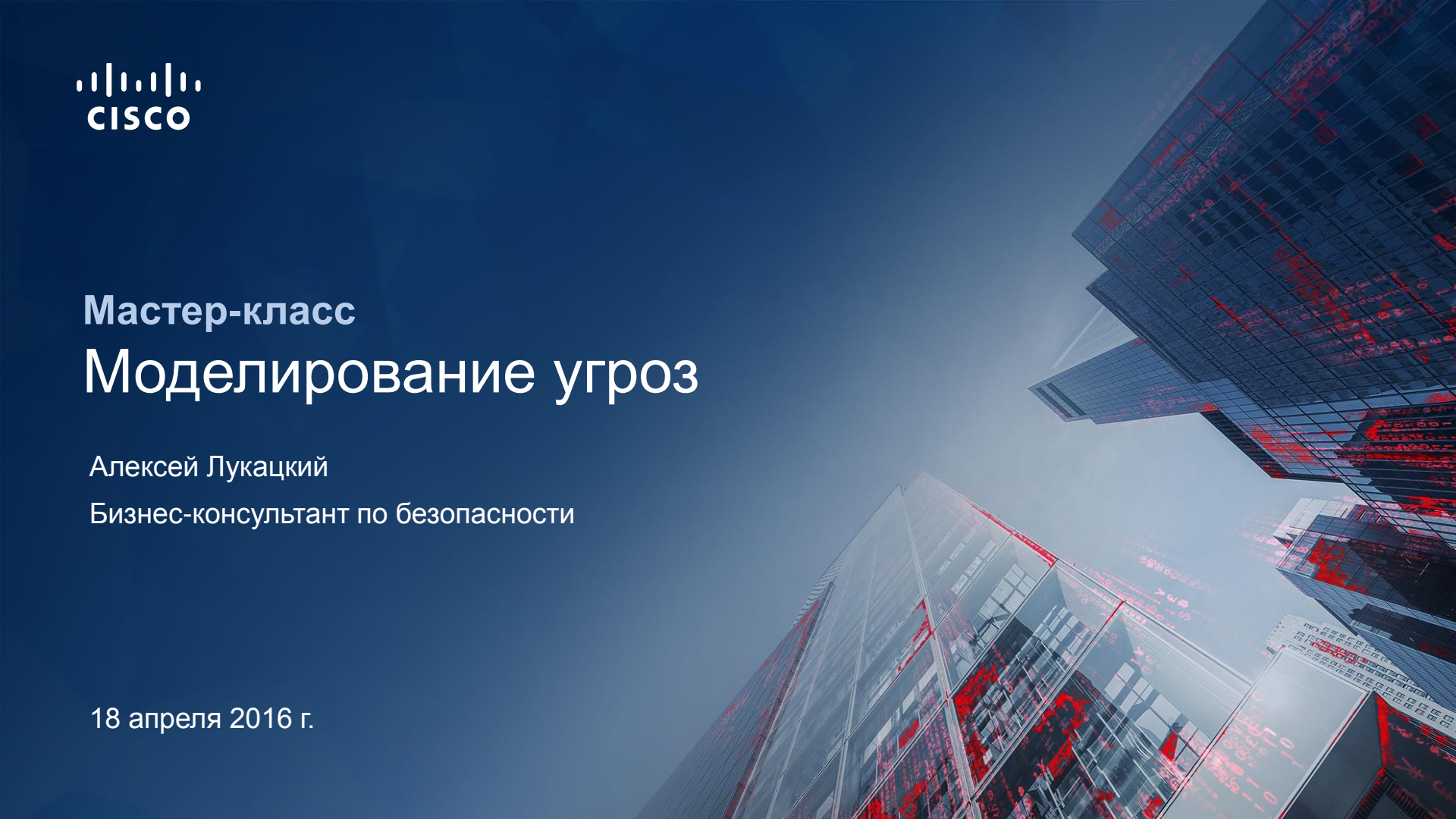


Мастер-класс

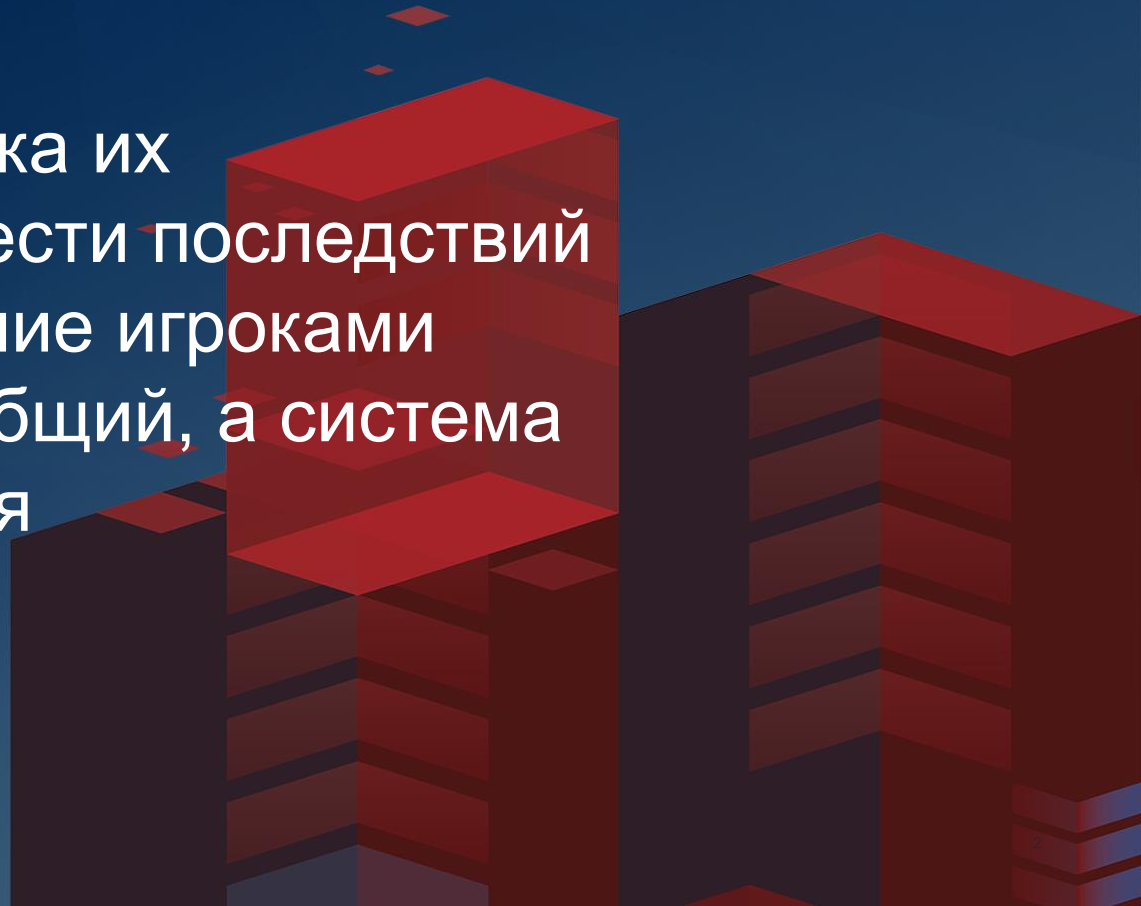
Моделирование угроз

Алексей Лукацкий

Бизнес-консультант по безопасности

18 апреля 2016 г.

Анализ угроз, оценка их вероятности и тяжести последствий похожа на посещение игроками Лас-Вегаса – зал общий, а система игры у каждого своя



Совет №1

- Поймите, что для вас угроза

Угрозы или угрозы?

