КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОНЛАЙН

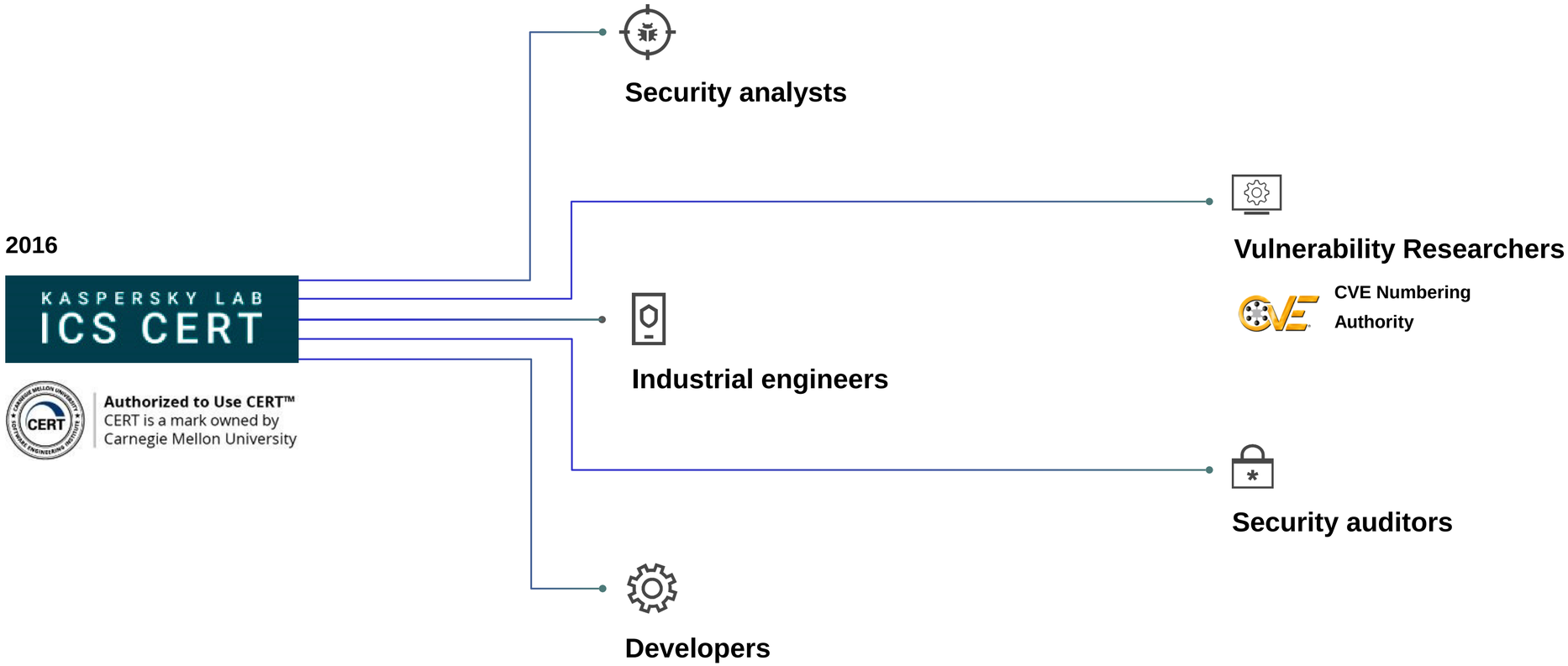
Ландшафт угроз для систем промышленной автоматизации. 2019 год

Азат Шайхутдинов
АО «Лаборатория Касперского»

Kaspersky Lab ICS CERT: Ландшафт угроз для АСУ ТП

Источники данных

- Kaspersky Security Network (KSN) и открытые источники
- Kaspersky Industrial CyberSecurity сервисные проекты
- Глобальные опросы



