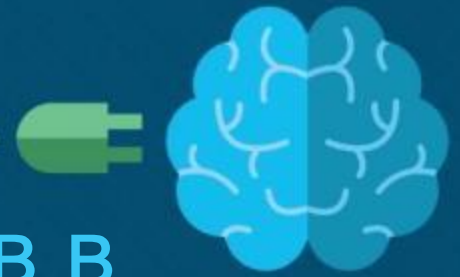
Лекція 6: Уразливість і оцінка ризиків в системі Інтернету речей

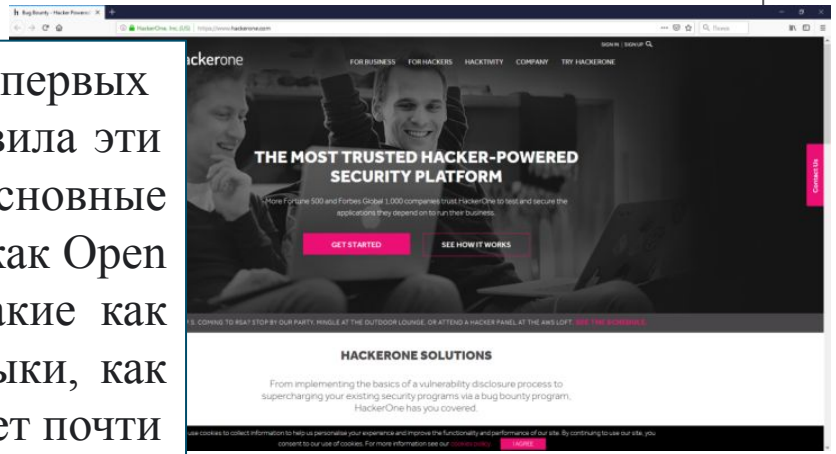


IoT Security 1.0 v2.0

Оценка уязвимости

Bug Bounty Hunters - талантливые этические хакеры, нанятые краудсорсинговыми службами безопасности для тестирования сетей своих клиентов. Компания имеет доступ к широкому спектру творческих хакерских талантов.

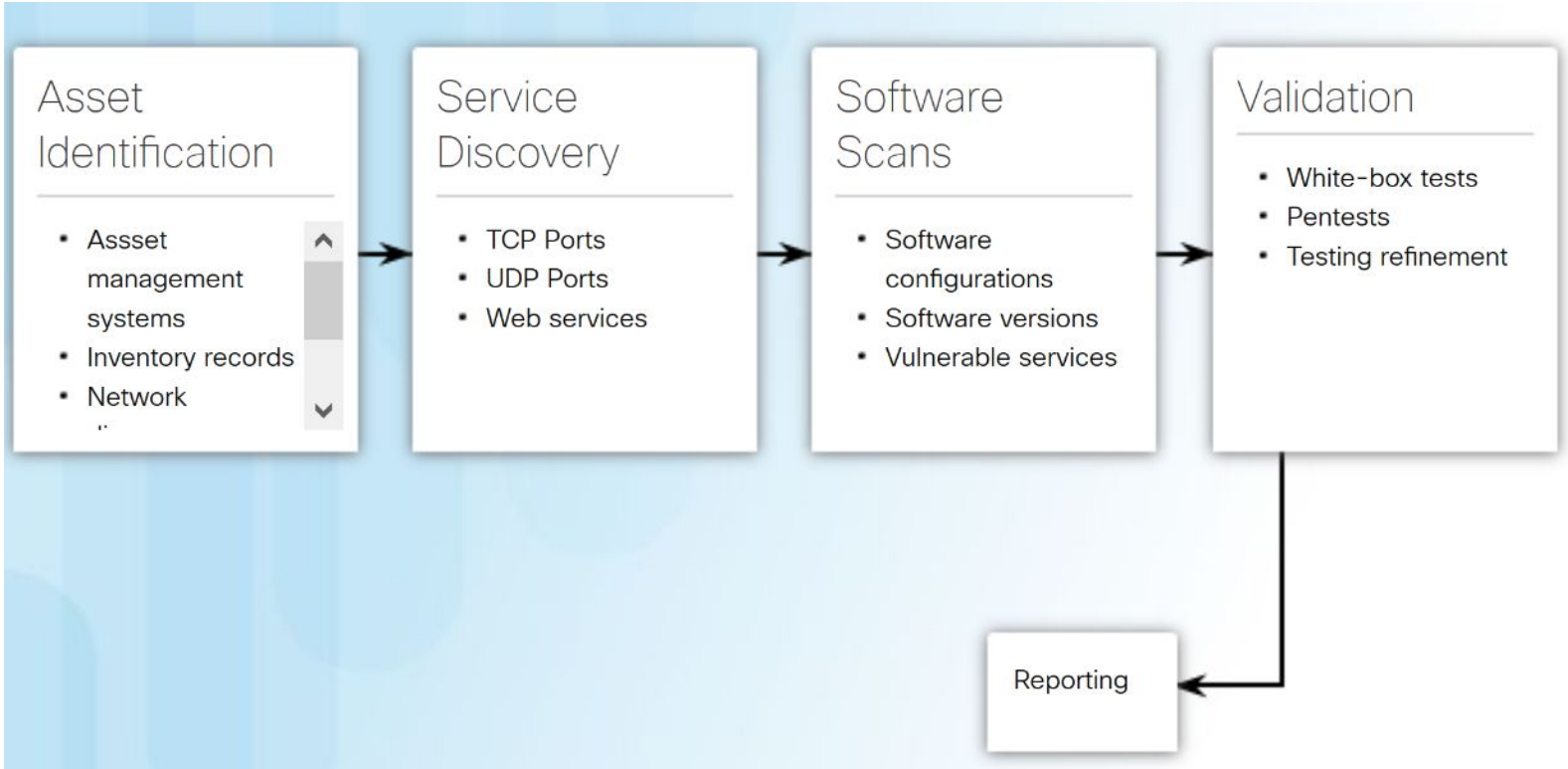
Hacker One - одна из первых компаний, которая предоставила эти услуги. Также тестирует основные интернет-технологии, такие как Open SSL, различные серверы, такие как Nginx и Apache, и такие языки, как PHP, Python и Perl. Привлекает почти 100 000 хакеров для обнаружения уязвимостей и выплатил миллионы долларов в виде вознаграждений за ошибки в Интернете



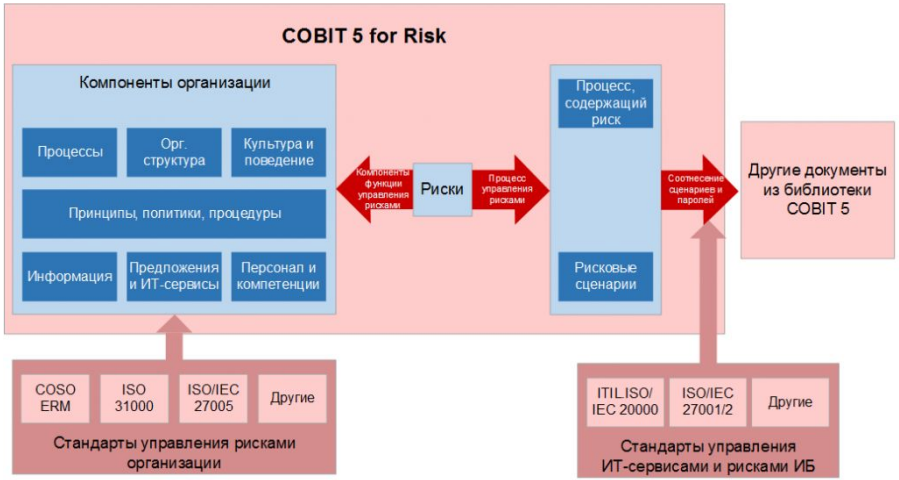
Оценка уязвимости

- Оценка уязвимости выявляет уязвимости, которые могут быть использованы злоумышленниками.
- Оценки уязвимости могут проводиться регулярно и регулярно или могут быть нацелены на определенные компоненты системы IoT.
- Оценка уязвимости часто выполняется с использованием готовых инструментов, например, в Kali Linux.

Оценка уязвимости
Процесс оценки уязвимости



Оценка уязвимости
Процесс оценки уязвимости



Методология COBIT for Risk разработана ассоциацией ISACA (Information Systems Audit and Control Association) в 2013 году и базируется на лучших практиках управления рисками (COSO ERM, ISO 31000, ISO\IEC 27xxx и др.).

Методология рассматривает риски информационной безопасности применительно к рискам основной деятельности организации, описывает подходы к реализации функции управления рисками информационной безопасности в организации и к процессам качественного анализа рисков информационной безопасности и управления ими.

Оценка уязвимости

При реализации функции и процесса управления рисками в организации методология выделяет следующие компоненты, влияющие как на риски информационной безопасности, так и на процесс управления ими:
Принципы, политики, процедуры организации;
Процессы;
Организационная структура;
Корпоративная культура, этика и правила поведения;
Информация;
ИТ-сервисы, ИТ-инфраструктура и приложения;
Люди, их опыт и компетенции.

Оценка уязвимости

Основным элементом анализа и управления рисками информационной безопасности в соответствии с методологией являются рисковые сценарии.

Каждый сценарий представляет собой «описание события, которое в случае возникновения, может привести к неопределенному (позитивному или негативному) воздействию на достижение целей организации».

Для каждого рискового сценария в методологии определена степень его принадлежности к каждому типу рисков:

Стратегические риски – риски, связанные с упущенными возможностями использования ИТ для развития и повышения эффективности основной деятельности организации;

Проектные риски – риски, связанные с влиянием ИТ на создание или развитие существующих процессов организации;

Риски управления ИТ и предоставления ИТ-сервисов – риски, связанные с обеспечением доступности, стабильности и предоставления пользователям ИТ-сервисов с необходимым уровнем качества, проблемы с которыми могут привести к ущербу для основной деятельности организации.

Оценка уязвимости

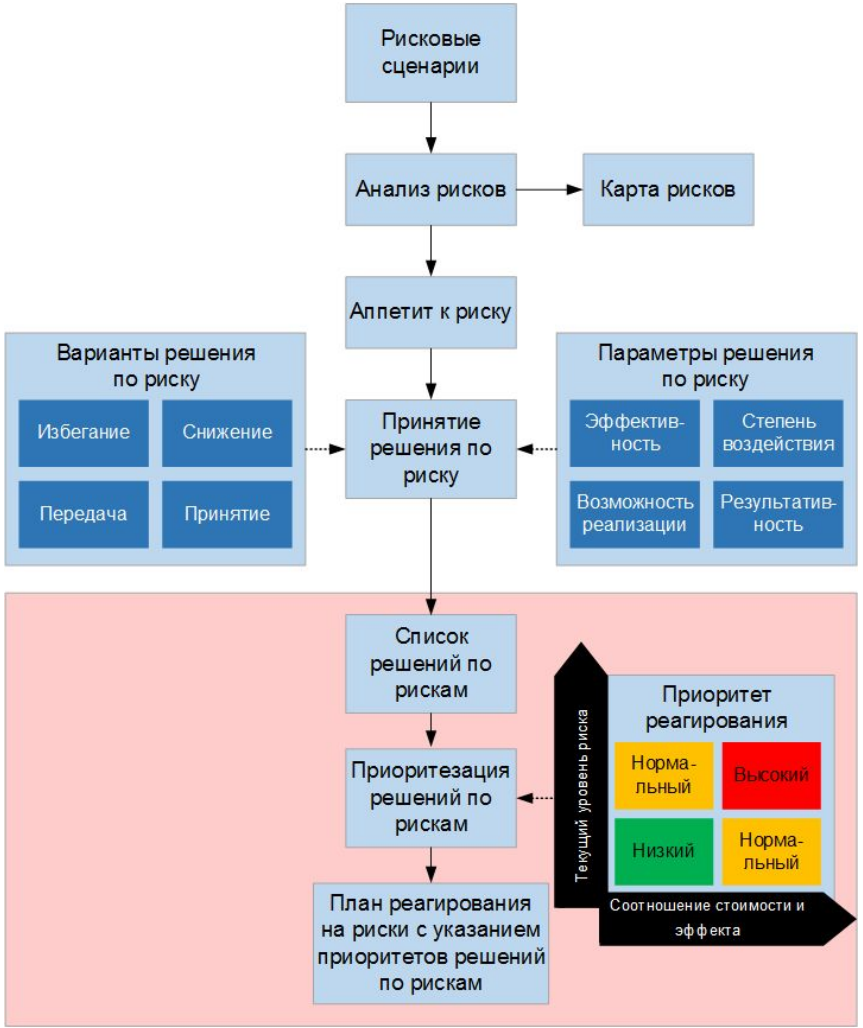
Каждый рисковый сценарий содержит следующую информацию:

- Тип источника угрозы - внутренний/внешний.
- Тип угрозы - злонамеренное действия, природное явление, ошибка и др.
- Описание события - доступ к информации, уничтожение, внесение изменений, раскрытие информации, кража и др.
- Типы активов (компонентов) организации, на которые влияет событие - люди, процессы, ИТ-инфраструктура и др.
- Время события.