Все зависит от вашего понимания ИБ

- Информационная безопасность - состояние защищенности интересов стейкхолдеров предприятия в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества, государства и бизнеса
- Очень емкое и многоуровневое определение
- Может без изменения применяться в любой организации

  Меняться будет только наполнение ее ключевых элементов – стейкхолдеры, информационная сфера, интересы

Стейкхолдеры ИБ

Внутри предприятия

- ИТ
- **ИБ**
- Юристы
- Служба внутреннего контроля
- HR
- Бизнес-подразделения
- Руководство
- Пользователи

Снаружи предприятия

- Акционеры
- Клиенты
- Партнеры
- Аудиторы

Регуляторы

- **ФСТЭК**
- **ФСБ**
- **Роскомнадзор**
- СВР
- **МО**
- Банк России

Информационная сфера

- Информационная сфера - это совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений
- В данном определении информационная инфраструктура включает в себя также и технологии обработки информации

Интересы стейкхолдеров

- Универсального списка интересов не существует – у каждого предприятия на каждом этапе его развития в различном окружении при различных руководителях интересы различны

ИБ	Юристы	Регуляторы
• Конфиденциальность • Целостность • Доступность	• Соответствие • Защита от преследования • Новые законы	• Соответствие
Пользователи	**Акционеры**	**ИТ**
• Тайна переписки • Бесперебойный Интернет • Комфорт работы	• Рост стоимости акций • Контроль топ-менеджмента • Прозрачность	• Доступность сервисов • Интеграция • Снижение CapEx

Интересы бизнеса

- Рост (доли рынка, маржинальности, доходности…)
- Экспансия (новые рынки, новые целевые аудитории)
- Рост продуктивности сотрудников
- Соответствие требованиям
- Инновации и новые бизнес-практики
- Реинжиниринг бизнес-процессов
- Взаимоотношения с клиентами (лояльность)
- …

Некоторые угрозы с киберучений в Магнитогорске и в Санкт-Петербурге

- А что если завтра отключат обновления приобретенных вами средств защиты?
- А что если завтра введут санкции в области ИТ/ИБ и нельзя будет купить средства защиты, которые использовались ранее?
- А что если к вам придет проверка РКН по жалобе о нарушении вами 242-ФЗ?
- А что если на форуме pastebin появятся доказательства компрометации вашей внутренней сети?

Некоторые угрозы с киберучений в Магнитогорске и в Санкт-Петербурге

- А что если ваше руководство решило сократить CapEx, переориентировав свои расходы на OpEx?
- А что если к вам пришла проверка МВД по поводу лицензионности софта и изъято оборудование, включая средства защиты
- А что если некоторые сотрудники, судя по информации в социальных сетях, выражают неудовольствие своей работой, руководством и уровнем своих доходов, сами испытывают материальные трудности, но гонятся за «красивой жизнью». Значит, они являются потенциальными инсайдерами для злоумышленников

Некоторые угрозы с киберучений в Магнитогорске и в Санкт-Петербурге

- А что если на банк ведётся активная информационная атака в социальных сетях: распространяется информация о текущих трудностях и множатся негативные оценки дальнейших перспектив. Налицо угроза оттока клиентов
- А что если вендор вывез вас заграницу и об этом сообщили вашему руководству, обвинив в коррупции?
- А что если вы работаете в госоргане и вам вручили подарок свыше 3000 рублей?
- А что если сертификат на СКЗИ закончился и его не продлевает производитель

Угрозы электронной личности руководителя госоргана

Угрозы информационным правам

- Компрометация персональных данных
- Нарушение тайны личности
- Размещение компрометирующих материалов

Угрозы воздействия информации на личность

- Навязывание информации, враждебная пропаганда
- Манипулирование сознанием и поведением
- Ложная и недостоверная информация, дезинформация

Угрозы взаимодействию

- Деанонимизация виртуальных личностей
- Сбор открытой и незащищенной информации
- «Троллинг»
- Взлом и похищение аккаунтов и виртуальных личностей

Угрозы для беспилотника

- Для физлица – кража
- Для логистической компании - выведение из строя
- Для МинОбороны – перехват управления

Что нас заставляет заниматься моделированием угроз?

Совет №2

- Определитесь с объектом защиты. Масштаб и детализация имеют значение

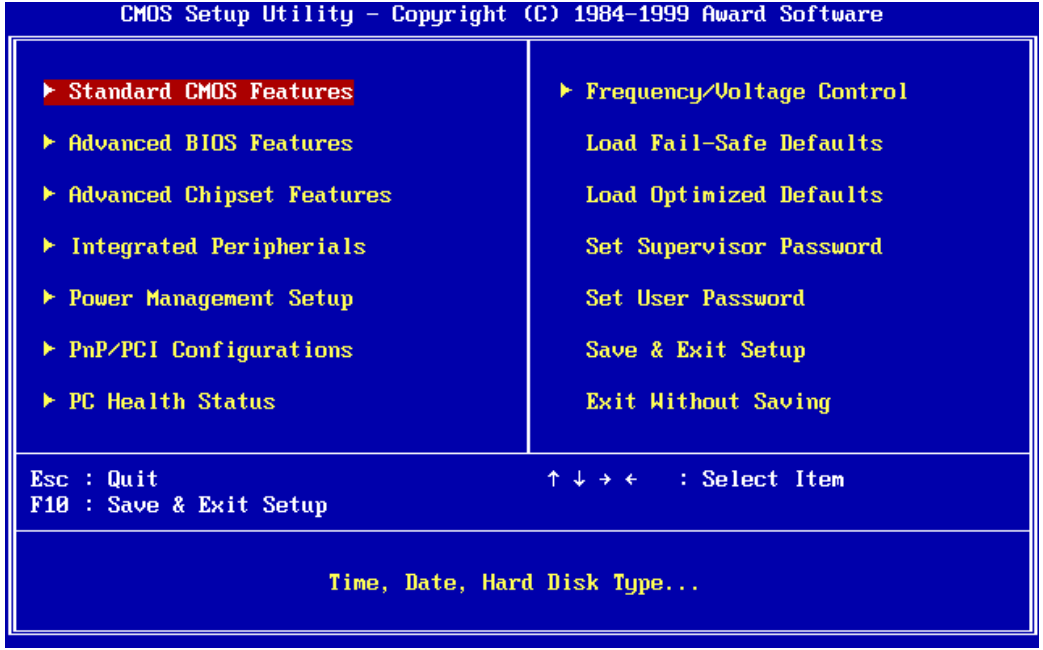
АСУ ТП

Секс-робот

Умные часы Apple Watch

WATCH

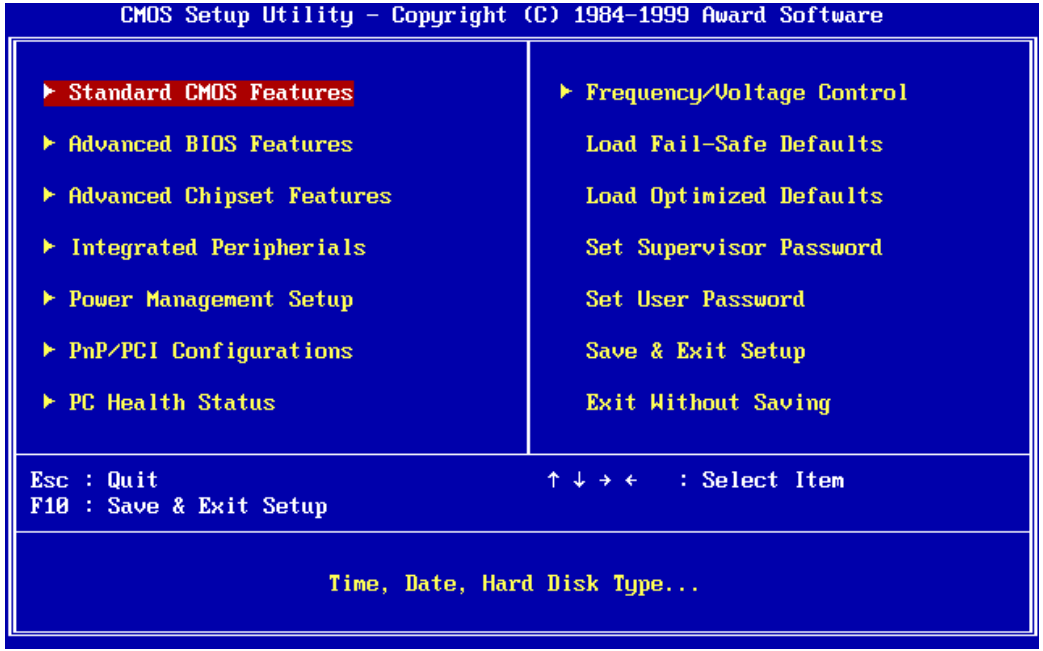
BIOS / UEFI


CMOS Setup Utility – Copyright (C) 1984-1999 Award Software
Standard CMOS Features
Advanced BIOS Features
Advanced Chipset Features
Integrated Peripherials
Power Management Setup
PnP/PCI Configurations
PC Health Status
Frequency/Voltage Control
Load Fail-Safe Defaults
Load Optimized Defaults
Set Supervisor Password
Set User Password
Save & Exit Setup
Exit Without Saving
Esc : Quit
F10 : Save & Exit Setup
↑ ↓ → ← : Select Item
Time, Date, Hard Disk Type...

