SECURITY
ARCHITECTURE

Безопасность в мире IOT: Вьвовы и Стратегии

Холод Денис и Молодёнова Александра

МТС: кластер «IOT и Умный дом»

SECURITY
ARCHITECTURE

О себе

МТС: архитектура ИБ

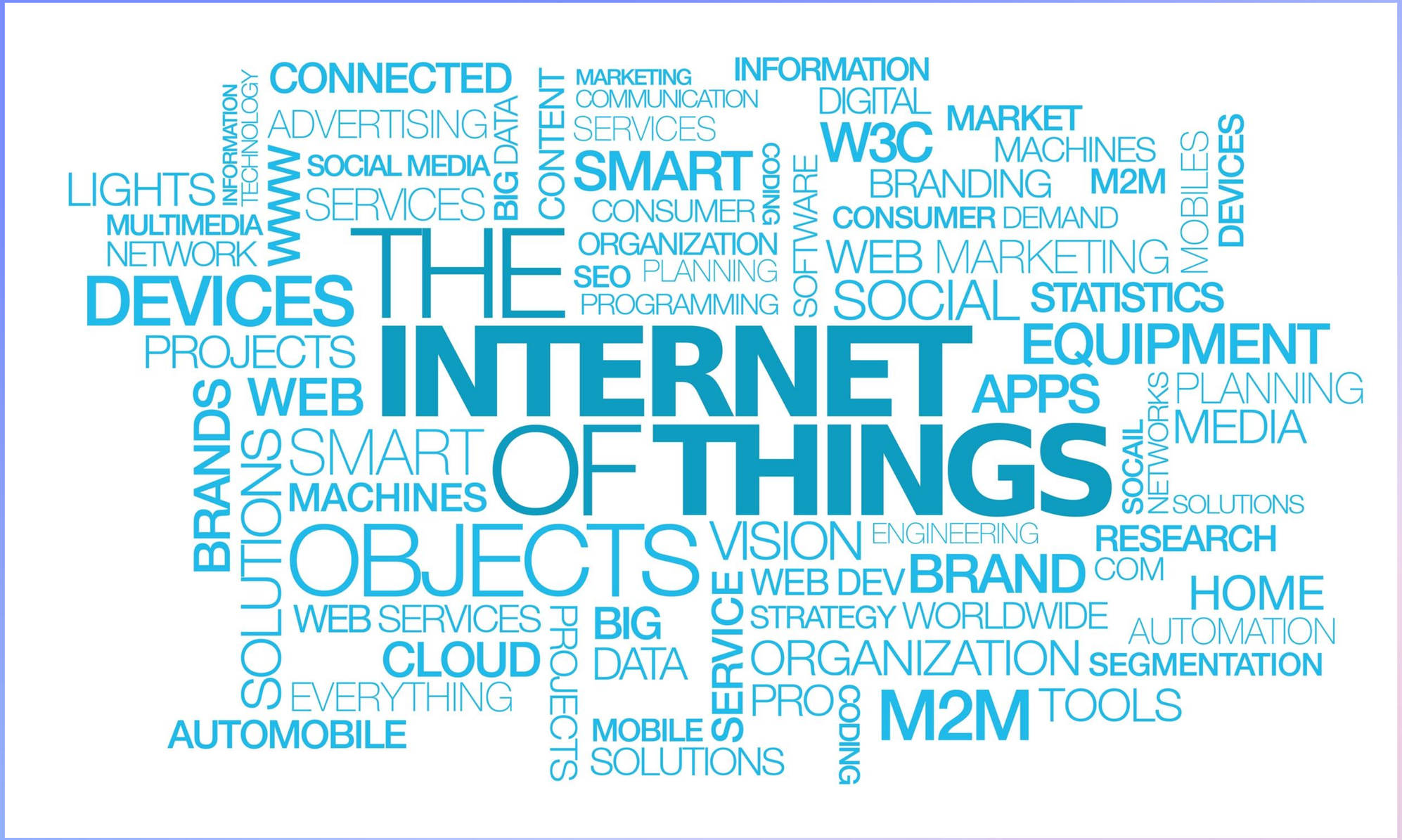
Кластер Умный дом&IOT

Холод Денис

Молодёнова
Александра

SECURITY
ARCHITECTURE

Актуальность IoT



SECURITY
ARCHITECTURE

Хайп vs Security

- Инновационные возможности и
- Повышение безопасности
- Смарт-ритейл
- Экологические преимущества
- Умный дом
- Повышение эффективности
- Улучшение качества обслуживания
- Экологические приемущества
- Мониторинг и управление
- Автономные транспортные средства
- Умное здравоохранение
- Улучшение пользовательского опыта
- Экономия ресурсов
- Умный город

SECURITY
ARCHITECTURE

Мир интернета вещей глазами...

Потребителей

Разработчиков

Специалистов ИБ

SECURITY
ARCHITECTURE

Вызовы интернета вещей

1

Безопасность не успевает за развитием IoT
Проблемы развития НПА и формирования границ доверия

2

Камни преткновения на этапах жизненного цикла устройств IoT
Путь от формирования требований до эксплуатации

3

Эксплуатация = возможная компрометация
Необходимость кастомизации требований ИБ для устройств IoT

4

Неконтролируемый рост устройств IoT
Последствия масштабирования «умных» технологий

SECURITY
ARCHITECTURE

Безопасность не успевает за IoT

Регуляторное покрытие

Размытые границы доверия

Небезопасные интеграции

Привязка к аппаратной реализации

Базовая модель угроз для IoT устройств

Стандарты и спецификации проектирования безопасной архитектуры IoT решений

Регуляторное покрытие как промышленного IoT так и бытового

SECURITY ARCHITECTURE

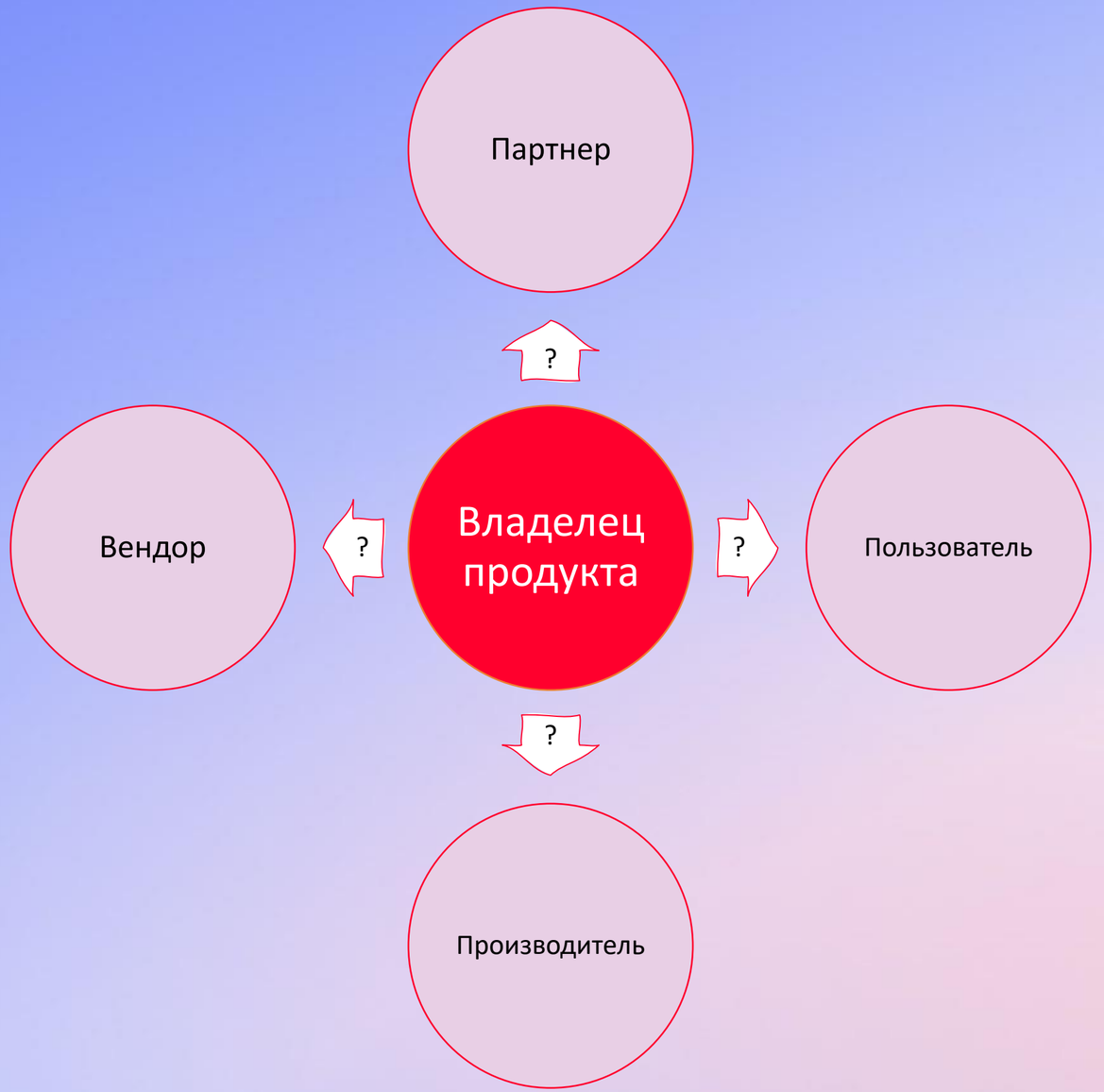
Безопасность не успевает за IoT

Регуляторное покрытие

Размытые границы доверия

Небезопасные интеграции

Привязка к аппаратной реализации



SECURITY ARCHITECTURE

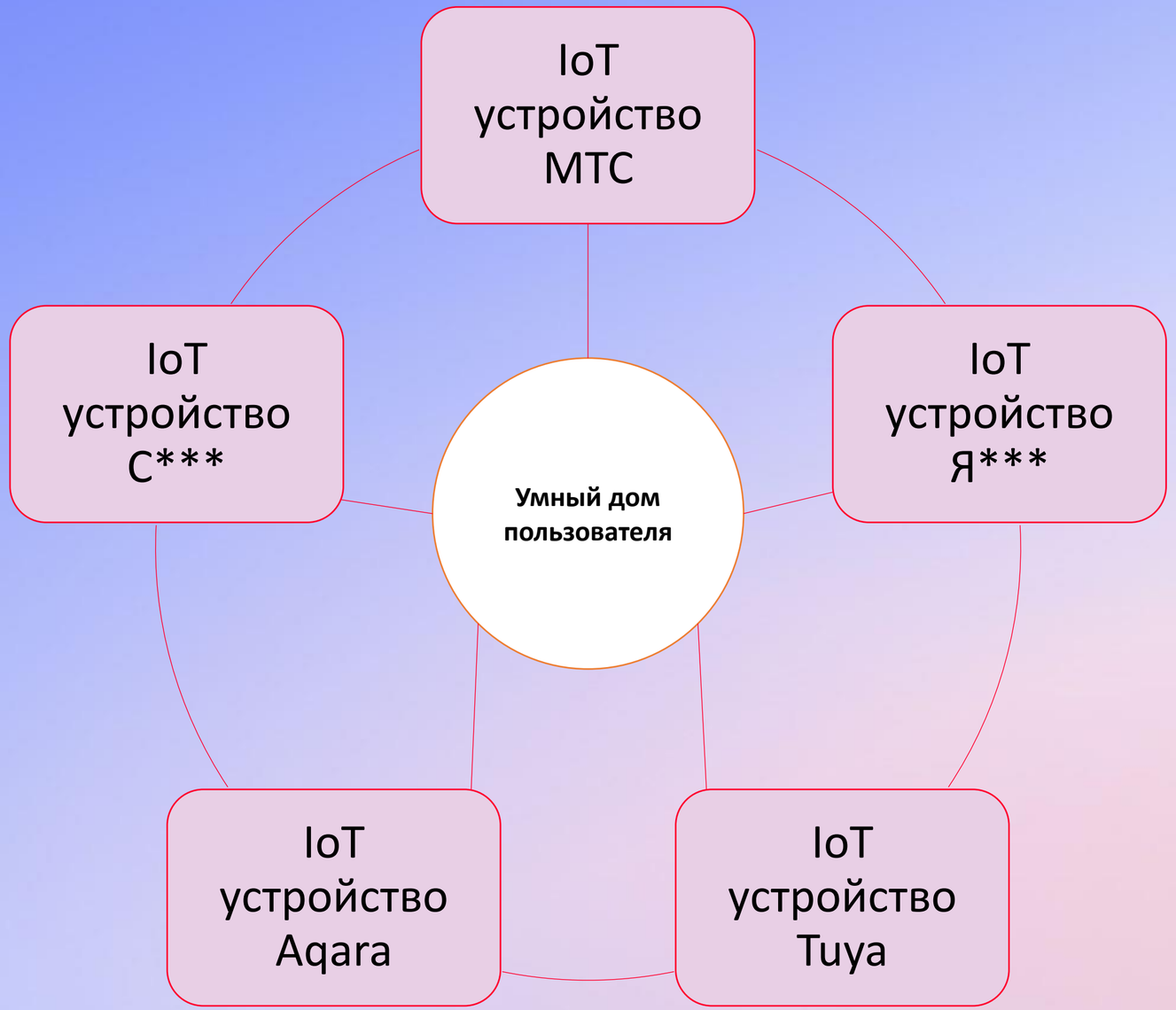
Безопасность не успевает за IoT

Регуляторное покрытие

Размытые границы доверия

Небезопасные интеграции

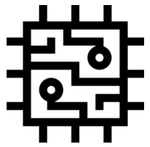
Привязка к аппаратной реализации



SECURITY
ARCHITECTURE

Безопасность не успевает за IoT

- Регуляторное покрытие
- Размытые границы доверия
- Небезопасные интеграции
- **Привязка к аппаратной реализации**



Огромное количество IoT устройств с уязвимой аппаратной реализацией

Новые уязвимости аппаратных протоколов

Доверие к иностранным сертификациям/производствам

SECURITY
ARCHITECTURE

Реально ли поднять ИБ до уровня развития IoT?

