ЭЛВИС-ПЛЮС

# Корневая проблема информационной безопасности в Облаке

Вернер Олег Витальевич,
к.т.н., начальник лаборатории доверенной среды

ЭЛВИС-ПЛЮС

# Основные проблемы ИБ в Облаке

## Нормативно-правовые

- Нет нормативов и требований по защите и типовой модели угроз
- Нет концептуальных подходов к безопасности
- Нет правовой основы отношений провайдер/пользователь
- Не урегулированы отношения при трансграничности облачной среды

## Технологические

- Сужение возможности использования традиционных средств защиты
- Непрозрачность процедуры управления инфраструктурой для пользователя
- Проблема конфиденциальности и целостности удаленного доступа
- Обязательное наличие виртуализатора и проблема его целостности
- Проблема динамичности ВМ и наличия бездействующих клонов
- **Проблема ДОВЕРИЯ**

ЭЛВИС-ПЛЮС

# Руководящие документы ФСТЭК

## Приказы

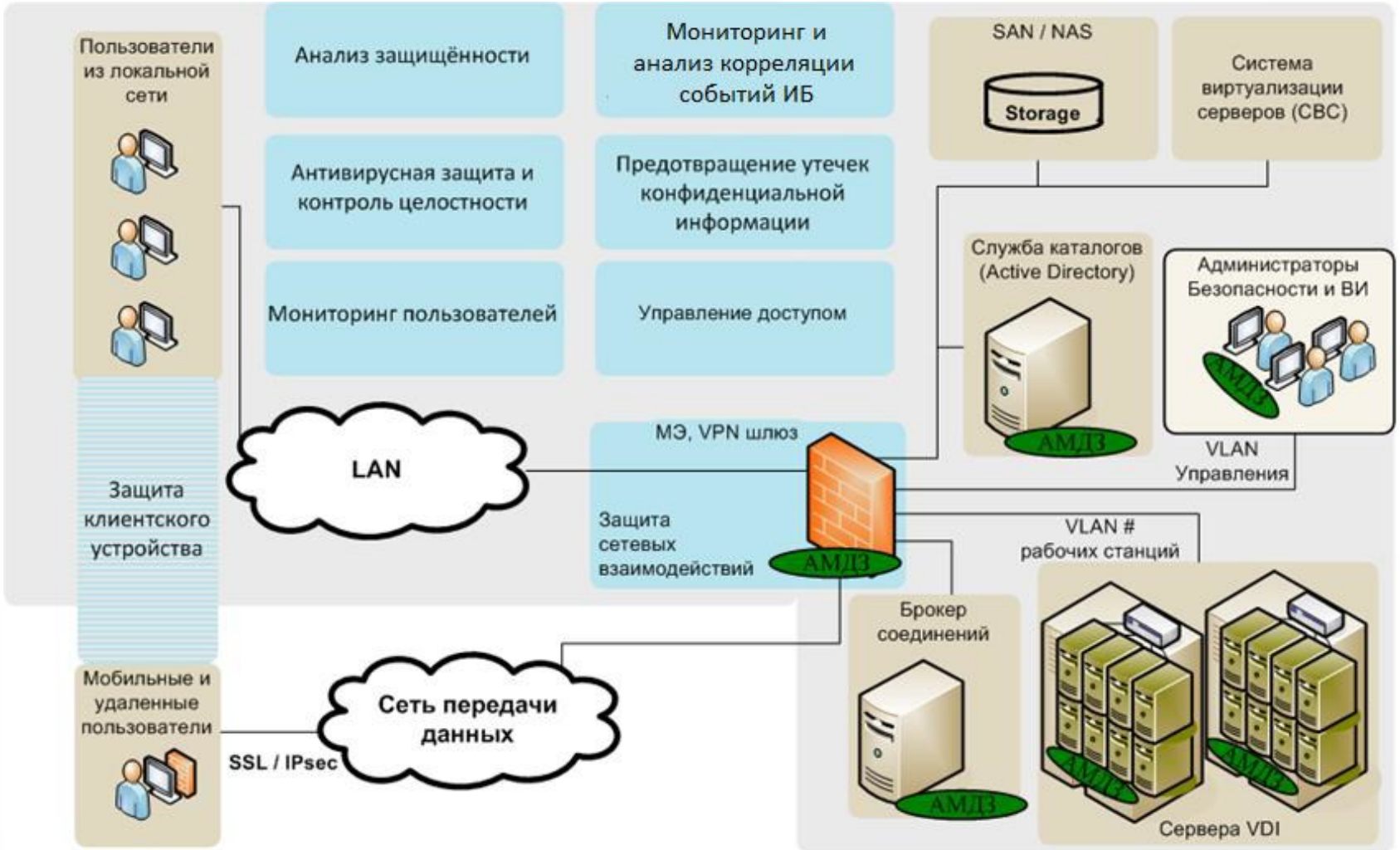
- Приказ №17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. 11 февраля 2013

