s·terra

c s p

Доверенный сеанс: позиционирование технологий

Рябко С.Д., генеральный директор ЗАО «С-Терра СиЭсПи», к.ф.-м.н.

Доклад на XV конференции «РусКрипто'2013», 29 марта 2013 г.

Две проблемы

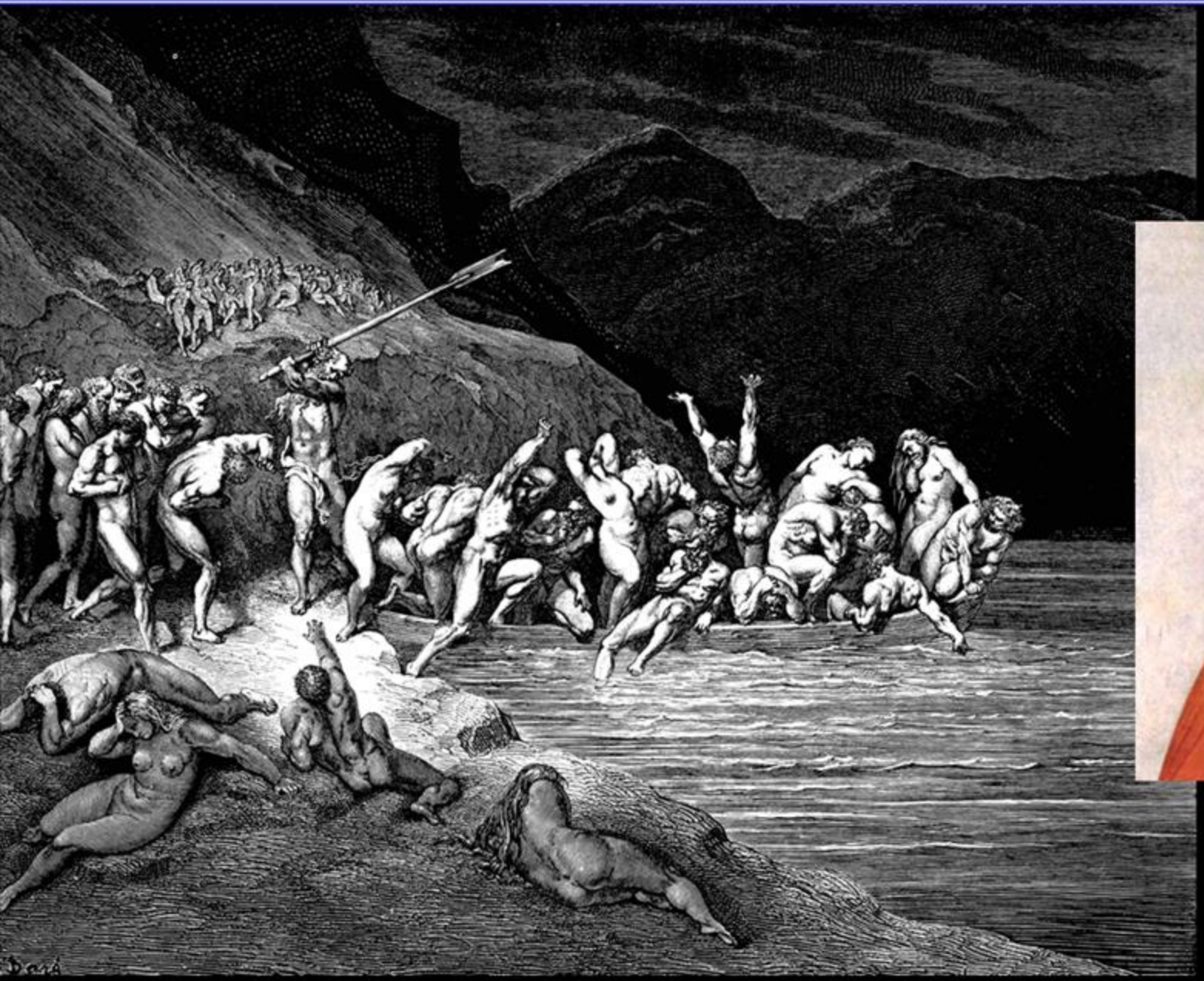
2026: сингулярность Вернора Винджа

Защита отстает от прогресса техники

- Реальные деньги в Сети порождают атаки на перехват управления в защищенных системах
- Прогрессивное развитие кибероружия и включение государств в гонку кибервооружений
- Глобализация и глобальная потеря контроля над производством ИКТ
- BIOS/EFI руткиты
- Технологии виртуализации процессорных ресурсов

Понимание того, что мы не можем доверять традиционным технологиям защиты, охватывает все большее число специалистов…

