

Сертифицированные программные продукты **Microsoft**

Возможность оптимизации расходов
на защиту информации

Аввакумов Владимир
Группа компаний «Перемена»





ГК «Перемена» - это:

- ❑ более 20 компаний из различных областей бизнеса в разных городах России в составе ГК;
 - ❑ партнерство с крупнейшими мировыми производителями серверного, компьютерного и программного обеспечения;
 - ❑ большой штат сертифицированных технических специалистов;
 - ❑ проектная деятельность в области системной интеграции;
 - ❑ защита конфиденциальной информации;
 - ❑ собственный сервисный центр.
-



Партнерские статусы:



Microsoft® Partner

- Gold OEM Hardware
- Gold Volume Licensing
- Gold Virtualization
- Gold Data Platform
- Gold Application Integration
- Gold Business Intelligence
- Silver Hosting
- Silver Mobility
- Silver Desktop
- Silver Server Platform
- Silver Identity and Security
- Silver Midmarket Solution Provider



Preferred Partner

GOLD



Защита информации:

- ❑ **ЗАО «АЛТЭКС-СОФТ»**
(сертифицированные средства Microsoft)
 - ❑ **ООО «Код Безопасности»**
(АПКШ «Континент», Secret Net, ПАК Соболь и др.)
 - ❑ **ООО «Конфидент»** (Dallas Lock)
 - ❑ **ОАО «ИнфоТеКС»** (в планах)
-

Лицензии:

□ ФСТЭК:

- деятельность по технической защите конфиденциальной информации;
- деятельность по разработке и (или) производству средств защиты конфиденциальной информации

□ ФСБ:

- распространение шифровальных (криптографических) средств защиты информации;
 - техническое обслуживание шифровальных (криптографических) средств защиты информации;
 - предоставление услуг в области шифрования информации
-

Клиенты часто спрашивают...



Защита информации

(анализ разных подходов):

Встроенные средства защиты

- Полная совместимость
- Быстродействие систем
- Унифицированный интерфейс
- Отсутствие необходимости специальной подготовки
- Низкая стоимость решения
- Высококласная техническая поддержка Microsoft и его партнеров

Наложенные средства защиты

- Отсутствие гарантий совместимости с ОС и прикладным ПО
 - Отсутствие гарантий устойчивости работы систем
 - Потеря быстродействия
 - Специальная подготовка персонала для внедрения подобных систем и их пользователей
 - Неудобства в работе и другое
-

Что можно защищать
встроенными средствами?

