

Сертифицированные решения для построения систем защиты персональных данных и конфиденциальной информации

Калашников Иван
ЗАО «АЛТЭКС-
СОФТ»



Государственные Регуляторы в области защиты персональных данных

Устанавливает методы и способы
защиты информации в
информационных системах
некриптографическими
методами



**Федеральная служба по
техническому и экспортному
контролю (ФСТЭК России)**

Устанавливает методы и способы
защиты информации в
информационных системах
криптографическими методами



**Федеральная служба
безопасности
(ФСБ России)**

Контроль и надзор за
соответствием обработки ПДн
требованиям
законодательства



**Федеральная служба по
надзору в сфере связи,
информационных технологий
и массовых коммуникаций
(Роскомнадзор)**

Нормативная база, регламентирующая требования по защите персональных данных

Федеральные законы

- Об информации, информационных технологиях и о защите информации от 27 июля 2006 года № 149-ФЗ
- О персональных данных от 27 июля 2006 года № 152-ФЗ

Нормативно-методические документы ФСТЭК России

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Положение о методах и способах защиты информации в информационных системах персональных данных (Приказ ФСТЭК России от 5 февраля 2010 г. N 58)
- Постановление № 781 Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных
- другие

Основные факторы определяющие выбор средств защиты информации



Наиболее распространенные классы ИСПДн на территории РФ

В соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных» (Приказ ФСТЭК России № 58 от 05 февраля 2010 г.), для защиты ПД в информационных системах персональных данных классов К3 и К2 (наиболее распространенные классы ПДн) должны использоваться сертифицированные ФСТЭК России СЗИ.



ИСПДн класса К2:

1. Персональные данные категории 2 - ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию.
2. В ИСПДн одновременно обрабатываются данные от 1 000 до 100 000 субъектов ПДн.
3. Распределенная информационная система, состоящей из комплексов АРМ и(или) локальных ИС, объединенных в единую ИС с использованием технологии удаленного доступа.
4. Может иметь подключение к Интернет.
5. Многопользовательская.
6. Разграничение прав доступа.
7. Находиться на территории Российской Федерации.

ФЗ № 152 «О персональных данных» вступил в силу 26 января 2007 года

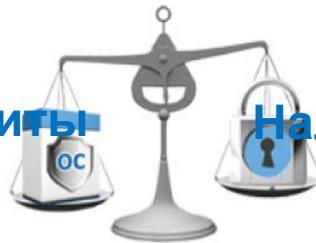
Крайний срок приведения ИСПДн в соответствие – 1 июля 2011

Программно-технические средства защиты информации от НСД

Выбор средств защиты информации сводится к выбору наложенных (дополнительных) средств защиты либо общесистемного и прикладного программного обеспечения со встроенными механизмами защиты информации.

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

Программные средства для построения защищенных информационных систем

Microsoft®

- Windows XP/Vista/7
 - Windows Server 2003/2003R2/2008/2008R2
 - SQL Server 2005/2008
 - Office 2003/2007
 - ISA Server 2006 Standard
 - ForefrontSecurity
 - ExchangeServer 2007 Standard, Enterprise
 - BizTalkServer 2006 R2/2009
 - SharePointServer 2007 R2
 - System Center Operation Manager/ Configuration Manager/
 - Protection Manager
 - Dynamics CRM/ AX/ NAV.
- 
- Windows
- 
- Office
- 
- Forefront
- 
- SQL Server
- 
- Windows Server

DeviceLock

SmartLine
Proactive Network Security

- Advanced Workstation
- Advanced Server
- Server for Windows

Acronis®
COMPUTE WITH CONFIDENCE

UserGate
PROXY & FIREWALL 5.2.F

entensys

Антивирусные средства
Dr.Web, Kaspersky lab., NOD 32 и др.

Сертифицированные решения на платформе общесистемного ПО Microsoft



Сертифицированные программные продукты Microsoft позволяют создать защищенную ИСПДн до 2-го класса включительно с минимальным набором наложенных средств защиты информации

Microsoft

- Windows XP/Vista/7
- Windows Server 2003/2003R2/2008/2008R2
- SQL Server 2005/2008
- Office 2003/2007
- ISA Server 2006 Standard
- ForefrontSecurity
- ExchangeServer 2007 Standard, Enterprise
- BizTalkServer 2006 R2/2009
- SharePointServer 2007 R2
- System Center Operation Manager/ Configuration Manager/ Protection Manager
- Dynamics CRM/ AX/ NAV.