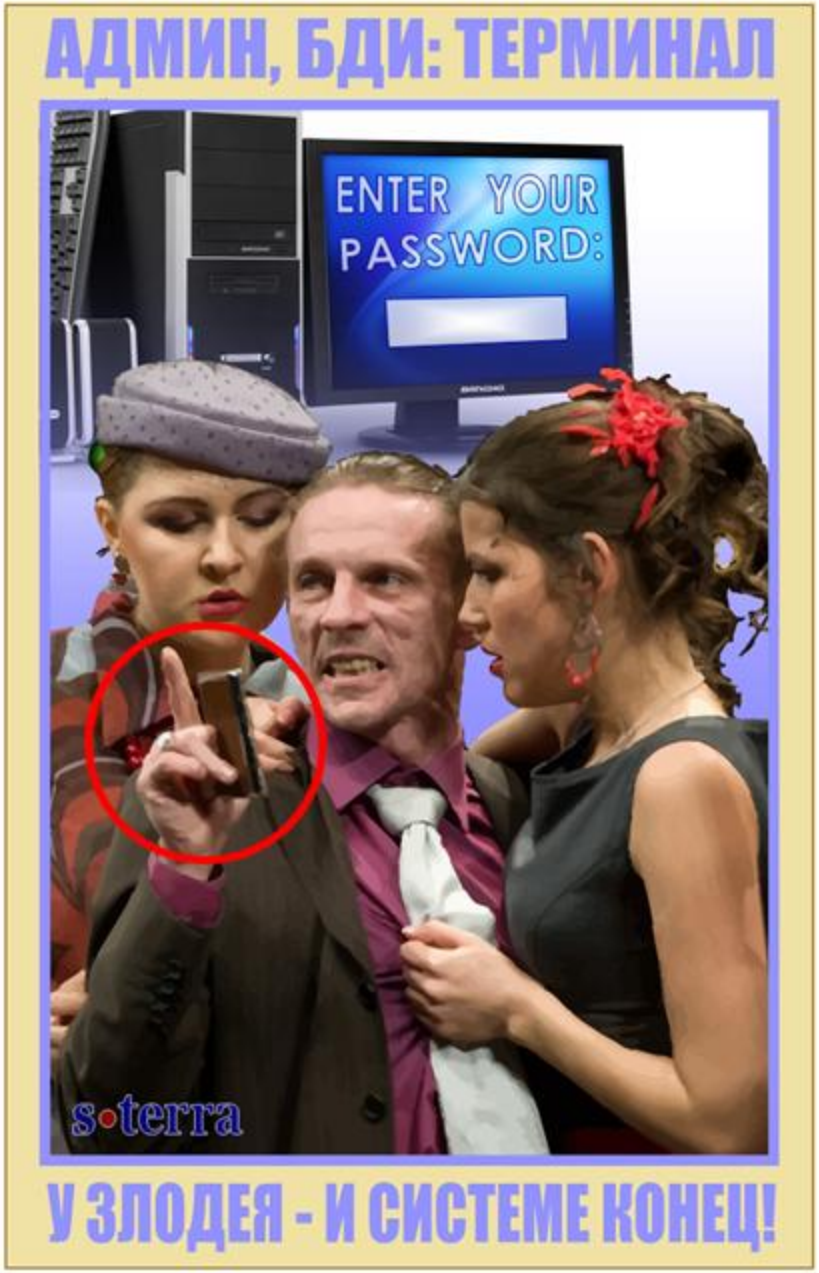
Il mal seme d'Adamo



Человечество в массе не квалифицировано

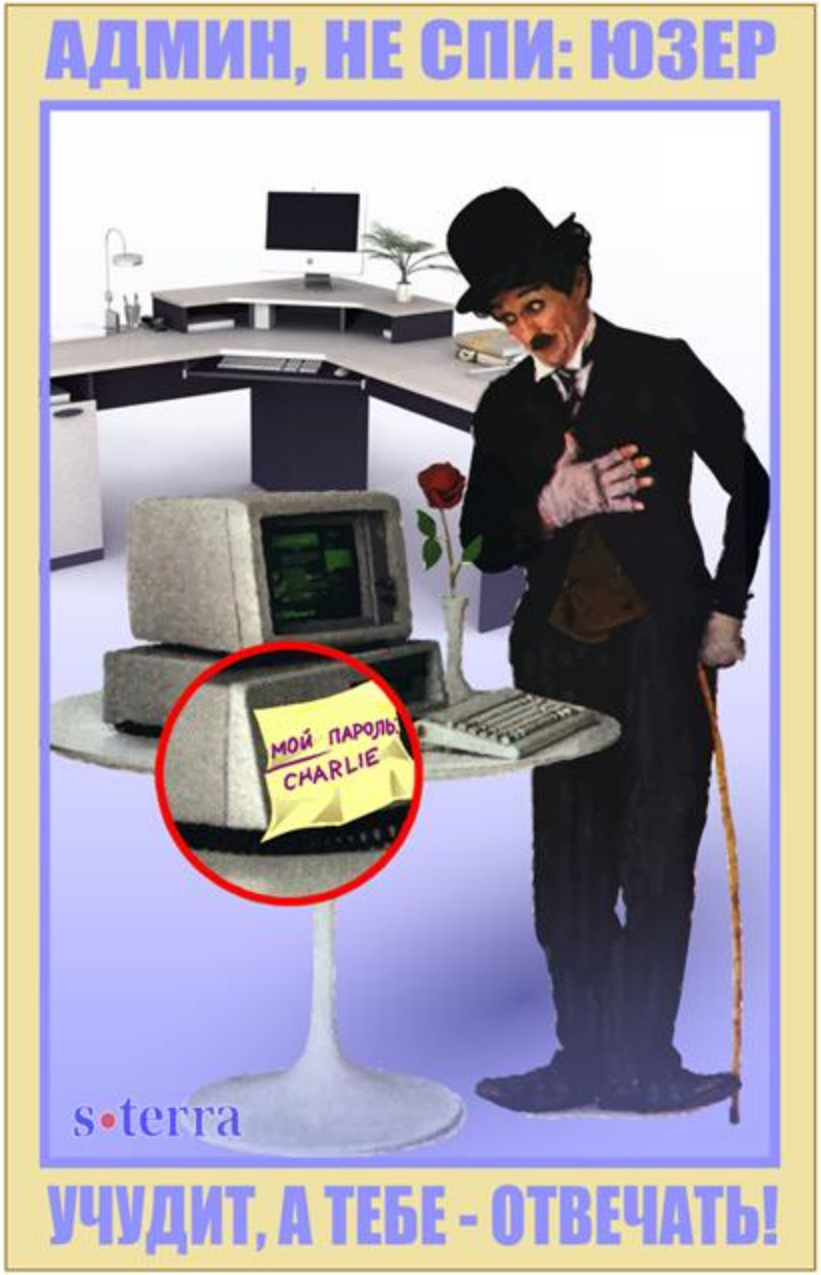
- Решение по информационной безопасности в идеале не должно требовать от пользователя каких либо компетенций, дополнительных к его повседневным навыкам
- Решение должно быть устойчиво к несанкционированному изменению конфигурации защиты, наличию уязвимостей или опасного кода на рабочем месте некомпетентного пользователя

