

СПб ГУТ)))



**«ПРОБЛЕМНЫЕ ВОПРОСЫ И ТЕНДЕНЦИИ
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ В ОБЛАСТИ
ТЕЛЕКОММУНИКАЦИЙ:
УГРОЗЫ, УЯЗВИМОСТИ, РЕШЕНИЯ»**

Проф. М.В. Буйневич

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда
 - 1.1. Доверенная маршрутизация
 - 1.2. Проприетарное ПО ТКУ
 - 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей
 - 2.1. Ложные облака
 - 2.2. Клоны
 - 2.3. Отъем энергии
 - 2.4. ЭМ-воздействие

3. Крипто vs Стего
 - 2.1. Пост-квантовая криптография
 - 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

1.1. Доверенная маршрутизация

1.2. Проприетарное ПО ТКУ

1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

2.1. Ложные облака

2.2. Клоны

2.3. Отъем энергии

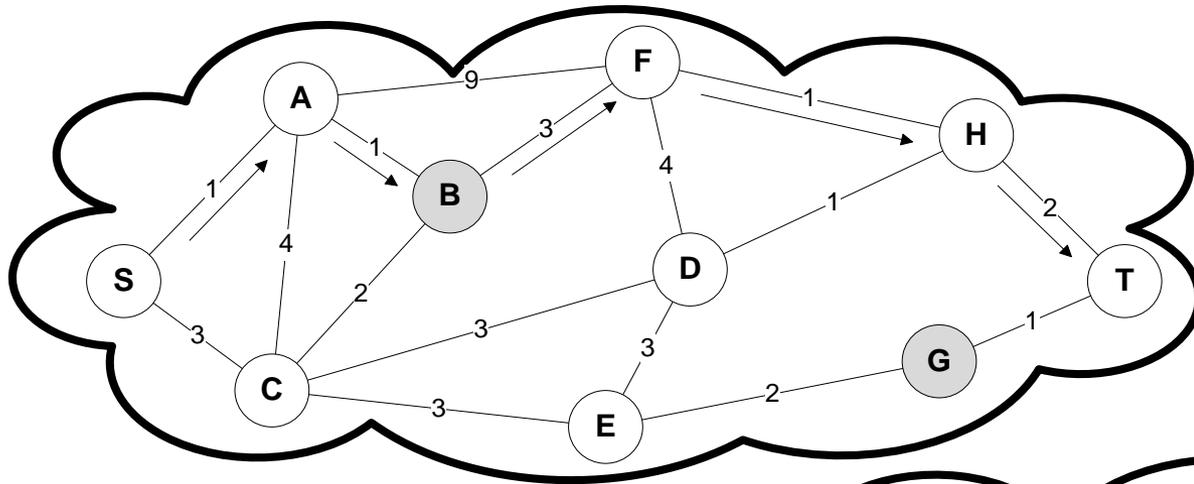
2.4. ЭМ-воздействие

3. Крипто vs Стего

2.1. Пост-квантовая криптография

2.2. Стегосистемы и ЦВЗ

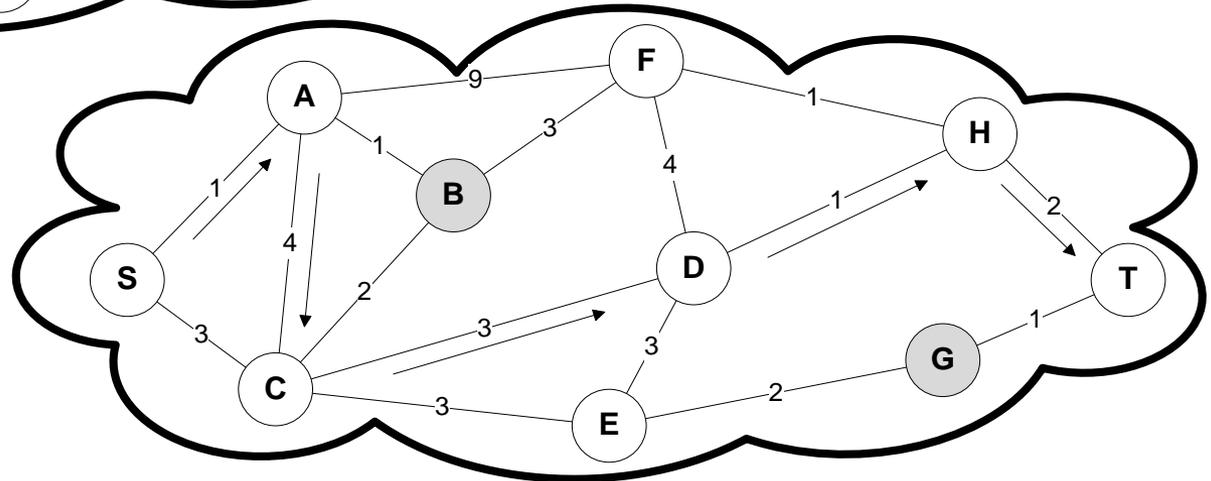
1.1. Доверенная маршрутизация



○ - Доверенный узел

● - Недоверенный узел

→ - Направление потока



Модификация алгоритма Дейкстры

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

