

Kaspersky Industrial Cybersecurity Conference 2021

Системный подход к защите КИИ

Кирилл Набойщиков
Лидер направления защиты КИИ
Лаборатория Касперского

kaspersky

15000

Заказов

Бизнес-результат

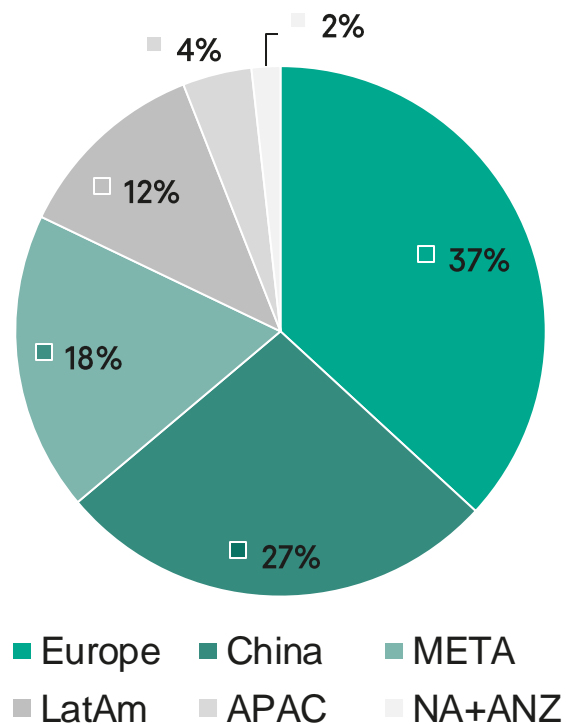
**Уверенная
десятизначная
выручка**

350 промышленных заказчиков

250 сетей защищено

**4x повышение эффективности
канального бизнеса**

Международные заказы



Глобальное присутствие
Конкуренция с иностранными решениями мотивирует развитие

Перспективы
Потенциал развития экспортного канального бизнеса

Партнёрская сеть
Сильный партнёр – в центре каждого успеха

Реализованные проекты

The logo for KAMAZ, featuring the word "KAMAZ" in a bold, blue, sans-serif font.The logo for BOSCH, consisting of a circular emblem with a stylized 'H' and the word "BOSCH" in a bold, red, sans-serif font.The logo for РОССЕТИ СЕВЕРО-ЗАПАД, featuring a blue circular emblem with a stylized globe and the text "РОССЕТИ СЕВЕРО-ЗАПАД" in a blue, sans-serif font.The logo for SIEMENS, featuring the word "SIEMENS" in a bold, teal, sans-serif font.The logo for Сетевая Компания, featuring a blue circular emblem with a stylized globe and the text "Сетевая Компания" in a blue, sans-serif font.The logo for WATERFALL, featuring a red and white stylized waterfall icon and the text "WATERFALL" in a bold, black, sans-serif font, with the tagline "Stronger Than Firewalls" in a smaller, red, sans-serif font below it.

Почему выбирают KICS?

- Качество и полнота реализации защиты
- Незначительное влияние на защищаемые устройства
- Высокая совместимость
- Удобство и простота эксплуатации и интеграции
- Сертификация ФСТЭК и ФСБ, наличие в реестре отечественного ПО

FROST & SULLIVAN

“ Kaspersky удостоен награды Global Company of the Year 2020 на рынке промышленной кибербезопасности.

FORRESTER®

“ Возврат инвестиций составил 135% от внедрения KICS for Networks и 368% KICS for Nodes.

VDC | Research

“ Kaspersky – ведущий поставщик в категории промышленной кибербезопасности на основе оценок более 250 специалистов.

Сертификация 2020-2021



Разрешено вендорами

Получено 15 сертификатов на 25 систем



Протестировано

С 3 российскими и 11 зарубежными производителями систем автоматизации



Проверено регулятором

Получены сертификаты от двух Российских регуляторов



Международный стандарт

Соответствует ГОСТ МЭК 62443 4-1:2018
- не ниже 3 уровня зрелости

Центр экспертизы по корпоративным решениям

Поддержка ключевых
внедрений и пилотов

Сопровождение
заказчиков

Поддержка продаж

Интеграции и испытания



Об экспертизе

Kaspersky ICS CERT

Основные факты

30+ экспертов в поиске и анализе угроз и уязвимостей АСУТП

Обнаружили и помогли исправить
сотни 0-day в продуктах и технологиях для АСУТП

Написали 120+ коммерческих отчётов об угрозах и уязвимостях
Авторизованный CVE Numbering Authority (CNA)*