Пользователь – главная уязвимость



- Непрофессионал простодушен, мошенник – изощренно коварен и работает по действенному, продуманному плану
- Большинство комплексных атак начинаются с атаки на пользователя (social engineering)

Пользователь не заслуживает полного доверия



- **Пользователь по ошибке, халатности или злому умыслу может неправильно использовать защиту и даже внести уязвимость в защищенную систему**

Мы не можем изменить природу человека.

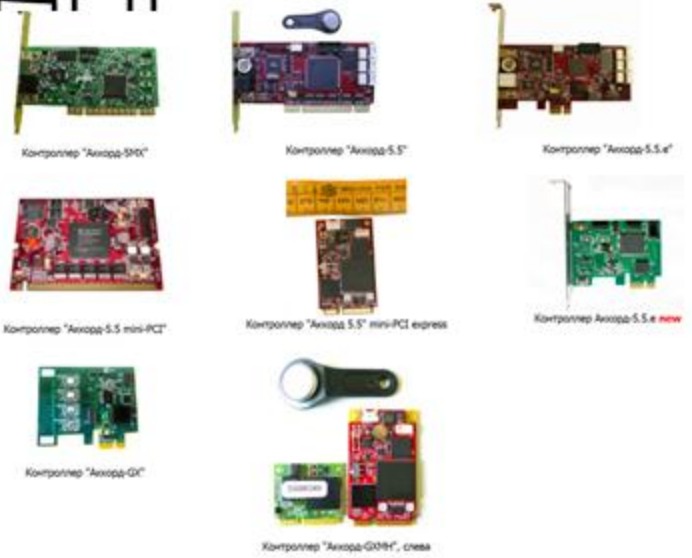
Поэтому корректно спроектированная система информационной безопасности должна сохранять свойства защиты даже в тех случаях, когда пользователь не заслуживает доверия, а его рабочее место не стерильно

Решения

s-terra
csp
Cisco Solution Technology Integrator

«Классический» АМДЗ

1994 ОКБ АПР



Код Безопасности
ГК «Информзащита»

ANGSTREM CUSTOM DESIGN LTD

- **Позиционирование от производителя:**
  - Защита от НСД к ПЭВМ (в т.ч. по расписанию)
  - Аутентификация оператора до загрузки ОС
  - Аппаратный контроль целостности файлов и доверенная загрузка ОС
  - Целостность данных
  - Контроль доступа к процессам, данным, периферии
  - Индивидуальная изолированная программная среда
  - Дополняется криптографическими функциями: ДСЧ, ЭЦП и проч.
- **Pro:**
  - Отработанная технология
  - Сертификация и рекомендации регуляторов
  - Развитая функциональность (диверсификация по продуктам)
  - Наличие независимого питания и процессора позволяет осуществить «внешний» контроль по отношению к АРМ
- **Contra:**
  - Злоумышленник с отверткой может вынуть замок
  - Установить можно далеко не везде
  - Проблемы совместимости с некоторой периферией
  - Не исключено вирусопоражение, теоретически хитрый руткит или malware applet может «обмануть» устройство

МДЗ-ЭШЕЛОН

2008 Эшелон
комплексная безопасность

- **Позиционирование от производителя :**
  - Доверенная загрузка тонкого клиента, контроль целостности, идентификация и аутентификация пользователя до передачи управления операционной системе
- **Концепция продукта:**
  - «программный замок» в BIOS + загрузчик на жестком диске
  - позволяет загружать любую ОС, установленную на отдельный раздел жесткого диска, включая МСВС и Windows (QNX, Linux, WinCE с boot-сектором, FreeBSD)
- **Pro (по представлению производителя):**
  - программная реализация, не требующая аппаратных средств
  - первое средство защиты виртуальных машин
  - единственное на рынке средство доверенной загрузки, позволяющее противостоять атакам, направленным на модификацию BIOS
  - экономичность, связанная с отсутствием аппаратных компонентов
- **Contra:**
  - Трудоемкий процесс встраивания в новые платформы
  - Ограниченный набор поддерживаемых платформ

