Моделирование угроз для BIOS/UEFI

Алексей Лукацкий
Бизнес-консультант по безопасности

Загнивающая интеллигенция объясняет рабочему классу как моделировать угрозы

Что такое BIOS и UEFI?

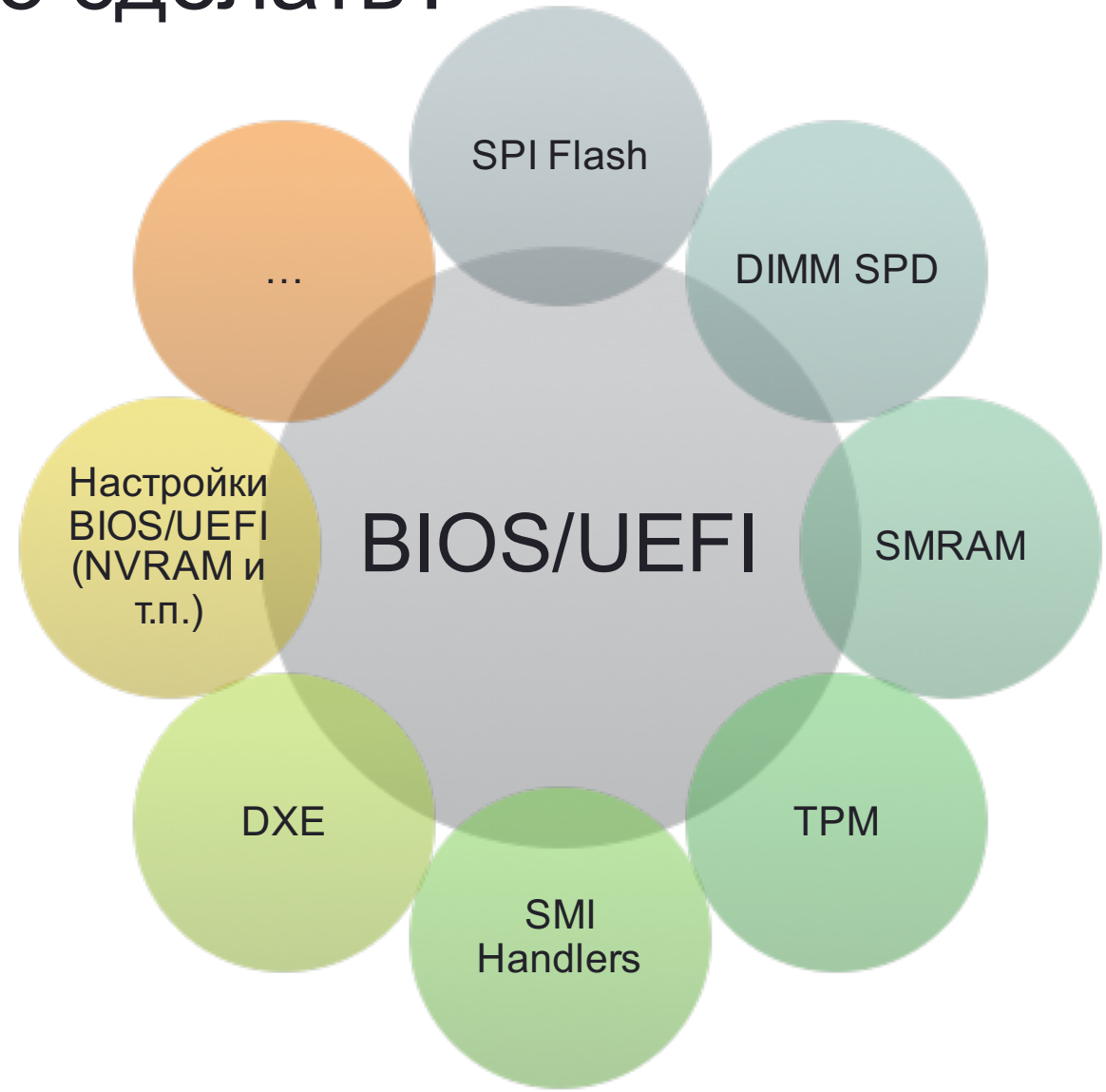
- BIOS (**b**asic **i**nput/**o**utput **s**ystem) / UEFI (**U**nified **E**xtensible **F**irmware **I**nterface) – интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования (ПК, мобильных устройств, сетевого оборудования и т.п.)
- Основное предназначение – корректная инициализация оборудования при включении системы и передача управления загрузчику операционной системы (MS Windows, Linux, Cisco IOS и т.п.)
- UEFI предназначен для замены «устаревшей» BIOS

Что плохого можно сделать с/через BIOS/UEFI?