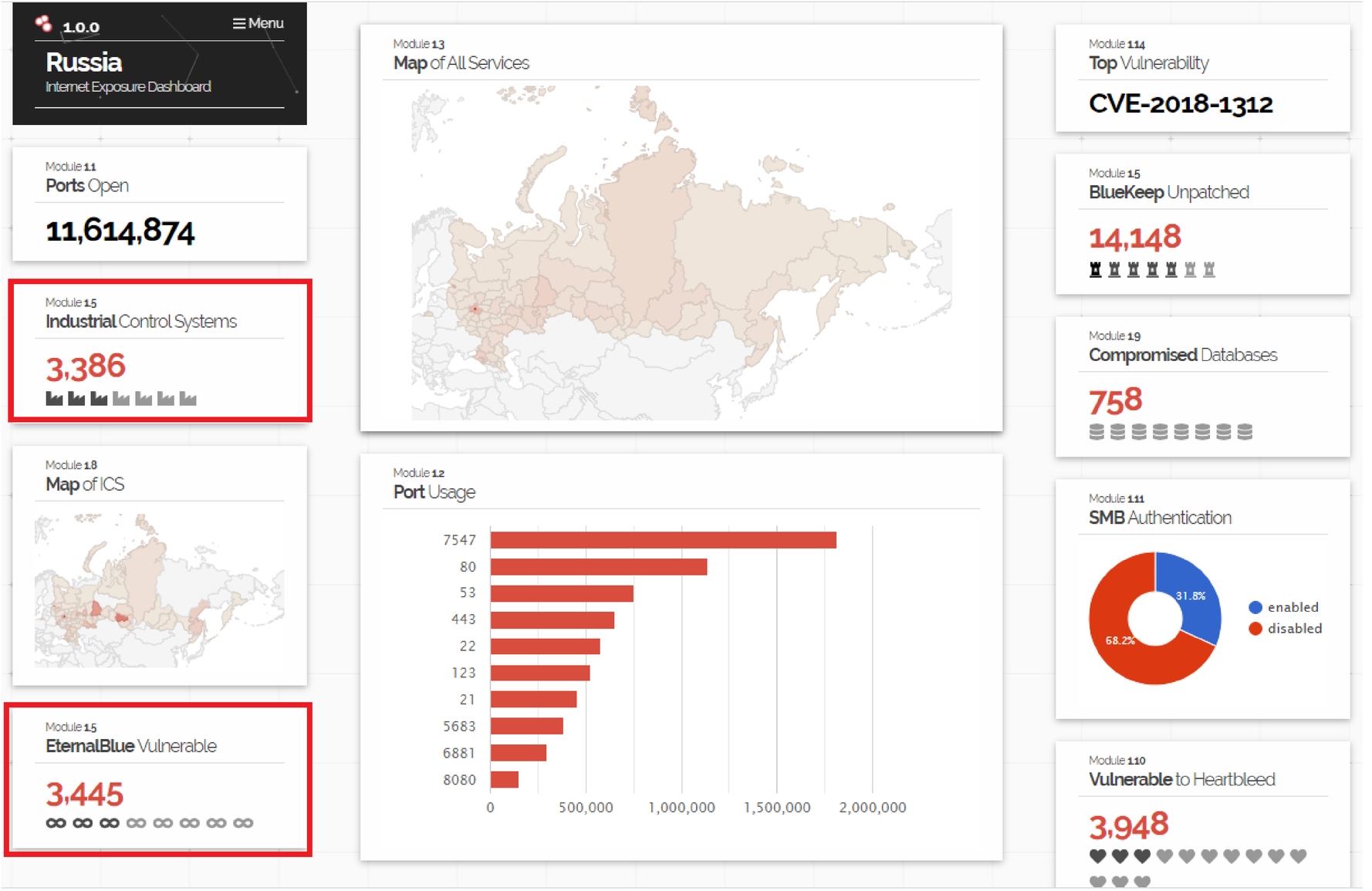
Методология исследования

Все статистические данные, использованные в отчете, получены с помощью распределенной антивирусной сети Kaspersky Security Network (KSN). Данные получены от тех пользователей KSN, которые подтвердили свое согласие на их анонимную передачу. В силу ограничений продукта и законодательных ограничений мы не идентифицируем конкретную компанию / организацию, от которой KSN получает статистические данные.

- **Компьютеры АСУ ТП защищенные продуктами Kaspersky Lab**
  - серверы управления и сбора данных (SCADA);
  - серверы хранения данных (Historian);
  - шлюзы данных (OPC);
  - стационарные рабочие станции инженеров и операторов;
  - мобильные рабочие станции инженеров и операторов;
  - Human Machine Interface (HMI)

Около 40% машин регулярно или постоянно подключаются к интернету

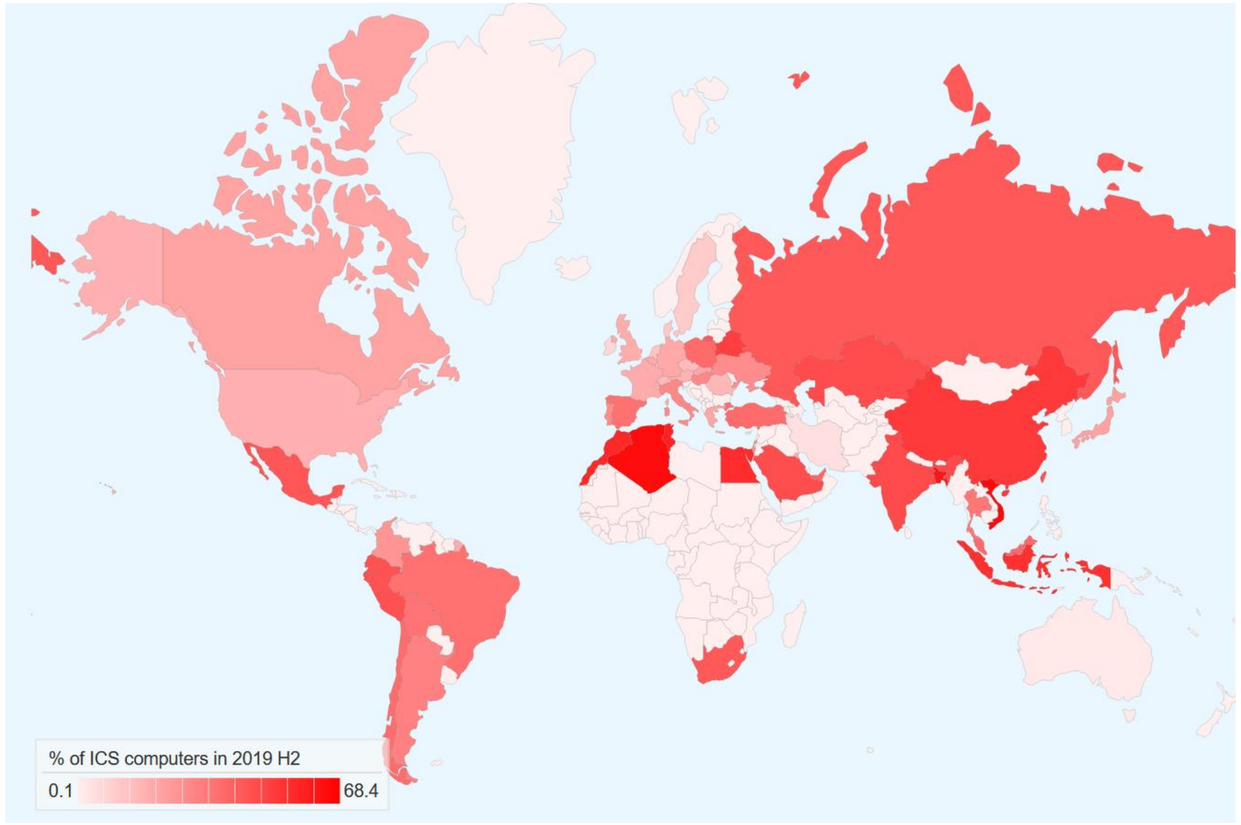
Подключенные компоненты АСУ к Internet в России



