РУТОКЕН

Вебинар

Прекрасное недалеко

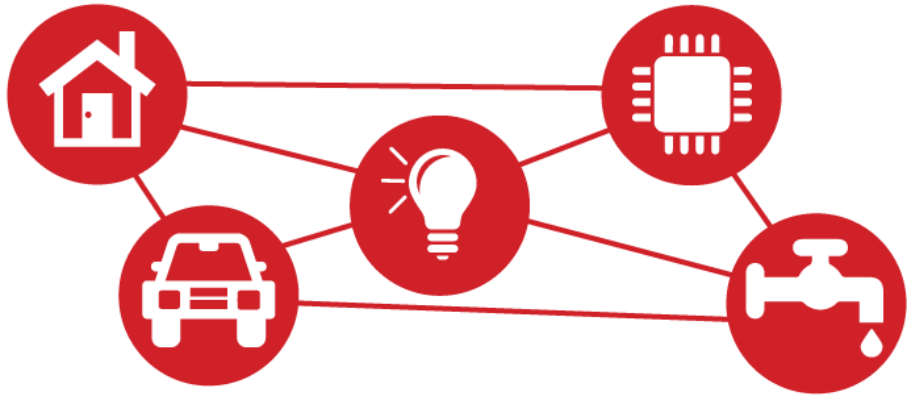
Как защититься в мире интернета вещей?

Алексей Лазарев,
ведущий менеджер проектов

РУТОКЕН

Что дает IOT?

- Управление механизмами (M2M, АСУ ТП)
- Мониторинг расхода энергоресурсов
- Транспорт и логистика
- Мониторинг безопасности
- Умные бытовые приборы
- Сбор статистики и определение трендов



Экономят время, ресурсы, деньги.

Работают тогда, когда это реально нужно.

РУТОКЕН

Что мешает объединению в глобальный IOT?

- Молодость явления
- Проблемы собственности
- Отсутствие универсальной платформы
- Конкуренция схожих по сути технологий
- Быстро меняются экономические условия
- Проблемы законодательства и общества
- Зависимость от смежных отраслей
- Высокая стоимость
- Проблемы безопасности

Проблемы обеспечения безопасности

- Зоопарк всевозможных устройств.
  Слабость базы стандартов
- Развитие бизнеса требует изменения технологической базы
- Проблемы модернизации старых работающих каналов связи
- Нехватка времени, компетенций, ресурсов, чтобы довести до ума
- Слабые чипы в автономных устройствах.
  Экономия батареи
- Мы видим не все уязвимости

РУТОКЕН

Виды атак

Атаки на канал связи:

- Перехват и подмена пакета
- Атаки повторения сигнала
- Перехват данных идентификации

Атаки на устройства:

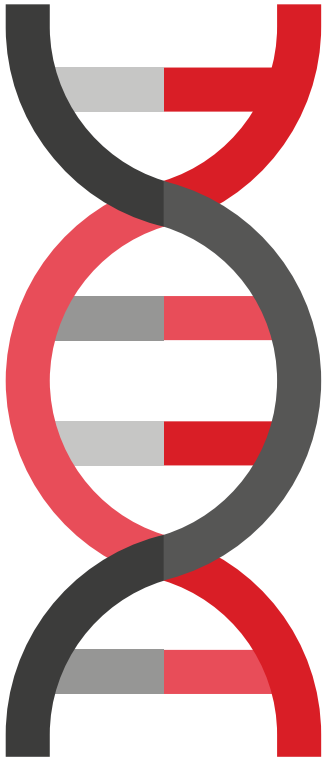
- Атака в момент активации или замены устройства
- DOS-атаки
- Подмена устройства
- Взлома чипа
- Атаки на сервера и базовые станции

Прочие атаки:

- Попытка манипуляции украденным ID или биометрией
- Инсайд
- Троянец с отложенной активацией
- Активация вредоноса через закладки в оборудовании

Генезис угроз

- Хулиганство, саботаж, терроризм
- Недобросовестная конкуренция
- Кража технологии
- Зависимость от импорта
- Кража персональных данных и биометрии с целью продажи третьим лицам
- Не зависящие от нас факторы: климат, катастрофы
- Человеческий фактор



Факторы, способствующие успешным атакам

- Малый размер пакета
- Легкость идентификации устройства
- Открытый доступ к оборудованию и базовым станциям
- Устаревшая прошивка устройства с известными «дырами»
- Компоненты из сомнительных источников с закладками
- Хранение секрета в ненадежном месте
- Отношение к безопасности со стороны самого бизнеса