Как это можно сделать?

- Установка и запуск вредоносного кода
- Смена порядка загрузки ОС или невозможность загрузки ОС
- Перехват данных (например, пароля BIOS)
- Манипуляция или порча переменных, процедур, регистров, областей памяти и т.п. в компонентах BIOS / UEFI
- Запрет подсистемы защиты или обход защищенной загрузки (secure boot)
- Кража криптографических ключей и сертификатов

Где это можно сделать?



Это реальность

Как управлять всем, что мы знаем?

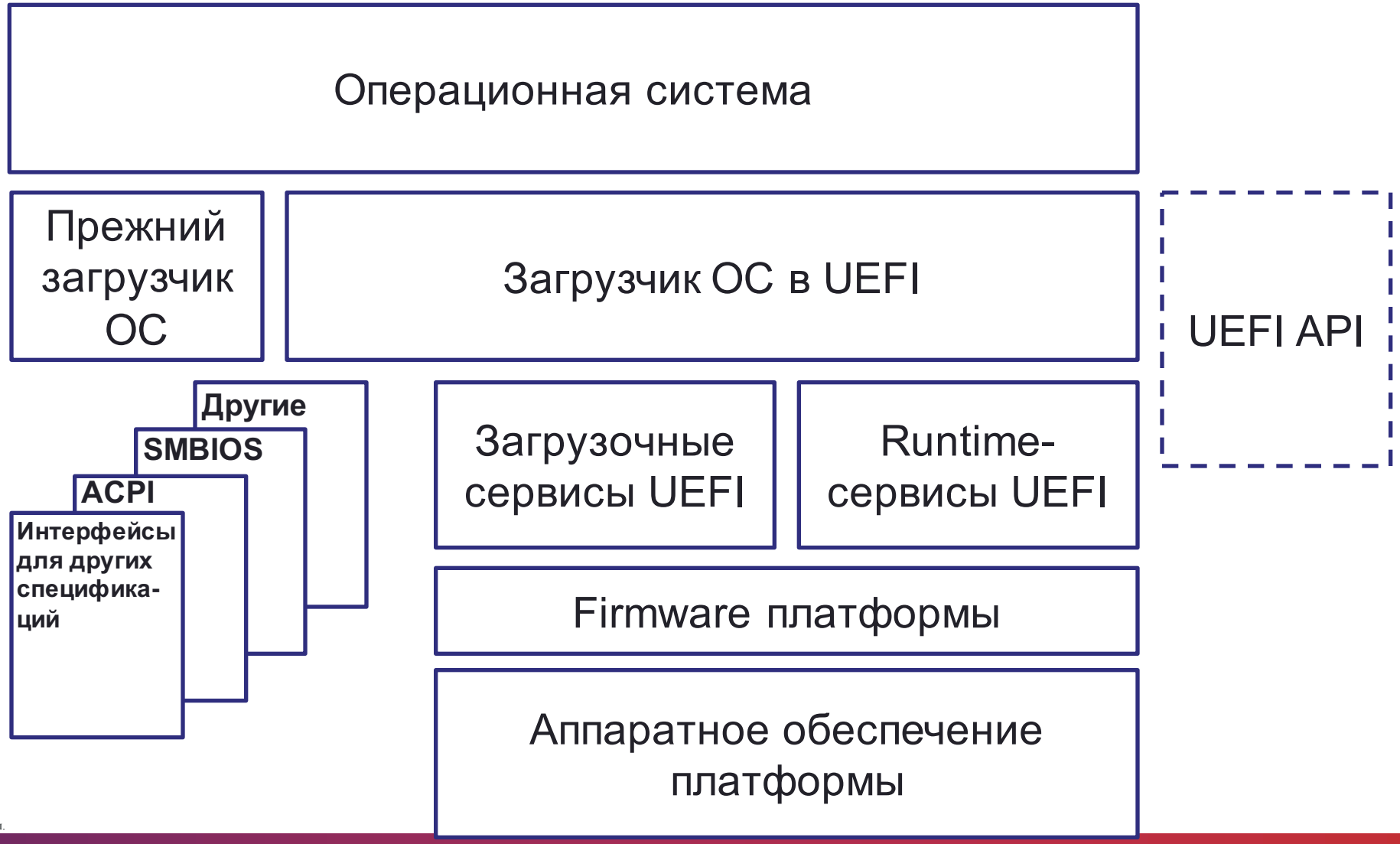
3 подхода к моделированию угроз

- Ориентированный на объекты защиты (asset centric)
- Ориентированный на нарушителя (attacker centric)
- Ориентированный на дизайн (software centric, defense centric)