1.1. Доверенная маршрутизация

1.2. Проприетарное ПО ТКУ

1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

2.1. Ложные облака

2.2. Клоны

2.3. Отъем энергии

2.4. ЭМ-воздействие

3. Крипто vs Стего

2.1. Пост-квантовая криптография

2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

1.1. Доверенная маршрутизация

1.2. Проприетарное ПО ТКУ

1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

2.1. Ложные облака

2.2. Клоны

2.3. Отъем энергии

2.4. ЭМ-воздействие

3. Крипто vs Стего

2.1. Пост-квантовая криптография

2.2. Стегосистемы и ЦВЗ

1.2. Проприетарное ПО ТКУ



Метод алгоритмизации машинного кода

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

1.1. Доверенная маршрутизация

1.2. Проприетарное ПО ТКУ

1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

2.1. Ложные облака

2.2. Клоны

2.3. Отъем энергии

2.4. ЭМ-воздействие

3. Крипто vs Стего

2.1. Пост-квантовая криптография

2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

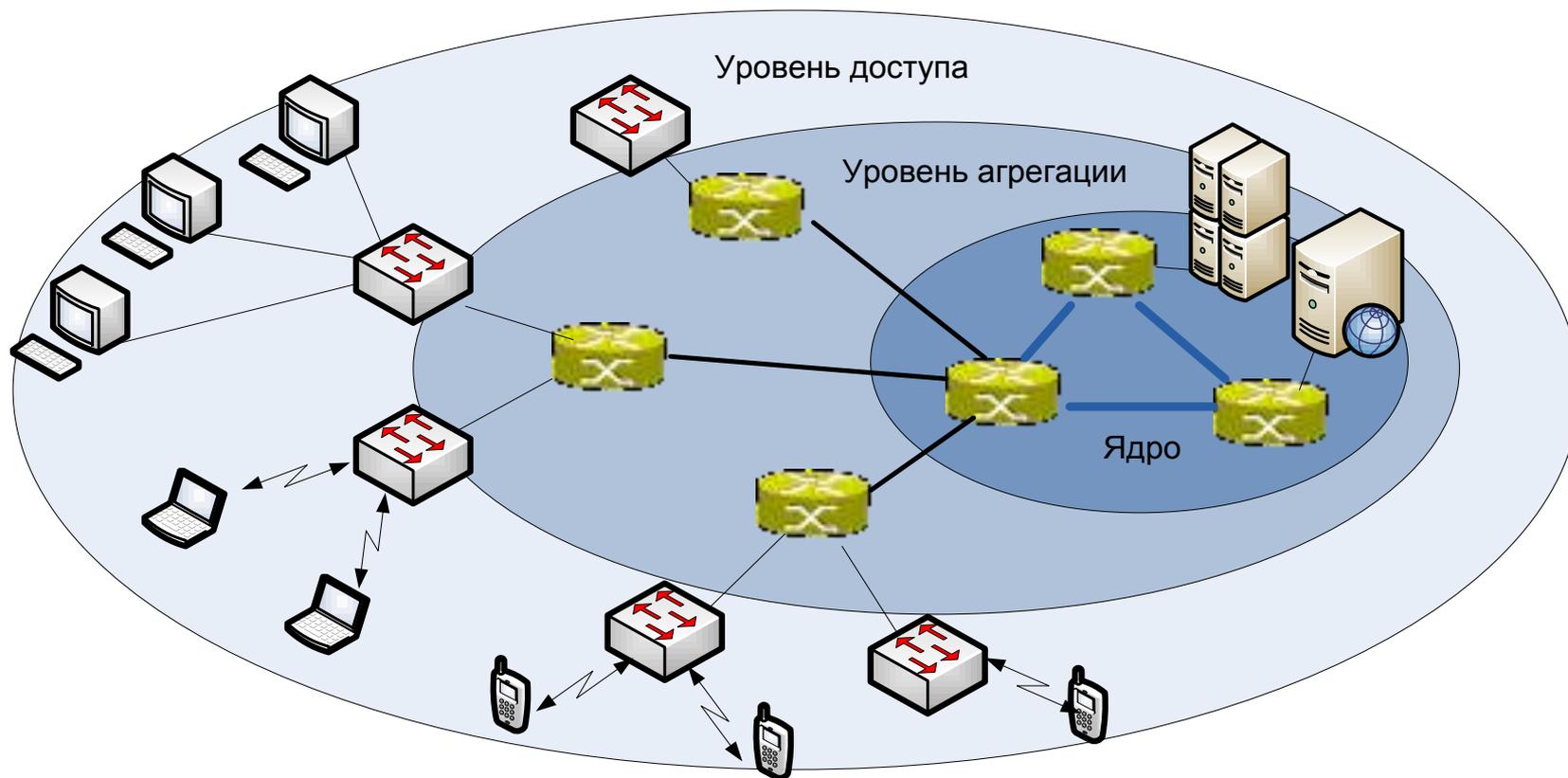
2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