Авторизованы использовать торговую марку CERT**
Университетом Carnegie Mellon

Члены FIRST

... и других уважаемых организаций:



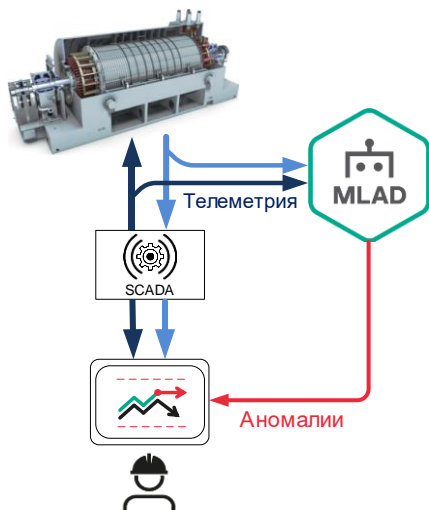
GLOBALPLATFORM®







* https://cve.mitre.org/cve/request_id.html#k

** <https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/authorized-users/index.cfm>

Kaspersky MLAD

детектор аномалий
на основе искусственного интеллекта



-  Предотвращение перегрева обмотки статора турбогенератора
-  Предсказание аварийной остановки газового компрессора
-  Защита от ошибок оператора металлообрабатывающего станка
-  Сокращение объемов брака в пищевой промышленности
-  Увеличение срока службы инженерного оборудования зданий
-  Выявление стрессового состояния оператора опасного производства



Экспресс-аудит

ICS Express audit на базе KICS Portable

31 устройство заказано
региональными офисами
и активно участвуют в
продажах и тест-драйвах
решения KICS for
Networks

14 экспертов HQ привлекались
к удалённым аудитам без
выезда за рубеж

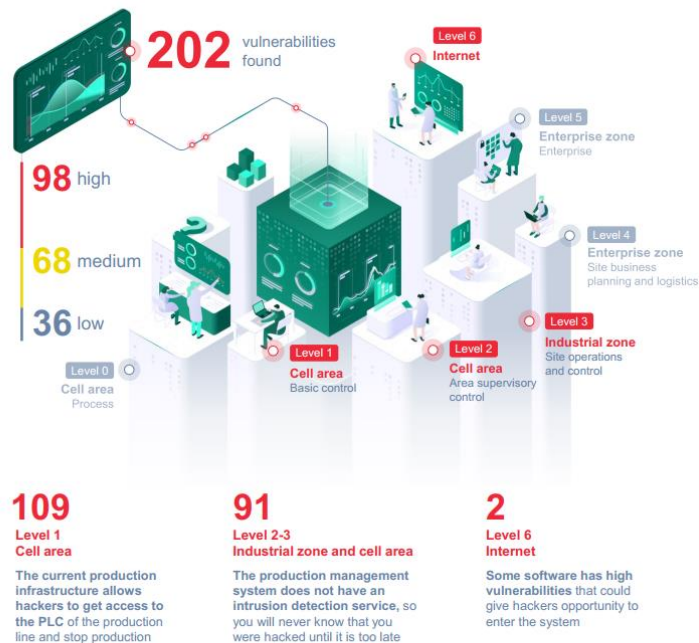
В первой половине 2021 года, в
среднем, презентуем клиентам
1 отчёт об аудите в месяц

В плане - 33% платных
экспресс-аудитов

Резюме для руководства

Инфографика с ключевыми выводами: найденные нарушения на каждом уровне АСУ и рекомендации по исправлению

EXECUTIVE SUMMARY



Summary of recommendations



Conduct a deep security audit to detect hidden vulnerabilities



Install software for monitoring changes in the production management system and filtering suspicious traffic



Implement a control policy for industrial network access by defining distinct areas in the network architecture

Система автоматизации

Интерпретация найденных KICS for Networks данных об активах и коммуникациях экспертом по автоматизации

THE SYSTEM



APPROACH TO OT NETWORK MONITORING AND DEPLOYMENT

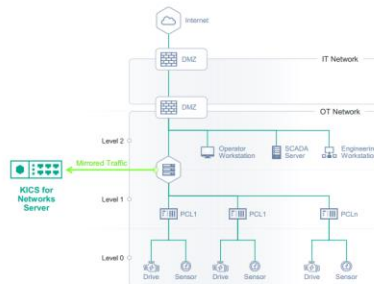
It is advised to execute OT network monitoring in passive mode by analysis of network traffic passing between Level 1 and Level 2 of Purdue ICS model. Such connection example is shown in picture below.

