Intel Active Management Technology

Процессорная технология Intel® vPro™

Процессор

Набор микросхем (чипсет)

Сетевой адаптер

Ключевые технологии Intel

Программное обеспечение

Intel Active Management Technology

ОБЗОР

Ингредиенты vPro в десктопах

- **45-нм процессоры**
  - Core 2 Duo (E8xxx)
  - Core 2 Quad (Q9xxx)
  - Поддержка VTx и TXT
- **Чипсет Intel Q45 Express с южным мостом ICH10**
- **Сетевой адаптер Intel 82567LM (Boazman)**
- **BIOS и Firmware**
  - Микропрограмма Intel AMT 5.0

Ингредиенты vPro в ноутбуках

- **45-нм процессоры**
  - Core 2 Duo
  - Core 2 Quad
  - Поддержка VTx и TXT
- **Мобильные чипсеты Intel GM47, GM45 и PM45 с южным мостом ICH9M**
  - GS45 + ICH9M-SFF
- **Сетевой адаптер Intel 82567LM (Boazman)**
- **Беспроводной адаптер Intel WiMAX/WiFi Link 5350 или Intel® WiFi Link 5300**
- **BIOS и Firmware**
  - Микропрограмма Intel AMT 4.0
  - Intel Anti-Theft Technology (AT-p)

Эволюция

2006

Кодовое имя "Averill"
Сентябрь 2006
Intel® AMT 2.0
Intel ® VT-x
Готова для Virtual Appliance

2007

Кодовое имя "Weybridge"
Август 2007
Intel® AMT 3.0
Intel VT-x
Intel VT-d
Intel® TXT

2008

Кодовое имя "McCreary"
Intel® AMT 5.0
DASH 1..0
Intel VT-x
Intel VT-d
Intel TXT
Встроенный TPM

2009/10

Кросс-платформенная
Кодовое имя "Piketon/Calpella"
Intel AMT 6.0
Anti-Theft Technology
Intel® VT-x, VT-d
Intel® TXT

Десктопы

Ноутбуки

Кодовое имя "Santa Rosa"
Май 2007
Intel® AMT 2.5

Кодовое имя "Montevina"
AT-p
Intel® AMT 4.0
DASH 1..0
Intel® VTx, VT-d
Intel® TXT
WiMax

Active Management Technology 5

- **Аппаратная система удаленного управления, независимая от установленной операционной системы**
  - Управление питанием ПК
  - Контроль событий на аппаратном уровне + аудит
  - Инвентаризация оборудования и ПО
  - ***IDE Redirection***, управление процессом загрузки ПК
  - ***Serial over LAN***, удаленная текстовая консоль (+ доступ в BIOS)
  - ***System Defense***, фильтрация сетевого трафика
  - ***Agent Presence***, контроль выполнения системных приложений*
  - ***Client Initiated Remote Access***, запрос помощи администратора

AMT является уникальной технологией

*** - при установленной ОС, системных драйверах и поддержке данной функции приложением**

AMT: особенности использования

- **Для доступа ко всем функциям AMT требуется центральная консоль управления**
- **AMT доступна только через интегрированный сетевой контроллер при наличии электропитания**

- **Требуется предварительная активация функций AMT**
  - Вручную в BIOS (режимы SMB и Enterprise)
  - С помощью ключа на USB-дискете (One-Touch Configuration, только в режиме Enterprise)
  - С помощью специального ПО (Remote Configuration, только в режиме Enterprise)

AMT расширяет возможности систем централизованного управления

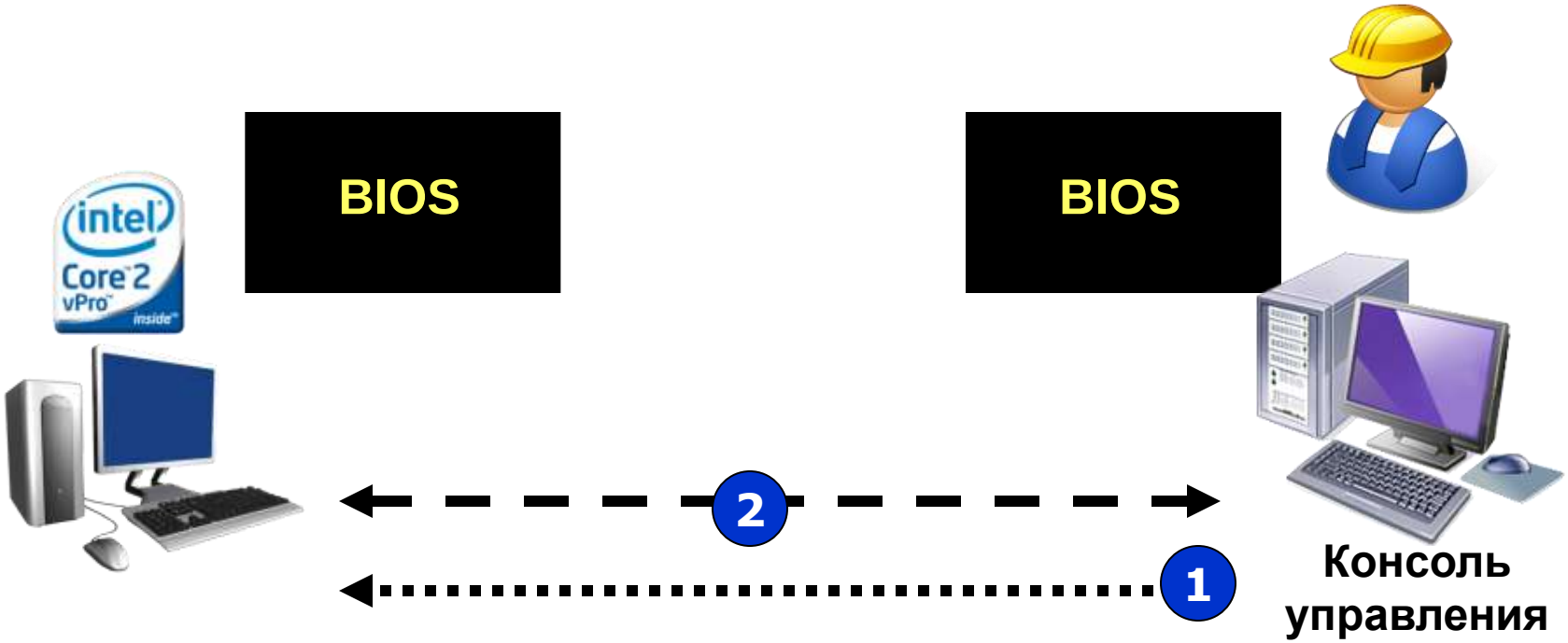
Сценарий 1: настройка BIOS

BIOS

ПК без vPro

Обычный ПК: администратор должен иметь физический доступ
Проблема: значительные затраты времени

Сценарий 1 с AMT: настройка BIOS

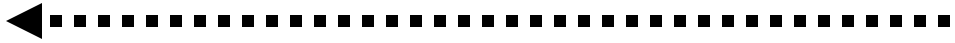


ПК с процессорной технологией Intel vPro

1. Команда на включение питания по внеполосному каналу
2. Текстовая консоль *Serial-over-LAN*

Настройка оборудования без потерь времени

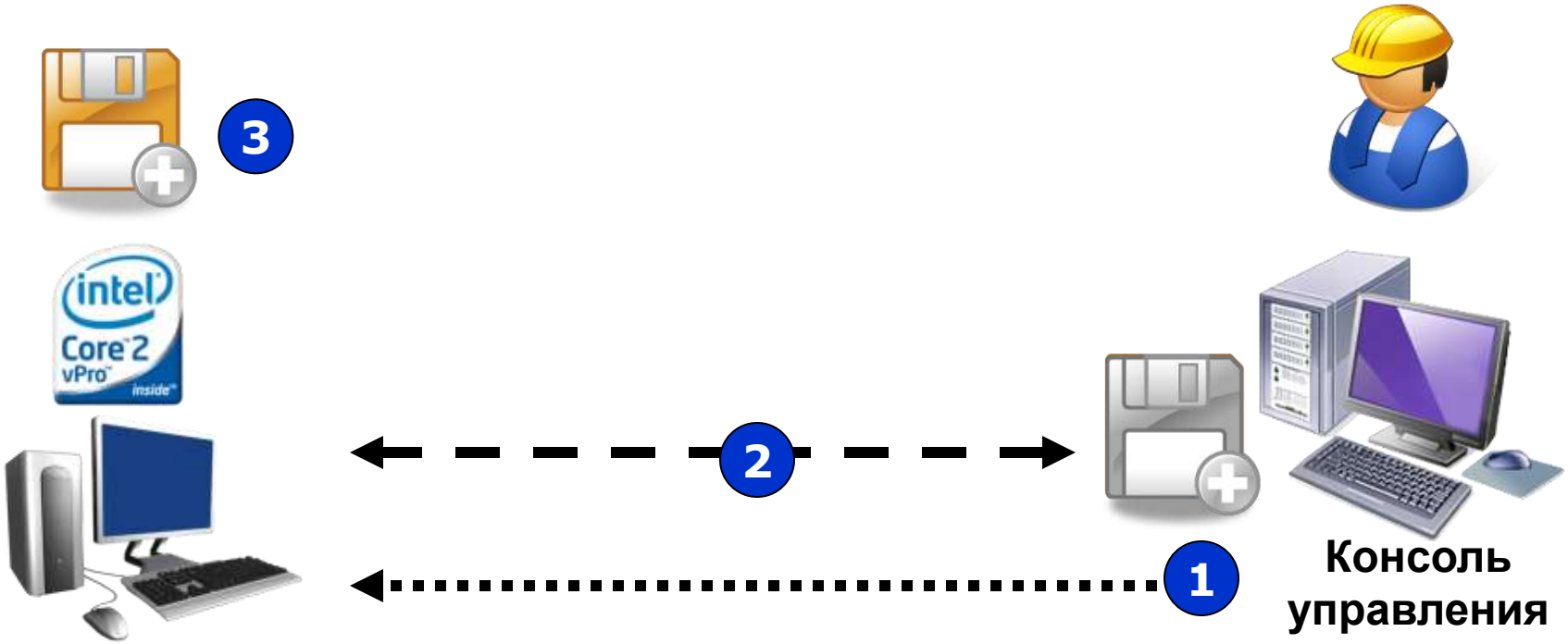
Сценарий 2: установка ОС



ПК без vPro

Обычный ПК: администратор должен иметь физический доступ
Проблема: значительные затраты времени на подготовку ПК