ИСПДн класса К2 / К3

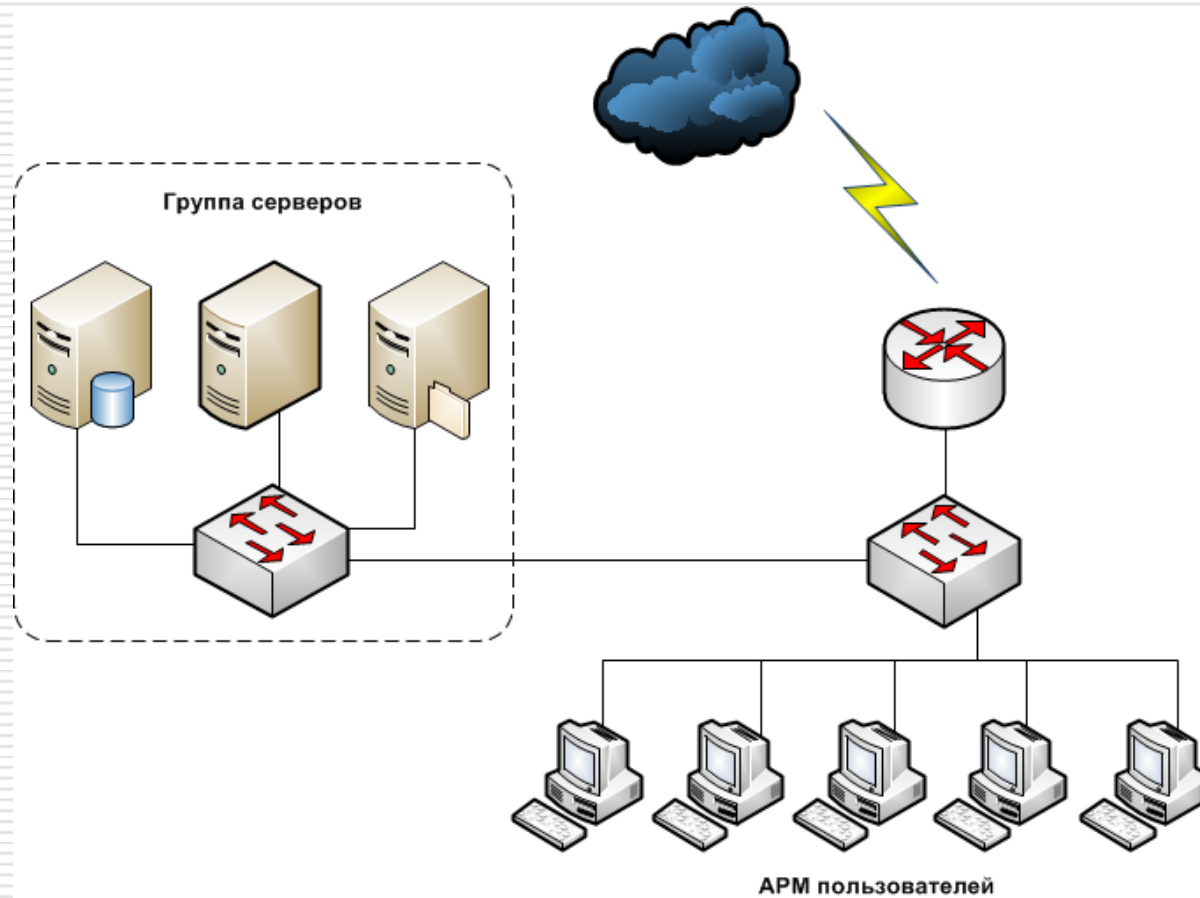
Самые распространенные ИСПДн – класса К3 и К2

$X_{\text{пд}} \setminus X_{\text{нпд}}$	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

ИСПДн класса К2 – чаще всего это:

- ❑ ИС, обрабатывающая персональные данные категории 2
 - ❑ В ИС одновременно обрабатываются данные от 1000 до 100 000 субъектов ПДн
 - ❑ Распределенная ИС, состоящая из АРМ и(или) локальных ИС, объединенных в единую ИС с использованием технологии удаленного доступа
 - ❑ Может иметь подключение к Интернет
 - ❑ Многопользовательская ИС
 - ❑ Разграничение прав доступа
 - ❑ Находится на территории Российской Федерации
-