The product is connected to one of core Customer OT Ethernet switches, configured for traffic mirroring. The traffic from other network switches in infrastructure (not shown in the outlined diagram) is sent to the core switch via RSPAN technology, thus allowing us to receive and process all the relevant communication traffic from OT segment.

Product implementation process is as simple as connection of monitoring system to source of network traffic and enabling learning to whitelist legitimate network nodes and their network communications.

By having extended product integration capabilities the product may give additional advantages of:

- SIEM and/or Syslog server integration
- Mobile and e-mail alerting capabilities
- Integration to Kaspersky Security Center for local security event collection and reporting
- Integration to Kaspersky Machine Learning Anomaly Detection, allowing to use neural network and machine learning for process model definition and threat/anomaly detection based on this model and real-time process parameters' monitoring.
- Firewall integration and rule activation triggering via product API when necessary
- The listed items can be a subject of separate discussion and corresponding works.

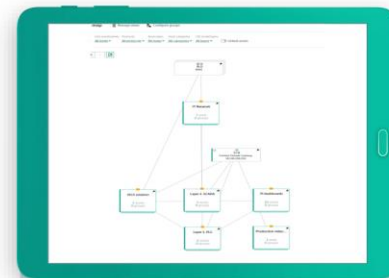


THE SYSTEM



DISCOVERED NETWORK COMMUNICATIONS

- **Level1_PLC** contains all PLCs discovered in Customer network.
- **Level2_SCADA** contains all SCADA, HMI and Engineering machines
- **KICS solution** contains all nodes of implemented KICS solution for infrastructure protection and monitoring from host server to KSC and KICS for Networks server
- **Production video monitoring** contains all machines responsible for video surveillance of manufacturing accuracy
- **PI dashboards** contains all nodes based on Raspberry PI for internal production dashboards
- **IT network** contains all hosts found in IT network infrastructure



Wide area network (WAN) object presence shows that some external communications are available

L2 network equipment (Ethernet switches) is not reflected on the communications diagram due to its transparency for network monitoring except Fortinet device, which works on L3 level of OSI network model and thus has been shown.

Выводы об уязвимостях системы

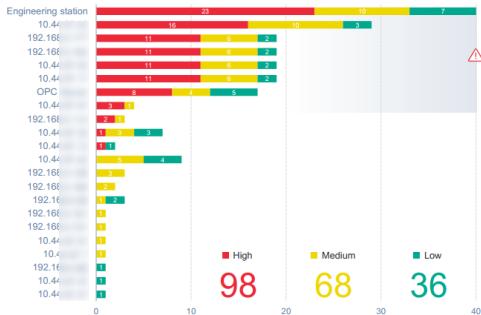
THE VULNERABILITIES AND FINDINGS

SECURITY FINDINGS AND YOUR INFRASTRUCTURE

We identified more than 200 security findings (vulnerabilities, configuration issues and other weaknesses) with different severity levels that relate to most of the resources in provided dataset for analysis.

Most vulnerable resource of industrial environment are PLCs

Engineering station and OPC Server.



Summary of security findings

- Can adversary get inside industrial network? Suspicious communications from industrial network to Internet were identified. Lack of network filtering and network segmentation
- Can adversary get access to resources in industrial network? Vulnerable and exploitable software, and weak passwords
- Can adversary impact industrial process? No protection of main automation components - PLCs

Summary of recommendations

- Perform full-blown security assessment to get complete picture of security issues and remediation guidelines, practical compliance violations and baseline security posture
- Following the remediation guidelines, learn to implement security with your system integrator and maintainers (in accordance with IEC 62443), and introduce compensational measures into the network
- Choose security operations friendly compensational measures (SOC-enabled) to jump-start your security maturity to a new level

THE VULNERABILITIES AND FINDINGS

SECURITY FINDINGS ON PURDUE MODEL

Where are all those findings in the industrial environment? Network traffic and role-based suggestion were made to map analyzed resources on Purdue model*. We also provide description of usual impact from exploitation of

targeted attacks or commodity malware infection (e.g. ransomware), are developed from the enterprise network segments. Network segmentation and filtering security issues that were identified during analysis are very critical, but not easily addressed topics in industrial network. Nevertheless, they should be considered one the first remediation steps to plan and implement.