Совет №3

- Поймите, что делает объект защиты и учитывайте, что он может менять свой функционал с течением времени

BIOS / UEFI



- Инициализация оборудования при включении системы и передача управления загрузчику ОС
- Может быть неизменяемой

Секс-робот

- Занимается сексом
- Возможно обновление прошивки и получение новых «программ»

Умные часы Apple Watch

WATCH

- Показывают время
- Отслеживают местоположение
- Измеряет активность
- Имеют доступ к почте
- И многое другое

Умные часы Apple Watch

Клиника Майо

August Smart Lock

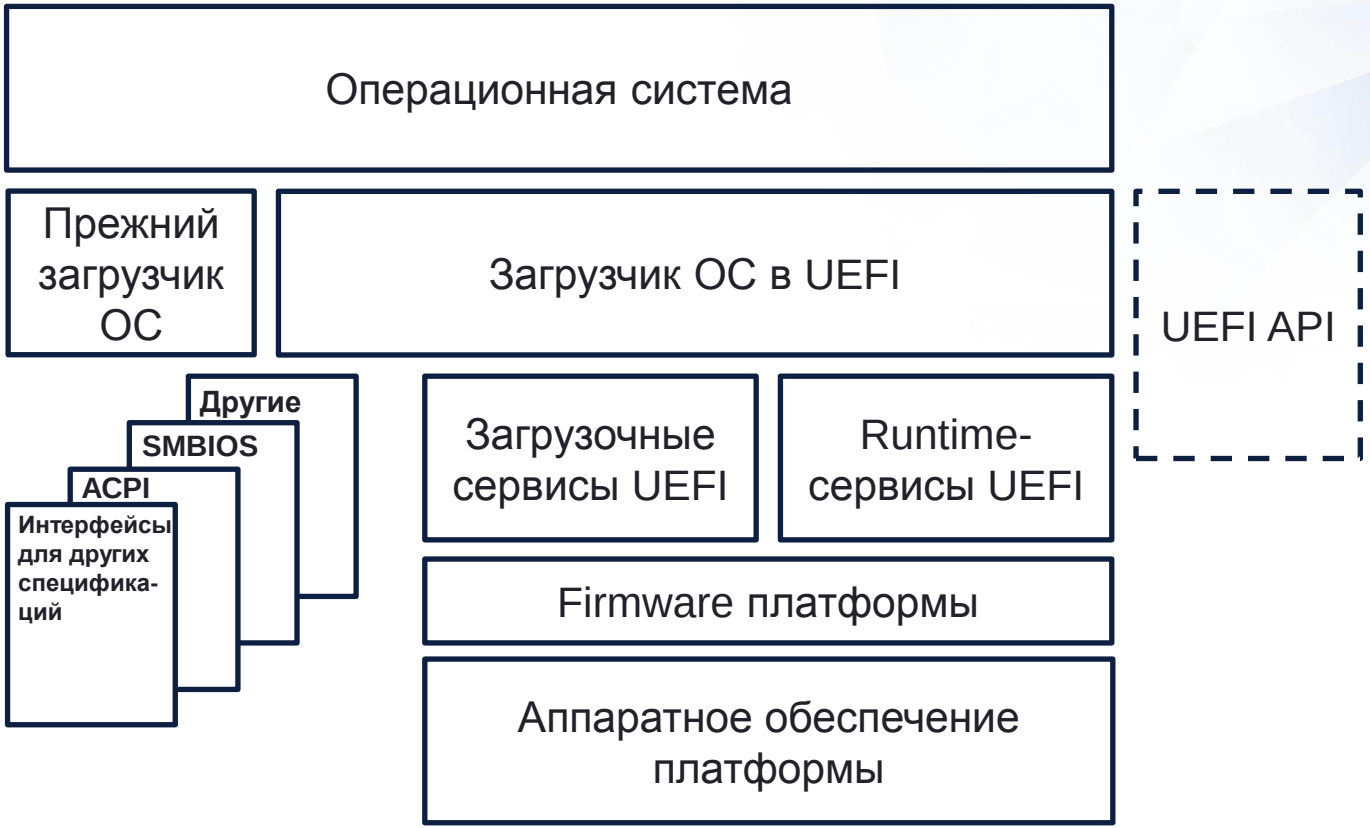
Starbucks

Do It

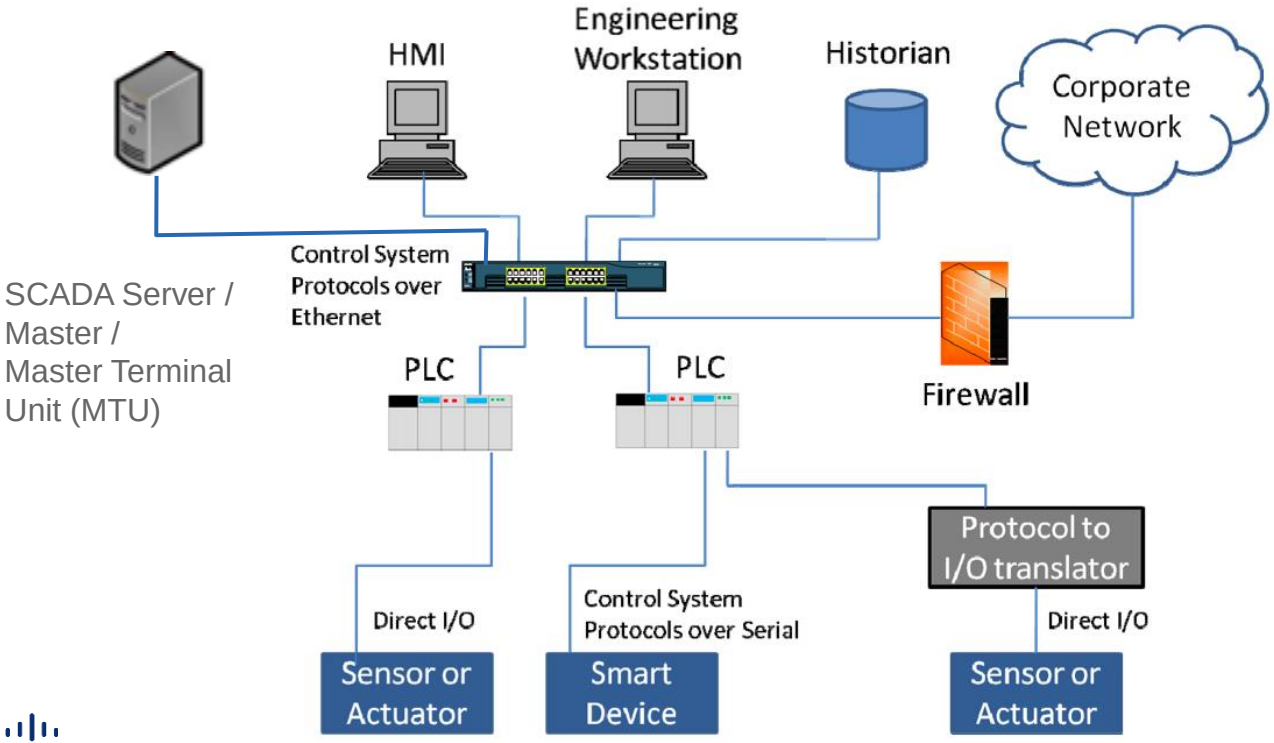
Совет №4

- Очертите границы объекта защиты и точки входа/выхода

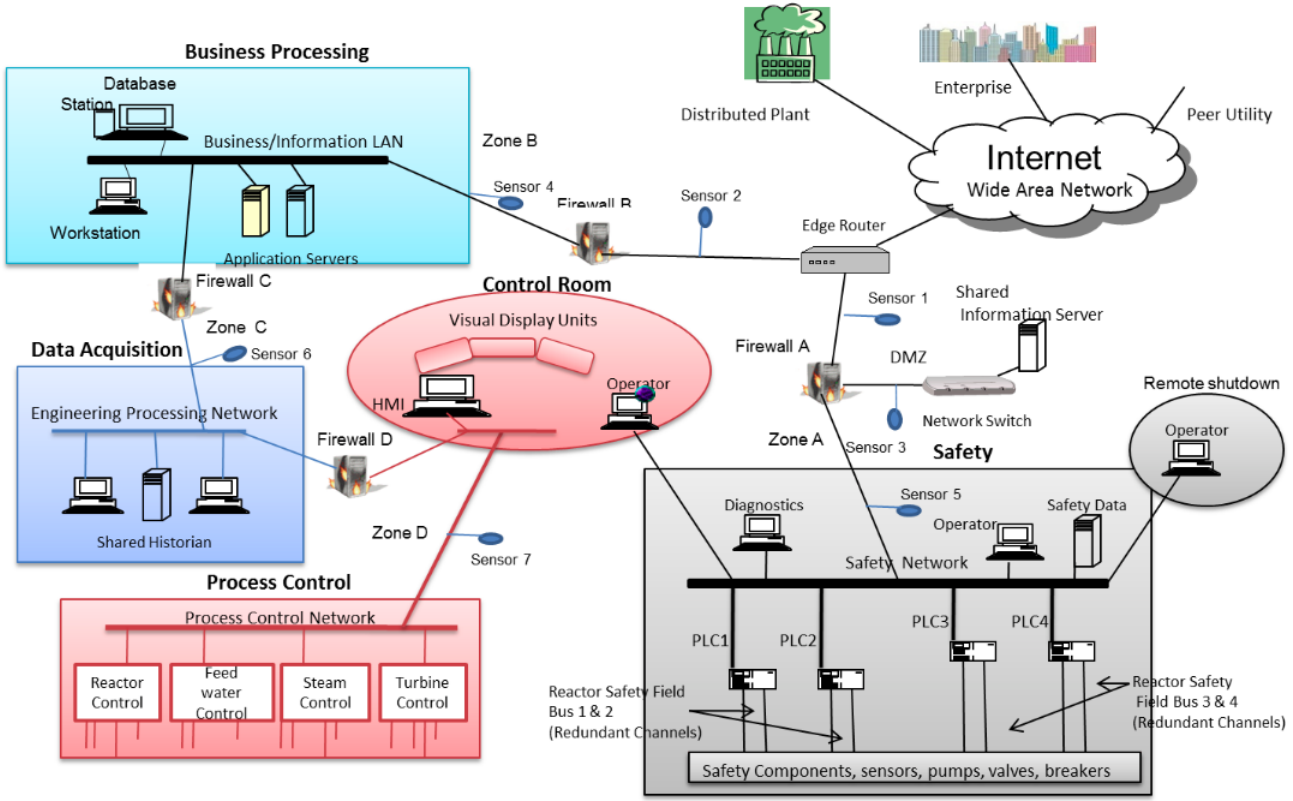
Структура UEFI



Типичная архитектура АСУ ТП



Границы и точки входа на атомной электростанции в США

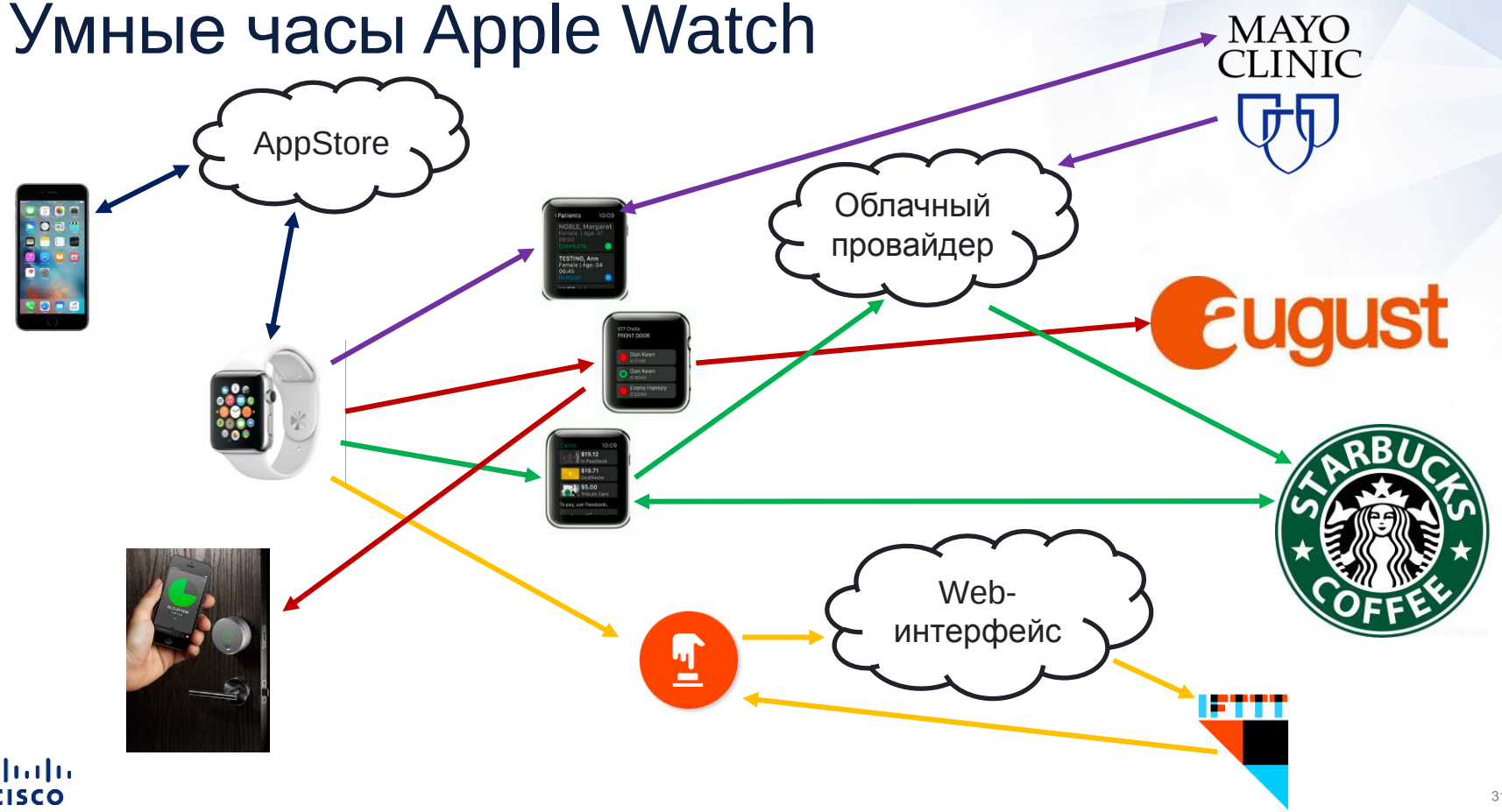


Умные часы Apple Watch

WATCH

- Часы
- Смартфон iPhone
- Сервера Apple
  - AppStore
  - iCloud
- Каналы связи
- Инфраструктура приложений
- Хранилища данных

