ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

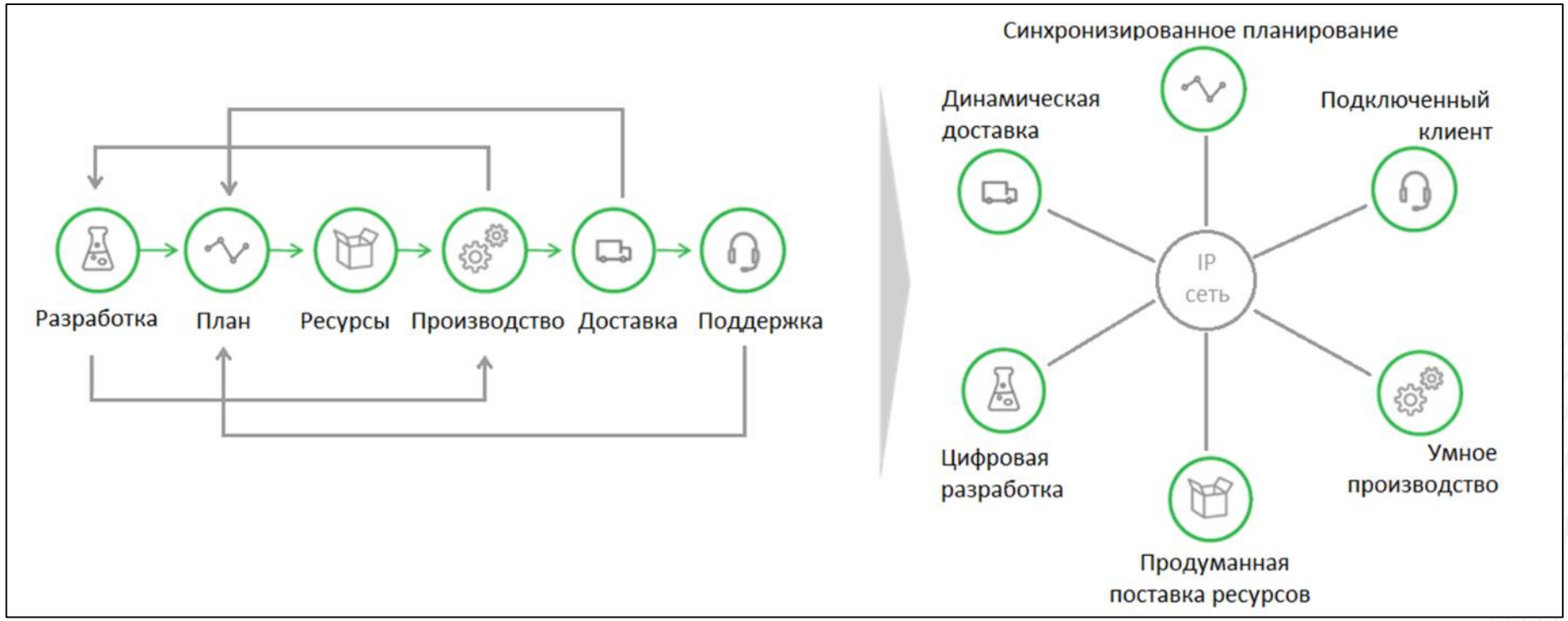
Применение чесночной маршрутизации для обеспечения безопасного взаимодействия сегментов сети цифрового производства

Зегжда Д.П., Москвин Д.А., Дахнович А.Д.

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение № 14.578.21.0231, уникальный идентификатор соглашения RFMEFI57817X0231).

Отличительные признаки цифрового производства

ЦП – промышленный процесс, контролируемый SCADA и подобными системами, связанных по сети и взаимодействующих на всех этапах производства (цепочки создания ценности) для образования умной производственной системы (SPS).



Интернет Вещей как драйвер цифрового производства

Устройства Интернета Вещей:

- Взаимодействуют с физическим миром
- Имеют коммуникации (устройство-человек, устройство-устройство, устройство-много устройство)
- Поддерживают некоторую обработку данных (принимают самостоятельные решения)

По Gartner, к 2020 году будет **20,6 млн.** подключенных к сети устройств IoT.

По Jupiter Research – **38.5** млн. устройств

Статистика атак на «умные устройства»

С 2016 года ботнеты

- Mirai (380 тыс. устройств)
- IOtroop (более 1 млн. организаций)
- Doubledoor (без оценки)

По данным The SpamHaus Project, в 2017 выявлено ~9500 C&C серверов ботнетов.

