Проблемы безопасности промышленного интернета вещей.

Подготовили студентки группы УИ31:
Шелкоплясова Анна и Щербатова Анастасия

Понятие промышленного интернета вещей

Промышленный интернет вещей - это совокупность физических объектов, датчиков, систем управления и других устройств в единую сеть, позволяющую собирать и анализировать данные в реальном времени.

Цель - оптимизация производственных процессов, повышение эффективности и безопасности на предприятии.

Проблемы безопасности IOT

- Очень большая площадь атаки: Пользователи могут не знать, что IoT в значительной степени основывается на сборе и обработке больших объемов данных из различных источников, включая и конфиденциальные данные, и обмене ими.

- Сложность экосистемы IoT: IoT следует рассматривать как широкую экосистему, включающую устройства, коммуникации, интерфейсы и людей.

Проблемы безопасности IOT

- Отсутствие законодательных актов, норм, стандартов и правил

- Широкое внедрение в критически важные системы

Медленное принятие стандартов и правил для внедрения мер безопасности в сфере IoT, а также постоянное появление новых технологий еще более усложняют проблему.
Проникновение технологий IoT в критически важную инфраструктуру, имеющую стратегическое значение для государства, несет угрозу безопасности.

- Сложность интеграции систем безопасности

Сложность заключается в наличии потенциально противоречивых точек зрения. Например, разные устройства и системы IoT могут использовать разные решения аутентификации.

- Экономия производителей на безопасности

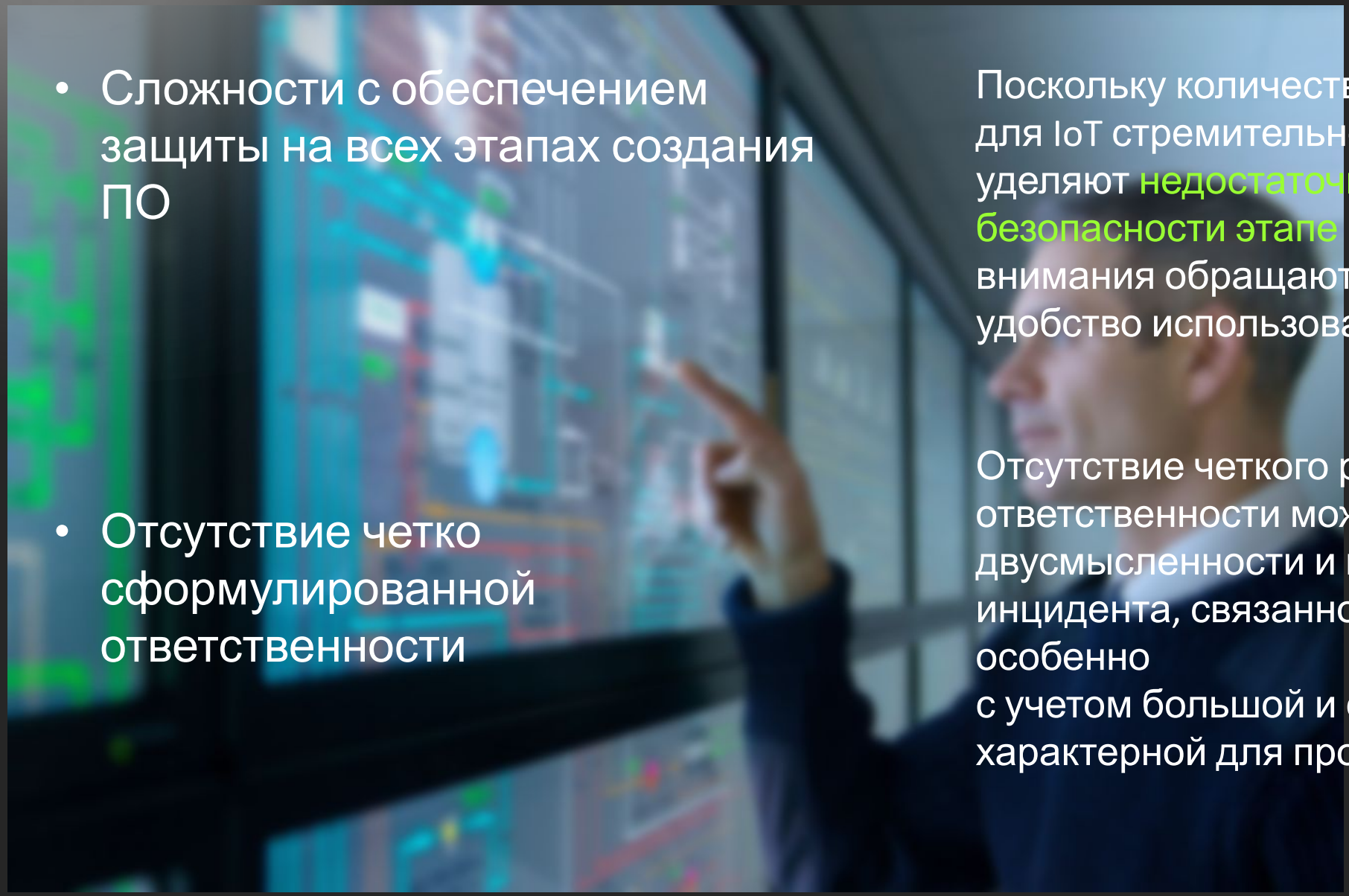
Экономия затрат осуществляется благодаря использованию таких функций, как потоки данных, расширенный мониторинг, интеграция и многие другие.