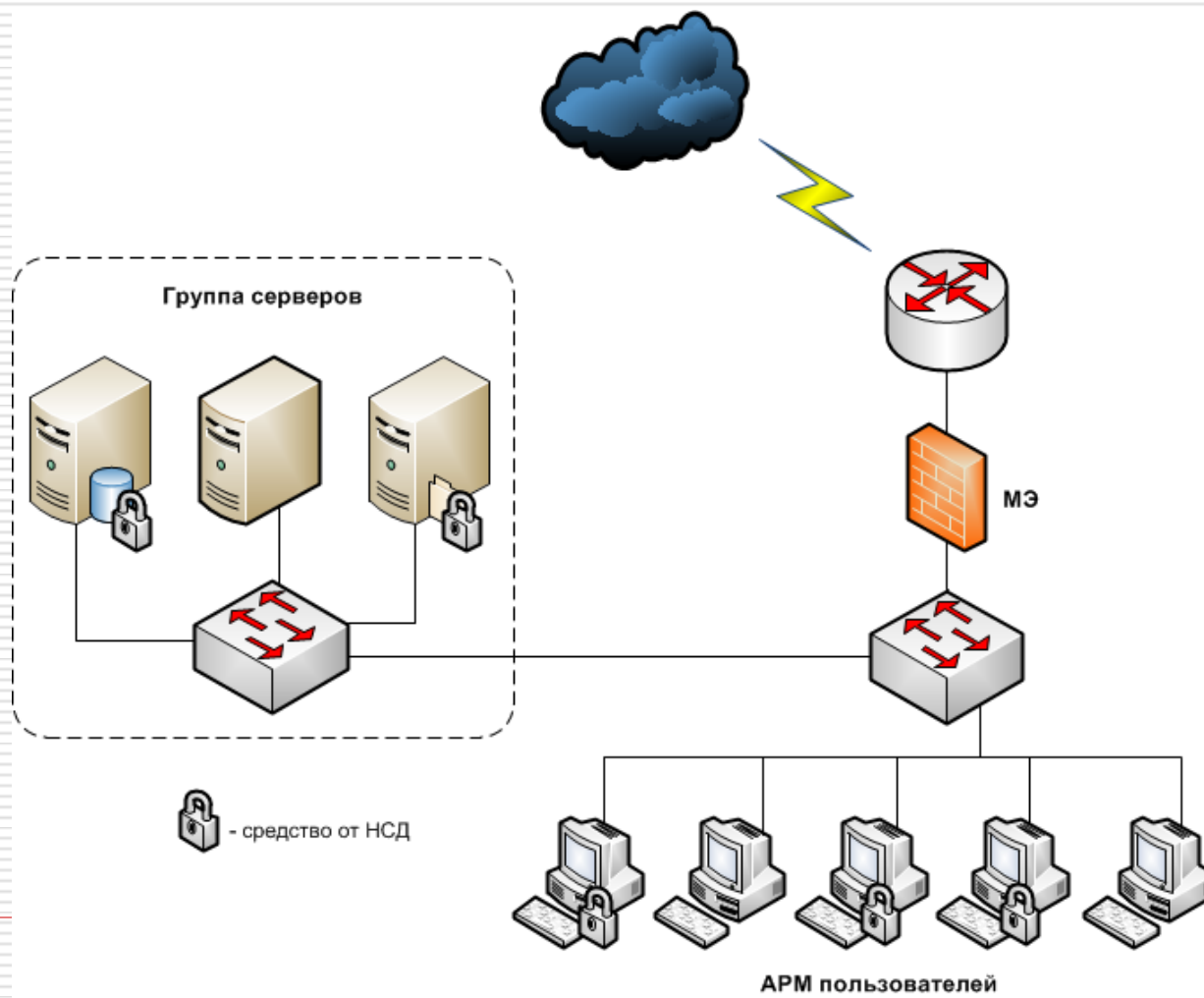
Типовая информационная структура организации