Обновление НПА

- ГОСТ Р 59026-2020
- ПНСТ 518-2021
- ПНСТ 516-2021
- ГОСТ Р 71168-2023
- ГОСТ Р 72200-2023
- ГОСТ Р 71199-2023

АНО УМКД

- Объединение бизнеса и регуляторов
- Выработка системных подходов по обеспечению ИБ и комплексной работы IoT устройств
- Участие в разработке стандартов работы IoT

SecArch

- Формирование модели угроз для устройств IoT
- Формирование кастомизированных требований ИБ с учетом специфики работы IoT устройств

SECURITY
ARCHITECTURE

Вызовы интернета вещей

1

Безопасность не успевает за развитием IoT
Проблемы развития НПА и формирования границ доверия

2

Камни преткновения на этапах жизненного цикла устройств IoT
Путь от формирования требований до эксплуатации

3

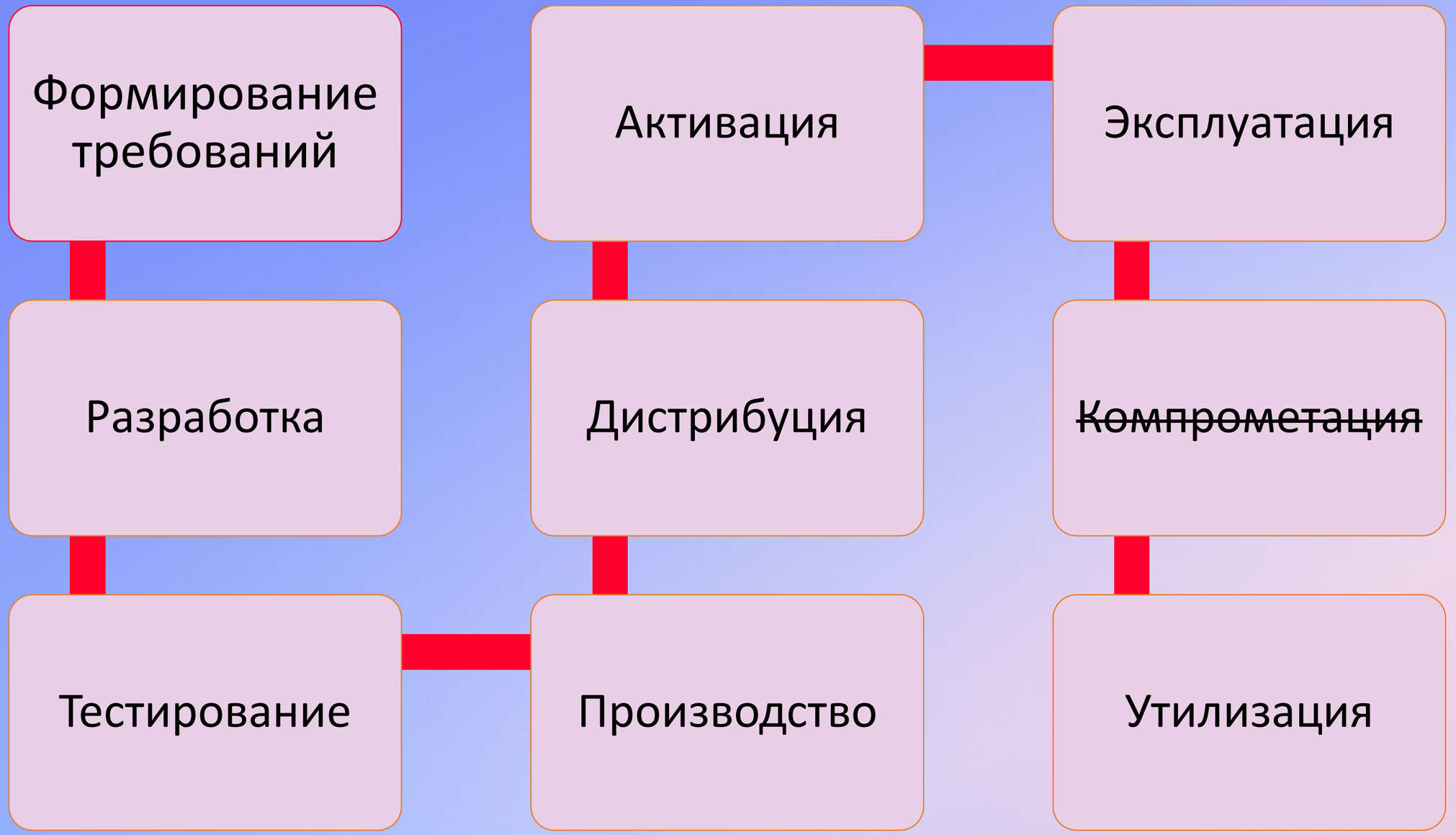
Эксплуатация = возможная компрометация
Необходимость кастомизации требований ИБ для устройств IoT

4

Неконтролируемый рост устройств IoT
Последствия масштабирования «умных» технологий