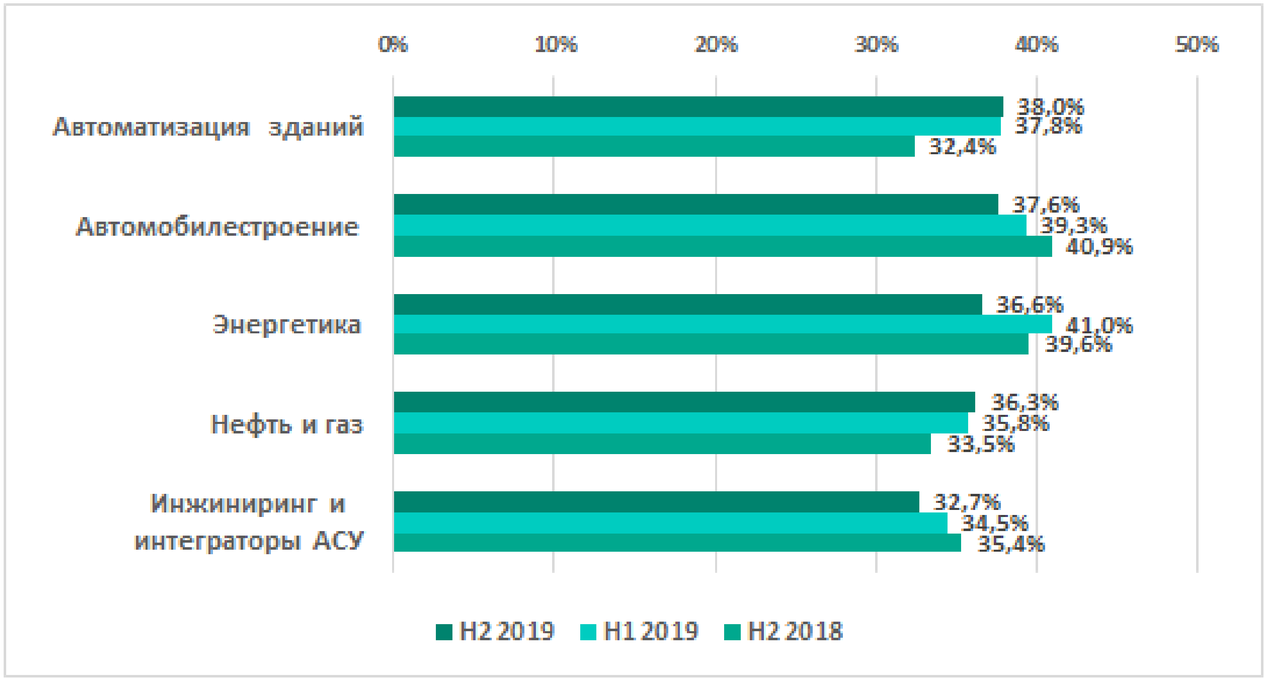
https://exposure.shodan.io/#/RU

KASPERSKY lab

География атак на системы промышленной автоматизации



География атак на системы промышленной автоматизации, второе полугодие 2019 (процент в стране компьютеров АСУ, на которых были задетектированы вредоносные объекты)