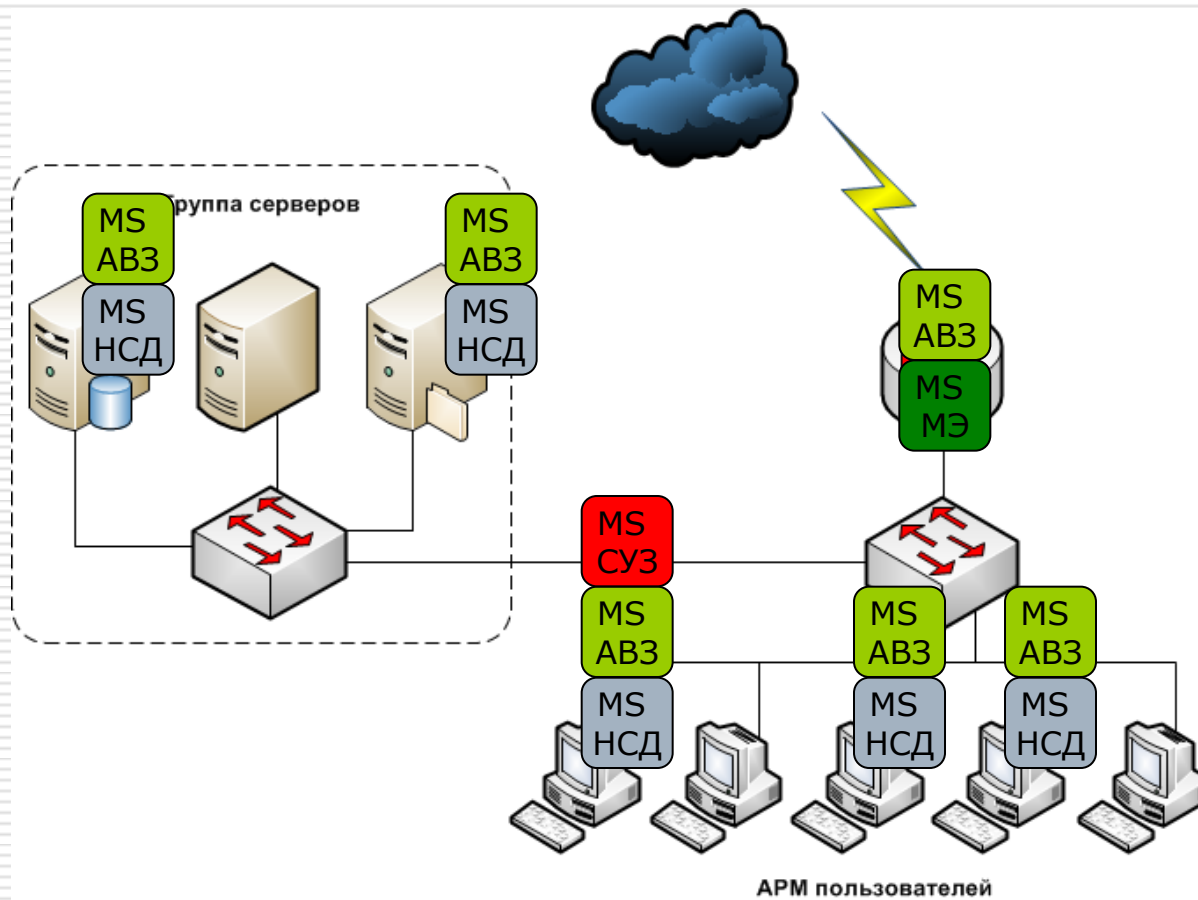
Подсистемы защиты информации (для типовой ИСПДн К2):

- управления доступом; ●
 - регистрации и учета; ●
 - обеспечения целостности; ●
 - межсетевого экранирования; ●
 - антивирусной защиты; ●
 - обнаружения вторжений; ●
 - анализа защищенности; ●
 - централизованного управления СЗИ ●
-

Типовая схема защиты ПДн



Защита ИСПДн К2 средствами Microsoft:



Перечень сертифицированного ПО Microsoft:

- OC Windows XP / Vista/ 7
 - OC Windows Server 2003 / 2003R2 /2008 /2008R2
 - SQL Server 2005 /2008
 - Office 2003 /2007
 - ISA Server 2006 Standard
 - Forefront Security
 - Exchange Server 2007 Standard, Enterprise
 - BizTalk Server 2006 R2 /2009
 - SharePoint Server 2007 R2
 - System Center Operation Manager / Configuration Manager / Data Protection Manager
 - Dynamics CRM / AX / NAV
-

Сертифицированное ПО Microsoft – это:


стандартное лицензионное программное обеспечение, прошедшее испытания на соответствие установленным требованиям РД Регуляторов, обладающее сертификатом соответствия ФСТЭК или ФСБ России, настроенное и эксплуатируемое в соответствии с сертифицированными параметрами

Что подлежит сертификации:

Сертификацию проходят заявленные в задании по безопасности или ТУ механизмы защиты программного обеспечения, к которым относятся:

- аутентификация и идентификация;
- контроль доступа;
- регистрация и учет;
- аудит;
- обеспечение целостности;
- блокирование запуска вредоносных программ;
- обеспечения функций межсетевое экранирования;
- другие функции безопасности

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 844/2

Выдан 3 декабря 2004 г.
Действителен до 3 декабря 2007 г.