Сценарий 2 с AMT: установка ОС



ПК с процессорной технологией Intel vPro

1. Команда на включение питания с опцией *IDE Redirection*
2. ПК использует удаленный источник загрузки
3. Производится развертывание образа ОС

Сокращаем затраты на внедрение новых ПК

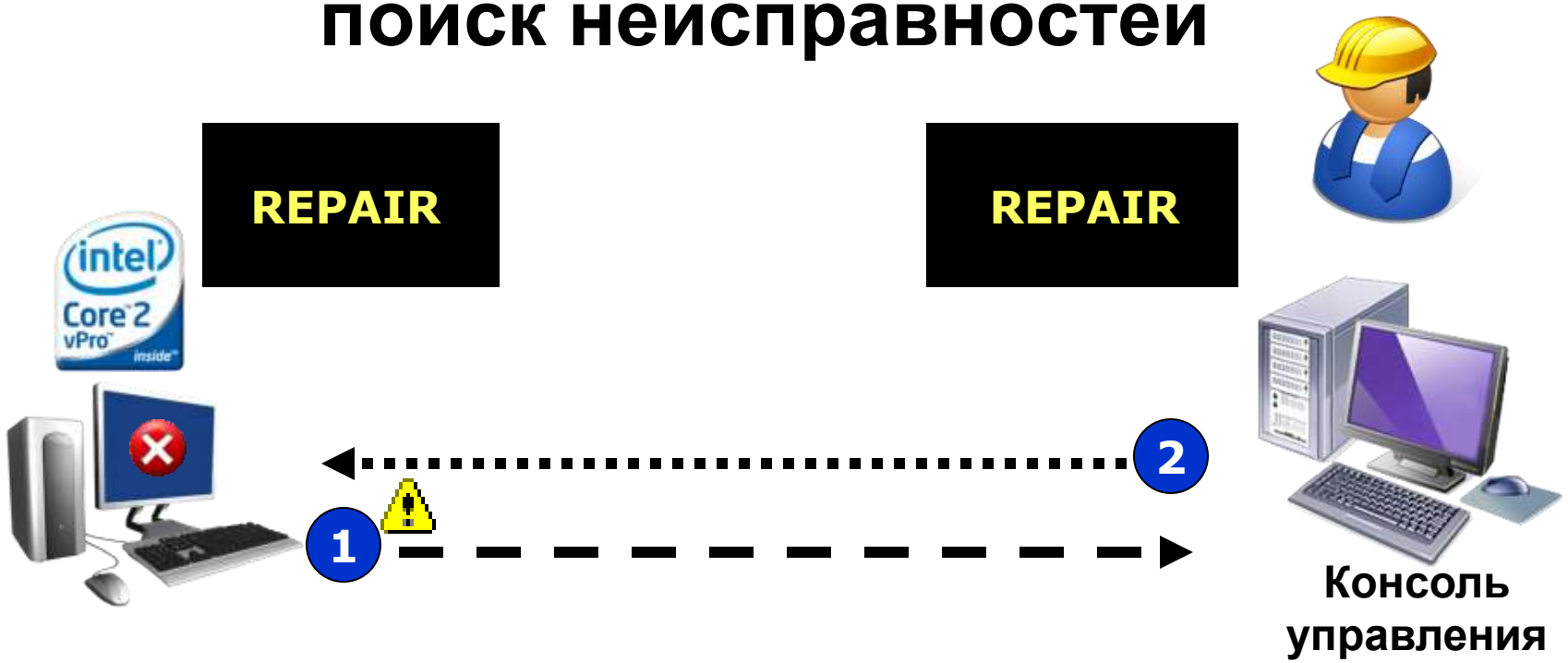
Сценарий 3: поиск неисправностей

REPAIR

ПК без vPro

Проблема обычных ПК:
Для диагностики требуется прямой доступ к компьютеру, даже если сбой вызван ПО
Большие потери рабочего времени

Сценарий 3 с AMT : поиск неисправностей



ПК с процессорной технологией Intel vPro

1. Может уведомить об аппаратном сбое по SNMP
2. Администратор может запустить на ПК утилиты диагностики, используя *IDE Redirection* и *SoL*
3. Выезд только в случае аппаратной неисправности

Эффективное решение самой острой проблемы

Intel® vPro™ + консоль управления: результаты эксплуатации

- **Сокращение количества выходов на место сбоя:**
  - При программных неисправностях – **на 91%**
  - При аппаратных неисправностях – **на 56%**
- **Сокращение потерь времени сотрудников**
  - При программных неисправностях – **на 83-98%**
  - При аппаратных неисправностях – **на 65-70%**
- **Сокращение времени на обновление ПО**
  - При установке на 1000 ПК – **на 85%**
  - Для достижения приемлемого уровня защиты – **на 94%**

ИТ служба работает более эффективно!

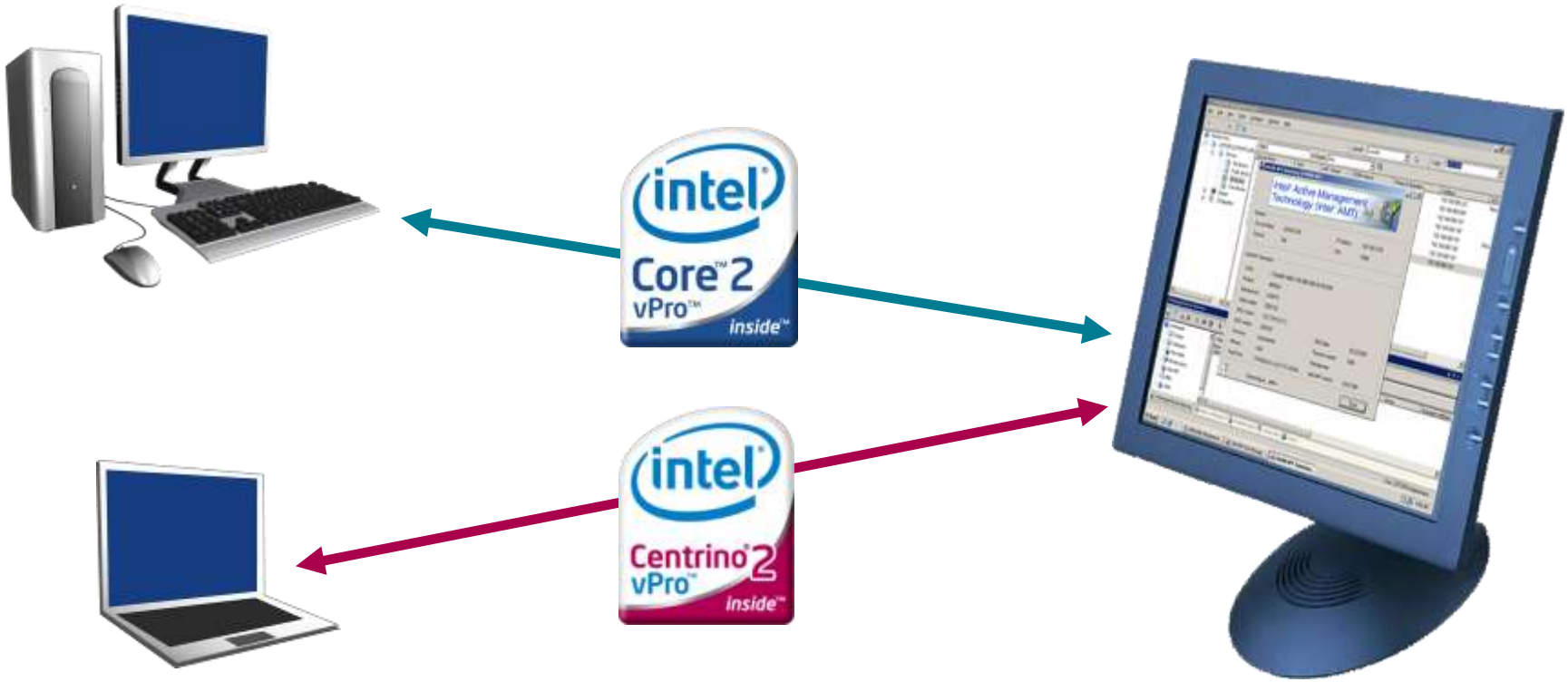
Источник: Анализ предварительного тестирования процессорной технологии Intel® vPro™ в крупных IT-подразделениях; 2006-2007

Системы управления с поддержкой процессорной технологии Intel® vPro™

- **Интегрированная поддержка:**
  - SyAM Software* System Area Manager* 3.45
  - LANDesk* Management Suite* 8.8
  - Altiris* Management Suites*
  - Microsoft* System Center* Configuration Manager* 2007 SP1
  - HP* Configuration Management Software*
  - CA* Unicenter*
  - Famatech* Remote Administrator* 3.3
- **Специальные обновления от Intel:**
  - Microsoft* Systems Management Server* 2003 R2 SP3
  - Microsoft* System Center Operations Manager* 2007
  - Microsoft* System Center Essentials* 2007

Ведущие производители ПО поддерживают vPro!

Консистентное использование



Управление ПК, ноутбуками и серверами

AMT

ЕДИНАЯ

Консоль управления

AMT

IPMI,
RMM,
IMS RMC

Реальное управление всеми устройствами в сети!