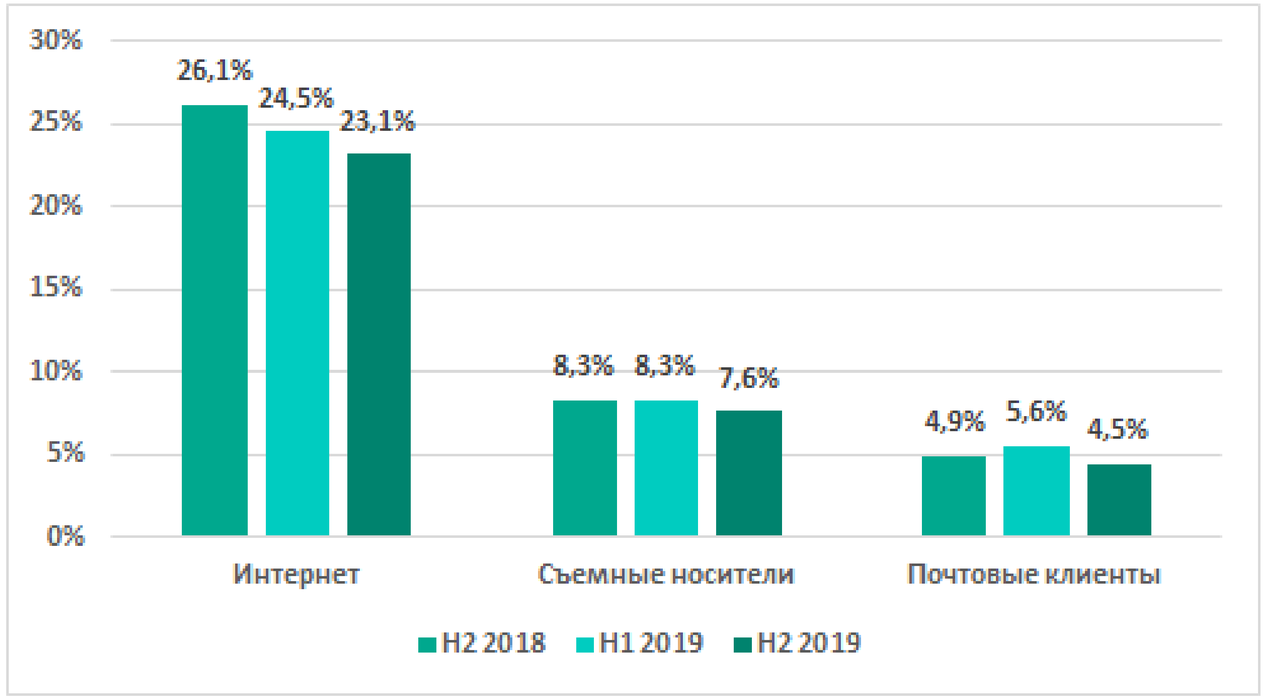


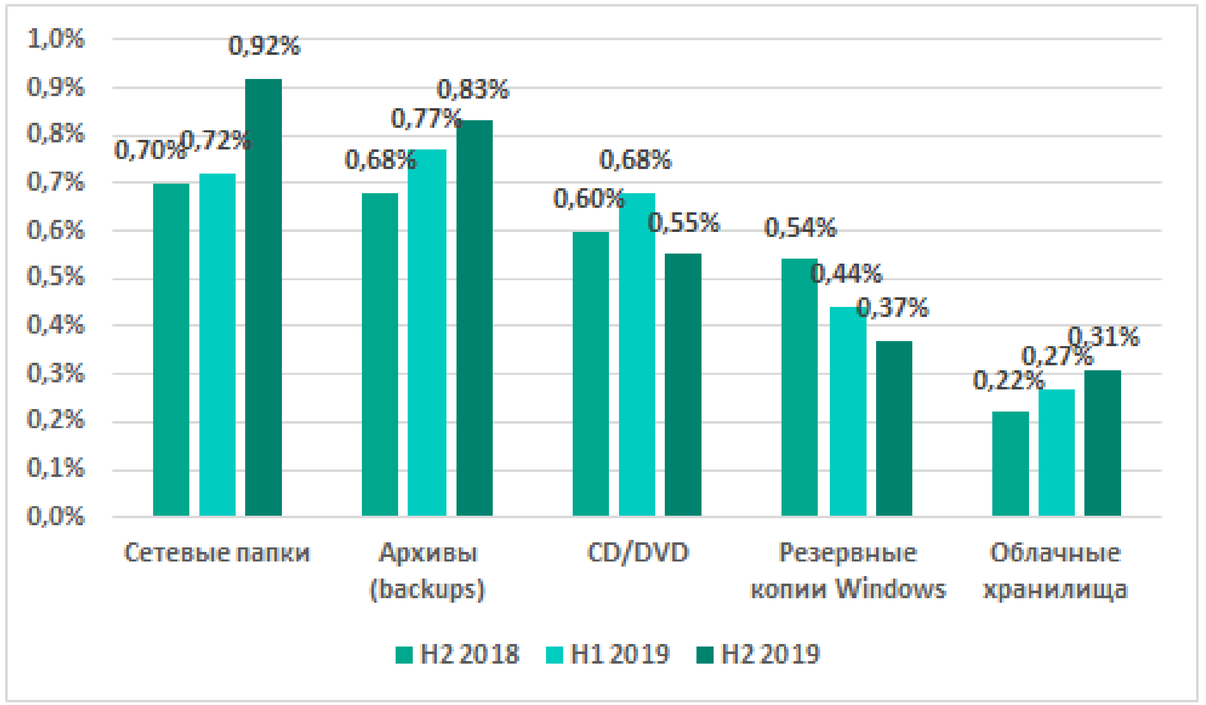
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых индустриях

Это только компьютеры АСУ на которых установленные продукты Kaspersky Lab отправляющие статистику в KSN

KASPERSKY lab

Основные источники и типы угроз заблокированных на компьютерах АСУ





Основными источниками угроз для компьютеров в технологической инфраструктуре организаций на протяжении последних лет являются интернет, съемные носители и электронная почта.
Но не стоит исключать и такие редкие источники, как архивы и т.д.

Основные причины проблем

- **Архитектура технологических сетей:**
  - Отсутствие разделение IT/OT;
  - Отсутствие сегментации и контроля доступа между OT подсетями;
  - Отсутствие сенсоров и средств кибербезопасности;
  - Устаревшие ОС и отсутствие процессов управления обновлениями

- **Поведение пользователей в технологических сетях:**
  - ***Неконтролируемое использование средств удаленного управления ;***
  - Отсутствие осведомлённости об угрозах кибербезопасности;
  - Отсутствие ответственности за обеспечение кибербезопасность АСУ ТП

Стеганография в атаках на промышленные предприятия, как индикатор уровня творческого подхода злоумышленников – пример из 2020 год

Данные сокрыты в изображении при помощи методов стеганографии и извлекаются вредоносной программой из пикселей, номера которых заданы алгоритмом. Использование стеганографии позволяет злоумышленникам обойти некоторые средства защиты, в частности, сканеры сетевого трафика.

https://ics-cert.kaspersky.ru/reports/2020/06/17/steganography-in-attacks-on-industrial-enterprises/