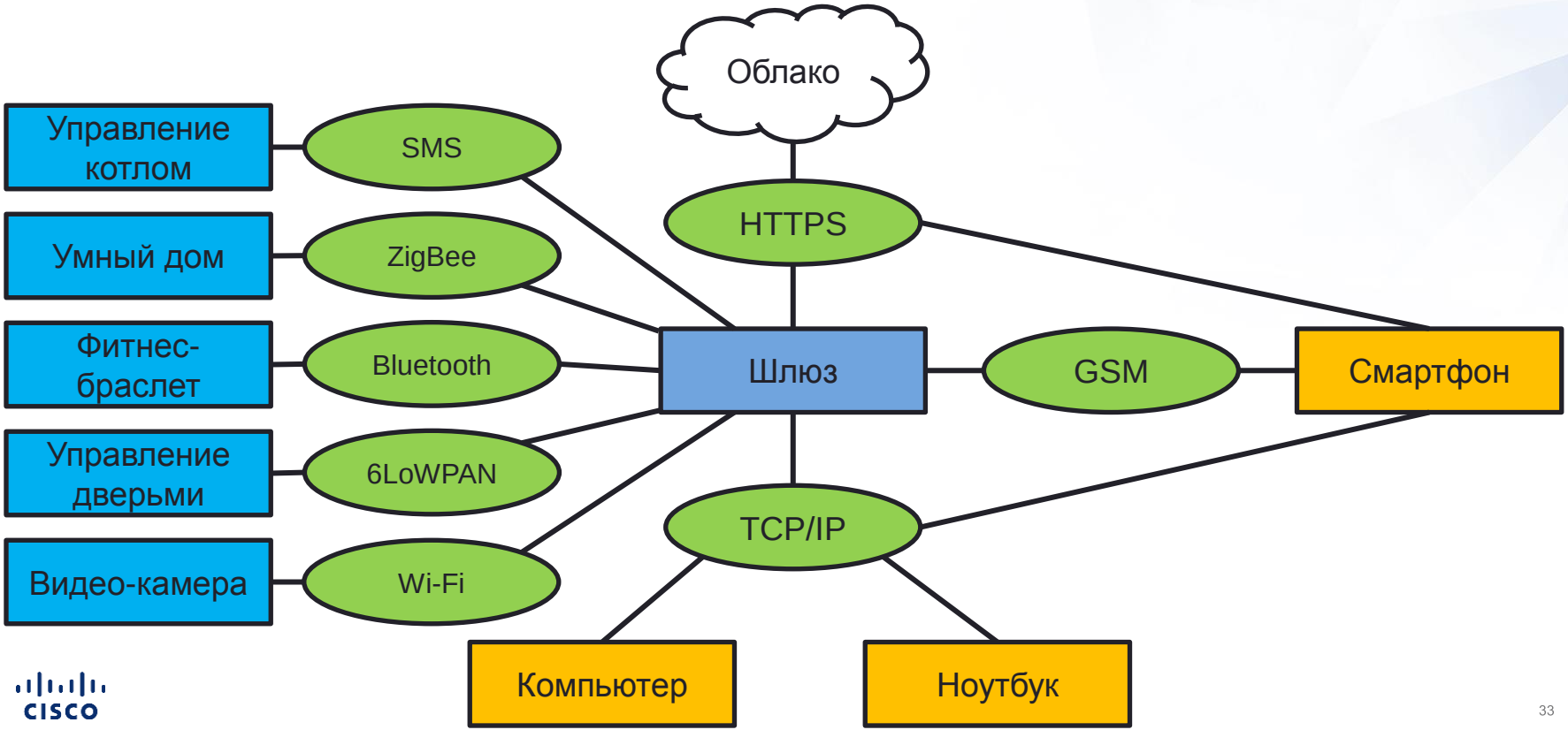
Умные часы Apple Watch



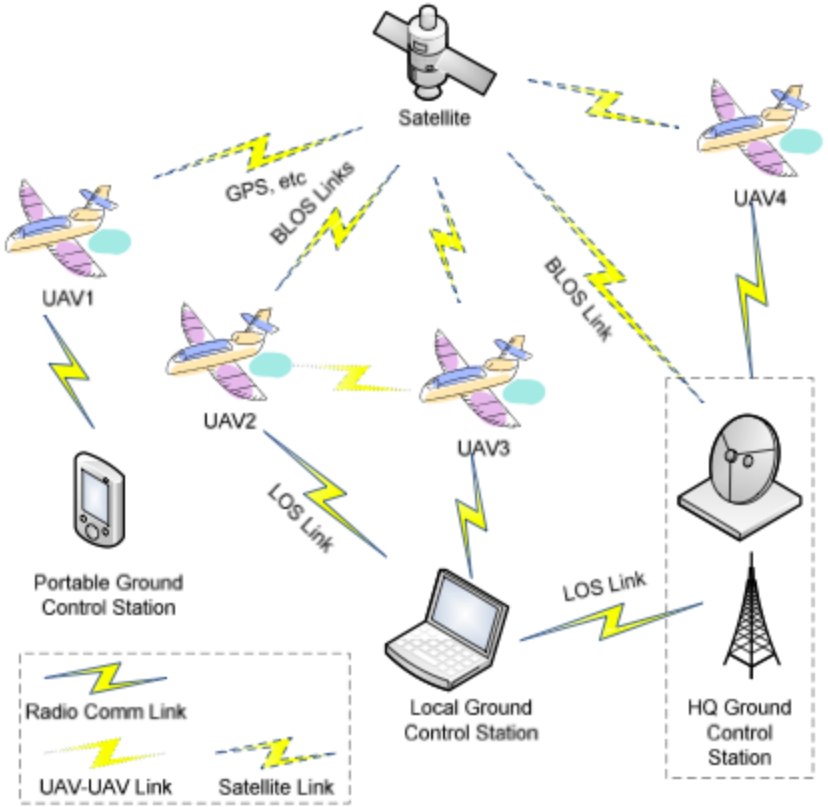
Секс-робот

- Устройство
- Каналы связи (USB, Wi-Fi, Bluetooth)
- Сервер обновлений

Типичная архитектура IoT



Беспилотник



Совет №5

- Обратите внимание на обслуживающую инфраструктуру
  - Персонал
  - Инфраструктура оператора связи
  - Подстанция, дающая электричество для работы систем защиты
  - DNS-сервера
  - Облачные инфраструктуры
  - Социальные сети

Совет №6

- При оценке угрозы необходимо принимать во внимание человеческий фактор
  - Взаимодействие человек – техсредство
  - Взаимодействие между людьми
  - Психологические аспекты
  - Эргономические факторы
  - Способность осознавать риск в данной ситуации (зависит от обучения, опыта или способностей)

Куда девать токен или смарткарту?

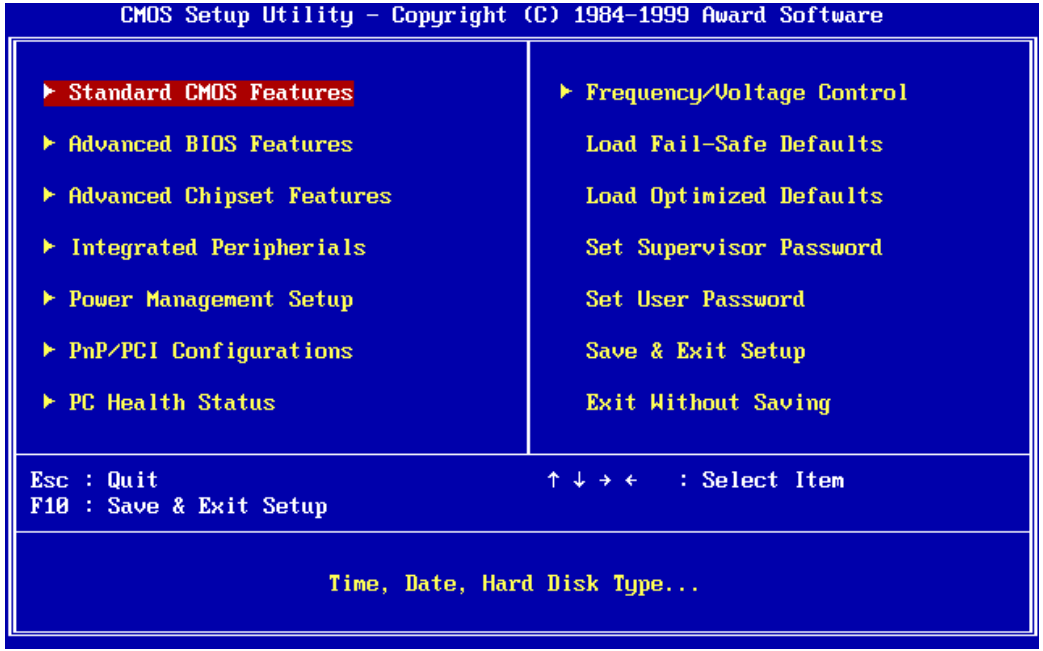
Отключение средств защиты

- При оценке риска необходимо принимать во внимание возможность отключения или расстройства защитных средств
- Побуждение сделать это возникает когда
  - Средства защиты снижают выпуск продукции или мешают другим действиям и намерениям потребителя
  - Средства защиты трудно применить
  - Должны быть привлечены не операторы, а другой персонал
  - Средства защиты не признаются или неприемлемы для их назначения
- Возможность отключения зависит как от их типа, так и от конструктивных особенностей

Совет №7

- Поймите, где может быть атакован объект защиты

BIOS / UEFI



- SPI Flash
- DIMM SPD
- SMRAM
- TPM
- SMI Handlers
- DXE
- Настройки BIOS /UEFI (NVRAM и т.п.)

Умные часы Apple Watch

WATCH

- Непосредственно у вас
- При сдаче в ремонт
- При покупке
- При логистике
- При сборке
- При разработке

Процедура производства и поставки оборудования (пример)

Совет №8

- Поймите, как может быть атакован объект защиты

BIOS/UEFI

- 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

Умные часы Apple Watch

- Могу я перехватить данные в процессе связывания устройств?
- Могу я получить доступ к данным на устройстве?
- Могу я перехватить данные в процессе синхронизации?
- Могу я получить доступ через уязвимое приложение?
- Могу ли я получить доступ к учетной записи?
- Могу ли я организовать DoS через доступ к чему-либо?
- Что я могу еще сделать?

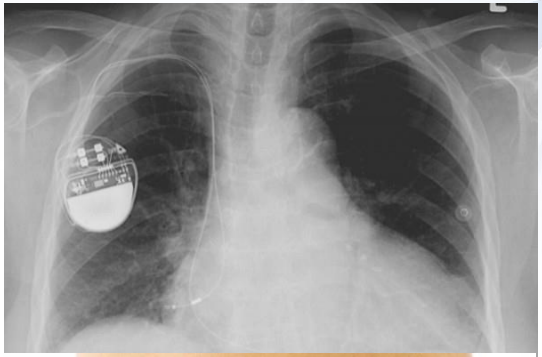
Секс-робот

- Отказ в обслуживании ☺
- Подмена прошивки
- Нарушение работоспособности
- Составление профиля клиента

Кто это?