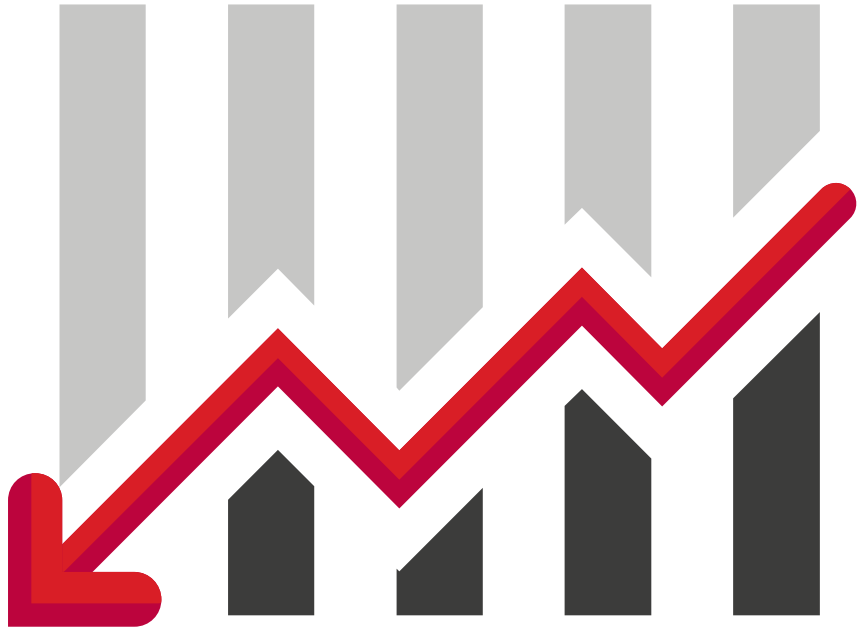
РУТОКЕН

Отношение бизнеса к безопасности

- Нет времени
- Нет денег
- Не ясно, чего начать
- Не понятно, как считать
- В протоколе все предусмотрено
- Пронесет

Потери

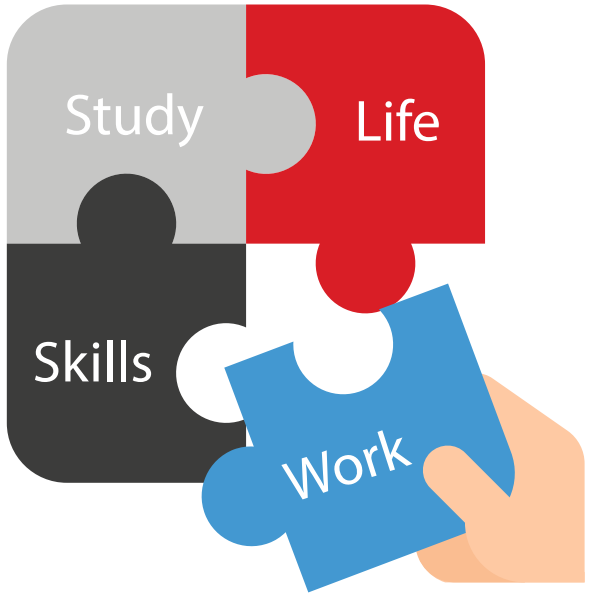
- Человеческие жертвы
- Юридические
- Финансовые
- Инфраструктурные
- Временные
- Репутационные



РУТОКЕН

Как систематизировать подход к безопасности?

- Накопление опыта. Больше решений — больше данных
- Обмен опытом. Общедоступная база знаний
- Проекция в будущее. Каким будет ваш бизнес через годы?
- Выработка алгоритма действий (сбор данных, анализ, реализация)
- Оттачивание алгоритма на практике



Нужна методика!

РУТОКЕН

Сбор данных

- Определить сферы ответственности
- Определить объекты, требующие защиты
- Представить источники угроз, характер угроз
- К чему приведет недостаток ресурсов?
- Что предпринимали в похожих проектах?
- Что говорит законодательство?
- Что в смежных, зависимых, зависящих областях?
- Каковы возможные последствия реализации угроз?
- Меры противодействия угрозам, их стоимость
- Средства противодействия угрозам, их стоимость
- Куда пойдет эволюция системы?
- Что говорят специалисты?