Процессорная технология Intel® vPro™

- Энергоэффективная производительность
- Уникальная технология управления Active Management Technology
- Снижение затрат на обслуживание
- Широкая поддержка ИТ отрасли

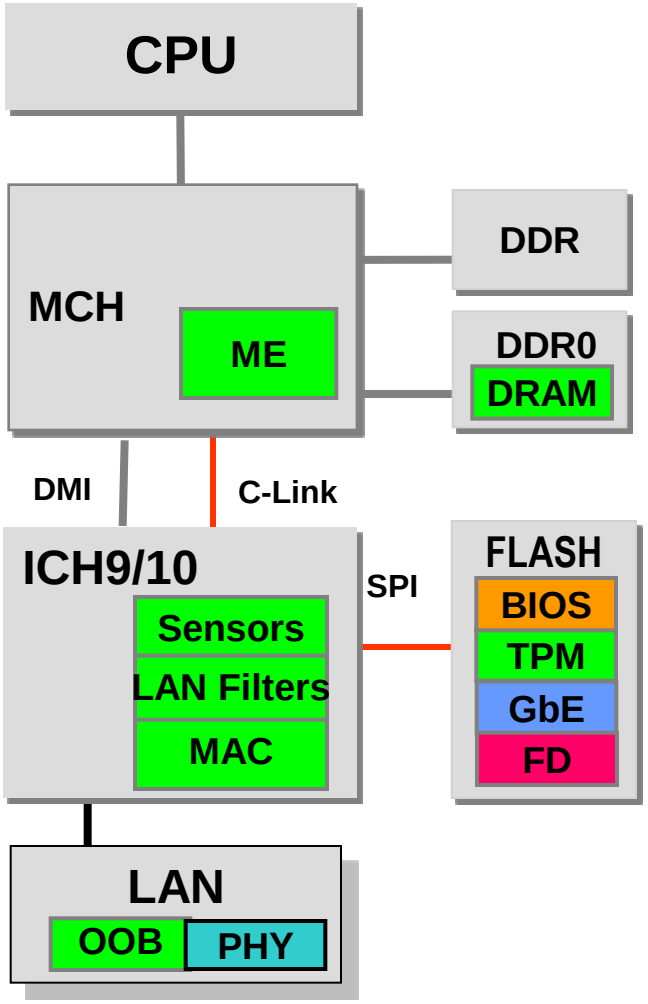
Будьте эффективны вместе с Intel® vPro™!

Intel Active Management Technology

УСТРОЙСТВО

AMT: архитектура

- **Manageability Engine (ME) в MCH**
- **Внеполосный канал управления**
  - Активен даже в состоянии S5
  - Не зависит от работы ОС
- **Используются 16Мб ОЗУ (банк 0)**
- **Фильтры трафика в ICH**
- **Специальная область данных в микросхеме флеш-памяти**
  - Хранение кода ME
  - Хранение данных с шифрованием

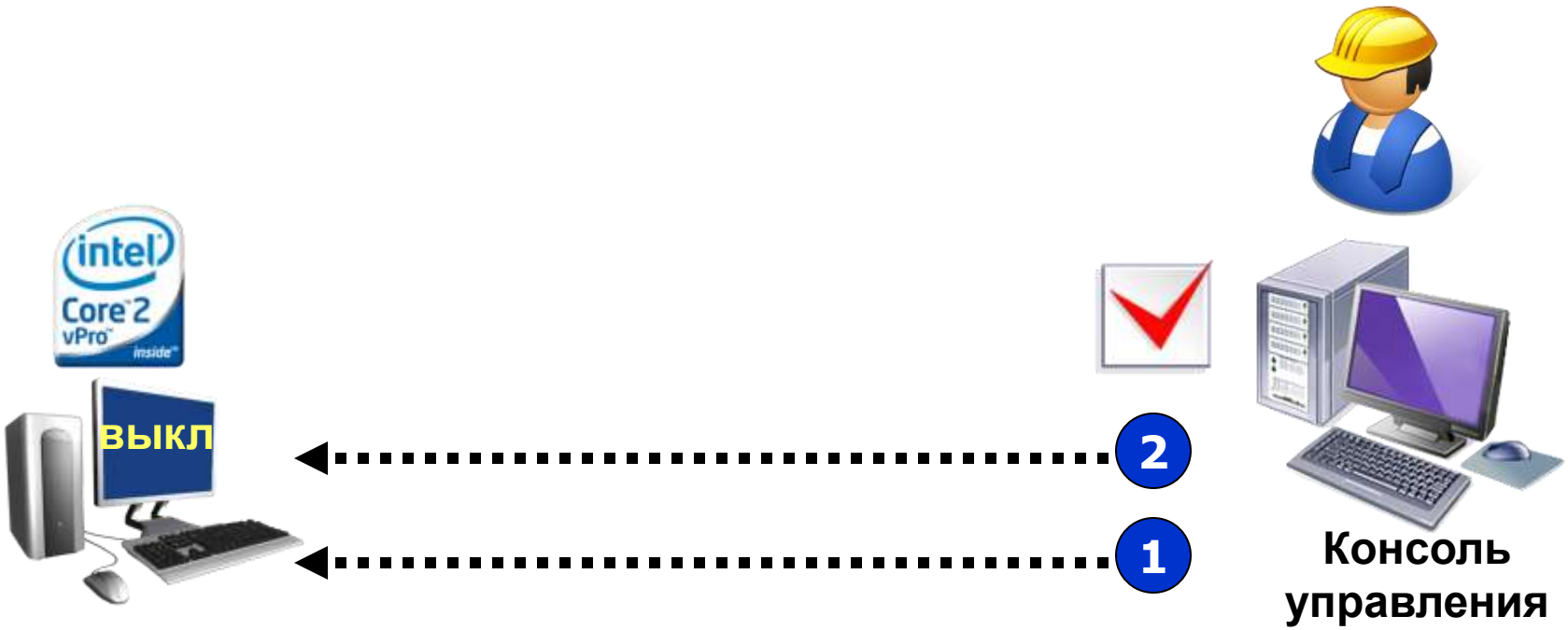


Сценарий 4: инвентаризация

ПК без vPro

Обычный ПК: администратор должен иметь физический доступ
Проблема: недостоверные данные о выключенных ПК
До 20% устройств остаются «в тени»
Юридические риски, связанные с лицензиями на ПО

Сценарий 4 с AMT: инвентаризация



ПК с процессорной технологией Intel vPro

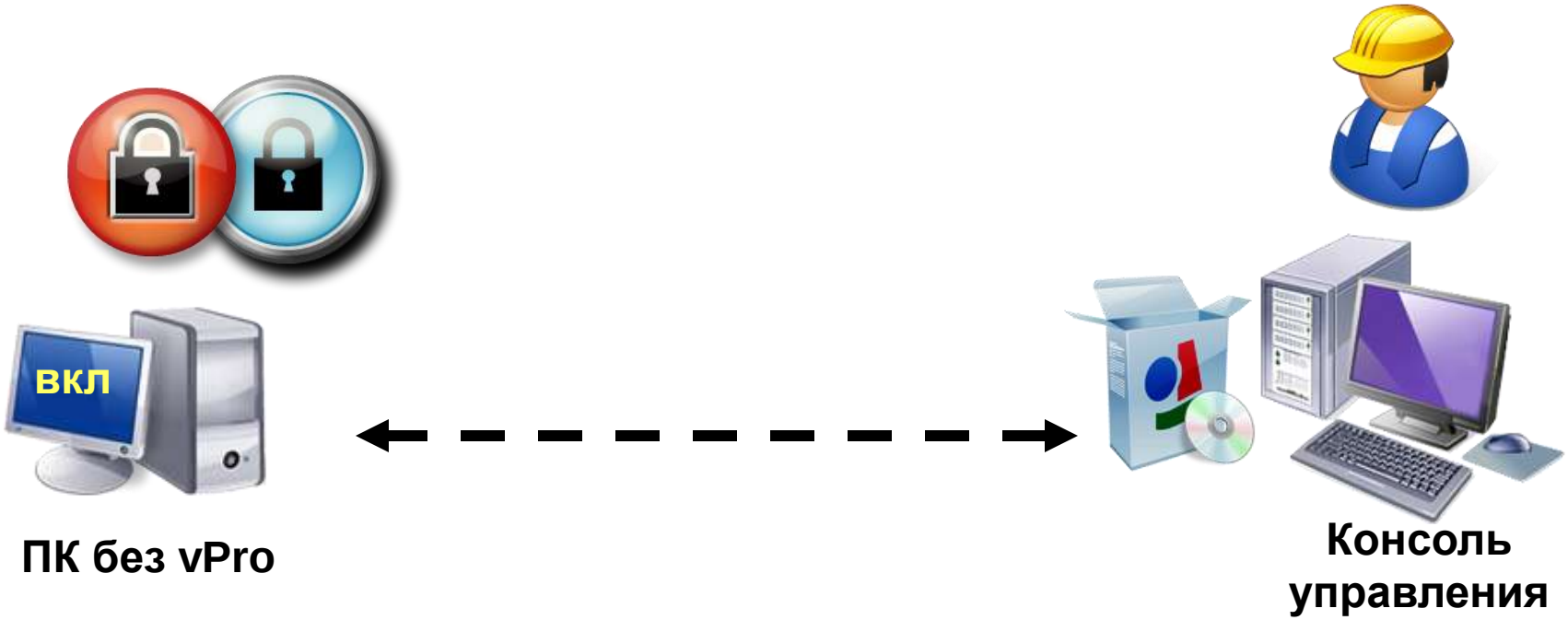
1. Считываем данные из энергонезависимой памяти AMT
   даже с выключенного ПК!
2. Можем включить ПК и провести инвентаризацию по запросу