- Приказ №21 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
  18 февраля 2013

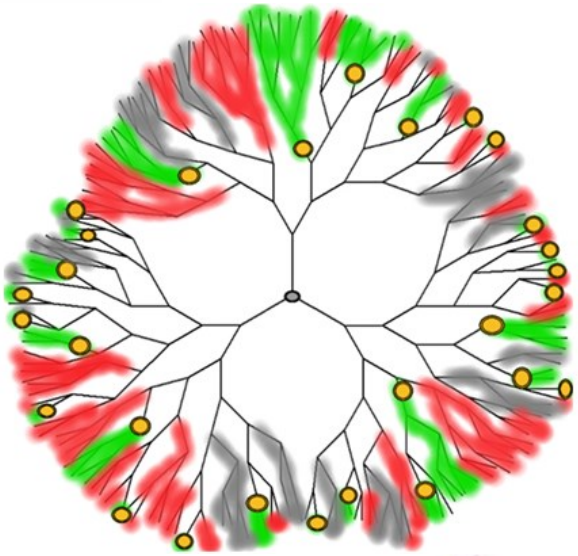
## НИР

- Подготовка методического документа «Меры защиты информации в государственных информационных системах» (раздел ЗАЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ - ЗСВ).

# Традиционный подход к СЗИ Облака



# От традиционного подхода к Доверенной среде

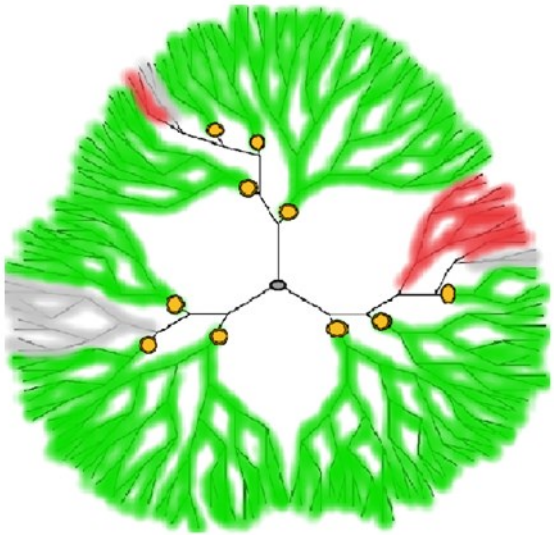


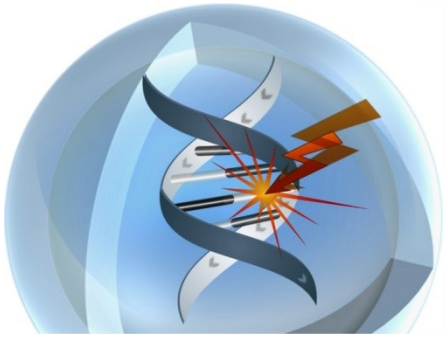
Контрмера

Защищенная

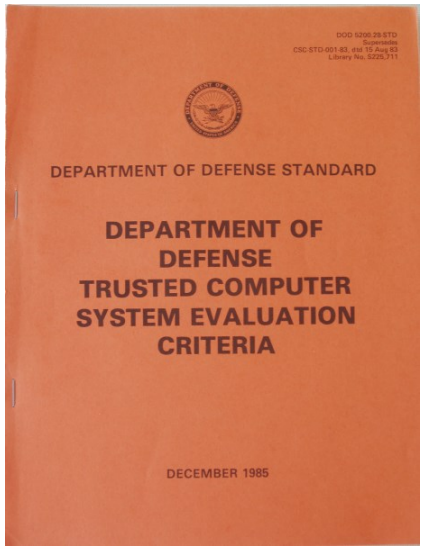
Незащищенная

Непроверенная,
Неизвестная





# ДОВЕРЕННАЯ СИСТЕМА




- система, использующая аппаратные и программные средства для обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа.