Программный «АМДЗ» Аладдин TSM

2010
Аладдин РД

kraftway
ТЕХНОЛОГИИ ДЛЯ ЛЮДЕЙ

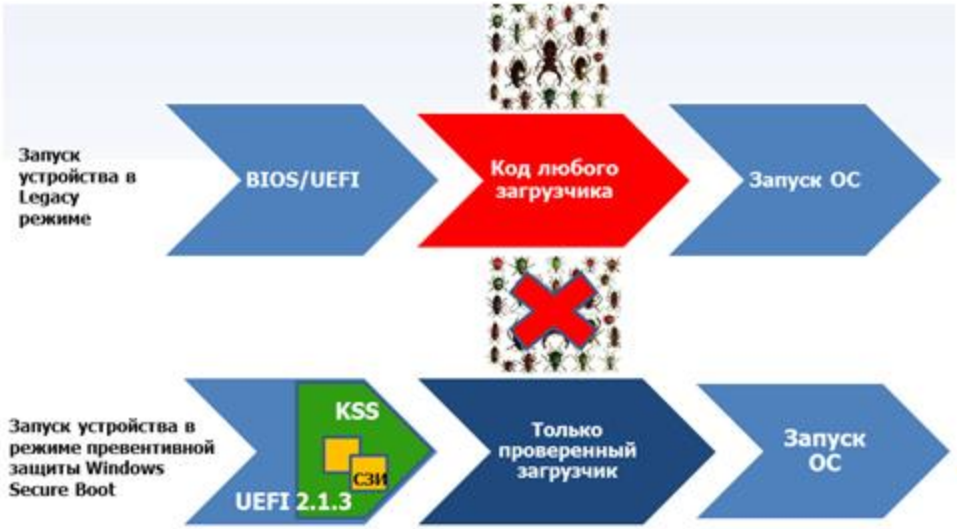
FUJITSU

- Позиционирование от производителя (продукт Aladdin TSM, Trusted Security Module):
  - Практически вся базовая функциональность АМДЗ
- Pro (по представлению производителя):
  - Защита от руткитов и виртуальных гипервизоров
  - Невозможность извлечения TSM, защита BIOS от перезаписи и сброса настроек
- Contra:
  - Трудоемкий процесс встраивания в новые платформы
  - Затруднения при модернизации, техобслуживании и ремонте
  - «Контроль машины со стороны себя самой», возможность для злоумышленника безнаказанно повторять попытки логина
  - Ограничения пространства BIOS для реализации функциональности АМДЗ

Технология Kraftway Secure Shell

2010

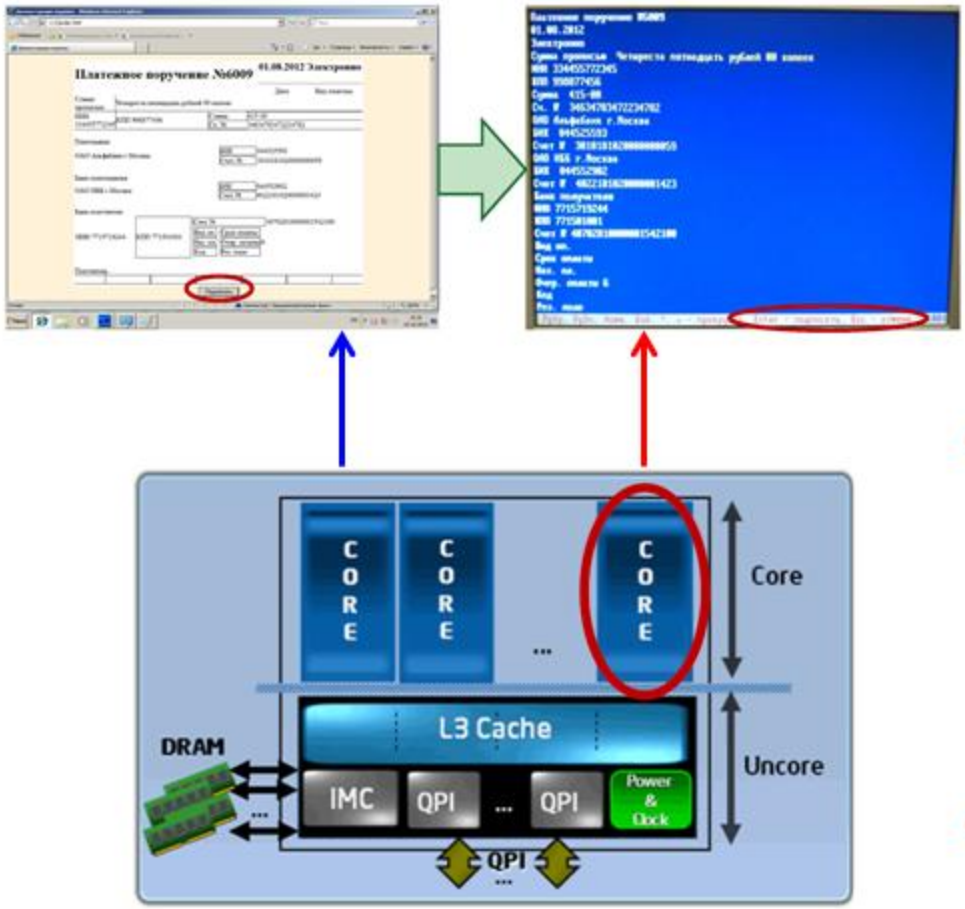
kraftway®
ТЕХНОЛОГИИ ДЛЯ ЛЮДЕЙ



- Развитие программных замков
- Pro:
  - Исключение области содержащей модули безопасности из общего адресного пространства (после загрузки ос нет доступа)
  - Запуск СЗИ НСД до запуска функции поиска загрузочного устройства
  - Контроль состава оборудования (аппаратная целостность)
  - Контроль программной среды
  - Интегрированный сторожевой таймер
  - Инфраструктура и расширяемость оболочки KSS
- Contra:
  - Трудоемкий процесс встраивания в новые платформы
  - Ограничения пространства BIOS для реализации функциональности АМДЗ
  - Ограниченный состав платформ

Технология Jinn, «Код Безопасности»

2012
Код Безопасности
ГК «Информзащита»