1.3. Архитектурные уязвимости моделей ЦТКС



Базовая иерархическая модель сети

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

2.1. Ложные облака

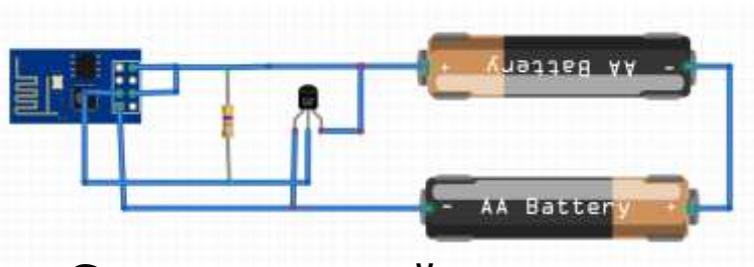
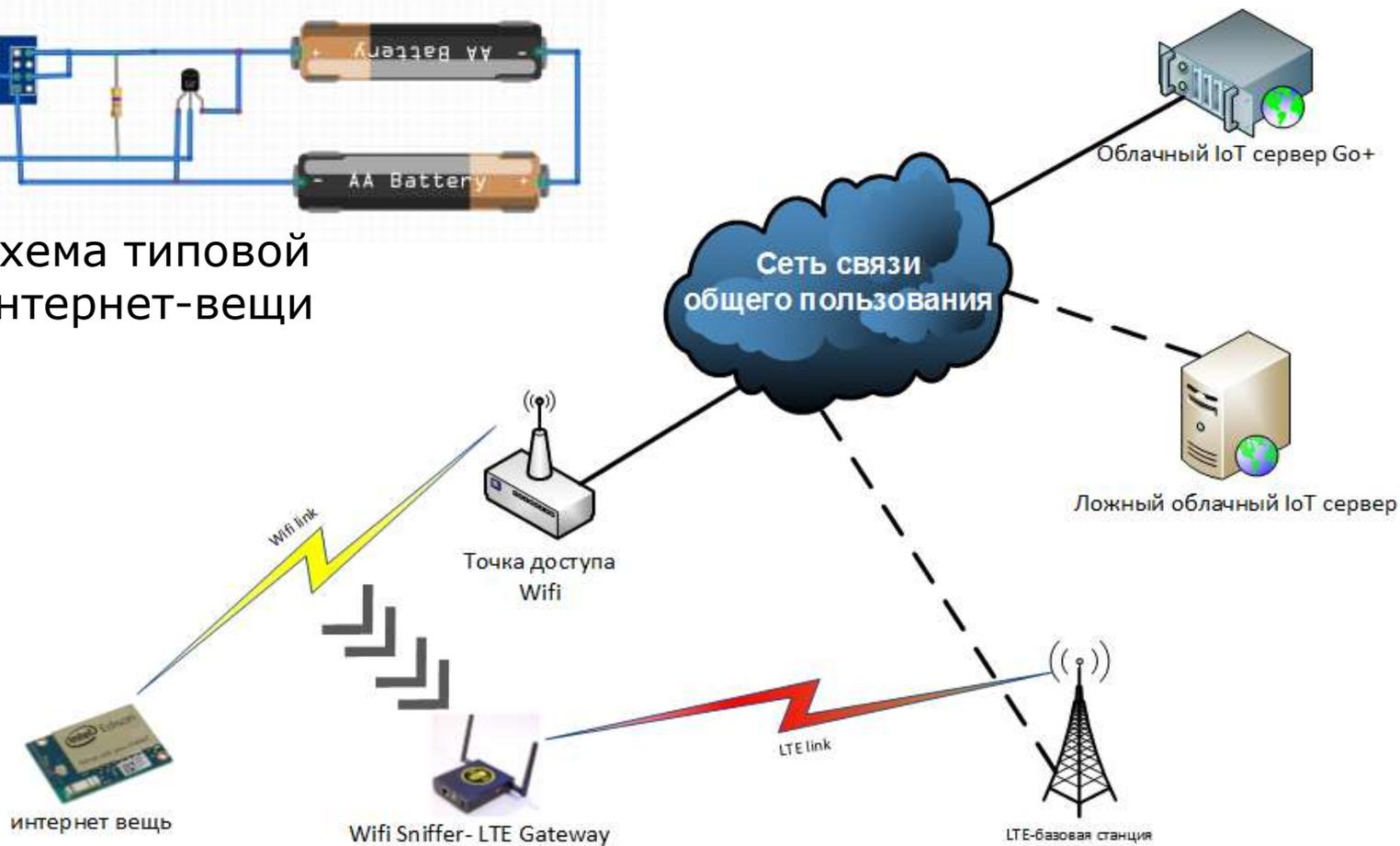