Корневой проблемой обеспечения информационной безопасности в Облаке является проблема

**ДОВЕРИЯ**

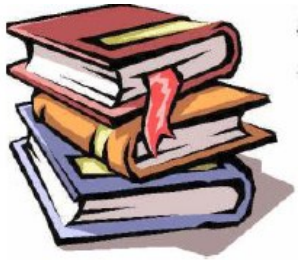
# Обеспечение информационной безопасности в Облаке

Просто верить поставщику услуг

Юристы

или

Контролировать доверие



Стандарты

Технология


Сертификация

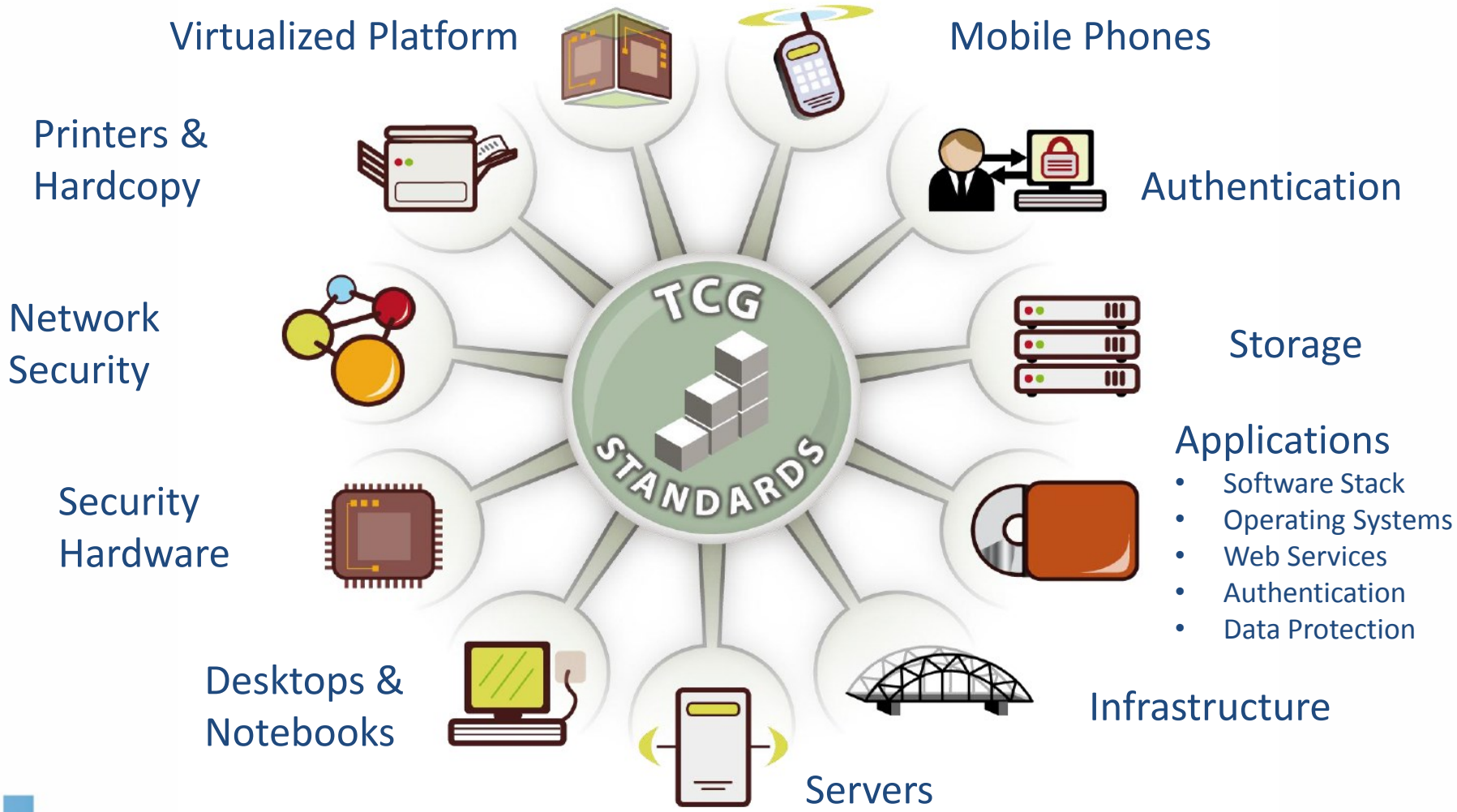
ЭЛВИС-ПЛЮС

# Доверенная Среда

- **Среда, обеспечивающая возможность непосредственно верифицировать доверенную вычислительную платформу или доверенную вычислительную базу (Trusted Computing Base – TCB) в Облаке**

