Составные элементы процессорной технологии Intel® vPro™

Двухъядерный процессор Intel® Core™2 Duo

Intel® 82566DM Gigabit Network Connection

Intel® Q965 Express Chipset

Прошивка Intel

Архитектура на базе технологии Intel® vPro™

ME в чипсете

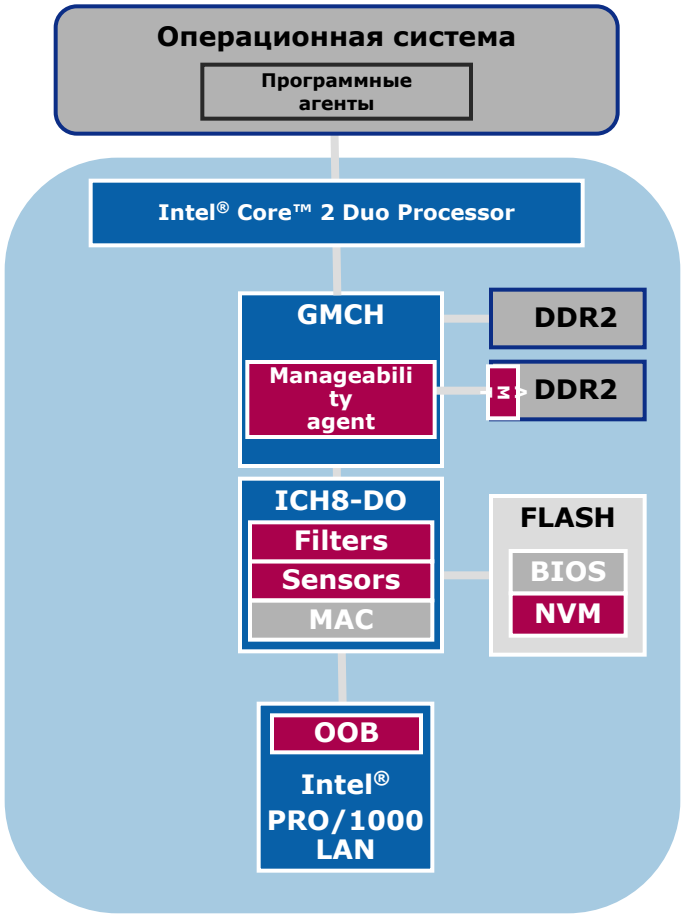
- Независимость от питания и состояния ОС
- Использует 16Мб нулевого канала системной памяти

Сетевые фильтры в чипсете

- Контроль Ethernet-трафика
- Возможность внутреннего отключения сети Ethernet

Выделенная флэш-память

- Хранение прошивки агента управления (ME)
- Хранение данных инвентаризации ресурсов
- Хранение данных о независимых поставщиках программного обеспечения



Флэш-память Intel® vPro™

Скрытые данные ME
- Ключи безопасности
- Данные инвентаризации аппаратных средств

Данные третьих сторон
- ~380 кБ для независимых поставщиков ПО
- Партнеры: до 84 кБ
  - 4kB приращение
- Ограничение для не являющихся партнерами 8 кБ

- Независимые поставщики решают как использовать свое пространство

Данные о ресурсах при форматировании или отключении жесткого диска больше не теряются!

Технология vPro iAMT - Применение

Intel® Active Management Technology
Применение

- Удаленная инвентаризация ресурсов
- Инвентаризация аппаратных и программных средств
- Удаленная диагностика и ремонт
- Проверка наличия агента
- Шифрованное, удаленное включение и обновление
- Изоляция и восстановление на аппаратном уровне

Intel® Active Management Technology

Удаленная инвентаризация ресурсов

Подсчет количества ПК в сети, даже если компьютеры выключены или ОС не работает

- Компании не досчитываются в среднем до 20% своих аппаратных ресурсов[1]
- Результаты неточной инвентаризации ресурсов:
  - Приобретение лишнего количества ПК для замены "отсутствующих"
  - Юридическая ответственность за предоставление неточных отчетных данных
  - Нарушение безопасности: компания не может обеспечить безопасность компьютера, местоположение которого не получается обнаружить
- Удаленная инвентаризация помогает сократить количество визитов на рабочие места и снизить расходы
  - Снижение затрат на кадровые ресурсы
  - Ускорение инвентаризации
  - Более точное прогнозирование
- Способствует выполнению требований государственных постановлений

