, например, Word, Excel, Acrobat Reader). Дополнительно политика на запрет запуска приложений, скриптов из Word, Excel, Reader.
- Запуск файла из почты порождает процесс, этому процессу запрещено обращаться к ранее созданным размеченным файлам.

# Контроль подключения съемных носителей

Возможность использования только определённых (зарегистрированных) съемных устройств

Контроль копирования информации на съёмные носители (фиксация событий в журнале аудита)

Защита от запуска программ и скриптов с внешних накопителей

# «Классические механизмы» для современных проблем

- Защита от внедрения и выполнения вредоносных программ и кода
- Защита от атак на повышение привилегий
- Защита данных от атак на уязвимости системного ПО
- Защита от инсайдеров
- Защита данных от атак на уязвимости прикладного ПО

Подписывайтесь
на наши соцсети,
там много интересного

infotecs

Спасибо за внимание!