Точная информация – корректная работа ИТ отдела

Особенности аппаратной инвентаризации

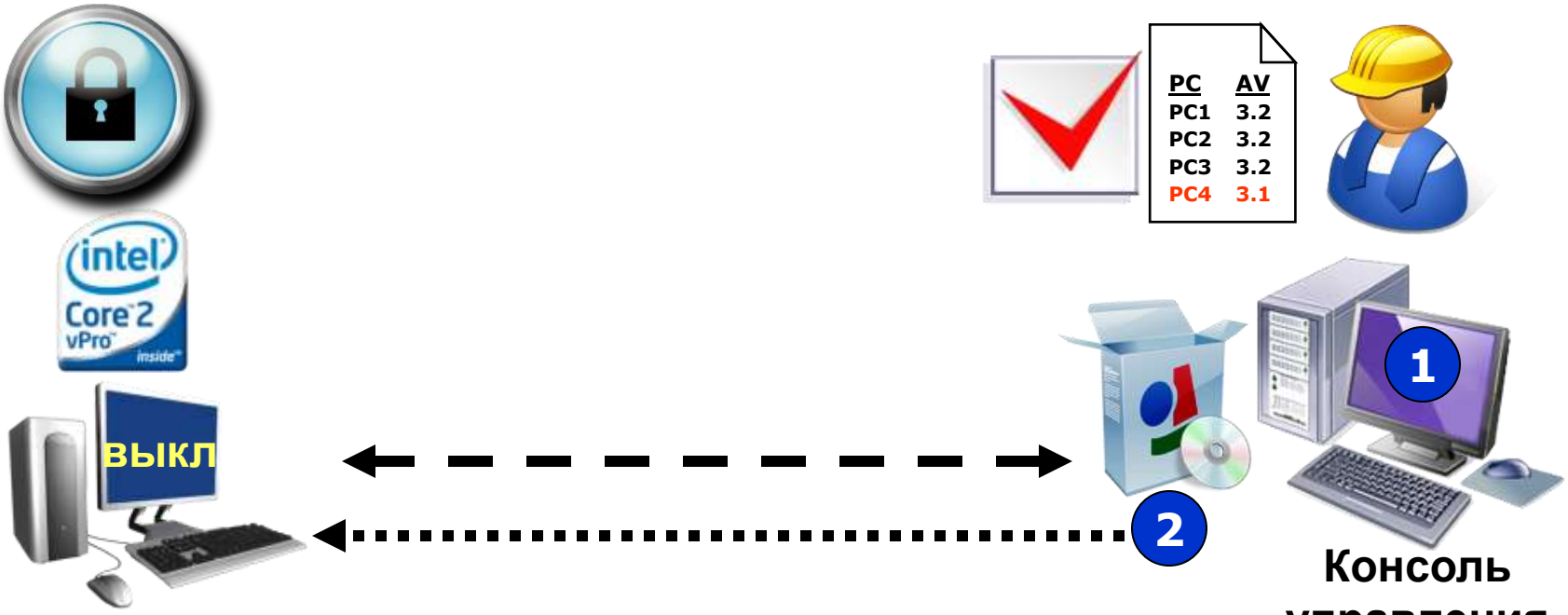
- **Доступные данные**
  - Системная плата
  - Процессор
  - ОЗУ
  - Жёсткий диск
- **USB устройства и периферия недоступны**
- **Поставщик BIOS определяет объём**
- **Консоль определяет, какие данные можно использовать**

Сценарий 5: обновление ПО



Обычный ПК: обновление возможно только в рабочее время
Проблема: пользователи теряют время, ожидая завершения работ
Установка обновления на все ПК требует много времени

Сценарий 5 с AMT: обновление ПО



ПК с процессорной технологией Intel vPro

1. **Консоль управления может обновлять ПК по заданному расписанию, используя данные инвентаризации**
2. **Консоль управления может включить ПК самостоятельно, провести обновление и снова выключить ПК**

Быстрое обновление повышает уровень защищенности

Особенности инвентаризации ПО

- **Инвентаризацию ПО осуществляют специальные программные агенты**
- **Разработчики агентов определяют:**
  - Формат данных
  - Содержание записей
  - Периодичность обновления информации
- **Данные хранятся в NVRAM**
- **Данные о ПО доступны только с консоли**

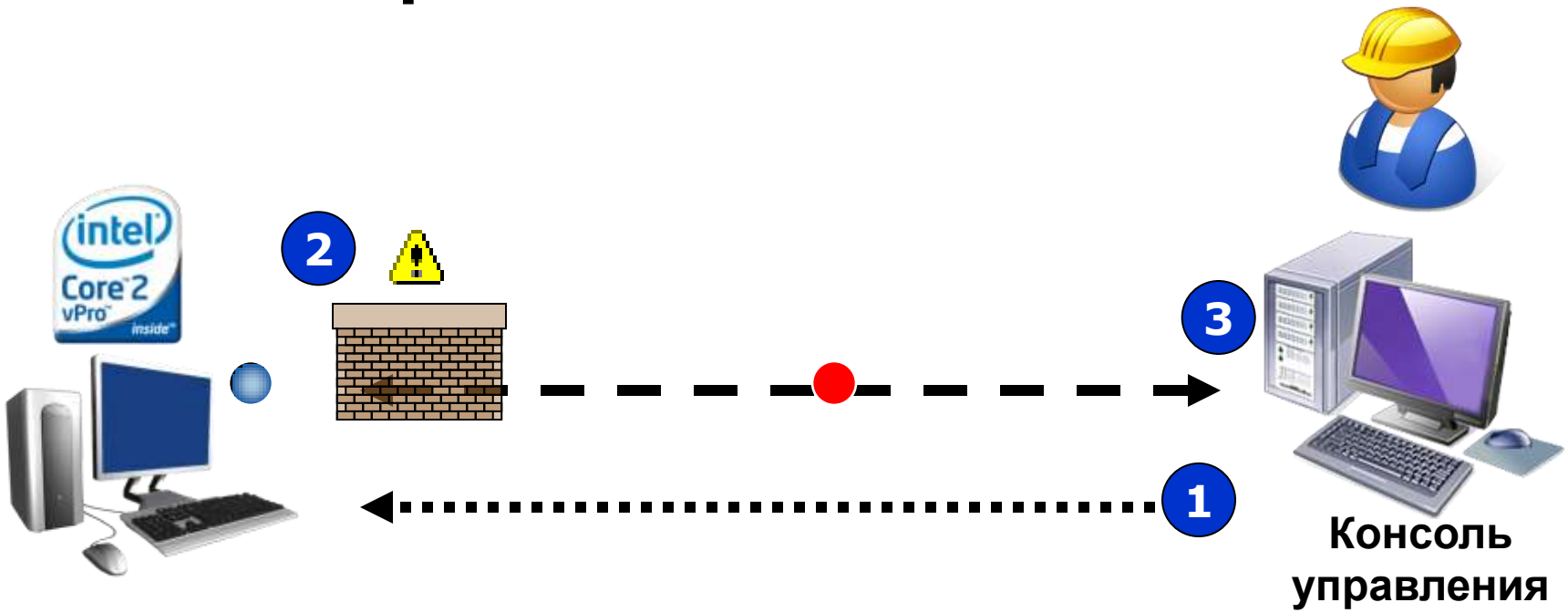
Сценарий 6: защита сети

ПК без vPro

Консоль управления

Проблема обычных ПК: с момента появления новой сетевой угрозы до обновления ПО безопасности есть период повышенной угрозы

Сценарий 6 с AMT: защита сети



ПК с процессорной технологией Intel vPro

1. Администратор задает фильтры сетевого трафика ***System Defense***
2. Система самостоятельно анализирует вх/исх пакеты данных
3. При срабатывании фильтра администратор получает уведомление

Отражаем сетевые атаки на аппаратном уровне

Принципы фильтрации трафика

- **Правила задаются с консоли**
- **Фильтры пакетов IPv4**
  - 32 фильтра RX
  - 32 фильтра TX
  - 1 Rx/Tx фильтр по умолчанию
  - 1 Rx/Tx фильтр Anti-Spoofing (подмена адреса)
- **Политики – наборы фильтров**
  - Одна политика активна единовременно
  - Политики имеют приоритеты для координации работы System Defense с Agent Presence
  - Количество фильтров в политике зависит от типов используемых фильтров

Параметры фильтров

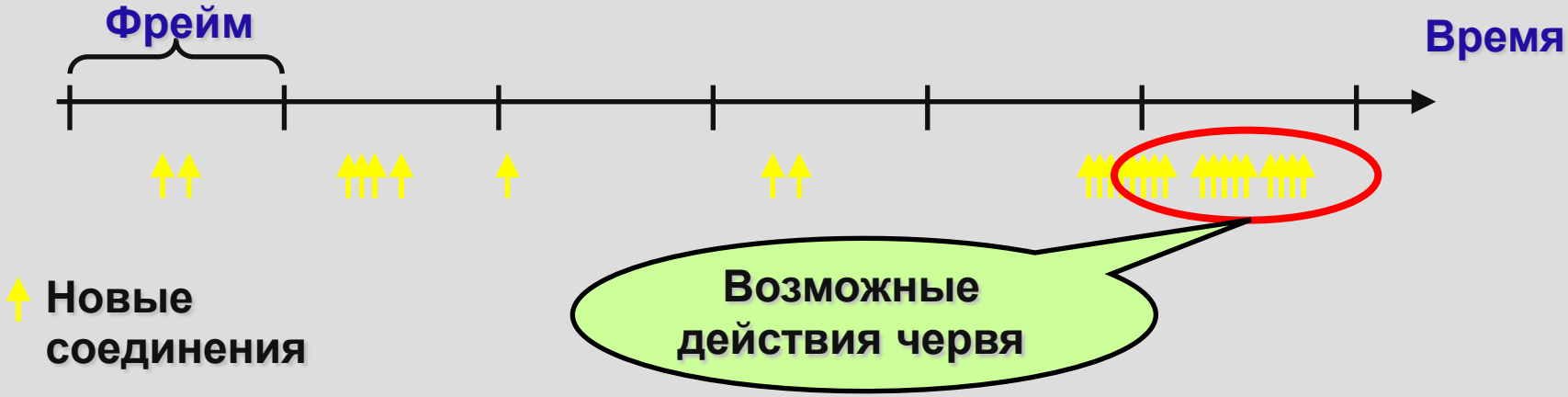
- **Виды фильтров**
  - Основной – блокировка по параметрам пакета
  - Rate Limit – ограничение количества пакетов за единицу времени
  - Статистический – учёт количества пакетов
- **Параметры для анализа**
  - IP адреса отправителя и получателя
  - Тип протокола L2
  - Тип следующего заголовка
  - Флаги TCP
  - Исходящий и входящий TCP/UDP порты

Сценарий 7: защита от «червей»