SECURITY
ARCHITECTURE

Жизненный цикл УУ



SECURITY
ARCHITECTURE

Жизненный цикл УУ

SECURITY
ARCHITECTURE

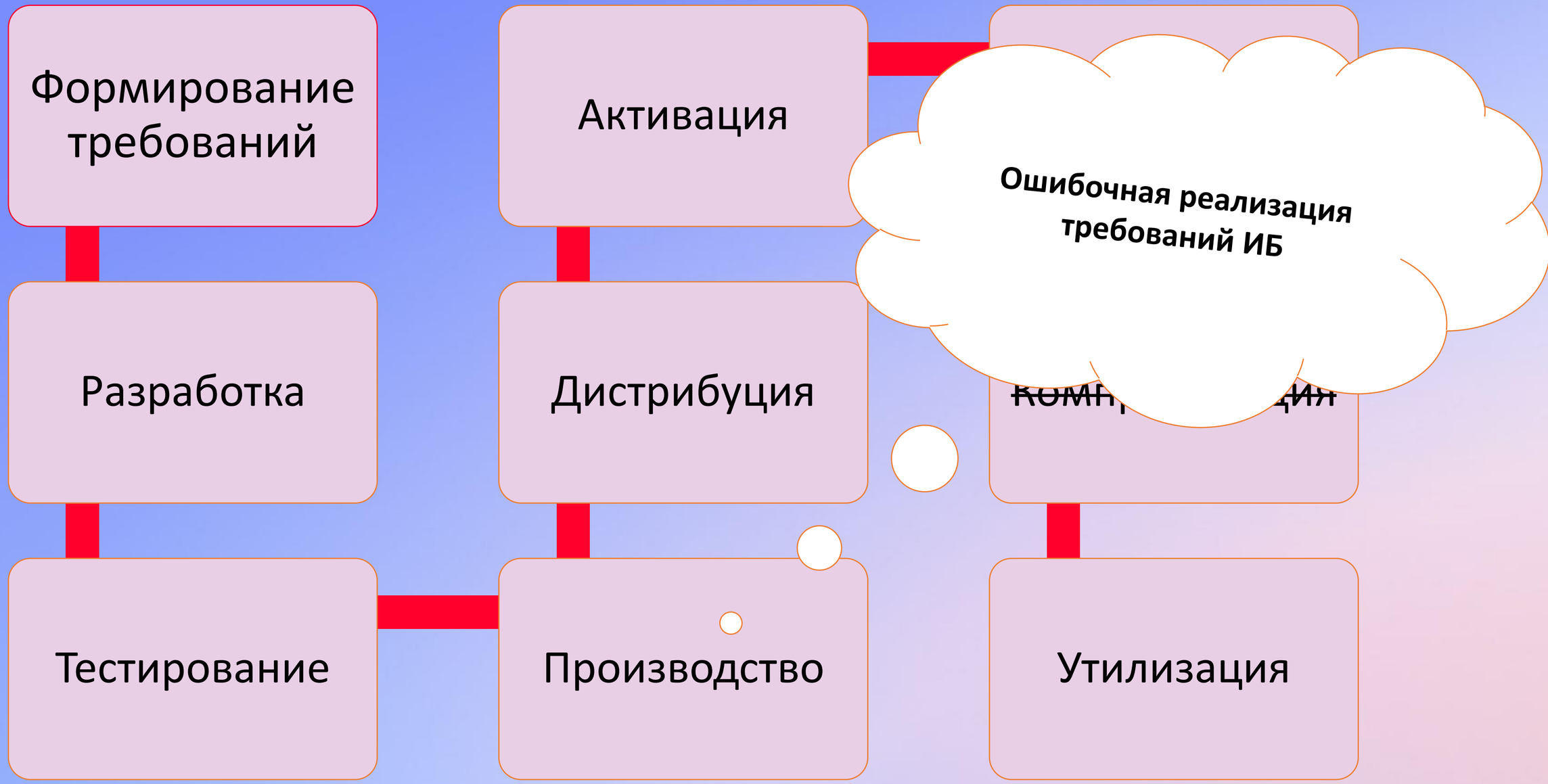
Жизненный цикл УУ

SECURITY
ARCHITECTURE

Жизненный цикл УУ

SECURITY
ARCHITECTURE

Жизненный цикл УУ



SECURITY
ARCHITECTURE

Жизненный цикл УУ

Отсутствие доверенной цепочки поставок

Активация

Эксплуатация

Разработка

Дистрибуция

~~Компрометация~~

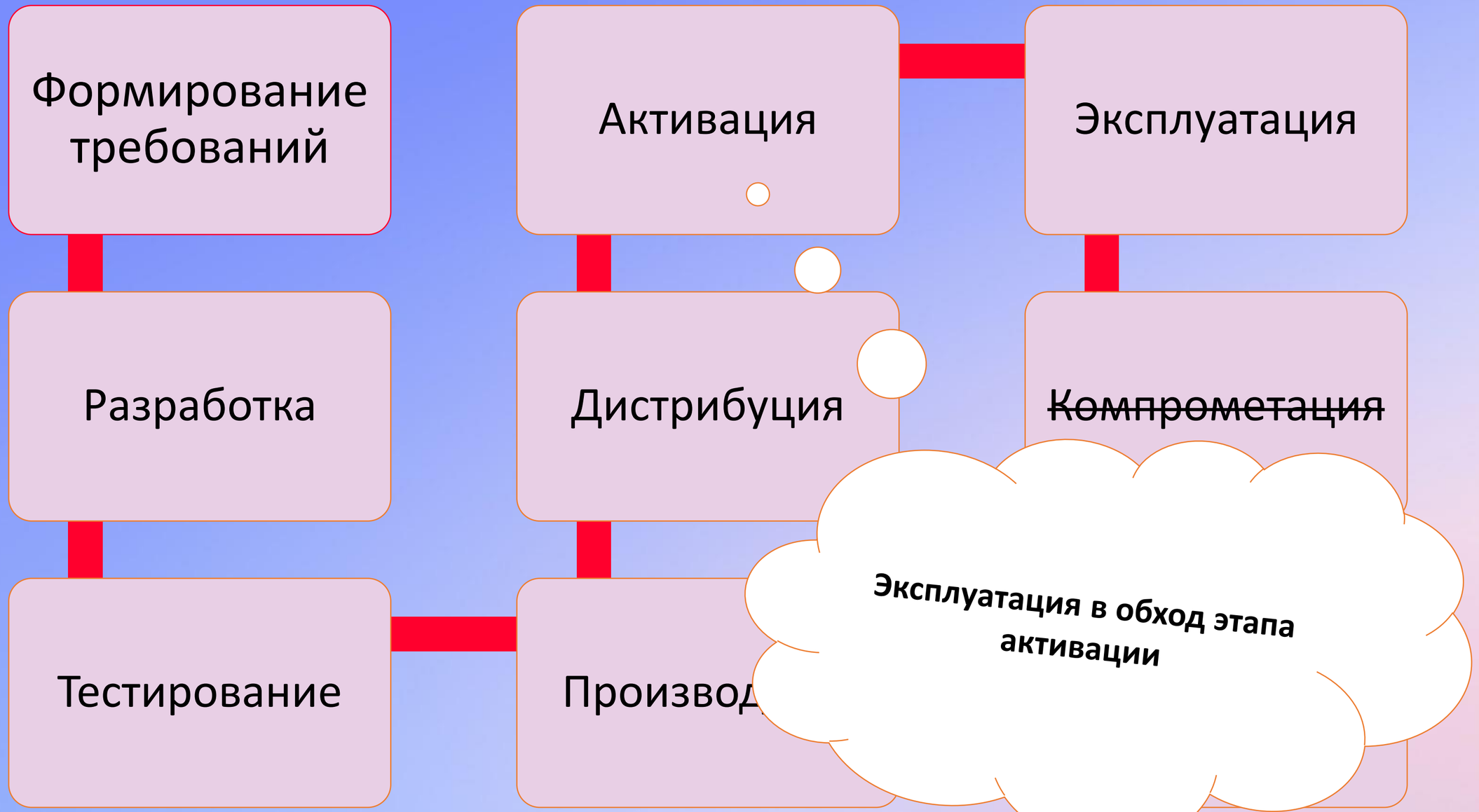
Тестирование

Производство

Утилизация

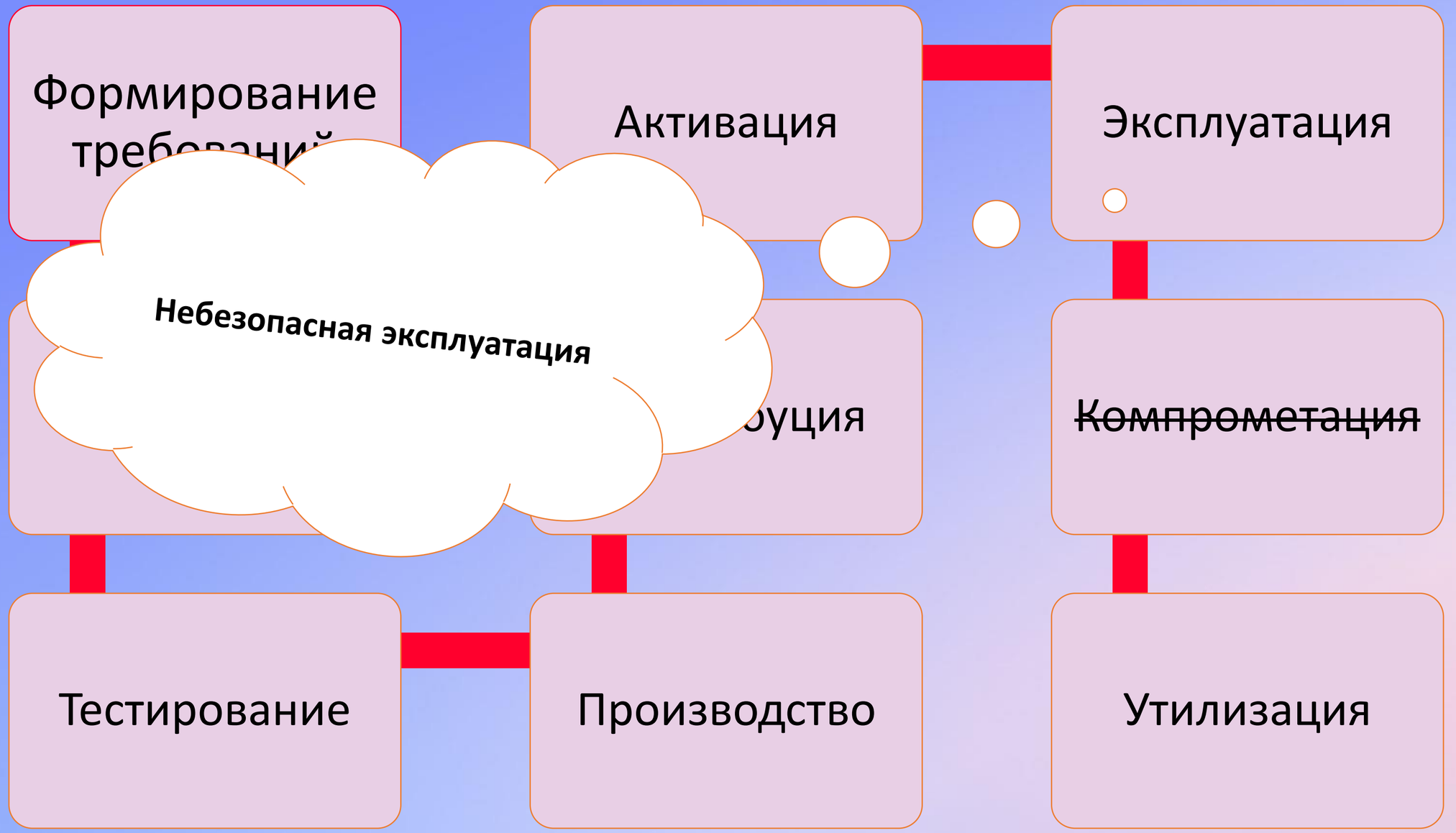
SECURITY
ARCHITECTURE

Жизненный цикл УУ



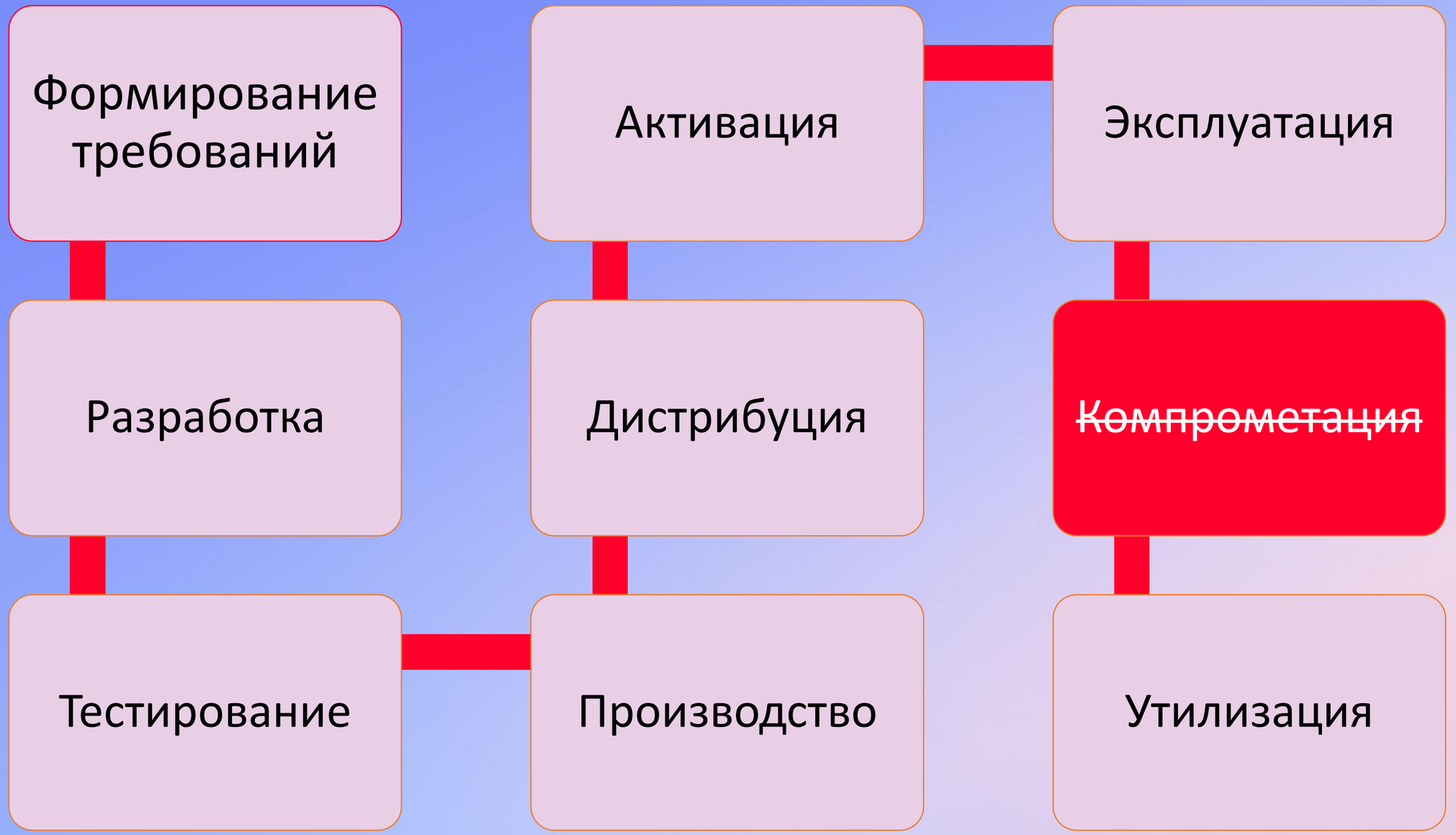
SECURITY
ARCHITECTURE

Жизненный цикл УУ



SECURITY
ARCHITECTURE

Жизненный цикл УУ

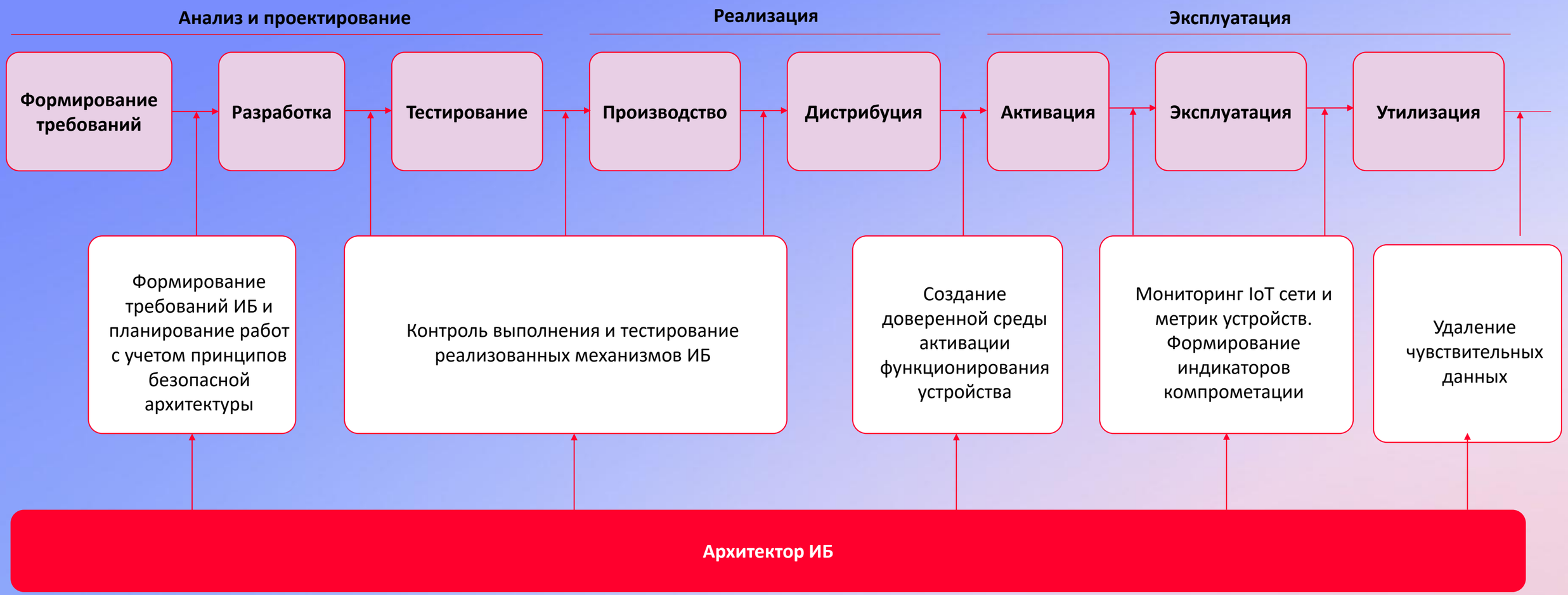


SECURITY
ARCHITECTURE

Жизненный цикл УУ

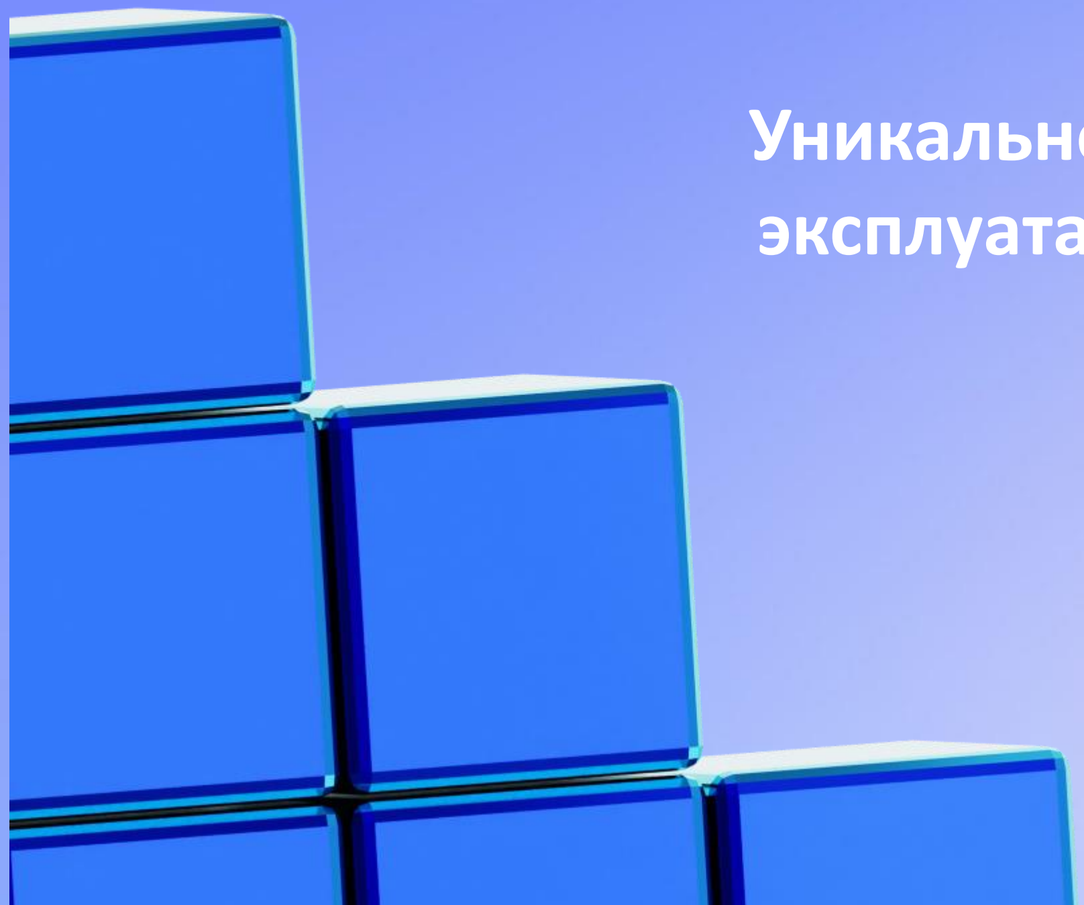
SECURITY
ARCHITECTURE

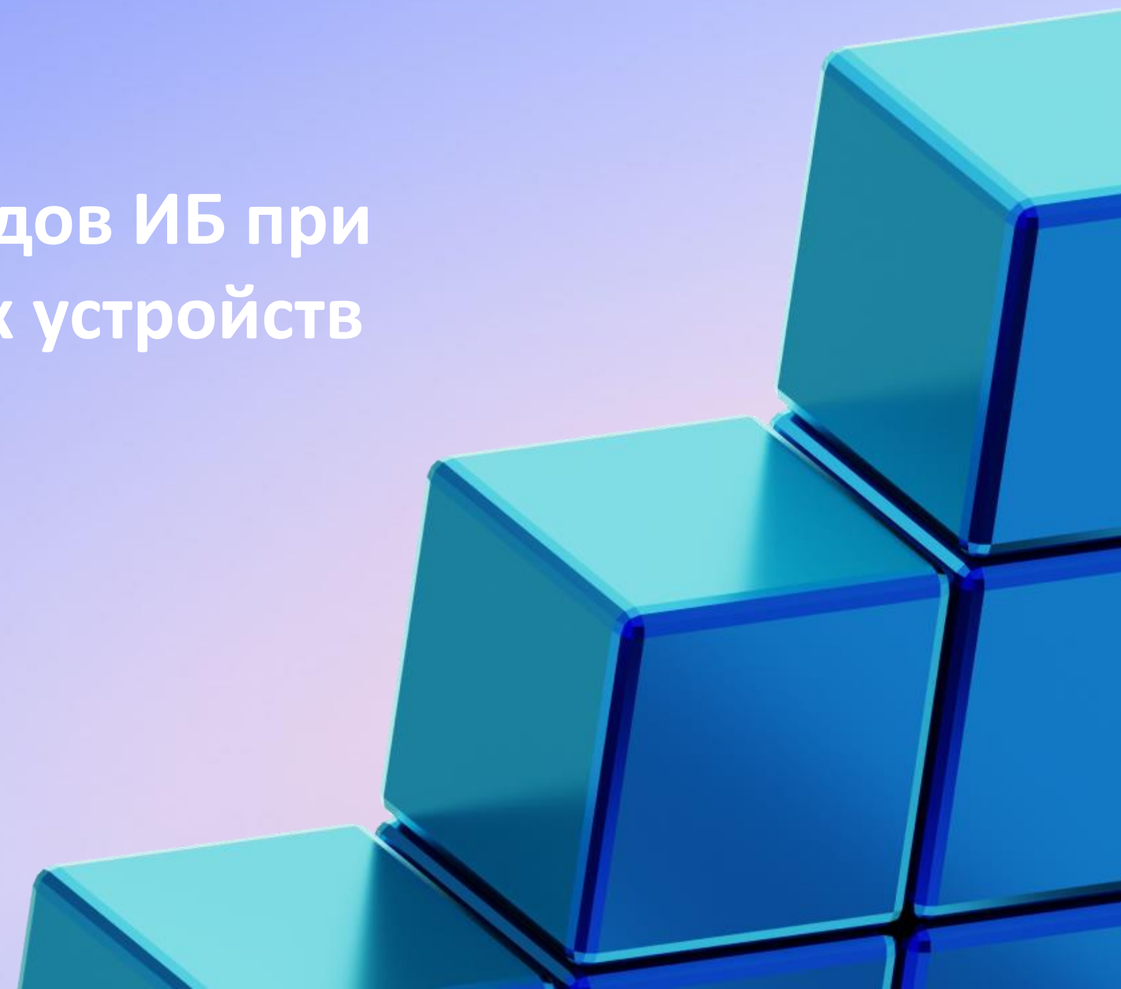
Интеграция ИБ в цикл разработки УУ



SECURITY
ARCHITECTURE

Уникальность подходов ИБ при эксплуатации умных устройств





SECURITY
ARCHITECTURE

Особенности мира интернета вещей

Стандартный клиент

- Унификация подходов обеспечения ИБ
  - стандартные подходы к аутентификации, защите каналов, мониторингу для МП и WEB
- Закрепленные Best Practice
  - Корректная реализация => корректная настройка, т.к. требования ИБ реализуемы через стандартные библиотеки
  - Богатый инструментарий для проведения проверок
  - Единые принятые механизмы защиты
- Четкое разграничение зон ответственности
  - На стороне клиента (смартфона, браузера, пользовательской ОС) реализуются: изоляция процессов, хранение чувствительной информации, реализации сетевых протоколов и т.д.

VS

«Умный» клиент

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

SECURITY
ARCHITECTURE

Особенности мира интернета вещей

Стандартный клиент

- Унификация подходов обеспечения ИБ
  - стандартные подходы к аутентификации, защите каналов, мониторингу для МП и WEB
- Закрепленные Best Practice
  - Корректная реализация => корректная настройка, т.к. требования ИБ реализуемы через стандартные библиотеки
  - Богатый инструментарий для проведения проверок
  - Единые принятые механизмы защиты
- Четкое разграничение зон ответственности
  - На стороне клиента (смартфона, браузера, пользовательской ОС) реализуются: изоляция процессов, хранение чувствительной информации, реализации сетевых протоколов и т.д.

VS

«Умный» клиент

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

SECURITY
ARCHITECTURE

Особенности мира интернета вещей

Стандартный клиент

- Унификация подходов обеспечения ИБ
  - стандартные подходы к аутентификации, защите каналов, мониторингу для МП и WEB
- Закрепленные Best Practice
  - Корректная реализация => корректная настройка, т.к. требования ИБ реализуемы через стандартные библиотеки
  - Богатый инструментарий для проведения проверок
  - Единые принятые механизмы защиты
- Четкое разграничение зон ответственности
  - На стороне клиента (смартфона, браузера, пользовательской ОС) реализуются: изоляция процессов, хранение чувствительной информации, реализации сетевых протоколов и т.д.

VS

«Умный» клиент

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

SECURITY
ARCHITECTURE

Особенности мира интернета вещей

Стандартный клиент

- Унификация подходов обеспечения ИБ
  - стандартные подходы к аутентификации, защите каналов, мониторингу для МП и WEB
- Закрепленные Best Practice
  - Корректная реализация => корректная настройка, т.к. требования ИБ реализуемы через стандартные библиотеки
  - Богатый инструментарий для проведения проверок
  - Единые принятые механизмы защиты
- Четкое разграничение зон ответственности
  - На стороне клиента (смартфона, браузера, пользовательской ОС) реализуются: изоляция процессов, хранение чувствительной информации, реализации сетевых протоколов и т.д.

VS

«Умный» клиент

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

SECURITY
ARCHITECTURE

Особенности мира интернета вещей

Стандартный клиент

- Унификация подходов обеспечения ИБ
  - стандартные подходы к аутентификации, защите каналов, мониторингу для МП и WEB
- Закрепленные Best Practice
  - Корректная реализация => корректная настройка, т.к. требования ИБ реализуемы через стандартные библиотеки
  - Богатый инструментарий для проведения проверок
  - Единые принятые механизмы защиты
- Четкое разграничение зон ответственности
  - На стороне клиента (смартфона, браузера, пользовательской ОС) реализуются: изоляция процессов, хранение чувствительной информации, реализации сетевых протоколов и т.д.

VS

«Умный» клиент

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

SECURITY
ARCHITECTURE

Вызовы интернета вещей

1

Безопасность не успевает за развитием IoT
Проблемы развития НПА и формирования границ доверия

2

Камни преткновения на этапах жизненного цикла устройств IoT
Путь от формирования требований до эксплуатации

3

Эксплуатация = возможная компрометация
Необходимость кастомизации требований ИБ для устройств IoT

4

Неконтролируемый рост устройств IoT
Последствия масштабирования «умных» технологий

SECURITY
ARCHITECTURE

Эксплуатация: вызовы

Особенности клиента

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

SECURITY
ARCHITECTURE

Эксплуатация: вызовы

Особенности клиента

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

SECURITY
ARCHITECTURE

Эксплуатация: вызовы