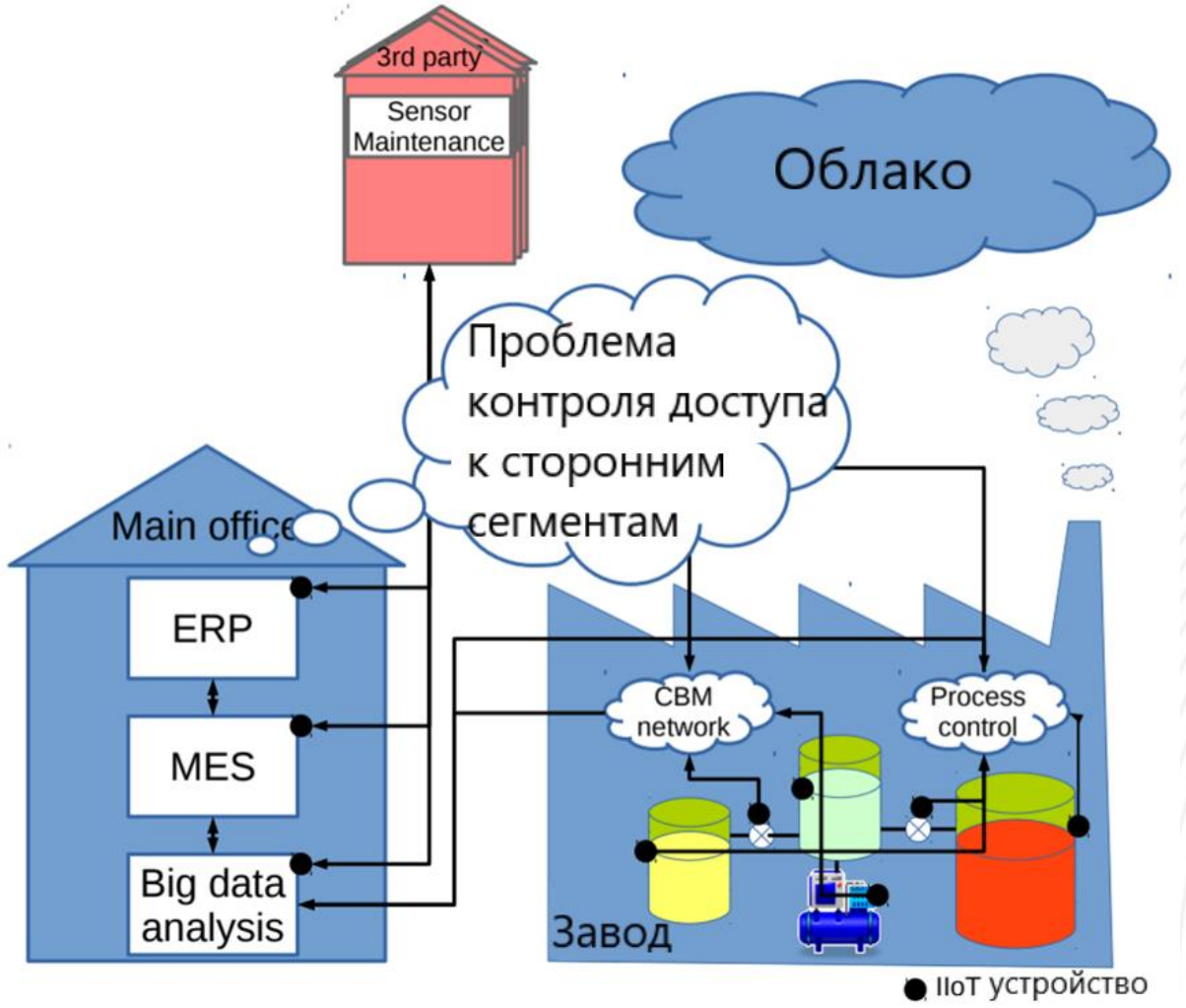
На втором месте – вредоносное ПО для IoT. С 2016 количество почти утроилось (с 393 до 943 шт.)

Взаимодействие между сегментами сети цифрового производства

Устройств становится больше, производство становится «умнее»

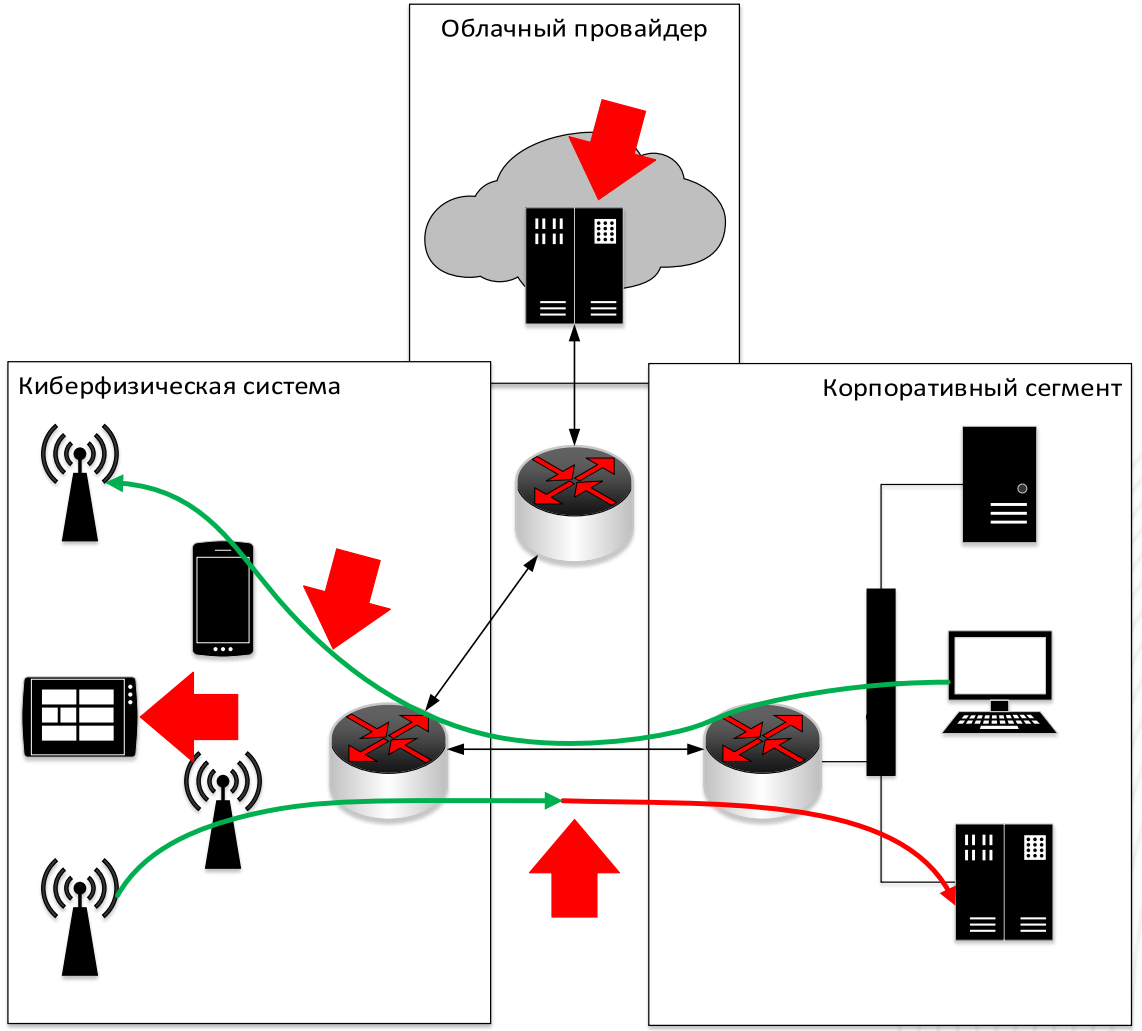
Для поддержания работоспособности «умного производства» необходимо вмешательство сторонних экспертов (провайдеров)

Появляется взаимодействие с внешними поставщиками, т.е. различными сегментами сети



Угрозы безопасности при организации взаимодействия между сегментами сети цифрового производства

- Атаки на умное устройство (ОС, ПО)
- Атаки на каналы связи (получение информации и модификация данных)
- Атаки на сторонних провайдеров услуг



Статистика угроз безопасности АСУ ТП

За 2017 год 54% компаний подвергались атакам на системы АСУ ТП (по данным Business Advantage).

