

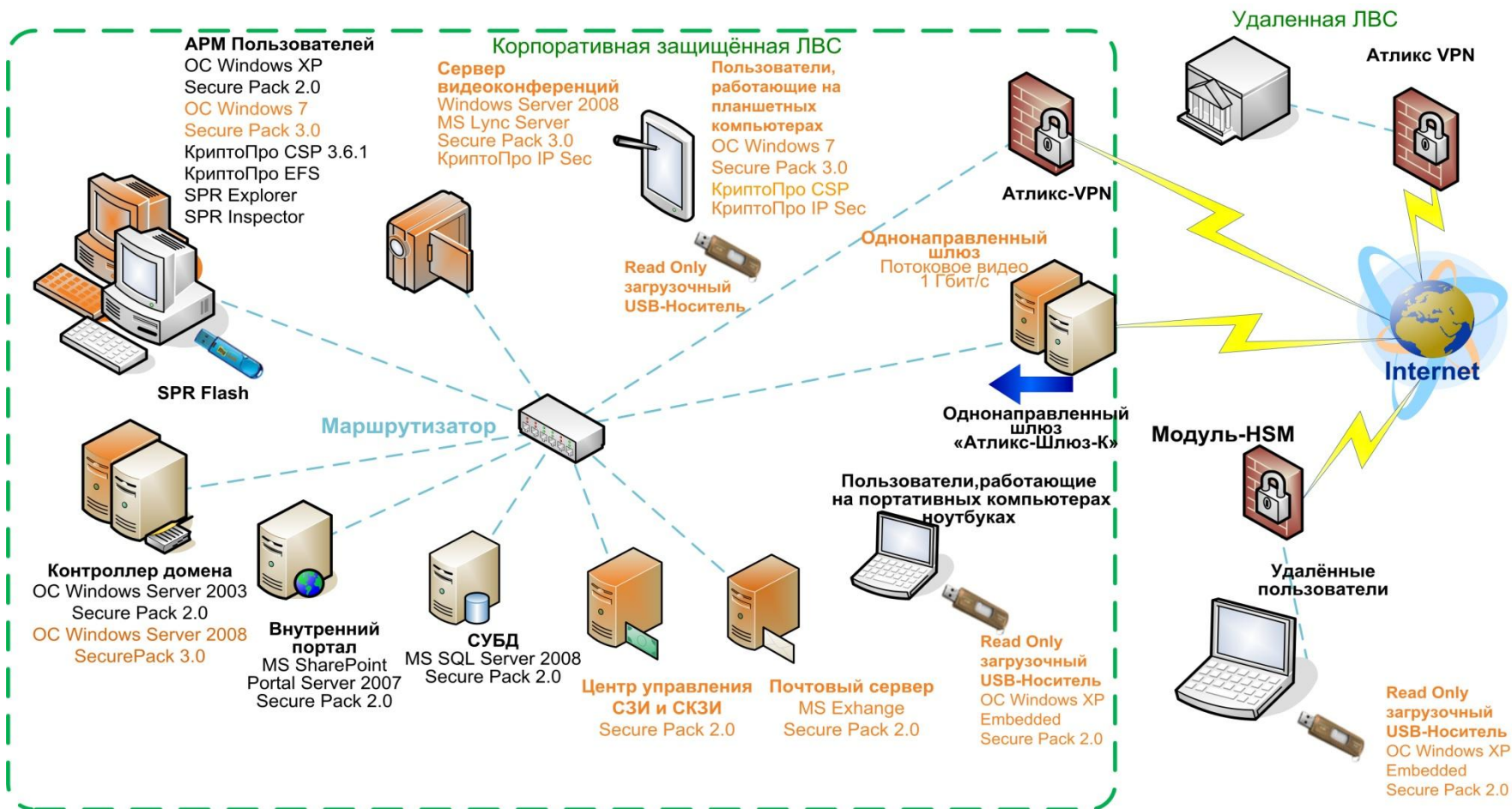


**Сертифицированные решения для защиты
планшетных компьютеров на базе
программных продуктов корпорации Microsoft**

Доклад ФГУП «НТЦ «Атлас»



Решения по комплексной защите территориально распределённых защищённых автоматизированных информационных систем с обеспечением выполнения требований ФСБ и ФСТЭК России



В качестве удаленных объектов могут быть ЦОД-ы (в том числе, использующие «облачные вычисления»²)



Семейство программно-аппаратных комплексов (ПАК) «Атликс-VPN», «Модуль-HSM»



ПАК «Атликс-VPN»



ПАК «Модуль-HSM»

ПАК «Атликс-VPN» и «Модуль-HSM» предназначены для создания и взаимодействия высокозащищенных (по уровню КВ2) виртуальных сетей (VPN) на основе протокола IPSec и стандарта X.509 с использованием российских криптографических алгоритмов.