Оценка уязвимости
Процесс оценки уязвимости

Дальнейшее управление рисками осуществляется путем анализа остаточного уровня рисков и принятия решения о необходимости реализации дополнительных мер снижения рисков.

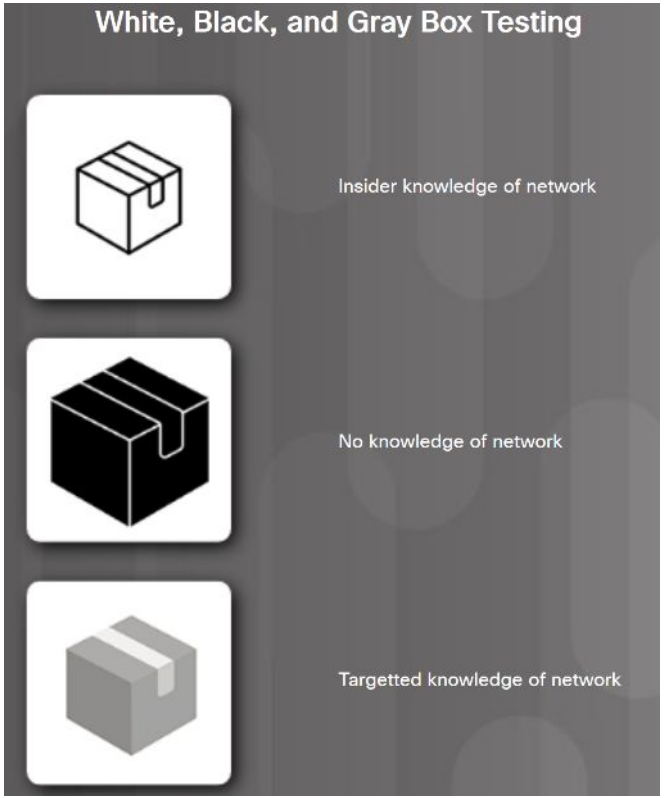
Методология содержит рекомендации по внедрению мер снижения рисков применительно к каждому из типов компонентов организации.



Оценка уязвимости
Типы оценки уязвимости

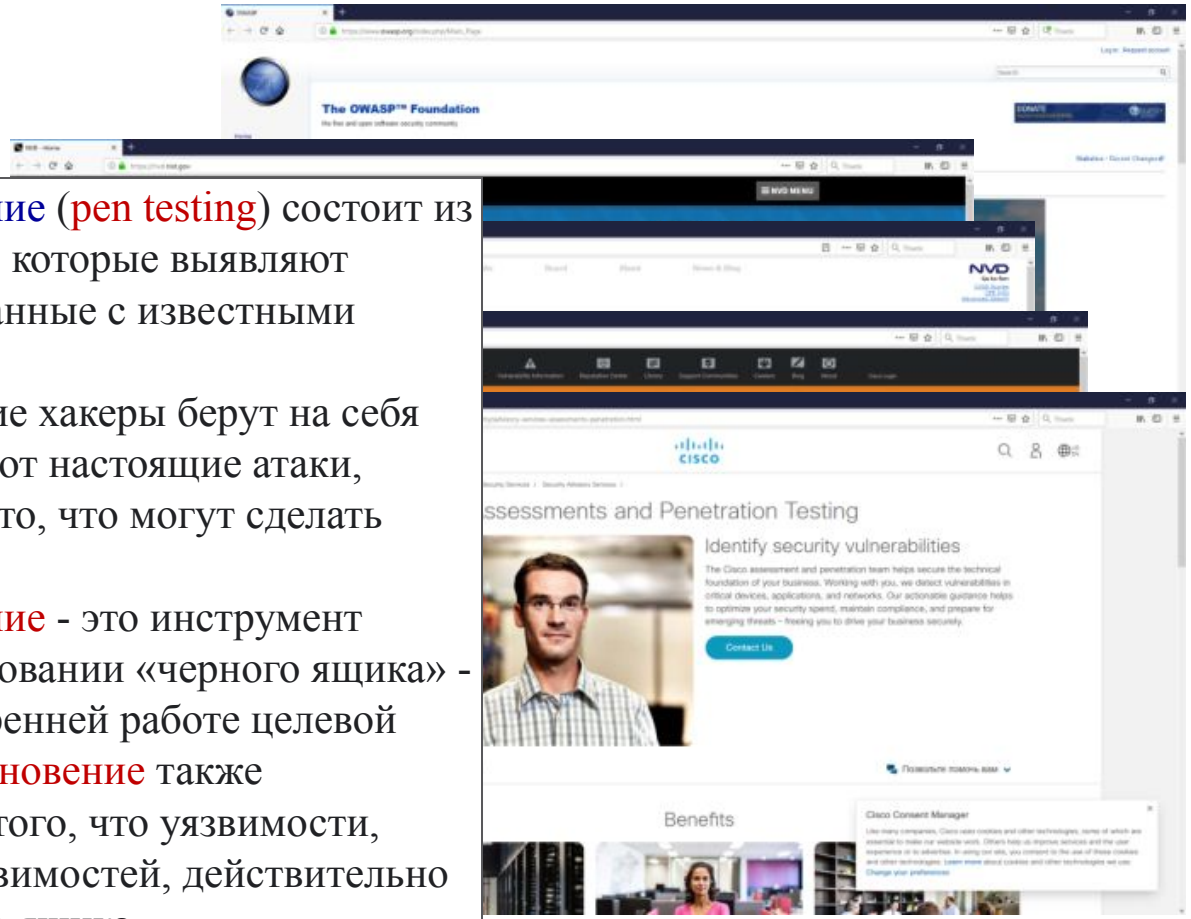
Оценку уязвимости можно разделить на три типа:

- Белый ящик - оценщики знакомы с сетевыми системами и часто работают внутри организации. Они часто сосредотачиваются на определенных аспектах системы.
- Черный ящик - эта оценка наиболее близка к реальной атаке. Оценщики, которые обычно работают с третьей стороной, не знают сетевой архитектуры.
- Серый ящик - тестировщик частично знаком с тестируемыми сетевыми системами, включая доступ к документации внутренней сетевой архитектуры. Цель состоит в том, чтобы проверить уязвимости, определить легкость их использования и определить потенциальное воздействие эксплойтов.



Оценка уязвимости
Типы оценки уязвимости

Оценка уязвимости
Тестирование на проникновение



Тестирование на проникновение (pen testing) состоит из реальных целенаправленных атак, которые выявляют потенциальные воздействия, связанные с известными уязвимостями.

Квалифицированные этические хакеры берут на себя роль злоумышленников и запускают настоящие атаки, которые призваны воспроизвести то, что могут сделать злоумышленники.

Тестирование на проникновение - это инструмент оценки, используемый при тестировании «черного ящика» - хакеры действуют, не зная о внутренней работе целевой системы. Тестирование на проникновение также используется для подтверждения того, что уязвимости, выявленные в других оценках уязвимостей, действительно существуют - тестирование серого ящика.

Пен-тесты используются для подтверждения эффективности мер, принятых для устранения уязвимости.

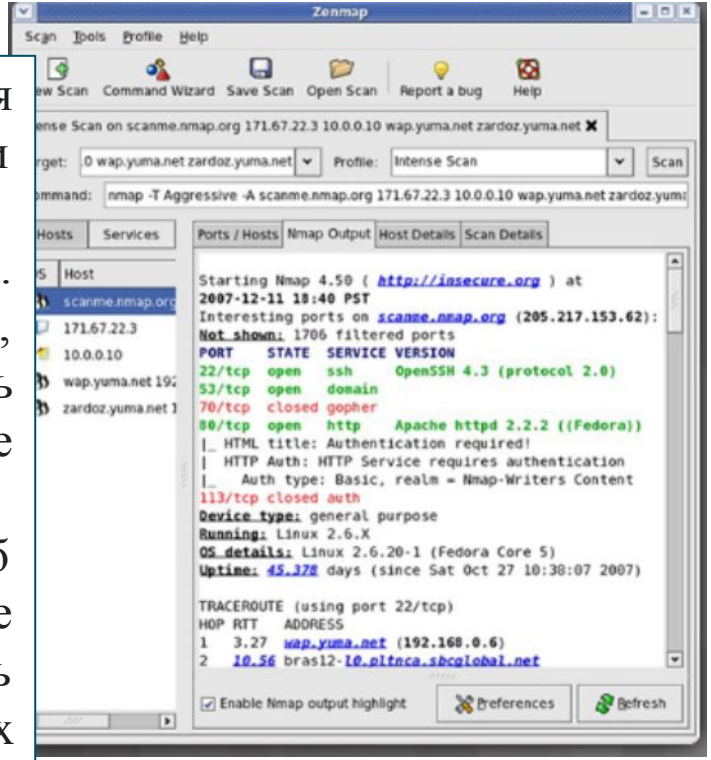
Оценка уязвимости
Инструменты отображения портов

Инструменты сопоставления портов используются для обнаружения открытых портов в конечных системах и сетевых устройствах.

Примеры: Nmap, Netcat или сканер портов SolarWinds.

Форма графического интерфейса пользователя Nmap, называемая Zenmap, может предоставить очень подробную информацию об одной системе или о ряде систем в сегменте сети.

Может обнаруживать хосты в сети. Могу сообщить об открытых портах. Может определять операционные системы, работающие на хостах. Может раскрывать подробности о службах, работающих на открытых портах, включая версии программного обеспечения, в процессе, известном как снятие отпечатков пальцев.