ПК без vPro

Обычный ПК: защиту от «червей» осуществляет только ПО
Проблема:
Есть периоды повышенной опасности, во время которых ПО не может уничтожать вирус
Значительный рост нагрузки на сеть
Угроза заражения других ПК

Сценарий 7 с AMT: защита от «червей»



ПК с процессорной технологией Intel vPro

1. Администратор активирует специальный фильтр *System Defense Heuristics*
2. Система самостоятельно считает кол-во исх. запросов на открытие соединений в ед. времени
3. При превышении порогового значения доступ в сеть блокируется

Изолируем зараженные ПК на аппаратном уровне

Эвристический анализ трафика

- **Последовательность событий**
  - Вирус проводит сканирование адресов и портов
  - Эвристический анализатор контролирует количество **исходящих** запросов на разные адреса в единицу времени
    - Сканируются все UDP и TCP/SYN заголовки (~1% трафика)
    - Количество подозрительных соединений 8-64
- **Варианты фильтрации**
  - Медленное сканирование (t=1~50 сек)
  - Быстрое сканирование (t=0.01~1 сек)
  - Защита от DoS атаки (более 100 пакетов за 10 мсек)

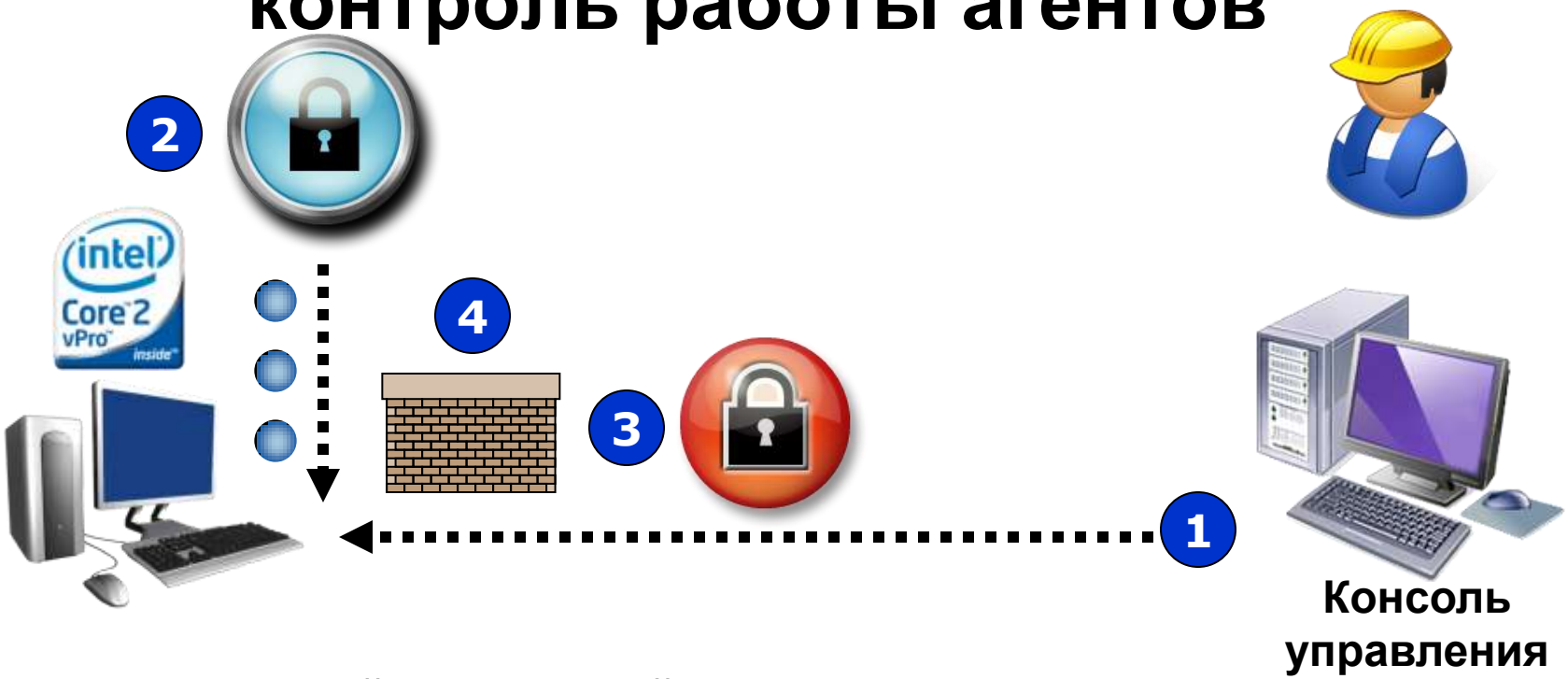
Сценарий 8:
контроль работы агентов

ПК без vPro

Консоль управления

Проблема обычных ПК:
Если системное приложение подверглось атаке и выключено, то администратор может узнать об этом слишком поздно

AMT сценарий 8: контроль работы агентов



ПК с процессорной технологией Intel vPro

1. Администратор задает правила *Agent Presence*
2. Приложение передает системе специальные уведомления
3. При отсутствии уведомлений активируется *System Defense*
4. При восстановлении работы приложения сеть разблокируется

Оперативное устранение угроз

Intel Active Management Technology

ВНЕДРЕНИЕ

Внедрение AMT и безопасность

- **Режим для малого бизнеса – SMB Mode**
  - Авторизация только по паре имя-пароль
- **Режим для предприятий – Enterprise Mode**
  - Защита соединения консоль-ПК
  - Использование ЭЦП
  - Интеграция с AD, применение Kerberos

Аутентификация: подлинность

- **HTTP Digest – для малого бизнеса**
  - Односторонняя аутентификация с хэшированием пароля по алгоритму MD5
- **HTTP Negotiate Authentication – для предприятий**
  - Эффективное применение инфраструктуры Active Directory и протокола Kerberos
    - Сертификаты хранятся в Active Directory
    - Облегчение регулярных изменений и быстрого отзыва
    - Ограничение прав
  - Поддерживает взаимную аутентификацию
    - “Действительно ли это клиент на базе vPro?”
    - “Действительно ли это авторизованный IT-специалист?”

Шифрование: целостность и защищённость

- **Для малого бизнеса: нет шифрования**
- **Для предприятий:**
  - Предпочтительно: TLS w/AES 128-bit
  - Опция: TLS w/RC4 128-bit
  - Опция: нет шифрования

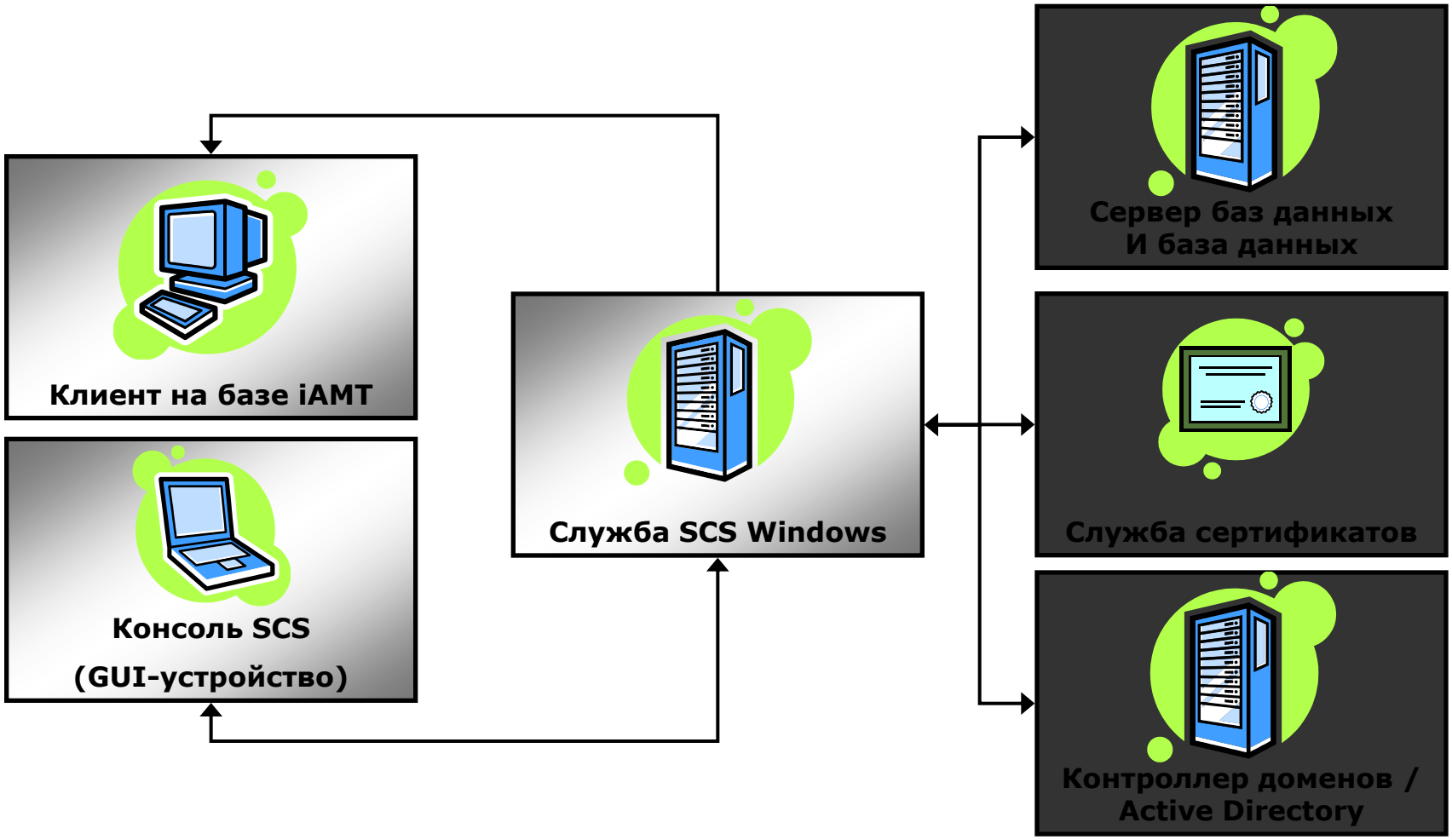
Защита клиента от локального ПО

- **Коммуникационная безопасность ME**
  - Шифрование и аутентификация трафика между ME и ISV
    - Используется та же система обеспечения безопасности, что и для внешнего трафика
    - Внутренний трафик защищен от прослушивания
    - Без электронного ключа Intel команды игнорируются
  - Коммуникационные пакеты имеют серийные номера
    - Невозможно повторить старые разрешенные команды
    - Невозможно подменить пакеты для Agent Presence
- **Память AMT изолируется на аппаратном уровне**
  - Процессор обычно не имеет доступа к флэш-памяти
    - Доступ только во время обновления прошивки
    - Прошивка снабжается цифровой подписью Intel
  - Флэш-память защищена от атак вредоносных программ, пытающихся получить к ней доступ
  - Процессор не имеет доступа к зоне SDRAM