- Недостаток опытных специалистов

Это довольно новая область, и поэтому не хватает людей с подходящим набором навыков и опытом в области безопасности IoT.

- Сложности с обеспечением безопасности при обновлении IoT-устройства:

Специфика пользовательских интерфейсов, доступных пользователям, не позволяет использовать традиционные механизмы обновления.



- Сложности с обеспечением защиты на всех этапах создания ПО

- Отсутствие четко сформулированной ответственности

Поскольку количество выпускаемых решений для IoT стремительно растет, производители уделяют недостаточно времени обеспечению безопасности этапе разработки. Больше внимания обращают на функциональность и удобство использования устройства.

Отсутствие четкого распределения ответственности может привести к двусмысленности и конфликтам в случае инцидента, связанного с безопасностью, особенно
с учетом большой и сложной цепочки, характерной для производства IoT-устройств.

Классификация угроз IOT

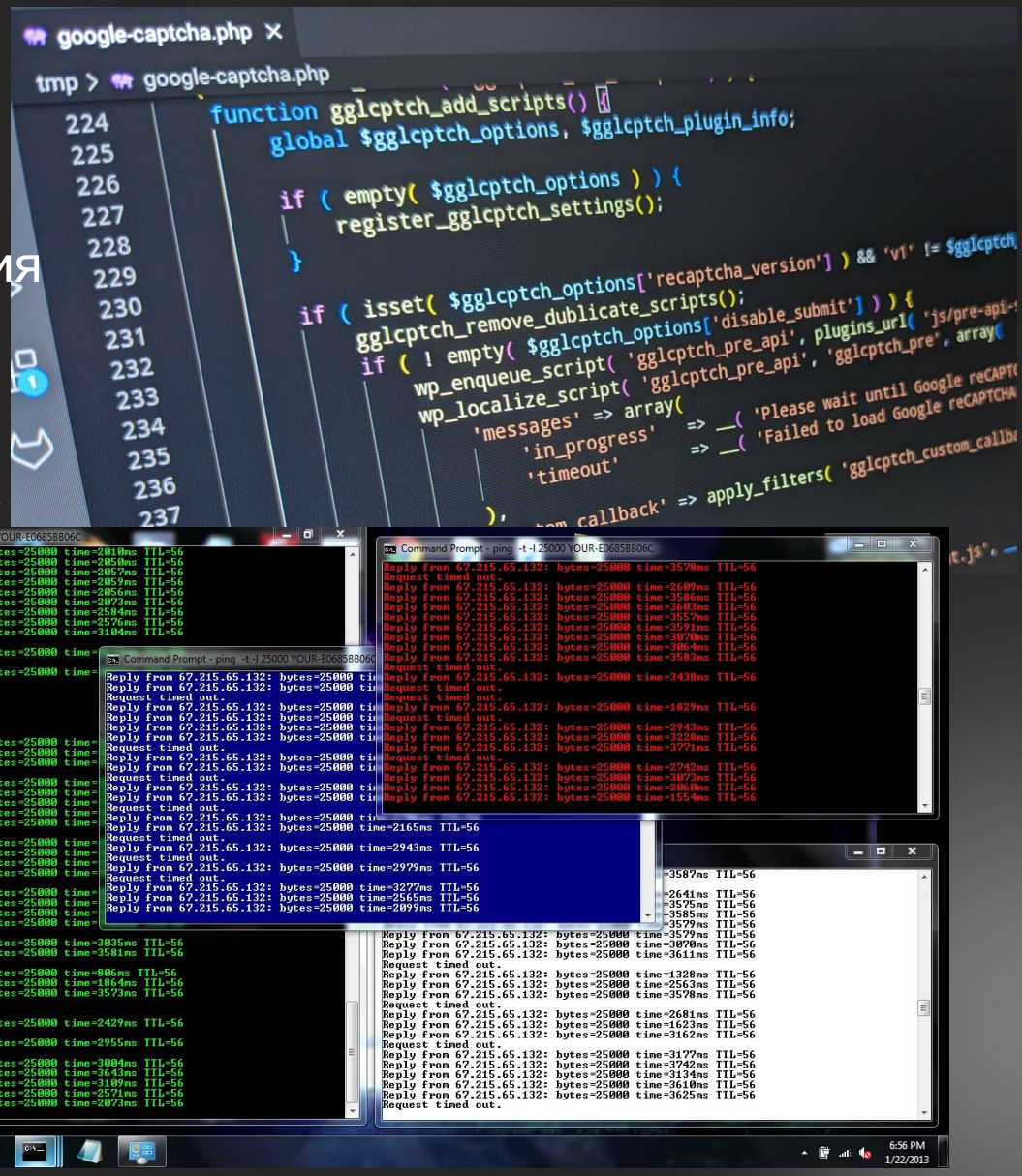
1. Умышленные действия

Вредоносное ПО - программное обеспечение, предназначенное для выполнения нежелательных и несанкционированных действий в системе без согласия пользователя.

Эксплойт - код, разработанный для использования уязвимости с целью получения доступа к системе. Эту угрозу трудно обнаружить.

Целевая атака - атака, предназначенная для конкретной цели, которая проводится в несколько этапов. Основная цель преступника – оставаться незамеченным и получить как можно больше информации.

DDoS-атака - несколько систем атакуют одну цель, чтобы нагрузить ее и привести к сбою.



Классификация угроз IOT

1. Умышленные действия

Скомпрометированное устройство: эти устройства обычно имеют бэкдоры и могут
использоваться для проведения атак на другие системы в окружающей среде

Модификация информации: цель состоит в манипуляции информацией, чтобы вызвать хаос илиполучить денежную прибыль

Утрата конфиденциальности: эта угроза опасна как утратой конфиденциальности пользователя, так и воздействием постороннего персонала на элементы сети