Чем известен Барнаби Джек?

- Удаленная команда кардиостимулятору на выпуск разряда в 800 вольт
  - Интернет-дефибриллятор
- Червь, распространяющийся через кардиостимуляторы
  - Что насчет массового убийства?
- Дистанционный взлом инсулиновых помп



Совет №9

- Помните, что нам свойственно преувеличиваем одни угрозы и преуменьшать другие
- Наше восприятие угроз чаще всего «хромает» в пяти направлениях
  - Степень серьезности угрозы
  - Вероятность угрозы
  - Объем затрат
  - Эффективность контрмер
  - Возможность адекватного сопоставления угроз и мер нейтрализации

Психология восприятия риска

- Даже при наличии фактов и достаточного объема информации об анализируемой системе у экспертов существует сложность с восприятием риска
- Безопасность основана не только на вероятности различных рисков и эффективности различных контрмер (реальность), но и на ощущениях
- Ощущения зависят от психологических реакций на риски и контрмеры

  Чего вы больше опасаетесь – попасть в авиакатастрофу или автоаварию?

  Что вероятнее – пасть жертвой террористов или погибнуть на дороге?

Совет №10

- Приоритезируйте угрозы в зависимости 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.

Секс-робот

- Смерть от непрерывного… ☺
- Вывод из строя и финансовый ущерб
- Утечка информации об использовании секс-робота
- Кракжа секс-робота

Совет №11

- Учитывайте, что потери могут принимать разные формы

Формы потерь

Продуктивность	• Простои • Ухудшение психологического климата
Реагирование	• Расследование инцидента • PR-активность
Замена	• Замена оборудования • Повторный ввод информации
Штрафы	• Судебные издержки, досудебное урегулирование • Приостановление деятельности
Конкуренты	• Ноу-хау, государственная, коммерческая тайна • Отток клиентов, обгон со стороны конкурента
Репутация	• Гудвил • Снижение капитализации, курса акций

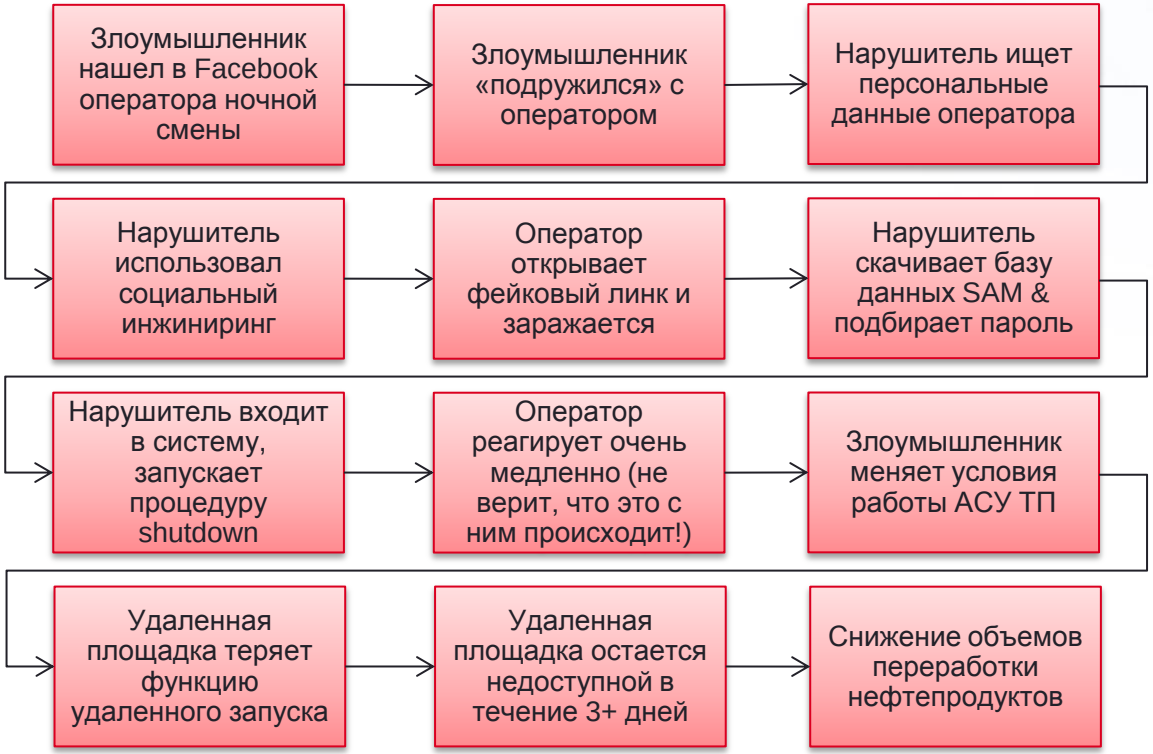
Совет №12

- Не усложняйте

Беспилотник

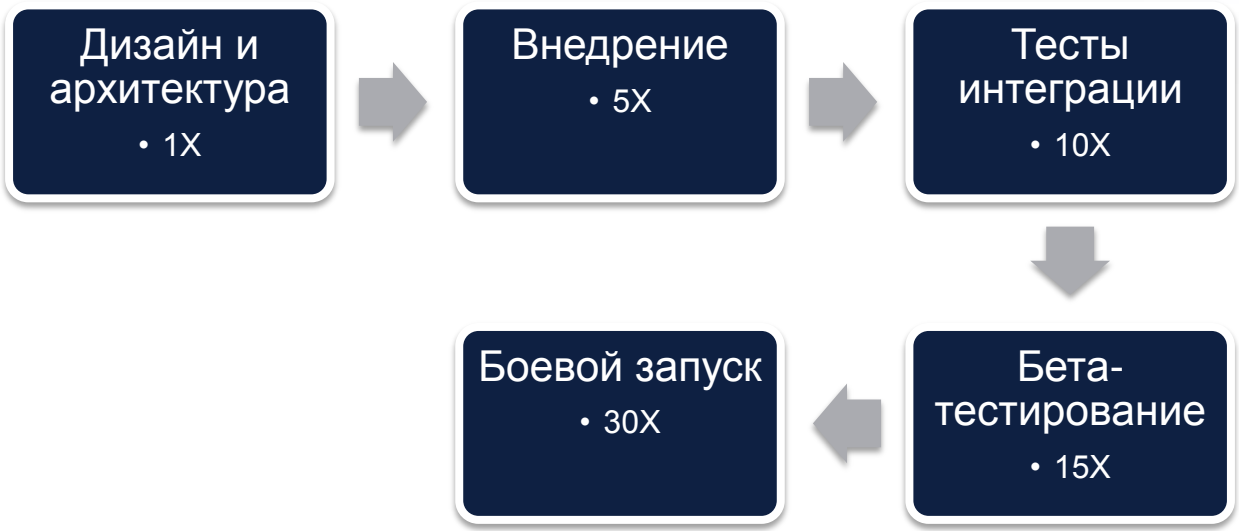
Что выгоднее при атаке объектов РВСН или системы управления войсками?

АСУ ТП


Злоумышленник нашел в Facebook оператора ночной смены
Злоумышленник «подружился» с оператором
Нарушитель ищет персональные данные оператора
Нарушитель использовал социальный инжиниринг
Оператор открывает фейковый линк и заражается
Нарушитель скачивает базу данных SAM & подбирает пароль
Нарушитель входит в систему, запускает процедуру shutdown
Оператор реагирует очень медленно (не верит, что это с ним происходит!)
Злоумышленник меняет условия работы АСУ ТП
Удаленная площадка теряет функцию удаленного запуска
Удаленная площадка остается недоступной в течение 3+ дней
Снижение объемов переработки нефтепродуктов