Note, almost all real attacks on industrial networks, whether they are highly advanced

Level	Zone / Area	Security Findings	Quantity
Level 6	Internet	Adversary is able to access industrial network from Internet	2
Level 5	Enterprise zone, Enterprise	Adversary leverages access from enterprise to industrial network	0
Level 4	Enterprise zone, Site business planning and logistics	Absence of telemetry, operations and history process data	0
Level 3	Industrial zone, Site operations and control	Absence of control and supervisory over the process	91
Level 2	Cell area, Area supervisory control	Absence of control and supervisory over the process	109
Level 1	Cell area, Basic control	Process disruption or modification	0
Level 0	Cell area, Process	Long-term and direct process disruption or modification	0

Key takeaways

01

Test the security of enterprise network and possibilities to get inside the industrial network

02

Learn and keep track on techniques, tactics and procedures of real adversaries attacking industrial organizations

03

Simulate attack steps of real adversaries in your network and assess your detection and response capabilities

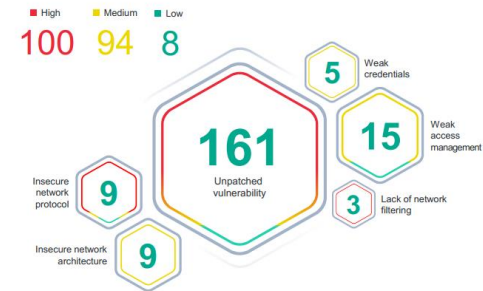
THE VULNERABILITIES AND FINDINGS

SECURITY FINDINGS DETAILS

Vulnerabilities proportion

What are the security findings identified during light assessment of provided dataset for analysis? Overwhelming number of findings came from unpatched vulnerabilities (lack of security updates), which is a widespread situation for industrial environments.

While being most widespread it is still important to address patch management: be aware of most critical vulnerabilities, have a process with system integrator to periodically update systems, have toolstack to detect exploitation of known vulnerabilities.



Vulnerabilities proportion

Light assessment methodology suggests that security findings will have different grades of certainty based on completeness of provided dataset for analysis. Probability of security findings ranges from low (which is more a suggestion) to high (evidence definitely suggest issue). Most of the issues have high or medium probability to be true positive.



Различия сервисов

Экспресс аудит

Узкая область анализа

Анализ трафика промышленного объекта

Методические ограничения

Выводы на основе сетевых взаимодействий

Удалённый анализ

- 1 аналитик-эксперт
- Без взаимодействия с собственником

Отчёт

15-20 страниц шаблонного отчёта

Минимальные рекомендации

Невозможность предоставления детальных рекомендаций по улучшению ситуации без изучения инфраструктуры

Вероятностный характер выводов

Возможность ложных выводов из-за неполноты данных

Оценка безопасности АСУ ТП

Полный анализ систем

Промышленные системы целиком попадают в область анализа

Методика без ограничений

Анализ сетевой архитектуры, трафика, хостов, тех. процесса, white/Grey box инструментальное тестирование, систем и компонентов АСУ (PLC, RTU, IED.) Детальные инструкции по противодействию угрозам, обнаружения угроз 0-day

Анализ на объекте

- Команда из 4-5 экспертов с разными областями экспертизы: сети, ИБ АСУ ТП, безопасность приложений, пен. тест, реверс-инжиниринг
- Непосредственный доступ к объекту анализа

Отчёт

- 90-200 страниц: уязвимости, стадии и процесс поиска, потенциальный вред, векторы
- 1-2 страницы отчёта для руководства

Подробные рекомендации по защите

Как действенные и практические рекомендации (обновление ПО, замена слабых паролей итп. Так и связанные с устойчивостью к атакам в долгосрочной перспективе (объекты и методы контроля, изменение архитектуры сети и т.п.)