Из них наиболее распространены:

1. Классические угрозы от компьютерных вирусов
2. Угрозы от сторонних сегментов (партнеры, вендоры, участники цепи поставок)
3. Умышленное нанесение ущерба изнутри сети
4. Целенаправленные атаки (APT)

Основные задачи безопасности и требования к средствам защиты в сетях цифрового производства

Должны обеспечивать защиту ЦП как от внешнего, так и от внутреннего нарушителя и решать следующие задачи:

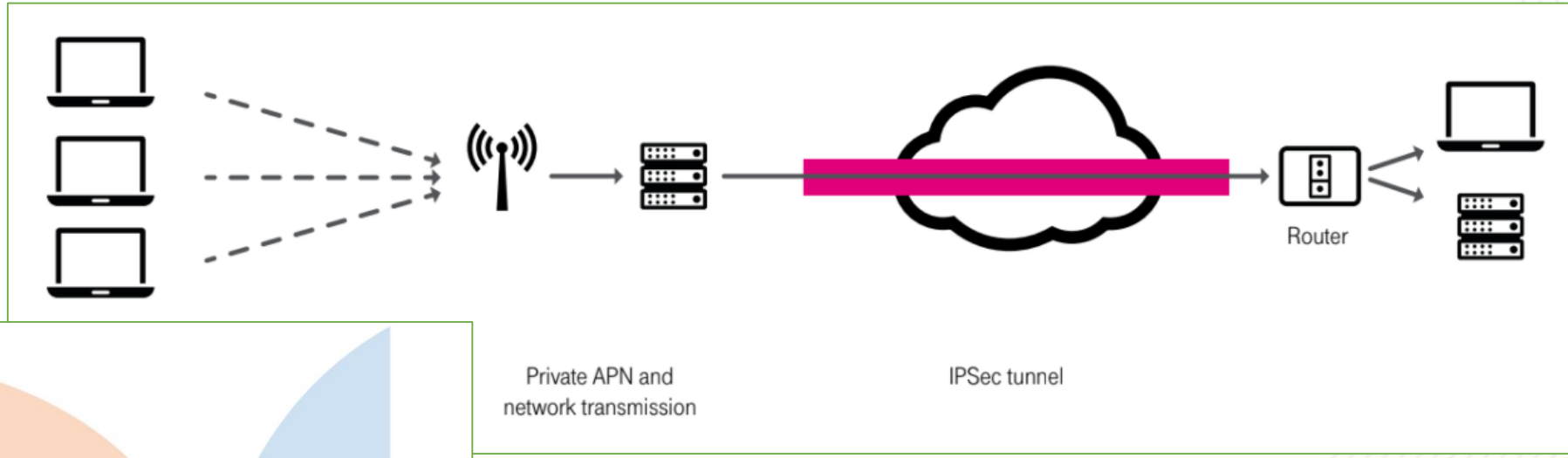
1. Разграничение доступа между сегментами и/или устройствам
2. Обеспечение безопасного обмена данными как между сегментами, так и внутри него

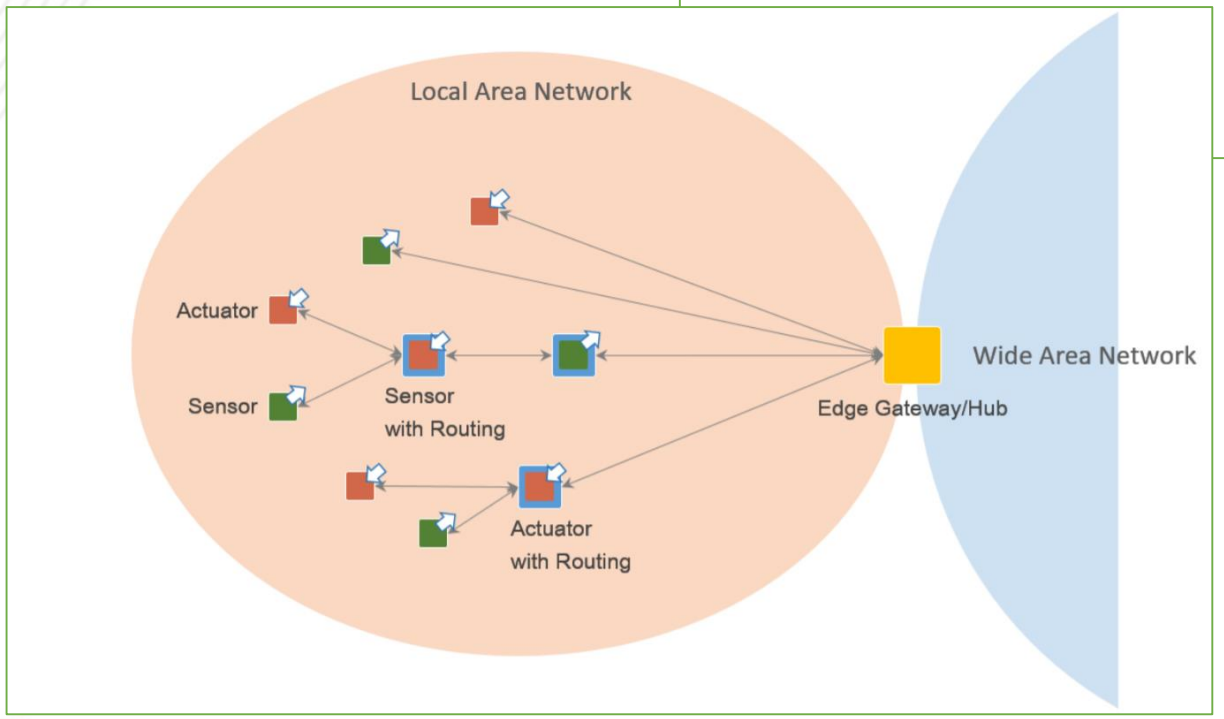
При этом средства защиты должны быть:

- Масштабируемыми (гранулированными)
- Не влиять на скорости работы (Real-Time)

Применяемые средства защиты в сетях ЦП

Криптографические средства защиты сети (VPN, TLS)





Ограничение доступа между сегментами сети с помощью специализированных шлюзов (Gateway).