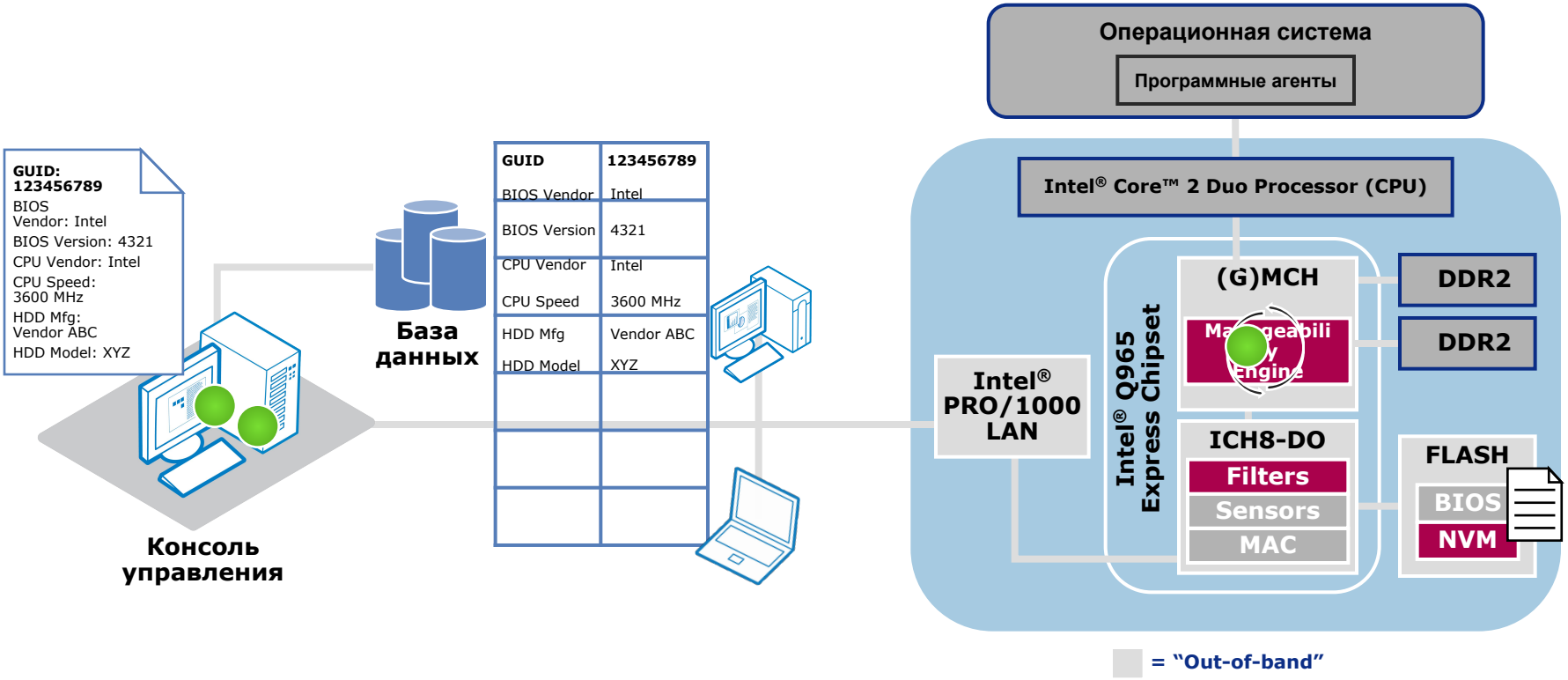
[1] Source: Intel white paper, Reducing Costs with Intel Active Management Technology.

Intel® Active Management Technology

Инвентаризация аппаратных и программных средств

Требования

- Поставщик ПО, поддерживающий Intel® AMT; клиент на основе технологии Intel® vPro; клиент, подключенный к сети питания и проводной локальной сети



Intel® Active Management Technology

Инвентаризация аппаратных и программных средств

Более точная инвентаризация аппаратных и программных средств

- Отказ от дорогостоящих и трудоемких способов инвентаризации аппаратных и программных средств вручную
- Проведение более точной инвентаризации аппаратных и программных средств, даже если компьютеры выключены или ОС не работает
- Снижение расходов на лицензирование ПО и сокращение рисков при точной инвентаризации ПО
- Удовлетворение требований государственных постановлений
  - Более точная инвентаризация обеспечивает предоставление реальной информации по основным фондам компании

Инвентаризация аппаратных средств

Инвентаризация аппаратных средств при каждой загрузке BIOS

- Доступные данные:

Системная плата
- **Производитель**
- **Продукт**
- **Версия**
- **Серийный №**
- **Метка**

Процессор
- **Производитель**
- **Type**
- **Семейство**
- **Скорость**

ОЗУ
- **Производитель**
- **Скорость**
- **Объем**
- **Серийный №**
- **Метка**

HDD
- **Модель**
- **Серийный №**
- **Объем**

- USB-устройства и прочая периферия не регистрируются
- Поставщик BIOS определяет объем данных, записываемых во флэш-память
- Консоль управления определяет, какие данные используются

Инвентаризация программных средств

Инвентаризацию программных средств осуществляют программные агенты независимых поставщиков

Независимые поставщики определяют график записи и данные, необходимые для записи

Intel® Active Management Technology

Удаленная диагностика и ремонт

Удаленная загрузка, диагностика, ремонт и восстановление ПК, сокращение визитов на рабочие места

