ЭКОНОМИКА

Информационная безопасность инфраструктуры и сервисов Интернета вещей на объектах КИИ

ТБ Форум 2023

Олег Демидов

Ведущий аналитик
Направление «Безопасная открытая инфраструктура»

IoT: развитие в России в 2022 г.

ЭКОНОМИКА

02.2022

Утвержден первый международный стандарт по промышленному IoT

Стандарт станет платформой для развития Национальной технологической инициативы и Цифровой экономики. Разработка велась по инициативе «Ростелекома» при поддержке Минпромторга России

04.2022

VK обновила возможности облачной IoT-платформы для разработчиков

VK Cloud Solutions представила обновленную платформу для интернета вещей – Cloud IoT Platform. На ее основе можно создавать приложения для умных домов и умных городов автоматизации и роботизации промышленности, подключенных автомобилей и смарт-сервисов ЖКХ.

06.2022

Минцифры представило платформу, основанную на IoT - решение для экомониторинга

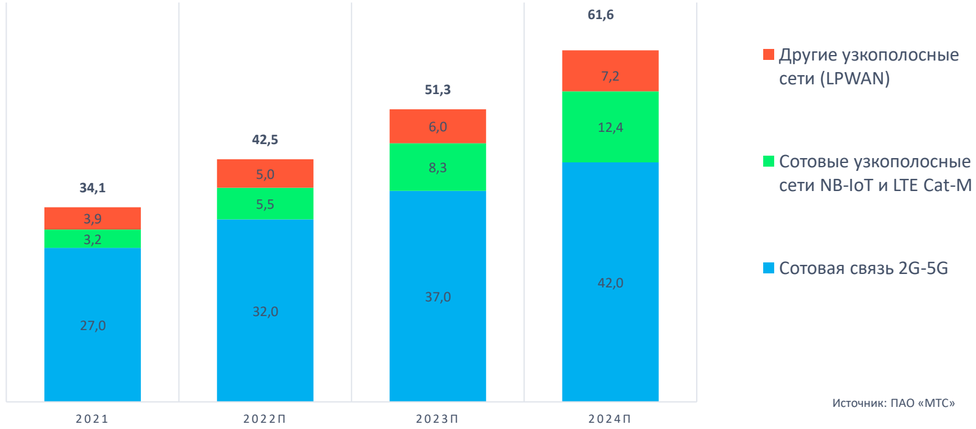
Данная платформа основана на технологии IoT, входит в состав облачного решения цифровизации ГИС «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности».

11.2022

Растет доля подключенных IoT – устройств через eSIM в России

К концу 2022 года доля IoT устройств, подключенных через eSIM составляет 7%. По прогнозам к концу 2025 года через eSIM будет подключено около 25% всех IoT-устройств в России.

Структура подключений IoT в сетях дальнего радиуса действия (WAN) в России
(млн)



Источник: ПАО «МТС»

183,5 млрд. руб.

составит объем российского рынка IoT к 2025 г.

Источники: J'son&Partners Consulting

42,5 млн

составит число подключений IoT в сетях дальнего радиуса действия (WAN) в России по итогам 2022 г.

Источник: ПАО «МТС»