Недостатки существующих средств защиты

VPN

- Не защищает от внутреннего нарушителя
- Плохо масштабируется в IoT

Шлюз

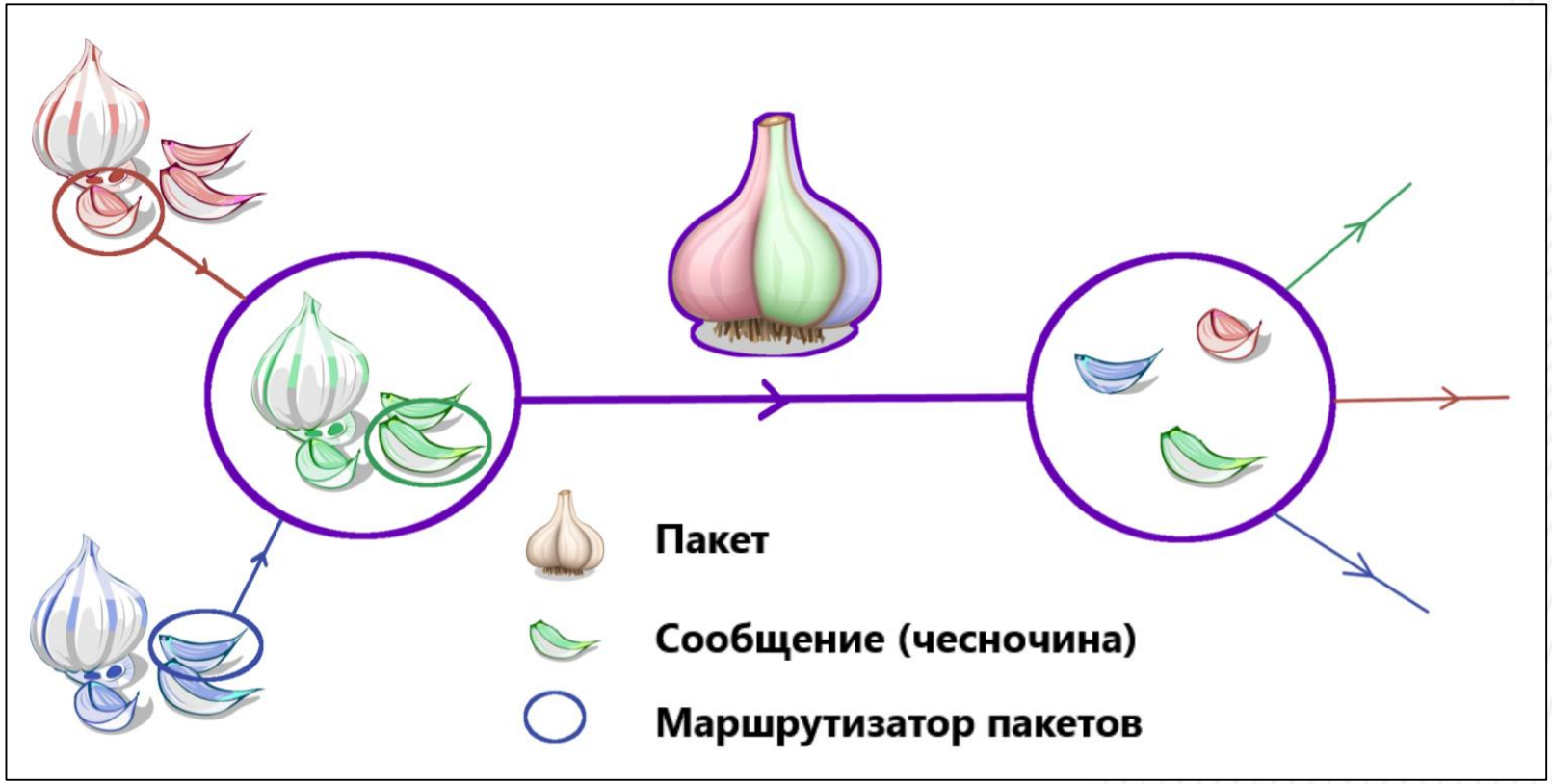
- Не позволяет детализированно разграничивать доступ к конкретным узлам сегмента без раскрытия особенностей инфраструктуры и ТП
- Не защищает от внутреннего нарушителя
- Единая точка отказа

Принципы чесночной маршрутизации

Чесночная маршрутизация – надстройка над луковой для защиты от атак анализа трафика.

Чеснок – пакет, передаваемый между устройствами.

Чесночины – сообщения от источников к адресатам.