- **Доверенная визуализация и электронная подпись документов**
- **Концепция продукта:**
  - Изоляция доверенного процесса на одном из ядер многоядерного процессора
  - *«Как это происходит – это ноу-хау ООО «Код безопасности». Jinn не использует виртуализацию и технологии гипервизоров, также он не использует оперативную память, только в качестве обмена данными между клиентской операционной системой и доверенной средой. Подтверждением безопасности и защищенности доверенной среды Jinn служит сертификат ФСБ на СКЗИ КС2»**

  *) Цитата из руководства пользователя СКЗИ Jinn-Client 1.0.
- **Pro:**
  - Доверенная среда для просмотра и подписи документа непосредственно на компьютере пользователя без дополнительных устройств
  - Микрокод доверенной среды и ключи пользователей хранятся в памяти выделенных ядер процессора
  - Простота встраивания в уже функционирующие системы
- **Contra:**
  - Ориентация на ЭП, комплексную функциональность защиты нужно обеспечивать отдельными мерами защиты в составе основного АРМ

Традиционный токен

1999
Аладдин РД

2002
Компания Актив

- Позиционирование от производителя
  - Двухфакторная аутентификация
  - Контроль доступа
  - Single Sign On
  - Ключевой носитель
  - Встраивание в инфраструктуры аутентификации, ключевого управления, приложения
- Pro:
  - Распространенная технология, готовые инфраструктуры
  - Стойкая аутентификация, стойкое хранилище ключа, неизвлекаемость ключа
  - Расширяемость: RFID, OTP, Java
- Contra:
  - Несамостоятельность (компонентность) решения: нужна внешняя криптобиблиотека и совместимое ПО
  - Нестойкость по отношению к руткитам и прочим атакам на перехват управления АРМ (главный способ взлома ДБО на сегодня)

Java-токены и Java-карты

Аладдин РД

- Производитель: «Аладдин РД» (eToken PRO/Java, eToken NG-FLASH/Java, eToken NG-OTP/Java), вдогонку работает «Актив» (ruToken с КриптоПро JSP)
- Pro (по представлению производителя):
  - Расширяемость функциональности за счет Java-апплетов
  - Гибкость (свободная замена апплетов и их централизованное распространение)
  - Отсутствие целевого ПО на рабочем месте оператора
  - Доверие к мобильным компонентам ПО: проверка подписей апплетов
- Contra:
  - Ограниченные возможности встроенной Java-машины, некоторые ограничения функциональности
  - Смарт-карта зарубежного производства
  - Нестойкость по отношению к «загрязнению» рабочей среды оператора (вирусы, руткиты, виртуализация BIOS)

«СПДС» на основе eToken NG Flash

2008
Аладдин РД
Алмитек
s•terra csp

- Первая попытка обеспечения доверенного сеанса (2008 год) на основе целостной информационной среды, загружаемой с USB-носителя
- Решение: загрузка виртуальной машины из области защищенной флэш-памяти
- Операционные системы: Windows XP, Windows XP embedded, Linux

- Проект не был завершен из-за ряда нерешенных технических и сертификационных проблем

Abra (Check Point)

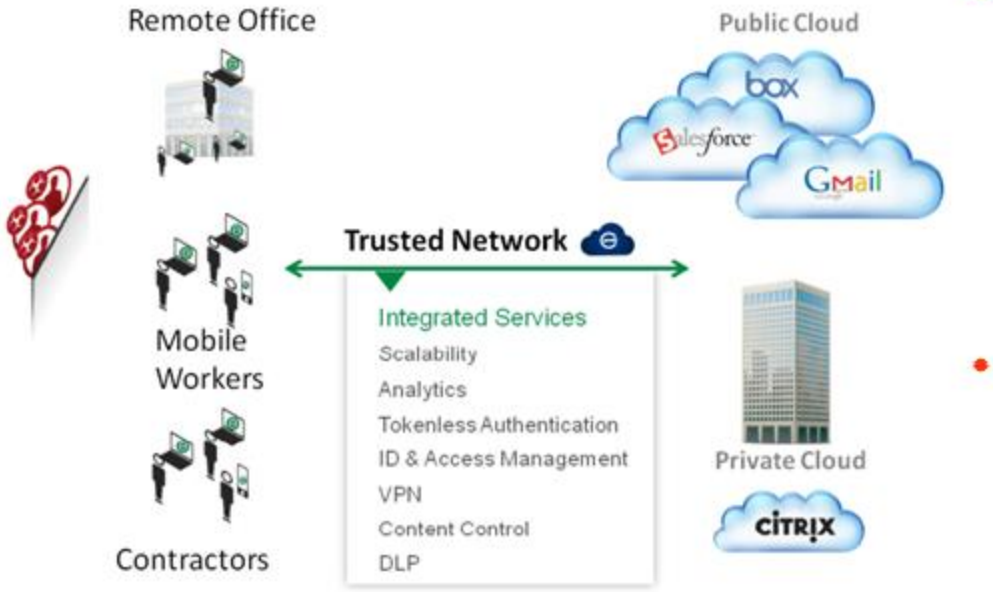
2010

Check Point
SOFTWARE TECHNOLOGIES LTD.

- Производитель: Check Point Software Technologies
- Концепция продукта:
  - «Офис в кармане»
  - Загрузка доверенный компонентов рабочего места оператора в виртуальную среду (гипервизор), содержащийся на носителе
  - Шифрование данных на носителе
- Pro:
  - Удобство, функциональность
  - Контроль доступа между материнской машиной и виртуальной защищенной средой
  - Доверие к целостным компонентам материнской среды
  - Отсутствие необходимости покупки дополнительных лицензий на ПО
- Contra:
  - Сомнения в изоляции виртуальной среды, потенциальная нестойкость к атакам из материнкой ОС
  - Весьма смутные перспективы сертификации СФК СКЗИ

Trusted Access (Iron Key)

2010 IRONKEY



The Trusted Network integrates a growing set of cloud services to simplify IT and reduce the cost of managing the extended enterprise.