Схема типовой интернет-вещи



Структура экспериментального стенда

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

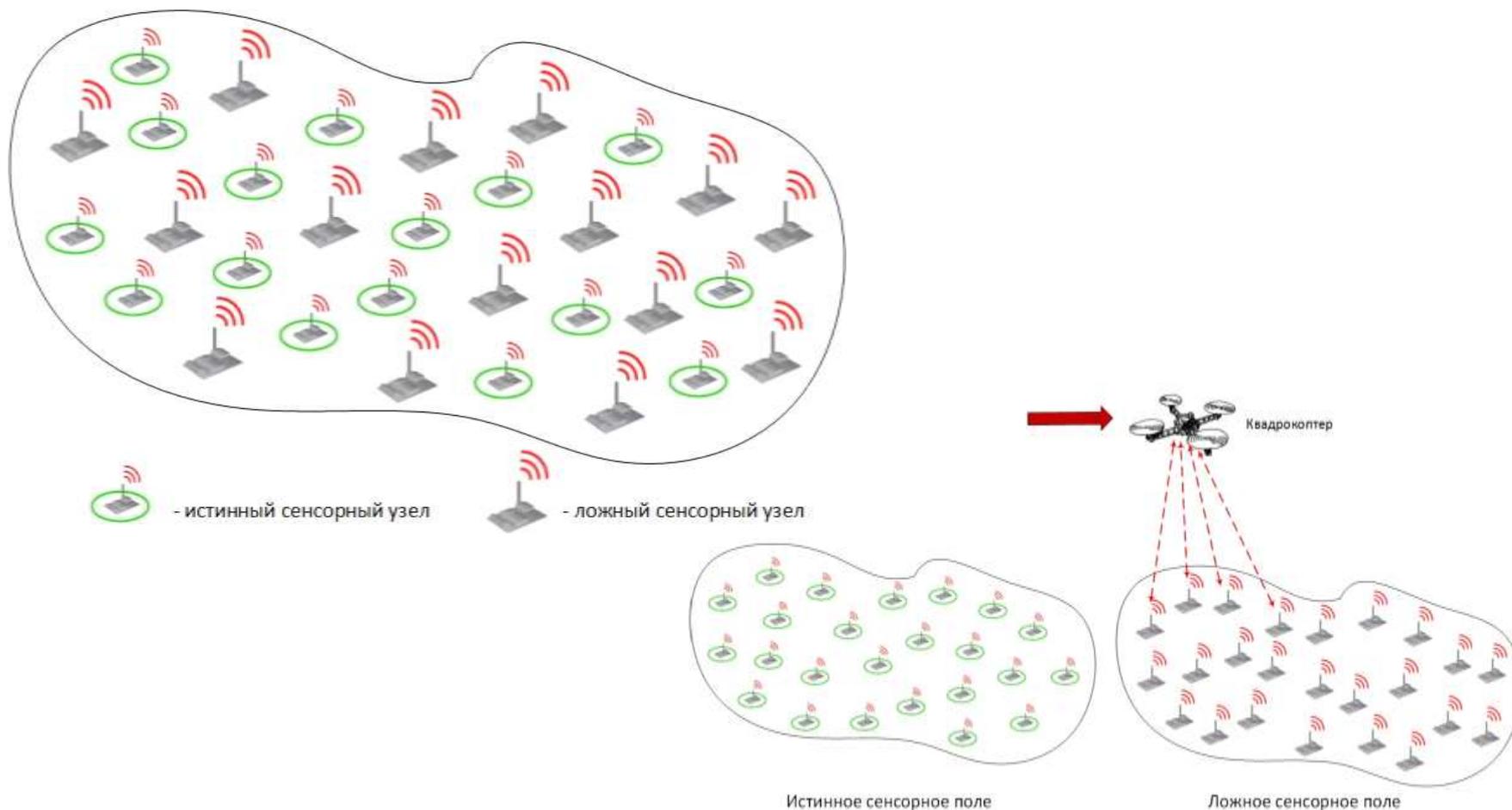
2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

2.2. Клоны



Клонирование сенсорных узлов и сенсорного поля

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

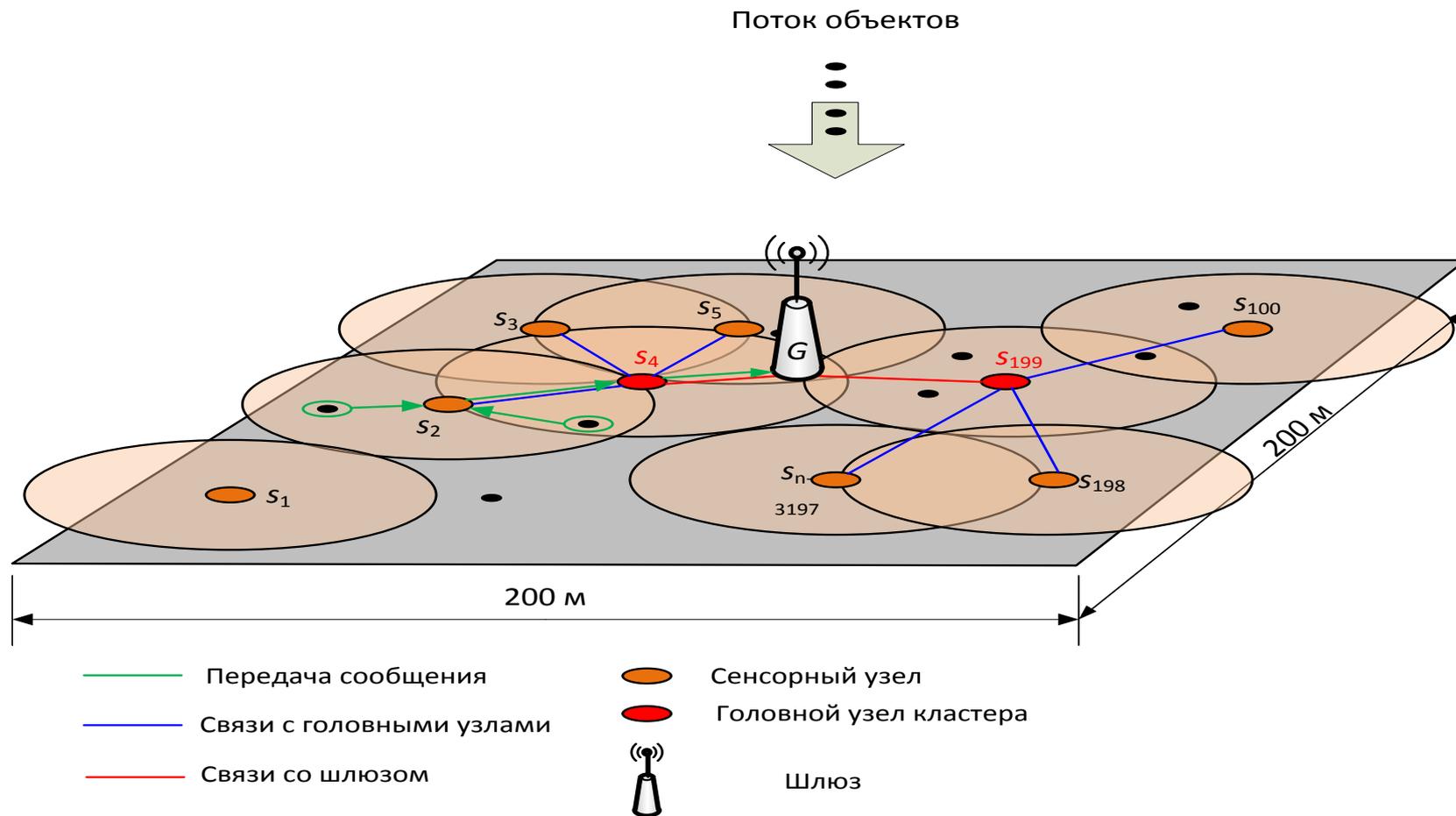
2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