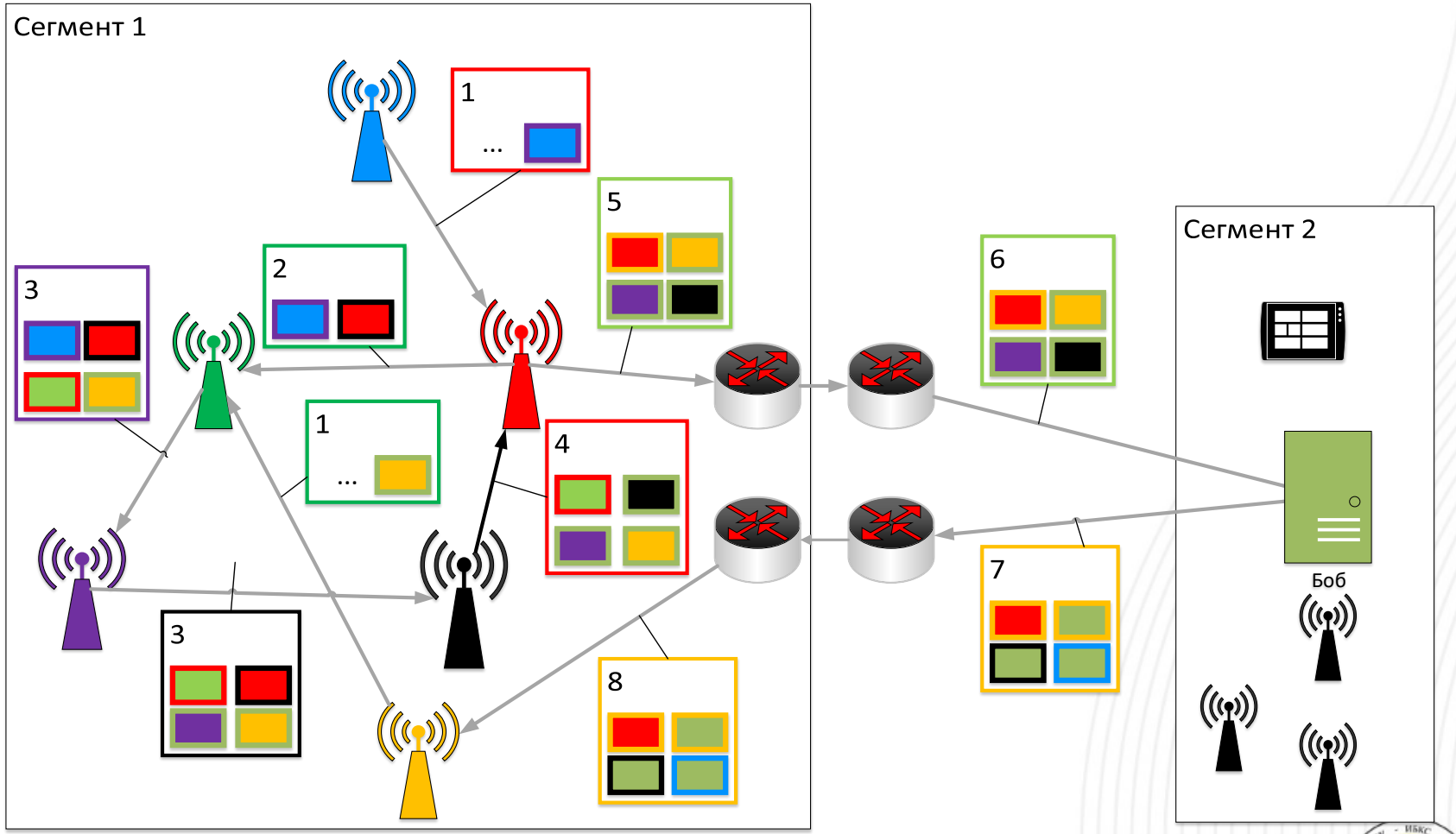
Применение чесночной маршрутизации для обеспечения безопасности ЦП

Сообщение *M*:

- $M = f(x_1) + f(x_2) + \ldots + f(x_n)$, где

$f(x_i)$ – зашифрованное «сообщение-чесночина»

- Size(*M*) = *const*
- «Сообщение-чесночину» может расшифровать только получатель.



База данных маршрутизации сегмента

Сегмент имеет свою база данных маршрутизации.

Таблицы 2-х типов:

1. Inbound – таблица о разрешенных входящих подключения
2. Outbound – таблица о разрешенных исходящих подключениях

Запись в таблице:

Таблица маршрутизации	
Адрес 1	$РК_1$, $РК_2$
Адрес 2	$РК_1$, $РК_2$

Узел – устройство или сегмент.

Каждый узел имеет:

- Ключ шифрования
- Ключ подписи

} Идентификатор узла

- Адрес (например, IP)

Пример реализация базы данных маршрутизации

Базы основного сегмента

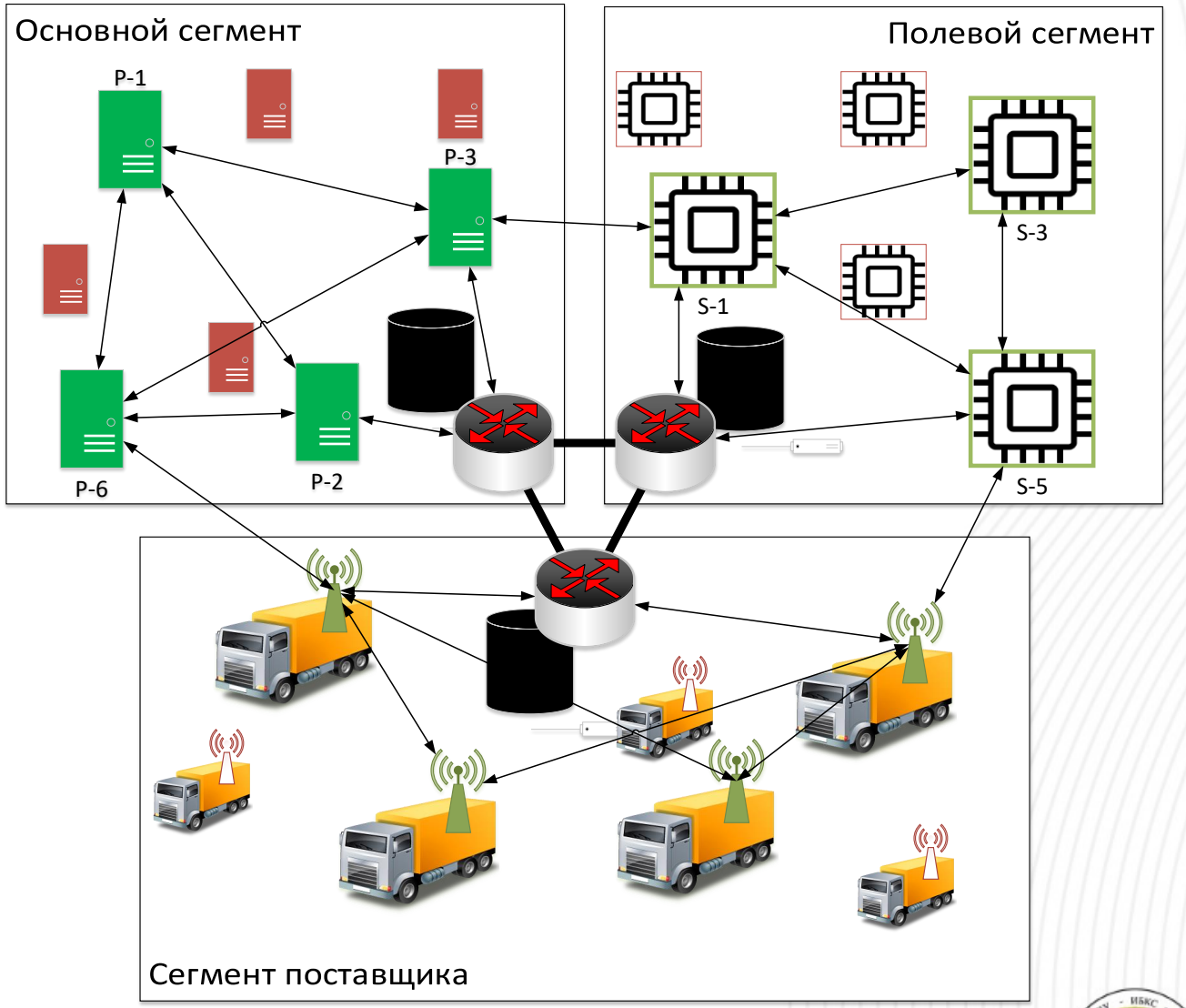
Inbound «Полевой сегмент»	
P-1	…
P-2	…
P-3	…
P-6	…