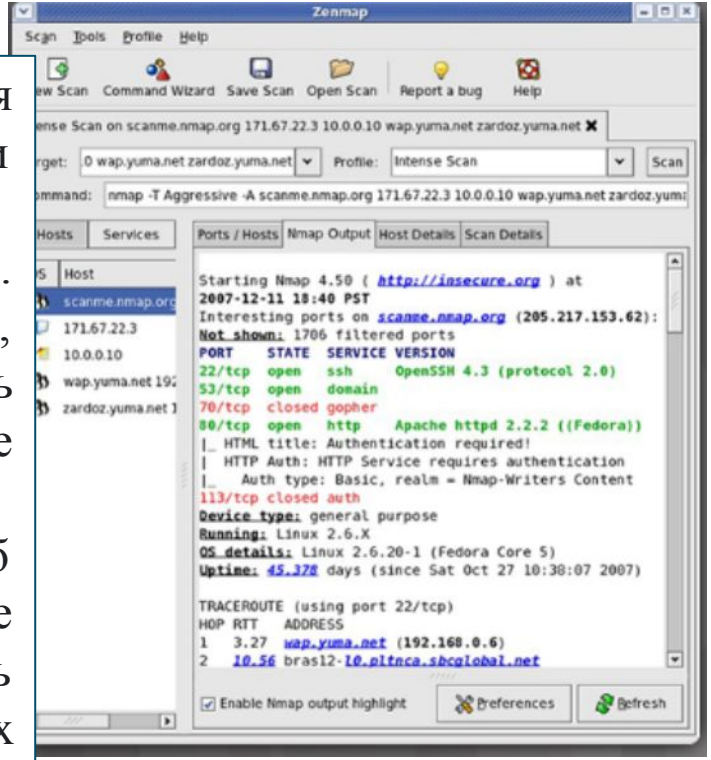
Оценка уязвимости
Инструменты отображения портов

Инструменты сопоставления портов используются для обнаружения открытых портов в конечных системах и сетевых устройствах.

Примеры: Nmap, Netcat или сканер портов SolarWinds.

Форма графического интерфейса пользователя Nmap, называемая Zenmap, может предоставить очень подробную информацию об одной системе или о ряде систем в сегменте сети.

Может обнаруживать хосты в сети. Могу сообщить об открытых портах. Может определять операционные системы, работающие на хостах. Может раскрывать подробности о службах, работающих на открытых портах, включая версии программного обеспечения, в процессе, известном как снятие отпечатков пальцев.



Оценка уязвимости
Инструменты защиты паролей

Слабые пароли на порталах приложений Интернета вещей вызывают беспокойство.

Несколько распространенных методов атаки на пароли, которые можно использовать для оценки безопасности паролей:

Грубая сила - эта атака является очень трудоемким, неэффективным, автоматизированным средством проверки всех возможных комбинаций букв, цифр и символов для проверки входа в систему.

Атака по словарю - эта атака использует списки слов, которые могут использоваться в качестве паролей.

Анализ и взлом паролей - анализаторы протокола могут использоваться для перехвата аутентификационного трафика, содержащего хешированные пароли.

Хешированные пароли также могут быть обнаружены в файловых системах устройств Интернета вещей. Такие инструменты, как John the Ripper и Aircrack-NG, могут использоваться для попытки взломать хэш-шифрование.

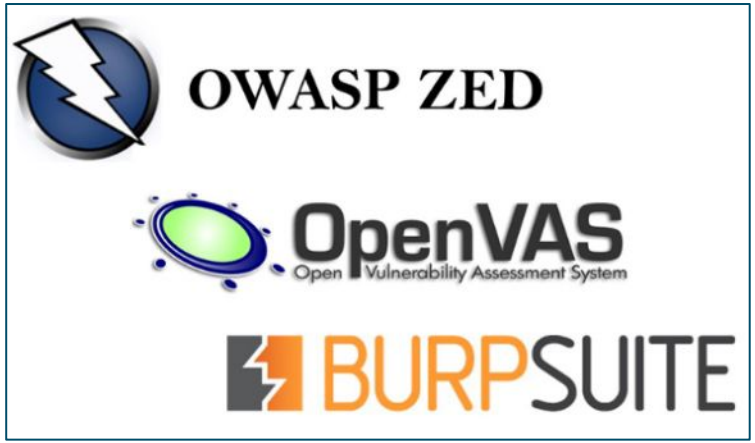
Оценка уязвимости
Инструменты защиты паролей

Безопасность имени пользователя имеет важное значение - блокировка учетной записи может быть злонамеренным отказом в обслуживании, при котором злоумышленники намеренно пытаются заблокировать законных пользователей.

Необходимо рассмотреть расширенные подходы к аутентификации в системах IoT, когда существует высокий риск нанесения ущерба или физического вреда людям, например, в промышленных системах управления Интернетом (IICS). Национальный институт стандартов и технологий США (NIST) разработал руководящие принципы для цифровых удостоверений.

Альянс FIDO (Fast IDentity Online), показанный на рисунке, разработал новые технологии и стандарты аутентификации для IoT.

Инструменты для работы с уязвимостями веб-приложений



Инструменты для работы с уязвимостями веб-приложений

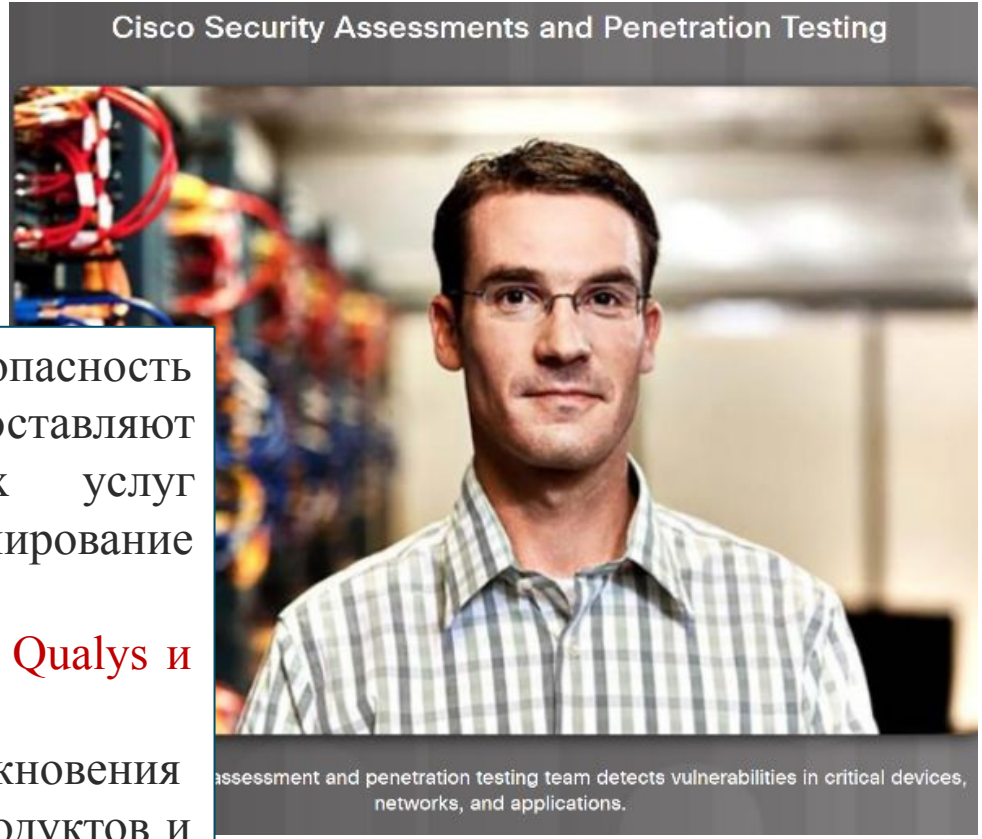
В дополнение к инструментам из пакета Kali, которые использовались в этом курсе, некоторые другие известные инструменты:

OWASP ZAP - Open Web Application Security Project (OWASP) - это основной справочник по уязвимостям веб-приложений. OWASP ZED Attack Proxy (OWASP ZAP) - это бесплатный инструмент оценки уязвимостей с открытым исходным кодом, используемый для тестирования «черным ящиком».

OpenVAS - платформа OpenVas объединяет ряд инструментов сканирования уязвимостей в единое приложение, которое включает в себя хранение данных об уязвимостях, планирование сканирования и создание отчетов.

Burp Suite - это комплексная группа инструментов для тестирования уязвимостей веб-приложений, которые могут определить наличие 10 основных уязвимостей OWASP. Он включает в себя сканер, настраиваемый автоматический инструмент атаки и веб-сканер, который может отображать файловую систему веб-приложения.

Услуги по оценке уязвимости



Компании, обеспечивающие безопасность как услугу (SECaaS), предоставляют широкий спектр управляемых услуг безопасности, включая сканирование уязвимостей.

Эти услуги предлагают Alienvault, Qualys и Mandiant.

Cisco предлагает оценку проникновения сети как часть своего портфеля продуктов и услуг в области безопасности.

Источники информации об уязвимостях

Ряд источников информации об угрозах усердно работают над обнаружением, исследованием и распространением информации об угрозах по мере их обнаружения.

Cisco Talos Intelligence Group - одна из крупнейших в мире групп коммерческого анализа угроз.

Talos защищает клиентов Cisco от известных и возникающих угроз.

Национальная база данных уязвимостей (NVD) NIST расширяет общие уязвимости и подверженности (CVE) дополнительным анализом, базой данных и детализированной поисковой системой.

Поставщики оборудования и программного обеспечения должны информировать клиентов и общественность об уязвимостях в своих продуктах и предоставлять исправления.

Оценка рисков Интернета вещей

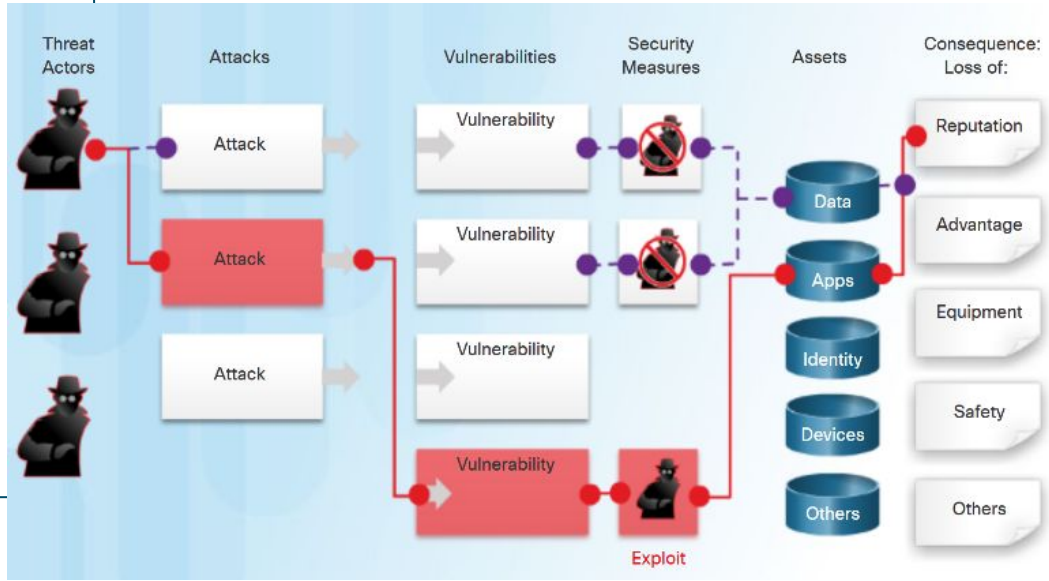
Большинство подходов к безопасности OT касаются безопасности людей и оборудования. OT-коммуникация часто представляет собой M2M с людьми, которые контролируют и контролируют промышленные, энергетические, экологические или интеллектуальные городские системы, среди прочего. IoT создает новый набор угроз безопасности из-за огромной поверхности атаки IoT.

Примером может служить компрометация критически важных компонентов промышленной инфраструктуры, которые теперь подключены к Интернету.

