

Подходы Microsoft к обеспечению безопасности, защите персональных данных и повышению надежности продуктов и сервисов

Андрей Иванов, РТО

Содержание

- › **Стратегия**
- › **Жизненный цикл безопасной разработки**
- › **Инструменты**
- › **Технологии защиты данных**
- › **Compliance**

Защищенные информационные системы (Trustworthy Computing)



Безопасность

- Защита от атак
- Обеспечение конфиденциальности, целостности и доступности данных и систем
- Помощь в управлении рисками

Privacy

- Защита от нежелательных коммуникаций
- Предоставление пользователю выбора и контроля
- Следование общепринятым принципам и нормам

Надежность

- Заслуживающий доверия, доступный, предсказуемый, последовательный сервис
- Поддерживаемый. Устойчивый, легко (быстро) восстанавливаемый

Бизнес практики

- Совместимость
- Признанный в индустрии лидер, партнер мирового уровня
- Открытость, прозрачность

Повсеместная защита клиентов

Защита от угроз



Защита данных



Безопасный доступ



Universal Extensible Firmware Interface (UEFI)

Trusted Platform Model (TPM)

Scenarios

- Maintain software with a patch management solution
- Deliver software that is secure by design
- Operate a malware resistant platform and applications

- Secure data that is at rest with encryption
- Protect data that is in motion with encryption
- Protect data that is in use with access controls

- Manage the full identity lifecycle
- Validate user identity with strong authentication
- Secured and always connected remote access
- Protect resources as environment changes

Features

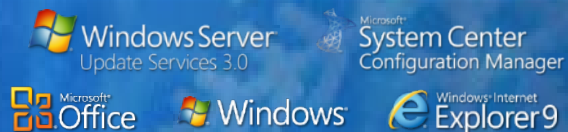
Secured Boot
Measured Boot
Protected View
IE Smart
Screen

Windows Standard User Accounts
User Account Control, and
AppLocker
Modern Applications
Security Development Lifecycle (SDL)

BitLocker
MDOP -BitLocker Administration and Monitoring
Office Information Rights Management (IRM)
Office Encrypted File System
Active Directory Rights Management Services z