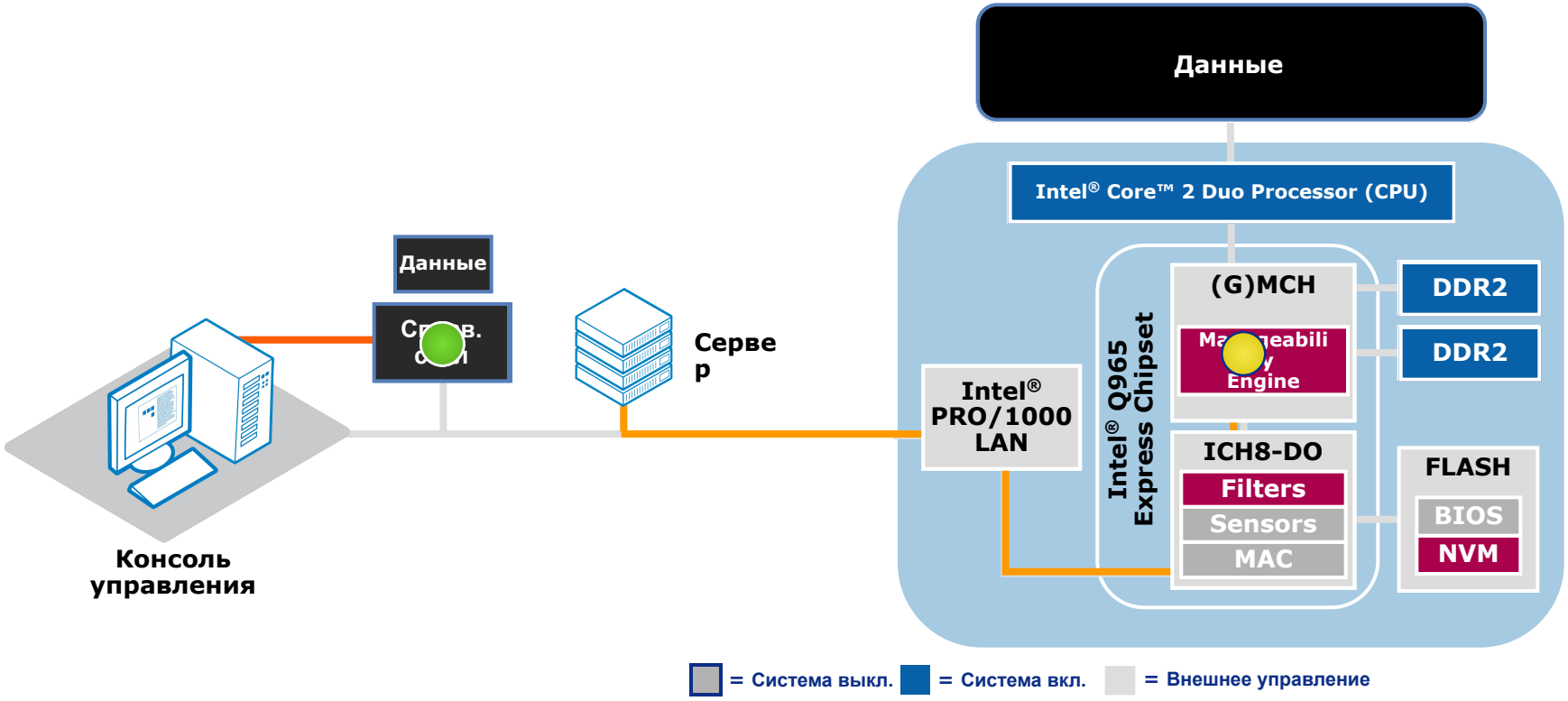
- Удаленная загрузка, поиск неисправности, ремонт и восстановление ПК независимо от его состояния и состояния ОС
- Удаленная загрузка неработающей системы с помощью образа на сервисном диске, чтобы получить возможность использования программ диагностики и удаленного управления
- Удаленный ремонт помогает сократить количество визитов на рабочие места и соответственно снизить расходы
- Удаленный ремонт обеспечивает быстрое восстановление работоспособности компьютера пользователя
- Информация о конфигурации системы всегда находится в доступе, даже если ОС не работает, таким образом техник получает корректную информацию уже при первом заходе

Intel® Active Management Technology

Удаленная диагностика и ремонт

Требования

- ПО с поддержкой Intel® AMT; клиент на базе технологии Intel® vPro с включенной опцией SOL/IDE-R в BIOS; клиент, подключенный к источнику питания и проводной локальной сети; образ в текстовом формате/средства диагностики.



Intel® Active Management Technology
Шифрованное, удаленное включение и обновление

Установка обновлений, даже если компьютер выключен

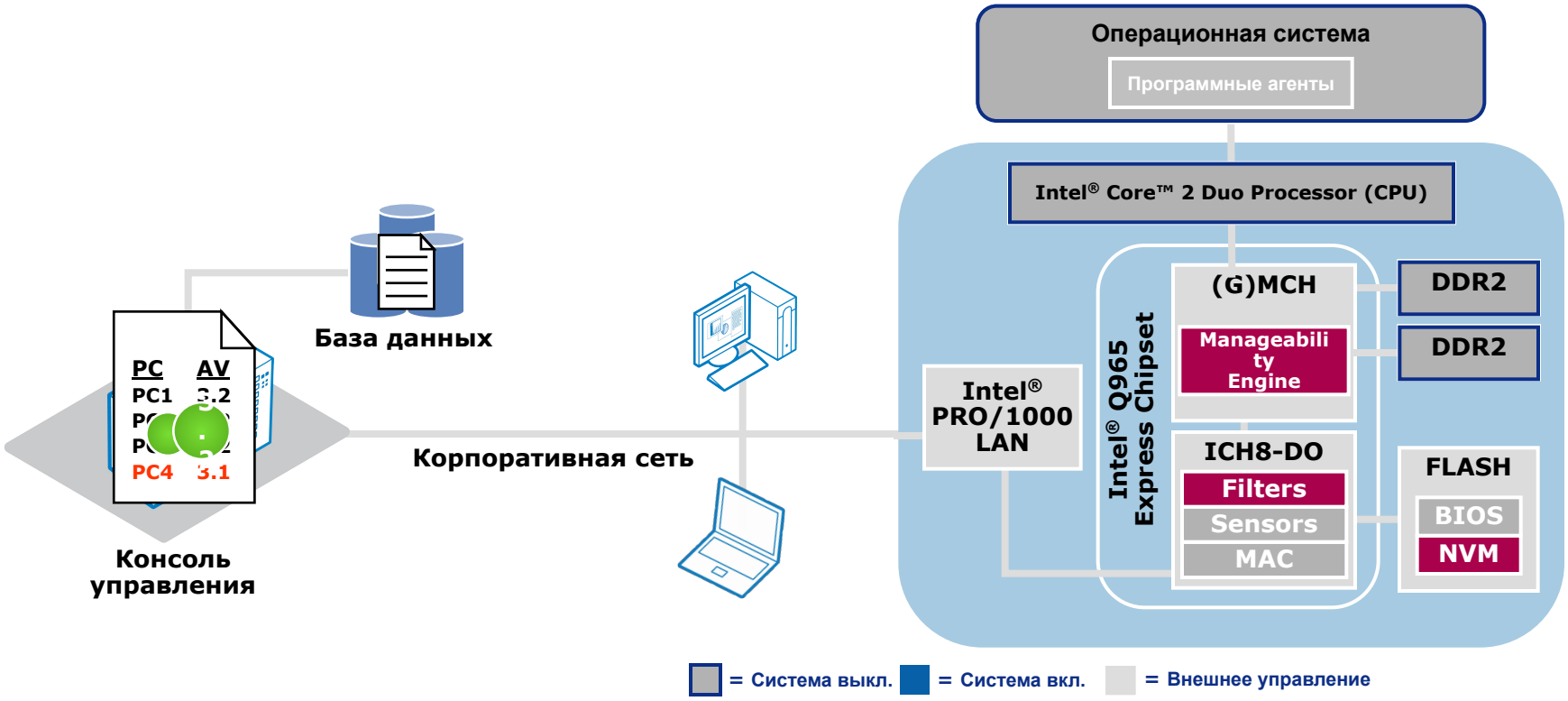
- Более безопасное включение/выключение системы в нерабочее время
- Оперативное обеспечение соответствия требованиям безопасности
- Снижение уязвимости
  - Установка обновлений системы безопасности без вмешательства пользователя
- Автоматизация процесса обновления ПО и антивирусной защиты
  - Экономия денег и ресурсов