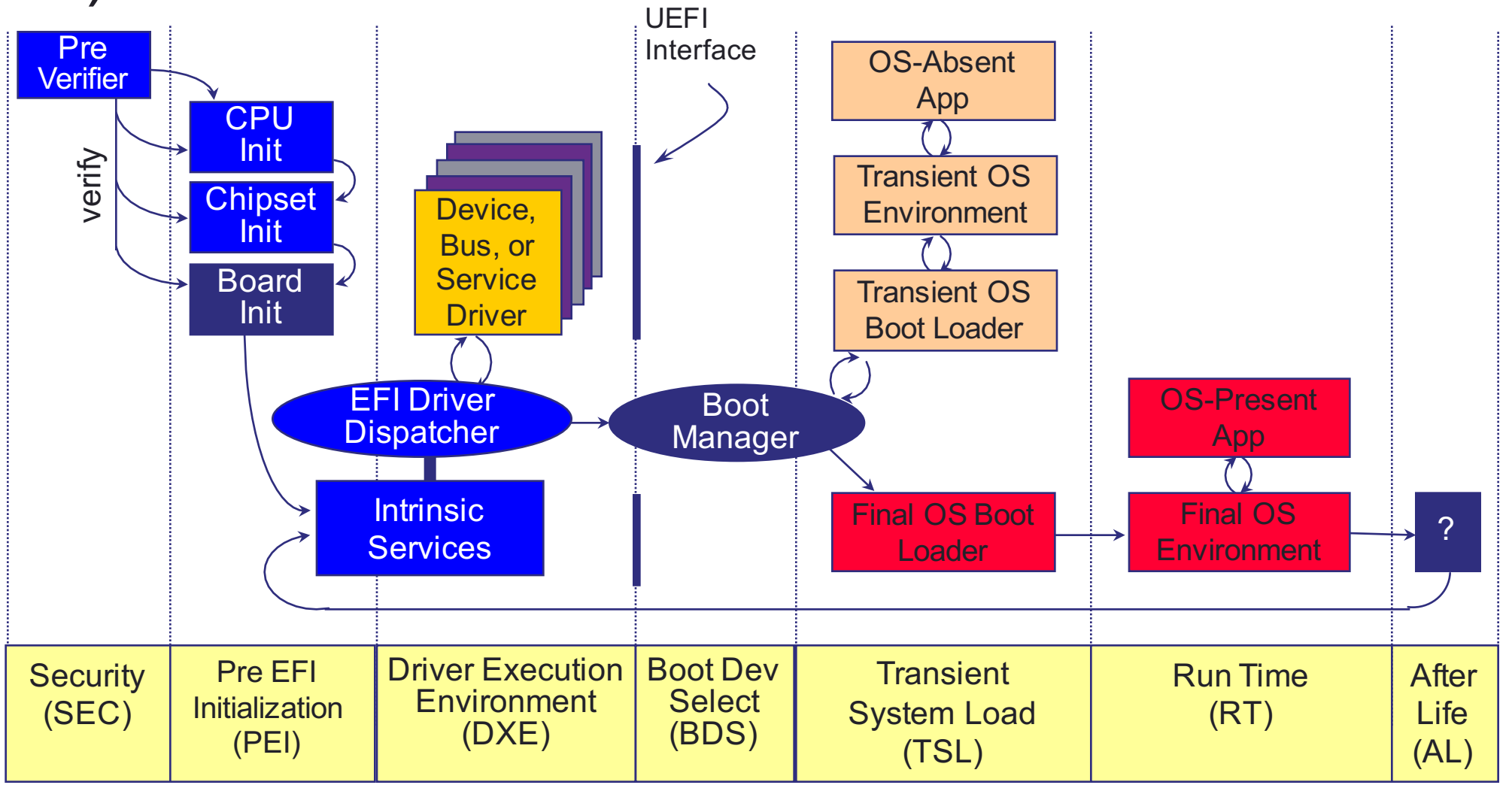
Ориентация на объекты защиты

- Объект защиты – элементы системы, которые требуют защиты от некорректного или несанкционированного использования
  - Программное обеспечение, компьютеры, сетевое оборудование, сегмент сети, информационная система, BIOS и т.п.
- Если рассматривать BIOS в качестве анализируемой с точки зрения угроз системы, то объектами защиты будут являться