Настоящий сертификат удостоверяет, что операционная система Microsoft Windows XP Professional, разработанная компанией Microsoft Corporation, функционирующая на рабочих станциях на базе процессора семейства Intel x86, и поставляемая ФГУП «Предприятие по поставкам продукции Управления делами Президента Российской Федерации» совместно с ЗАО «Алтракс-строй-2002» в соответствии с формуляром 17664448.82613410.501100-01 30, является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к конфиденциальной информации, соответствует заданию по безопасности MS.Win_XP.ЭБ и имеет оценочный уровень доверия ОУД 1 (усиленный) в соответствии с руководящим документом Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».


Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Центр безопасности информации» (аттестат аккредитации от 4.07.2003 № СЗИ RU.117.Б08.025) – технического отчета об оценке от 18.12.2003 и дополнения № 1 к нему от 8.11.2004, протокол испытаний от 14.06.2004, и отчета о сертификации Гостехкомиссии России от 28.06.2004 и дополнения № 1 к нему от 2.12.2004.

Заявитель: ФГУП «Предприятие по поставкам продукции Управления делами Президента Российской Федерации»
Адрес: 125047, г.Москва, ул.2-я Тверская-Ямская, д.16/18, стр.2
Телефон: (095) 250-3734, 251-8050

Заявитель: ЗАО «Алтракс-строй-2002»
Адрес: 125047, г.Москва, пл. Тверская Застава, д.3
Телефон: (095) 786-4365, 440-1075

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям руководящих документов Гостехкомиссии России осуществляется испытательной лабораторией ООО «Центр безопасности информации».


ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



А.Гапанов

Настоящий сертификат вступает в силу с момента подписания и действует до 03 декабря 2007 года.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

ОТВЕТСТВИЯ

данная система Microsoft Windows Vista с Microsoft Corporation, функционирующая на чипах (МБ) процессора, произведенная и управляемая делами Президента Российской Федерации, имеет оценочный уровень доверия ОУД 1 (повышенный) к конфиденциальной информации, соответствует заданию по безопасности MS.Win_XP.ЭБ и имеет оценочный уровень доверия ОУД 1 (усиленный) в соответствии с руководящим документом Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».

Испытания: проведенные испытания, проведенные лабораторией ООО «Центр безопасности информации» (аттестат аккредитации от 04.07.2003 № СЗИ RU.117.Б08.025) – технического отчета об оценке от 18.12.2003 и дополнения № 1 к нему от 8.11.2004, протокол испытаний от 14.06.2004, и отчета о сертификации Гостехкомиссии России от 28.06.2004 и дополнения № 1 к нему от 2.12.2004.

Испытательная лаборатория: ООО «Центр безопасности информации»
Адрес: 125047, г.Москва, ул. 2-я Тверская-Ямская, д.16/18, стр.2
Телефон: (095) 250-3734, 251-8050

Испытательная лаборатория: ЗАО «Алтракс-строй-2002»
Адрес: 125047, г.Москва, пл. Тверская Застава, д.3
Телефон: (095) 786-4365, 440-1075

Испытательная лаборатория: ООО «Центр безопасности информации»
Адрес: 125047, г.Москва, ул. 2-я Тверская-Ямская, д.16/18, стр.2
Телефон: (095) 250-3734, 251-8050

Испытательная лаборатория: ЗАО «Алтракс-строй-2002»
Адрес: 125047, г.Москва, пл. Тверская Застава, д.3
Телефон: (095) 786-4365, 440-1075