Порядка 12% в год

составит рост российского рынка IoT в ближайшей перспективе

Источники: Ассоциация Интернета вещей

На 16%

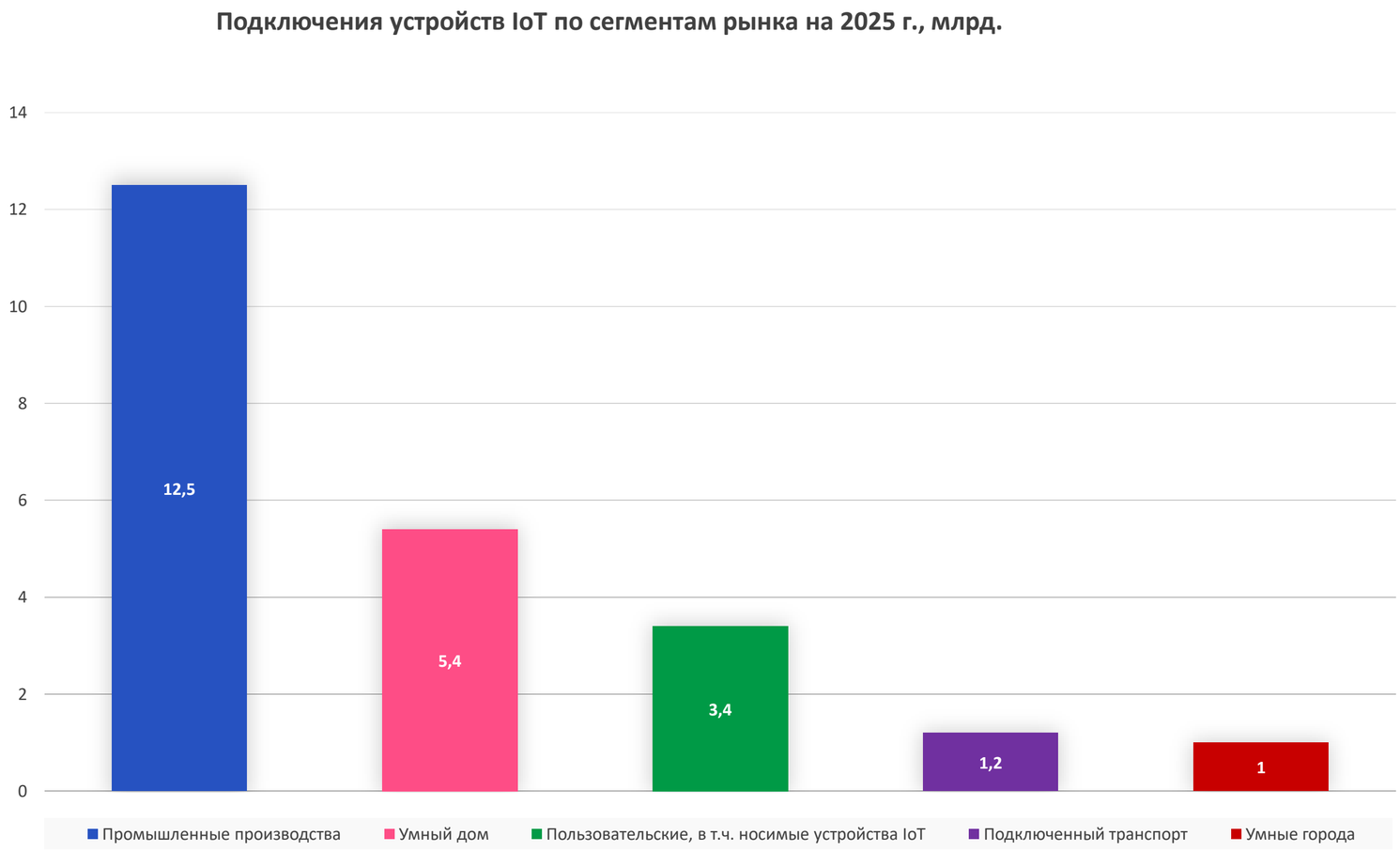
Выросло число подключений IoT в России за 2021 г.