Инструменты для работы с уязвимостями веб-приложений

Для определения риска в первую очередь необходимо ответить на следующие вопросы в рамках оценки риска:

Кто те угрозы, которые хотят напасть на нас?
Какие уязвимости могут использовать злоумышленники?
Как удачные атаки повлияют на организацию?
Какова вероятность возникновения разных атак?
Что может сделать организация для устранения риска?



Общая система оценки уязвимостей (Common Vulnerability Scoring System)

CVSS - это оценка риска, предназначенная для выявления общих атрибутов и серьезности уязвимостей в компьютерном оборудовании и программных системах.

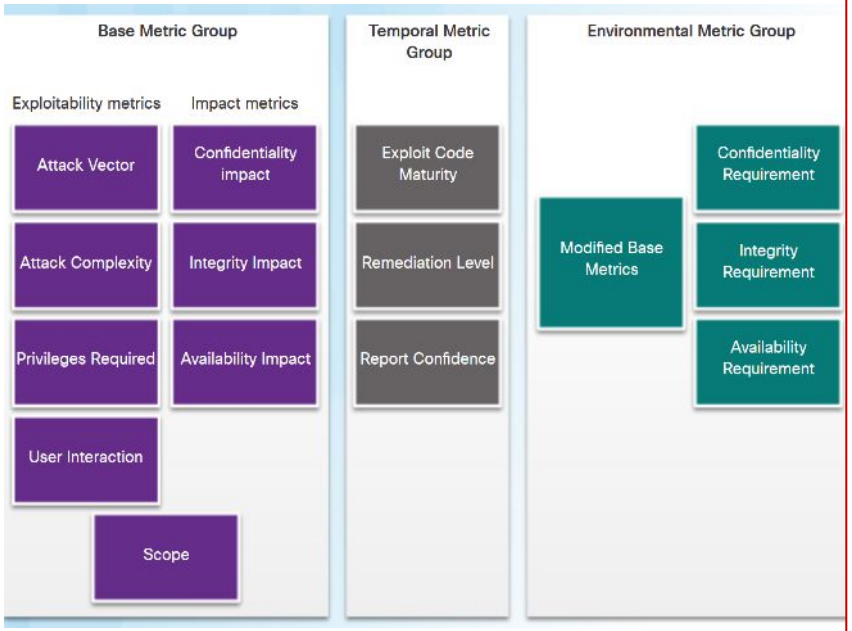
CVSS 3.0 - это не зависящий от производителя, отраслевой стандарт, открытый фреймворк для взвешивания рисков уязвимости с использованием различных показателей.

Эти веса в совокупности дают оценку риска, присущего уязвимости.

Числовая оценка может использоваться для определения срочности уязвимости и приоритета ее устранения.

Не включает показатели безопасности, потому что он был разработан для ИТ-безопасности. Будущие системы оценки должны включать дополнительные метрики, специфичные для реализаций IoT.

Группы показателей CVSS



Инструмент CVSS требует, чтобы оценщик выбрал значения в трех группах показателей для каждой выявленной уязвимости. На рисунке показаны три группы показателей и отдельные показатели, составляющие каждую группу.

Базовая группа показателей - представляет характеристики уязвимости, которые являются постоянными во времени и в разных контекстах.

Возможность использования - это особенности эксплойта, такие как вектор, сложность и взаимодействие с пользователем, необходимые для эксплойта.

Показатели воздействия. Воздействие эксплойта основано на триаде ЦРУ: конфиденциальность, целостность и доступность.

Temporal Metric Group - измеряет характеристики уязвимости, которые могут изменяться со временем, но не в разных пользовательских средах.

Environmental Metric Group - измеряет аспекты уязвимости, которые коренятся в среде конкретной организации.

Базовая метрическая группа CVSS

Метрики использования базовой группы метрик включают:

Вектор атаки - отражает близость к злоумышленнику.

Сложность атаки - выражает количество компонентов, программного обеспечения, оборудования или сетей, которые находятся вне контроля злоумышленника и которые должны присутствовать.

Требуемые привилегии - фиксирует необходимый уровень доступа.

Взаимодействие с пользователем - выражает наличие или отсутствие требования к взаимодействию с пользователем.

Объем - указывает, должны ли быть задействованы несколько органов.

Метрики воздействия базовой группы метрик включают:

Влияние на конфиденциальность - измеряет влияние на конфиденциальность из-за успешно использованной уязвимости.

Влияние на целостность - измеряет влияние на целостность из-за успешно использованной уязвимости.

Влияние на доступность - измеряет влияние на доступность из-за успешно использованной уязвимости.

Процесс CVSS

CVSS Base Metrics Group - это способ оценки уязвимостей безопасности, обнаруженных в программных и аппаратных системах.

Он описывает серьезность уязвимости на основе характеристик успешного использования уязвимости.

Другие группы показателей изменяют базовую оценку серьезности, учитывая влияние времени и факторов окружающей среды на базовую оценку серьезности.

В процессе CVSS используется инструмент под названием Калькулятор CVSS v3.0.

Калькулятор похож на анкету, в которой выбираются варианты, описывающие уязвимость для каждой группы показателей, а затем генерируется оценка.

- В дополнение к числовому рейтингу серьезности также создается векторная строка, которая суммирует сделанный выбор.
- Затем значения метрики Temporal и Environment изменяют результаты базовой метрики, чтобы получить общую оценку.

Углубленное моделирование угроз

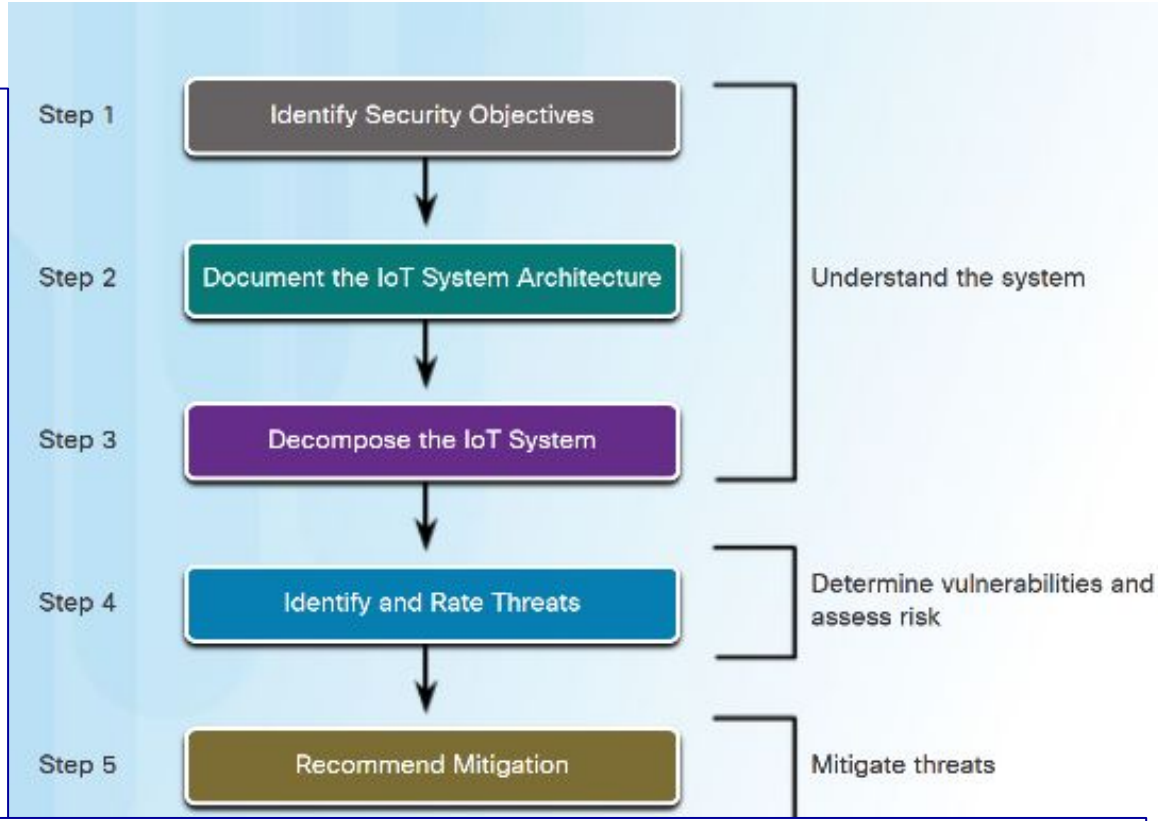
Моделирование угроз - это проактивный подход к оценке безопасности систем и программного обеспечения. Моделирование угроз лучше всего применять на протяжении всего процесса разработки.

Три подхода к моделированию угроз:

Атакующий - с точки зрения злоумышленника.

Ориентация на защиту - анализирует архитектуру системы для выявления угроз различным элементам. Используется в этом классе.

Ориентация на активы - фокусируется на классификации активов и присвоении им стоимости.



Процесс моделирования угроз начинается с понимания системы и ответов на следующие вопросы:
Что мы моделируем? Каковы потенциальные угрозы?
Какие риски? Что можно сделать для устранения рисков?

Цели безопасности системы

Первый шаг - определить цели безопасности для системы, исходя из ее назначения и работы.

Важно понимать, какие типы данных обрабатываются системой, а также последствия кражи или уничтожения данных.

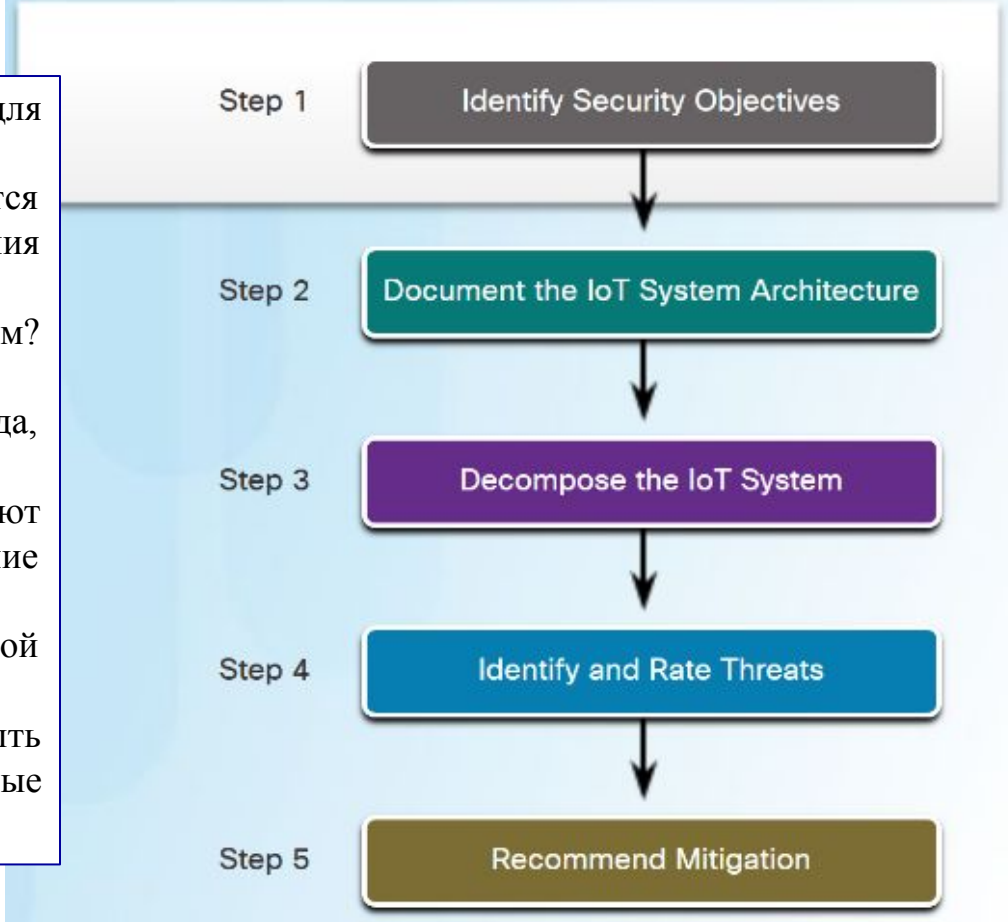
Приведет ли потеря данных к финансовым потерям? Если да, то в какой степени?