Особенности клиента

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

SECURITY
ARCHITECTURE

Эксплуатация: вызовы

Особенности клиента

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

SECURITY
ARCHITECTURE

Эксплуатация: вызовы

Особенности клиента

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

SECURITY
ARCHITECTURE

Эксплуатация: вызовы

Особенности клиента

- Умное устройство (УУ) – тоже актив
- Разнообразие клиентов => Сложность унификации подходов
  - Различия УУ от умных лифтов до умных кнопок (в т.ч. на аппаратном уровне)
  - Различие сценариев использования (#управляющие УУ, умные приборы, устройства мониторинга и т.д.)
- Аппаратные ограничения
  - Функционал реализуется отдельными модулями, которые необходимо интегрировать в плату на этапе разработки (#активация через BLE)
- Корректная настройка => безопасная реализация
- Реализация механизмов безопасности клиента – зона ответственности производителя УУ

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

SECURITY
ARCHITECTURE

Эксплуатация: стратегии

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

Стратегии

- Мониторинг IOT сети и метрик Умных Устройств
  - Интеграция логов УУ с SIEM, мониторинг расхода батареи, загрузки процессора, фоновых процессов
  - Мониторинг сети IOT на устройствах управления
- Реализация доверия в сети и единых схем
  - Создание единых схем с учетом специфики УУ
- Производство собственных устройств
  - Реализация требований ИБ на этапе разработки
  - Интеграция необходимых модулей
- Развитие сферы безопасности IOT
  - Создание новых СЗИ, модулей, инструментов
  - Временные меры: собственная реализация механизмов безопасности, использование существующих СЗИ
- Создание специфичных требований и НПА

SECURITY
ARCHITECTURE

Эксплуатация: стратегии

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

Стратегии

- Мониторинг IOT сети и метрик Умных Устройств
  - Интеграция логов УУ с SIEM, мониторинг расхода батареи, загрузки процессора, фоновых процессов
  - Мониторинг сети IOT на устройствах управления
- Реализация доверия в сети и единых схем
  - Создание единых схем с учетом специфики УУ
- Производство собственных устройств
  - Реализация требований ИБ на этапе разработки
  - Интеграция необходимых модулей
- Развитие сферы безопасности IOT
  - Создание новых СЗИ, модулей, инструментов
  - Временные меры: собственная реализация механизмов безопасности, использование существующих СЗИ
- Создание специфичных требований и НПА

SECURITY
ARCHITECTURE

Эксплуатация: стратегии

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

Стратегии

- Мониторинг IOT сети и метрик Умных Устройств
  - Интеграция логов УУ с SIEM, мониторинг расхода батареи, загрузки процессора, фоновых процессов
  - Мониторинг сети IOT на устройствах управления
- Реализация доверия в сети и единых схем
  - Создание единых схем с учетом специфики УУ
- Производство собственных устройств
  - Реализация требований ИБ на этапе разработки
  - Интеграция необходимых модулей
- Развитие сферы безопасности IOT
  - Создание новых СЗИ, модулей, инструментов
  - Временные меры: собственная реализация механизмов безопасности, использование существующих СЗИ
- Создание специфичных требований и НПА

SECURITY
ARCHITECTURE

Эксплуатация: стратегии

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

Стратегии

- Мониторинг IOT сети и метрик Умных Устройств
  - Интеграция логов УУ с SIEM, мониторинг расхода батареи, загрузки процессора, фоновых процессов
  - Мониторинг сети IOT на устройствах управления
- Реализация доверия в сети и единых схем
  - Создание единых схем с учетом специфики УУ
- Производство собственных устройств
  - Реализация требований ИБ на этапе разработки
  - Интеграция необходимых модулей
- Развитие сферы безопасности IOT
  - Создание новых СЗИ, модулей, инструментов
  - Временные меры: собственная реализация механизмов безопасности, использование существующих СЗИ
- Создание специфичных требований и НПА

SECURITY
ARCHITECTURE

Эксплуатация: стратегии

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

Стратегии

- Мониторинг IOT сети и метрик Умных Устройств
  - Интеграция логов УУ с SIEM, мониторинг расхода батареи, загрузки процессора, фоновых процессов
  - Мониторинг сети IOT на устройствах управления
- Реализация доверия в сети и единых схем
  - Создание единых схем с учетом специфики УУ
- Производство собственных устройств
  - Реализация требований ИБ на этапе разработки
  - Интеграция необходимых модулей
- Развитие сферы безопасности IOT
  - Создание новых СЗИ, модулей, инструментов
  - Временные меры: собственная реализация механизмов безопасности, использование существующих СЗИ
- Создание специфичных требований и НПА

SECURITY
ARCHITECTURE

Эксплуатация: стратегии

Вызовы

- Компрометация УУ
  - Не валидное использование УУ (#botnet)
  - Новые угрозы (#досрочно разрядить УУ)
- Обнаружение и противодействие атакам в IOT сети
- Отсутствие единых схем
  - Проблема доверия в сети
- Аппаратные ограничения
  - Невозможность реализации части требований ИБ на этапе эксплуатации, обновления
- Специфичные СЗИ
  - Отсутствие специфичных СЗИ, сторонних frameworks, реализующих механизмы безопасности => собственная реализация механизмов безопасности
- Необходимость проработки требований
  - К сборке прошивки, изоляции, виртуализации, контейнерам и т.д.