Что такое сертифицированное ПО Microsoft:

- Дистрибутив, соответствующий эталонному экземпляру, подвергнутому сертификационным испытаниям
 - Сопроводительная документация, заверенная копия Сертификата, голографический знак соответствия ФСТЭК России
 - Механизмы защиты развернутой версии, настроенные в соответствии с сертифицированными параметрами
 - Установленные актуальные сертифицированные обновления безопасности
 - Контролируемые в процессе эксплуатации механизмы безопасности
-

Требования к дистрибутивам ПО, отдаваемых на сертификацию

- Дистрибутив должен быть лицензионным, установленного образца, произведен официальным репликатором Microsoft. **На сертификацию не принимаются диски восстановления, поставляемые в составе ПЭВМ с предустановленным ПО Microsoft, содержащими OEM-версии программного обеспечения.** Отличительной особенностью таких дисков является наличие наименования компании-поставщика оборудования на лицевой части носителя.
 - Дистрибутив должен содержать ту версию программного обеспечения, которая указана в сертификате ФСТЭК России, и на которую имеется соответствующая лицензия
-

Особенности поставки сертифицированного ПО Microsoft

Комплект поставки сертифицированной версии ФСТЭК включает две обязательные позиции:

- 1) Пакет сертифицированной версии ПО для использования на необходимом количестве АРМ
- 2) Лицензия на использование программы контроля сертифицированной версии по количеству защищаемых АРМ

Примечание: к серверному программному обеспечению могут быть поставлены пакеты сертифицированного клиентского и терминального доступа.

При первой поставке сертифицированных версий Microsoft дополнительно приобретается USB-ключ eToken PRO для получения сертифицированных обновлений. Приобретается один ключ на организацию для всех используемых сертифицированных версий Microsoft.

Виды комплектов (пакетов) сертифицированного ПО Microsoft

- Пакет «**Базовый**»
 - Пакет «**Базовый контроль**»
 - Пакет «**Полный**»
-

Пакет «Базовый»

- Верифицированный установочный комплект ПО.
 - Бессрочный абонемент на получение сертифицированных online-обновлений
 - Техническая поддержка (информационные и консультационные услуги)
 - Формуляр на сертифицируемое ПО, промаркированный Голографическим специальным знаком соответствия ФСТЭК России.
 - Копии Сертификатов ФСТЭК России на поставляемое ПО, заверенные печатью Поставщика.
 - Формуляр на программу контроля сертифицированной версии ПО Check.
 - Медиа-Кит (CD-диск)
 - Лицензии на право использования Программы контроля сертифицированного ПО, приобретаются по количеству пользователей отдельно
 - Сертифицированный USB-ключ eToken PRO с записанным цифровым сертификатом для получения сертифицированных обновлений (для доступа к [доверенной части сайта](#))
-

Пакет «Базовый контроль»

Отличие от пакета «Базовый»:

- наличие сертифицированной версии программного комплекса контроля доступа к сменным носителям и устройствам DeviceLock 6.4.1
 - CD-диск для сертифицированной версии DeviceLock, содержащий:
 - файлы с кодами активации ПО;
 - руководства по установке, настройке и работе с ПО;
 - набор информационных материалов
 - Лицензионное соглашение на использование программного комплекса Device Lock (приобретается отдельно по кол-ву защищаемых АРМ)
-

Пакет «Полный»

Отличие от пакета «Базовый»:

- ПАК в составе сертифицированного электронного USB-ключа (или смарт-карты) eToken PRO и сертифицированной программой eToken Network Logon

Сертифицированные USB-ключи eToken PRO для усиленной аутентификации пользователей (дополнительной защиты от НСД) приобретаются по количеству пользователей.