Будет ли нанесен ущерб репутации компании? Если да, то каковы будут последствия для бизнеса?

Правительства и другие организации принимают правила, регулирующие сбор, передачу и хранение данных.

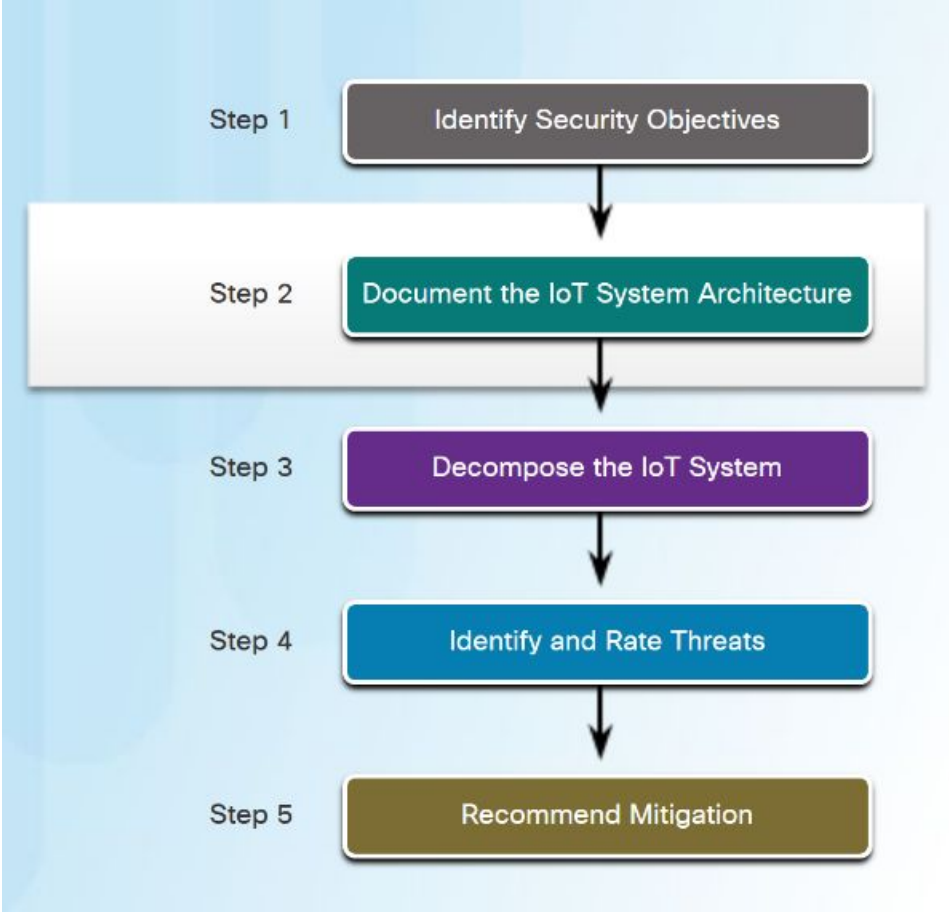
Нарушение этих правил может повлечь за собой серьезные финансовые и юридические штрафы.

Критические системы инфраструктуры должны быть всегда доступны, сбои могут иметь серьезные последствия.



Потоки данных

После того, как цели безопасности определены, функции архитектуры системы должны быть представлены в виде схемы.
Диаграммы потоков данных **Data flow diagrams** (DFD) чрезвычайно полезны для визуализации системы IoT.
DFD отображают пути, по которым данные будут проходить между различными функциональными компонентами системы, включая точки входа в систему, а также устройства и людей, использующих эти точки входа.



Компоненты диаграмм потоков данных

Компоненты, входящие в систему IoT DFD:

IoT устройства:

Шлюзы IoT - позволяют передавать данные датчиков по IP-сети.

Местные приложения:

Пограничные устройства - разрешите отправку внутреннего IP-трафика между местоположениями и Интернетом или облаком.

Приложения данных

Хранилище данных:

Управляющие приложения - обрабатывают данные для принятия решений, вводящих в действие контроль.

Мобильные приложения

DFD используют 4 символа для обозначения этих устройств.

Data Flow Diagram Symbols

Type	Description	Gane and Sarson	Yourdon and Coad
External Entity	Users, contractors, and partners outside of the control of the system that send or receive data		
Process	Data output from sensing, actuating, traffic forwarding, analysis, control systems		
Data Store	Data at rest in local, fog, cloud, or data center storage		
Data Flow	Single headed arrows indicated uni-directional data flow; Double headed arrows indicate bi-directional data flow		

Субъекты DFD должны соответствовать основным правилам:

Любой процесс должен иметь как минимум один вход и один выход.

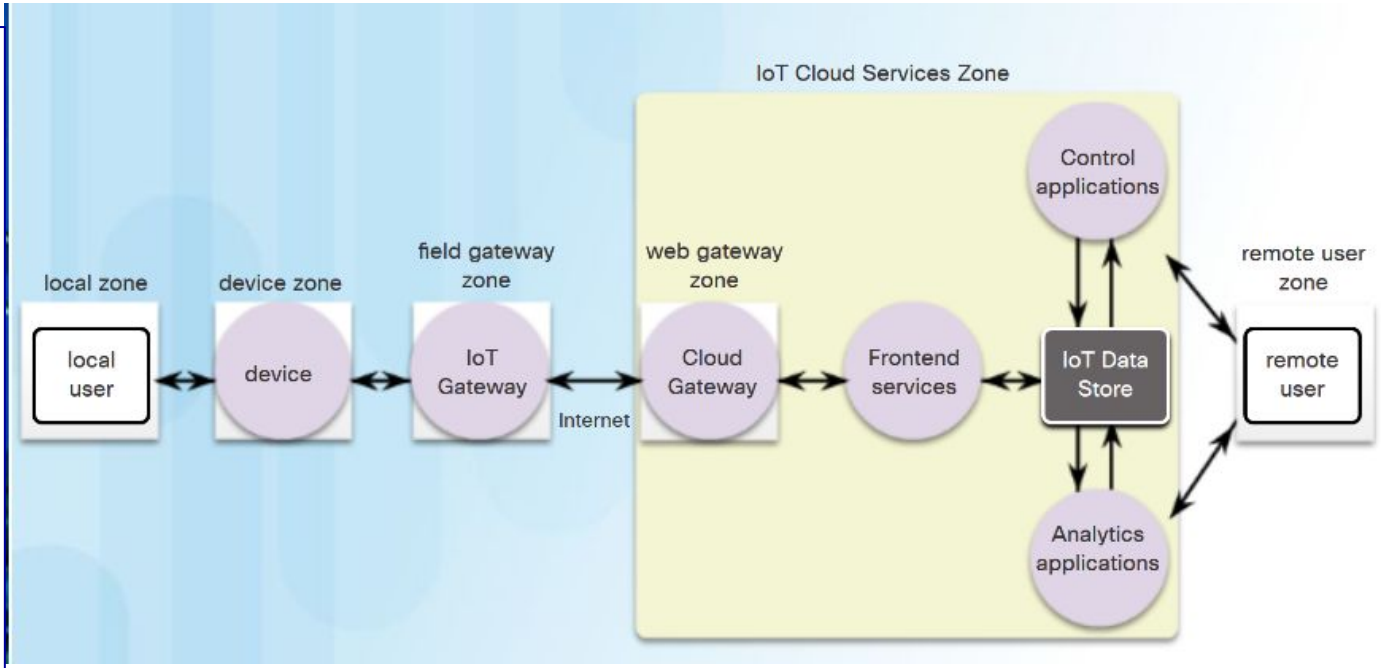
Хранилища данных должны иметь потоки для доступа для записи и чтения.

Данные, хранящиеся в системе, должны пройти хотя бы один процесс.

Зоны системы

Зоны можно определить как области системы, требующие различной авторизации и аутентификации.

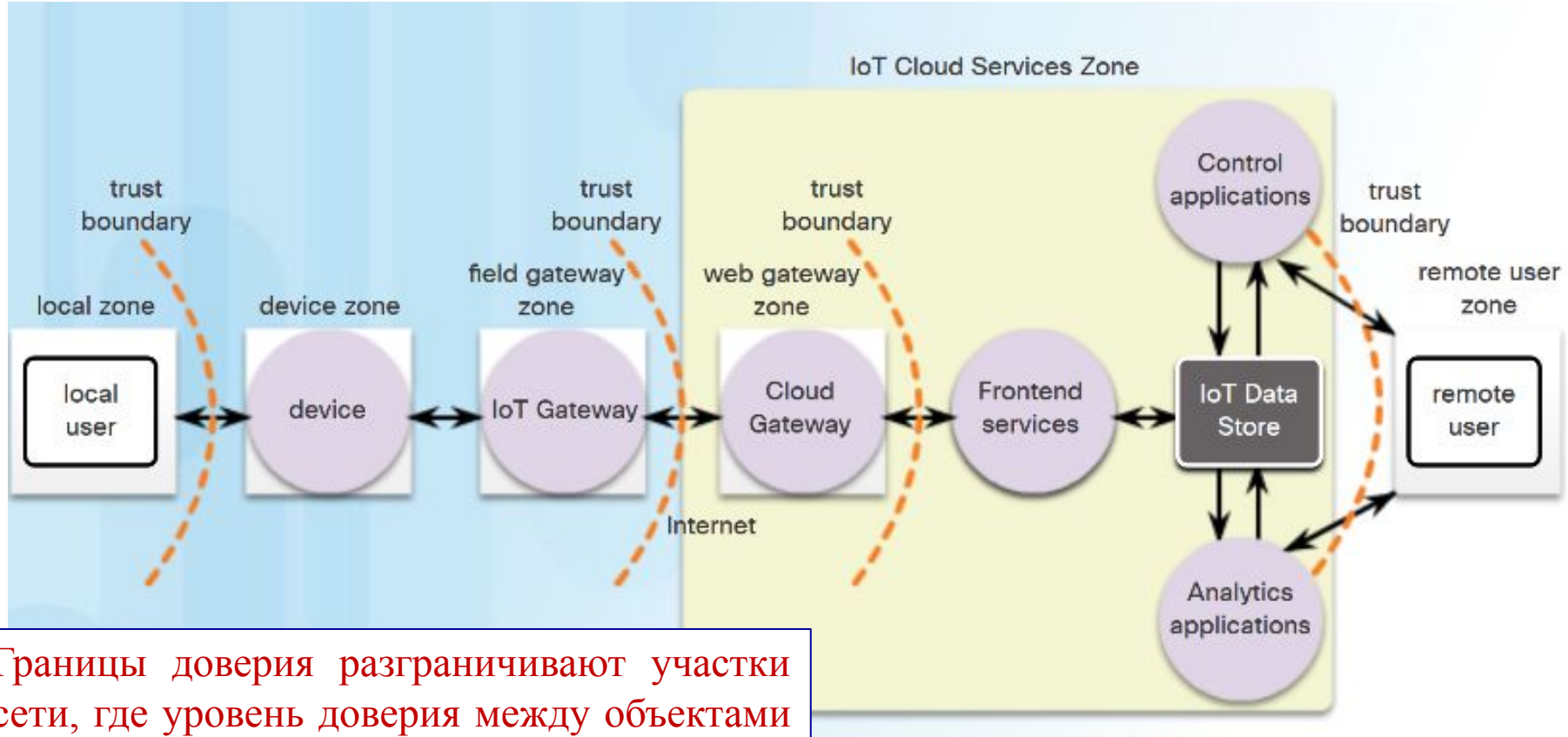
Зоны также помогают ограничить подверженность различных частей системы уязвимостям, связанным с каждой зоной.