Active Directory
Direct Access
Network Access Protection
Dynamic Access Control

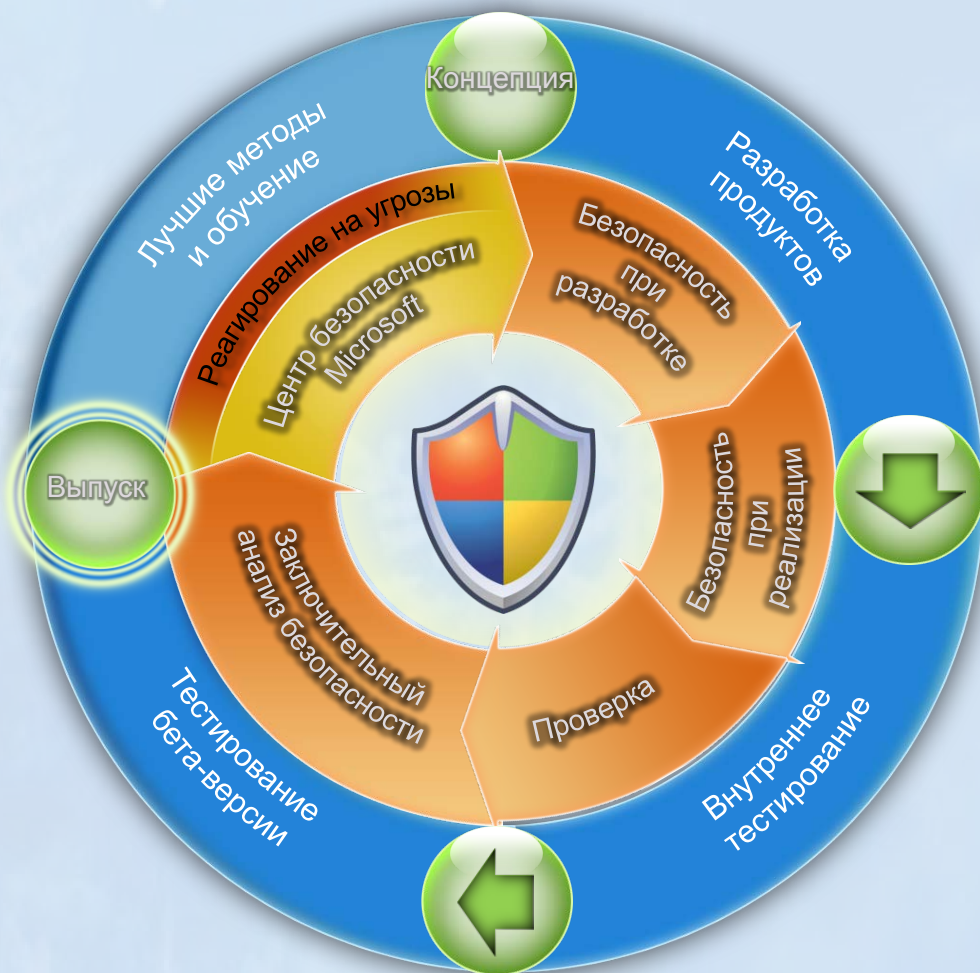
Products



Содержание

- › Стратегия
- › **Жизненный цикл безопасной разработки**
- › Инструменты
- › Технологии защиты данных
- › Compliance

Security Development Lifecycle



Цели

Защита пользователей:

- сокращение количества уязвимостей;
- сокращение опасности уязвимостей.

Основные принципы

- Практический подход
- Упреждение угроз - это не просто поиск ошибок
- Решение проблем безопасности на ранних стадиях
- Безопасность при разработке
- Безопасность после выпуска ПО

Зачем вам разработка безопасного ПО?

- › Новейшие исследования показывают однозначную связь между разработкой безопасного ПО и бизнес эффективностью компании:
- Исследование Aberdeen:
 - › Предотвращение одной уязвимости почти полностью покрывает годовые затраты на повышение безопасности разработки
 - › Предотвратить проблему с безопасностью в 4 раза дешевле чем разбираться с ее последствиями
- Исследование Forrester:
 - › Разработка безопасного ПО еще не стала широко распространенной практикой
 - › Компании применяющие методы SDL демонстрируют гораздо более быстрый возврат инвестиций

Стоимость устранения уязвимостей

Исправлять ошибки **после выпуска дороже в 30 раз** чем на стадии разработки дизайна