2.3. Отъем энергии



Ложные потоки (энергетические атаки)

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

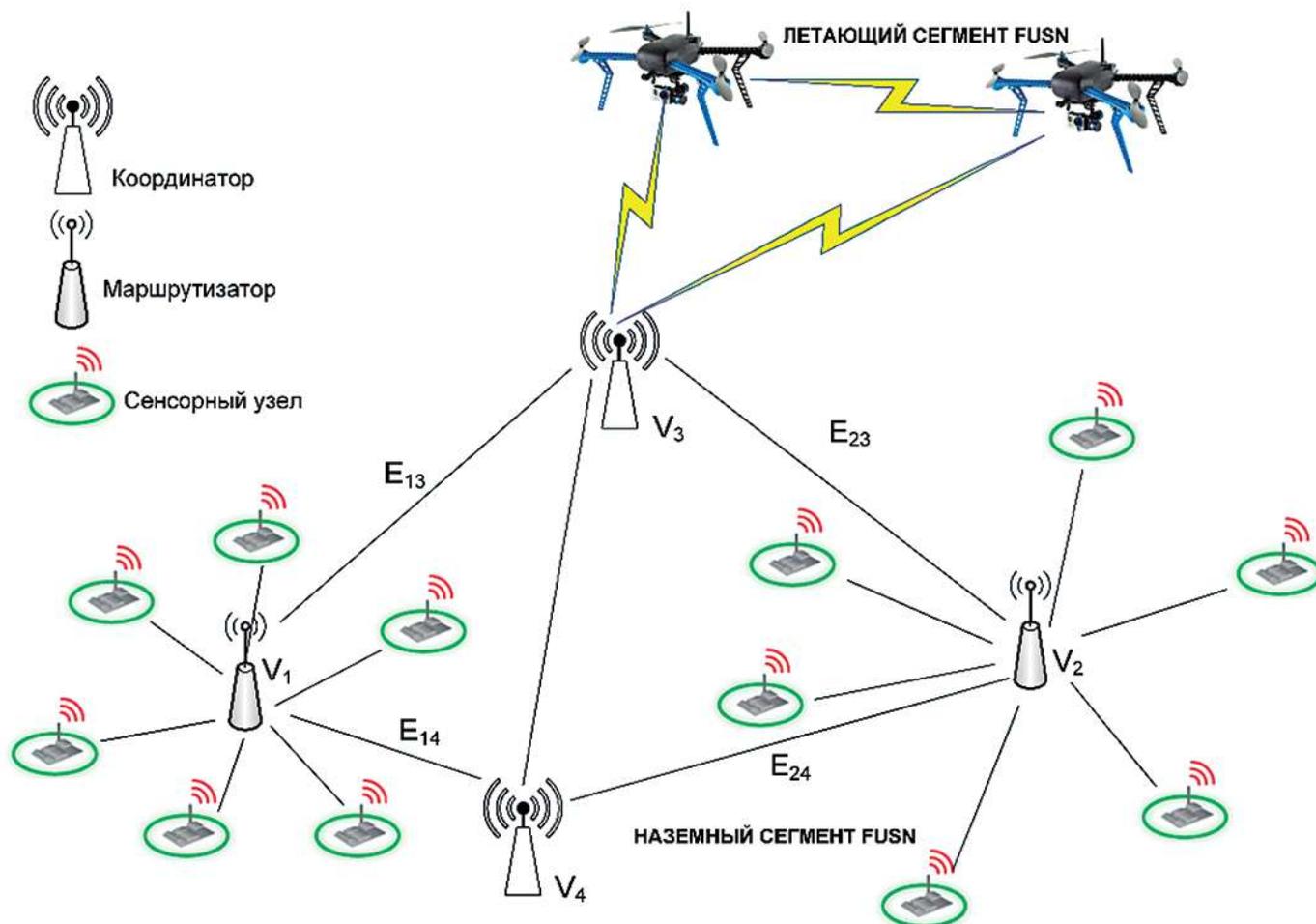
2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