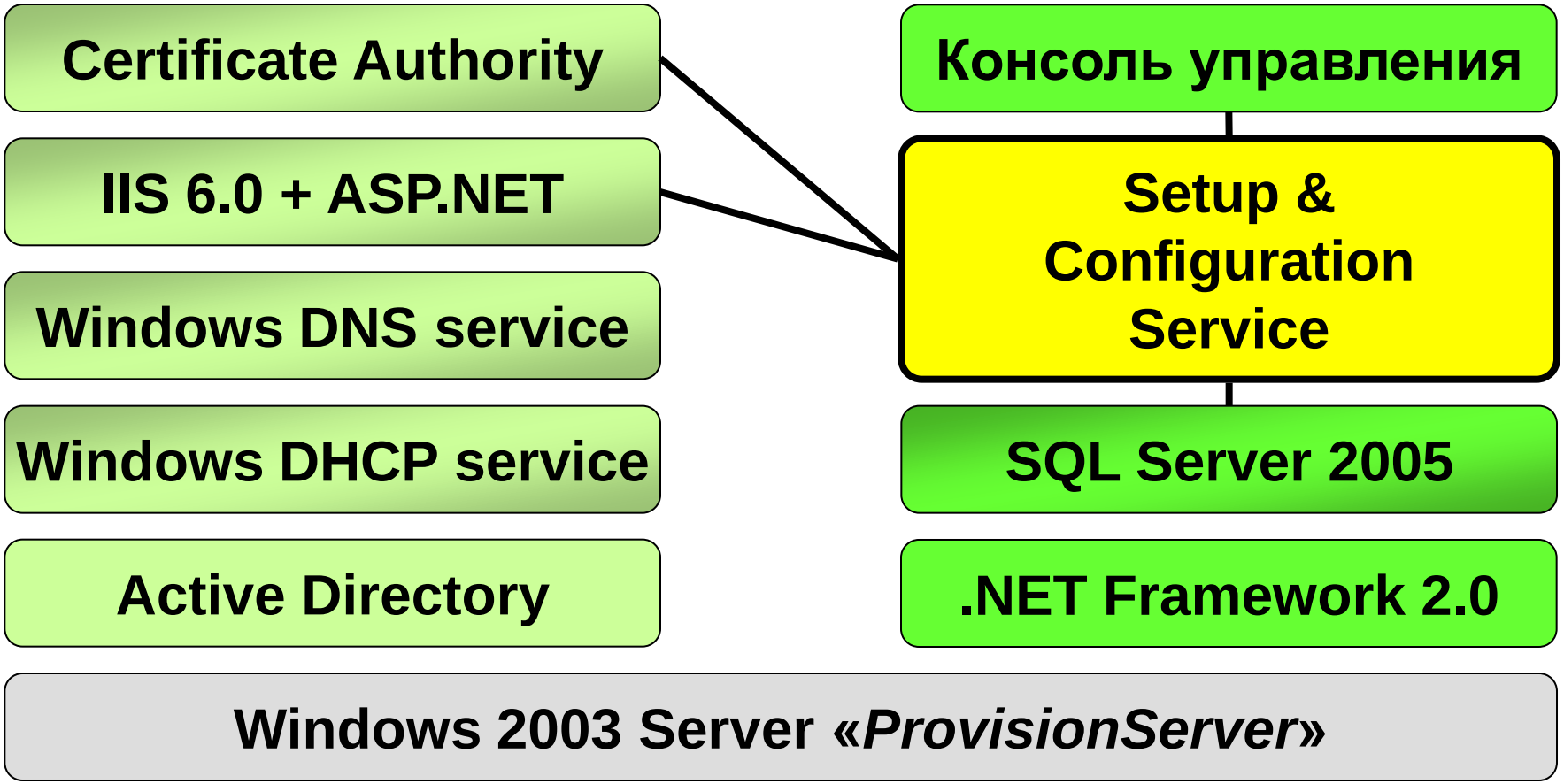
Функции AMT с контролем доступа

Управление безопасностью	**Списки прав доступа, параметры протокола Kerberos, параметры протокола TLS и т.п.**
Администрирование сети	**Опции сети, если не используется DHCP**
Инвентаризация аппаратных средств	**Используется для получения данных об аппаратных средствах**
Удаленное управление	**Удаленное включение / выключение**
Память	**Конфигурирование, запись или считывание из флэш-памяти**
Администрирование памяти	**Распределение и использование флэш-памяти**
Управление событиями	**Конфигурирование событий, генерирующих предупреждения**
Переадресация	**Serial over LAN, IDE Redirection**
Наличие местного агента	**Позволяет программе посылать сообщения ME**
Наличие удаленного агента	**Конфигурирование ответа при исчезновении агента**
Отключение	**Определяет фильтры и политики контроля трафика**
Сетевое время	**Настройка и синхронизация часов AMT**
Общая информация	**Чтение установочной и статусной информации**
Обновление прошивки	**Обновление прошивки AMT**

Инфраструктура для режима Enterprise



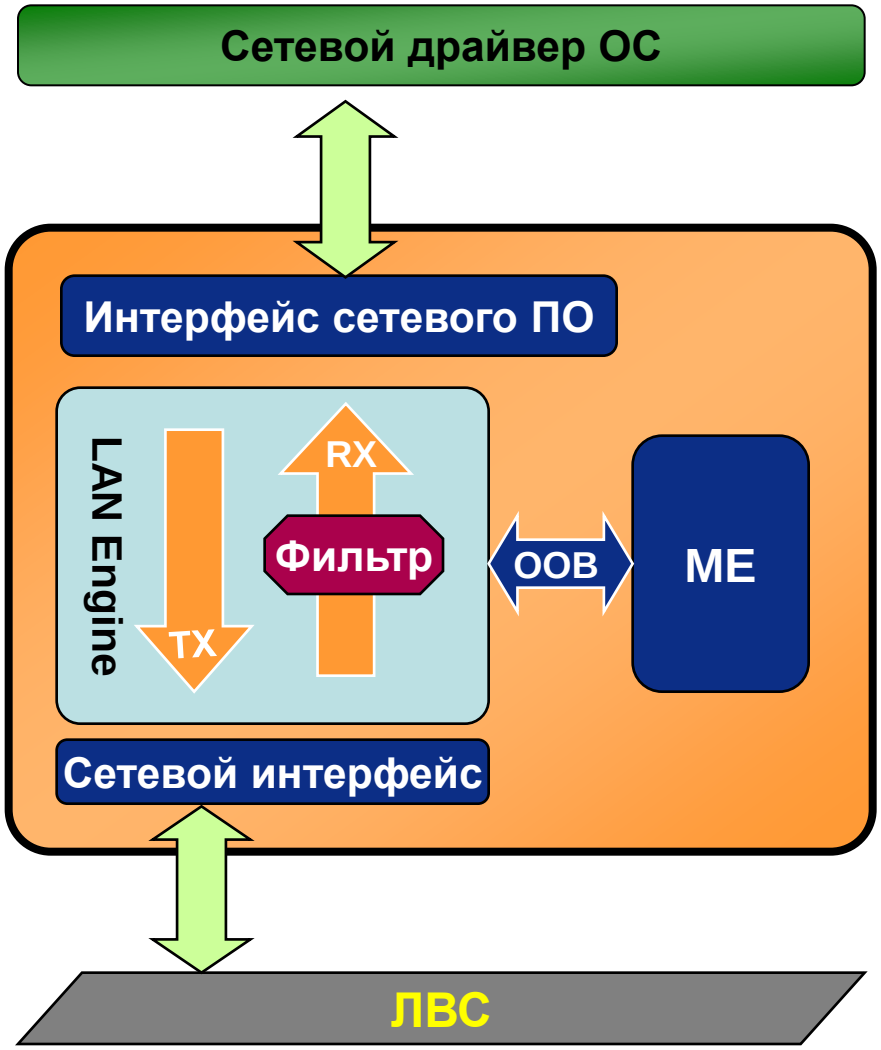
Инфраструктура Enterprise



Основные задачи SCS

- **Подготовка (Pre-Setup)**
  - Подготовка пар PID-PSK для новых ПК
  - Подготовка USB-диска с ключами (One-Touch)
  - Подготовка профилей ПК
    - Настройки сети
    - Права доступа
    - Режимы энергопотребления
- **Процедура Provisioning**
  - Регистрация новых ПК в БД SCS и AD
  - Загрузка профиля на ПК

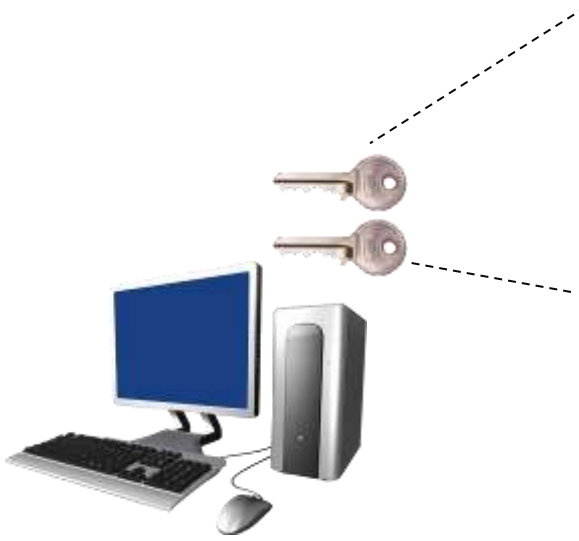
Разделение трафика



- **Используемые порты TCP**
  - 16992-16995 (зарезервированы IANA)
  - 9971 (для SCS)
- **Эффективное использование сетевых адресов и имен**
  - 1 MAC адрес
  - 1 IP-адрес и одно имя ПК в режиме DHCP
    ИЛИ
  - 2 статических IP-адреса и два имени