Intel® Active Management Technology

Шифрованное, удаленное включение и обновление

Требования

- ПО с поддержкой Intel® AMT; средства установки "заплатки"; клиент на базе технологии Intel® vPro; клиент, подключенный к источнику питания и проводной локальной сети.



Проверка агента

Контроль корректной работы агента

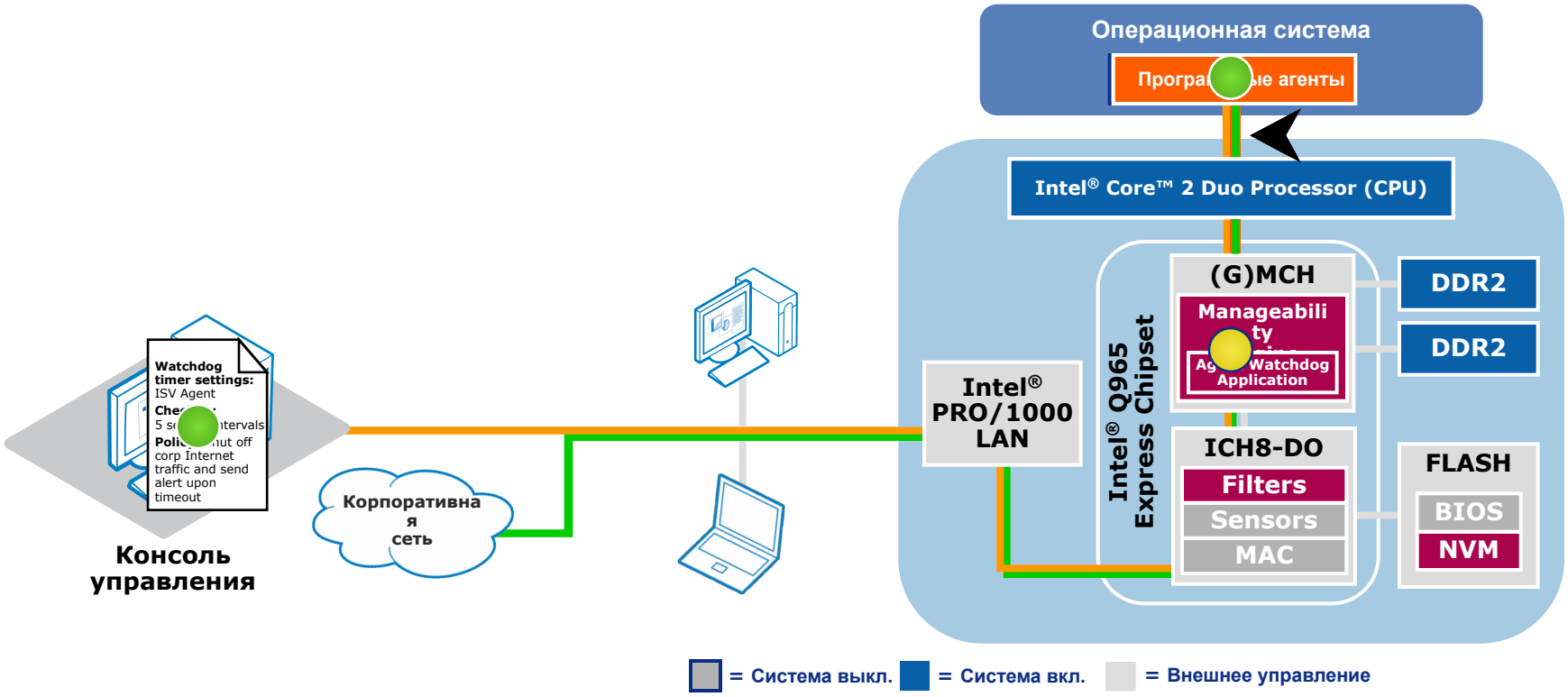
- Простое автоматическое слежение за работой агентов ОС
- Предотвращение вмешательства в работу или отключения уязвимых агентов
- Обеспечение более точной инвентаризации ресурсов ПК при работе всех агентов управления
- Контроль конфигурации на консоли с помощью системных данных, хранящихся на аппаратном уровне, доступ к которым имеется даже при выключенной системе

Intel® Active Management Technology

Проверка агента

Требования

- ПО с поддержкой Intel® AMT; клиент на базе технологии Intel® vPro; клиент, подключенный к источнику питания и проводной локальной сети.