Относительная стоимость устранения ошибок



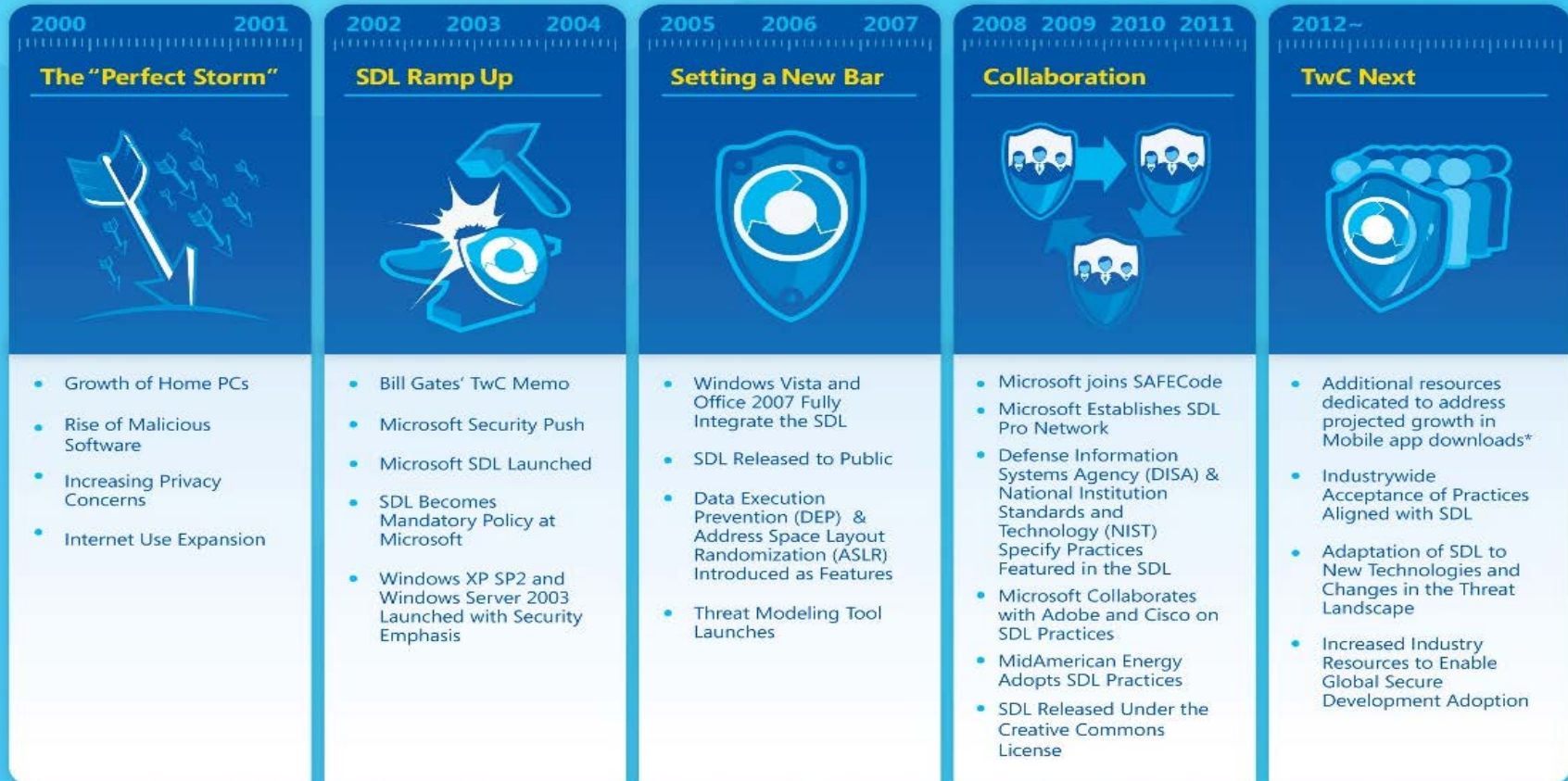
История развития SDL

Microsoft Security Development Lifecycle (SDL) Evolution

TwC Next: Marking a Milestone. Continuing Our Commitment.

The Microsoft SDL is the industry-leading software security assurance process. A Microsoft wide initiative and mandatory policy since 2004, the Microsoft Security Development Lifecycle (SDL) has played a critical role in improving the security and privacy of Microsoft software and services with the goal of reducing customer risk. Combining a holistic

and practical approach, the Microsoft SDL embeds security and privacy throughout the development process. We believe that by freely sharing the SDL resources, tools, and collaborating with the industry on secure application development, together we can help build safer more trusted computing experiences for everyone.



Microsoft Secure Software Development Conference.

<http://mssdcon.ru>

О конференции

MSSD-3 — третья по счету конференция, посвященная всестороннему обсуждению популярной и важной темы – минимизация уязвимостей программного обеспечения при его разработке. Ведущие российские и западные эксперты, сотрудники партнерских компаний, специализирующихся на аудите и анализе защищенности информационных систем, а также представители заказчиков примут участие в дискуссии о том, как разработать защищенный продукт, удовлетворяющий всем требованиям, предъявляемым к системам обработки критически важных данных.

Читать далее



Докладчики



Стив Липнер
Старший директор по направлению стратегического планирования корпорации Microsoft

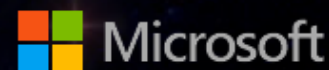


Рустэм Хайретдинов
CEO Appercut Security

Посмотреть всех докладчиков



Организаторы



Посмотреть всех партнеров



5.03.2013

Содержание

- › Стратегия
- › Жизненный цикл безопасной разработки
- › **Инструменты**
- › Технологии защиты данных
- › Compliance

Инструменты

SDL

- **Этап: Требования**
 - Шаблоны SDL процесса для VSTS
- **Этап: Проектирование**
 - Инструмент моделирования угроз (SDL Threat Modeling Tool version 3.1.8)
- **Этап: Реализация**
 - Microsoft Code Analysis Tool .NET (CAT.NET)
 - FxCop
 - banned.h
 - Anti-Cross Site Scripting (Anti-XSS) Library
- **Этап: Проверка**
 - SDL MiniFuzz File Fuzzer
 - BinScope Binary Analyzer
 - Attack Surface Analyzer