Windows



Office



Microsoft
Forefront



Microsoft
SQL Server



Windows Server



**Более 40 сертификатов ФСТЭК
России**

Сертифицированное средство для контроля доступа к внешним устройствам DeviceLock



Сертифицированное решение DeviceLock - надежное средство для защиты от инсайдерских угроз, утечек информации, протоколирования действий пользователей. Используется для построения защищенных ИСПДн до 1-го класса включительно

Обеспечивает контроль:

DeviceLock

- USB-портов;
- дисководов;
- CD/DVD-приводов;
- шин IEEE 1394 (FireWire);
- инфракрасных портов;
- параллельных и последовательных портов;
- WiFi и Bluetooth-адаптеров;
- ленточных накопителей;
- КПК и смартфонов (iPhone, Palm и пр.);
- сетевых и локальных принтеров;
- любых внутренних и внешних сменных накопителей и жестких дисков;
- доступ к определенным типам файлов вне зависимости от установленных на устройство разрешений (более 3800 различных типов файлов).
- Для каждого пользователя или группы мож
но задать свой список устройств, доступ к которым будет всегда разрешен. Устройства идентифицируются по модели и по уникальному серийному номеру.

- Российская разработка
- В 2009 году база инсталляций продукта превысила четыре миллиона компьютеров по всему миру
- Сертификат ФСТЭК России отсутствия недеklarированных возможностей

Сертифицированные средства для резервного копирования и восстановления Acronis



Сертифицированные решения Acronis - профессиональные средства для резервного копирования и восстановления информации. Используется при построении защищенных ИСПДн до 1-го класса включительно.

Сертифицированы версии:

- ABR 10 Advanced Workstation
- ABR 10 Advanced Server
- ABR 10 Server for Windows

Ключевые особенности:

- Резервное копирование на уровне файлов
- Полное резервное копирование
- Инкрементное резервное копирование
- Дифференциальное резервное копирование
- Устройства хранения резервных копий
- Локальные диски, сетевые хранилища (NAS и SAN)
- сетевых и локальных принтеров;



- Дедупликация данных
- Восстановление
- Восстановление на «голое железо»
- Технология Acronis Active Restore для восстановления приоритетных приложений
- Централизованная консоль управления
- Резервное копирование на основе политик
- Функция резервного копирования и восстановления с сервера
- Безопасность

- Передовое средство для резервирования и восстановления информации
- Многолетний опыт использования для создания защищенных объектов информатизации
- Сертификат ФСТЭК России отсутствия недеklarированных возможностей



Сертифицированные средства для резервного копирования и восстановления информации

Сертифицированные решения Acronis – средства защиты информации

R 10 являются программными средствами со встроенными средствами защиты от НСД, относящимися к программам контроля и восстановления файловой структуры на внешних запоминающих устройствах. (Перечень СЗИ, подлежащих сертификации в Системе сертификации № РОСС RU.0001.01БИ00, Положение №199 Гостехкомиссия России)

Сертифицированные Средства резервирования и восстановления – составная часть системы защиты ИСПДн

Методы и способы защиты информации от НСД (РД «Автоматизированные системы», Положение «Методы и способы защиты информации от НСД...»):

- наличие средств восстановления системы защиты персональных данных, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности.

Возможность незамедлительного восстановления информации – прямая обязанность оператора ПД (ФЗ №149 ФСТЭК России, Постановление

правительства РФ) Информационной системы обязан обеспечить возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней

Сертифицированное средство для межсетевого экранирования UserGate



Сертифицированное решение UserGate 5.2.F – средство для межсетевого экранирования и безопасного доступа в интернет для защищенных ИСПДн

до 1-го класса включительно.