Состав решений по требованиям ФСБ и ФСТЭК

Клиентская ОС- Windows XP	Сертификат ФСБ	Сертификат ФСТЭК
Клиентская ОС – Windows 7 <ul style="list-style-type: none">• Для рабочих станций• Для планшетов	Сертификат ФСБ	Сертификат ФСТЭК
Серверная ОС - Windows Server 2003	Сертификат ФСБ	Сертификат ФСТЭК
Серверная ОС – Windows Server 2008 R2	Сертификат ФСБ	Сертификат ФСТЭК
Сервер документооборота/портал – SharePoint Server 2007	Сертификат ФСБ	Сертификат ФСТЭК
Сервер баз данных – SQL Server 2008	Сертификат ФСБ	Сертификат ФСТЭК
Интернет Шлюз – «Атликс-Шлюз-К»	Заключение ФСБ	
Программно-аппаратный комплекс «Атликс-VPN»	Сертификат ФСБ	Сертификат ФСТЭК
Программно-аппаратный комплекс «Модуль-HSM»	Заключение ФСБ	В стадии сертификации
Почтовый сервер – Exchange Server 2010	В стадии сертификации	В стадии сертификации
Сервер теле-видео конференций – MS Lync 2010	Планируется сертификация	



Защита информации в корпоративных АИС от внутреннего нарушителя, являющегося пользователем АИС

- **Защита от неумышленной установки вредоносного ПО;**
- **Защита от выноса конфиденциальной информации, в том числе персональных данных на носителях.**

При отсутствии СКЗИ в АИС требуется сертификация средств защиты информации по требованиям ФСТЭК России до класса 1Г включительно.

В случае использования в АИС СКЗИ, например, для работы с ЭЦП, средства защиты информации должны быть сертифицированы по классам АК2/АК3 требований ФСБ России по защите от НСД в АИС.

Представленные решения по защите полностью удовлетворяют вышеперечисленным требованиям ФСТЭК и ФСБ России. Эти решения основаны на штатных механизмах Windows, не ограничивает исходную функциональность ОС и не требует проведение дополнительного обучения сотрудников в части управления системой разграничения доступа.



Решения на планшетах

1-й режим – работа в Интернет с незащищенными данными

Работа с данными из незащищенной области планшета

Свободный серфинг в Интернете, открытая почта (mail.ru), ...

2-й режим – работа с конфиденциальными данными

Запуск сертифицированной ФСБ Windows 7 с внешнего USB-носителя

Блокирование подключаемых внешних носителей

Подъем защищенного канала доступа к корпоративной сети (использование российской криптографии ГОСТ)

Работа с данными из защищенной области планшета



Сравнение планшетов, работающих под ОС Windows 7 и iOS

Базовые устройства для удаленного АРМ	Сертифицированные СКЗИ (КС2/КС3) и СЗИ от НСД (АК2/АК3) по требованиям ФСБ	Сертифицированные средства шифрования трафика (Wi-Fi, GPRS, др) по требованиям ФСБ	Сертифицированные средства шифрования данных на локальном и съемных носителях по требованиям ФСБ	Механизм доверенной загрузки	Официальный доступ к исходным кодам ОС и прикладного ПО
Планшеты под Windows 7	ЕСТЬ	В стадии сертификации	ЕСТЬ	В стадии сертификации	ЕСТЬ
Планшеты iPad Apple под iOS	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ



Благодарим за внимание !

ФГУП НТЦ «АТЛАС»

127018, г.Москва, ул.Образцова д.38

Тел. +7 (495) 689-16-34

E-mail: szd@stcnet.ru

Web: www.stcnet.ru