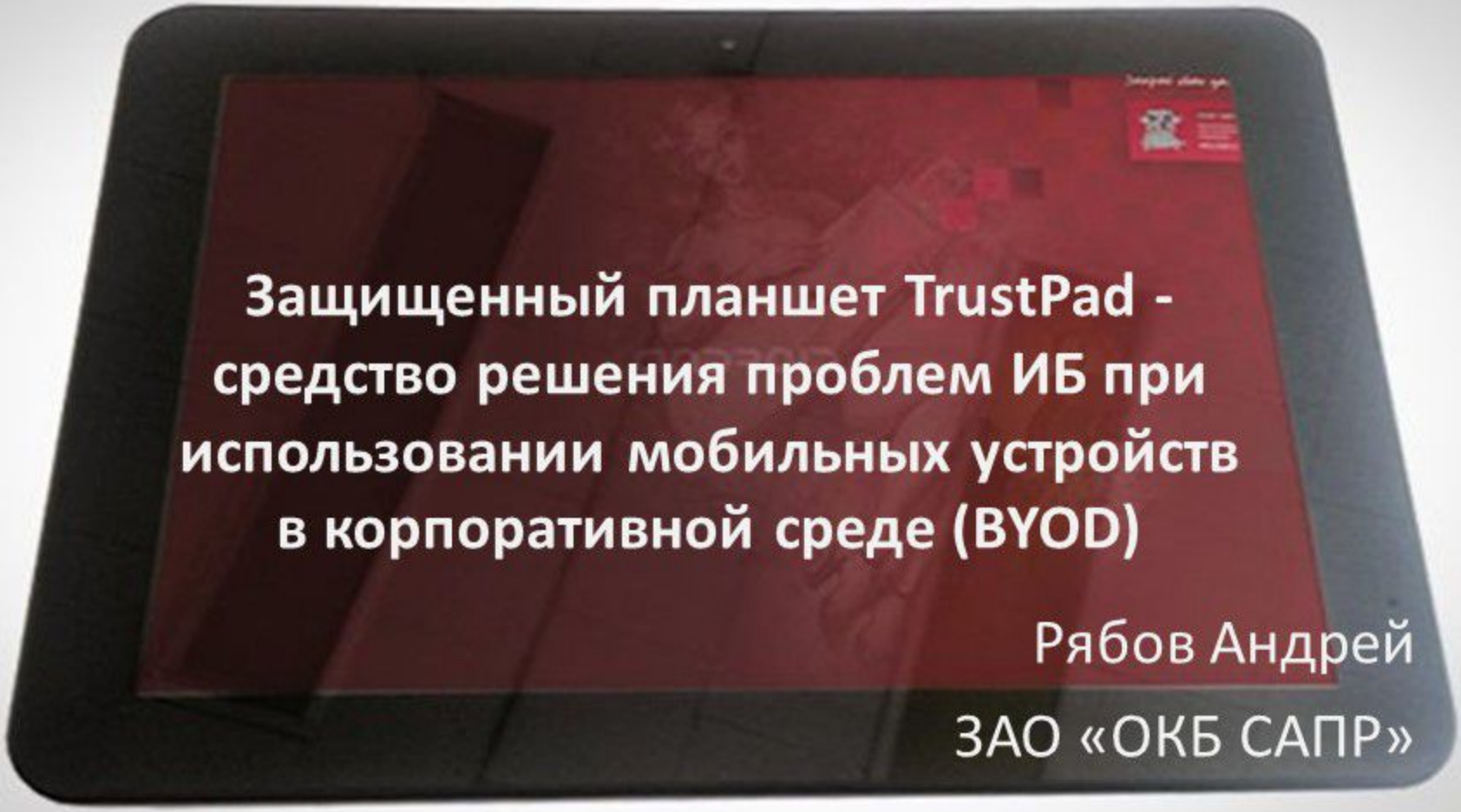

Защищенный планшет TrustPad - средство решения проблем ИБ при использовании мобильных устройств в корпоративной среде (BYOD)

Рябов Андрей

ЗАО «ОКБ САПР»

О чем сегодня пойдет речь?

1. Какие проблемы ИБ существуют при реализации концепции BYOD
2. Почему применение DLP и MDM недостаточно, чтобы контролировать мобильные устройства
3. «Серебряная пуля» - Корпоративный защищенный планшет (российская разработка, импортозамещение, сертифицирован во ФСТЭК)

Bring Your Own Device (BYOD)— «принеси свое устройство»

- Сотрудникам для выполнения служебных задач требуется удаленный доступ к корпоративным «облачным» ресурсам
- Для этого чаще всего работники используют личные мобильные устройства, например, планшеты.