Достоверные выводы

- Достоверно подтверждённые находки
- Действия симулирующие действия атакующего – проверка всех систем безопасности
- Практически и полезные результаты оценки

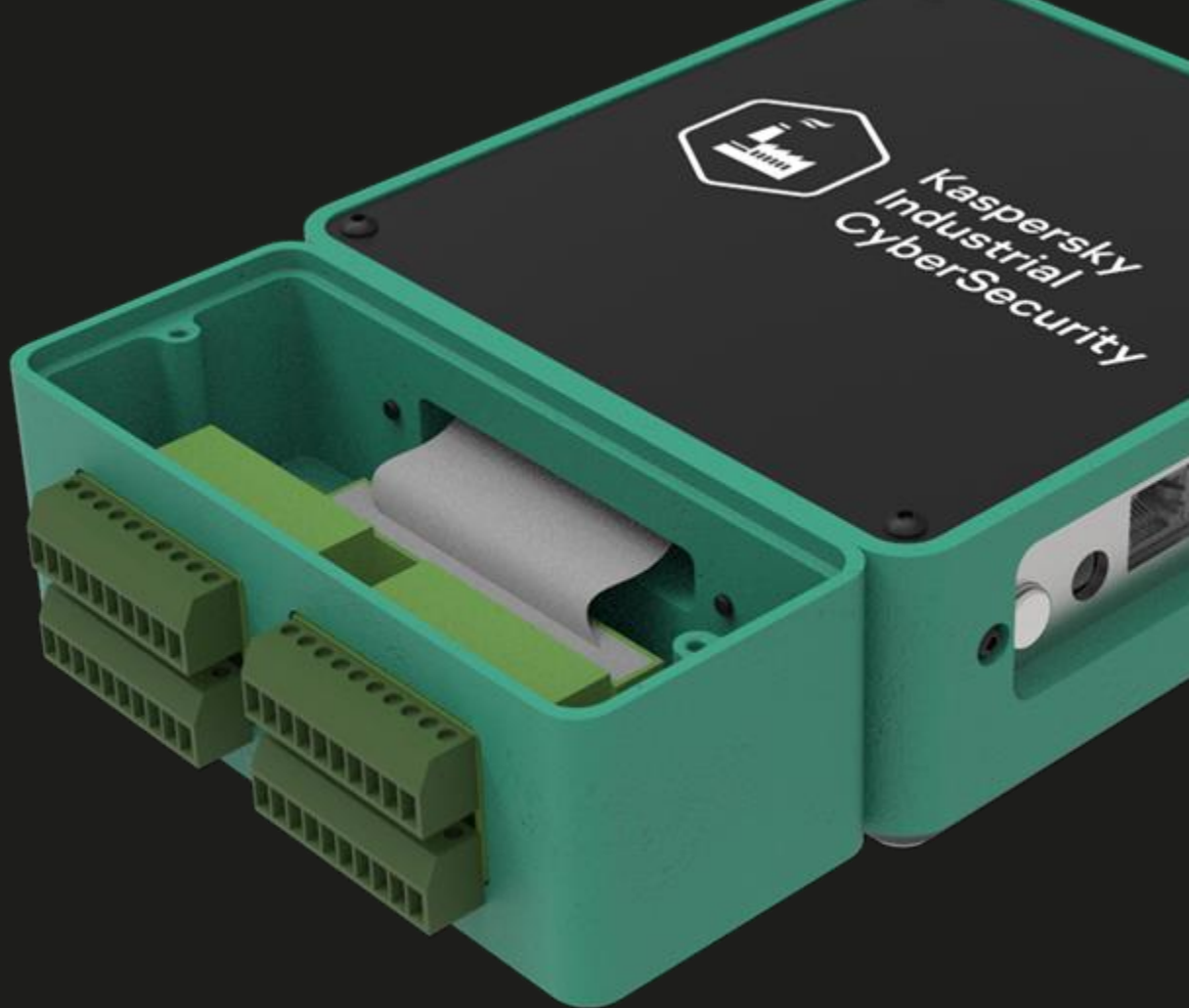
☞ Люди всерьёз работающие над программным обеспечением должны сделать своё оборудование

Alan Key

KICS Portable

Прототип

KICS Portable v.3 в
демо-зоне



Обновление продуктов

Ближайшие релизы.