2.4. ЭМ-воздействие



Структура экспериментального стенда

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

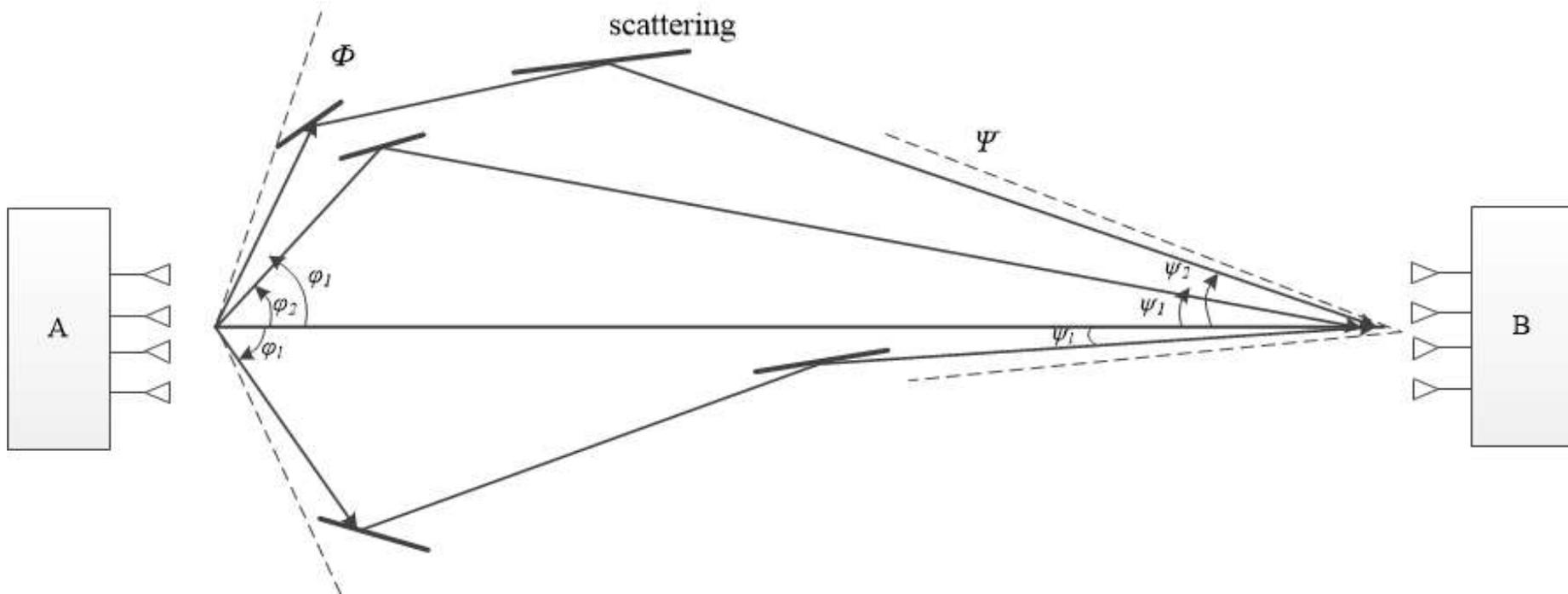
2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

2.1. Пост-квантовая криптография



Общая модель канала с множественным входом и выходом между подвижным пользователем и базовой станцией
(Гданьск, сентябрь 2016 г.)

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

2.2. Стегосистемы и ЦВЗ



81 мин., PAL

Проблемные вопросы

1. Доверенная сеть vs недоверенная телекоммуникационная среда

- 1.1. Доверенная маршрутизация
- 1.2. Проприетарное ПО ТКУ
- 1.3. Архитектурные уязвимости моделей ЦТКС

2. Информационная безопасность vs Интернет Вещей

- 2.1. Ложные облака
- 2.2. Клоны
- 2.3. Отъем энергии
- 2.4. ЭМ-воздействие

3. Крипто vs Стего

- 2.1. Пост-квантовая криптография
- 2.2. Стегосистемы и ЦВЗ

Угрозы, уязвимости, решения

№	Проблема	Угроза	Уязвимость	Решение
1.1	Доверенная маршрутизация	Перенаправление трафика	Алгоритмы маршрутизации	Алгоритмы доверенной маршрутизации
1.2	Проприетарное ПО ТКУ	Программные закладки	Отсутствие исходного кода	Алгоритмизация машинного кода
1.3	Архитектурные уязвимости	Многообразие атак	Дефекты концепций	Синтез безопасных моделей
2.1	Ложные облака	Перенаправление трафика	Клонирование пакетов	Уникальные паттерны трафика
2.2	Клоны	Внедрение ложных объектов	Клонирование узлов	Уникальные паттерны трафика
2.3	Отъем энергии	Сокращение ЖЦ сети	Низкая энергоемкость	Аутентификация и ограничение трафика
2.4	ЭМ-воздействие	Нарушение структуры сети	Низкая энергоемкость	Комбинирование средств защиты
3.1	Пост-квантовая криптография	Компрометация ключей	Возможность перехвата	Физическая генерация потока ключей
3.1	Стегосистемы и ЦВЗ	«Неучтенный» трафик	Скрытые каналы	Статистический анализ

Угрозы, уязвимости, решения

№	Проблема	Угроза	Уязвимость	Решение
1.1	Доверенная маршрутизация	Перенаправление трафика	Алгоритмы маршрутизации	Алгоритмы доверенной маршрутизации
1.2	Проприетарное ПО ТКУ	Программные закладки	Отсутствие исходного кода	Алгоритмизация машинного кода
1.3	Архитектурные уязвимости	Многообразие атак	Дефекты концепций	Синтез безопасных моделей
2.1	Ложные облака	Перенаправление трафика	Клонирование пакетов	Уникальные паттерны трафика
2.2	Клоны	Внедрение ложных объектов	Клонирование узлов	Уникальные паттерны трафика
2.3	Отъем энергии	Сокращение ЖЦ сети	Низкая энергоемкость	Аутентификация и ограничение трафика
2.4	ЭМ-воздействие	Нарушение структуры сети	Низкая энергоемкость	Комбинирование средств защиты
3.1	Пост-квантовая криптография	Компрометация ключей	Возможность перехвата	Физическая генерация потока ключей
3.1	Стегосистемы и ЦВЗ	«Неучтенный» трафик	Скрытые каналы	Статистический анализатор