Примерами зон могут быть сенсорная зона сети, веб-приложения, IP-шлюз, граница сети и т. Д.

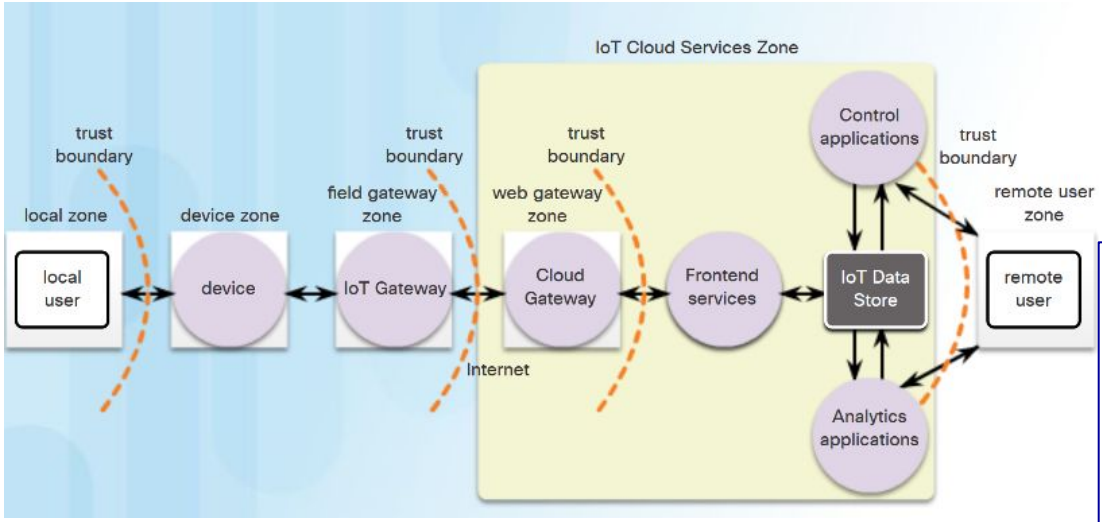
Зоны могут быть вложенными, если компоненты расположены внутри другой организации.

Определите границы доверия



Границы доверия разграничивают участки сети, где уровень доверия между объектами на обоих концах потока различен.

Определите границы доверия



Например, данные, передаваемые из шлюза Интернета вещей в облачный шлюз, пересекают границу доверия.

Разрешения для шлюза IoT отличаются от разрешений для облачного шлюза, который доступен в Интернете и доступен для многих пользователей.

Трафик данных, который пересекает эту границу, должен быть авторизован и аутентифицирован на входящем устройстве.

STRIDE

STRIDE Threat Classifications

Threat Classification	Definition	Example Threats
Spoofing	Impersonating a legitimate user or device	• Pretending to be a valid user or device • Pretending to be another server • Laptop impersonates IoT gateway to perform man in the middle data interception
Tampering	Modifying data, code, or device	• Modifying sensor data • Physical device hacking
Repudiation	Disabling ability to prove or disprove events	• Corrupt or destroy log files • Alter data record timestamps
Information Disclosure	Making privileged information available to unauthorized parties	• Gathering sensitive information from log files • Using SQL injection to steal personal data from web application
Denial of Service	Cause device to be unavailable to perform legitimate functions due to illegitimate traffic, data, or software	• Crashing a web site • Sending data absorbing CPU cycle, storage, or device power resources
Elevation of Privilege	Obtaining higher privileges than would normally be authorized	• Allowing remote user to run commands, switch from a limited user to admin • Using intercepted credentials to logon to data dashboard

STRIDE

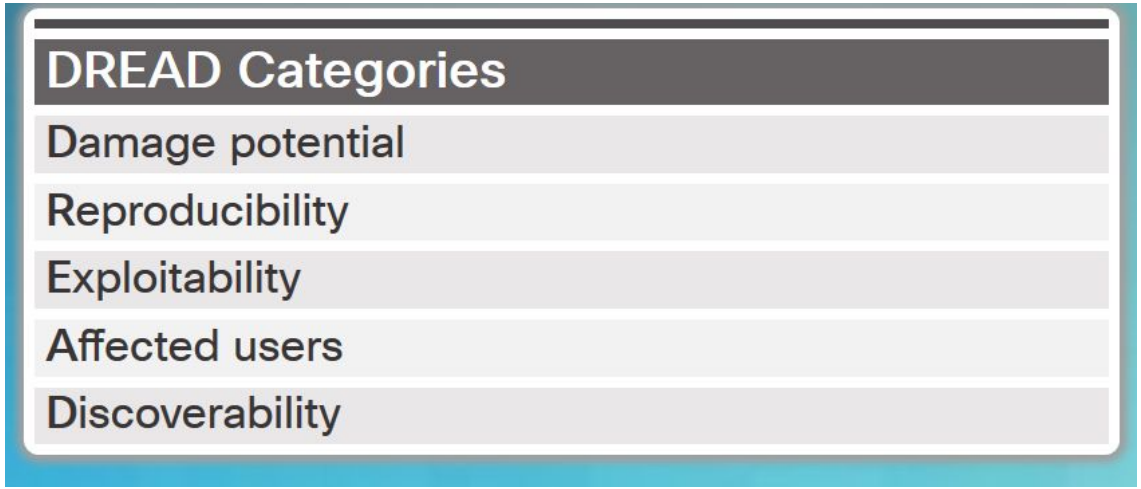
Подход STRIDE предоставляет набор категорий, которые очень полезны для выявления потенциальных угроз в системах Интернета вещей.

STRIDE - это аббревиатура от Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service и Elevation of Privatge.

STRIDE предоставляет схему классификации для идентификации угроз для каждого элемента DFD.

Понимание того, какие уязвимости относятся к каким элементам системы, поможет сэкономить время в процессе моделирования угроз.

Оценка рисков с помощью DREAD



- Каждая угроза, идентифицированная STRIDE, теперь должна быть оценена на предмет степени риска для организации.
- Модель DREAD дает количественную оценку риска.
- Этот балл можно использовать с оценками стоимости риска для оценки желательности и осуществимости снижения угрозы.

Модель оценки угроз DREAD

	Category	High (3)	Medium (2)	Low (1)
D	Damage potential	System down or under threat actor control; damage to people or facilities.	Loss of important data; some temporary system compromise or loss of availability.	Minor to medium loss of data or system impact.
R	Reproducibility	Every attempt will be successful.	Estimated to work half the time.	Difficult to reproduce, exploit requires special conditions.
E	Exploitability	Easily carried out by inexperienced threat actor.	Requires skilled attacker.	Requires very skilled attacker or attacking organization.
A	Affected users (or devices)	Enough devices to cause serious outages. All users who are up to standard.	Some devices that are not patched or in up to current standard.	Few users or devices under edge case configurations or roles.
D	Discoverability	Widely known in the attacker community. High value to attackers.	Little known and not widely present, some benefit to threat actors.	Little known and of little interest.

Модель оценки угроз DREAD

	Category	High (3)	Medium (2)	Low (1)
D	Damage potential	System down or under threat actor control; damage to people or facilities.	Loss of important data; some temporary system compromise or loss of availability.	Minor to medium loss of data or system impact.
R	Reproducibility	Every attempt will be successful.	Estimated to work half the time.	Difficult to reproduce, exploit requires special conditions.
E	Exploitability	Easily carried out by inexperienced threat	Requires skilled attacker.	Requires very skilled attacker or attacking organization.
			devices that are not d or in up to t standard.	Few users or devices under edge case configurations or roles.
			nown and not present, some to threat actors.	Little known and of little interest.

Для применения этих моделей к системам Интернета вещей могут потребоваться небольшие модификации, поскольку они были разработаны для программных систем.

Каждая уязвимость, идентифицированная STRIDE, оценивается по пяти категориям DREAD. Значения рейтинга:

3 = высокий

2 = средний

1 = низкий

На рисунке показано значение показателей для каждой категории. Эти значения относятся к организации и системе, на которые влияет уязвимость.

Рекомендации по смягчению последствий

Безопасная разработка и развертывание IoT-систем - наиболее эффективный способ снизить риски.

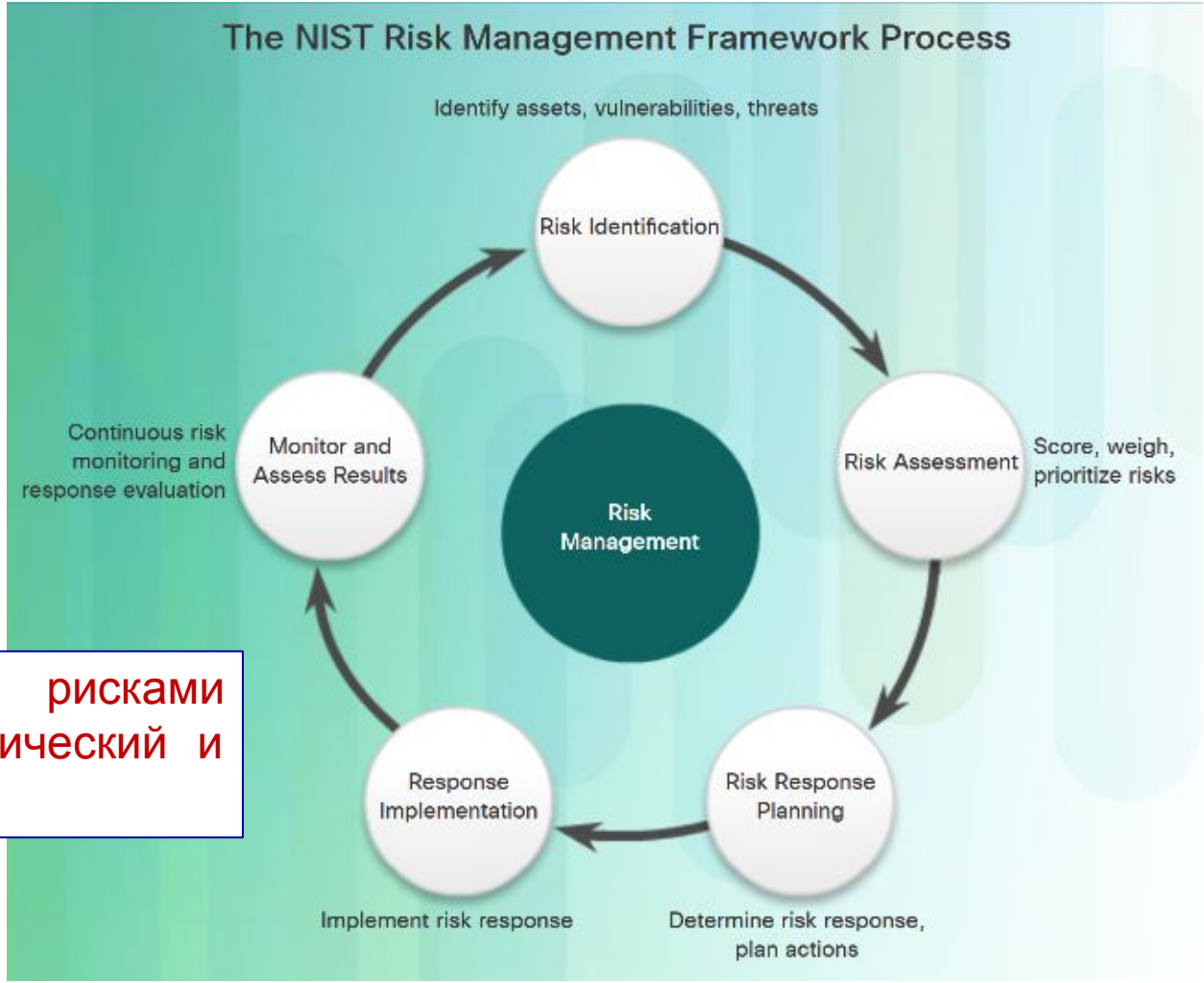
Несколько рекомендаций по безопасному дизайну:

- ❑ Учтите охват атаки - развертывания Интернета вещей будут иметь больший охват атаки на уровне устройства.
- ❑ Рассмотрите устройства, которые построены с безопасными конфигурациями по умолчанию и механизмами обновления.
- ❑ Учитывайте политики безопасности партнеров и сторонних сервисов.
- ❑ Думайте о безопасности во всем.