Классификация угроз IOT

2. Перехват информации

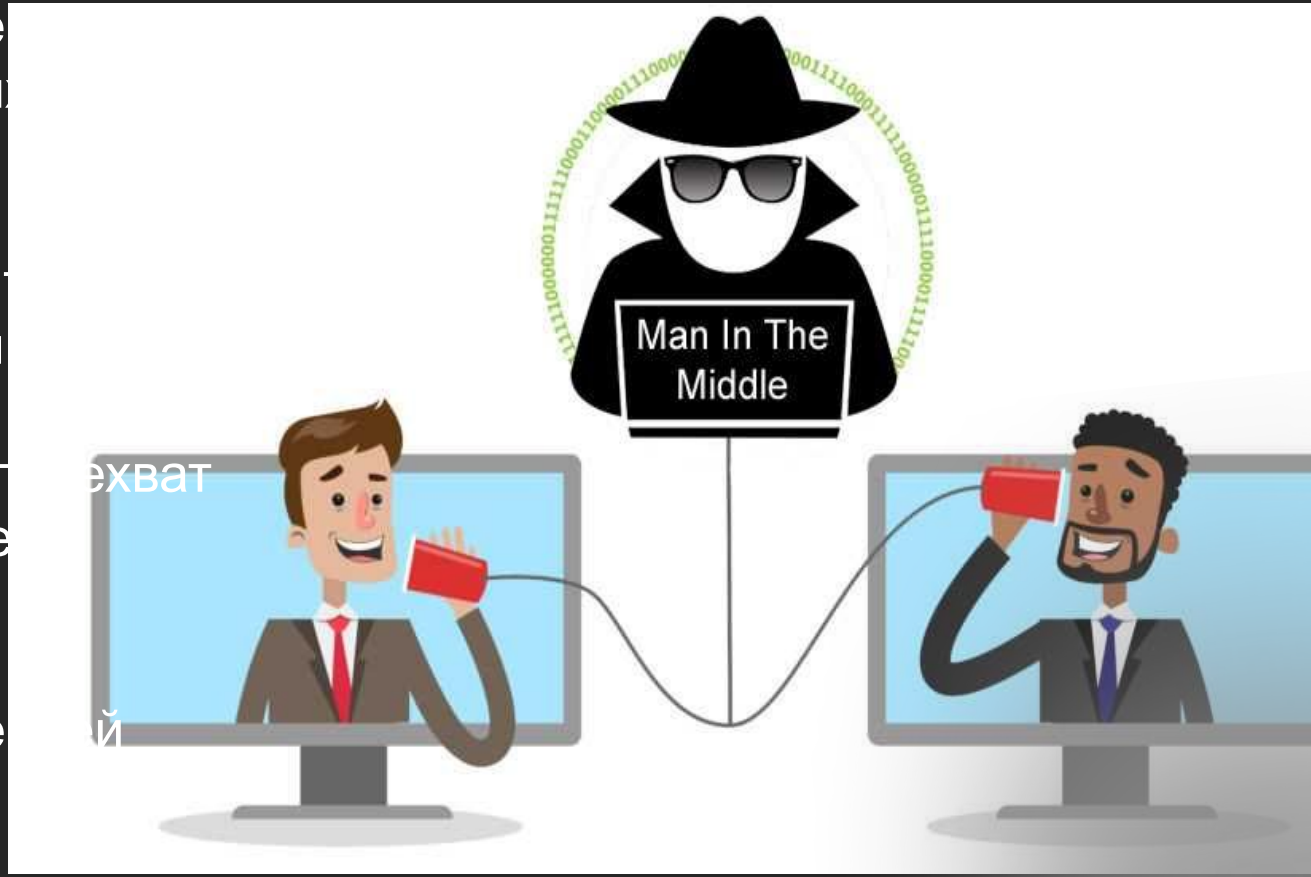
Атака «человек посередине» - активная атака подслушивания, при которой злоумышленник пе сообщения от одной жертвы другой, заставляя и поверить, что они разговаривают друг с другом

Подключение к активной сессии - взятие под конт активного сеанса связи между двумя элементам

Перехват информации - несанкционированный п ехват и модификация частной коммуникации, наприме телефонных звонков.

Сетевая разведка - пассивное получение внутре й информации о сети.

Перехват соединения - кража соединения для передачи данных.



Классификация угроз IOT

3. Отключение

Отключение питания - преднамеренное или случайное прерывание или сбой в сети.

Сбой устройства - сбой или выход из строя аппаратного устройства.

Сбой системы - сбой программных служб или приложений

Потеря сервиса поддержки - недоступность услуг поддержки, необходимых для правильной работы информационной системы.

Классификация угроз IOT

4. Технический сбой

Уязвимости на программном уровне: устройства IoT часто уязвимы из-за слабых паролей, неизмененных паролей, установленных по умолчанию, программных ошибок и ошибок конфигурации

Сторонние ошибки - ошибки в активном элементе сети, вызванные неправильной настройкой другого элемента, который имеет к нему прямое отношение

Классификация угроз IOT

5. Катастрофы

Стихийные бедствия: наводнения
сильные ветры, сильные снегопа
оползни и др.

Аварии в среде IoT - аварии в сре
развертывания IoT-оборудования
приводящие к их
неработоспособности