Стратегии

- Мониторинг IOT сети и метрик Умных Устройств
  - Интеграция логов УУ с SIEM, мониторинг расхода батареи, загрузки процессора, фоновых процессов
  - Мониторинг сети IOT на устройствах управления
- Реализация доверия в сети и единых схем
  - Создание единых схем с учетом специфики УУ
- Производство собственных устройств
  - Реализация требований ИБ на этапе разработки
  - Интеграция необходимых модулей
- Развитие сферы безопасности IOT
  - Создание новых СЗИ, модулей, инструментов
  - Временные меры: собственная реализация механизмов безопасности, использование существующих СЗИ
- Создание специфичных требований и НПА
  - иначе никак:)

SECURITY
ARCHITECTURE

Вызовы интернета вещей

1

Безопасность не успевает за развитием IoT
Проблемы развития НПА и формирования границ доверия

2

Камни преткновения на этапах жизненного цикла устройств IoT
Путь от формирования требований до эксплуатации

3

Эксплуатация = возможная компрометация
Необходимость кастомизации требований ИБ для устройств IoT

4

Неконтролируемый рост устройств IoT
Последствия масштабирования «умных» технологий

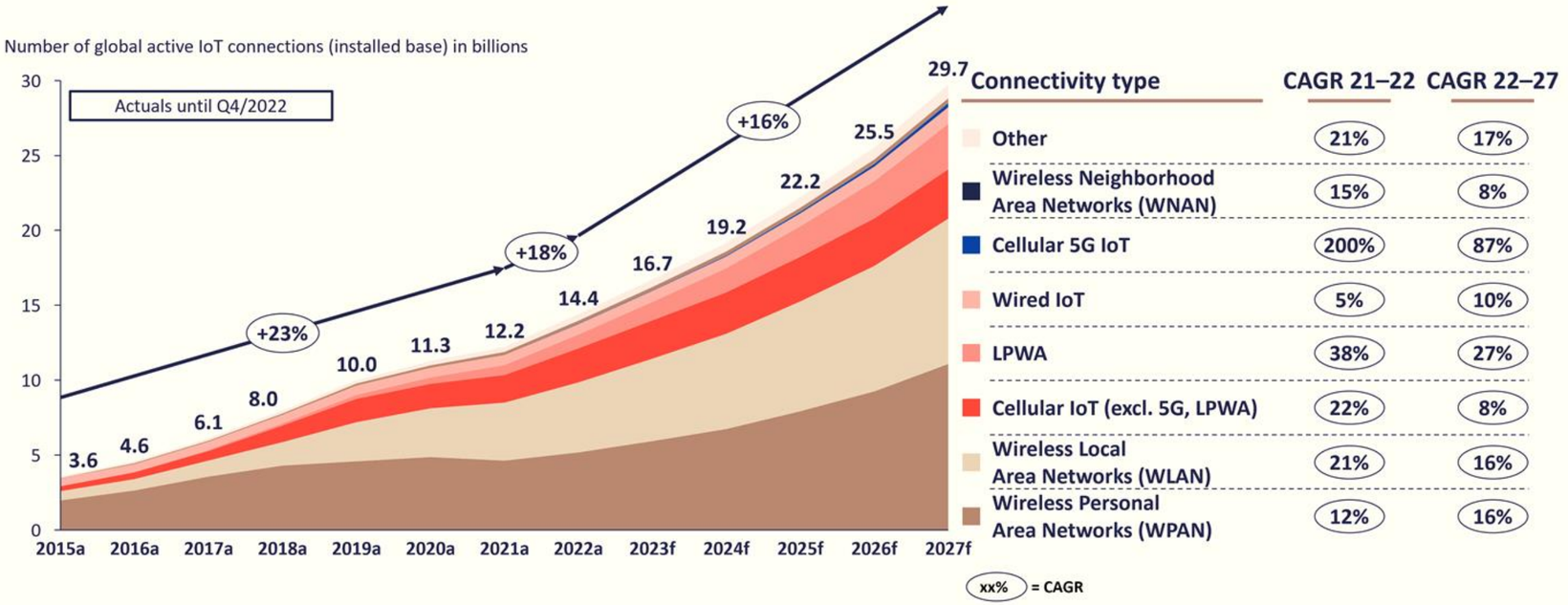
Тиражирование Умных Устройств

IOT ANALYTICS

May 2023

Your Global IoT Market Research Partner

Global IoT market forecast (in billions of connected IoT devices)



Note: IoT connections do not include any computers, laptops, fixed phones, cellphones, or consumers tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G, 5G; LPWA includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-Fi and related protocols; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.
Source: IoT Analytics Research 2023. We welcome republishing of images but ask for source citation with a link to the original post and company website.