Kaspersky ICS CERT: ICS/IIOT Vulnerability Research

Некоторые из АСУ ТП вендоров которым мы помогли

SIEMENS

EMERSON

GE

NR

CODESYS

MITSUBISHI ELECTRIC

MOXA®

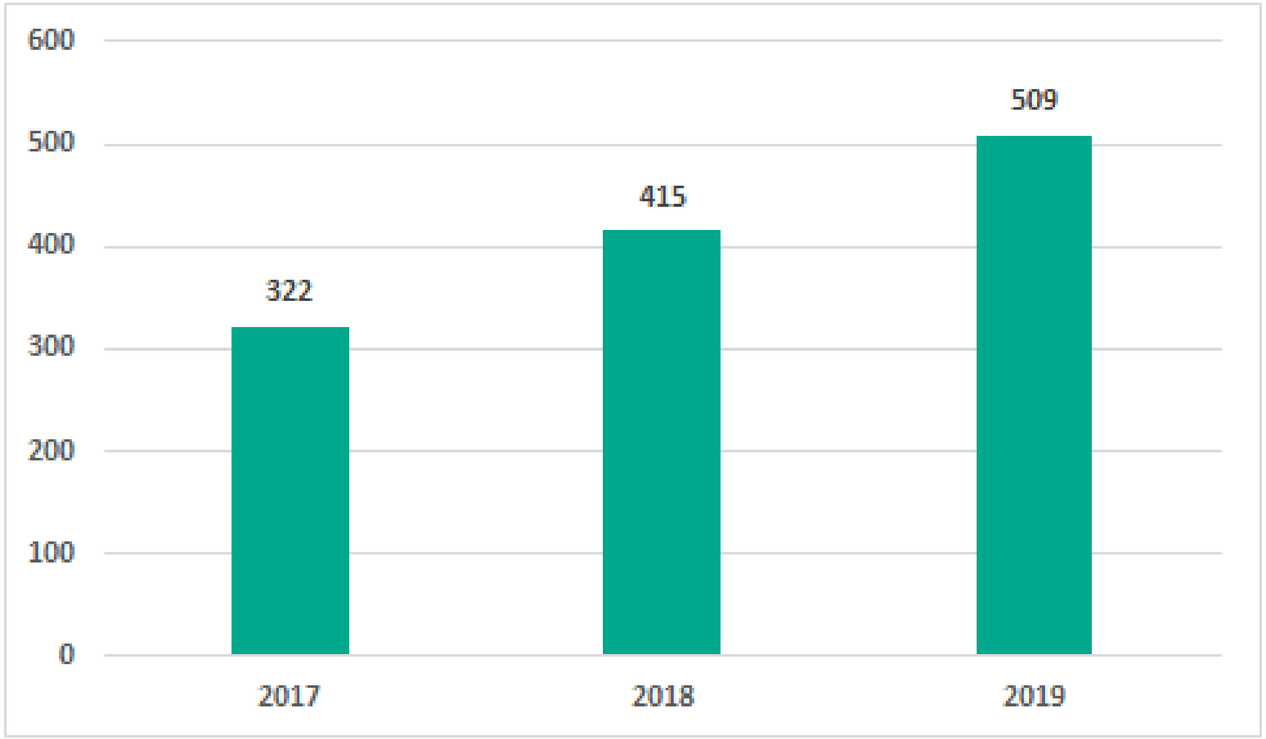
AUTOMATEDLOGIC
United Technologies

Fidelix

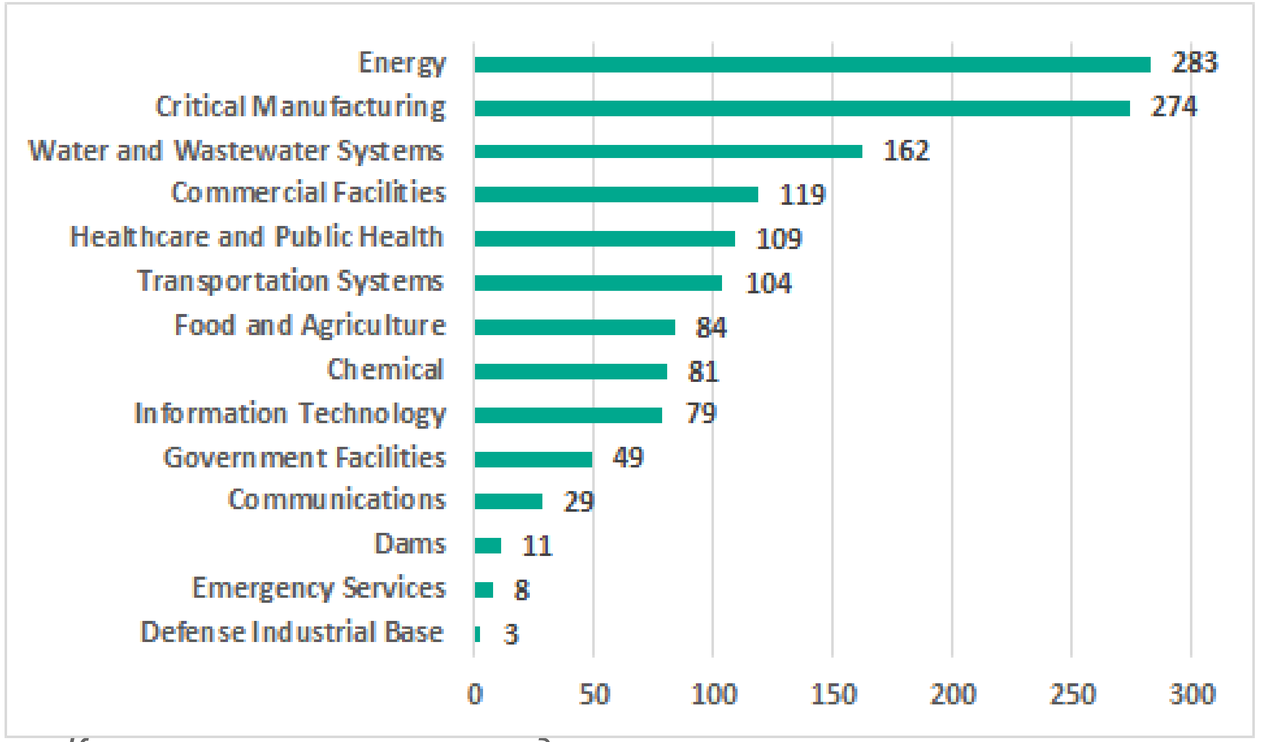
OPW
RETAIL FUELING
a DOVER company

https://ics-cert.us-cert.gov/advisories

Уязвимости в АСУ ТП обнаруженные в 2019



Количество уязвимостей в разных компонентах АСУ ТП, опубликованных на US ICS-CERT