Ключевые особенности:



- Межсетевой экран
 - Встроенная антивирусная защита
 - Усиленные механизмы аутентификации
 - Расширенный драйвер NAT
 - Организация доступа в Интернет
 - Фильтрация веб-сайтов
 - Ограничение трафика
 - Регулирование скорости доступа
 - Учет трафика
 - Модуль веб-статистики
 - Биллинговая система
 - Поддержка различных протоколов
 - Управление шириной канала
 - Кэширование трафика
 - Поддержка IP-телефонии
 - Маршрутизация
 - DNS-сервер
 - Публикация ресурса
 - Аудит и подробная статистика действий пользователей и администраторов
 - Защищенный доступа в Интернет
- Альтернатива дорогостоящим средствам межсетевого экранирования
 - Российская разработка с уникальными технологиями
 - Наличие широких функциональных возможностей
 - Сертификат ФСТЭК России отсутствия недеklarированных возможностей

Сертифицированные антивирусные средства Dr.Web, Kaspersky lab., NOD 32



Сертифицированные антивирусы – программные антивирусные средства от ведущих Российских разработчиков для реализации антивирусной защиты в ИСПДн любых классов

Ключевые особенности:

Сертифицированы ФСТЭК, ФСБ России.

Полностью соответствуют требованиям, предъявляемым к СЗИ для защиты персональных данных. Так же могут применяться в защищенных АС, обрабатывающих конфиденциальную информацию и государственную тайну.



Исследования
КА(ПЭР)(КОГО)

- Современные антивирусные средства, включающее в себя элементы защиты всех узлов корпоративной сети
- Российские разработки, которым доверяют защиту информации силовые структуры
- Наличие широкого спектра сертификатов ФСТЭК, ФСБ России

Сопоставление требований к системе защиты ИСПДн и функциональных возможностей СЗИ

Управление доступом	Механизмы идентификации, аутентификации и защиты данных:
	- пользовательских и серверных операционных систем Microsoft ;
	- офисных программных комплексов и СУБД Microsoft ;
	- электронных USB-ключей eToken и программы eToken Network Logon ; - средств контроля доступа к внешним носителям информации DeviceLock .
Регистрация и учет	Механизмы аудита безопасности:
	- пользовательских и серверных операционных систем Microsoft ; - средств протоколирования действий пользователей DeviceLock .
Обеспечения целостности	Административные мероприятия (внутренние инструкции).
	Механизмы тестирования (самотестирования) функций безопасности пользовательских и серверных операционных систем Microsoft .
	Административные мероприятия (внутренние инструкции) Контроль целостности основных конфигурационных файлов программами контроля сертифицированных версий ПО – семейство Check .
	Средства резервного копирования и аварийного восстановления Acronis Backup & Recovery 10 .
Антивирусная защита	Анализ защищенности встроенными механизмами операционных систем Microsoft
	Антивирусные средства Dr.Web, Kaspersky lab., NOD 32 и др.
Межсетевое экранирование	Механизмы фильтрации, идентификации и аутентификации, регистрации UserGate Proxy & Firewall 5.2.F, ISA Server 2006 SE

УПРАВЛЕНИЕ ДОСТУПОМ

Требование для ИСПДн класса К2

- 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 сим-волов.
- 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.

Средства, обеспечивающие выполнение

требований РД

Установка соответствующих параметров безопасности механизмов «Идентификации и аутентификации» при настройке операционной системы на сертифицированную конфигурацию для пользователей домена (для сетей ЭВМ) и локальных пользователей (для автономных рабочих мест).

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»

Настройка и использование функций безопасности «управление доступом» программного комплекса DeviceLock для реализации политики управления доступом пользователей к портам ввода/вывода и объектов доступа для пользователей домена (для сетей ЭВМ) и локальных пользователей (для автономных рабочих мест).

РЕГИСТРАЦИЯ И УЧЕТ

Требование ФСТЭК для ИСПДн класса К2

- Регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее програм-ного 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.

Средства, обеспечивающие выполнение

Реализуется с использованием механизмов «Аудит безопасности» и «Защита данных пользователя» операционной системы. Контролируется с использованием журнала событий операционной системы и других программных продуктов Microsoft.

Настройка и использование функций безопасности «Аудит безопасности» программного комплекса DeviceLock для генерации и регистрации событий связанных с контролируемыми субъектами доступа пользователей.

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ

Требование ФСТЭК для ИСПДн класса К2

- 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 попытки НСД
- Наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Средства, обеспечивающие выполнение требований РД

Обеспечивается использованием механизмов безопасности «Защита данных функций безопасности организации» операционной системы.

Контроль исполняемых файлов и библиотек как операционной системы, так и любого программного продукта, функционирующего под её управлением, с использованием программ настройки и контроля сертифицированных версий продуктов Microsoft семейства «Check».