Общие стратегии смягчения:

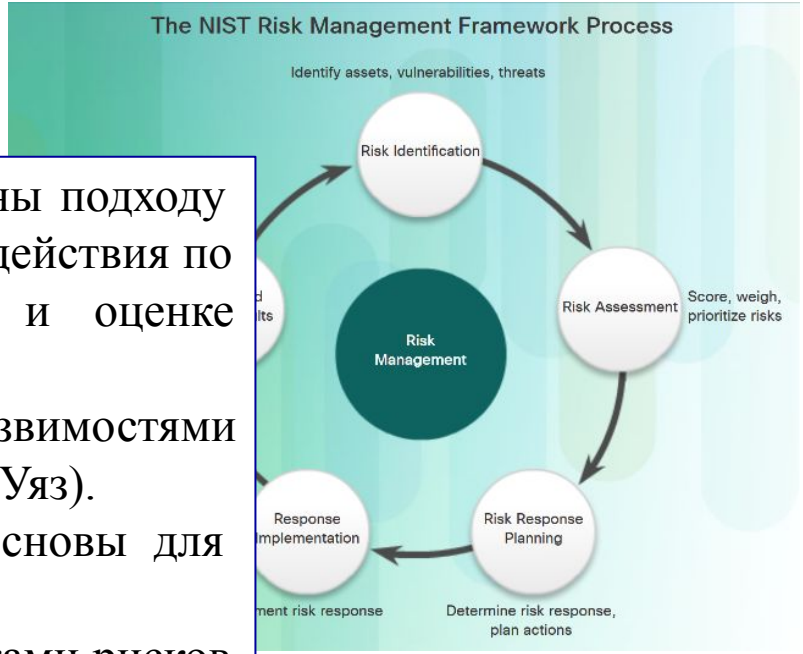
- Держите прошивку устройства в актуальном состоянии.
- Регулярно обновляйте прикладное программное обеспечение.
- Разделите трафик ИТ и Интернета вещей в сетях организации.
- По возможности обеспечьте физическую безопасность.
- Используйте безопасные протоколы обмена сообщениями и шифрование.
- Взаимодействуйте с персоналом сетевой безопасности внутри организации.

Стратегии управления рисками



Структура управления рисками NIST (RMF) - это циклический и непрерывный процесс.

Стратегии управления рисками



Идентификация рисков и оценка рисков параллельны подходу моделирования угроз. RMF замыкает круг, включая действия по реагированию на риски, оценке реагирования и оценке реагирования.

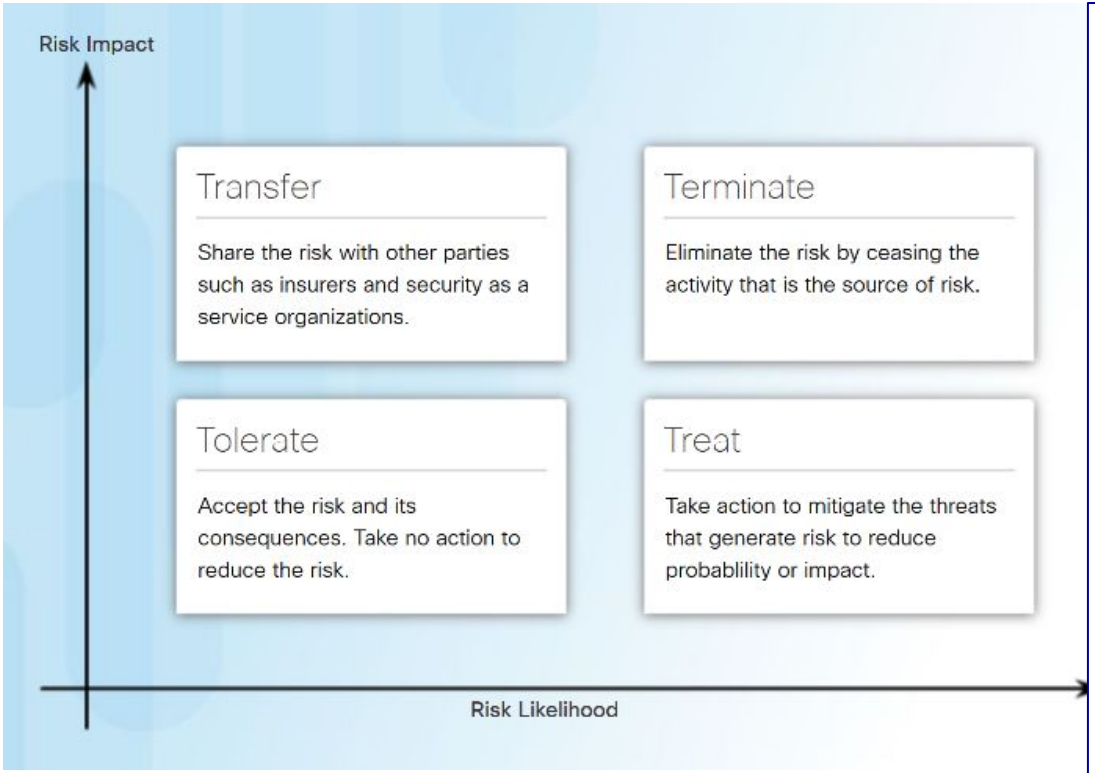
Идентификация и сопоставление угроз с уязвимостями называется объединением угроз и уязвимостей (Угр-Уяз).

Пары Угр-Уяз могут использоваться в качестве основы для обозначения риска до внедрения мер безопасности.

Базовый уровень можно сравнить с текущими оценками рисков как средством оценки эффективности управления рисками.

Это определяет неотъемлемый профиль риска организации. Риски могут быть оценены или взвешены как способ определения приоритетности стратегий снижения риска.

Реагирование на риск



Четыре «Т» реакции на риск:

Предотвращение риска (Прекратить) - Прекратить выполнение действий, создающих риск.

Снижение риска (лечение) - Уменьшите риск, приняв меры по снижению уязвимости.

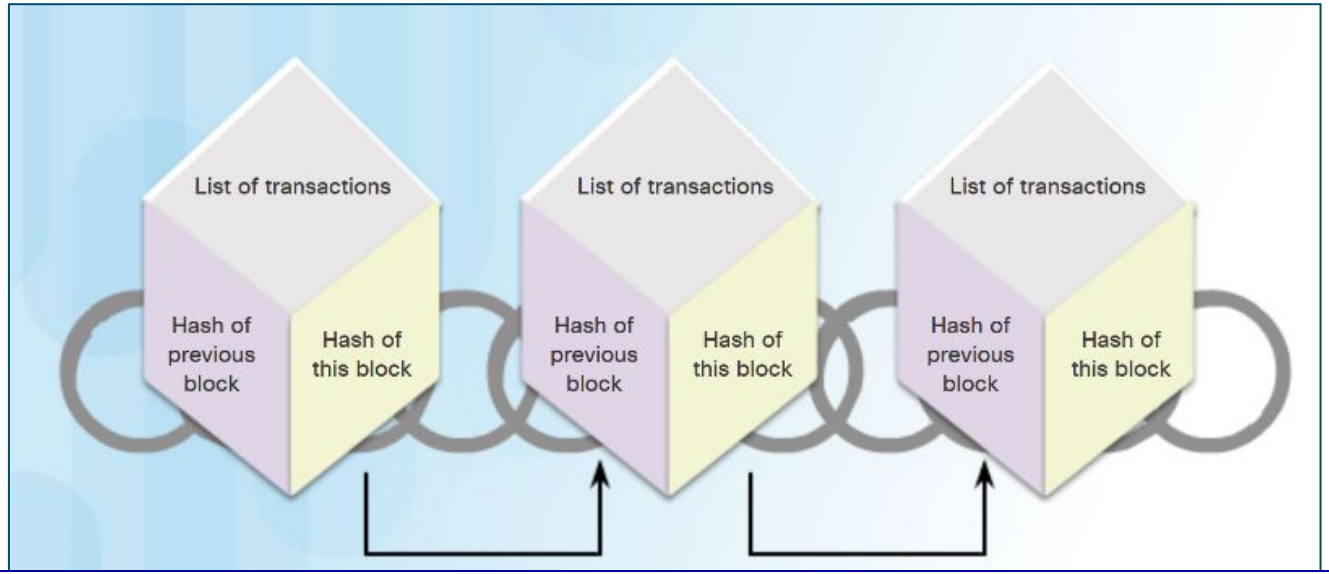
Разделение риска (передача) - переложите часть риска на другие стороны.

Удержание риска (терпимость) - Примите риск и его последствия.

На рисунке показано, что руководство по принятию решения о том, какой ответ предпринять, включает взвешивание потенциального воздействия риска с вероятностью его возникновения.