Источник: J'son&Partners Consulting

2

Промышленный IoT: тенденции развития

ЭКОНОМИКА



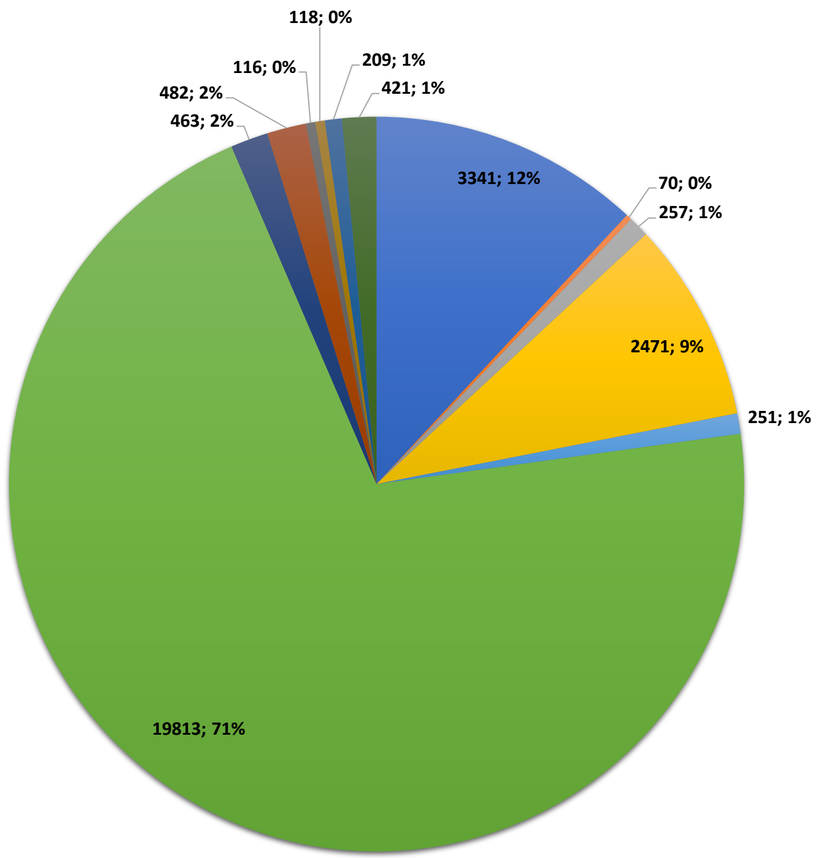
- Промышленный IoT – в ближайшей перспективе крупнейший сегмент глобального рынка Интернета вещей
- До сих пор основную долю подключений устройств IoT обеспечивал пользовательский сегмент: 7 млн против 6 млн промышленных подключений в 2020 г., 9 млн против 8 млн в 2022 г.
- В 2023 г. два сегмента сравняются по числу подключений
- С 2024 г. промышленный IoT будет устойчиво лидировать: в 2025 г. в мире будет 14 млрд. промышленных подключений IoT против 11 млрд. пользовательских

3

Отраслевое распределение ОКИИ и применения IoT

ЭКОНОМИКА

Количественное распределение объектов КИИ Российской Федерации по отраслям (2019 г.)