Использование функций создания резервных копий данных, управления дисками, администрирования системы резервирования данных, восстановления информации с резервных копий данных Acronis Backup & Recovery 10 для ведения копий и реализации восстановления информационных массивов и средств защиты информации. Возможно централизованное управление.

МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

Требование ФСТЭК России к межсетевому экранированию ИСПДн класса К2

Соответствие функций МЭ Usergate 5.2.F требованиям

Фильтрация на сетевом уровне для каждого сетевого пакета	+
Фильтрация пакетов служебных протоколов	+
Фильтрация с учетом выходного и входного сетевого интерфейса	+
Фильтрация с учетом полей сетевых пакетов	+
Идентификация и аутентификация	+
Регистрация входа (выхода)	+
Регистрация и учет фильтруемых пакетов	+
Регистрация запуска программ и процессов	+
Контроль целостности	+
Сигнализация попыток нарушения правил фильтрации	+
Восстановление свойств после сбоев и отказов	+
Регламентное тестирование	+

АНТИВИРУСНАЯ ЗАЩИТА

Требование ФСТЭК для ИСПДн
класса К2

Средства, обеспечивающие
выполнение

• 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.).

Использование антивирусов Dr.Web, Kaspersky lab., NOD 32 и др.

Типовые решения для для обработки ПД или конфиденциальной информации

Решения по защите рабочих мест для обработки персональных данных представляют собой защищенные:

- автономные АРМ;
- АРМ с выходом во внешние сети;
- локальные сети без выхода во внешние сети;
- локальные сети с выходом во внешние сети, в т. ч. Internet.

Режим обработки информации в системах – многопользовательский или однопользовательский

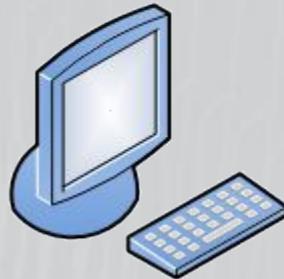
В системах пользователи имеют разные права доступа к персональным данным

Самые популярные классы ИСПДн - 2 или 3 (К2 и К3)

Типовые рабочие места для защиты ПД или конфиденциальной информации

Автономное рабочее

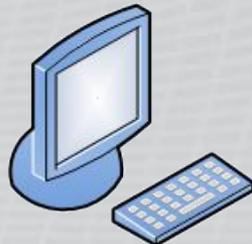
Место
АРМ пользователя



ОС Windows XP/Vista/7
ПК Office 2003/2007
MS Forefront/Dr.Web/Kaspersky
ПК DeviceLock
Acronis Advanced Workstation

Рабочее место с Internet

АРМ пользователя



ОС Windows XP/Vista/7
ПК Office 2003/2007
MS Forefront/Dr.Web/Kaspersky
ПК DeviceLock
Acronis Advanced Workstation