6. Физическая атака

Модификация устройства - внесение
изменений в устройство

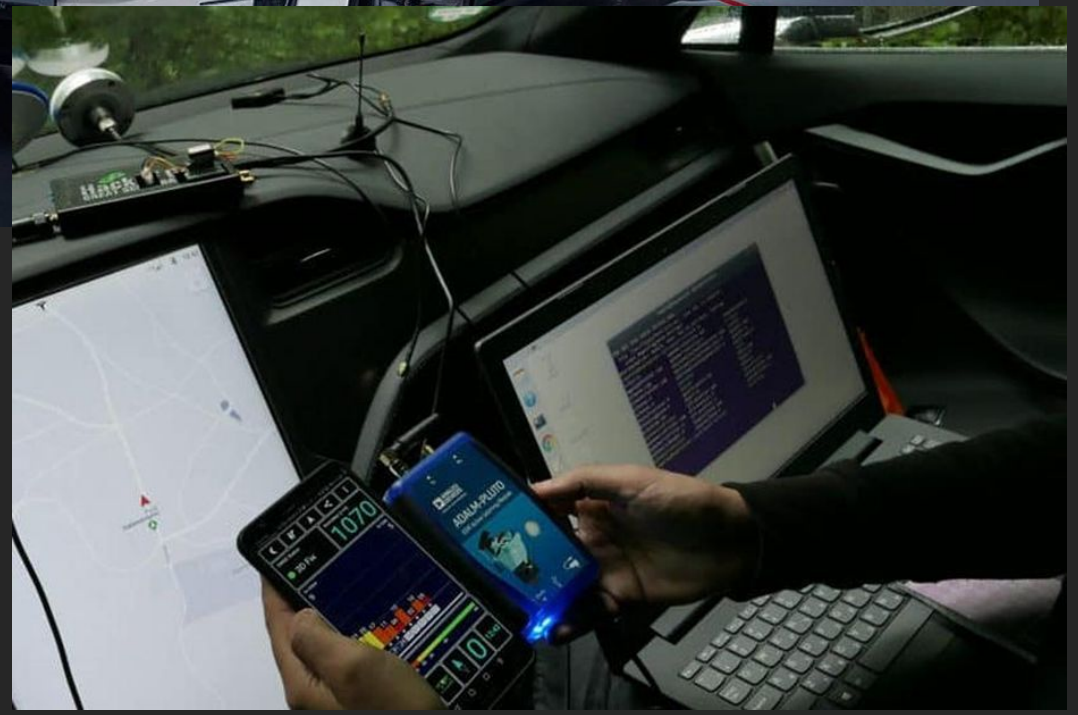
Уничтожение устройства - порча, кража и т.
п.

Примеры нарушений безопасности интернета вещей

В последние годы имел место ряд громких случаев компрометации устройств интернета вещей киберпреступниками. Среди них:

2020 – взлом Tesla Model X

Эксперт по кибербезопасности взломал Tesla Model X менее чем за две минуты, воспользовавшись уязвимостью Bluetooth. Аналогичным атакам также подверглись другие автомобили, для открытия и запуска которых используются беспроводные ключи.



2020 – взлом Tesla Model X

По словам аспиранта Лёвенского университета в Бельгии - Леннерта Воутерса, «слабым звеном» в системе защиты электрокара стал процесс обновления прошивки фирменного брелока Tesla Model X. Для получения контроля над умным автомобилем можно использовать электронный блок управления, взятого с любого старого Model X.

«Хакерская установка» обошлась сравнительно недорого. Она включает микрокомпьютер ($35), плату расширения ($30), модифицированный брелок для ключей, блок управления от старого автомобиля ($100) и аккумулятор ($30). Единственный недостаток устройства — приличные габариты, хотя оно вполне влезет в рюкзак или большую сумку.

Воутерс отметил, что после того, как он связался с представителями Tesla, автопроизводитель выпустил обновление прошивки 2020.48, исправляющее уязвимость.

2021 – взлом камеры Verkada

Verkada – компания по производству камер наблюдения. В 2021 году швейцарские хакеры получили доступ к 150 000 прямых трансляций с камер этой компании. Это были камеры наблюдения внутри зданий государственных
ы, тюрьмы,

2021 – взлом камеры Verkada

Среди пострадавших значится также компания Илона Маска Tesla, которая является клиентом стартапа. Сообщается, что преступники смогли взломать камеры на фабрике производителя электрокаров в Шанхае, а также нескольких складах.

На связь с Bloomberg вышел Тилли Коттман, один из участников атаки.

По его словам, взлом был осуществлен международной хакерской группировкой, которая своими действиями хотела привлечь внимание к повсеместному распространению систем видеонаблюдения, а также легкости, с которой такие камеры могут быть скомпрометированы.

Ранее Коттман брал на себя ответственность за атаки на производителя чипов Intel Corp. и автокомпанию Nissan Motor Co. Он отметил, что его группировка занимается хакерством «из любопытства, а также в рамках борьбы за свободу информации и против интеллектуальной собственности, ради антикапитализма и щепотки анархизма».