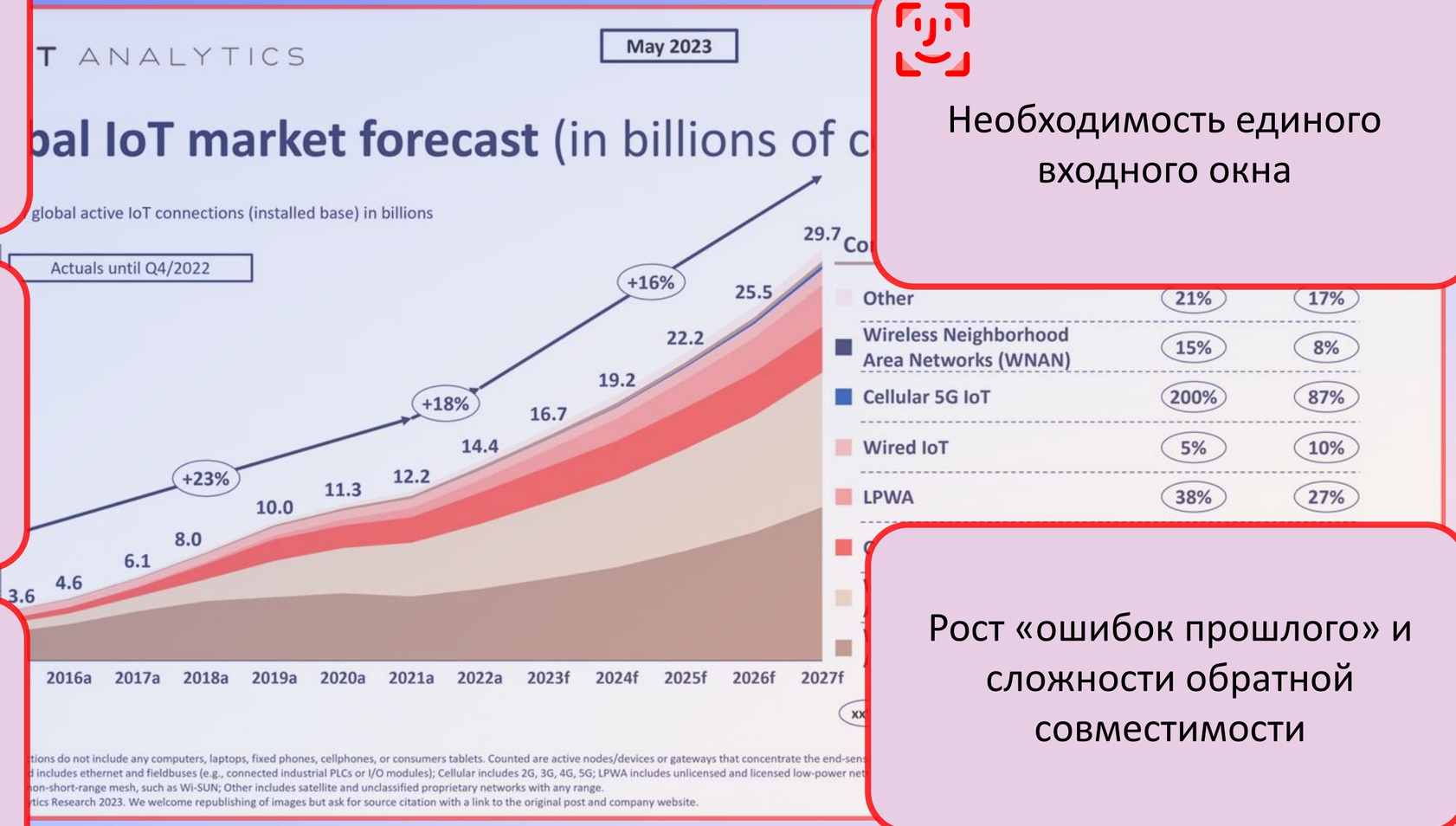
SECURITY
ARCHITECTURE

Тиражирование: вызовы

Кратный рост нагрузки на сервисы: PKI, WAF, SIEM…

Рост вероятности реализации атак

Рост уровня квалификации нарушителя



Необходимость единого входного окна

Рост «ошибок прошлого» и сложности обратной совместимости

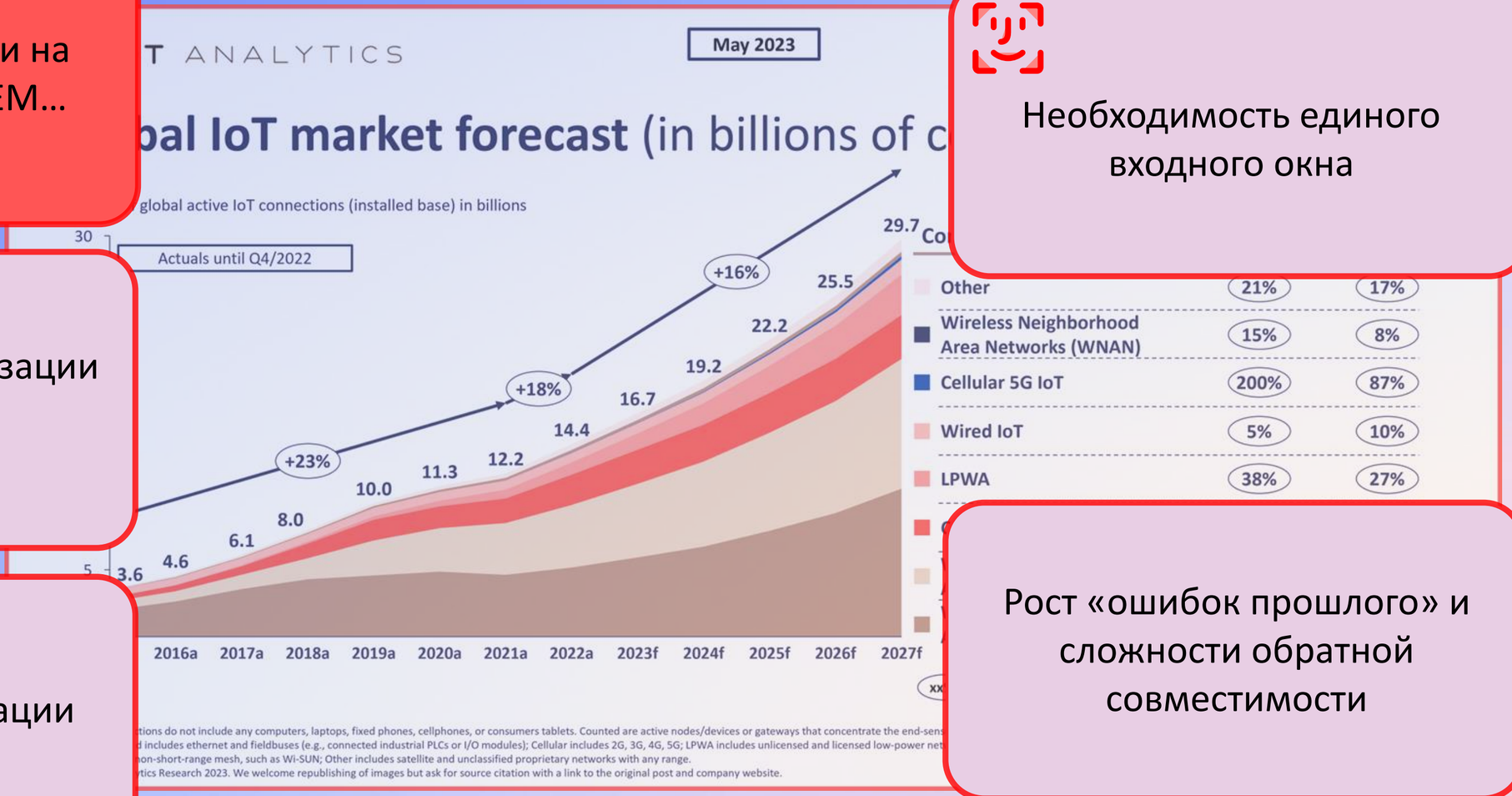
SECURITY
ARCHITECTURE

Тиражирование: вызовы

Кратный рост нагрузки на сервисы: PKI, WAF, SIEM…

Рост вероятности реализации атак

Рост уровня квалификации нарушителя



Необходимость единого входного окна

Рост «ошибок прошлого» и сложности обратной совместимости

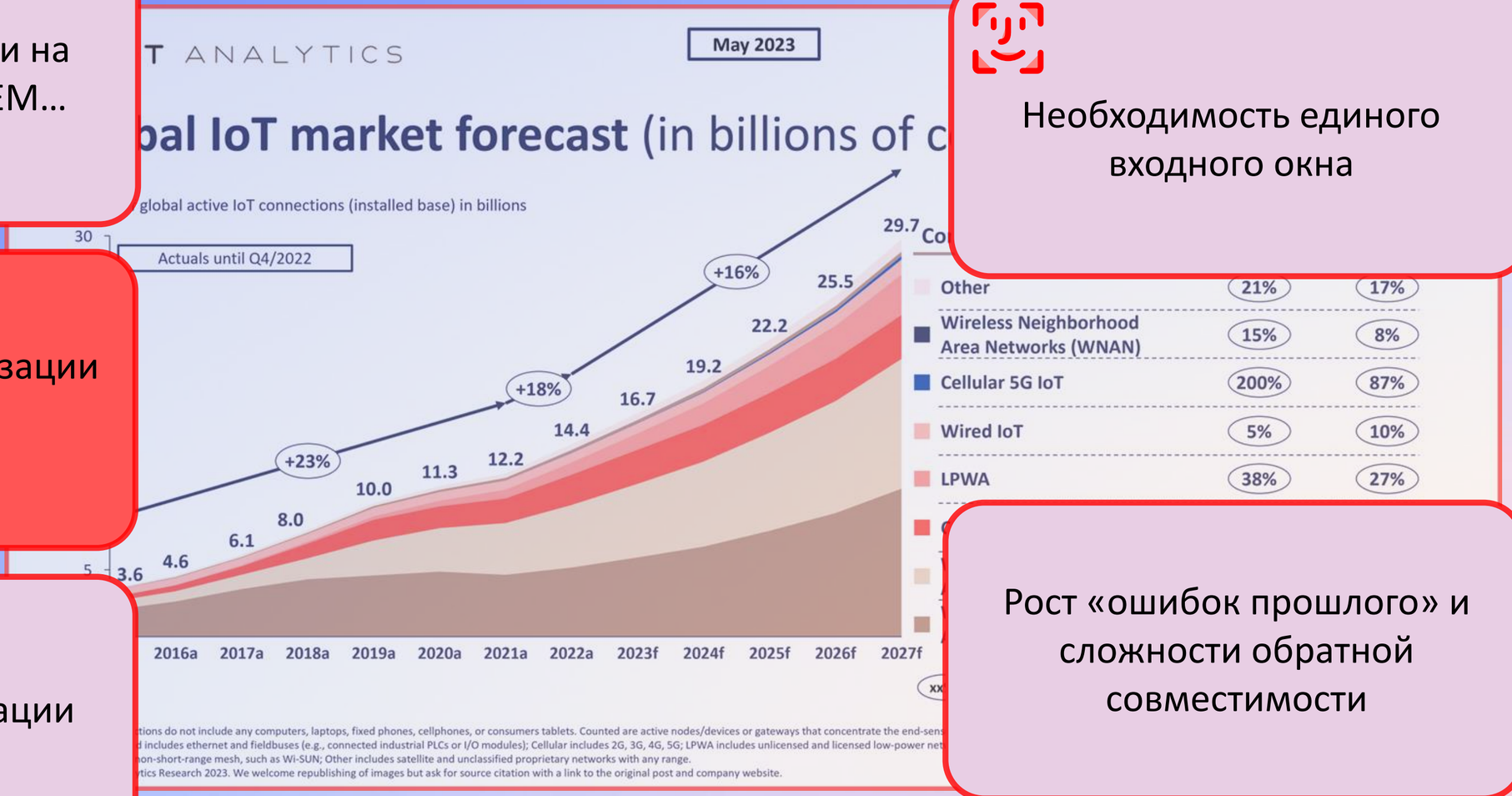
SECURITY
ARCHITECTURE

Тиражирование: вызовы

Кратный рост нагрузки на сервисы: PKI, WAF, SIEM…

Рост вероятности реализации атак

Рост уровня квалификации нарушителя



Необходимость единого входного окна

Рост «ошибок прошлого» и сложности обратной совместимости

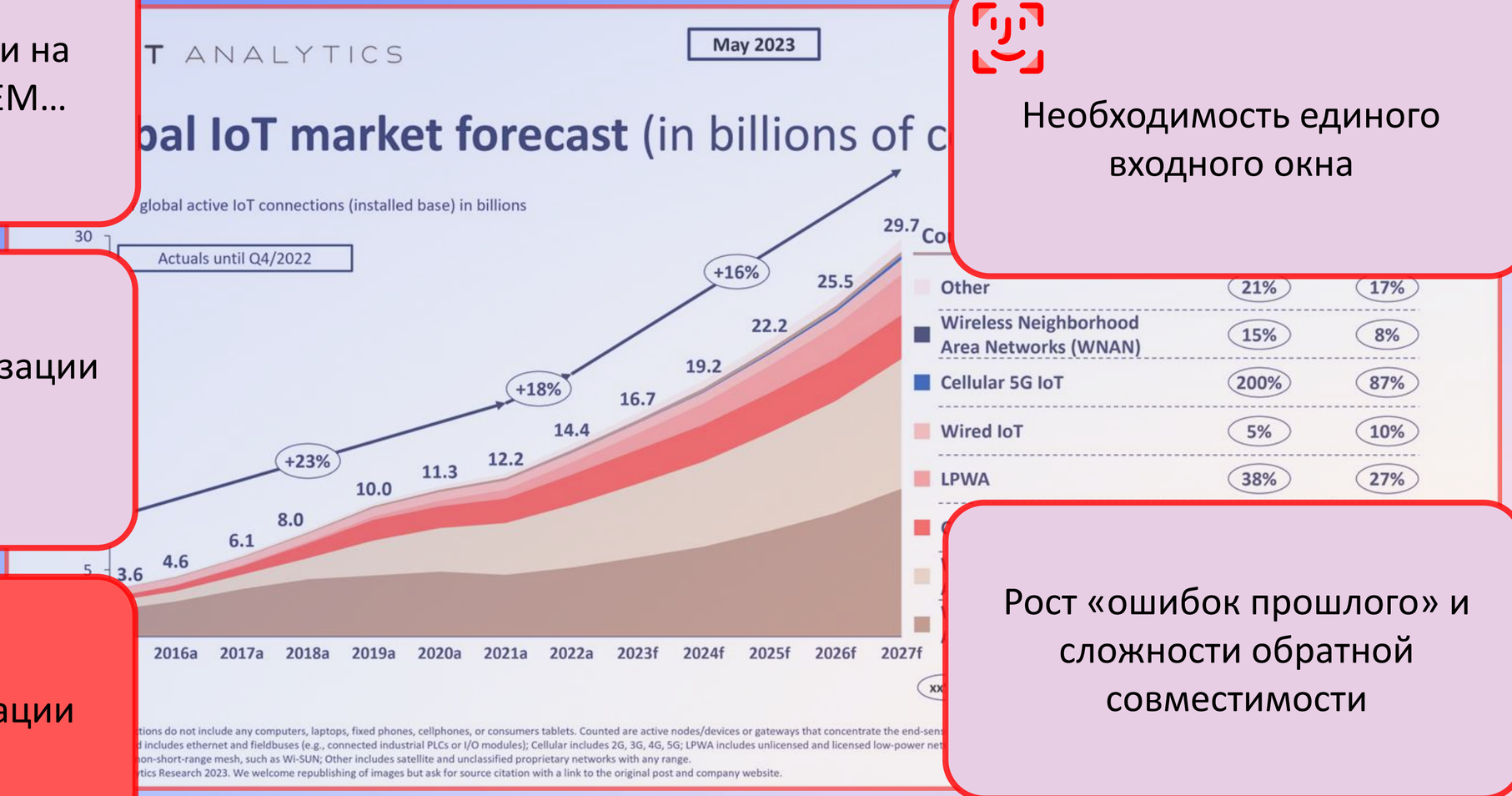
SECURITY
ARCHITECTURE

Тиражирование: вызовы

Кратный рост нагрузки на сервисы: PKI, WAF, SIEM…

Рост вероятности реализации атак

Рост уровня квалификации нарушителя



Необходимость единого входного окна

Рост «ошибок прошлого» и сложности обратной совместимости

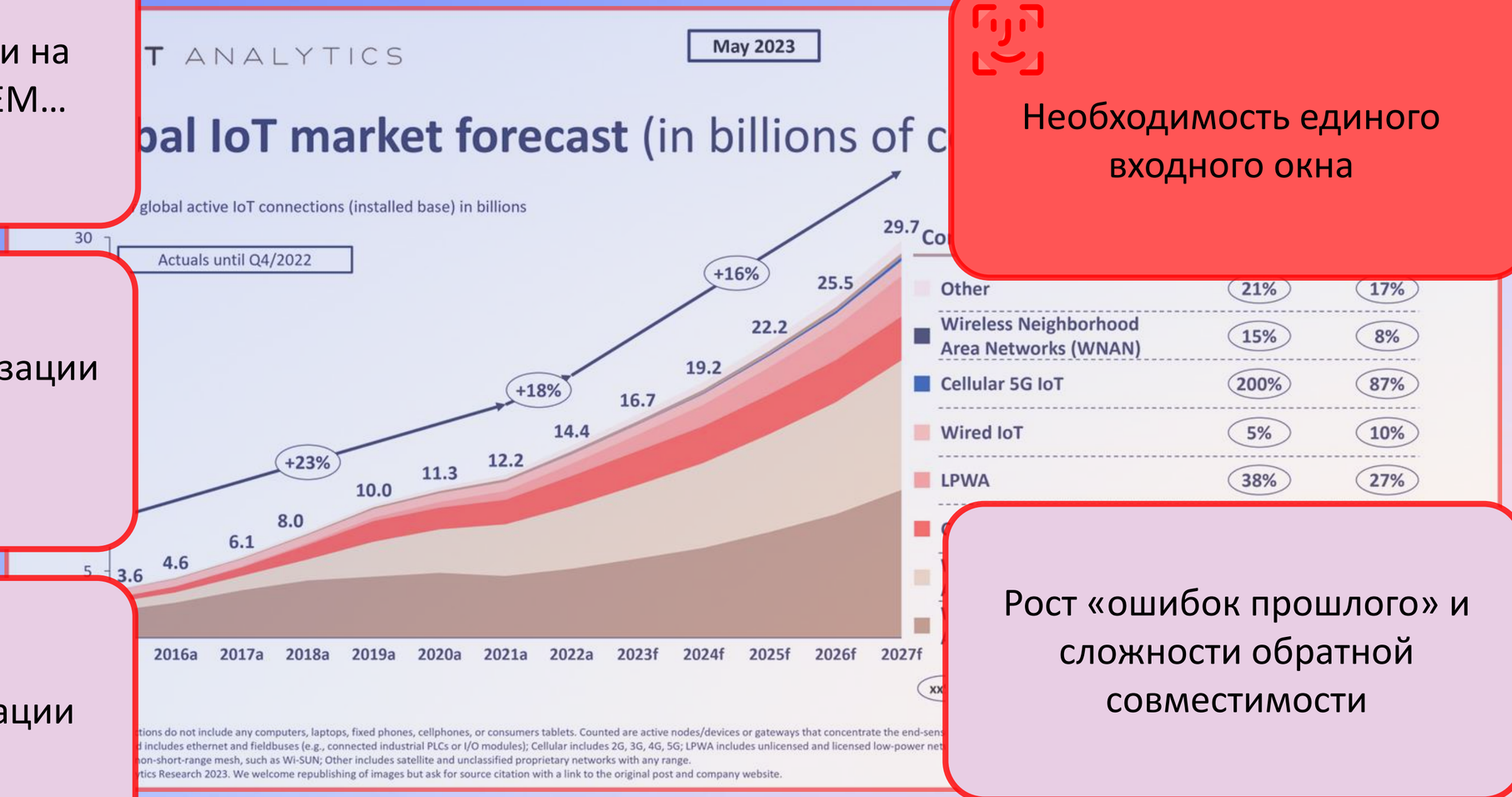
SECURITY
ARCHITECTURE

Тиражирование: вызовы

Кратный рост нагрузки на сервисы: PKI, WAF, SIEM…

Рост вероятности реализации атак

Рост уровня квалификации нарушителя



Необходимость единого входного окна

Рост «ошибок прошлого» и сложности обратной совместимости

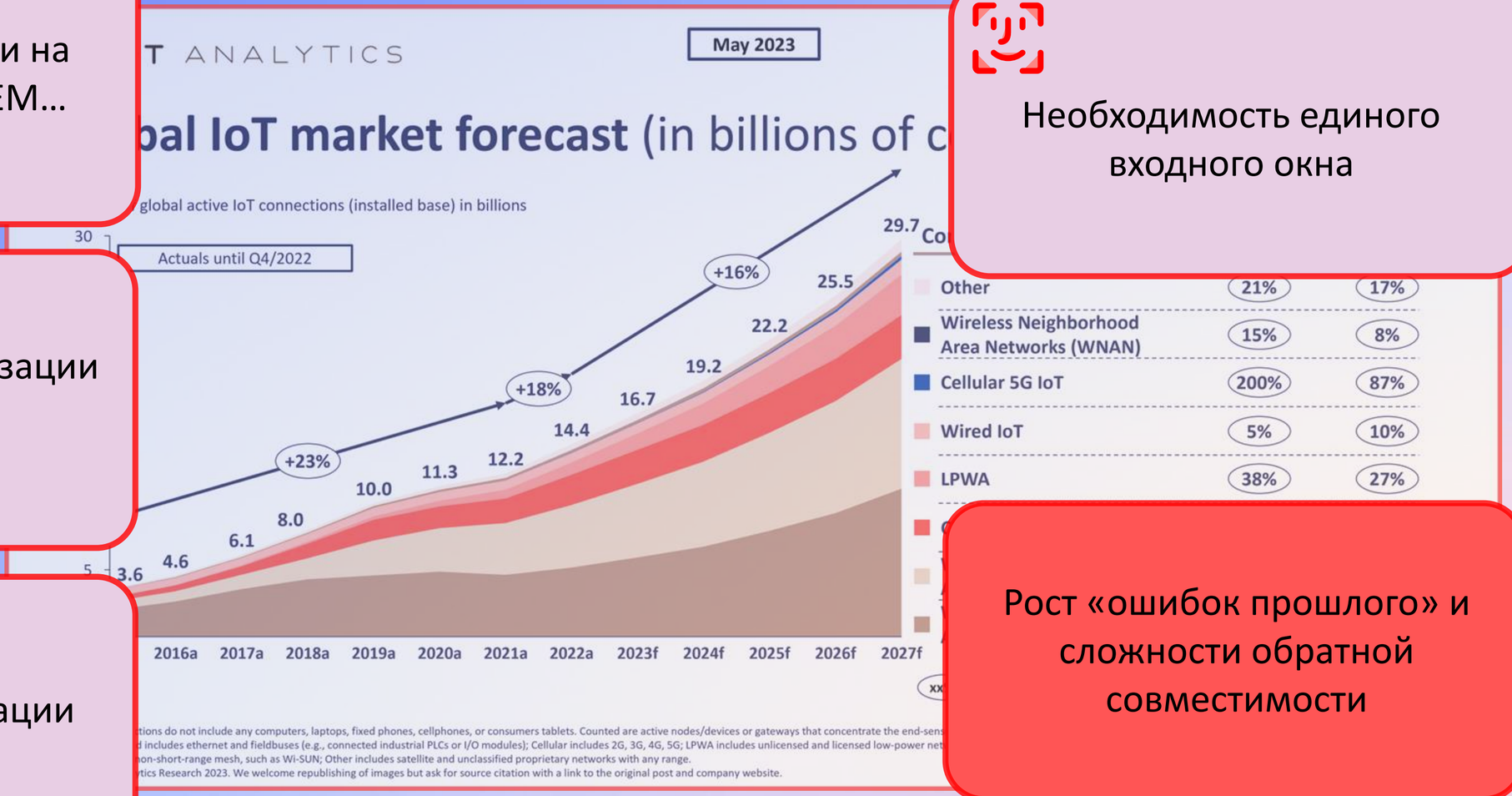
SECURITY
ARCHITECTURE

Тиражирование: вызовы

Кратный рост нагрузки на сервисы: PKI, WAF, SIEM…

Рост вероятности реализации атак