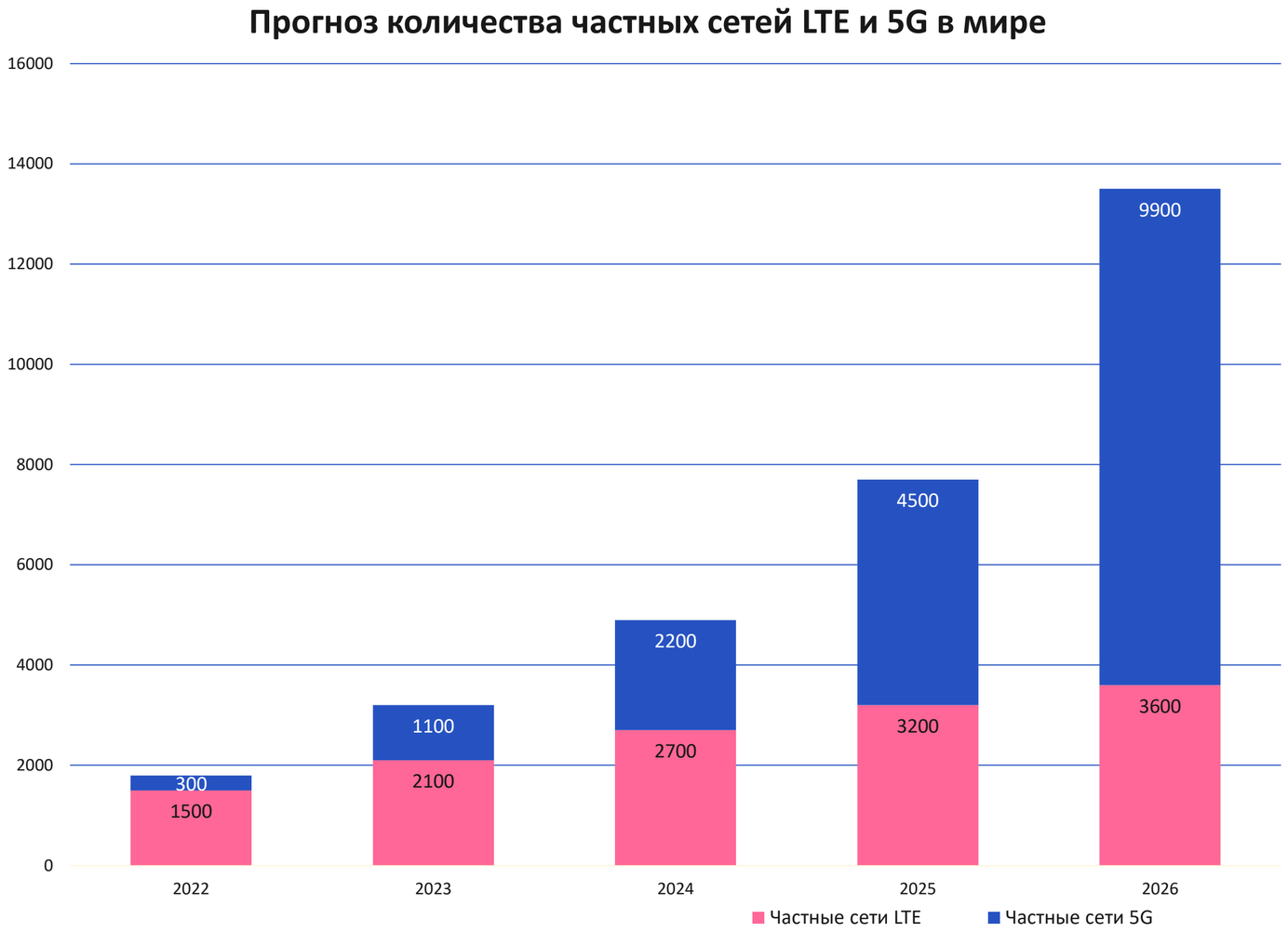
- Сфера здравоохранения
- Сфера науки
- Сфера транспорта
- Сфера связи
- Банковская сфера и иные сферы финансового рынка
- Сфера энергетики и ТЭК
- Атомная энергетика
- Оборонная промышленность
- Ракетно-космическая промышленность
- Горнодобывающая промышленность
- Металлургическая промышленность
- Химическая промышленность

- Наиболее крупными отраслевыми сегментами ОКИИ остаются объекты ТЭК, отрасли связи и здравоохранения
- Наиболее широко используемые технологии IoT: узкополосные сети LPWAN (NB-IoT, LoRa), частные сотовые сети LTE; на отдельных объектах развертываются сети на базе российских узкополосных стандартов (NB-Fi, Стриж)
- Наиболее распространенные сценарии применения сервисов IoT: видеонаблюдение и видеофиксация, цифровая диспетчеризация и АСУ ТП на различных технологических переделах, учет и контроль безопасности персонала на территории предприятия
- По предварительным оценкам, на сегодняшний день действие Указов № 166 и № 250 затрагивает инфраструктуры и сервисы IoT не менее чем на 50–60 % от общего числа категорированных объектов КИИ России, т.е. более 20 тыс. таких объектов