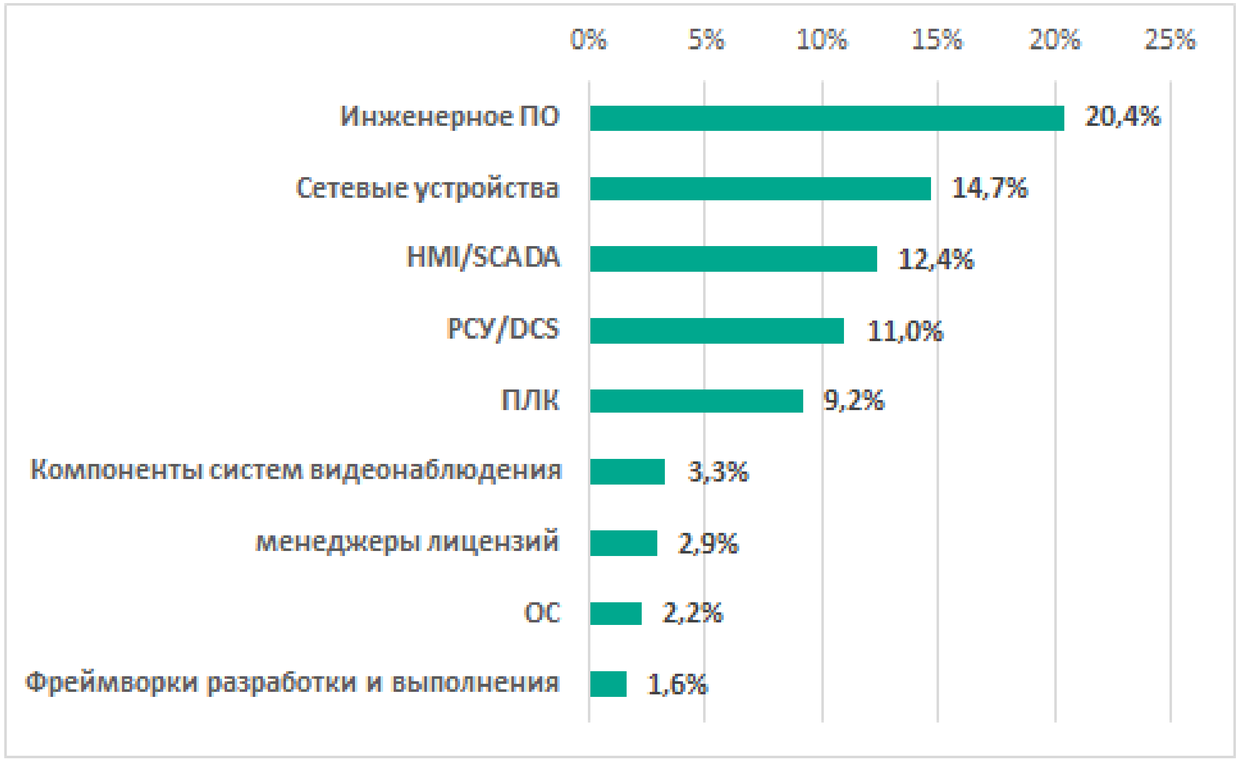


Количество уязвимых продуктов, используемых в различных отраслях (US ICS-CERT 2019)

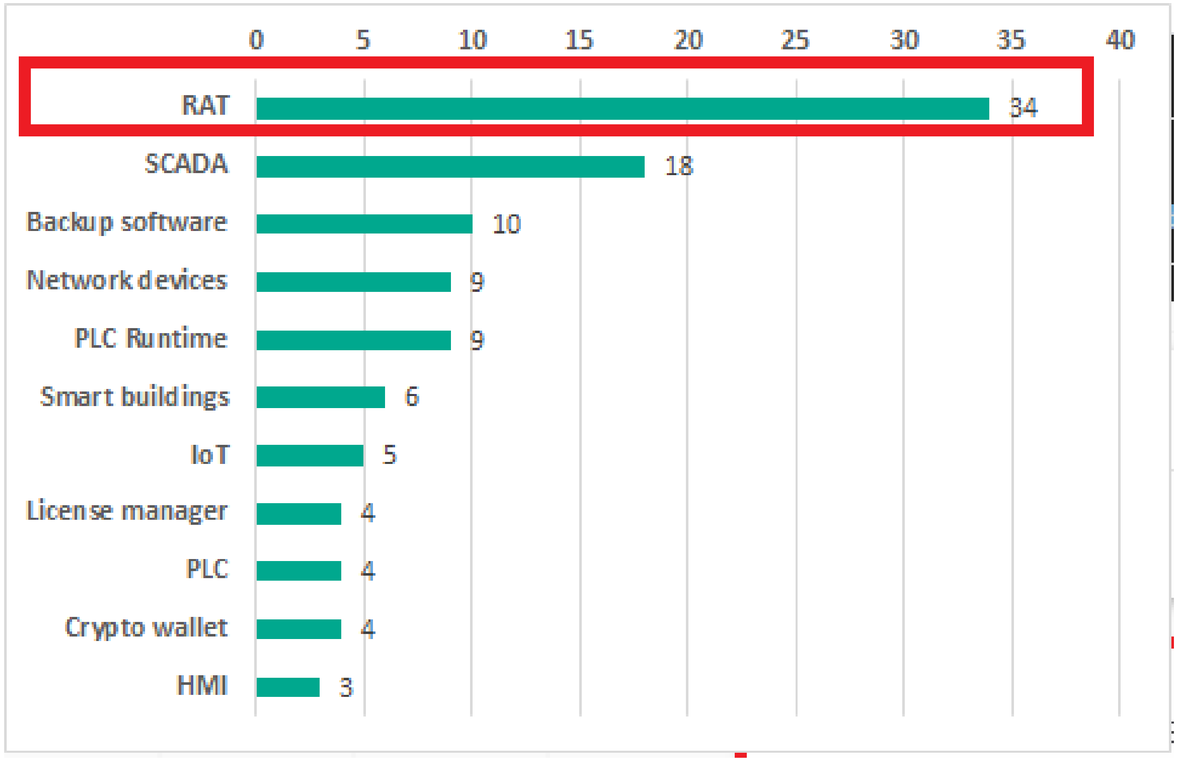
Оценка степени риска	от 9 до 10 (критическая)	от 7 до 8,9 (высокая)	от 4 до 6,9 (средняя)	от 0 до 3,9 (низкая)
Количество уязвимостей	97	249	143	18

Kaspersky Lab ICS CERT выявил **103 уязвимости** промышленных и IIoT/IoT систем в 2019.
33 из обнаруженных нами уязвимостей до сих пор не исправлены производителями соответствующих продуктов, хотя они получили для этого всю необходимую информацию.