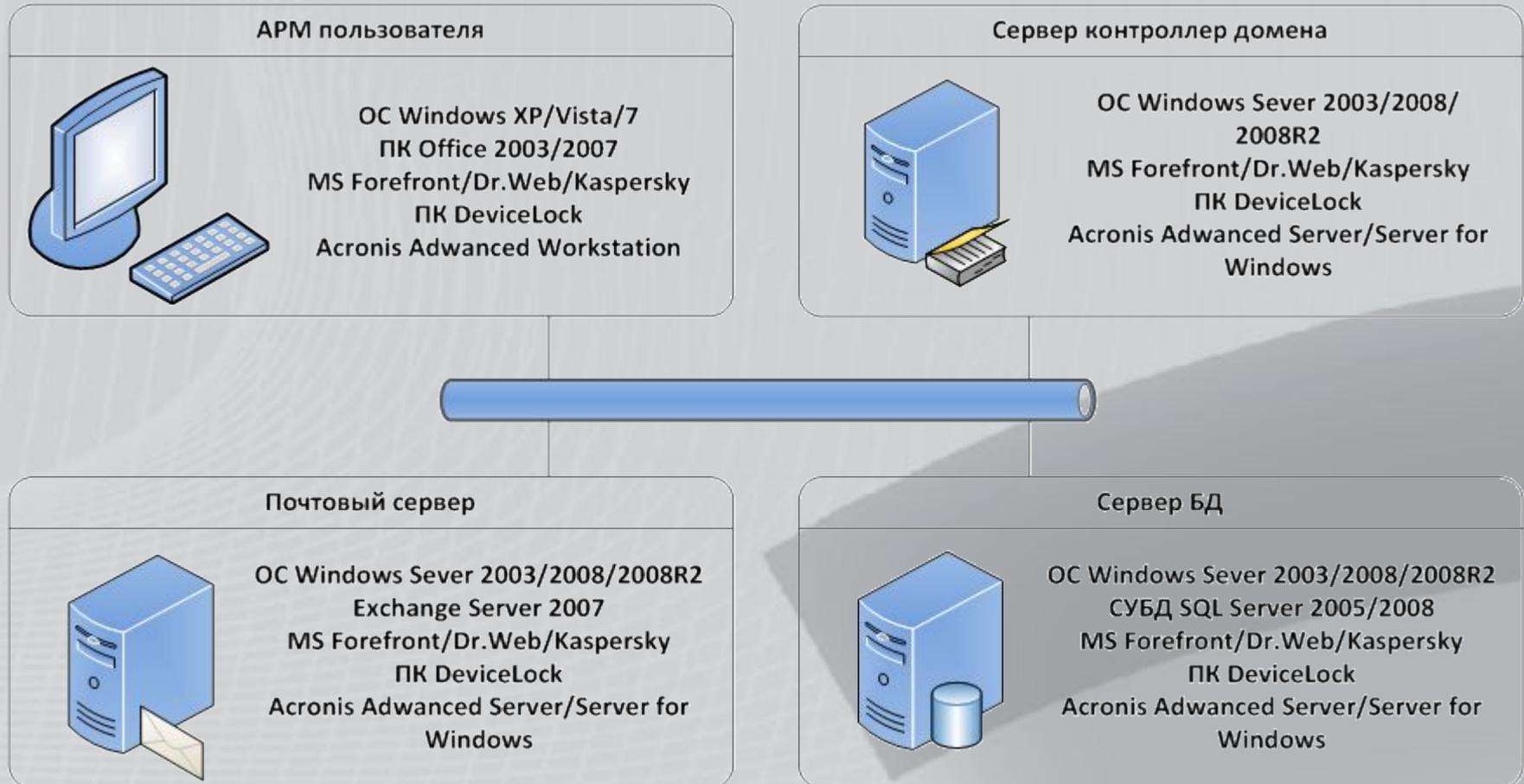
МЭ UserGate 5.2.F/ISA Server 2006



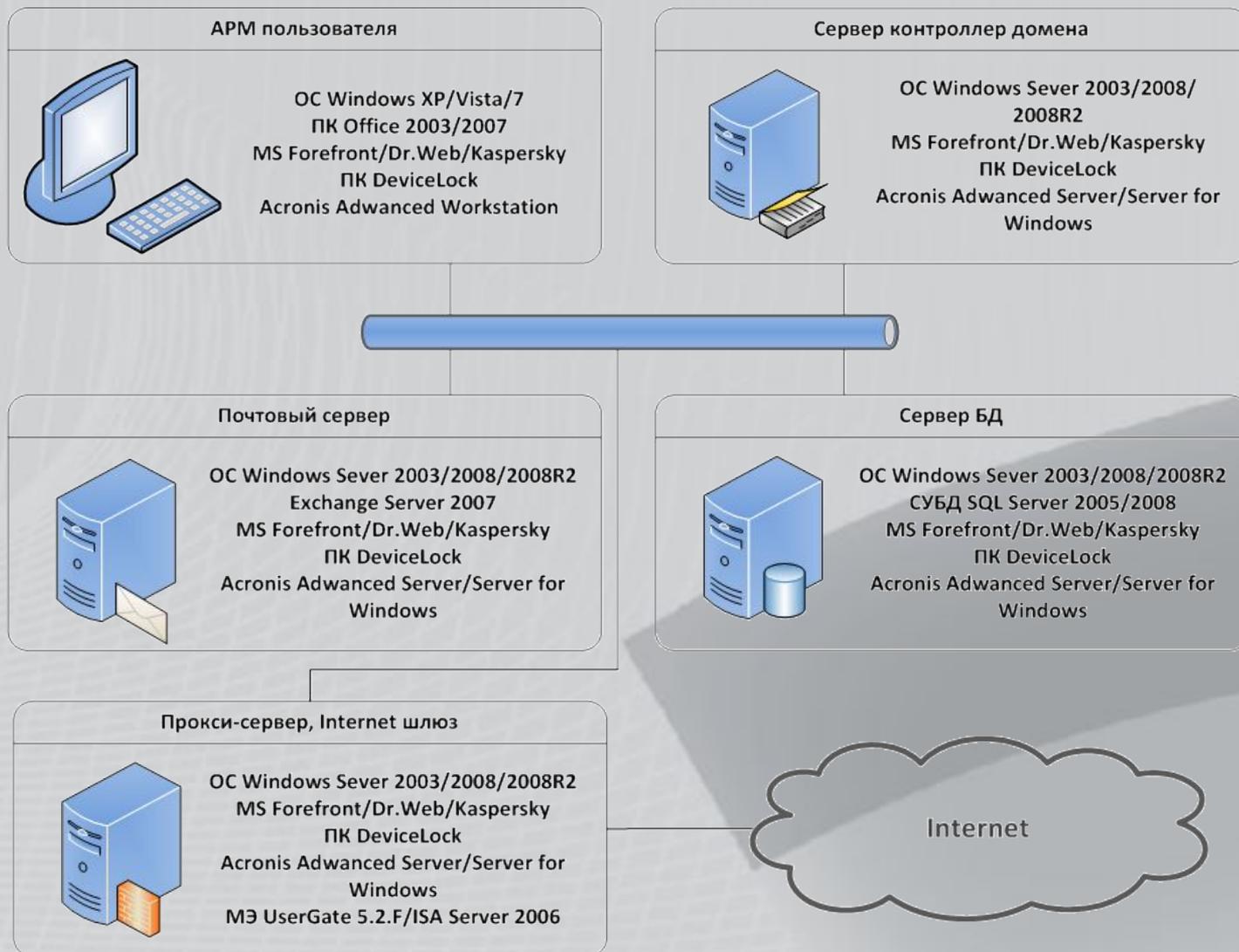
Internet



Типовая локальная сеть для защиты персональных данных



Типовая сеть с выходом Internet для защиты персональных данных



Ключевые особенности рассматриваемых СЗИ

1. Соответствие национальным стандартам и требованиям Регуляторов к средствам защиты информации;
2. Все СЗИ имеют сертификаты ФСТЭК России;
3. Линейка сертифицированных продуктов Microsoft позволяет строить системы защиты ИСПДн классов К3-К2 с минимальным набором дополнительных наложенных СЗИ сторонних производителей;
4. Полностью совместимы между собой и не способствуют негативному влиянию на другие программы в информационной системе;
5. Не требуют специальных подготовки обслуживающего персонала;
6. Производитель гарантирует бессрочную сертификационную поддержку

Дополнительные преимущества рассматриваемых СЗИ

- Стоимость
- Возможность использования уже имеющегося лицензионного ПО для проведения сертификации
- Гибкие условия приобретения и поставки
- Нулевая стоимость поддержки в течении всего срока эксплуатации
- Экономия финансовых затрат конечного пользователя или интегратора на внедрение
- Экономия финансовых затрат на сопровождение в процессе эксплуатации

Комплект сертифицированного ПО Microsoft

1. Верифицированный установочный комплект ПО
2. Бессрочный абонемент на получение сертифицированных on-line обновлений
3. Техническая поддержка (информационные и консультационные услуги)
4. Формуляр на сертифицируемое ПО, промаркированный **голографическим знаком соответствия ФСТЭК России**
5. Копия Сертификата ФСТЭК России на поставляемое ПО, заверенная печатью Заявителя.
6. Медиа-Кит (CD-диск), содержащий:
 - программу контроля сертифицированной версии ПО;
 - Руководство по безопасной настройке и контролю сертифицированного ПО;
 - Руководство по получению сертифицированных обновлений.
7. USB-ключ с записанным цифровым сертификатом для получения сертифицированных обновлений