  - Flash
  - TPM (Trusted Platform Module)
  - NVRAM (Non-volatile random-access memory)
  - SMM (System Management Mode)
  - SMI (System Management Interrupt)
  - GPIO (general-purpose input/output)
  - Драйвера DXE (Driver Execution Environment)
  - И другие

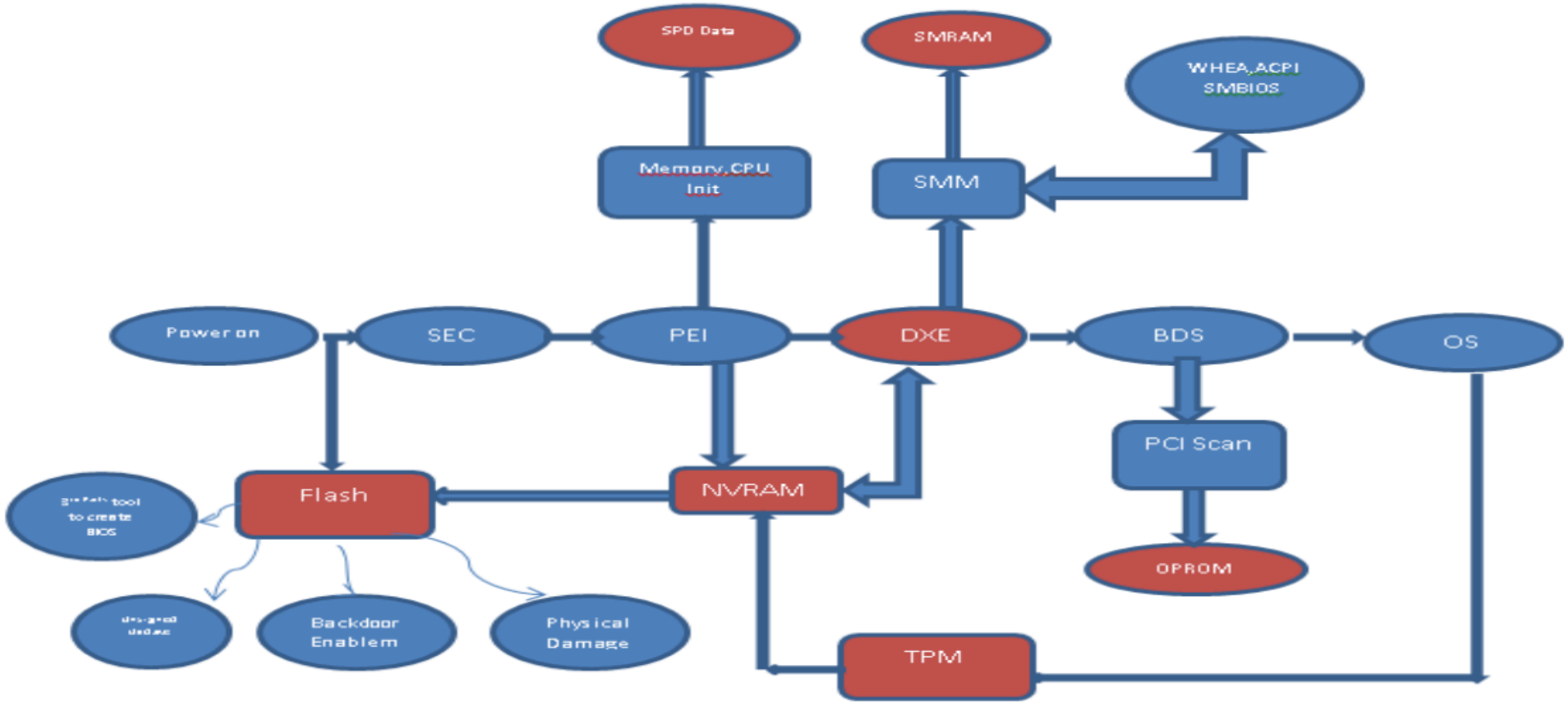
Структура UEFI (как объекта защиты)