4

Наиболее быстрорастущая ниша применений промышленного IoT на объектах КИИ: частные сети LTE

ЭКОНОМИКА



Источник: Enterprise IoT Insights, март 2022

Март 2022 г.: в мире развернуто более 1 тыс. частных сетей LTE и еще 200-300 частных сетей 5G

Прогноз на 2026 г.: более 13,5 тыс. частных сетей LTE/5G (рост x10, CAGR 55%)

Самые распространенные ниши внедрения Private LTE/5G: обрабатывающие производства (28 %), транспортная и логистическая инфраструктура (15%), энергогенерация и горнодобывающие производства (13%)

Инвестиции промышленных предприятий и других бизнес-субъектов в частные сети LTE/5G многократно вырастут:

- Консервативная оценка: рост в 6,5 раз с 2021 по 2026 гг. до $5 млрд.
- Оптимистичная оценка: рост до $16,7 млрд. только по сегменту Private LTE к 2025 г.

5

Картина уязвимостей в ПО промышленного IoT

ЭКОНОМИКА

- В 2021 г. рост числа выявленных уязвимостей безопасности IoT и АСУ ТП (16% и 50% соответственно) многократно превысил общую динамику уязвимостей в ИТ-продуктах (+0,4%)

- Из 797 уязвимостей АСУ ТП, выявленных за вторую половину 2021 г., 128 (17%) составили уязвимости в ПО и оборудовании IoT, причем 60 из них (8%) пришлось на нишу медицинских устройств IoT (всего за 2021 год в АСУ ТП было выявлено 1439 уязвимостей против 942 годом ранее)

- В 2021 г. выявлено 19 уязвимостей нулевого дня, включая критические, такие как Ripple20, в библиотеке TCP/IP компании Treck Inc., широко используемой для разработки сервисов IoT

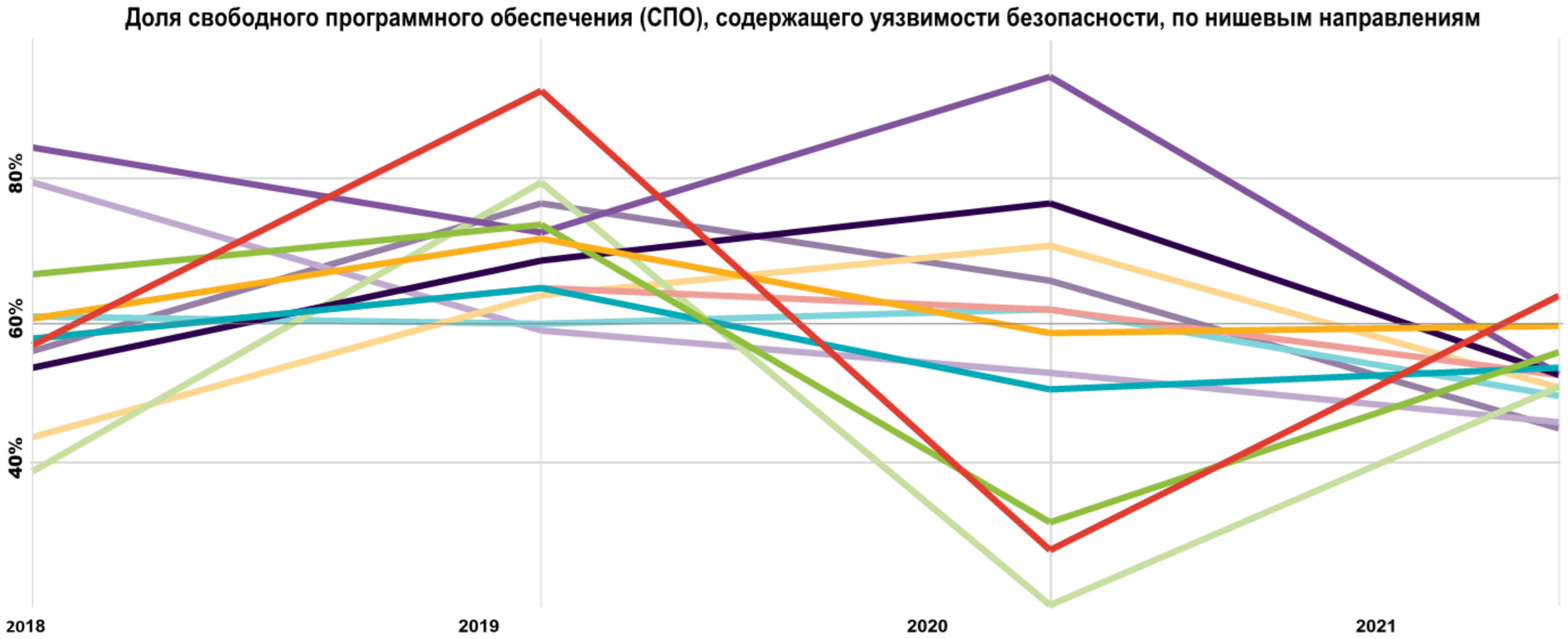
- Log4j (CVE-2021-44228): выявлена в 2021 г., регулярно эксплуатировалась в течение 2022 г., в т.ч. в критических системах промышленной автоматизации и IIoT, включая АСУ ТП и SCADA, системы управления энергопотреблением (EMS) и рабочие инженерные станции