TRUSTED COMPUTING GROUP™

# TCG: стандарты для доверенной среды



# Доверенные системы: функции безопасности

## Клиенты

встроенные в
- TPM
- MTM

Аутентификация
Шифрование
Аттестация

## Сервера


встроенные в
- TPM
- Secure Virtualization
- Secure Cloud

Аутентификация
Шифрование
Аттестация

## Хранилища

встроенные в
- Self Encrypted Drive (SED)

Шифрование
Аутентификация

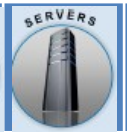
## Сети

согласованные и встроенные в
- Trusted Network Connect (TNC)

Аутентификация
Проверка готовности
Монитор поведения
Исполнение политики

ЭЛВИС-ПЛЮС

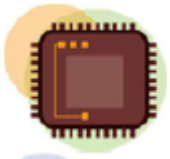
# Cloud Security Alliance:
## Руководство по обеспечению безопасности облачных вычислений

| CSA Domain Type |  |  |  |  | Примеры |
|---|---|---|---|---|---|
| Управление / Управление рисками | + | + | + | + | Снижение риска |
| Сбор судебной и электронной информации | + | | | | Восстановление данных и шифрование |
| Соответствие требованиям и Аудит | | + | | | Аттестация сервера (Server Attestation) |
| Управление жизненным циклом информации | + | | | | Безопасное уничтожение данных |
| Портируемость и Интероперабельность | | | + | | Политика предоставления доступа к метаданным |
| Традиционная безопасность | | | + | | Контроль доступа в сеть (NAC) |
| Реагирование на инциденты | | | + | + | Согласованная политика безопасности |
| Шифрование / Управление ключами | + | | | | Самошифрующиеся накопители (SED), аппаратные хранилища ключевой информации |
| Идентификация / Управление доступом | | | | + | Аутентификация на базе аппаратного токена |
| Виртуализация | | + | | | Доверенная Мультиарендность (Trusted Multitenancy) |

# Стандарты TCG: Доверенное Облако

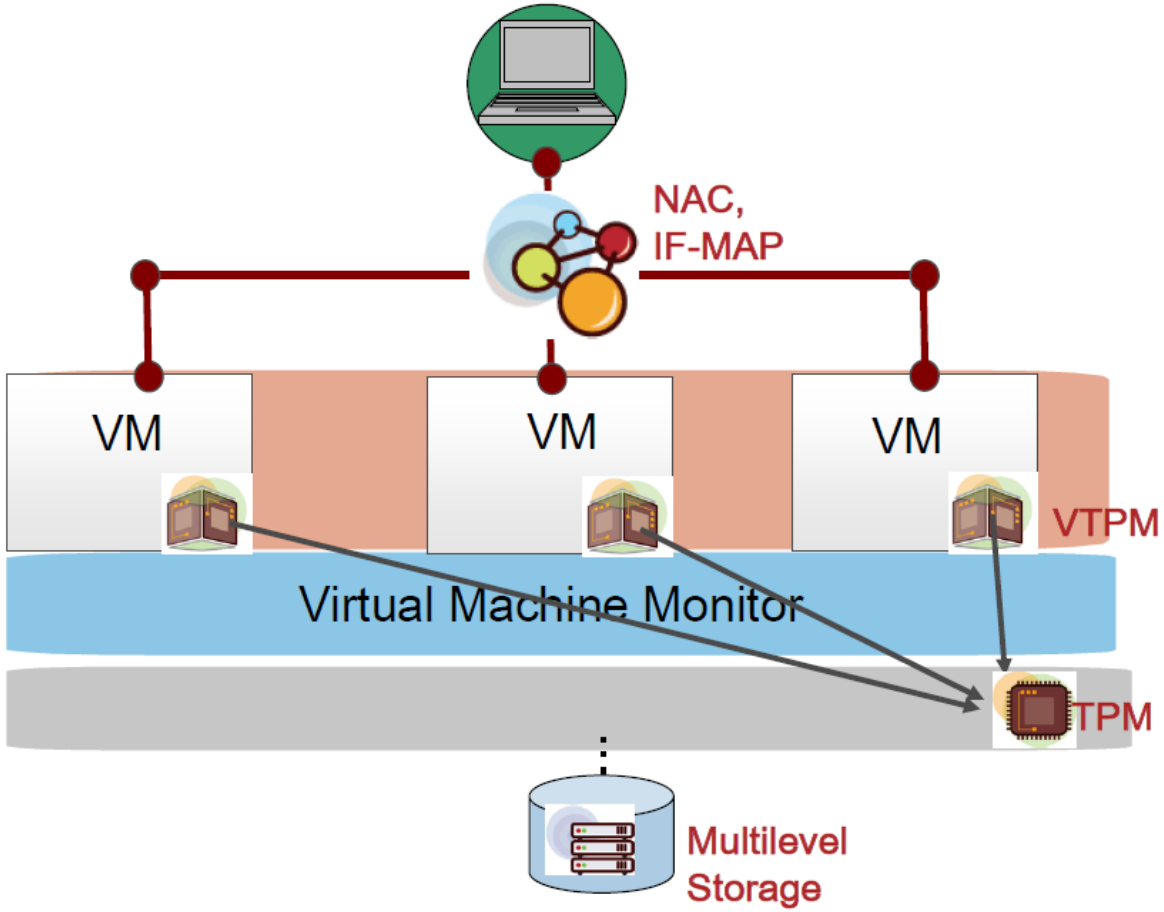
Virtualization workgroup
(virtual certificates,
virtual TPM, migration)