Outbound «Полевой сегмент»	
S-1	…
S-3	…
S-5	…

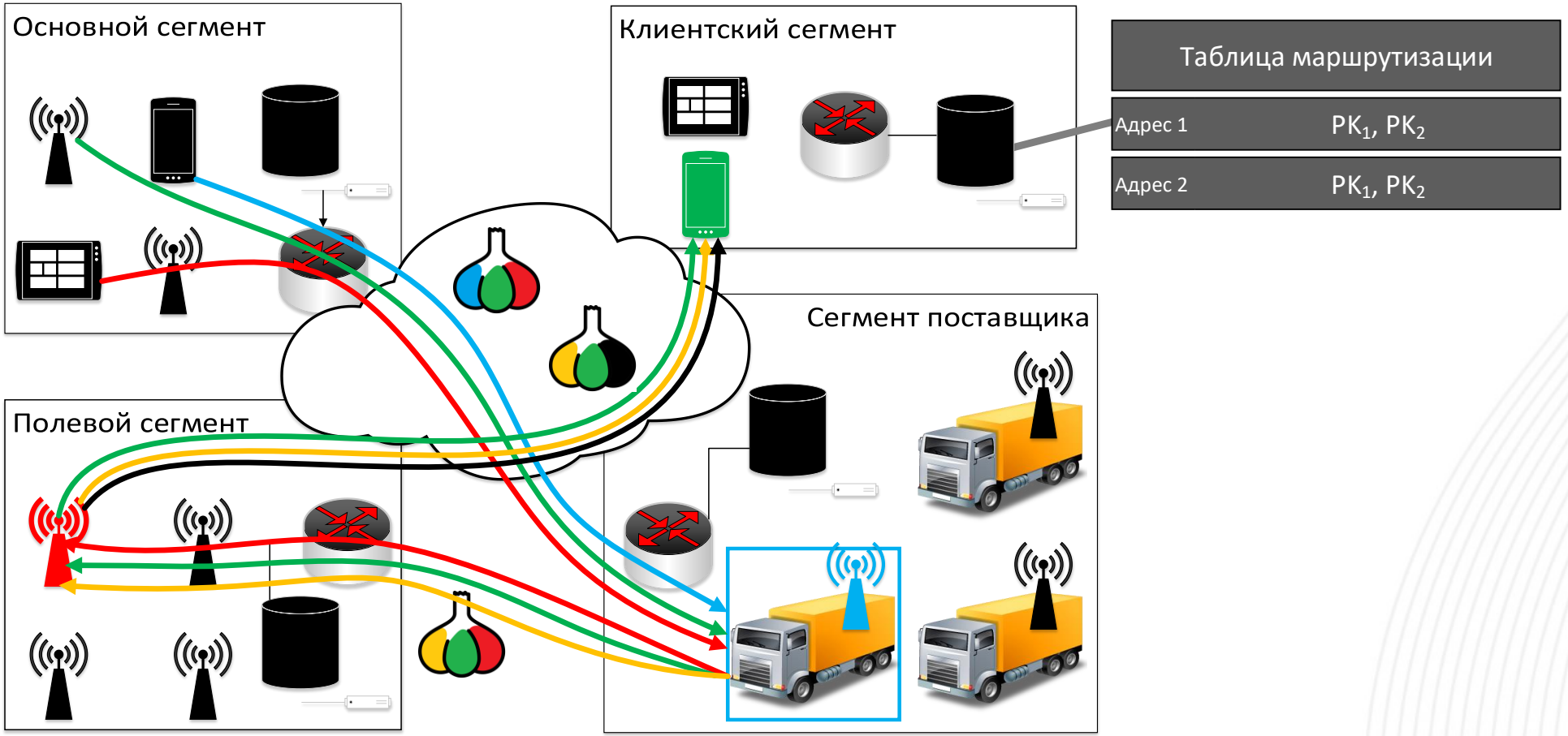
Inbound «Сегмент поставщика»

Outbound «Сегмент поставщика»