Установка – шаг 1

- **Создайте уникальный ключ одноразового использования для каждого клиента**



PID	**0000-004G**
PPS	**GXGE-P2CH-N2SV-QRAC-CGCP-DB46-MQ3T-0UPX**
Пароль по умолчанию	**admin**
Новый пароль	**5%ji2qx**

Консоль управления

Клиенты на базе Intel® vPro™

Установка – шаг 2

- Передайте ключи клиентам

Консоль управления

Клиенты на базе Intel® vPro™

Установка – шаг 3

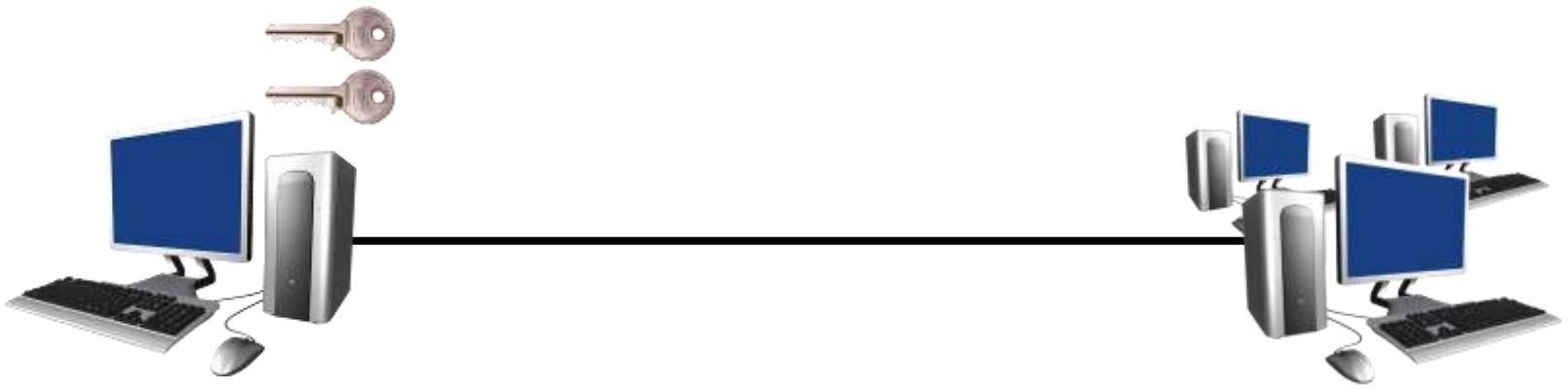
- **Клиент на базе Intel® AMT посылает запрос на конфигурирование**

Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование – шаг 1

Сервер конфигурирования отвечает на запрос клиента. Для установления достоверного соединения используются временные ключи



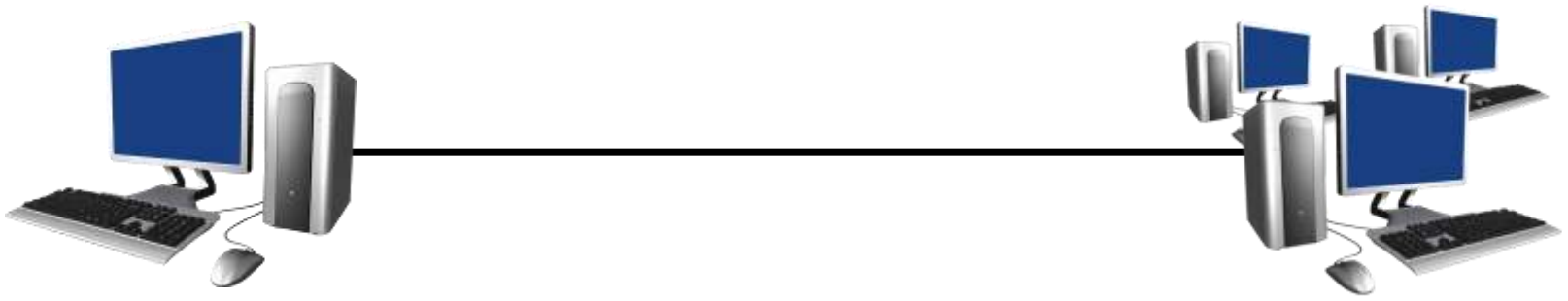
Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование – шаг 2

Сервер конфигурирования регистрируется на клиенте на базе Intel® AMT. Используется заводской пароль администратора сети HTTP-Digest, предлагаемый по умолчанию

Имя
Пароль

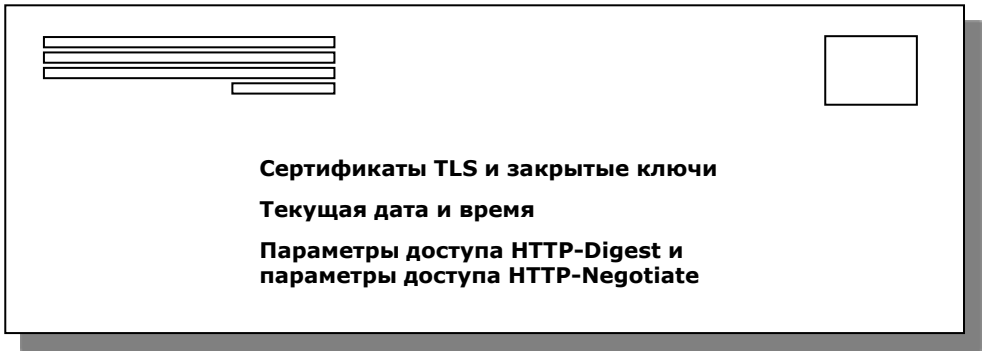


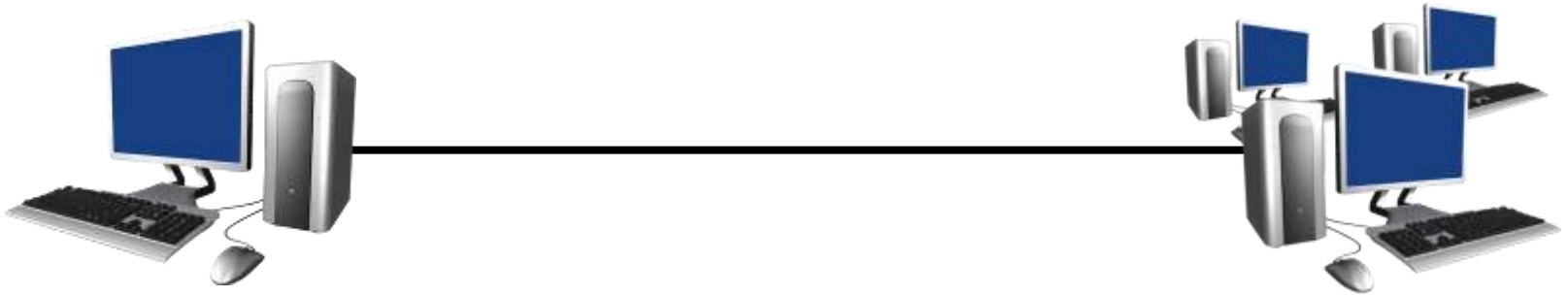
Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование – шаг 3