- **Производитель: Iron Key, ведущий производитель защищенных USB-носителей**
- **Концепция продукта:**
  - Как и Check Point Abra, базируется на виртуализации (механизмы не ясны)
  - В отличие от Abra – доверенный сеанс
  - Основывается на веб-приложениях
  - Защита соединений (Cisco IPsec VPN)
  - Централизованное управление
  - Предложение облачной услуги
- **Pro:**
  - **Удобство, функциональность**
  - **Защищенная архитектура, read only data, шифрование диска, защита от key logger'ов**
- **Contra:**
  - **Виртуализация – не доказана стойкость к атакам из материнкой ОС**
  - **Нестойкость к загрузке BIOS-руткита**
  - **Полное отсутствие перспектив сертификации (хотя есть ironkey.ru)**
  - **Темный маркетинг, «trust me, it's secure»**

СПДС «Марш!», «ПОСТ»

2010

s·terra csp

ОКБ САПР

- Производители: «С-Терра» свой VPN на базе СЗН «Марш!», «ПОСТ», ОКБ САПР («Марш!», ОЕМ ряда поставщиков СКЗИ и VPN)
- Концепция продукта:
  - Защищенный носитель с загрузкой доверенной среды, СКЗИ, VPN
- Pro:
  - Защищенная архитектура
  - Гибкость (централизация вычислительных и информационных ресурсов), простота решения
  - Унификация рабочих мест и/или переносимость среды
  - Экономическая эффективность
  - Сервисопригодность
  - Централизация управления и эксплуатации
  - Сертификаты ФСБ и ФСТЭК России (с февраля 2011 года)
- Contra:
  - Требуются специальные меры защиты от виртуализации BIOS (требование ФСБ России)
  - Загрузка выделенного сеанса, несосуществование с другими процессами (материнская машина уходит в HIBERNATE)
  - Необходимость дополнительных мер защиты при организации файлового обмена
  - Необходимость интегрировать криптосреду и инфраструктуру приложений в соответствии с требованиями Заказчика

AppGate MOVE USB

2012 cryptzone

- MOVE: My Own Virtual Environment
- Концепция продукта:
  - Еще один безопасный офис в кармане
  - Защищенный носитель с загрузкой доверенной среды, СКЗИ, фиксированного состава приложений
- Pro:
  - Защищенная архитектура
  - Переносимость среды стандартных приложений
  - AppGate server
  - Аутертификация – различные способы и инфраструктуры (пароли, Cryptzone OTP, токены, SecurID, RADIUS)
    Межсетевой экран
- Contra:
  - Требуются специальные меры защиты от виртуализации BIOS
  - Ориентация на персональную безопасность профессионала, отсутствие средств интеграции в корпоративные информационные системы

АНКАДЕР

2013

- Персональное средство комплексной защиты конфиденциальной информации
- Концепция продукта:
  - USB-носитель с загрузкой доверенной среды, с защищенным носителем ключей. Возможно будет использовать как токен.
- Pro (заявлены производителем):
  - Строгая аутентификация
  - Возможность использования на любом компьютере
  - Встроенный контроль целостности доверенной среды
  - Электронная цифровая подпись
  - Невысокая стоимость
- Contra:
  - Продукт есть, но не доработан
  - При подключении к Windows-ПК позволяет записать данные в открытую область, не спрашивая права
  - Нет функционала VPN
  - Нет сетевых драйверов
  - Можно обойти контроль количества неправильных попыток ввода пароля пользователя

ruToken PINpad

2011

- PIN-pad'ы существуют очень давно для ввода PIN-кодов смарт-карт. Иные PIN-pad'ы совмещают также с защищенными дисками и прочей периферией. Продукт «ruToken PINpad» – это нечто большее
- Концепция продукта:
  - Доверенная среда для электронной подписи
  - «What you see – what you sing», неотчуждаемость подписываемого контекста от процесса подписи
- Pro:
  - Изолированная доверенная среда для просмотра и подписи документа
  - Применение защищенного сертифицированного ключевого носителя
  - Простота и удобство пользования
  - Качество и привлекательная цена изделия
- Contra:
  - Ориентация только на ЭЦП, более сложную функциональность (например, обеспечение конфиденциальности в недоверенной среде) нужно обеспечивать отдельными мерами защиты в составе основного АРМ
  - Трудности при работе с большими документами, возможность подсунуть из недоверенной среды на подпись не оригинальный, а «похожий» документ
  - Необходимость встраивания в клиентские приложения

Кард-ридер/трастскрин Safe Touch

2012 SafeTech
SAFETY TECHNOLOGIES

- Кард-ридер со встроенной визуализацией и функцией электронной подписи
- Концепция продукта:
  - применяется в качестве замены токену
  - криптографические алгоритмы реализуются средствами смарт-карты
  - пользователю предоставляется возможность визуального контроля целостности значимых полей документа (номер счета, сумма) документ не может быть подписан до момента физического нажатия на кнопку подтверждения транзакции
- Pro:
  - Простота встраивания в систему (драйверы на кард-ридер поставляются в комплекте ПО Windows)
  - Взаимозаменяемость смарт-карт, совместимость с сертифицированными ФСБ России смарт-картами
- Contra:
  - Решение неполное (нет собственной криптозащиты)
  - Для визуализации подписываемого документа необходимо произвести встраивание (производитель поставляет SDK)