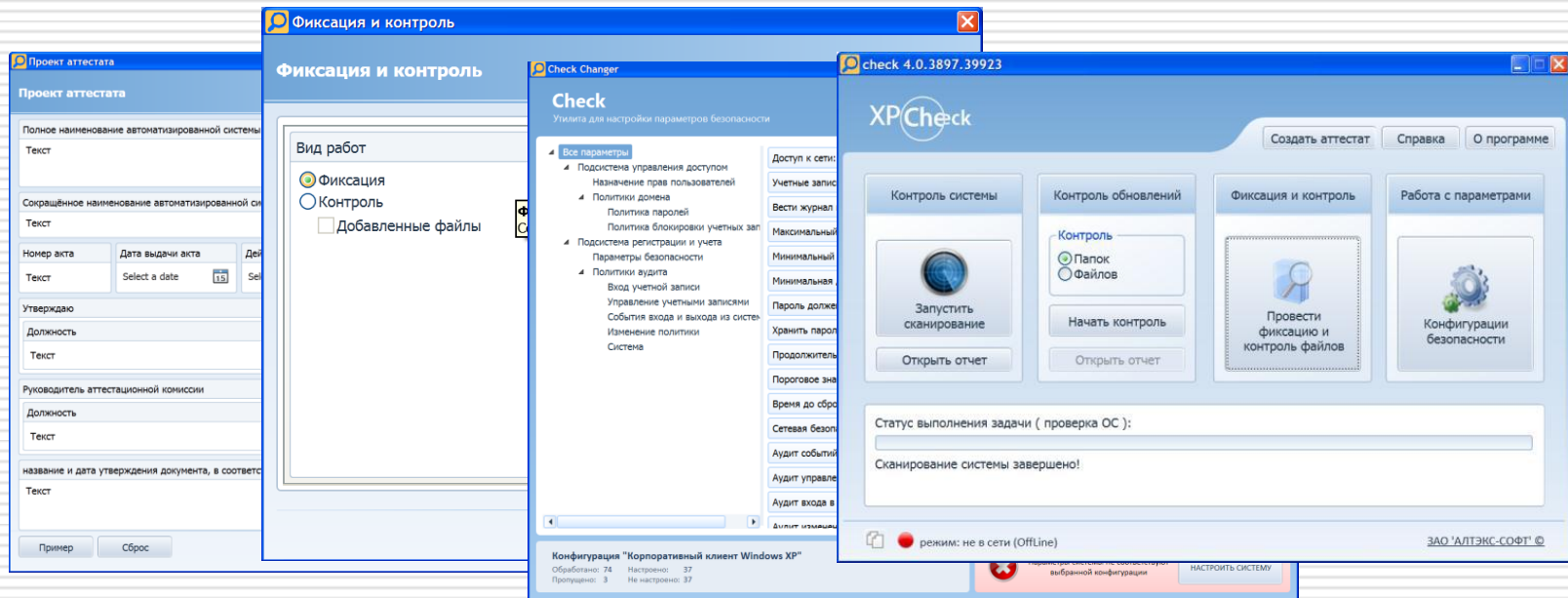
На заметку:

- При сертификации OEM и коробочных версий ПО Microsoft количество дистрибутивов должно соответствовать количеству имеющихся лицензий
- Для корпоративных лицензий (OLP, OV, OVS и пр.) разрешенное количество установок сертифицированных версий соответствует заявленному количеству лицензий и указывается в формуляре, входящем в состав пакета сертификации

Для сертификации достаточно предоставить один дистрибутив (Disk Kit) и подтвердить количество лицензий на требуемое сертифицируемое ПО

Автоматизация настройки и контроля сертифицированного ПО Microsoft

Программы семейства **Check** - эффективный инструмент для приведения в соответствие с требованиями параметров безопасности систем защиты ИСПДн и их контроля



Ключевые функциональные особенности программ контроля и настройки **Check**

- сбор данных и формирование отчетов о соответствии установленного продукта сертифицированной версии;
 - отчеты об установленных и не установленных сертифицированных обновлениях безопасности;
 - контроль загруженных обновлений на предмет соответствия сертифицированным обновлениям продуктов Microsoft;
 - фиксация и контроль целостности исполняемых файлов и библиотек;
 - контроль и настройка параметров безопасности в автоматизированном и ручном режимах;
 - создание пользовательских конфигураций параметров безопасности с возможностью наследования значений от сертифицированных конфигураций и др.
-