Solution Accelerators

- **Security Compliance Manager**
- **Compliance Solution Accelerators**
 - Data Classification Toolkit for WS 2012
 - IT Compliance Management Series

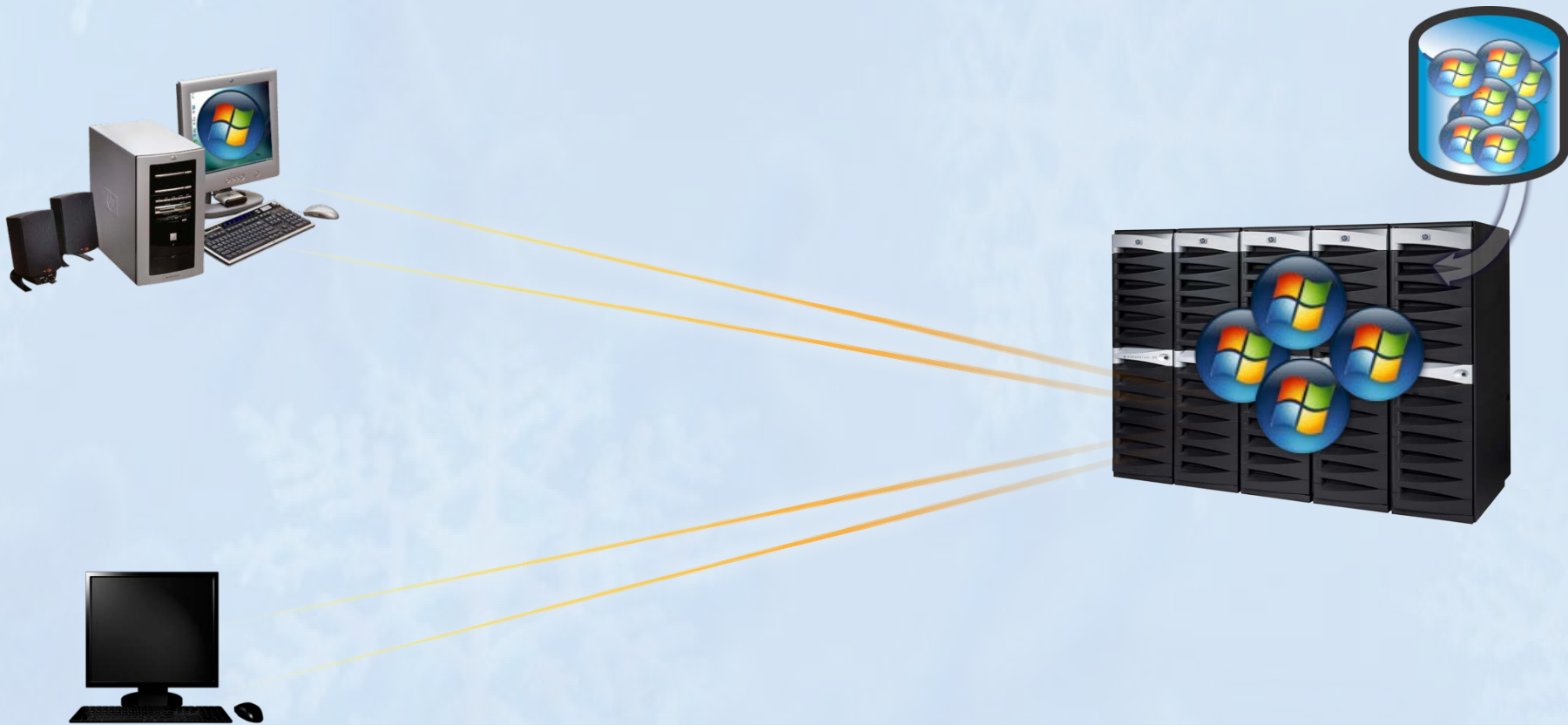
SRMG

- Data Gathering Tool