Конфигурирует все необходимые параметры



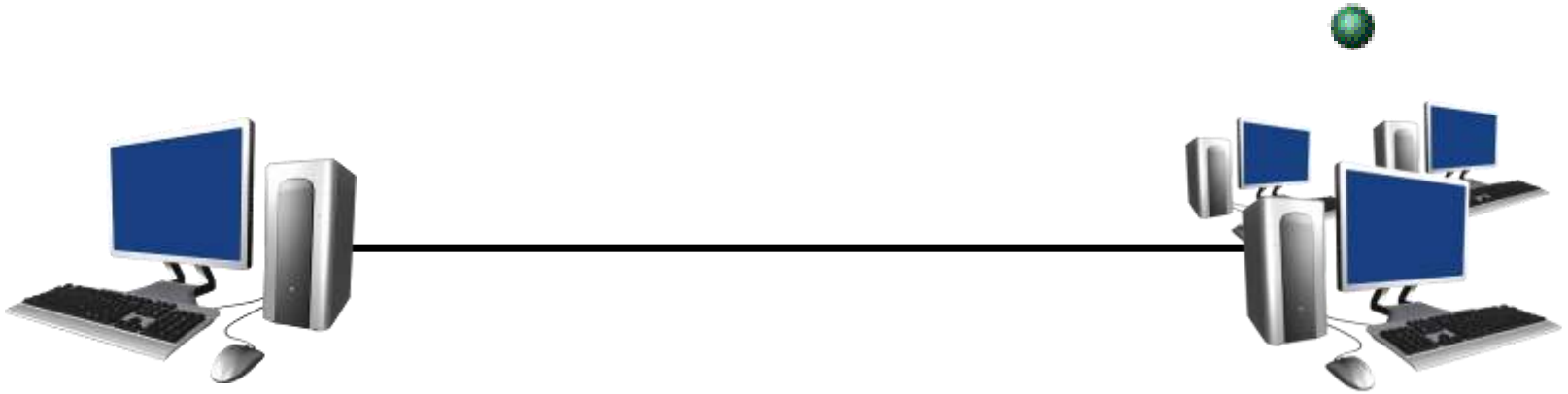


Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование – шаг 4

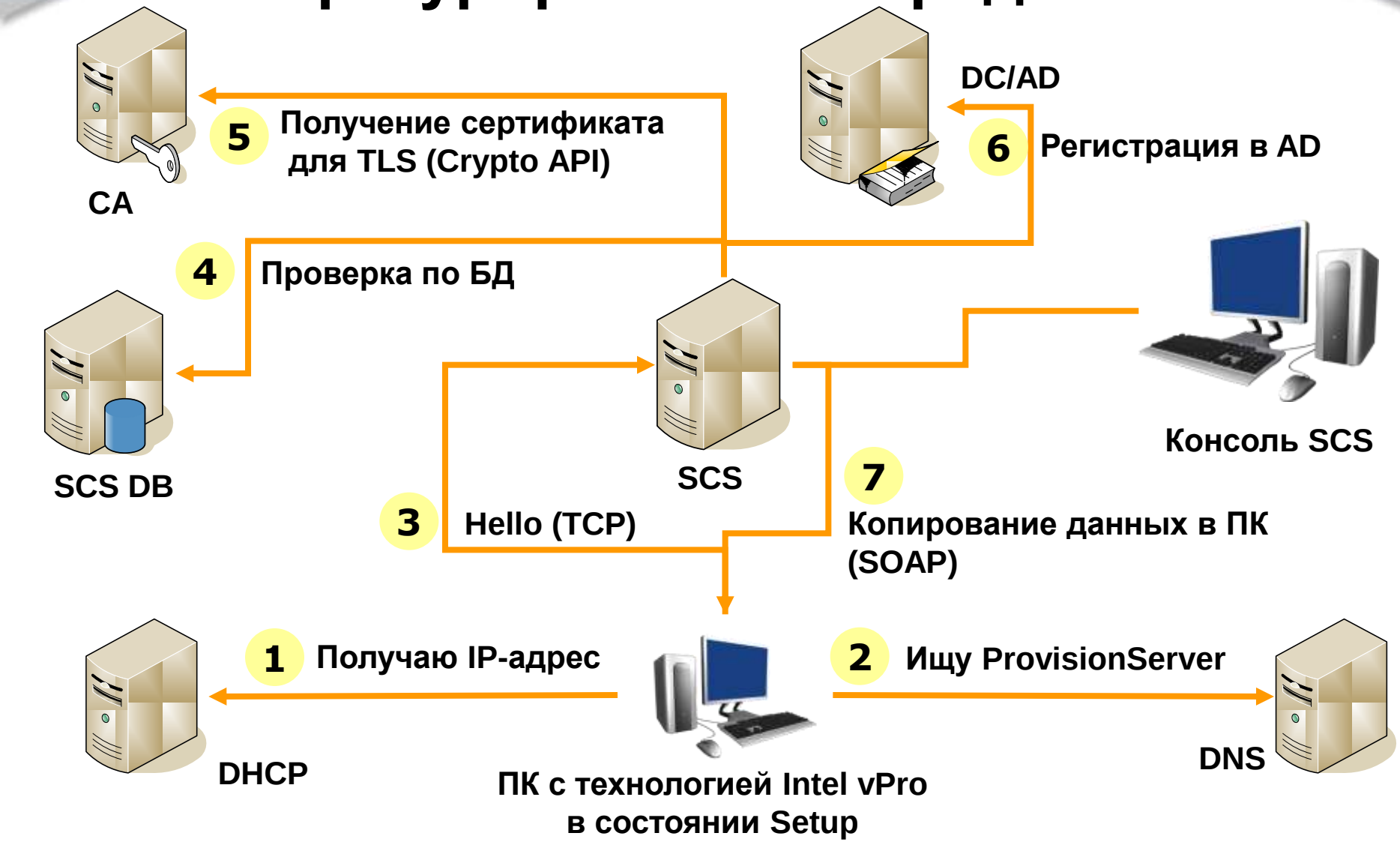
Клиент на базе Intel® AMT перезагружается и начинает нормальную работу



Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование в среде DHCP



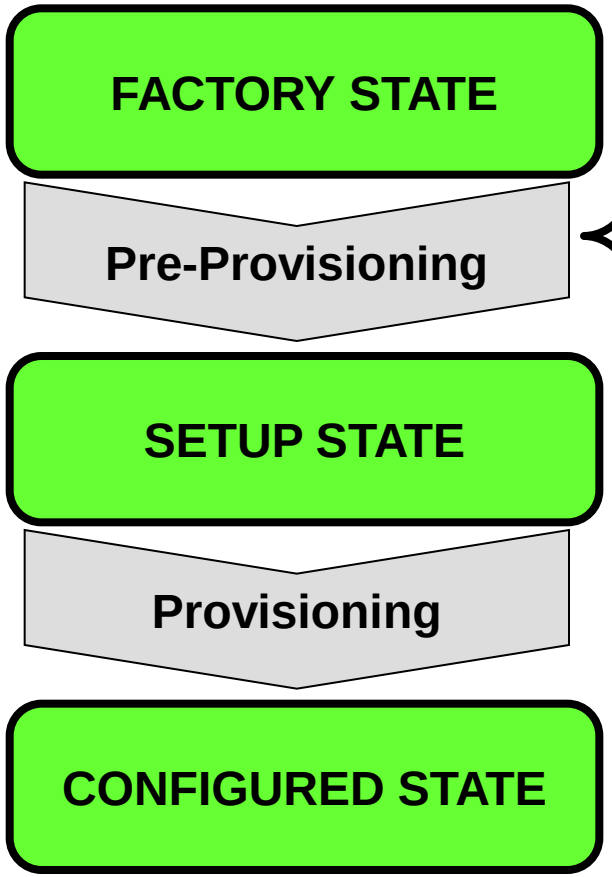
Переход в состояние Pre-Provisioning

One-Touch Configuration

Pre-Provisioning «в одно касание» с использованием загрузочного USB диска

Выполняется IT-службой предприятия или поставщиком

Provisioning производится автоматически после перезагрузки



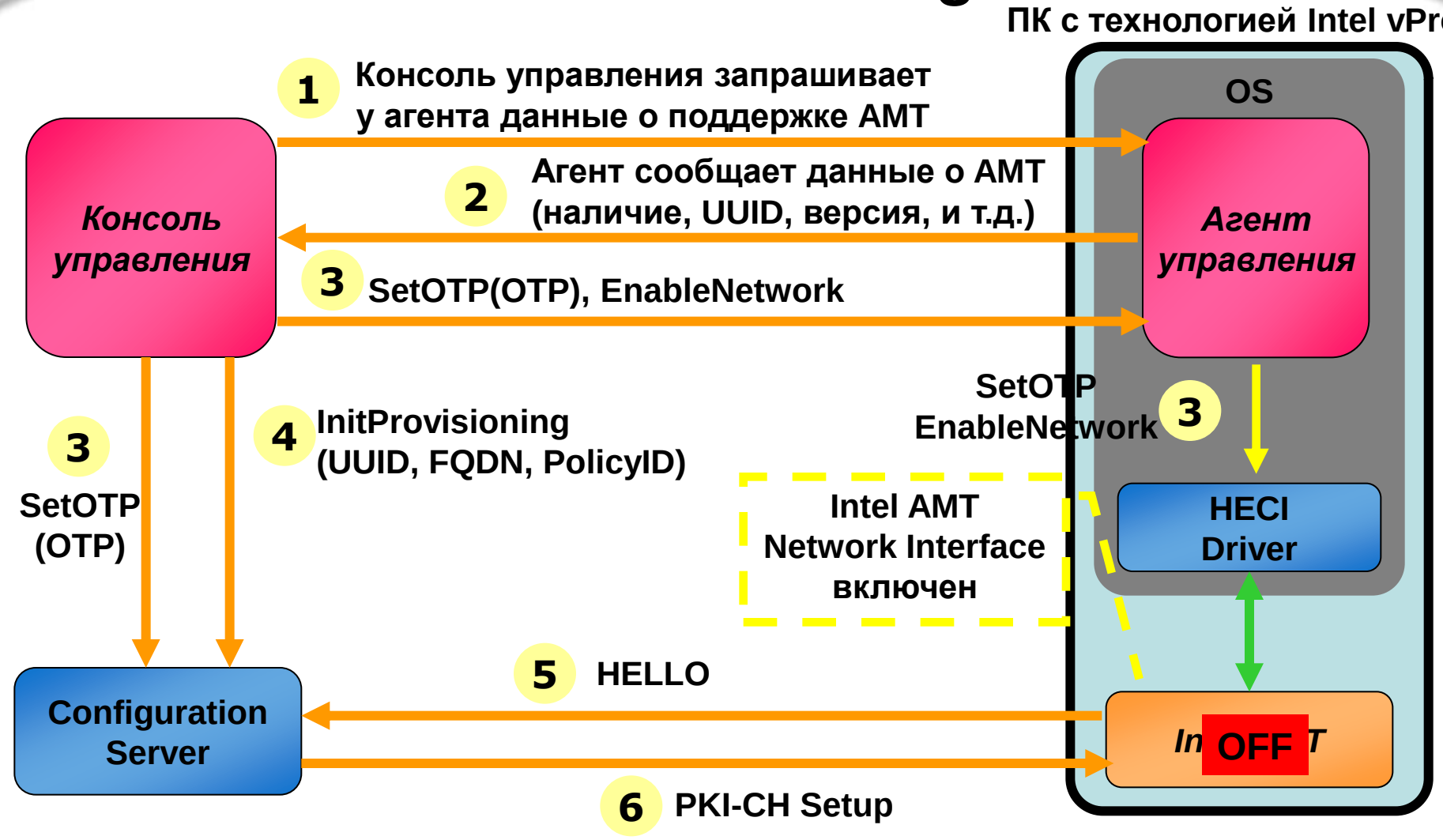
Настройка вручную

На каждом ПК в BIOS вносятся предварительные настройки (IP,TLS-PSK)

Подготовка ПК осуществляется IT-службой

Provisioning производится автоматически после перезагрузки

Режим Remote Configuration



Разработано Intel ПО сторонних производителей

Тонкости Remote Configuration

- **AMT**
  - Содержит hash-коды корневых сертификатов «доверенных» CA
    - Список сертификатов можно редактировать
  - Генерирует временный self-signed сертификат для TLS
- **Configuration Server**
  - Имеет специальный сертификат для конфигурирования AMT
  - Сертификат выдан «доверенным» CA
  - Разрешено использование self-signed сертификатов