Комплекты сертифицированных версий DeviceLock, UserGate, Acronis

1. Верифицированный установочный комплект ПО;
2. Бессрочный абонемент на получение сертифицированных online-обновлений поставляемых программных продуктов;
3. Голографические специальные знаки соответствия ФСТЭК России на поставляемые программные продукты;
4. Техническая поддержка (информационные и консультационные услуги) поставляемых программных продуктов в течение 12 месяцев с момента поставки;
5. Копия Сертификата ФСТЭК России на поставляемое ПО, заверенная печатью Заявителя;
6. Формуляр на сертифицируемое ПО;
7. CD-диск, содержащий:
 - Файлы с ключами активации ПО;
 - Руководства по установке, настройке и работе с ПО.
8. Лицензионное соглашение на использование сертифицированного программного продукта

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

SQL08 Check

Seven Check

Server08 Check

The image displays several overlapping windows from the Check software suite:

- Проект аттестата**: A form for entering system details for certification.
- Фиксация и контроль**: A window showing the current task status, with options for 'Фиксация' (Fixation) and 'Контроль' (Control).
- check 4.0.3897.39923**: The main application window with a sidebar menu and a central control panel. The status bar indicates 'режим: не в сети (Offline)'. A message at the bottom states 'Сканирование системы завершено!' (System scanning completed!).
- Check Changer**: A configuration window for security parameters. It lists various settings such as 'Доступ к сети', 'Учетные записи', and 'Политика паролей', each with a 'НАСТРОИТЬ' (Configure) button. A summary at the bottom shows 'Обработано: 74' (Processed: 74) and 'Пропущено: 2' (Skipped: 2).
- Фиксация. Содержимое выбранного каталога**: A table listing system parameters and their current status.

Категория	Имя	Стандартное значение	Подсистема управл.
Политика паролей	Минимальный срок действия пароля	1 день	1 день
Политика паролей	Максимальный срок действия пароля	90 дней	350 дней
Политика паролей	Минимальная длина пароля	8 знаков	5 знаков
Политика паролей	Пароль должен отвечать требованиям сложности	Включен	Включен
Политика паролей	Вести журнал паролей	24 сохраненных паролей	0 сохраненных
Политика безопасности учетных записей	Пороговое значение блокировки	50 ошибок входа в систему	0 ошибок
Политика безопасности учетных записей	Время до сброса системы блокировки	15 мин.	Не определено
Политика безопасности учетных записей	Продолжительность блокировки учетной записи	15 мин.	Не определено
Политика паролей	Хранить пароли, используя обратное шифрование	Отключен	Отключен

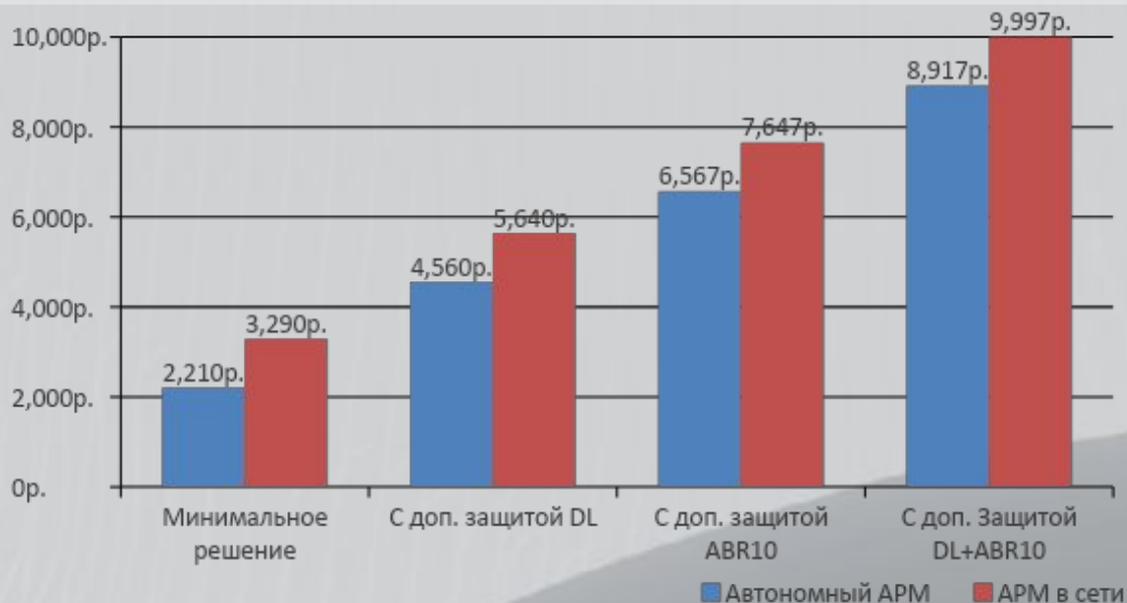
Ключевые функциональные особенности программ контроля и настройки «Check»