- Detailed Level Risk Prioritization
- Summary Risk Level

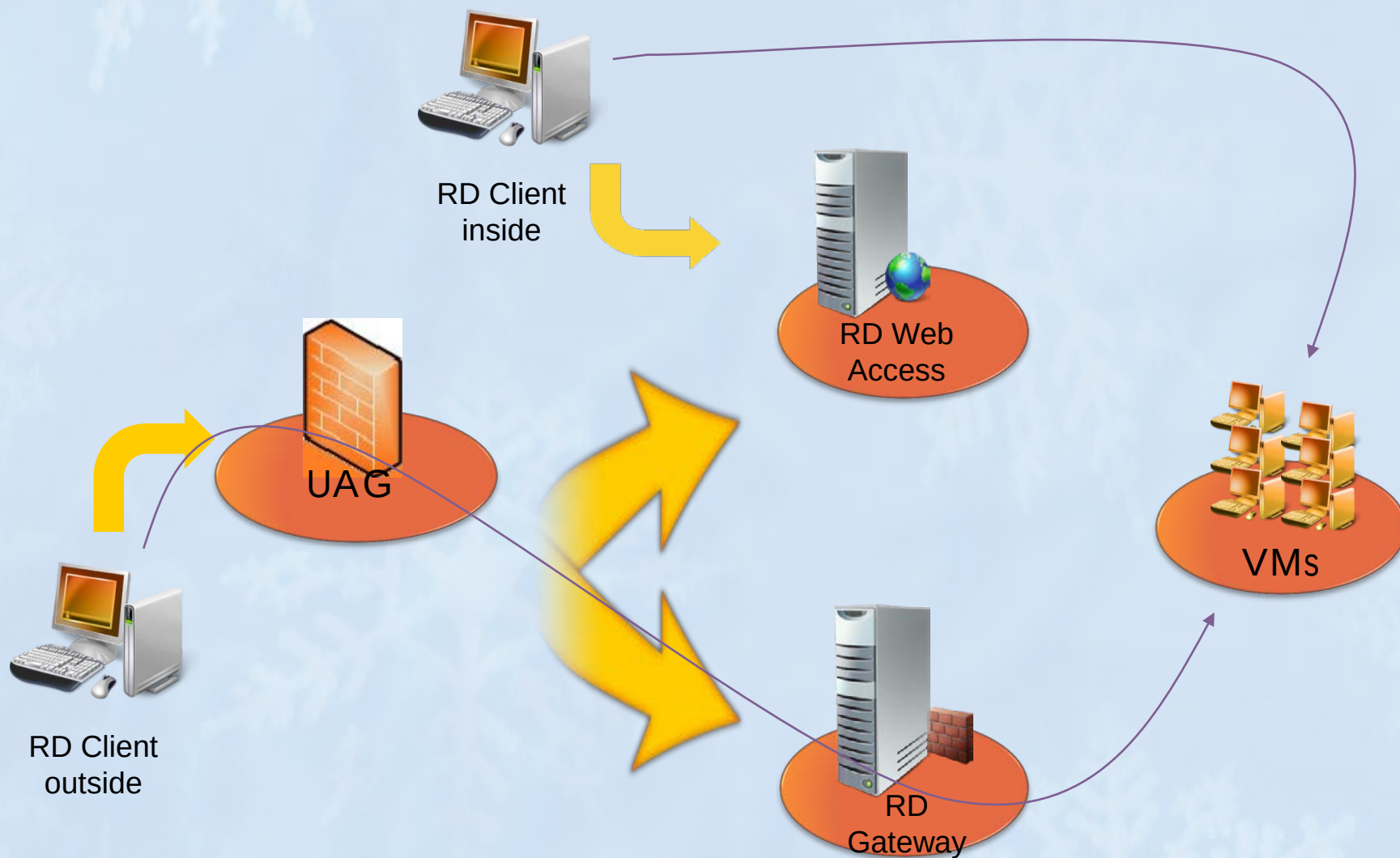
Содержание

- › Стратегия
- › Жизненный цикл безопасной разработки
- › Инструменты
- › Технологии защиты данных
- › Compliance