Рост уровня квалификации нарушителя



Необходимость единого входного окна

Рост «ошибок прошлого» и сложности обратной совместимости

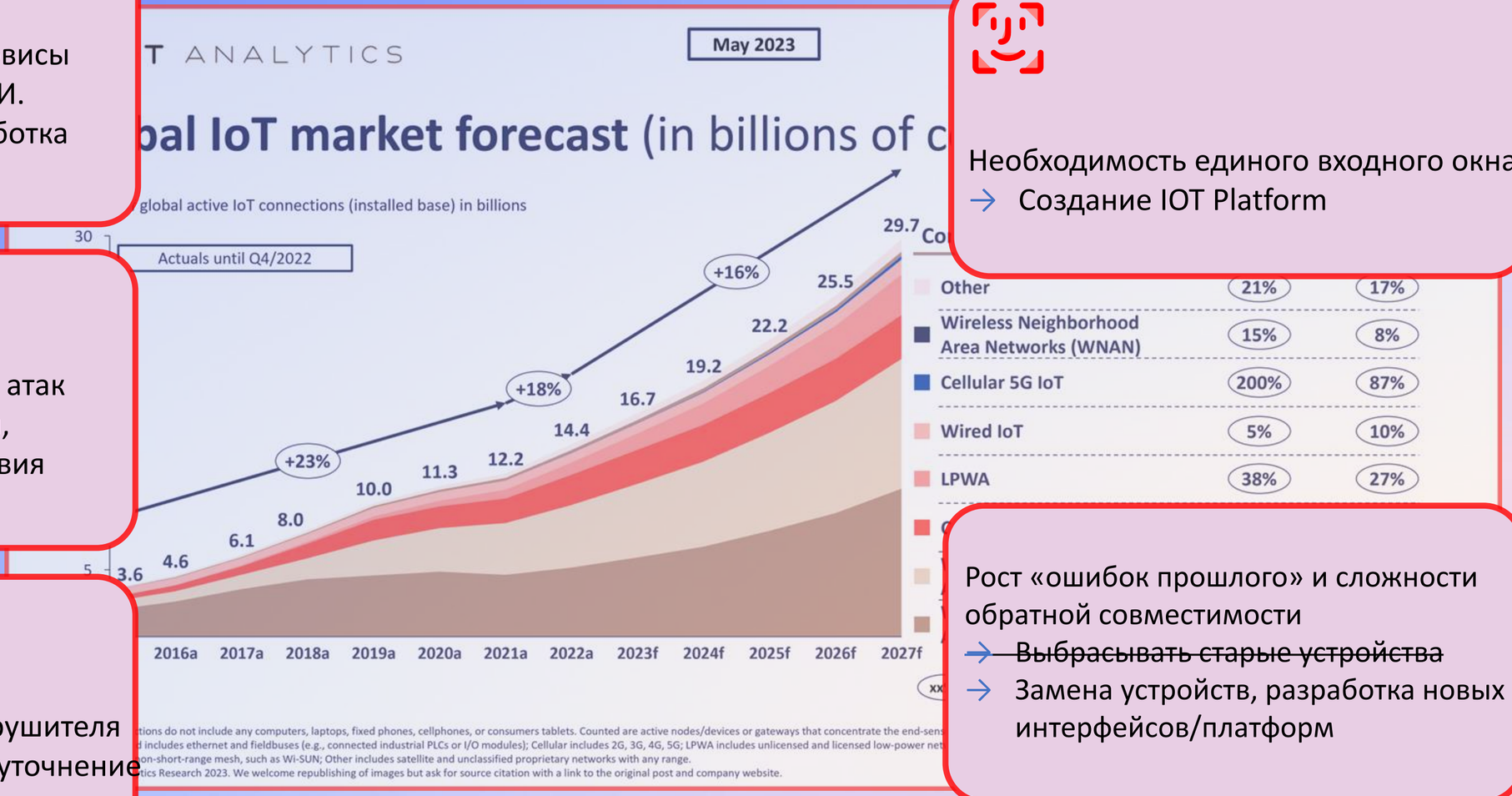
SECURITY
ARCHITECTURE

Тиражирование: стратегии

Кратный рост нагрузки на сервисы
→ Учитывать при закупке СЗИ. Заблаговременная проработка роста нагрузки

Рост вероятности реализации атак
→ Мониторинг событий сети, проработка противодействия атакам

Рост уровня квалификации нарушителя
→ Постепенное улучшение и уточнение требований ИБ



Необходимость единого входного окна
→ Создание IOT Platform

Рост «ошибок прошлого» и сложности обратной совместимости
→ ~~Выбрасывать старые устройства~~
→ Замена устройств, разработка новых интерфейсов/платформ

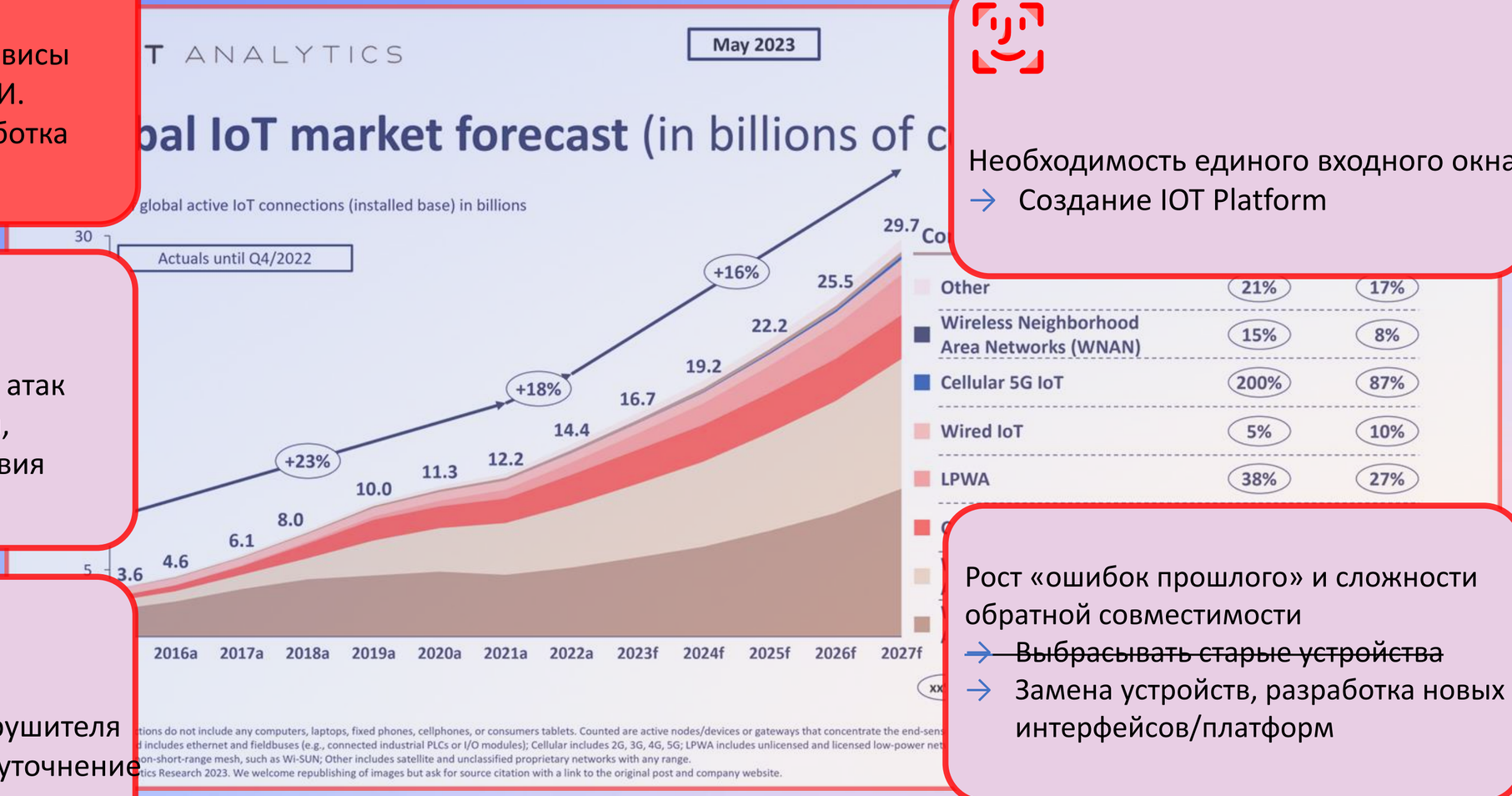
SECURITY
ARCHITECTURE

Тиражирование: стратегии

Кратный рост нагрузки на сервисы
→ Учитывать при закупке СЗИ. Заблаговременная проработка роста нагрузки

Рост вероятности реализации атак
→ Мониторинг событий сети, проработка противодействия атакам

Рост уровня квалификации нарушителя
→ Постепенное улучшение и уточнение требований ИБ



Необходимость единого входного окна
→ Создание IOT Platform

Рост «ошибок прошлого» и сложности обратной совместимости
→ ~~Выбрасывать старые устройства~~
→ Замена устройств, разработка новых интерфейсов/платформ

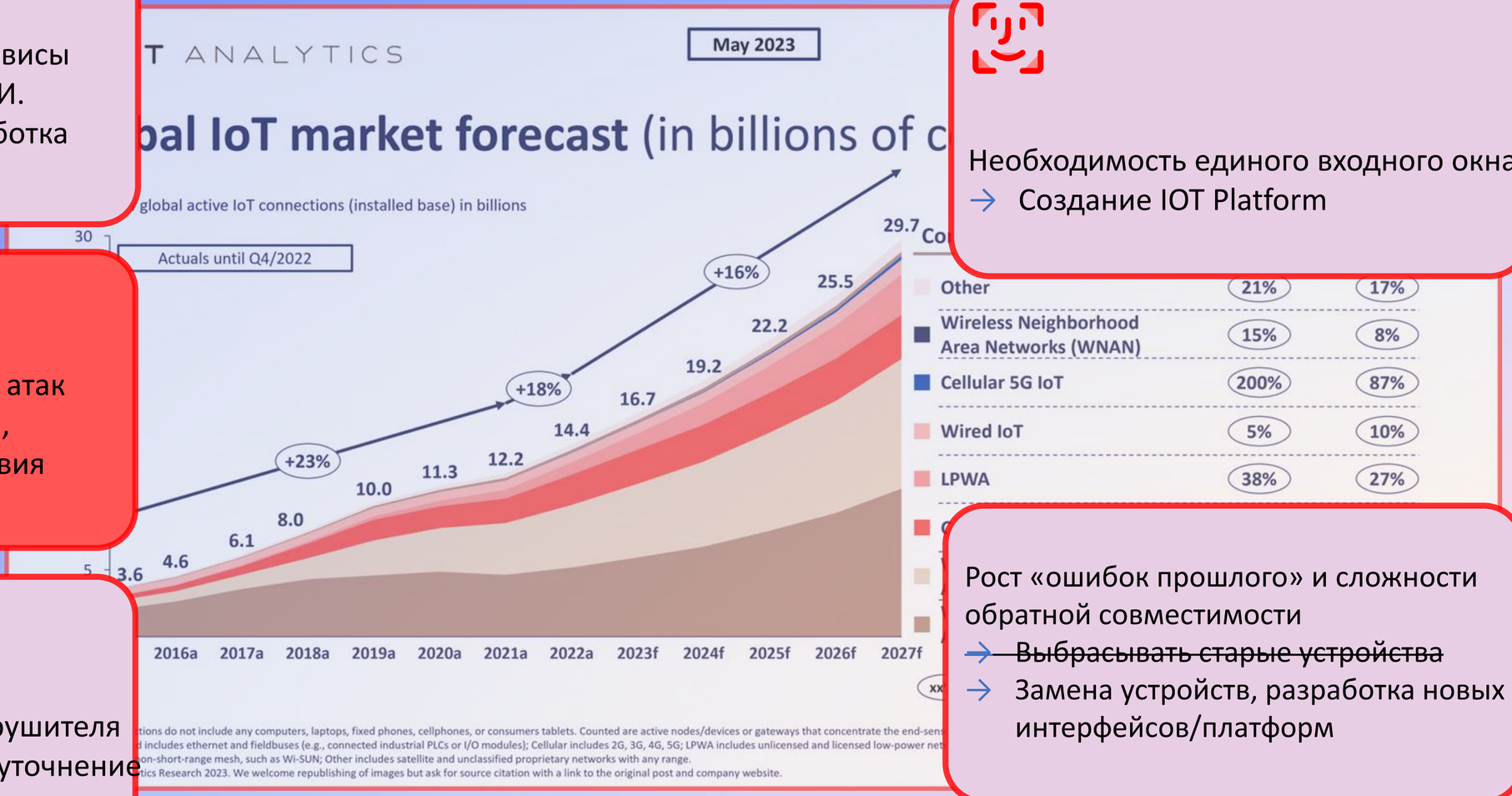
SECURITY
ARCHITECTURE

Тиражирование: стратегии

Кратный рост нагрузки на сервисы
→ Учитывать при закупке СЗИ. Заблаговременная проработка роста нагрузки

Рост вероятности реализации атак
→ Мониторинг событий сети, проработка противодействия атакам

Рост уровня квалификации нарушителя
→ Постепенное улучшение и уточнение требований ИБ