Совет №13

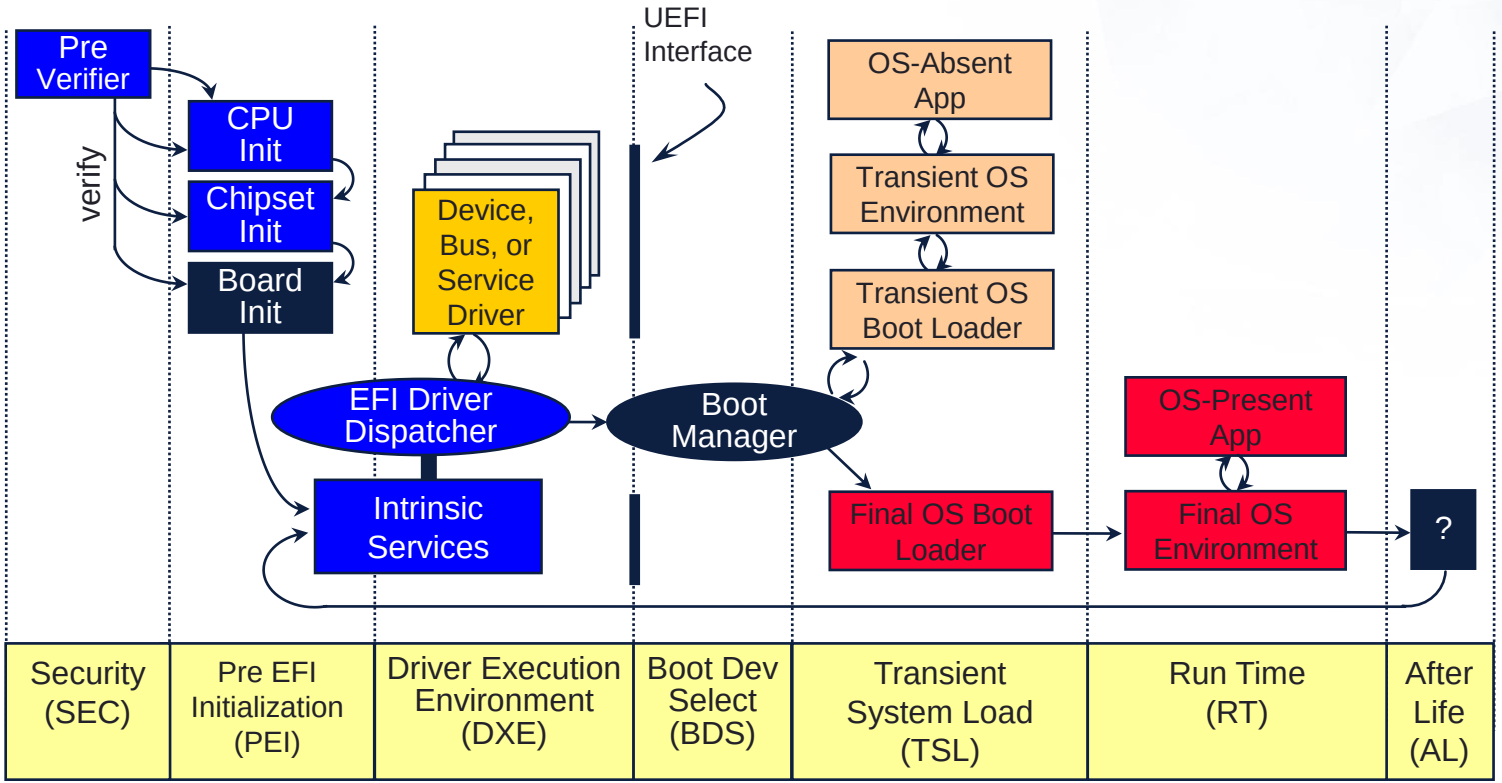
- Начинайте моделирование угроз, как можно раньше - чем позже осуществляется моделирование угроз, тем дороже обходится борьба с ними



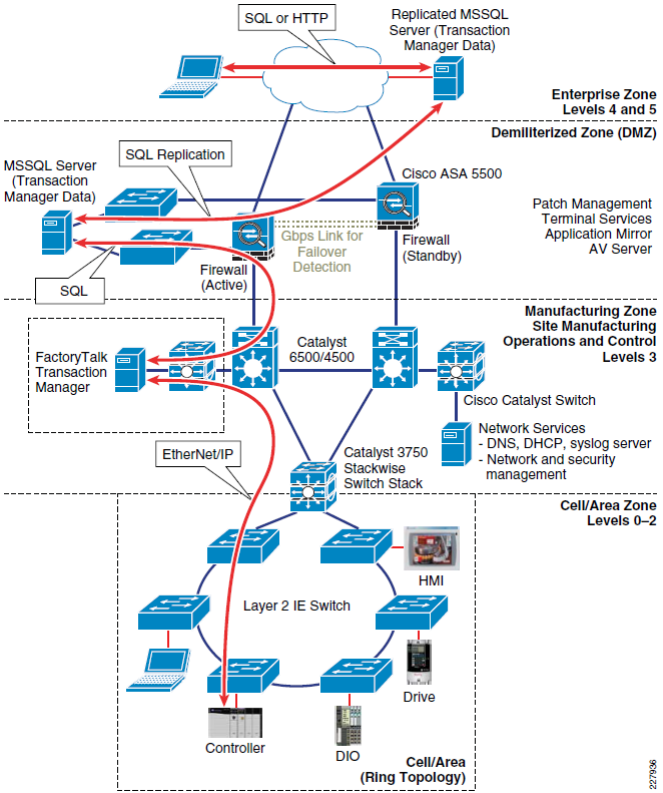
Совет №14

- Поймите информационные потоки между элементами объекта защиты и внешним миром

Процесс загрузки устройства (информационные потоки)



Потоки трафика в ДМЗ АСУ ТП



В данном примере данные АСУ ТП собираются и передаются в бизнес систему в Enterprise зоне

Данные не хранятся и не используются в зоне Manufacturing, таким образом отказ зоны DMZ не влияет на процесс производства

Данные АСУ ТП должны буфферизоваться на тот случай если не будет связи с DMZ

Совет №15

- Определите своего нарушителя – лицо, которое способно некорректно или несанкционированно использовать защищаемую систему
  - Сотрудник, хакер, ОПГ, спецслужбы, государства и т.п.

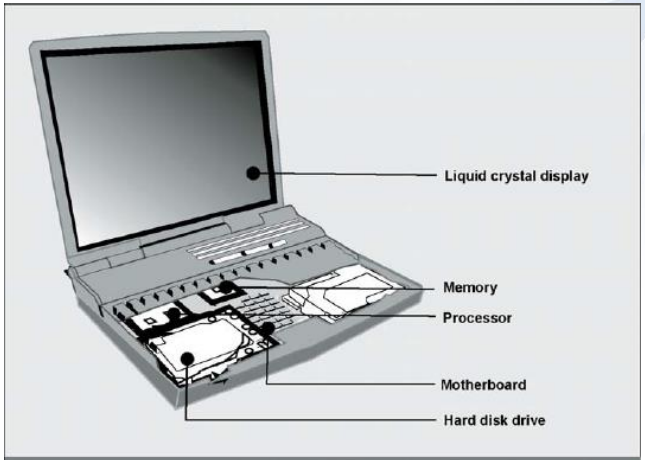
Нарушители для BIOS/UEFI

- 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

Новые угрозы: какова модель нарушителя?

- «Железо» и ПО содержит закладки
- Контрафактное ПО и «железо»
- Инсталляция ПО и «железа» с уязвимостями
- Stuxnet – флешка или закладка в оборудование?!



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

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		

Совет №16

- По возможности определите мотивацию и потенциал злоумышленника

Атаковать может каждый, но не каждый будет делать это

Доступ + **Экспертиза**

Возможность выполнения команд в АСУ ТП

Знакомство с АСУ ТП для реализации нужного эффекта

- Взлом системы
- Поиск инсайдера
- Кража учетной записи инсайдера
- Размещение ПО
- Размещение железа