Анализ

Модель угроз и эффективность защиты

Зона эффективного применения СЗИ

Phishing, social engineering

Несанкционированный доступ пользователя

Вирусы, malware, spyware

Zero Day exploit, кибероружие, криптоанализ

Загрузка недоверенной среды

Несанкционированная виртуализация, руткит-гипервизор

BIOS-руткит

Закладка от производителя

Закрытые технологии Intel, AMD, BIOS/UEFI

Верить в наше время нельзя никому

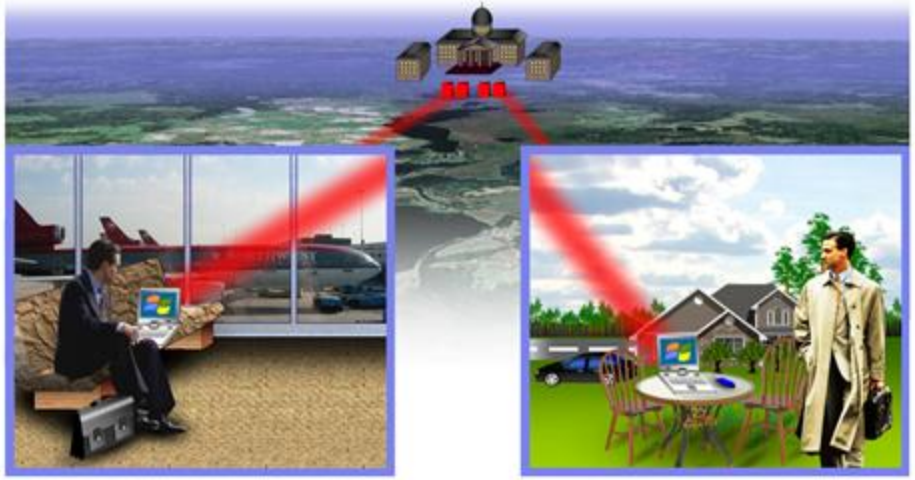
Продукт «ПОСТ»

s-terra
csp
Cisco Solution Technology Integrator

- Верить в наше время нельзя никому.

Мне – можно

Угрозы для систем удаленного доступа



- В современном мире при удаленном доступе пользователей администратор безопасности чувствует себя очень дискомфортно, поскольку ***вне контролируемой зоны все угрозы «человеческого фактора» многократно возрастают***

- Для решения этих проблем мы поставили перед собой ряд требований:
  - Обеспечить целостность программной среды терминала удаленного доступа в условиях эксплуатации нелояльным пользователем в «грязной», вирусопораженной среде
  - Обеспечить изоляцию вычислительного процесса клиента удаленного доступа при использовании «грязной» (недоверенной) среды
  - Обеспечить строгую двухфакторную аутентификацию пользователя, изоляцию сетевой среды, защиту потока пакетов от внедрения посторонних данных
  - Масштабируемость сети удаленного доступа до сотен тысяч пользователей
  - Применение сертифицированных средств криптографической защиты информации

Среда построения доверенного сеанса «Пост»

- Загрузка ОС АРМ осуществляется со съемного USB устройства СЗН «СПДС-USB-01»
  - на АРМ допустима неконтролируемая, не заслуживающая доверия среда, может отсутствовать как ОС, так и вообще жесткий диск
  - целостность среды функционирования пользователя обеспечивается
    - загрузкой эталонного ПО из защищенной области носителя
    - отсутствием записи в среду функционирования ПО
    - одноразовым использованием загруженного ПО
  - после загрузки ОС на АРМ пользователь имеет доступ только к одному приложению – терминалу или браузеру. Доступ в среду ОС и к другим приложениям запрещен
- VPN-клиент полностью исключает неконтролируемый доступ из сети в изолированную среду удаленного доступа
  - политика безопасности VPN-клиента устанавливает связь только с VPN-шлюзом центрального узла
  - для аутентификации пользователя при доступе к VPN-концентратору используются сертификаты X.509
  - ключи аутентификации хранятся в аппаратном криптографическом контейнере
- Особенности решения:
  - возможен удаленный доступ администратора к ОС, загруженной на АРМ
  - возможно автоматическое обновление сертификатов (отправка запроса, получения подписанного сертификата)

СПДС «ПОСТ», загрузочный носитель

Высокоскоростной интерфейс USB 2.0
обеспечивает лучшую в своем классе устройств на рынке скорость загрузки

Аппаратный токен для хранения критических объектов
российская схемотехника и карточная операционная система

Центральный процессор СЗН
обеспечивает контроль доступа к среде построения доверенного сеанса

Структурированная защищенная память СЗН
содержит разделы:

- **Носитель СЗН «СПДС-USB-01»**
- **Производитель: «С-Терра СиЭсПи»**
- **База производства: аттестованный для производства оборудования Cisco зеленоградский завод «Альтоника»**
- **Отличия:**
  - **Усовершенствован контроль доступа**
  - **Российский аппаратный токен**
  - **Более высокая скорость чтения**
  - **Параметризуемые области памяти**