Необходимость единого входного окна
→ Создание IOT Platform

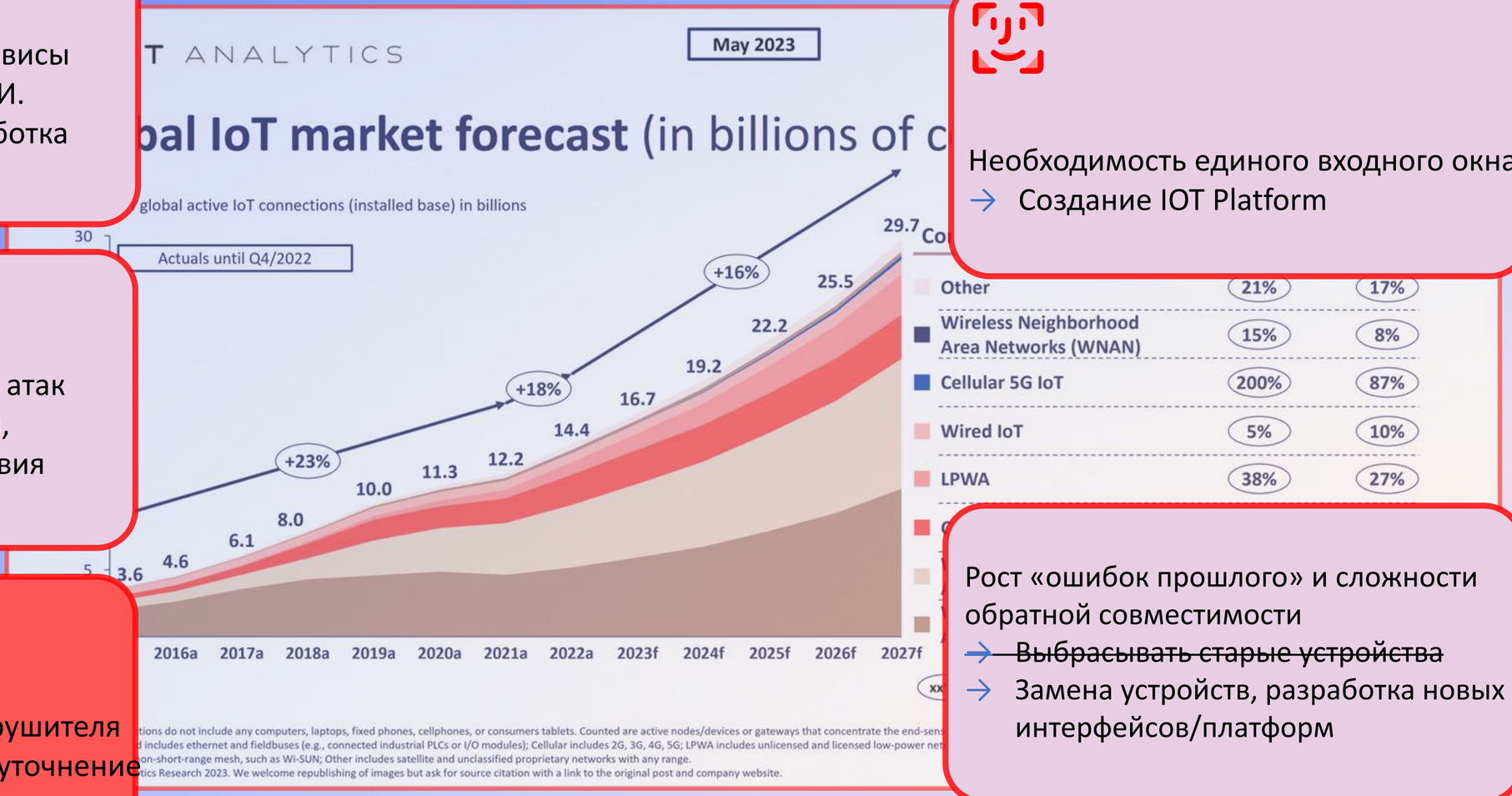
Рост «ошибок прошлого» и сложности обратной совместимости
→ ~~Выбрасывать старые устройства~~
→ Замена устройств, разработка новых интерфейсов/платформ

Тиражирование: стратегии

Кратный рост нагрузки на сервисы
→ Учитывать при закупке СЗИ. Заблаговременная проработка роста нагрузки

Рост вероятности реализации атак
→ Мониторинг событий сети, проработка противодействия атакам

Рост уровня квалификации нарушителя
→ Постепенное улучшение и уточнение требований ИБ



Необходимость единого входного окна
→ Создание IOT Platform

Рост «ошибок прошлого» и сложности обратной совместимости
→ ~~Выбрасывать старые устройства~~
→ Замена устройств, разработка новых интерфейсов/платформ

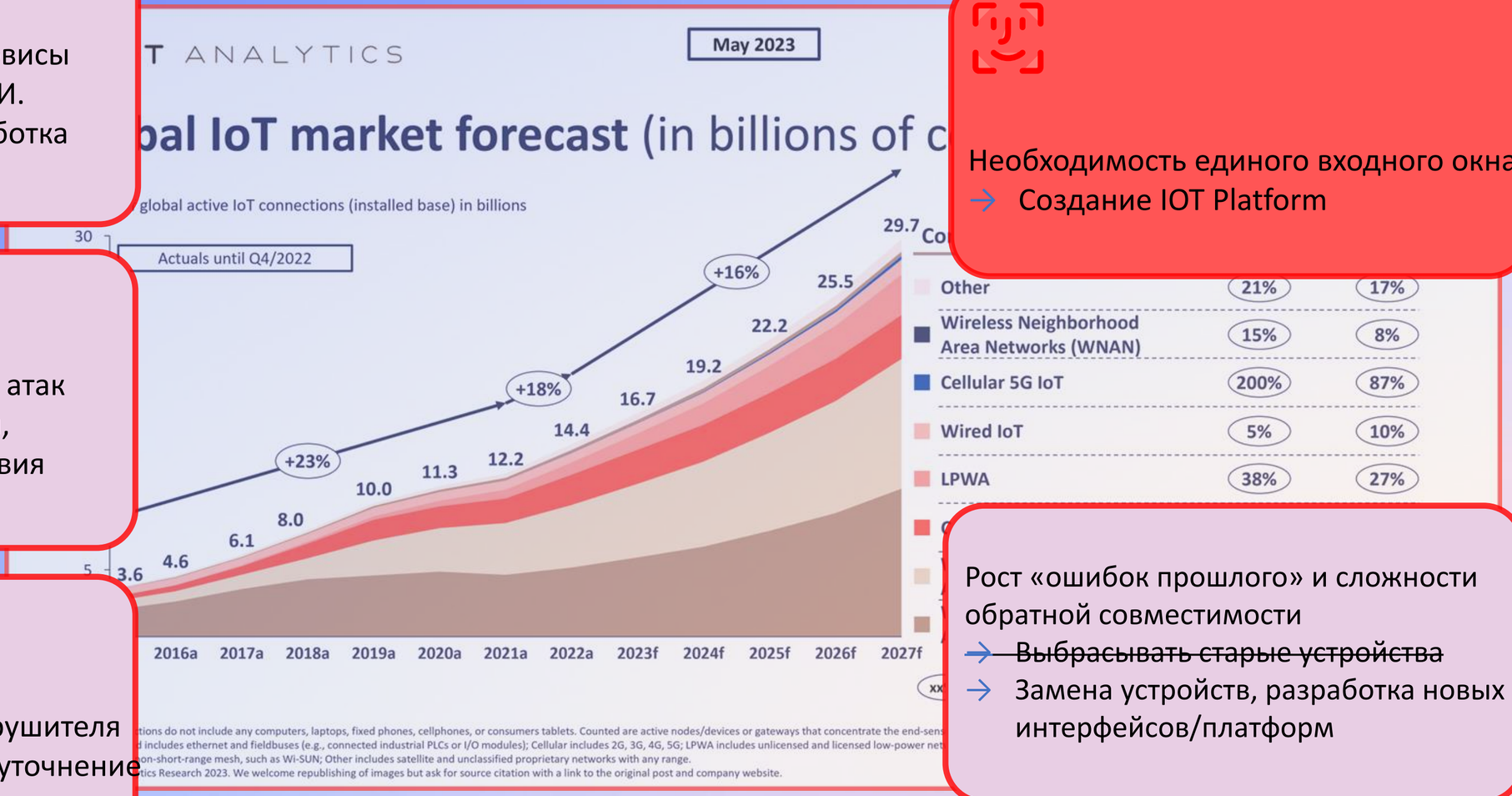
SECURITY
ARCHITECTURE

Тиражирование: стратегии

Кратный рост нагрузки на сервисы
→ Учитывать при закупке СЗИ. Заблаговременная проработка роста нагрузки

Рост вероятности реализации атак
→ Мониторинг событий сети, проработка противодействия атакам

Рост уровня квалификации нарушителя
→ Постепенное улучшение и уточнение требований ИБ



Необходимость единого входного окна
→ Создание IOT Platform

Рост «ошибок прошлого» и сложности обратной совместимости
→ ~~Выбрасывать старые устройства~~
→ Замена устройств, разработка новых интерфейсов/платформ

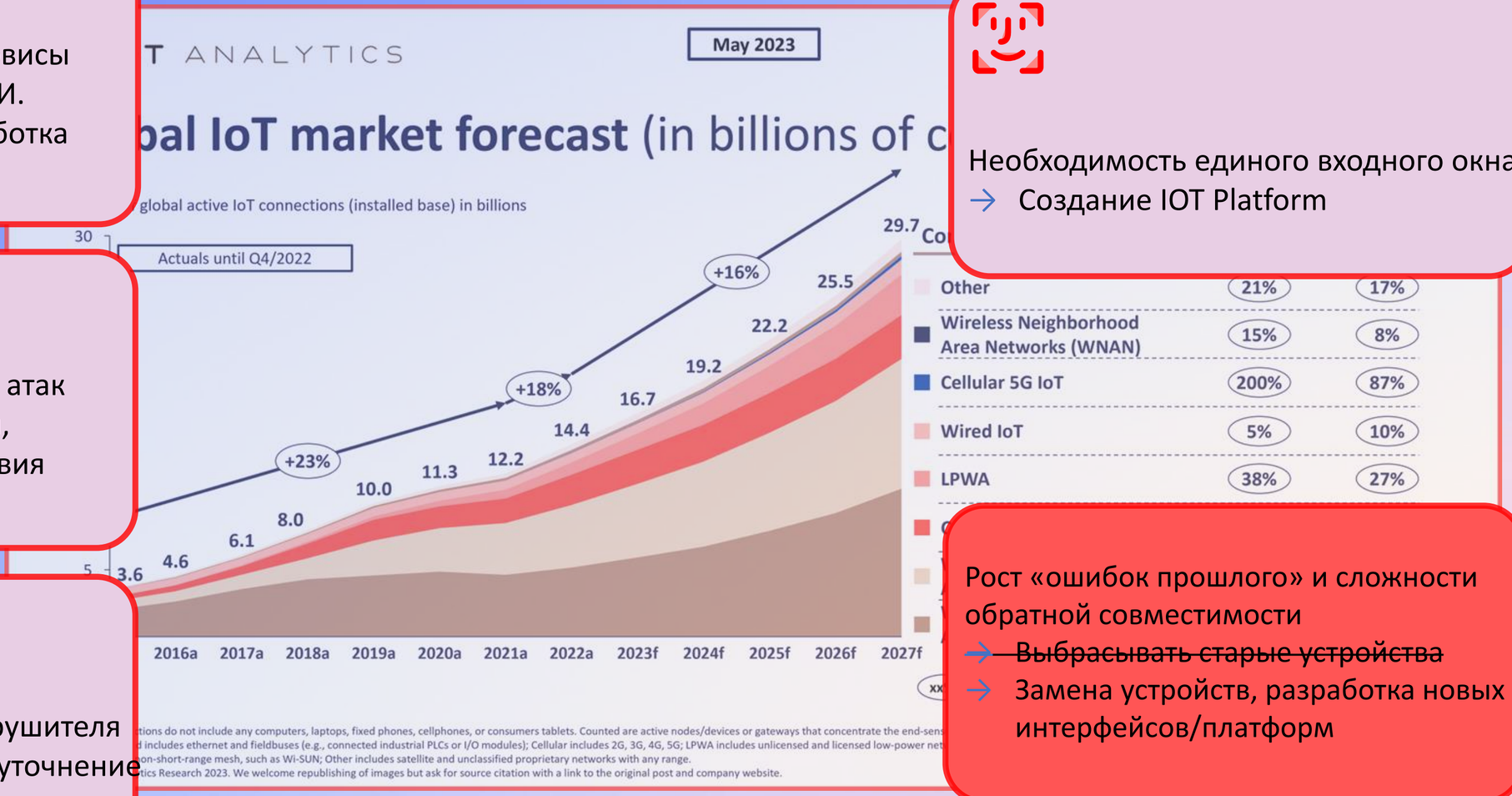
SECURITY
ARCHITECTURE

Тиражирование: стратегии

Кратный рост нагрузки на сервисы
→ Учитывать при закупке СЗИ. Заблаговременная проработка роста нагрузки

Рост вероятности реализации атак
→ Мониторинг событий сети, проработка противодействия атакам

Рост уровня квалификации нарушителя
→ Постепенное улучшение и уточнение требований ИБ



Необходимость единого входного окна
→ Создание IOT Platform

Рост «ошибок прошлого» и сложности обратной совместимости
→ ~~Выбрасывать старые устройства~~
→ Замена устройств, разработка новых интерфейсов/платформ

SECURITY
ARCHITECTURE

Хайп vs Security

- Инновационные возможности и
- Повышение безопасности
- Смарт-ритейл
- Экологические преимущества
- Умный дом
- Повышение эффективности
- Улучшение качества обслуживания
- Экологические приемущества
- Мониторинг и управление
- Автономные транспортные средства
- Умное здравоохранение
- Улучшение пользовательского опыта
- Экономия ресурсов
- Умный город

SecArch

SECURITY
ARCHITECTURE

Безопасность в мире IOT: Вызовы и Стратегии

МТС: архитектура ИБ

Холод Денис
@dekholod

Молоденова Александра
@solinenarany