Угрозы, уязвимости, решения

№	Проблема	Угроза	Уязвимость	Решение
1.1	Доверенная маршрутизация	Перенаправление трафика	Алгоритмы маршрутизации	Алгоритмы доверенной маршрутизации
1.2	Проприетарное ПО ТКУ	Программные закладки	Отсутствие исходного кода	Алгоритмизация машинного кода
1.3	Архитектурные уязвимости	Многообразие атак	Дефекты концепций	Синтез безопасных моделей
2.1	Ложные облака	Перенаправление трафика	Клонирование пакетов	Уникальные паттерны трафика
2.2	Клоны	Внедрение ложных объектов	Клонирование узлов	Уникальные паттерны трафика
2.3	Отъем энергии	Сокращение ЖЦ сети	Низкая энергоемкость	Аутентификация и ограничение трафика
2.4	ЭМ-воздействие	Нарушение структуры сети	Низкая энергоемкость	Комбинирование средств защиты
3.1	Пост-квантовая криптография	Компрометация ключей	Возможность перехвата	Физическая генерация потока ключей
3.1	Стегосистемы и ЦВЗ	«Неучтенный» трафик	Скрытые каналы	Статистический анализатор

Угрозы, уязвимости, решения

№	Проблема	Угроза	Уязвимость	Решение
1.1	Доверенная маршрутизация	Перенаправление трафика	Алгоритмы маршрутизации	Алгоритмы доверенной маршрутизации
1.2	Проприетарное ПО ТКУ	Программные закладки	Отсутствие исходного кода	Алгоритмизация машинного кода
1.3	Архитектурные уязвимости	Многообразие атак	Дефекты концепций	Синтез безопасных моделей
2.1	Ложные облака	Перенаправление трафика	Клонирование пакетов	Уникальные паттерны трафика
2.2	Клоны	Внедрение ложных объектов	Клонирование узлов	Уникальные паттерны трафика
2.3	Отъем энергии	Сокращение ЖЦ сети	Низкая энергоемкость	Аутентификация и ограничение трафика
2.4	ЭМ-воздействие	Нарушение структуры сети	Низкая энергоемкость	Комбинирование средств защиты
3.1	Пост-квантовая криптография	Компрометация ключей	Возможность перехвата	Физическая генерация потока ключей
3.1	Стегосистемы и ЦВЗ	«Неучтенный» трафик	Скрытые каналы	Статистический анализатор

Угрозы, уязвимости, решения

№	Проблема	Угроза	Уязвимость	Решение
1.1	Доверенная маршрутизация	Перенаправление трафика	Алгоритмы маршрутизации	Алгоритмы доверенной маршрутизации
1.2	Проприетарное ПО ТКУ	Программные закладки	Отсутствие исходного кода	Алгоритмизация машинного кода
1.3	Архитектурные уязвимости	Многообразии атак	Дефекты концепций	Синтез безопасных моделей
2.1	Ложные облака	Перенаправление трафика	Клонирование пакетов	Уникальные паттерны трафика
2.2	Клоны	Внедрение ложных объектов	Клонирование узлов	Уникальные паттерны трафика
2.3	Отъем энергии	Сокращение ЖЦ сети	Низкая энергоемкость	Аутентификация и ограничение трафика
2.4	ЭМ-воздействие	Нарушение структуры сети	Низкая энергоемкость	Комбинирование средств защиты
3.1	Пост-квантовая криптография	Компрометация ключей	Возможность перехвата	Физическая генерация потока ключей
3.1	Стегосистемы и ЦВЗ	«Неучтенный» трафик	Скрытые каналы	Статистический анализатор

Тенденции

- ❑ Обеспечение инфраструктурной составляющей информационного суверенитета России (обеспечение концепции доверенных сетей)
- ❑ Смещение акцентов от классической криптографии к пост-квантовой и компьютерной стеганографии
- ❑ Погружение проблематики информационной безопасности в «микромир» телекоммуникаций – Интернет Вещей
- ❑ Моделирование и прогнозирование угроз информационной безопасности архитектурных концепций перспективных ЦТКС

Использованная литература. Проблемные вопросы 1.N

1. **Буйневич М.В., Владыко А.Г., Доценко С.М., Симонина О.А.** Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования. СПб.: СПбГУТ, 2013. 144 с.
2. **Тиамийу О.А.** Устройство доверенной маршрутизации в телекоммуникационных сетях // Патент на полезную модель RU 150245. Опубл. 10.02.2015. Бюл. № 4.
3. **Тиамийу О.А.** Доверенная маршрутизация vs MPLS: безопасность данных, качество обслуживания и масштабируемость // Информационные технологии и телекоммуникации. 2013. №. 3(3). С. 4-39.
4. **Тиамийу О.А.** Выбор и обоснование алгоритма определения топологии сети в интересах доверенной маршрутизации // Информационные технологии и телекоммуникации. 2014. – Вып. 1(5). – С. 54-66.
5. **Буйневич М.В., Тиамийу О.А.** Программная архитектура системы управления доверенной маршрутизацией в глобальных телекоммуникационных сетях // Информатизация и связь. 2014. № 3. С. 35-38.
6. **Буйневич М.В., Осуолале Т.А.** Имитационные эксперименты с моделью полносвязной телекоммуникационной сети по исследованию механизма доверенной маршрутизации // Телекоммуникации. 2014. № 2. С. 06-15.
7. **Буйневич М.В., Израилов К.Е.** Автоматизированное средство алгоритмизации машинного кода телекоммуникационных устройств // Телекоммуникации. 2013. № 6. С. 2-9.
8. **Буйневич М.В., Израилов К.Е.** Метод алгоритмизации машинного кода телекоммуникационных устройств // Телекоммуникации. 2012. № 12. С. 2–6.
9. **Буйневич М.В., Щербаков О.В., Израилов К.Е.** Структурная модель машинного кода, специализированная для поиска уязвимостей в программном обеспечении автоматизированных систем управления // Проблемы управления рисками в техносфере. 2014. № 3(31). С. 68-74.
10. **Buinevich M., Izrailov K., Vladyko A.** Method and prototype of utility for partial recovering source code for low-level and medium-level vulnerability search // 18th International Conference on Advanced Communication Technology (ICACT). 2016. С. 700-707.
11. **Buinevich M., Izrailov K., Vladyko A.** Method for partial recovering source code of telecommunication devices for vulnerability search // 17th International Conference On Advanced Communications Technology (ICACT). 2015. С. 76-80.
12. **Buinevich M., Izrailov K.** Method and utility for recovering code algorithms of telecommunication