СПДС «ПОСТ», СФК и приложения

Прикладное программное обеспечение

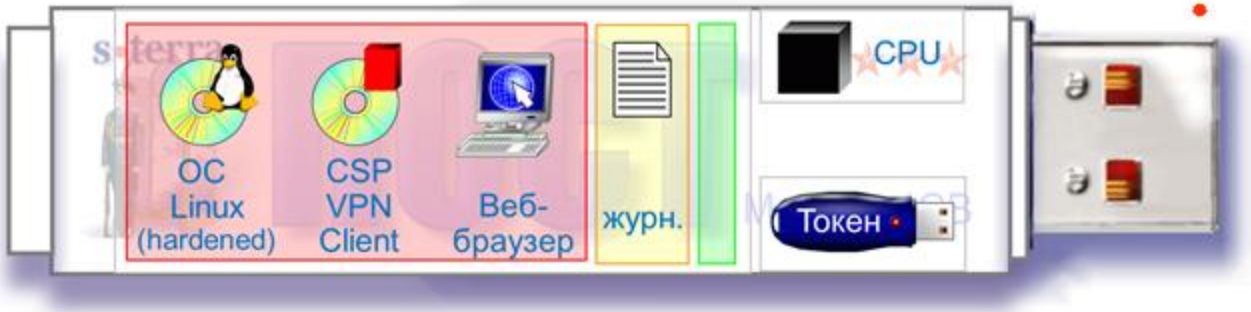
Среда функционирования (СФ) прикладного ПО

Модуль доверенной загрузки СФ

Специальный загрузочный носитель

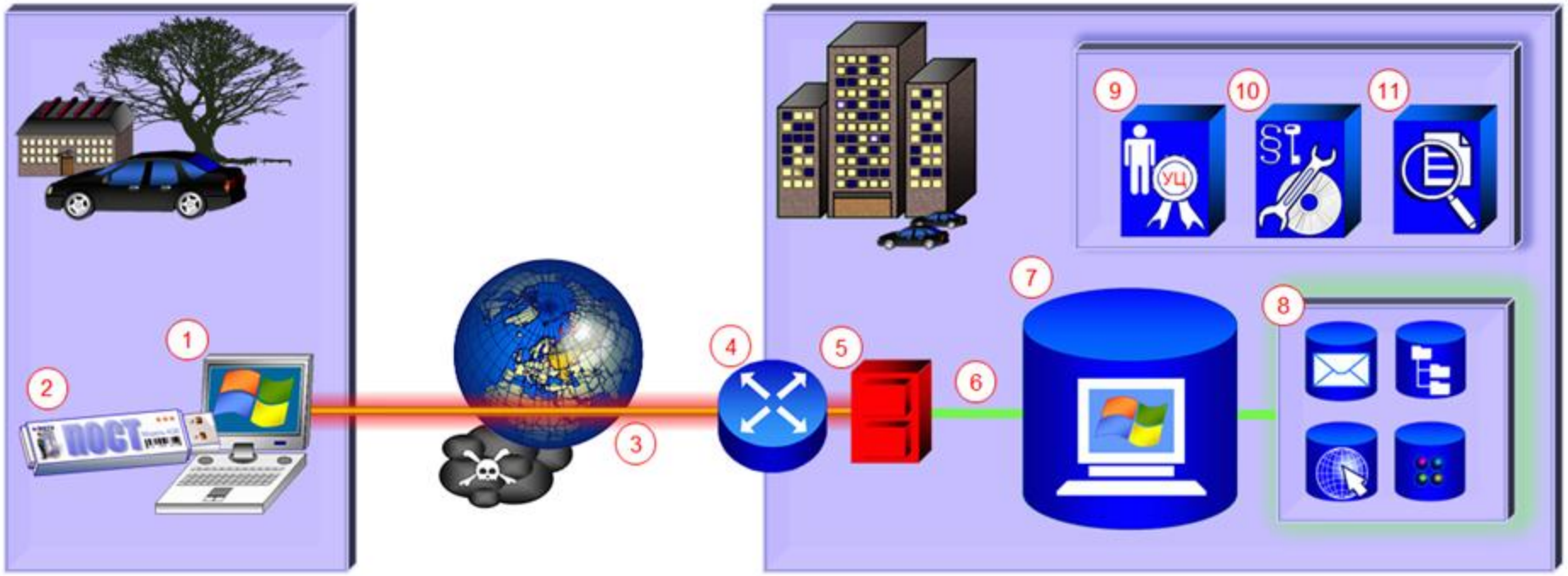
Состав ПО СПДС «Пост-Т», «Пост-W»

- В защищенной области памяти формируется целостная программная среда, включающая:
  1. Ограниченную ОС Linux
     - изъяты все ненужные и недоверенные сервисы
     - оболочка (shell) недоступна пользователю
  2. VPN-клиент полностью изолирует трафик из изолированной среды, исключает НСД из сети, поскольку не пропускает открытый IP-трафик
  3. Веб- или терминальный клиент (серии «W» и «T»)



- Целостность программной среды обеспечивается:
  1. запретом доступа любых процессов в область ROM
  2. однократной загрузкой одного и того же эталона среды в начале доверенного сеанса
  3. возможностью контроля хэш-суммы по коду доверенной среды (производится администратором)

Структурная схема решения



1. Рабочее место пользователя
2. СПДС «ПОСТ»
3. Защищенная терминальная сессия
4. Пограничный маршрутизатор
5. Кластер VPN-шлюзов
6. Терминальная сессия (открытый трафик)
7. Терминальный сервер
8. Опубликованные на терминальном сервере приложения (серверы)
9. Удостоверяющий центр
10. СИИТО
11. Система мониторинга и аудита

КОНТАКТЫ

e-mail: information@s-terra.com
web: http://www.s-terra.com/

Тел.: +7 (499) 940 9001
+7 (495) 726 9891
Факс: +7 (499) 720 6928

Вопросы?

Обращайтесь к нам!

s·terra
csp
Cisco Solution Technology Integrator