Intel® Active Management Technology
Изоляция и восстановление на аппаратном уровне

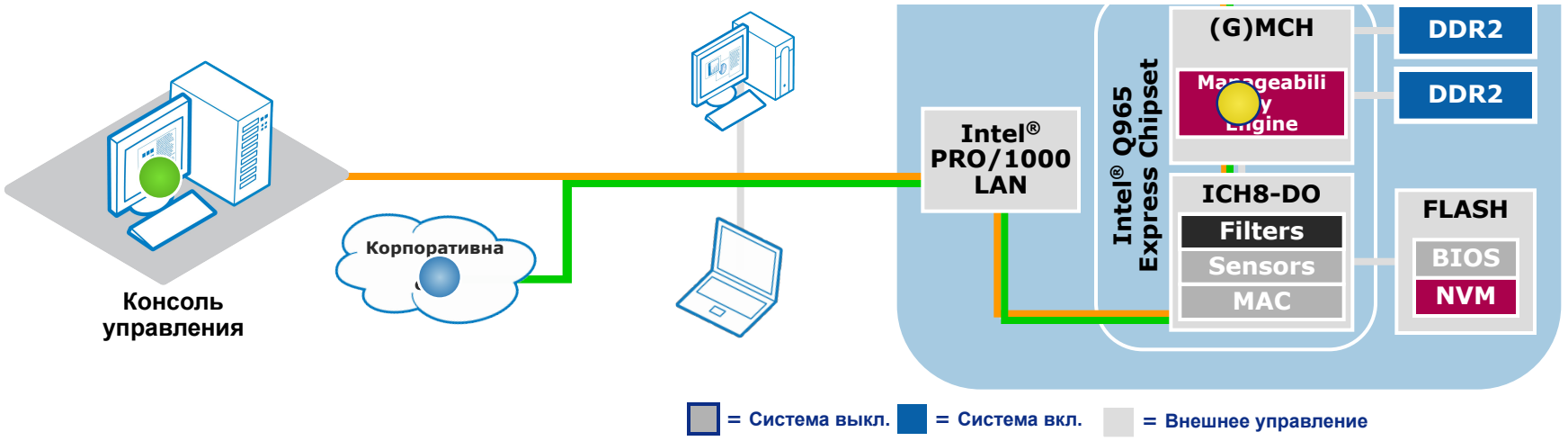
Фильтрация вирусов и изоляция зараженных ПК

- 64 встроенных программируемых аппаратных фильтра
- Проверка входящих и исходящих пакетов на вирусы
- Использование готовых программных продуктов независимых поставщиков для установки политик отдельных фильтров
- Настройка фильтров в соответствии с потребностями компании
- Изоляция одного или нескольких зараженных компьютеров в сети с поддержкой защищенного канала восстановления
- Быстрый возврат компьютера в сеть с использованием более безопасных каналов

Intel® Active Management Technology
Изоляция и восстановление на аппаратном уровне

Требования

- ПО с поддержкой Intel® AMT и System Defense; клиент на базе технологии Intel® vPro; клиент, подключенный к источнику питания и проводной локальной сети.



Фильтры системы безопасности

Фильтры входящего и исходящего трафика

- 31 на TX (+ 1 контрольный фильтр)
- 31 на RX (+ 1 контрольный фильтр)
- 16 счетчиков статистики

Фильтры устанавливаются на:

- Тип протокола L2
- Исходящий IP-адрес
- IP-адрес назначения
- Тип следующего IP-заголовка
- Флаги TCP
- Исходящий порт UDP/TCP
- Порт назначения UDP/TCP

Поддержка протокола IPv6

- Поддержку IPv6 можно обеспечить путем объединения 4-х фильтров для работы одним цельным блоком

Безопасность и технология Intel® vPro™

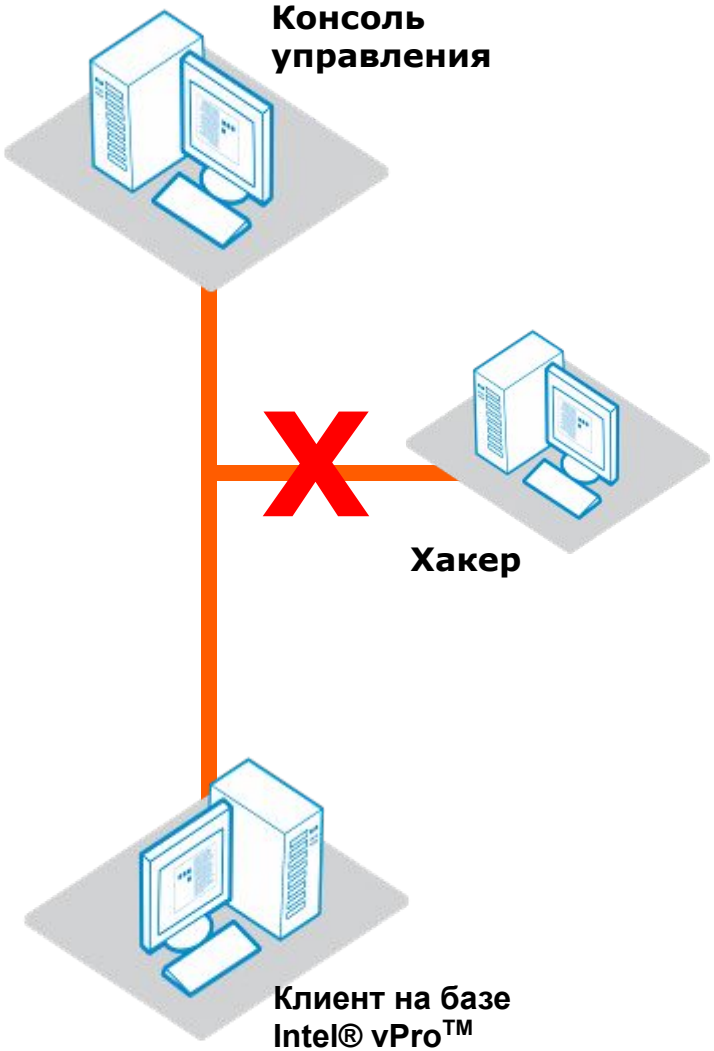
Технология Intel® vPro™ обеспечивает защиту клиента с внешней стороны

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
      - Инженеры не могут управлять ПК финансового отдела
  - Поддерживает взаимную аутентификацию
    - "Действительно ли это клиент на базе vPro?"
    - "Действительно ли это авторизованный IT представитель?"