Virtual Desktop Infrastructure



Доступ к виртуальным машинам



BitLocker

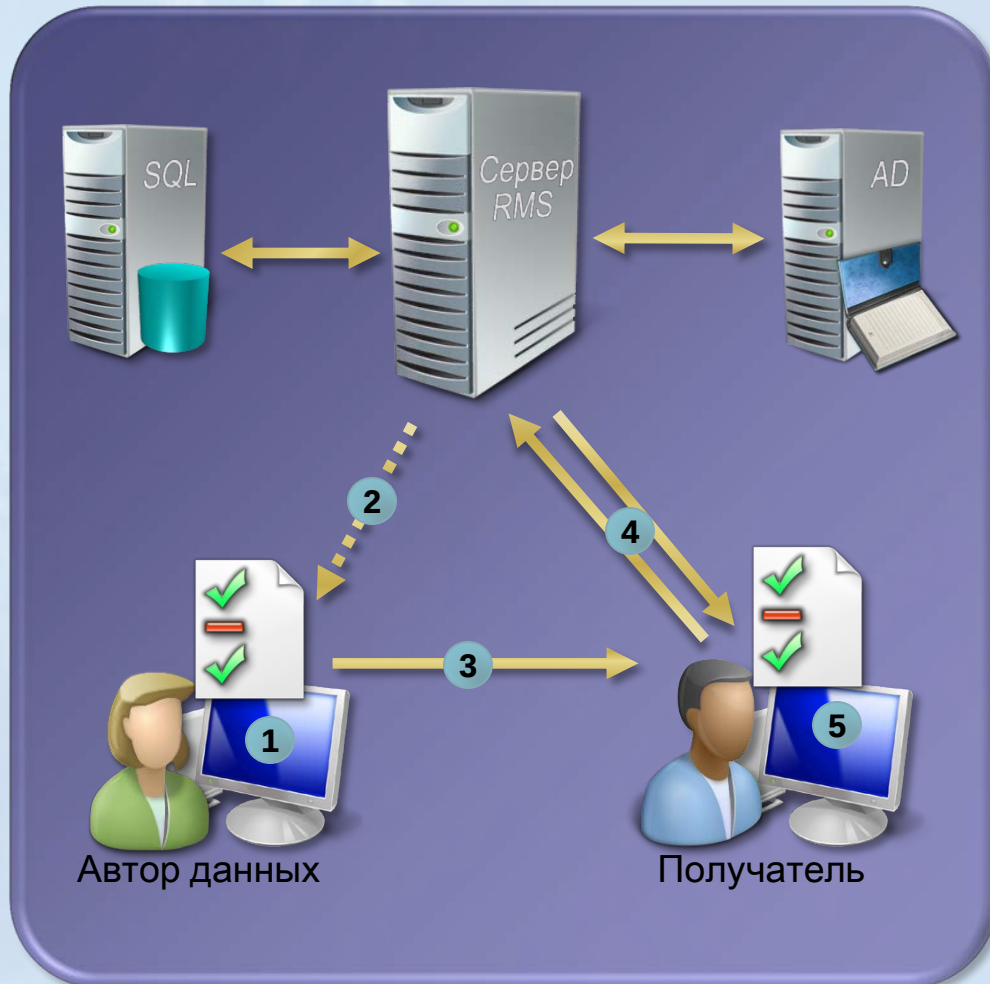
- › Использование TPM
- › Защита информации на дисках (в том числе системном)
- › Проверка целостности загрузочных компонент
- › Возможность восстановления
- › Активация при установке ОС
- › Шифрование только занятого места на диске
- › Network Unlock



Windows To Go

- › Загрузочная флешка с Windows 8
- › Автоматизированное распространение (разливка)
- › Безопасность
 - Отключение внутренних дисков
 - Bitlocker
 - Выключение системы при отключении флешки
 - Политики безопасности