Обработка данных

- Расстановка угроз по приоритетам угрозы по приоритетам
- Привлечение специалистов
- Выработка мер по устранение угроз
- Выбор средств устранения угроз
- Документирование кейсов, результатов
- Документирование инцидентов, ошибок, их
- Статистический анализ

РУТОКЕН

Выработка мер

239

- Раздача прав участникам
- Разграничение зон доступа
- Должностные инструкции
- Защита оборудования от внешнего воздействия
- Защита каналов связи и аутентификация устройств и данных
- Мониторинг состояния оборудования, прогноз состояния
- Мониторинг состояния сотрудников (здоровье, трезвость)
- Проработка реакции системы на случившийся инцидент
- План взаимодействия со СМИ на случай инцидента
- Резервирование

Объекты и угрозы

Объект	Виды атак	Средства противодействия	Стоимость мер
Канал связи	Репит-атака	Имитозащита канала	
	Перехват пакета	Шифрование	
	Подмена пакета	Подпись	
	MITM-атака	Аутентификация абонентов	
Сервер	DDOS-атака	Распределенность, закрытие доступа в глобальную сеть, фильтрация, VPN, тайминг	
	Атака на механизм аутентификации	Строгая аутентификация по ряду параметров.	
	Атака на уязвимости протоколов	Защищенное обновление	
	Открытые порты и сервисы	Firewall, закрытие ненужных каналов	
	Инсайд	Доверенная загрузка и установка ПО	
Датчик	Вандализм	Предотвращение доступа, защита	
	Подмена устройства		
	Атака на мех-м обновления прошивки	Подпись прошивки	
Шлюз, Б/С	Засорение эфира, См выше.	Смена частот	

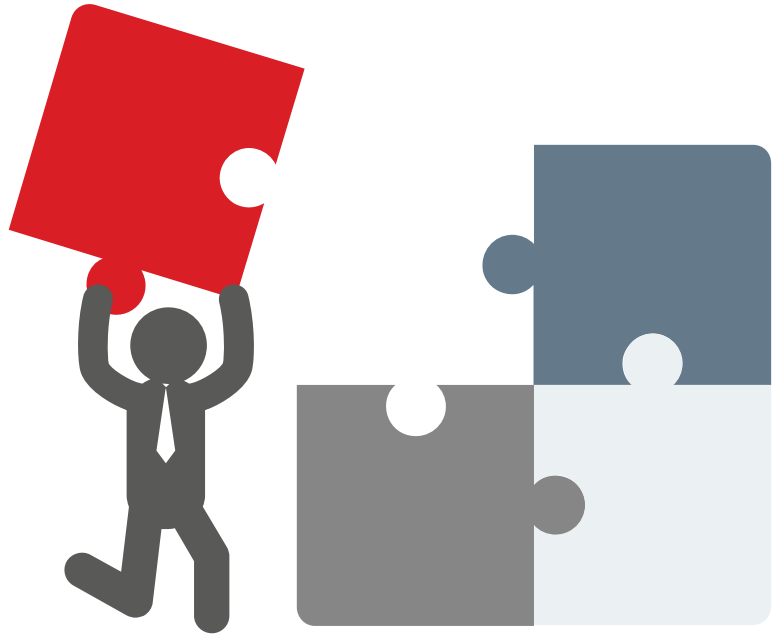
РУТОКЕН

Расстановка приоритетов

Угроза	Источник	Последствия	Цена меры противодействия	Цена последствий и их устранения	Важность
DDOS	Конкурент	Потеря контроля над системой	Распределение, настройка доступа	Восстановление доступа	70
Атаки на канал связи	Хакер	Неверная интерпретация данных	Рутокен M2M	Замена датчиков	60
Отключение энергии	Неуплата, Погодный катаклизм	Люди (Отключение СЖО)	Стоимость и установка генератора	Судебные издержки#, Репутационные издержки, Финансовые потери, Восстановление оборудования	110

Действуем

- Устраняем угрозы жизни и здоровью
- Устраняем противоречия с законом
- Устраняем возможность несанкционированного доступа к данным
- Защищаем каналы связи
- Защищаем устройства и данные
- Протоколируем меры
- Делимся опытом
- Проводим регулярный аудит с учетом новых факторов



Советы обывателю

- Изучать проблематику технологических новшеств
- Ответственно относиться к персональным данным и данным биометрии
- Взаимодействовать только с аккредитованными организациями
- Не оставлять электронные следы
- Использовать сложные пароли, а лучше – персональные устройства двухфакторной аутентификации
- Использовать только сертифицированные приборы и устройства
- Использовать электронную подпись с неизвлекаемым ключом

РУТОКЕН

Контактная информация

Алексей Лазарев

Электронная почта:

hotline@rutoken.ru

Сайты:

www.rutoken.ru

www.aktiv-company.ru

Телефон:

+7 495 925-77-90

https://www.youtube.com/user/AktivCompany