- Систематическая проблема: на 2022 г. доля незашифрованного трафика в сетях IoT (включая сервисы для промышленных систем) составляла от 82 до 91%, оставшаяся доля шифровалась в основном протоколом SSL

6

Динамика уязвимостей в библиотеках СПО для IoT

ЭКОНОМИКА



64% Интернет вещей
60% Транспортный сектор, автоиндустрия, авиакосмическая отрасль
56% Интернет и мобильные приложения
54% Образовательный сектор
53% Маркетинговые приложения и сервисы
53% Сервисы для энергетики и устойчивого развития
53% Финансовые сервисы
51% Ритейл и электронная коммерция
51% Промышленное производство и робототехника
50% Корпоративное ПО-как-услуга (SaaS)
46% VR, игровая индустрия, онлайн-медиа и сфера развлечений
45% Здравоохранение и медицина

Источник: Open Source Security and Risk Analysis Report 2022 (OSSRA)

7

Картина уязвимостей в ПО промышленного IoT

ЭКОНОМИКА

- В 2021 г. рост числа выявленных уязвимостей безопасности IoT и АСУ ТП (16% и 50% соответственно) многократно превысил общую динамику уязвимостей в ИТ-продуктах (+0,4%)

- Из 797 уязвимостей АСУ ТП, выявленных за вторую половину 2021 г., 128 (17%) составили уязвимости в ПО и оборудовании IoT, причем 60 из них (8%) пришлось на нишу медицинских устройств IoT (всего за 2021 год в АСУ ТП было выявлено 1439 уязвимостей против 942 годом ранее)

- В 2021 г. выявлено 19 уязвимостей нулевого дня, включая критические, такие как Ripple20, в библиотеке TCP/IP компании Treck Inc., широко используемой для разработки сервисов IoT

- Log4j (CVE-2021-44228): выявлена в 2021 г., регулярно эксплуатировалась в течение 2022 г., в т.ч. в критических системах промышленной автоматизации и IIoT, включая АСУ ТП и SCADA, системы управления энергопотреблением (EMS) и рабочие инженерные станции

- Систематическая проблема: на 2022 г. доля незашифрованного трафика в сетях IoT (включая сервисы для промышленных систем) составляла от 82 до 91%, оставшаяся доля шифровалась в основном протоколом SSL

8

Угрозы ИБ для инфраструктур и сервисов IIoT

ЭКОНОМИКА

Атаки, эксплуатирующие инфраструктуры IoT:

- Ботнеты: обновленный Mirai, Gafgyt, Simps, Zhtrap и проч.
- Лаборатория Касперского зафиксировала двукратный рост атак ботнетов на инфраструктуру IoT в 2021 г. по сравнению с 2020 г.
- 2022 г. – еще более высокие темпы активности ботнетов на базе скомпрометированной инфраструктуры и устройств IoT (100+%)
- Тренд 2022 г.: использование скомпрометированной инфраструктуры IoT для криптомайнинга (Enemybot и др.)