Шифрование: целостность и защищенность

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



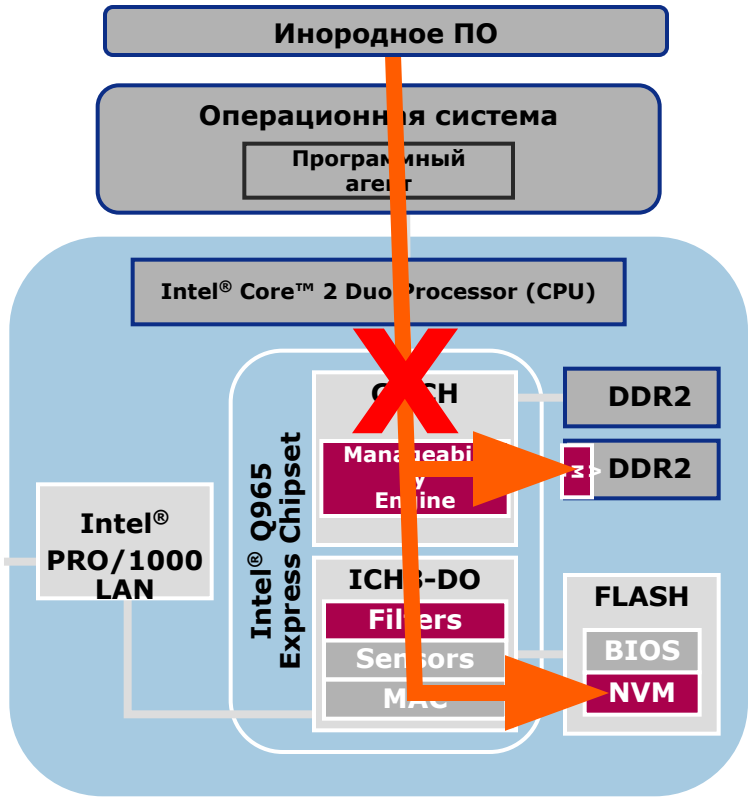
Технология Intel® vPro™ обеспечивает защиту клиента с внешней стороны

Коммуникационная безопасность ME

- Шифрование и аутентификация трафика между ME и ISV
  - Используется та же структура безопасности, что и для внешнего трафика
  - Предотвращение просматривания защищенного трафика
  - Без ключа Intel команды игнорируются
- Коммуникационные пакеты имеют серийные номера
  - Невозможность повторения старых, разрешенных команд
  - Невозможность послания старого контрольного сообщения

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
- Предотвращение износа флэш-памяти атаками вредоносных программ путем использования памяти от поставщиков, не являющихся партнерами
- Процессор не имеет доступа к зоне SDRAM



Функции Intel® 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

Список прав доступа дает/отзывает разрешение

Коммуникационная безопасность

Сетевые интерфейсы ME

Гигабитная проводная сеть по протоколу 802.3 и беспроводная сеть про протоколу 802.11 a/ b/ g

Обеспечение сетевой безопасности протоколом TLS

- Шифрованные XML сообщения, инкапсулированные в SOAP через HTTP
- Взаимная аутентификация TLS с использованием следующих наборов кодов
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_NULL_SHA (export/import)
  - Сертификаты RSA и ключи, сгенерированные в оффлайне и сконфигурированные (2048-битный модуль)

Безопасность порта проводной сети обеспечивается протоколом 802.1x (SR)

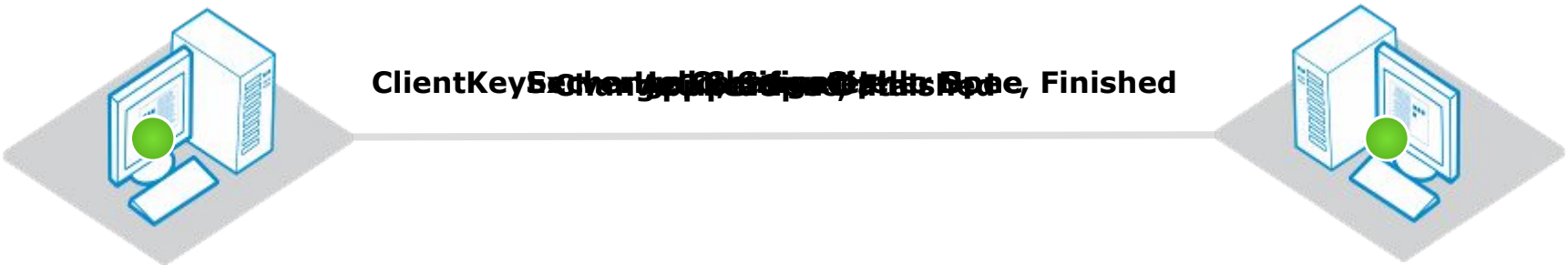
- PEAP MSCHAPv2 и EAP TLS
- EAP FAST и EAP TTLS (EAC)

Безопасность порта и соединения беспроводной сети обеспечивается WLAN Si (SR)