Процесс загрузки устройства (информационные потоки)



Взгляд на UEFI с точки зрения объекта защиты



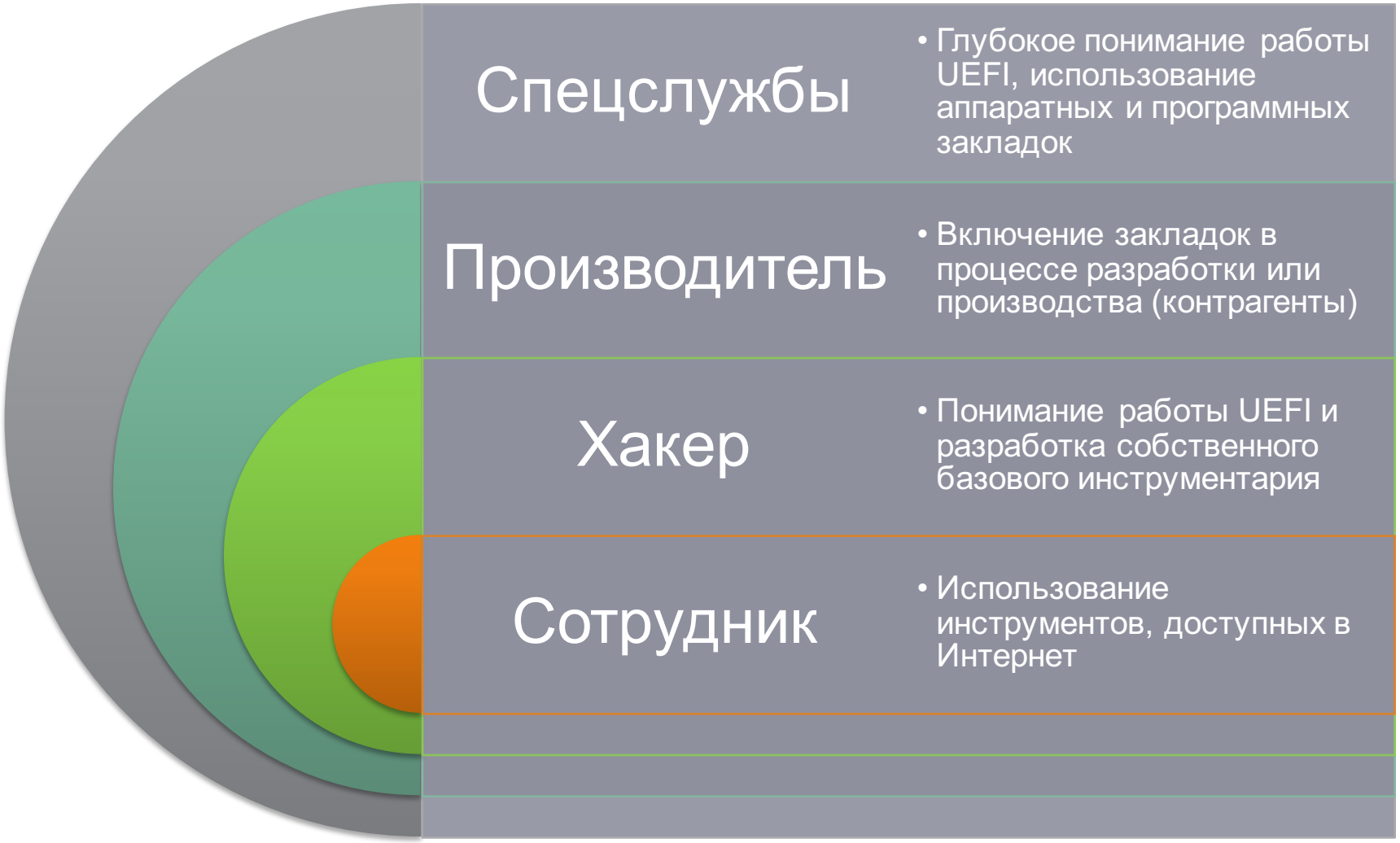
Взгляд на UEFI с точки зрения объекта защиты

