Технологии QNX и КПДА в России

Москва, 13 апреля 2017

«Аппаратно-программный комплекс доверенной загрузки "Тверца Зетта-М" и его интеграция с ЗОСРВ «Нейтрино»

Андрей Сазонов, ЗАО НИИ ЦПС

СВД Встраиваемые Системы

Работа без модуля доверенной загрузки

Отсутствие контроля доступа к загрузке ОС	Возможность загрузки ОС в нештатном режиме	Возможность загрузки ОС с нештатного носителя
• Получение доступа к предоставляемым ЭВМ сервисам в нештатное время	• Нарушение функционирования штатного ПО • Предоставление пользователю непредусмотренных возможностей	• Запуск программных закладок (например, гипервизора) с последующей загрузкой штатной ОС • Модификация штатных ОС и ПО • Доступ к данным в обход механизмов защиты уровня ОС

Нужен модуль доверенной загрузки!

Аппаратно-программный комплекс доверенной загрузки «Тверца Зетта-М»

- Разработка ЗАО НИИ ЦПС, г. Тверь
- Предназначен для обеспечения доверенной загрузки ОС, а также выполнения функций защиты информации без загрузки ОС либо в ходе работы ОС.
- Поставляется в составе аппаратно-программного комплекса защиты информации (АПКЗИ) «Ребус-М»

АПКДЗ «Тверца Зетта-М»
Состав

Аппаратные идентификаторы

Контроллеры СЗИ

- СЗИ8, СЗИ8А PCI «Тверца-2»
- СЗИ10, СЗИ12 PCI Express «Тверца-2»
- СЗИ13 mini PCI Express «Тверца-2»
- СЗИ14 mini PCI Express Half Size «Тверца-2»

АПКДЗ «Тверца Зетта-М»
Состав

Программное обеспечение

- Встроенное в контроллеры СЗИ8А, СЗИ12, СЗИ13
- Запускаемое с загрузочного дистрибутивного CD
- Устанавливаемое в ОС Windows, МСВС

- Администрирование контроллера
- Контроль целостности файлов
- Маскирующее удаление информации на диске
- Резервное копирование и восстановление разделов диска

АПКДЗ «Тверца Зетта-М»
Основные функции контроллера

- запрет загрузки со сторонних носителей (для непривилегированных пользователей)
- блокировка клавиатуры до загрузки ОС (для непривилегированных пользователей)
- идентификация и аутентификация пользователей до загрузки ОС
- поддержка аппаратных идентификаторов (iButton, брелок-идентификатор И-1)
- регистрация событий доступа и попыток несанкционированного доступа
- регистрация изъятия контроллера из ЭВМ
- блокировка доступа к ЭВМ непривилегированных пользователей при попытках НСД

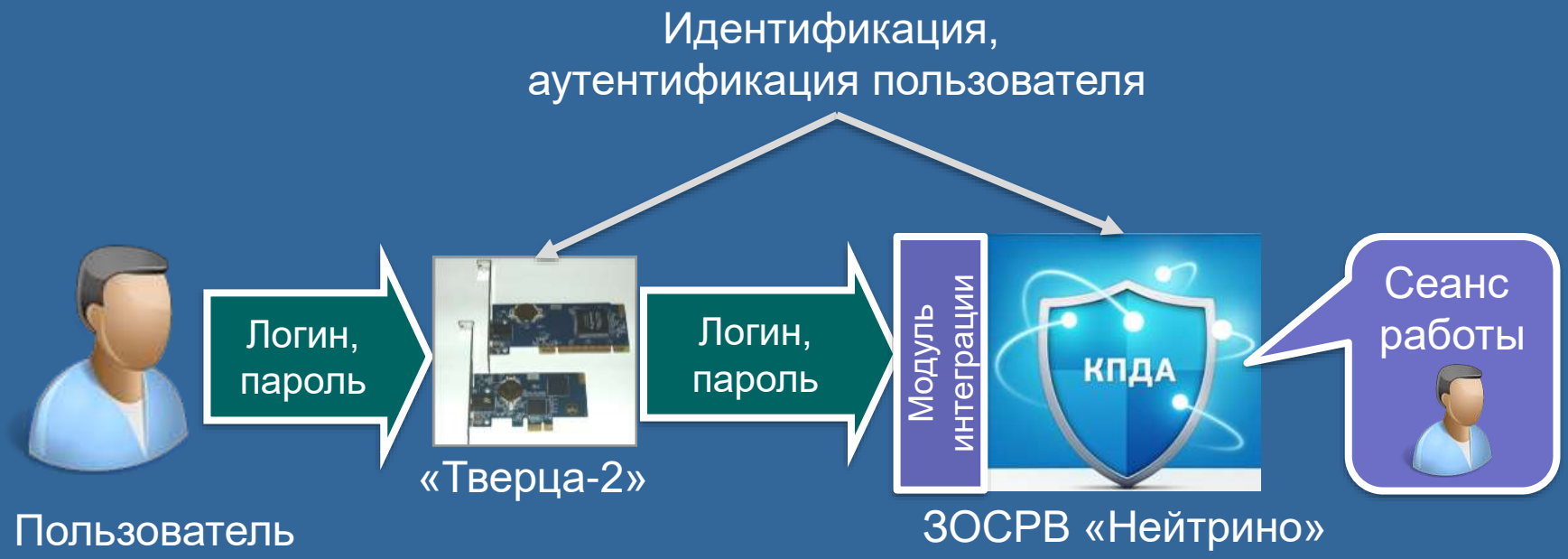
Работа с автономным модулем доверенной загрузки

Отсутствие взаимодействия механизмов защиты МДЗ и ОС	Усложнение работы
• Двойные идентификация и аутентификация пользователей • Двойное администрирование • Двойной аудит	• Непривилегированного пользователя • Администратора безопасности

Нужна интеграция механизмов защиты МДЗ и ОС!

Интеграция ЗОСРВ «Нейтрино» и контроллера «Тверца-2»

Сквозные идентификация и аутентификация



- Пользователь вводит логин и пароль один раз, до загрузки ОС
- ОС использует учётные данные из контроллера для запуска сеанса работы

Интеграция ЗОСРВ «Нейтрино» и контроллера «Тверца-2»

Единая настройка пользователей

- Администратор создаёт/редактирует учётную запись пользователя в одном месте
- Учётные данные пользователей автоматически записываются в контроллер

Интеграция ЗОСРВ «Нейтрино» и контроллера «Тверца-2»

Единый аудит

- События аудита контроллера сохраняются в журнал аудита ОС
- Администратору доступна единая цельная картина происходящего в системе

Результаты интеграции

Увеличение цепочки доверия

- Контроль доступа к загрузке ОС
- Предотвращение вмешательства в процесс загрузки ОС
- Предотвращение обхода механизмов защиты ОС

Упрощение работы пользователя

- Сквозные идентификация и аутентификация

Повышение эффективности администрирования

- Единая настройка пользователей
- Единый аудит

Спасибо за внимание!