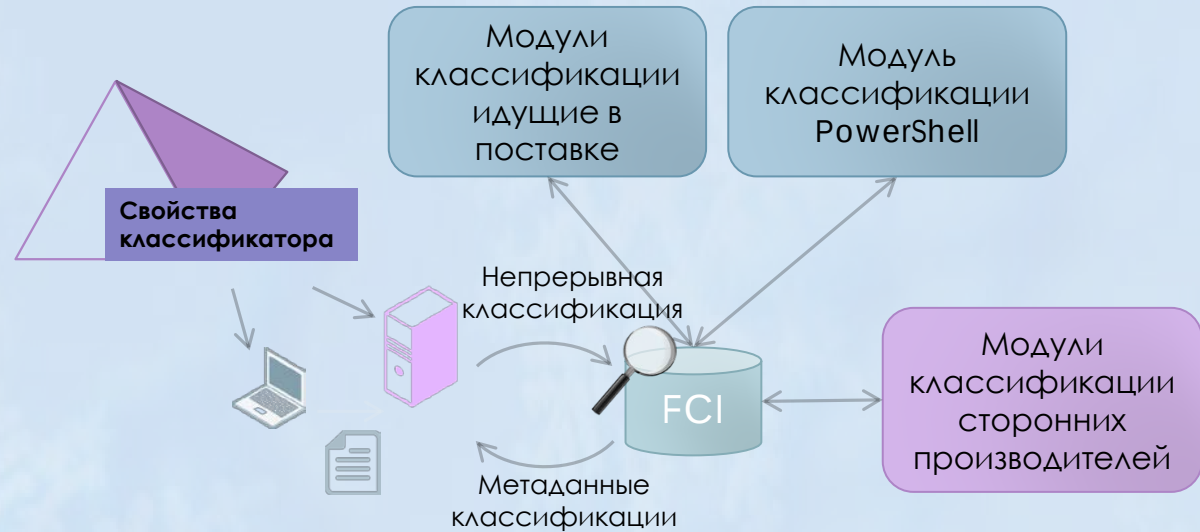
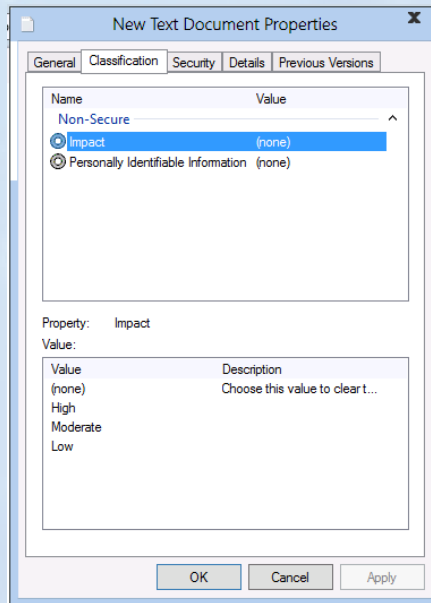
Служба управления доступом (AD RMS)



1. Автор получает сертификаты
2. Автор использует права и правила для файла создает "Издательскую лицензию" для файла и файл шифруется
3. Автор распространяет файл
4. При открытии файла получателем, приложение соединяется с RMS сервером, который проверяет пользователя и производит "Лицензию использования"
5. Приложение при работе с файлом обеспечивает исполнение правил