…

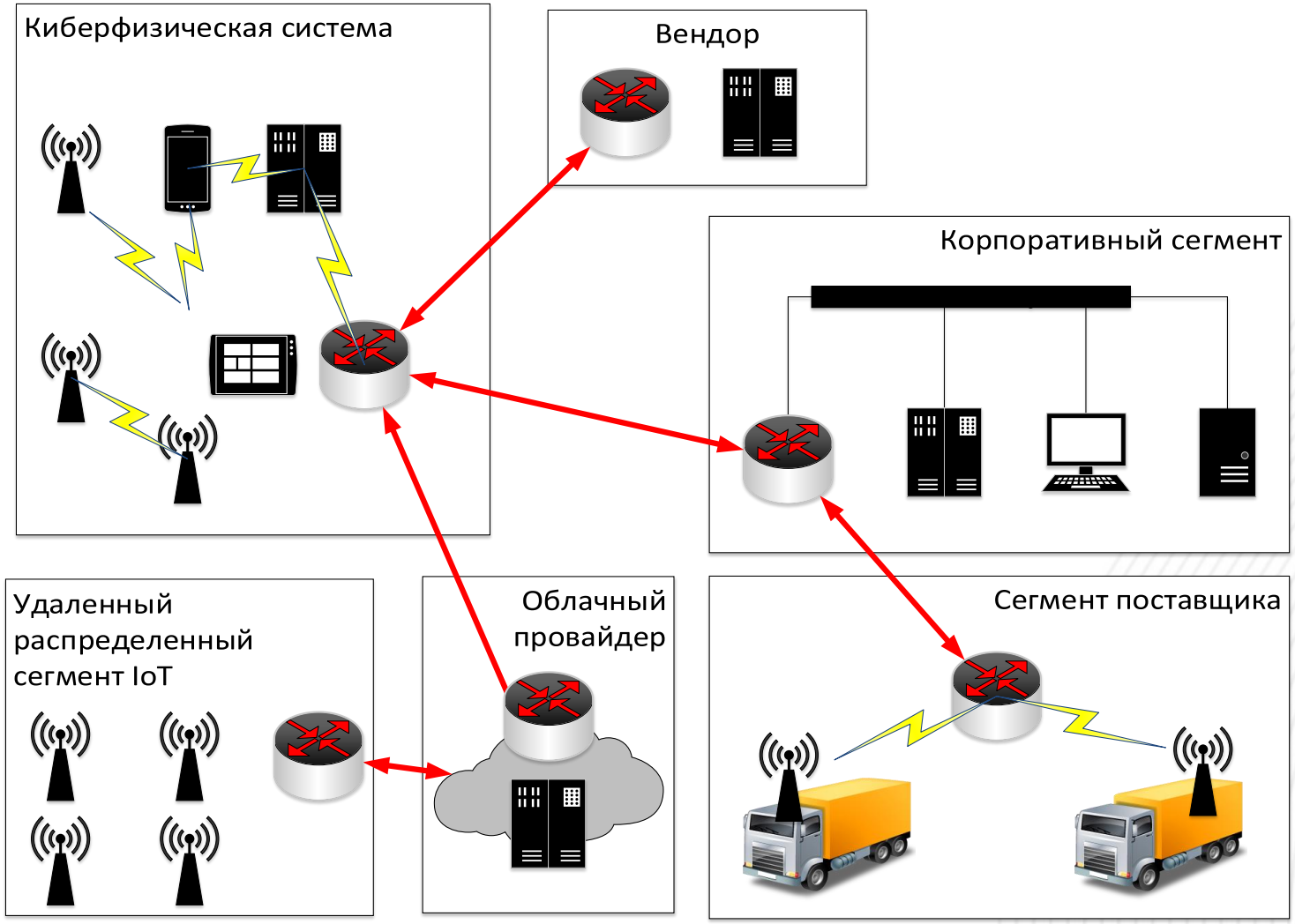


Маршрутизация сообщений в сети цифрового производства



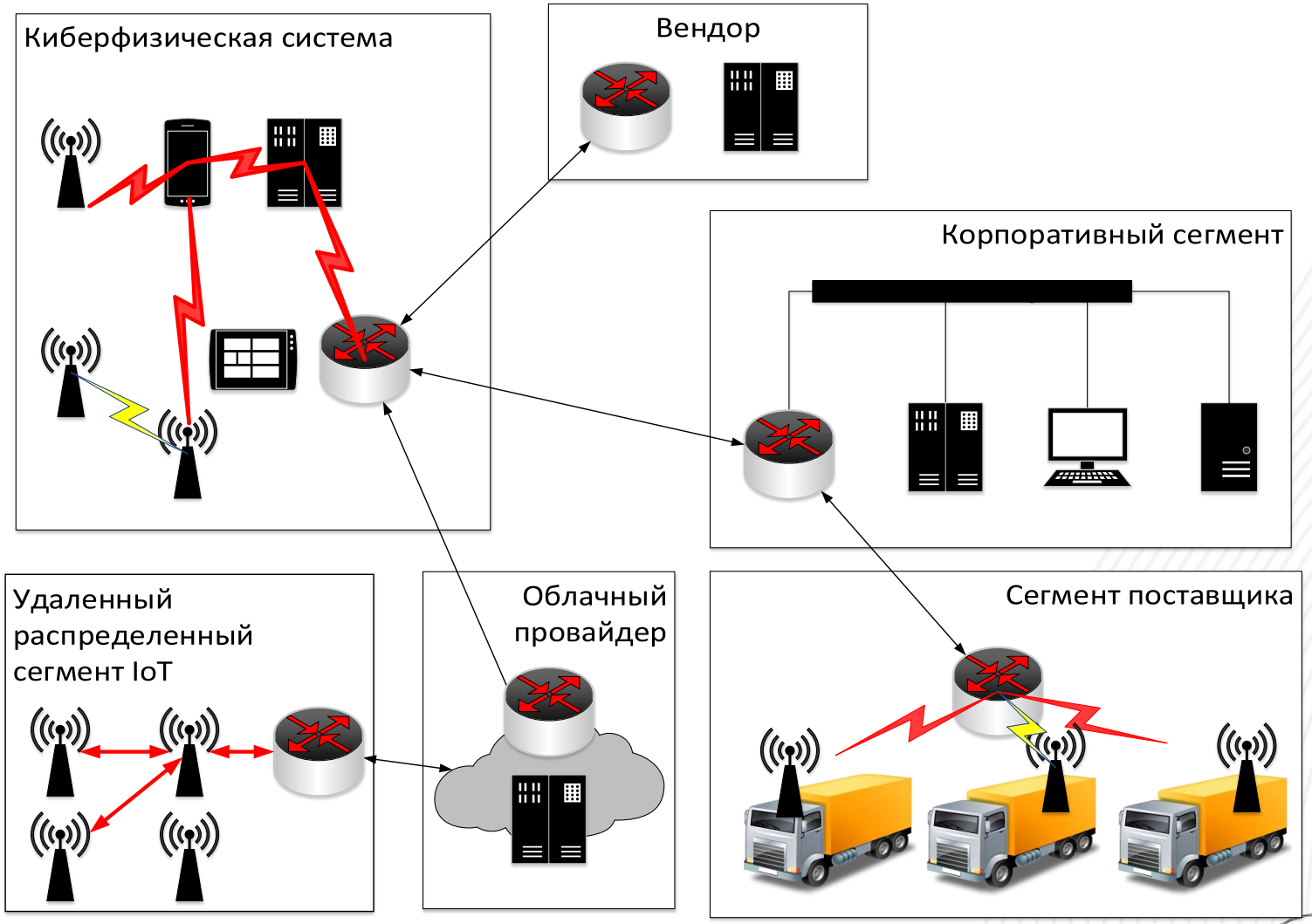
Защита от внешнего нарушителя

- Защита данных от внешнего нарушителя с помощью стандартных криптографических средств.



Защита от внутреннего нарушителя

- Защита от раскрытия информации о сети
- Шифрование каждой чесночины по-отдельности не влечет раскрытие информации, передаваемых с других устройств
- Подпись защищает данные от подделки



Преимущества применения чесночной маршрутизации

- Гибкое разграничение доступа к данным между сегментами сети
- Сокрытие внутренней инфраструктуры сегментов
- Защита как от внутреннего, так и внешнего нарушителя

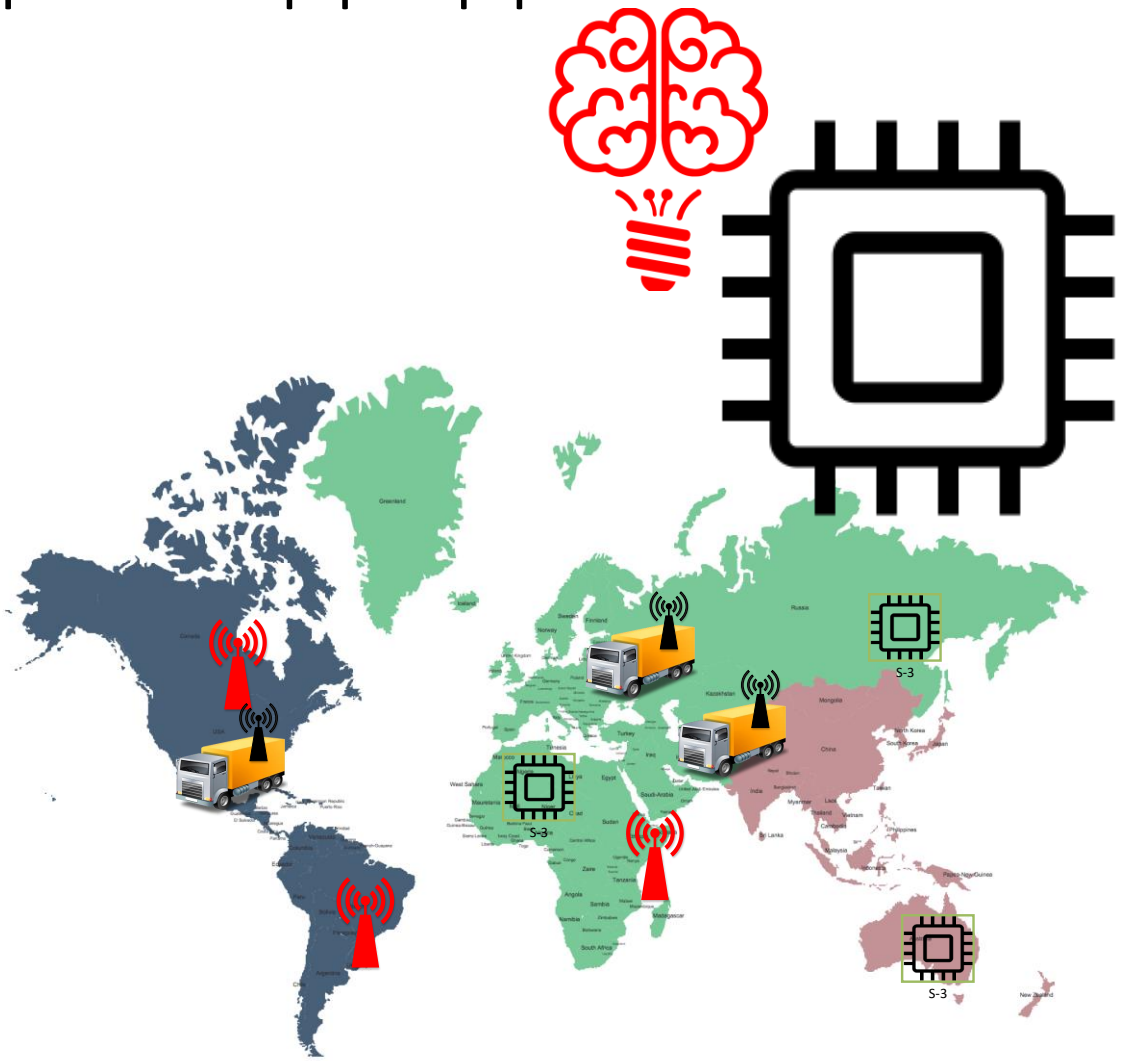
Дополнительно:

- Обеспечение доступности информации благодаря возможности отправки сообщений по нескольким маршрутам
- Масштабируемость решения
- Независимость от протоколов сетевого уровня

Недостатки реализации подхода

- Требует криптографических операций на стороне «умных устройств»

- Реализация на географически удаленных сегментах может привести к неоправданным задержкам доставки сообщений



ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

Спасибо за внимание

Применение чесночной маршрутизации для обеспечения безопасного взаимодействия сегментов сети цифрового производства

Зегжда Д.П., Москвин Д.А., Дахнович А.Д.

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение № 14.578.21.0231, уникальный идентификатор соглашения RFMEFI57817X0231).