TPM workgroup
(Server Attestation)



Storage workgroup
(multilevel storage)

Trusted Network Connect
(Policy definitions and
enforcement)



# Доверенный клиент: предварительные вопросы

Может ли **Владелец Устройства**:

- Быть уверен, что его данные не будут доступны со стороны Компании?
- Запускать ПО и приложения по своему выбору?
- Уволится из Компании без потери своих данных?

Работник – Владелец Устройства

Сервисы Компании

Может ли **Владелец Информации**:

- Доверять устройству удаленный доступ к сервисам Компании?
- Доверять обрабатываемым на устройстве данным (конфиденциальность и целостность)?
- Доверять устройству обработку данных?
- Закрыть доступ к своей информации в любой момент?

# Сценарии BYOD: разделение данных

**Личные Данные**
данные Владельца Устройства – $IO_1$

**Данные Компании**


**Владелец Устройства**

**Аппаратный Корень Доверия**
База для защиты на устройстве
- Корпоративных данных от неавторизованного доступа
- Личных данных от неавторизованного доступа владельцев информации

**IO = Владелец Информации**

# Аппаратный Корень Доверия: современные стандарты и технологии

TRUSTED COMPUTING GROUP™

## TPM 2.0


Infineon

INTEGRITY GUARD

intel

intel
Haswell

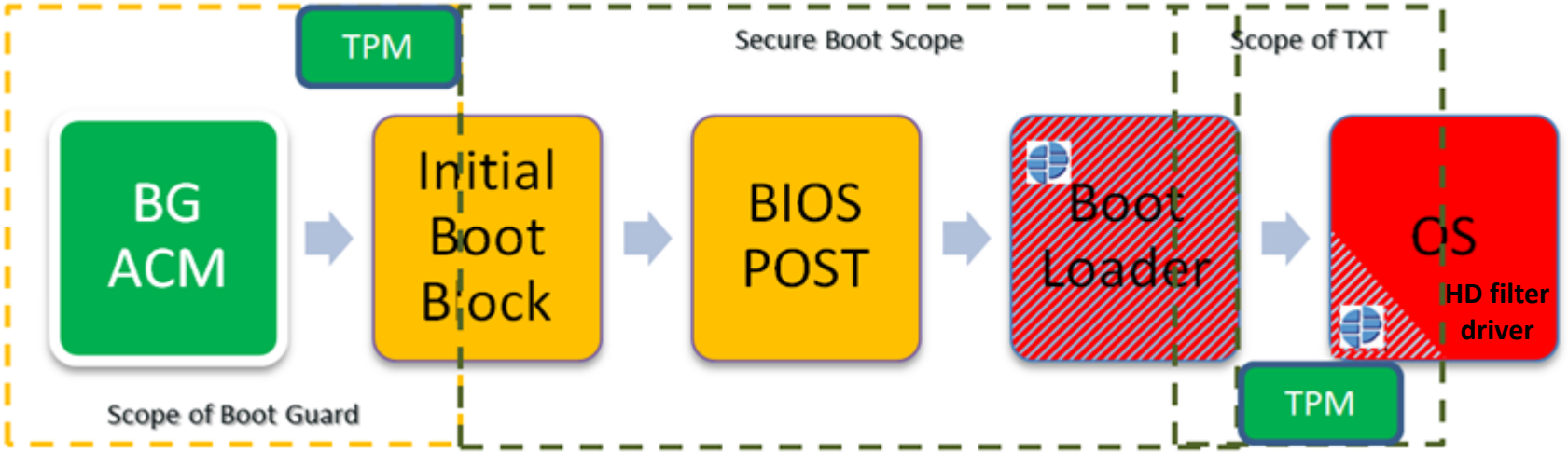
## BOOT GUARD

INTEGRITY GUARD


# Stefan Rüping, Marcus Janke и Andreas Wenzel – номинанты Немецкой премии будущего за 2012 год

# Логическая архитектура мобильного устройства

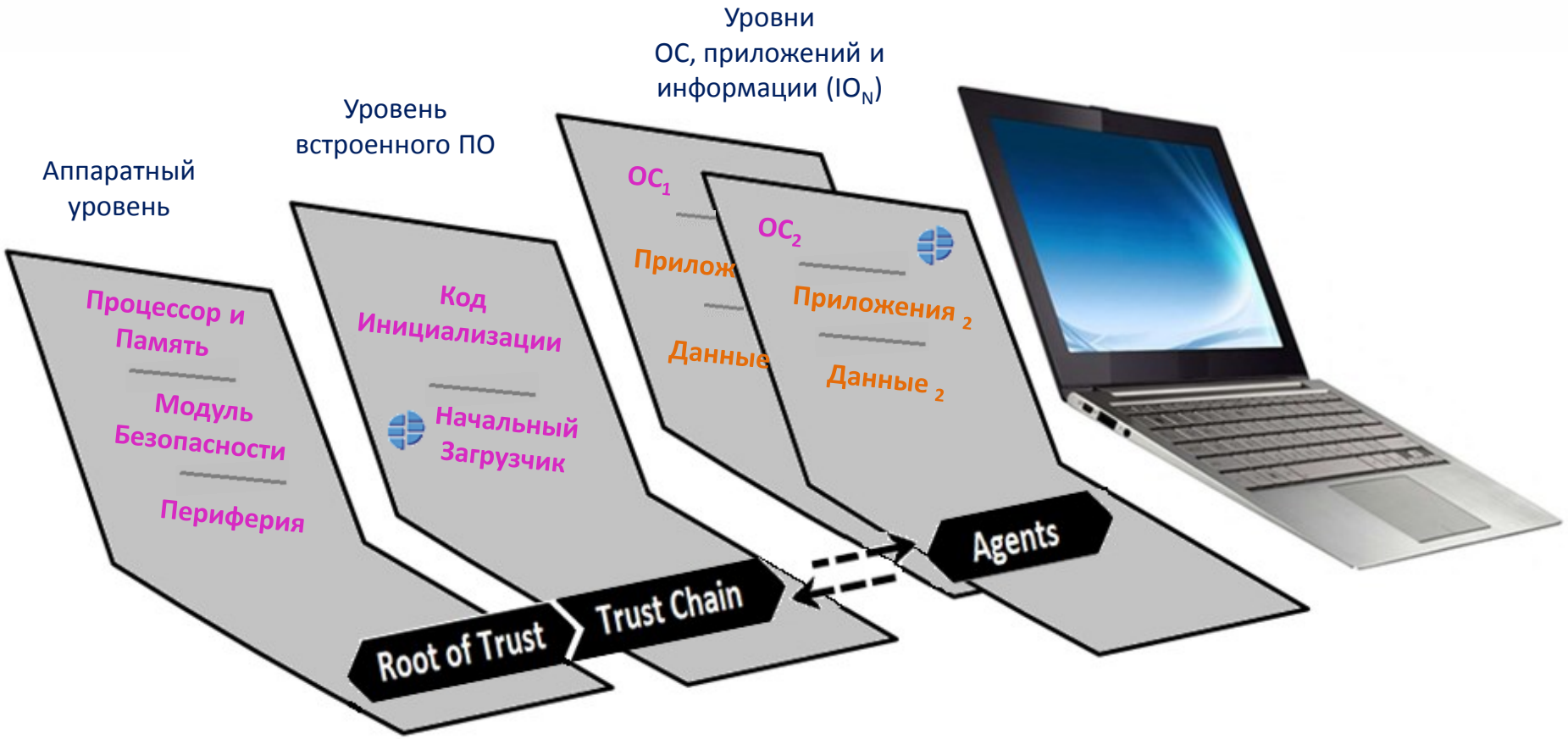
# Мобильное ЗАРМ - Модуль ДСК



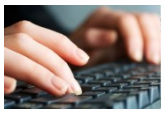

СПО ЭЛВИС+, разработанное в соответствии с требованиями регуляторов, предназначено для:

- доверенной начальной загрузки компьютера с контролем целостности его конфигурации, BIOS, начального сектора диска, СПО ЭЛВИС+ и критичных файлов и настроек ОС;
- обеспечения конфиденциальности хранимых данных при утере или краже компьютера за счет шифрования жесткого диска алгоритмами, соответствующими Российскому законодательству (до класса КС3).