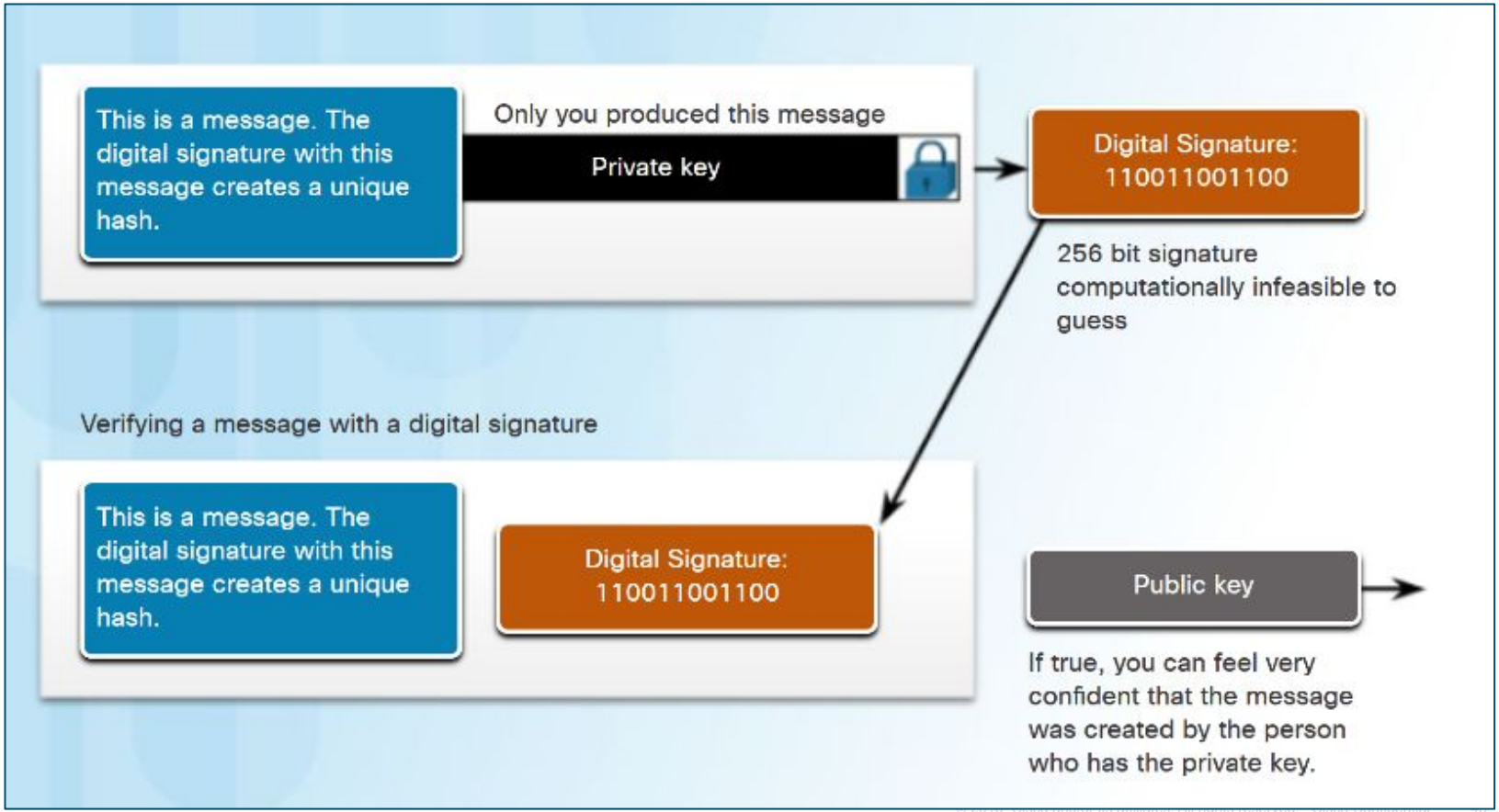
Введение в блокчейн
Перспективы блокчейна

Введение в блокчейн
Перспективы блокчейна

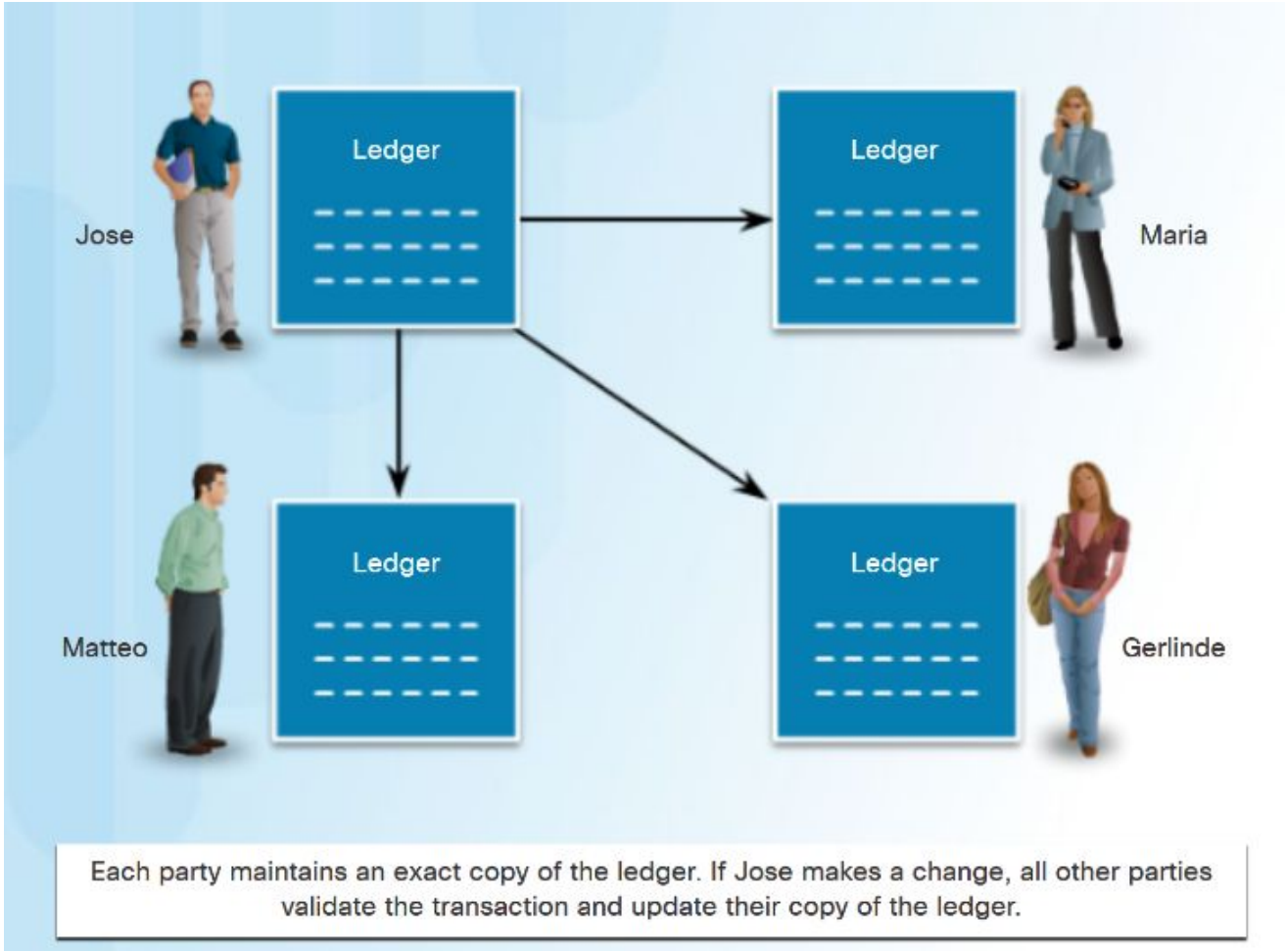


Блокчейн - это постоянно растущий список транзакций в виде блоков.
Эти блоки связаны и защищены с помощью криптографии.
Блокчейн использует следующее:
Цифровые подписи
Децентрализованный реестр
Алгоритм достижения консенсуса
Каждый блок включает в себя хеш предыдущего блока, образуя цепочку блоков, известную как цепочка блоков

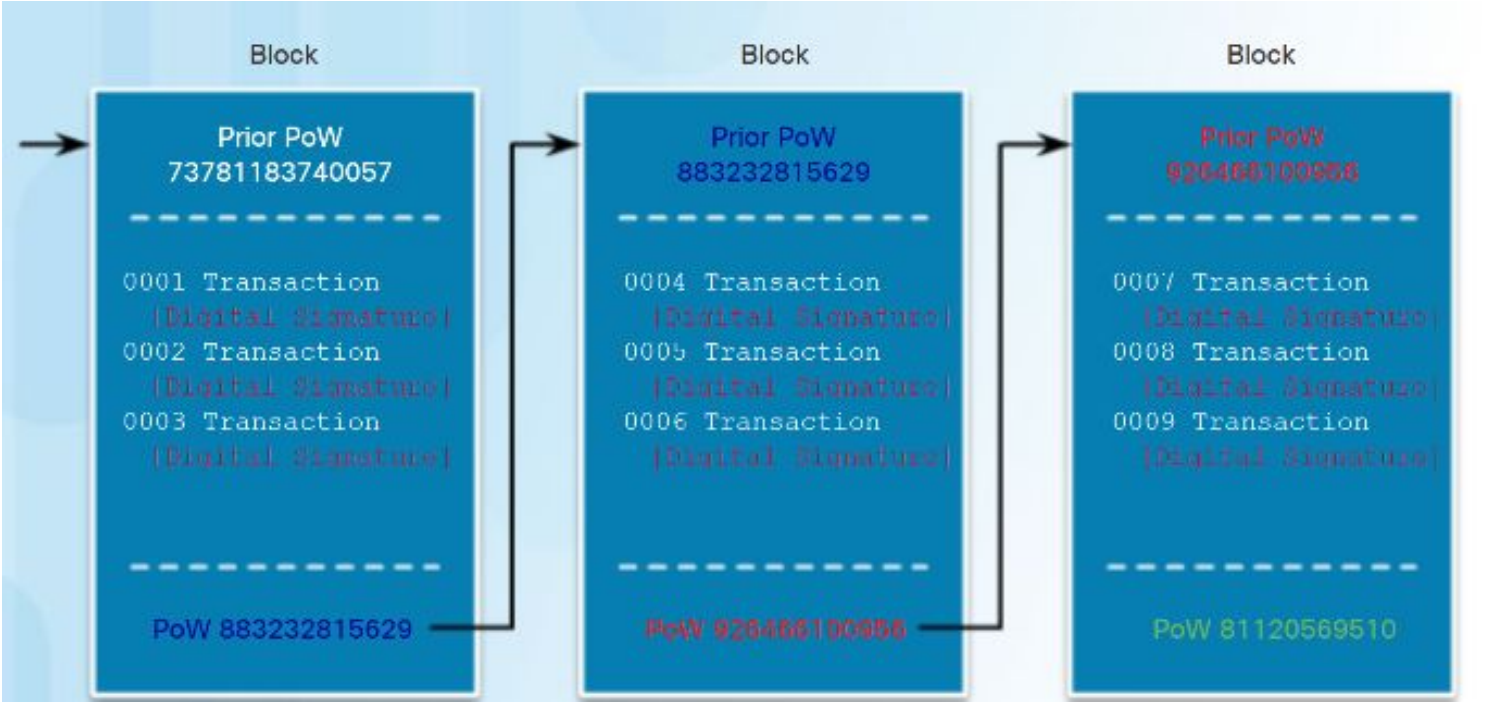
Введение в блокчейн
Цифровая подпись



Децентрализованная бухгалтерская книга



Достижение консенсуса



Для проверки транзакций в блоке используется процесс, известный как Proof of Work (PoW).

PoW - это алгоритм (хэш), выполняемый компьютерами, который требует большого объема вычислительной работы за относительно короткое время. Эти компьютеры известны как майнеры.

Блокчейн состоит из блоков. Каждый блок представляет собой список транзакций с хешем предыдущего блока и хешем этого блока, включая его PoW.

Хеш вычисляется с использованием хеша предыдущего блока (предыдущий PoW), а также всех транзакций в этом блоке с их цифровыми подписями.

Это делает невозможным с вычислительной точки зрения модификацию блока или изменение порядка блоков.

Блокчейн в применении к безопасности Интернета вещей

Блокчейн можно использовать для решения многих проблем безопасности и доверия для Интернета вещей:

- Отслеживание измерений данных датчиков и предотвращение вредоносных данных.
- Обеспечение идентификации устройства IoT, аутентификации и безопасной передачи данных.
- Разрешите датчикам Интернета вещей безопасно обмениваться данными напрямую друг с другом без посредников.
- Распределенный реестр устраняет единственный источник сбоев в экосистеме Интернета вещей.
- Развертывание IoT упрощается, а эксплуатационные расходы IoT снижаются благодаря отсутствию посредника.
- Устройства IoT напрямую адресуются с помощью блокчейна, обеспечивая неизменяемую историю.