Соответствие требованиям Регуляторов

Подсистема управления доступом

Требование ФСТЭК для ИСПДн класса К2	Средства, обеспечивающие выполнение требований РД
<ul style="list-style-type: none">- Идентификация и аутентификация (проверка подлинности) субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов- Идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам.- Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.- Контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа	<p>Реализуется с помощью установки соответствующих параметров безопасности механизмов «Идентификации и аутентификации» при настройке операционной системы на сертифицированную конфигурацию</p> <p>В случае использования других элементов общего программного обеспечения (SQL Server, Exchange Server и др.) дополнительно используются их встроенные механизмы «Идентификация и аутентификация» и «Защита данных пользователя», а также организационные меры</p>

Подсистема регистрации и учета

Требование ФСТЭК для ИСПДн класса К2	Средства, обеспечивающие выполнение требований РД
<ul style="list-style-type: none">- Регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.- Регистрация запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.- Регистрация попыток доступа программных средств (программ, заданий) к защищаемым файлам.- Регистрация попыток доступа программных средств к терминалам ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, записям	<p>Реализуется с использованием механизмов «Аудит безопасности» и «Защита данных пользователя» операционной системы.</p> <p>Контролируется с использованием журнала событий операционной системы и других программных продуктов Microsoft, а также с использованием организационных мер</p>

Подсистема обеспечения целостности

Требование ФСТЭК для ИСПДн класса К2	Средства, обеспечивающие выполнение требований РД
<ul style="list-style-type: none">- Обеспечение целостности программных средств СЗИ НСД, а также неизменность.- Периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытку НСД- Наличие средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности	<p>Обеспечивается использованием механизмов безопасности «Защита данных функций безопасности организации».</p> <p>Средствами защиты файлов ОС, механизмами программ контроля «Check», утилитами архивации, теневого копирования, восстановления, аварийного восстановления ОС</p>

Подсистема межсетевого экранирования

Требование ФСТЭК для ИСПДн класса К2	Средства, обеспечивающие выполнение требований РД
- Требования, предъявляемые к МЭ 4-го класса (РД МЭ) — максимального класса МЭ, необходимого для построения ИСПДн класса К2	Реализуется использованием МЭ Microsoft ISA Server 2006 Standard Edition , сертифицированного по 4-му классу согласно РД МЭ

Подсистема антивирусной защиты

Требование ФСТЭК для ИСПДн класса К2	Средства, обеспечивающие выполнение требований РД
- Требования «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (СТР-К) и «Положения о методах и способах защиты информации в информационных системах персональных данных» (Приказ ФСТЭК России N 58 от 5 февраля 2010 г.)	Реализуется использованием антивируса Microsoft Forefront Client Security

Подводя итоги:

- ПО Microsoft сертифицировано и соответствует строгим требованиям Регуляторов в области защиты персональных данных
 - Линейка сертифицированных продуктов Microsoft позволяет строить системы защиты ИСПДн классов КЗ-К2 без дополнительных наложенных СЗИ сторонних производителей
 - Использование единой платформы обеспечивает высокую безопасность, совместимость, устойчивость и быстродействие
 - Отсутствие необходимости приобретения дополнительных наложенных СЗИ существенно снижает затраты на построение ИСПДн
 - Применение сертифицированных конфигураций безопасности Microsoft повышает эффективность защиты системы
 - Программы Check автоматизируют процесс настройки безопасности и снижают риски, связанные с ошибками администраторов
-



Спасибо за внимание!

Аввакумов Владимир
Группа компаний «Перемена»
vavvakumov@peremenarussia.com
тел. (473) 226-88-77 (доб. 177)