Угрозы ИБ и атаки на OT IIoT:

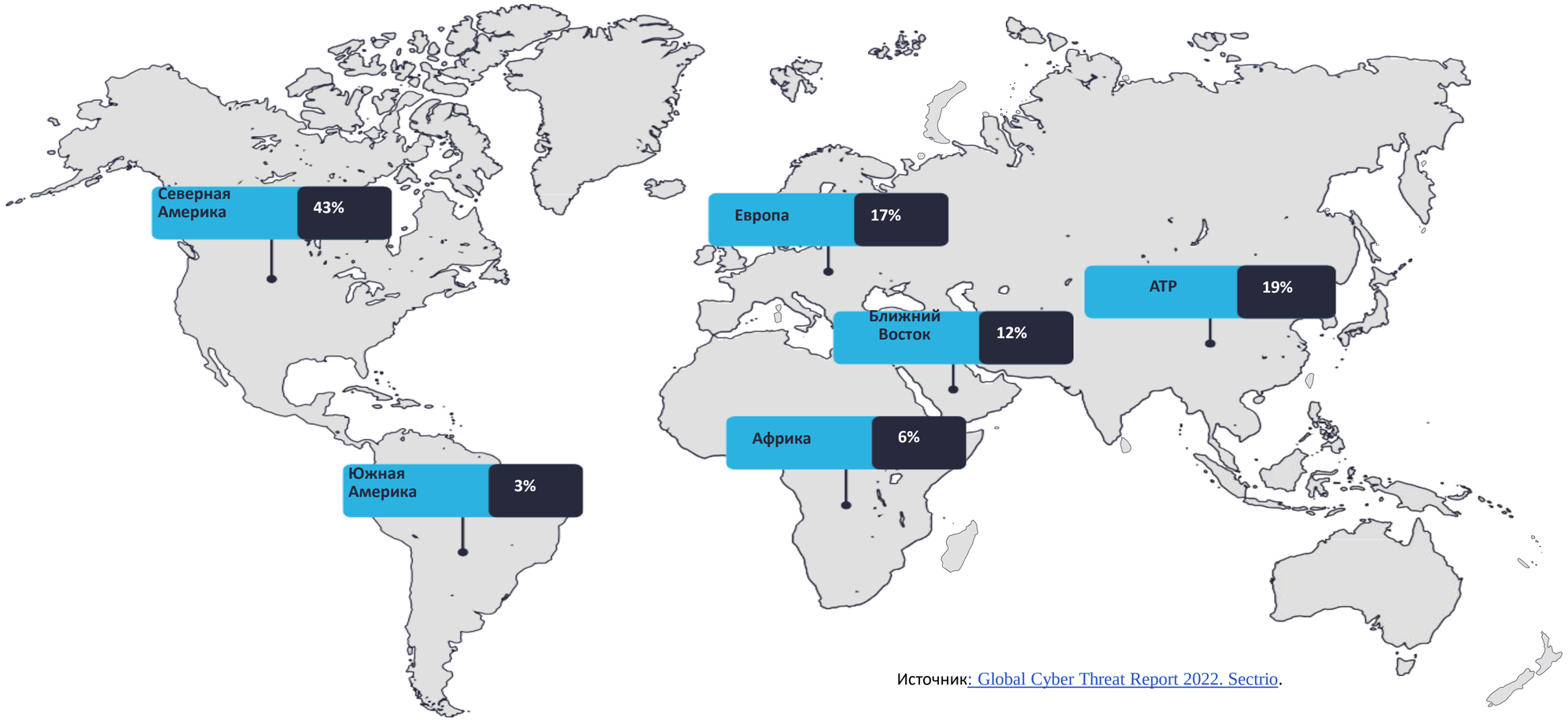
- WannaCry, Petya и NonPetya с 2017 г. по сегодня
- Colonial Pipeline в США: заражение привело к нарушению функционирования подключенной цифровой АСУ ТП
- JBS SA: парализовано управление ТП компании, включая работу подключенного оборудования на бойнях и конвейерах мясопереработки в США, Канаде и Австралии
- К 2031 г. общий ущерб от атак программ-вымогателей для компаний, использующих средства промышленной автоматизации, может достичь 265 млрд. долл. США