# Модуль ДСК: Логическая архитектура



# Доверенный режим Модуль ДСК

Встроенный чип безопасности


Загрузка доверенной ОС. Расшифровка данных.

Доверенная среда

Конфиденциальные данные

Корпоративная сеть

Internet

# Публичный режим Модуль ДСК

Встроенный чип безопасности


Загрузка базовой ОС. Конфиденциальные данные зашифрованы

Недоверенная среда

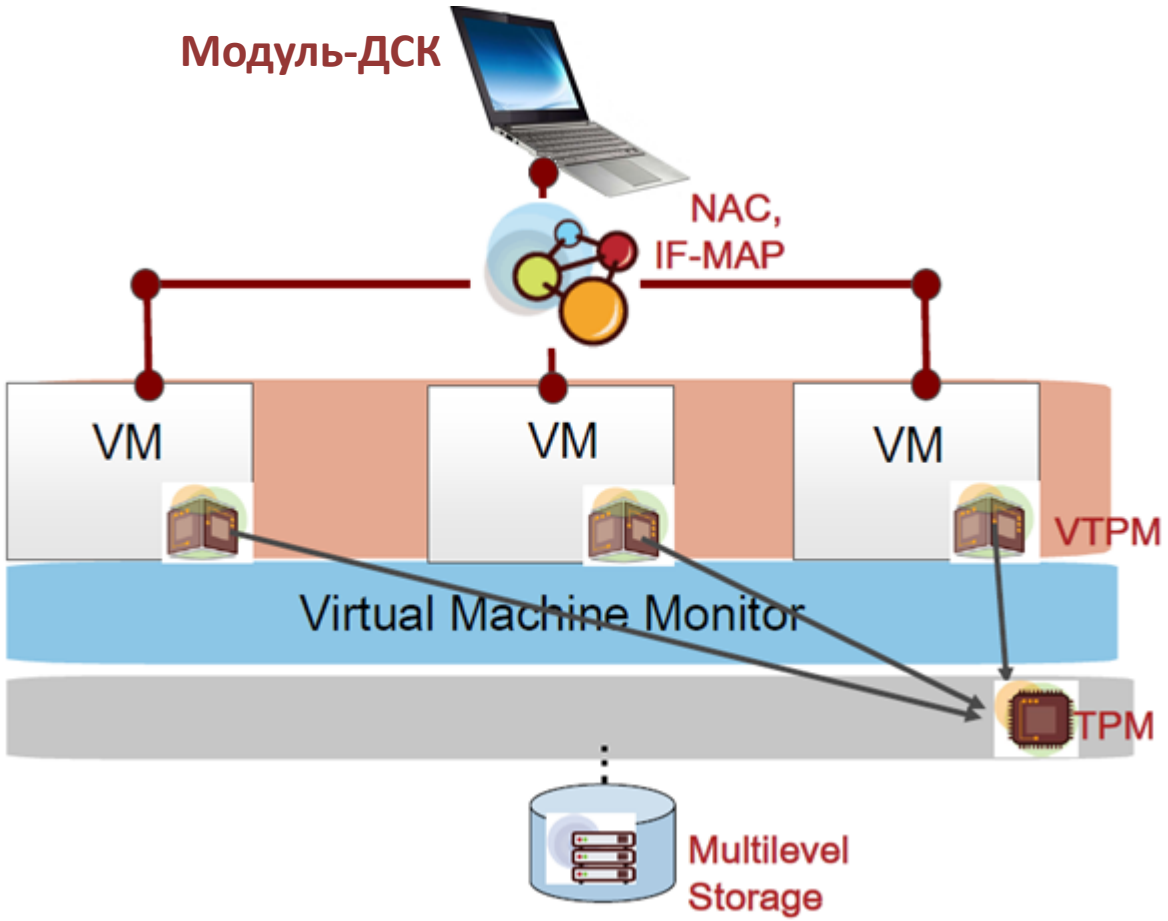
Конфиденциальные данные

Корпоративная сеть

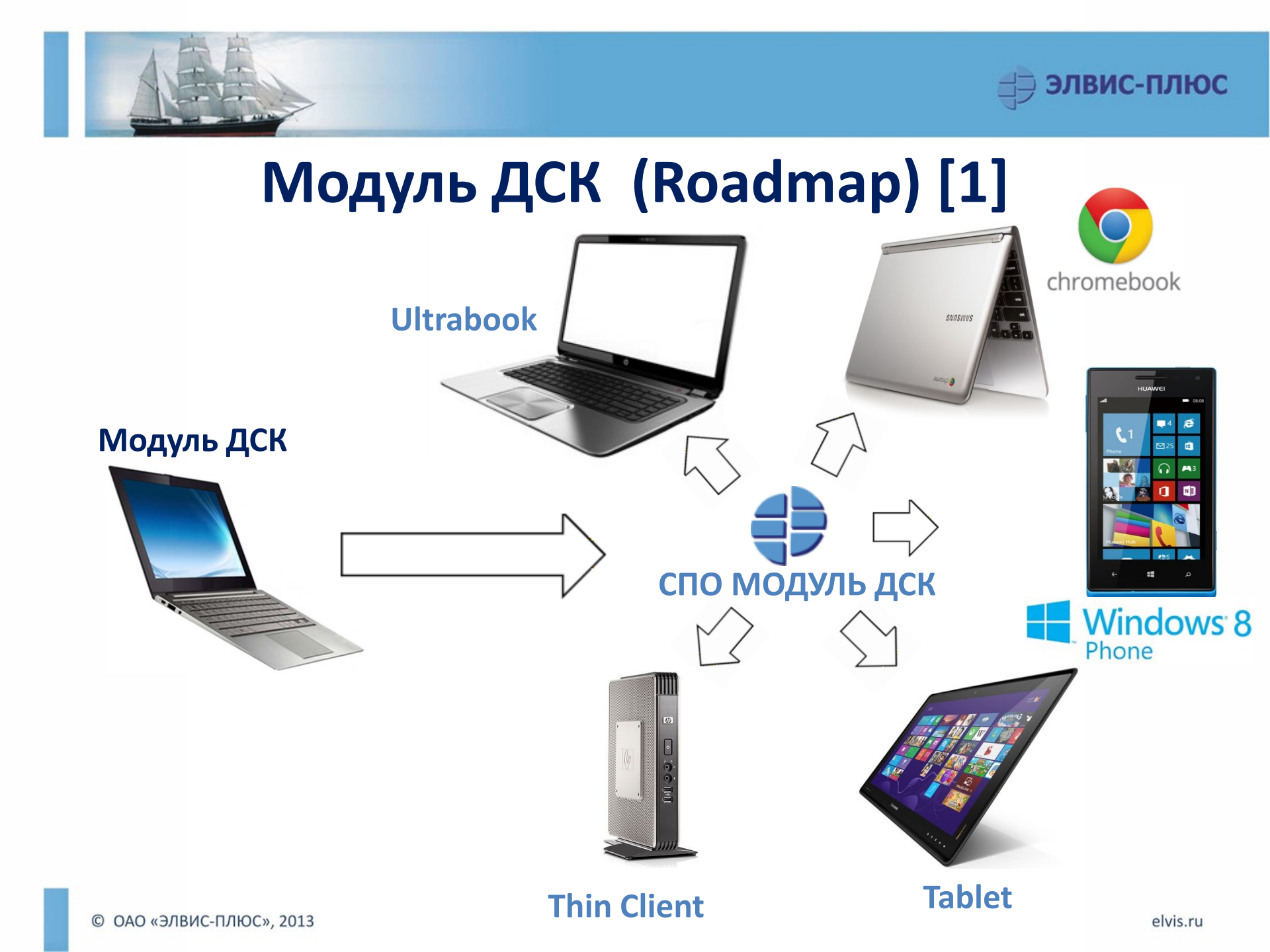
Зашифровано

Internet

# Модуль ДСК в структуре доверенного Облака



# Модуль ДСК (Roadmap) [1]



# Модуль ДСК (Roadmap) [2]


Сервер ДСК

Домен ДСК


Сеть ДСК

Доверенное Облако

# Доверенные Технологии Модуль ДСК (Roadmap)

Intel® VT-d, VT-x и Trusted Execution Technology (TXT)

Universal Extensible Firmware Interface (UEFI) v 2.2

Secure Boot

Trusted Platform Module (TPM) v 2.0

Intel® Platform Trust Technology

Intel® Boot Guard (Anchor Cove)

BIOS Guard

Криптография: ГОСТ 28147-89, ГОСТ Р 34.11-2012


Благодарю за внимание