Использованная литература. Проблемные вопросы 2.N

1. **Киричек Р.В., Кулик В.А., Владыко А.Г., Богданов И.А., Кучерявый А.Е.** Ложные облака для интернета вещей. Методы защиты // Информационные технологии и телекоммуникации. 2015. № 3 (11). С. 27-39.
2. **Kirichek R., Kulik V., Koucheryavy A.** False clouds for internet of things and methods of protection // 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 201-205.
3. **Кучерявый А.Е., Владыко А.Г., Киричек Р.В.** Теоретические и практические направления исследований в области летающих сенсорных сетей // Электросвязь. 2015. № 7. С. 9-11.
4. **Koucheryavy A., Vladuko A., Kirichek R.** State of the Art and Research Challenges for Public Flying Ubiquitous Sensor Networks // Lecture Notes in Computer Science. 2015. Vol. 9247. pp. 299-308.
5. **Епихин А.О., Киричек Р.В., Кучерявый А.Е.** Анализ жизненного цикла беспроводной сенсорной сети с использованием имитационного моделирования // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. С. 505-508.
6. **Киричек Р.В., Нгуен Д.К.** Исследование влияния потока ложных запросов в беспроводных сенсорных сетях на разряд батареи питания конечных узлов // Информационные технологии и телекоммуникации. 2015. № 1(9). С. 128-138.
7. **Кучерявый А.Е., Киричек Р.В., Парамонов А.И., Прокопьев А.В.** Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4. С. 29-41.
8. **Разумов А.А., Киричек Р.В.** Исследование устойчивости фрагмента летающей сенсорной сети к воздействию сверхкоротких электромагнитных импульсов // Электросвязь. 2015. № 9. С. 15-17.

Использованная литература. Проблемные вопросы 3.N

1. **Коржик В.И., Яковлев В.А., Тихонов С.В.** Бесключевая криптосистема с обеспечением секретности на физическом уровне: миф или реальность // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 79-89.
2. **Yakovlev V., Korzhik V., Morales-Luna G.** Key Distribution Protocols Based on Noisy Channels in Presence of an Active Adversary: Conventional and New Versions with Parameter Optimization // IEEE Transactions on Information Theory. 2008. Vol. 54. Iss. 6. pp. 2535-2549.
3. **Korzhik V., Yakovlev V., Ovechkin D., Kovajkin Y., Morales-Luna G.** Wireless Secret Key Sharing Based on the Use of a Variable-directional Antenna Over Multipath Channels // International Symposium Electronics in Marine. 52nd International Symposium, ELMAR-2010. Croatia, Zadar, 2010. pp. 277-279.
4. **Yakovlev V., Korzhik V., Bakaev M., Morales-Luna G.** Optimization of Key Distribution Protocols Based on Extractors for Noisy Channels within Active Adversaries // Lecture Notes in Computer Science. 2012. Vol. 7531. pp. 51-64.
5. **Korzhik V., Fedyanin I.** Steganographic Applications of the Nearest-Neighbor Approach to Kullback-Leibler Divergence Estimation // 3rd International Conference on Digital Information, Networking, and Wireless Communications (DINWC). 2015. pp. 133-138.
6. **Korzhik V., Morales-Luna G. Fedyanin I.** Design of high speed stegosystem based on trellis codes jointly with generalised Viterbi algorithm// International Journal of Computer Science and Applications. 2016. Vol. 13, No. 2, pp. 1-15.
7. **Герлинг Е.Ю., Догиль П.С., Кордик В.И., Небаева К.А., Федянин И.А.** Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография / Под. ред . В.И. Коржика, СПб.: СПбГУТ, 2016. 225 с.
8. **Korzhik V., Nebaeva K., Aleksejevs M., Morales-Luna G.** A Stegosystem with Blind Decoder Based on a Noisy Channel // 18th International Conference on Digital Signal Processing (DSP-2013). 2013. pp. 1-5.
9. **Коржик В.И., Федянин И.А., Копылова О.Д.** Синтез высокоскоростных стегоалгоритмов устойчивых к «слепому» стегоанализу // Вопросы защиты информации. 2014. № 2 (105). С. 51-56.
10. **Коржик В.И., Кочкарев А.И., Флакман Д.А.** Система цифровых водяных знаков с повторным вложением информации по различным алгоритмам // Телекоммуникации. 2014. 41 № 7. С. 22-33.
11. **Korzhik V., Kochkarev A., Flaxman D., Morales-Luna G.** Concatenated Digital Watermarking

СПб ГУТ)))



Благодарю за внимание!

2 сентября 2016 г.