Статистика из Oracle European BYOD Index Report:

В отчете приведены некоторые впечатляющие цифры:

- 44% (около половины) европейских компаний в настоящее время не одобряют концепцию BYOD или допускают ее применение лишь в исключительных обстоятельствах
- В 29% компаний устройства BYOD используются только руководителями
- В 22% компаний категорически запрещено размещение данных или информации на устройствах BYOD, а в 20% компаний нет никаких правил
- Более половины компаний не управляют смартфонами в рамках программы BYOD
- Безопасность информации является самой серьезной заботой — респонденты обеспокоены защитой устройств (45%), приложений (53%) и данных (63%)

Основные проблемы безопасности, возникающие при использовании BYOD

- Увеличение рисков утечки данных.
- Рост числа уязвимостей, которые может эксплуатировать злоумышленник
- Смешивание личных и бизнес-данных
- «Заражение» мобильных устройств вирусами, попадание вирусов в корпоративную сеть.
- Потеря или кража гаджета
- Разнообразие мобильных устройств не позволяет реализовать единый подход к безопасности.

Статистика: В половине (47%) компаний, разрешающих сотрудникам подключать свои персональные устройства к корпоративной сети, имели место случаи утечки конфиденциальной информации.

Все существующие решения и подходы сводятся к поиску компромисса между контролем со стороны работодателя и свободой для сотрудника

- Обеспечить максимальный контроль устройства, его среды и данных на нём, используя организационные меры и технические программные средства;
- Делегировать часть ответственности и обязанностей по обеспечению безопасности сотруднику;
- Проводить постоянное обучение сотрудников мерам безопасности;
- Грамотная многоуровневая организация системы безопасности инфраструктуры, к которой будет подключаться сотрудник.
- **Но! присутствует человеческий фактор…**

Почему применение DLP и MDM недостаточно, чтобы контролировать мобильные устройства

- Ключевая проблема безопасности BYOD сводиться **к невозможности** в рамках одного устройства (одной вычислительной среды) отделить **личное от рабочего**.
- С проявлением концепции BYOD многие разработчики ИБ-систем направили свои усилия на разработку решений для контроля мобильных устройств в корпоративной среде (решения класса MDM и DLP)
- **Но!** MDM и DLP «угрожает» приватности: «размывается» граница между работой и частной жизнью работника, т.к. эти системы отслеживают все действия на личном устройстве и считывают личные данные.
- **До какой степени ИТ-персонал контролирует мое устройство?**

Choose Your Own Device (CYOD)

- Ограничения концепции BYOD в сфере инфобезопасности может компенсировать ее последователь в корпоративной мобильности -- концепция Choose Your Own Device.
- В соответствии с концепцией CYOD (*дословный перевод: «выбери свое устройство»*) предприятие предоставляет своим сотрудникам те устройства, которые оно само приобрело

Концепция: Доверенный сеанс связи (ДСС) и Новая гарвардская архитектура

- Парадигма ДСС разработана и сформулирована вот уже почти как десятилетие назад
- Суть концепции ДСС заключается в том, что компьютер практически всегда используется в незащищенных сетях, и только иногда - в защищенных.

- «Новая Гарвардская» архитектура - ней используется память, для которой установлен режим «только чтение». При загрузке команды и данные размещаются в сеансовой памяти, в которой и исполняются.
- Новая архитектура характеризуется динамической изменяемостью, что обеспечивает защищенность и эффективность, неизменность операционной системы, «вирусный иммунитет». Она не мешает возможности применения адаптированных стандартных ОС и всего программного обеспечения, написанного для них.

Для корпоративного сектора нужны защищенные компьютеры планшетного типа:

- обладающие «вирусным иммунитетом»;
- позволяющие в защищенном режиме (в доверенной среде) работать с корпоративными «облачными» ресурсами;
- а также иметь возможность работать с ресурсами развлекательного характера, без каких- либо ограничений.

Сценарии применения TrusTPad

В незащищенном режиме:

- доступ к аудио и видео контенту с современным уровнем качества (потоковое видео и видеофайлы с качеством FullHD, Skype, YouTube, сервисы интернет-кинотеатров и т.д.)
- к играм (в том числе он-лайн, и тоже с высоким качеством видео),
- социальные сети и мессенджеры,
- личная почта (mail.ru, gmail.com)
- к прочим личным ресурсам.

Сценарии применения TrusTPad

В защищенном режиме:

– к корпоративной почте;

– к системам управления предприятием 1С,

– банковские работники могут получить доступ к автоматизированным банковским системам (АБС),

– участковый врач к медицинским информационным системам (МИС), например, при заполнении электронной карточки больного при обходе участка;

– к возможностям безопасного управления банковским счетом (ДБО),

– к видео конференциям в различных вариантах (телемедицинские консультации, дистанционное образование, корпоративное совещание),

– к обработке персональных данных в различных информационных системах,

– к информационным системам, обрабатывающим защищаемые данные,

– к госуслугам в электронном виде;

– и ко многим другим «облачным» сервисам, требующим хороший уровень ИБ.

Сертификат соответствия ФСТЭК России

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3569

Сертификат удостоверяет, что планшетный компьютер «TrusTPad» программно-техническим средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, предназначенным для обеспечения целостности и доступности защищаемой информации, реализующим функции управления доступом, очистки памяти, аутентификации, регистрации событий безопасности и контроля целостности

- Можно использовать в ИСПДн, ГИС, АСУ ТП.

Вопросы???

Спасибо за внимание!

С уважением,
Рябов Андрей
ЗАО «ОКБ САПР»
www: www.okbsapr.ru
email: asr@okbsapr.ru