Делает атаку **возможной**

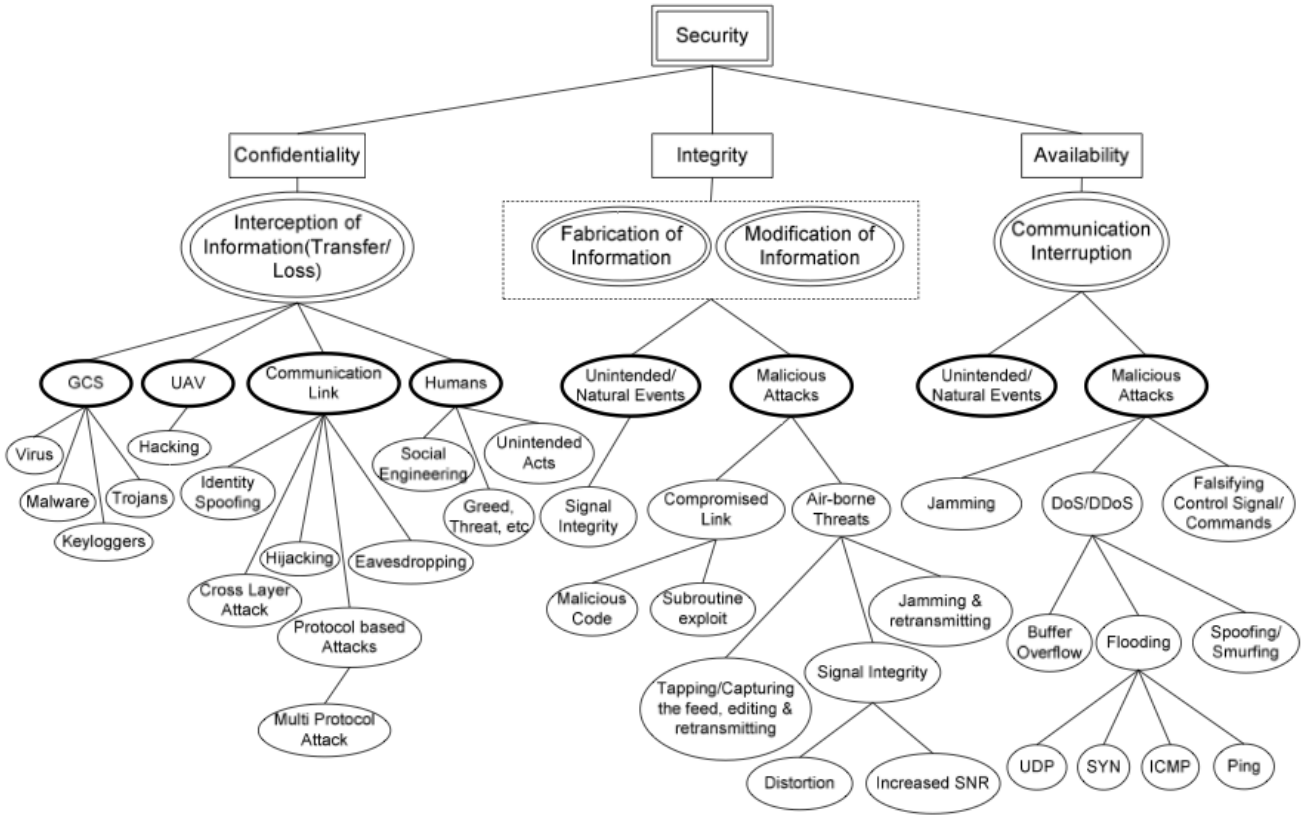
- Выбрать систему
- Выбор желаемого эффекта
- Эксперименты и практика
- Обойти контрмеры
- Остаться незаметным?

Делает атаку **успешной**

Совет №17

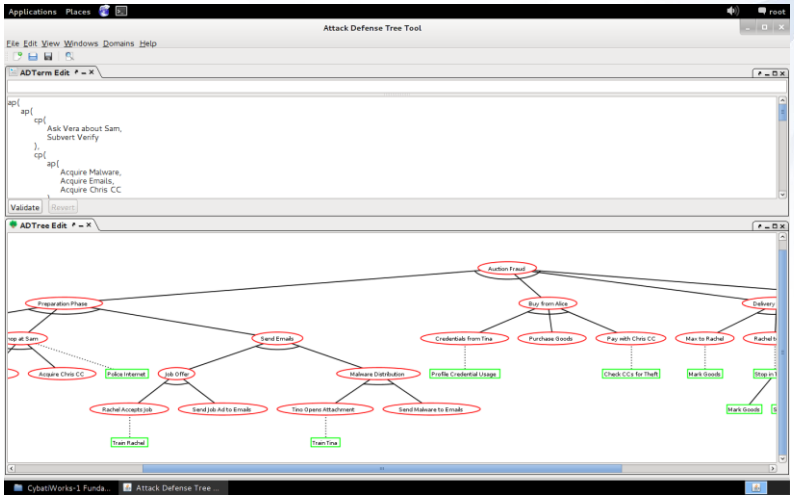
- Используйте деревья атак или библиотеки (банки данных) атак для перехода от высокоуровневых угроз (типов угроз) к низкоуровневым атакам

Беспилотник



ADTool

- Бесплатный инструмент на базе Java для моделирования угроз
  - Доступен для скачивания и в онлайн версии
- Позволяет создавать деревья атак и защитных мер



http://satoss.uni.lu/members/piotr/adtool/

Совет №18

- Автоматизируйте!

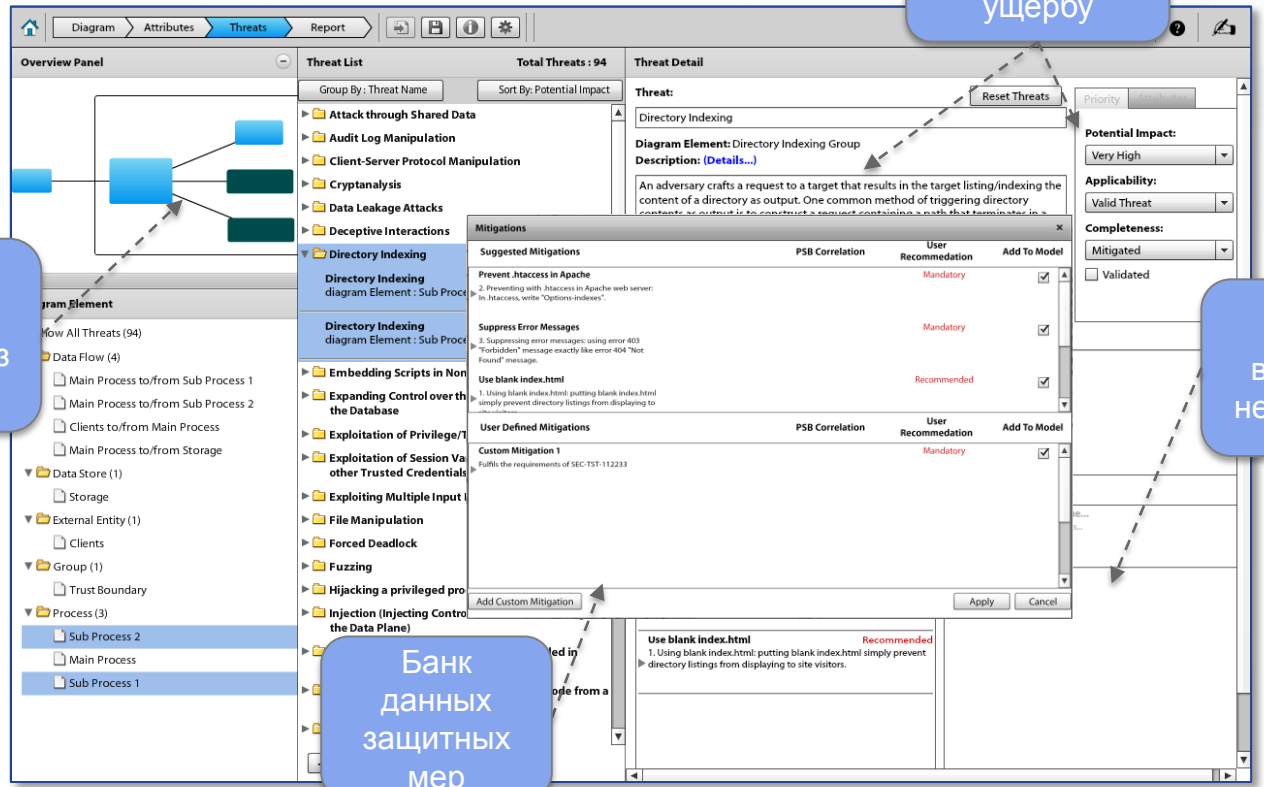
Cisco ThreatBuilder – средство автоматизации в рамках CSDL

Детали по угрозе и ущербу

Угрозы добавляются автоматически из банка данных

Проверка возможности нейтрализации

Банк данных защитных мер



В настоящее время нельзя говорить о правильном или неправильном методе анализа риска. Важно, чтобы организация пользовалась наиболее удобным и внушающем доверие методом, приносящим воспроизводимые результаты

Где вы можете узнать больше?

Пишите на security-request@cisco.com

Быть в курсе всех последних новостей вам помогут:

- http://www.facebook.com/CiscoRu
- http://twitter.com/CiscoRussia
- http://www.youtube.com/CiscoRussiaMedia
- http://www.flickr.com/photos/CiscoRussia
- http://vkontakte.ru/Cisco
- http://blogs.cisco.ru/
- http://habrahabr.ru/company/cisco
- http://linkedin.com/groups/Cisco-Russia-3798428
- http://slideshare.net/CiscoRu
- https://plus.google.com/106603907471961036146/posts
- http://www.cisco.ru/

Спасибо!

TOMORROW starts here.