- сбор данных и формирование отчетов о **соответствии установленного продукта сертифицированной версии;**
- формирование отчетов об **установленных и неустановленных сертифицированных обновлениях безопасности;**
- **контроль загруженных обновлений** на предмет соответствия сертифицированным обновлениям продуктов Microsoft;
- **фиксацию и контроль целостности** исполняемых файлов и библиотек;
- **контроль и настройку параметров безопасности** в автоматизированном (на основании сертифицированных конфигураций) и ручном (установка значений отдельных параметров безопасности) режимах;
- **создание произвольных пользовательских конфигураций параметров безопасности** с возможностью наследования значений от сертифицированных конфигураций или текущего

Цена на типовые наборы СЗИ для защиты АРМ в ИСПДн 2-го класса и АС 1Г

Стоимость СЗИ на 1 АРМ*

Windows XP**	1295 р.
Антивирус Dr.Web	915 р.
DeviceLock 6.4.1	2350 р.
Acronis Backup & Recovery 10	4357 р.
UserGate 5.2.F	1080 р.



1. Базовая защита – ОС Windows XP + Антивирус Dr.Web
2. С доп. защитой DL - ОС Windows XP + Антивирус Dr.Web + DeviceLock 6.4.1
3. С доп. защитой ABR10 - ОС Windows XP + Антивирус Dr.Web + Acronis Backup & Recovery 10
4. С доп. защитой DL + ABR10 - ОС Windows XP + Антивирус Dr.Web + Acronis Backup & Recovery 10 + DeviceLock 6.4.1
5. АРМ в сети – все решения + UserGate 5.2.F

* Приведена стоимость типового решения для защиты автономного АРМ и АРМ в составе сети из расчета партии в 10 АРМ

** В стоимость сертифицированной версии Windows XP не входит стоимость лицензии Microsoft на ОС и ключа для получения обновлений

О компании АЛТЭКС-СОФТ



Основное направление деятельности:
производство, поставка и сопровождение сертифицированных средств защиты информации Microsoft, Aladdin, Smartline Inc., Acronis, Entensys и др.

Другие направления:

- оказание консалтинговых услуг при подготовке и в проведении сертификации СЗИ;
- оказание услуг по защите конфиденциальной информации и государственной тайны;
- разработка программных и аппаратно-программных средств защиты информации.

Лицензии АЛТЭКС-СОФТ

Лицензии ФСТЭК России:

Лицензия ФСТЭК № 2435 от 11 ноября 2009г. на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации)

Лицензия ФСТЭК № 2436 от 11 ноября 2009г. на проведение работ, связанных с созданием средств защиты информации

Лицензия ФСТЭК России №0641 от 16 января 2008г. на деятельность по технической защите конфиденциальной информации

Лицензия ФСТЭК России №0369 от 16 января 2008г. на деятельность по разработке и (или) производству средств защиты конфиденциальной информации



Лицензии ФСБ России:

Лицензия ФСБ России №14685 от 02 июля 2009г. на осуществление работ, связанных с использованием сведений, составляющих государственную тайну

Лицензия ФСБ России №5515Р от 14 мая 2008г. на распространение шифровальных (криптографических) средств

Лицензия ФСБ России № 7075К от 22 апреля 2009г. на осуществление разработки и (или) производства средств защиты конфиденциальной информации

Лицензия ФСБ России №10053Х от 21 января 2011г. на осуществление технического обслуживания шифровальных (криптографических) средств

Лицензия ФСБ России №10052П от 21 января 2011г. на разработку, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем

Лицензия ФСБ России № 10055У от 21 января 2011г. на предоставление услуг в области шифрования информации



Благодарю за внимание!

Вы сможете задать вопросы:

kia@altx-soft.ru

Тел. (495) 543-31-01

ООО

«Консультант Плюс Коми»

ms@sbis.komi.com

тел. 8(8212)29-15-51

доб.(185-187)

ООО

«Консультант Безопасность»

sales@consbez.ru

тел. 8(8212)44-88-42

www.consbez.ru