Уязвимости в АСУ ТП обнаруженные в 2019 – влияние на 2020



Процент уязвимостей в различных компонентах АСУ ТП от общего числа уязвимостей.



Распределение уязвимостей, найденных Kaspersky ICS CERT в 2019 году, по типам исследованных компонентов

ПО / решение	Количество обнаруженных уязвимостей	Возможные последствия эксплуатации	Результат
RAT на основе VNC протокола	34	Уязвимости различного уровня критичности, некоторые позволяют выполнить произвольный код как на серверной, так и на клиентской части	Уязвимости устранены производителем. https://ics-cert.kaspersky.ru/reports/2019/11/13/vnc-vulnerability-research/

Уязвимостей разных уровней

Уязвимости в операционных системах

Так, в связи с **проблемами безопасности в ОС RUGGEDCOM ROX II** в 2019 году оказались уязвимыми все промышленные устройства Siemens RUGGEDCOM под управлением этой ОС.
Кроме того, множественные уязвимости, обнаруженные в ОС реального времени VxWorks, затронули решения вендоров **Rockwell Automation, Schneider Electric, Xerox, Dräger.**
Еще одним примером масштабного влияния уязвимостей ОС на безопасность решений является обнаружение уязвимости TCP SACK Panic в ядре Linux. Эта **уязвимость затронула множество продуктов компании Siemens.**

Уязвимости в фреймворках разработки и выполнения программ

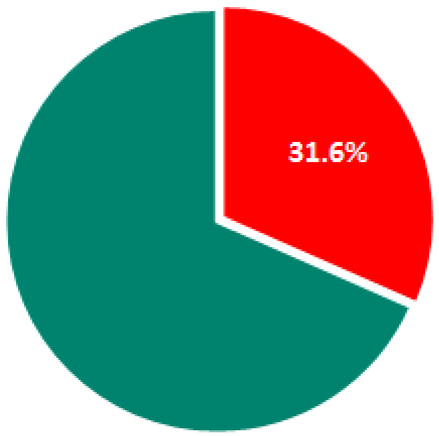
Отдельное внимание стоит уделить безопасности фреймворков, используемых вендорами для разработки и выполнения программ автоматизированного управления технологическим процессом. В 2019 году уязвимости были обнаружены сразу **в нескольких компонентах программного комплекса промышленной автоматизации CoDeSyS, включая веб-сервер, коммуникационный сервер и OPC UA сервер.**

Уязвимости в менеджерах лицензий

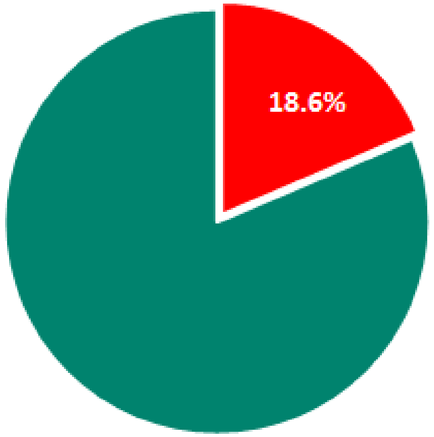
В 2019 году исследователи безопасности сообщили об уязвимостях сразу в нескольких менеджерах лицензий:
К примеру, за счет использования таких компонентов в составе различных решений уязвимости в них могут затрагивать сразу несколько промышленных продуктов. Так, распределенная система управления CENTUM VP и система автоматической противоаварийной защиты ProSafe-RS производства компании Yokogawa оказались подвержены уязвимостям, найденным в Yokogawa License Manager Service.

https://ics-cert.kaspersky.ru/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-vulnerabilities-identified-in-2019/

Использования инструментов RAT в АСУ ТП по данным KSN



Процент компьютеров АСУ, на которых легитимно установлены RAT



Процент RAT, установленных вместе с продуктами АСУ, среди всех обнаруженных RAT на компьютерах АСУ

https://ics-cert.kaspersky.ru/reports/2018/09/20/threats-posed-by-using-rats-in-ics/

Угрозы использования инструментов удаленного управления в АСУ ТП – как ни как актуально в 2020 на фоне массового перехода на удаленку

Средства удаленного администрирования широко используются в промышленных сетях для мониторинга, управления и обслуживания АСУ. Возможность проводить манипуляции удаленно существенно снижает стоимость обслуживания АСУ. Средства часто используются для:

- Для управления/мониторинга HMI с АРМ оператора (в том числе для вывода информации на большой экран);
- Для управления/обслуживания HMI с АРМ инженера;
- Для управления SCADA с АРМ оператора;
- Для обслуживания SCADA с АРМ инженера или компьютера подрядчика/вендора (из внешней сети);
- Для подключения множества операторов к одному АРМ оператора (архитектура а-ля тонкий клиент для экономии расходов на лицензии софта для АРМ);
- Для подключения из технологической сети через HMI к компьютеру в офисной сети с целью выполнения на нем различных задач (просмотр почты, доступ в интернет, работа с офисными документами).

Обзор рекомендаций по безопасной удаленной работе для предприятий критической инфраструктуры и не только