9

Географическое распределение атак на инфраструктуры и OT IoT

ЭКОНОМИКА

Географическое распределение кибератак на инфраструктуры IoT и операционные технологии (OT) в 2021 г.



Источник: Global Cyber Threat Report 2022. Sectrio.

10

Ключевые приоритеты для повышения защищенности инфраструктуры и сервисов IoT на ОКИИ: стандартизация

ЭКОНОМИКА

- Координация действий ТК 194 и других ТК Росстандарта для разработки отдельного комплекса технических стандартов ИБ для промышленного IoT (ТК 22, ТК 262, ПТК № 706) на 2024-2030 гг.

- Перспективная повестка стандартизации для ИБ IIoT:

  - Стандарты криптографической защиты информации (в том числе стандарты и спецификации криптографических систем, алгоритмов, функций и модулей) в сетях IIoT
  - Стандарты защиты информации в системах промышленной автоматизации и АСУ ТП;
  - Стандарты идентификации и аутентификации устройств и участников сетевых взаимодействий в сетях IIoT
  - Стандарты защиты данных в беспроводных протоколах IoT и сетях LPWAN
  - Стандарты ИБ облачных платформ и сервисов облачных вычислений IoT
  - Стандарты безопасности мобильных платформ и абонентских терминалов IoT
  - Стандарты безопасной передачи и обработки данных, собранных в рамках M2M-взаимодействий

- Международное сотрудничество в части стандартизации ИБ IIoT (КНР и другие страны БРИКС, площадки ИСО/МЭК и проч.)

11

Ключевые приоритеты для повышения защищенности инфраструктуры и сервисов IoT на ОКИИ: регулирование

ЭКОНОМИКА

- Обновление Концепции построения и развития узкополосных беспроводных сетей для IoT в РФ (утверждена Минцифры России приказом от 29 марта 2019 года N 113) в части требований к обеспечению ИБ IoT с учетом Указов Президента РФ №166 и №250, с целью скоординировать разработку и применение НПА и нормативно-технических актов в части разработки и утверждения требований по:
  - Применению стандартизированных, в том числе наложенных, решений по криптографической защиты каналов управления оборудованием и внутрисетевого трафика в промышленных сетях IoT (задача – обеспечить CIA M2M-данных, при этом существенно не снижая энергоэффективность сетей)
  - Применению средств сканирования сетевой инфраструктуры сети (систем мониторинга состояния оборудования) и средств обнаружения вторжений и атак на отдельные её компоненты и подсистемы
  - Применения средств сканирования сетевой инфраструктуры сети и средств обнаружения вторжений и атак на отдельные компоненты и подсистемы

- Разработка ФСТЭК России фреймворков к доверенному ПО и программно-аппаратным компонентам оконечных устройств и сетевого оборудования индустриального IoT

- Разработка ФСТЭК России отдельной модели угроз для цепочек поставок оборудования и ПО для сервисов IoT, включая как программную, так и аппаратную составляющие

12

ЭКОНОМИКА

Спасибо за внимание!

Олег Демидов

Ведущий аналитик
Направление «Безопасная открытая инфраструктура»