Объект защиты	Атака
Flash	Стереть, запустить вредоносный код, доступ на запись
GPIO	Манипуляция GPIO в процессе исполнения
DIMM SPD	Манипуляция/порча данных в микросхеме SPD на модулях памяти
3rd firmware и OPROM	Перехват (hooking) сервисов BIOS и UEFI
Драйвера DXE	Изменение драйверов или приложений UEFI
WHEA	Переполнение region FLASH
TPM	Манипуляция PCR
Переменные NVRAM	Переполнение или порча региона NVRAM
SMM	Перевод вызовов SMM на другие указатели
SMI	SW SMI может испортить BIOS, отказ в обслуживании
Файл BIOS Capsule	Подделка файла Capsule для внедрения собственного кода

Ориентация на нарушителя

- Нарушитель – лицо, которое способно некорректно или несанкционированно использовать защищаемую систему
  - Сотрудник, хакер, ОПГ, спецслужбы, государства и т.п.
- Если рассматривать BIOS в качестве анализируемой с точки зрения угроз системы, то нарушителями будут являться, например
  - Производители
  - Хакеры
  - Спецслужбы
  - И другие
- Данный подход активно использует ФСБ при сертификации средств криптографической защиты
  - Требования устанавливаются исходя не из объекта защиты (СКЗИ), а возможностей нарушителя

Возможности нарушителя



Взгляд на UEFI с точки зрения нарушителя

Сотрудник	Хакер	Производитель / спецслужбы
Редактор BIOS	Генератор SMI	Использование руткитов и буткитов
Взломщик паролей BIOS	Изменение настроек регистров MSR	Изменение регистров memmap
BIOSMD, Unicore BIOS Wizard	Запись бессмысленных данных в NVRAM	Модификация MSR
UniFlash		Манипуляция SMI
NVRAM Tool		Использование EDK API
amiutilities		Дизассемблер ASL для ACPI/ASL/AML
Скрипт удаление переменных UEFI		Команды IPMI для перехода в режим отладки
Утилиты работы с PCI-E		

Ориентация на дизайн

- Метод, обычно используемый при моделировании угроз для программного обеспечения, и опирающийся на анализ слабых мест, границ, точек входа, интерфейсов для ПО
- Обычно используется разработчиками ПО
  - Например, Microsoft, Cisco, EMC и другими
- В основу обычно положена модель STRIDE, предложенная Microsoft (не работает для новых и «творческих» угроз)
  - **S**poofing (подмена)
  - **T**ampering (искажение данных)
  - **R**epudiation (отказ от авторства)
  - **I**nformation disclosure (раскрытие информации)
  - **D**enial of Service (отказ в обслуживании)
  - **E**levation of privilege (повышение привилегий)

Взгляд на UEFI с точки зрения дизайна

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilige
Маскировка под администратора	Порча NVRAM	Декларация, но не удаление загрузочных переменных	Пароли BIOS	Бесконечный цикл SMI	Руткиты/буткиты для скрытия вредоносного кода
Использование утилиты настройки BIOS для изменения пользователя	Порча сертификатов	Манипуляция загрузкой	Логи BIOS	Установки таймера через IPMI	Контрольные суммы SMRAM
	Манипуляция данными на Flash	Очистка ключей TPM	Переменные UEFI	Предотвращение загрузки	Указатели API UEFI
	Манипуляция/модификация хранилища паролей		Последовательность загрузки	Манипуляции с TPM	Перехват ROM
	Таблицы ACPI		Раскрытие содержимого Flash BIOS		