Intel® Active Management Technology
Intel® AMT: TLS & HTTP-Digest

Шаг 1

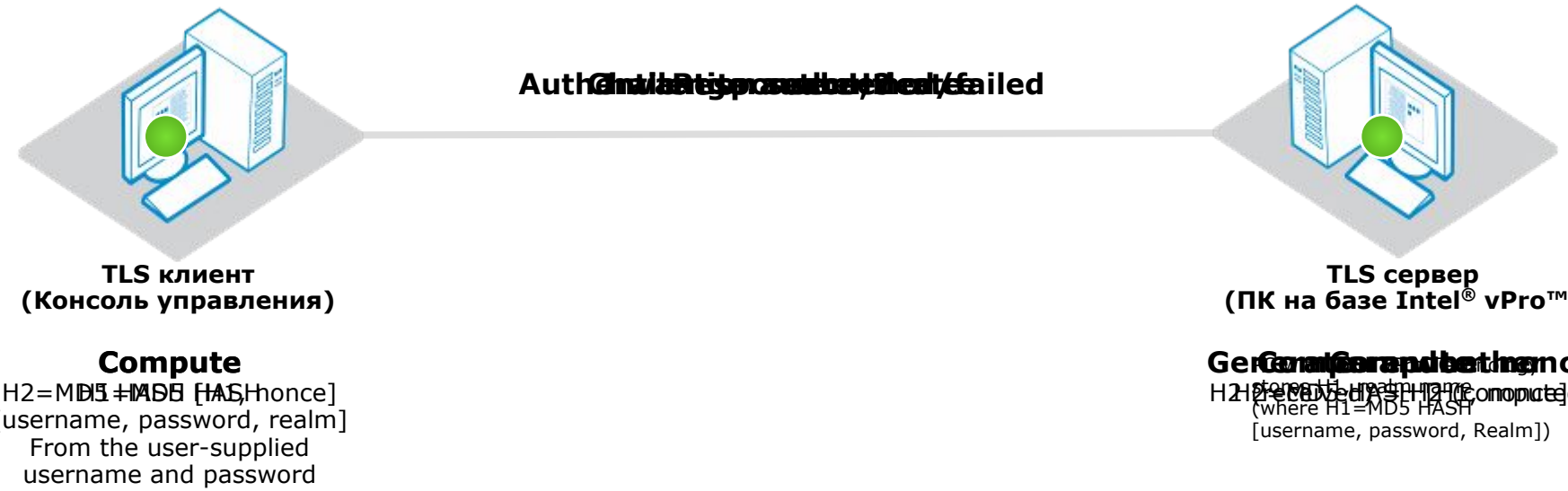
- Создание безопасного туннеля с TLS



Intel® Active Management Technology
Установка Intel® AMT: TLS & HTTP-digest

Шаг 2

- Защита данных в туннеле с помощью HTTP-Digest



802.1x – Информация

- **Основные характеристики протокола 802.1x:**
  - Схема аутентификации на уровне портов (туннелирование второго уровня)
  - Заменяет протокол PPP (Peer-to-Peer), что очень полезно при использовании сети не на TCP/IP, обеспечивает простоту и сокращение непроизводительных издержек
  - Разработка стандарта для передачи пакетов EAP по проводной/беспроводной сети
- **Протокол расширенной аутентификации EAP**
  - Реальный протокол с поддержкой процесса аутентификации (802.1x payload)
  - Гибкость: возможность выбора метода аутентификации, включая фирменные методы (от базового имени/пароля до PKI)
  - Три основных компонента (Port Access Entities)
    - Суппликант – клиент, требующий аутентификации
    - Сервер аутентификации – осуществляет фактический процесс аутентификации (например, RADIUS)
    - Аутентификатор – устройство между ними (например, Точка доступа беспроводной сети)
- **Протокол EAP изначально разрабатывался для проводных сетей, но он идеально подходит и для беспроводных сетей, поскольку точка доступа является непрограммируемым устройством (вся логика перемещена на сервер аутентификации)**
- **Строгий приемлемый стандарт.**

Поддержка протокола 802.1X

Протокол 802.1X не поддерживается в Intel® AMT Release 2.0, но будет поддерживаться в Intel AMT 2.5 и последующих версиях

Платформа Santa Rosa для поддержки беспроводных сетей требует как минимум протокола 802.1X

Протокол также требуется в качестве компоновочного модуля для поддержки контроллеров сетевого доступа (проводные и беспроводные сети).

Технология Intel AMT будет поддерживать следующие протоколы EAP:

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- PEAP

CCX: Cisco Client Extensions – поддерживает свой набор в ME

Для беспроводных сетей мы также будем поддерживать генерацию WPA ключа, предварительную аутентификацию

Настройка в «одно касание»
(*Инициализация*)

Установка и конфигурирование

Двухэтапный процесс – Установка и конфигурирование

- **Первый этап: Установка – современный подход к быстроте**
  - Создайте персональный идентификатор клиента
  - Ключ шифрования одноразового использования (для установления достоверного соединения)
  - PID (Provisioning ID) и PPS (Provisioning Passphrase)

- **Второй этап: Конфигурирование**
  - Установите достоверное соединение между клиентом и консолью управления
  - Создайте и обменяйтесь сертификатами и ключами шифрования

Поддерживаемые типы:

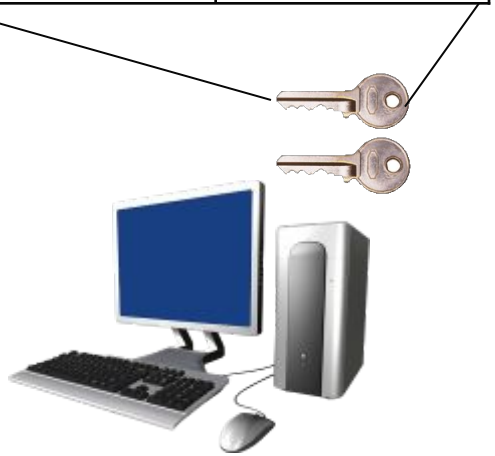
- Вариант для малого бизнеса
  - Простое имя и пароль
  - Нет шифрования
  - Предназначен для сетей, где отсутствует инфраструктура безопасности
- Вариант для предприятий
  - Требует инфраструктуры цифровой безопасности
  - Поддерживает шифрование и взаимную аутентификацию
  - Метод, рекомендованный Intel