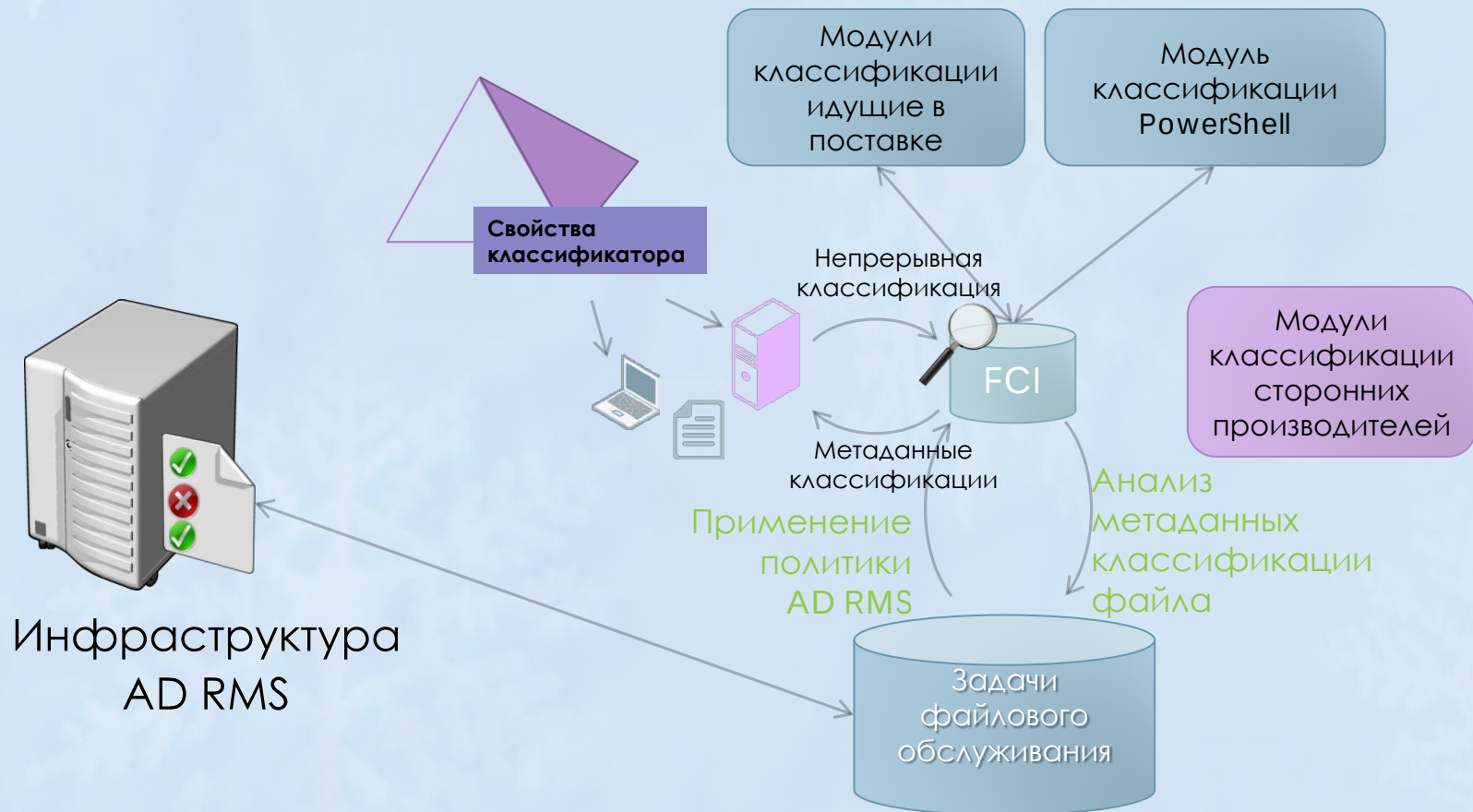
Механизмы классификации Windows Server 2012

File Classification Infrastructure



Механизмы классификации Windows Server 2012

File Management Tasks



Содержание

- › Стратегия
- › Жизненный цикл безопасной разработки
- › Инструменты
- › Технологии защиты данных
- › **Compliance**

Сертификация во ФСТЭК

- › Сертифицировано более 30 продуктов Майкрософт. Все продукты Майкрософт сертифицированы «как есть», без изменений, и могут быть использованы для построения автоматизированных систем уровня защищенности 1Г и для систем обработки персональных данных

- › **От**
 - Windows XP
 - Windows Server 2003 и
 - антивирусов Forefront

- › **До**
 - Windows 7
 - Office 2010 Professional Plus и
 - Lync 2010

Новые сертификаты ФСТЭК

- › **Forefront Endpoint Client Protection** антивирус
- › **Lync Server 2010**
- › **SharePoint Server 2010**
- › **Office 2010 Professional Plus**
- › **Dynamics CRM 2011**

Будут сертифицированы во ФСТЭК

- › **Windows 8**
- › **Windows Server 2012**
- › **System Center 2012**
- › **Office 2013**
- › **И многие другие продукты**

Сертификация в ФСБ

- › **Windows XP Professional** - сертификат
- › **Windows Server 2003 Enterprise** - сертификат
- › **SQL Server 2008** - сертификат
- › **Windows 7**
 - получено положительное заключение
- › **Windows Server 2008 R2**
 - получено положительное заключение
- › **Exchange Server 2010**
 - Сертификация закончена, идет экспертиза
- › **Windows 8**
 - Идет сертификация

Спасибо!

Хорошего вечера! 😊