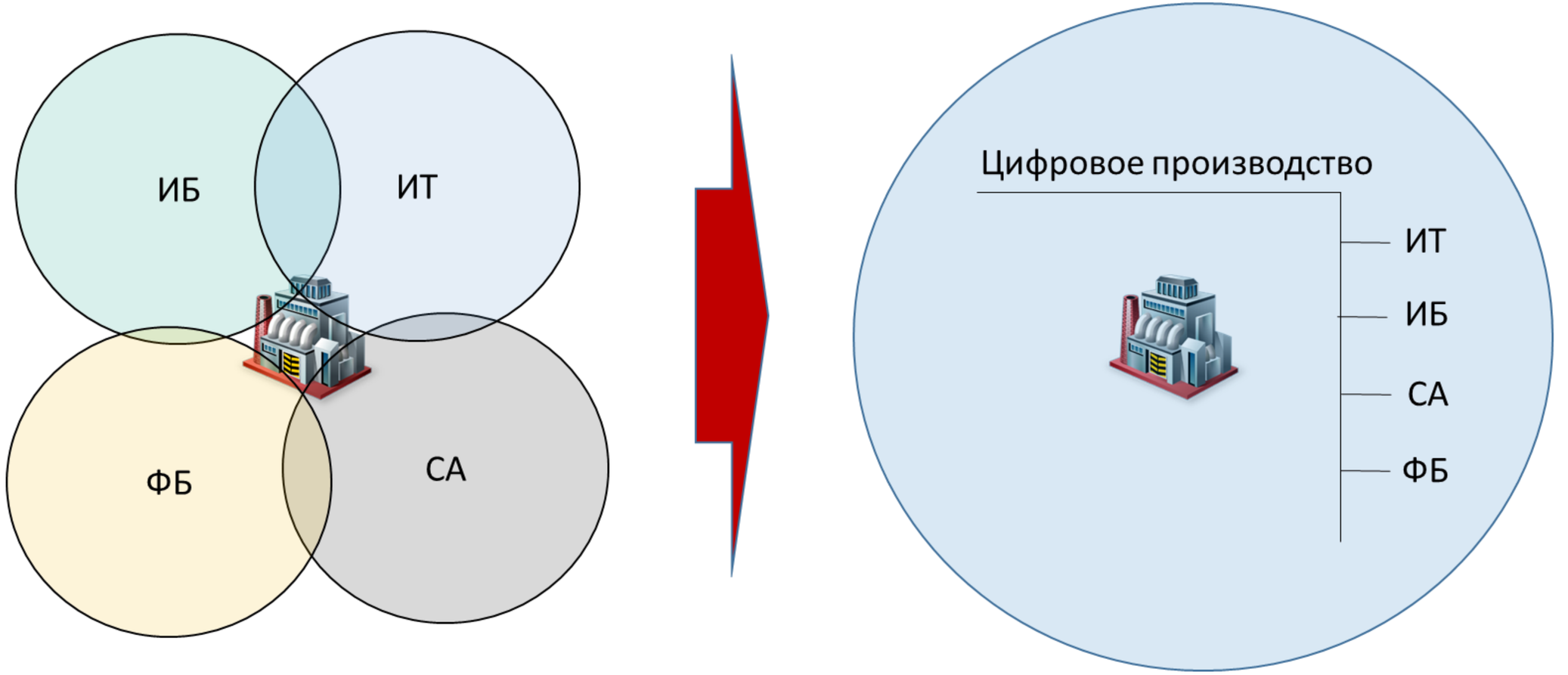
1. В России рекомендации по обеспечению безопасности объектов КИИ при удаленной работе в связи с COVID-19 опубликовала **ФСТЭК России**.
2. Национальный координационный центр по компьютерным инцидентам выпустил уведомление об угрозах безопасности информации, связанных с пандемией коронавируса.
3. Институт SANS в документе «Security Awareness Deployment Guide – Securely Working at Home» собрал список своих материалов, которые могут быть полезны для проведение обучения сотрудников по безопасной работе из дома.
4. Национальный институт стандартов и технологий США (NIST) выпустил бюллетень, содержащий рекомендации по безопасному удаленному доступу и удаленной работе.
5. Американское агентство кибербезопасности и безопасности инфраструктуры (CISA) опубликовало документ, в котором рассмотрело вопросы обеспечения кибербезопасности организаций в рамках глобального процесса управления рисками, связанными с COVID-19.
6. Агентство Европейского союза по кибербезопасности (ENISA) опубликовало советы по кибербезопасности при удаленной работе.

Сравнение рекомендаций по безопасной удаленной работе в условиях COVID-19

Рекомендации	ФСТЭК	НКЦКИ	SANS	NIST	ENISA	CISA

https://ics-cert.kaspersky.ru/reports/2020/04/30/secure-remote-work-for-critical-infrastructure/

Возможны соответствующие организационно-кадровые изменения



ИБ – информационная безопасность ИТ –Информационные технологии АС – системы автоматизации ФБ – функциональная безопасность

Kaspersky

«Инжиниринг безопасности систем — модель зрелости возможностей»

Увеличение сложности атак:

- по средствам социальной инженерии
- по средствам «прямого» воздействия на элементы
- по средствам проникновения в промышленную сеть

Фактические можно только «грубо» остановить производственный процесс (и то с определённой подготовкой)

Отсутствие возможности защититься
при использование не безопасных компонентов (и/или сервиса ИБ от поставщика)

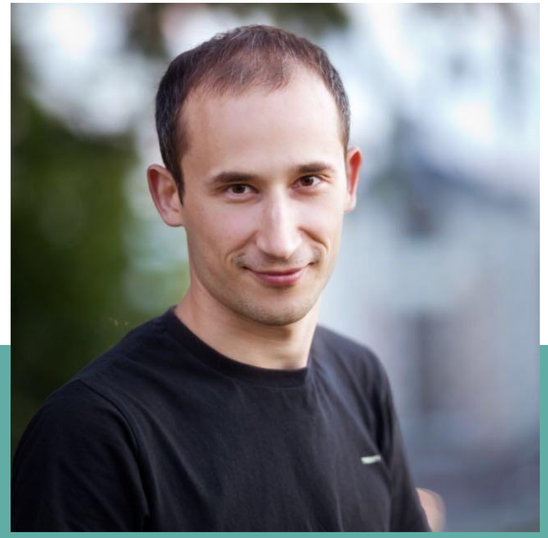
Kaspersky

Перспективные технологии ИБ АСУ ТП

- **Системы комплексной аналитики** производственных процессов
- **«Роботизированные»** системы администрирования средств и процессов ИБ
- **Системы поддержки принятия решений** по управлению производством (с учётом ИБ)
- **Системы автоматизированного категорирования /проектирования/ОРД**
- **Безопасные ОС**

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ



Азат Шайхутдинов
Менеджер по развитию бизнеса. Защита АСУТП
Azat.Shaykhutdinov@Kaspersky.com
+7 917 92 000 78
ics.kaspersky.com