Установка - 3 простых действия

Быстрая установка и конфигурирование

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 - 3 простых действия

Быстрая установка и конфигурирование

2. **Передайте ключи клиентам**

Консоль управления

Клиенты на базе Intel® vPro™

Установка - 3 простых действия

Быстрая установка и конфигурирование

3. **Клиент на базе Intel® AMT посылает запрос на конфигурирование**

Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование - 4 простых действия

Быстрая установка и конфигурирование

1. **Сервер конфигурирования отвечает на запрос клиента.**

   (для установления достоверного соединения используются временные ключи)

Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование - 4 простых действия

Быстрая установка и конфигурирование

2. Сервер конфигурирования регистрируется на клиенте на базе Intel® AMT client

(Используется заводской пароль администратора сети HTTP-Digest, предлагаемый по умолчанию)

Имя
Пароль

Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование - 4 простых действия

Быстрая установка и конфигурирование

3. Конфигурирует все необходимые параметры

Сертификаты TLS и закрытые ключи

Текущая дата и время

Параметры доступа HTTP-Digest и параметры доступа HTTP-Negotiate

Консоль управления

Клиенты на базе Intel® vPro™

Конфигурирование - 4 простых действия
Быстрая установка и конфигурирование

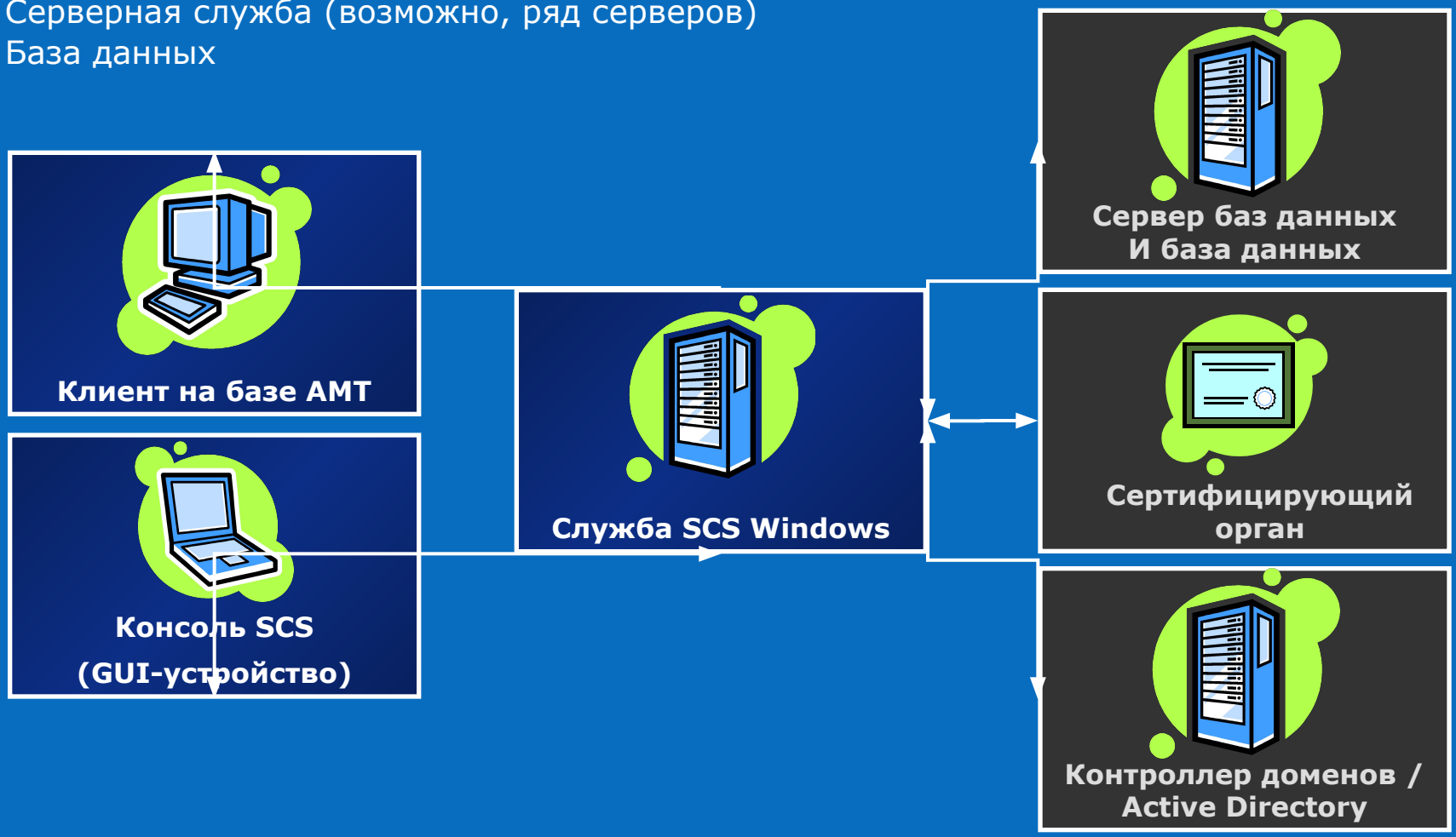
4. **Клиент на базе Intel® AMT перезагружается и начинает нормальную работу**

Консоль управления

Клиенты на базе Intel® vPro™

Инфраструктура для режима для предприятия

Консоль (GUI-устройство)
Серверная служба (возможно, ряд серверов)
База данных



Расконфигурирование
(*с вмешательством или без вмешательства пользователя*)

Расконфигурирование

Частичное расконфигурирование (waterfall internal)

- Возврат всех заводских установок по умолчанию, за исключением:
  - Хэш-коды доверенных корневых сертификатов
  - Хэш-код доверенного корневого сертификата, выбранного для использования в конфигурировании
  - Режим “Слушай” или “Говори” mode
  - Полное доменное имя сервера установки и конфигурирования
  - Значение фразы-пароля
- Это позволяет заказчику переконфигурировать имеющуюся платформу для другого сотрудника без необходимости повторного ввода информации

Полное расконфигурирование (waterfall external)

- Возврат всех заводских установок по умолчанию