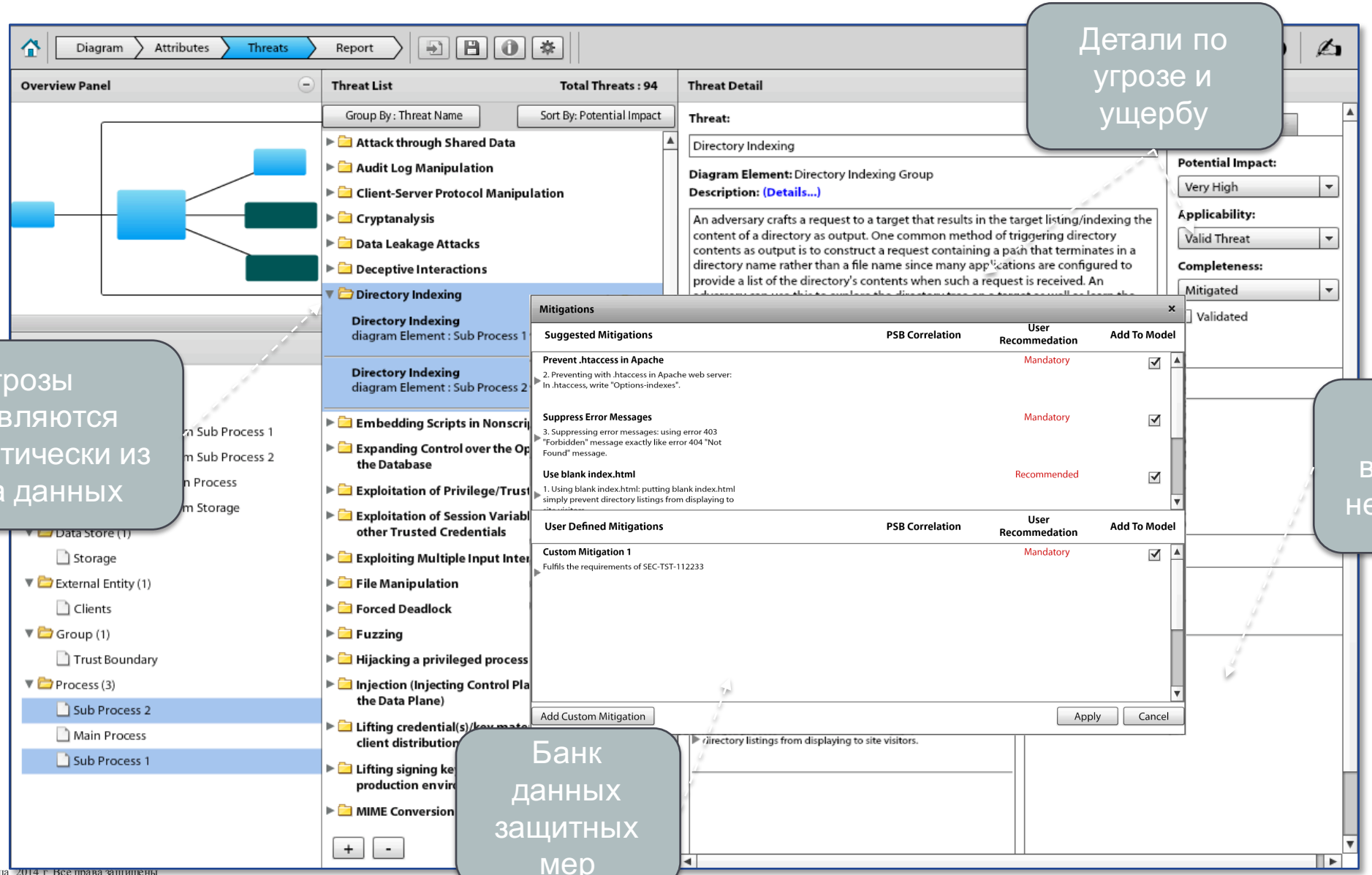
А дальше то что?

Что дальше?

- Приоритезация угроз зависит от приоритезации объектов защиты/нарушителей/компонентов ПО по возможному наносимому ущербу
- Ущерб может иметь разную форму, зависящую от масштаба объекта

  Например, потеря доверия, удар по репутации, ответственность перед законом, угроза персонала, финансовые потери, принятие неправильных решений, обман, прерывание коммерческих операций или технологических процессов, неспособность выполнить поставленные задачи, неконтролируемые действия, потеря управления и т.п.
- От высокоуровневых угроз (типов угроз) к низкоуровневым атакам, которые могут быть определены через дерево атак или библиотеку (банк данных) атак
- В обязательном порядке необходима схема/карта защищаемой системы
- Идеально, если процесс моделирования угроз будет базироваться на средствах автоматизации, облегчающих процесс выбора актуальных угроз (из банка данных или дерева атак)

Cisco ThreatBuilder – средство автоматизации в рамках CSDL



Детали по угрозе и ущербу

Угрозы добавляются автоматически из банка данных

Проверка возможности нейтрализации

Банк данных защитных мер

Ничего, и вас научим моделировать угрозы

Благодарю за внимание