В ближайшем релизе

Kaspersky Industrial CyberSecurity for Nodes 3.0

25 обновлений

Интеграция с KICS for Networks

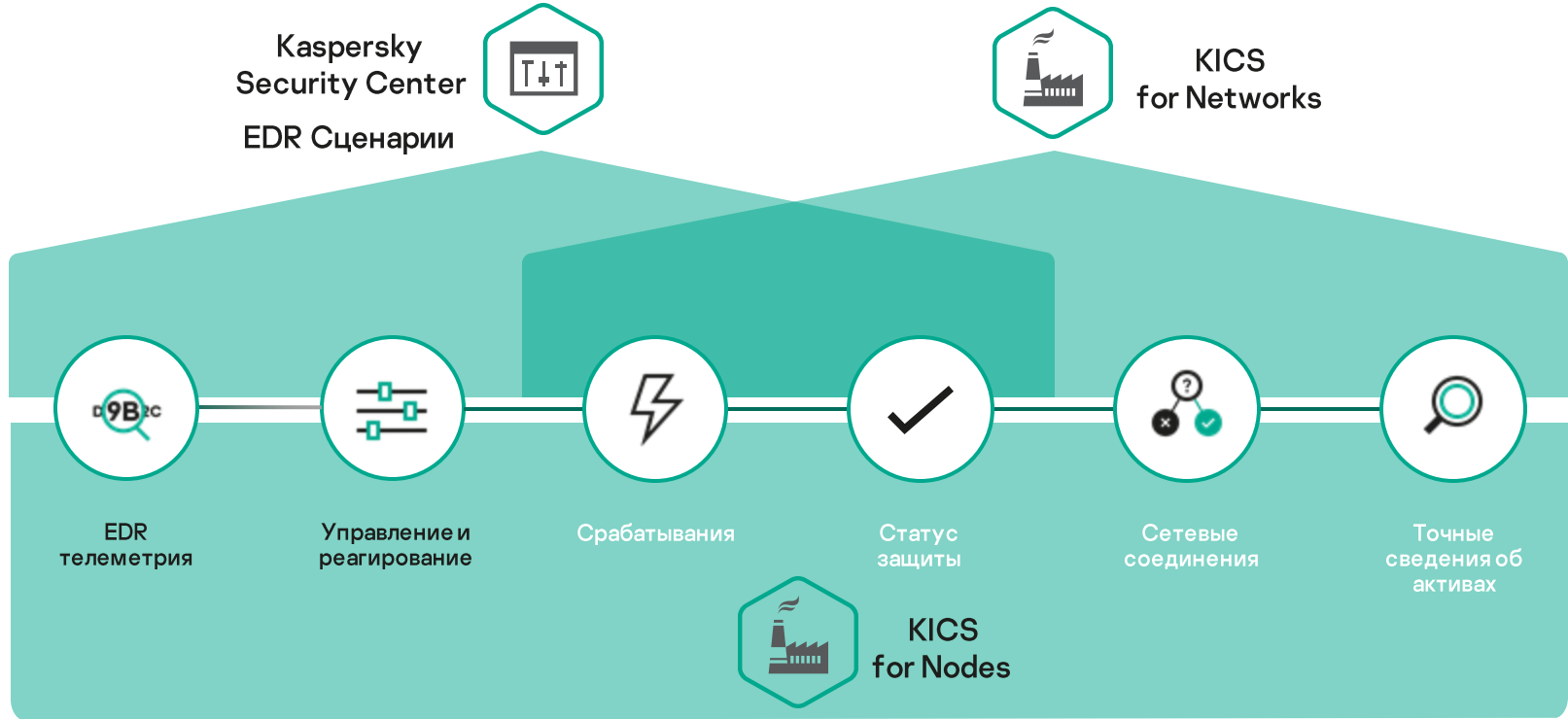
Защита от сетевых угроз

“Шаблоны” настроек для
некоторых систем АСУ ТП

Лицензирование “по подписке”

Ограничение потребления CPU

Интеграция



Новые функции

Kaspersky Industrial CyberSecurity for Networks

30 обновлений и улучшений

Интеграция с KICS for Nodes

Управление уязвимостями

Полнофункциональная веб-консоль

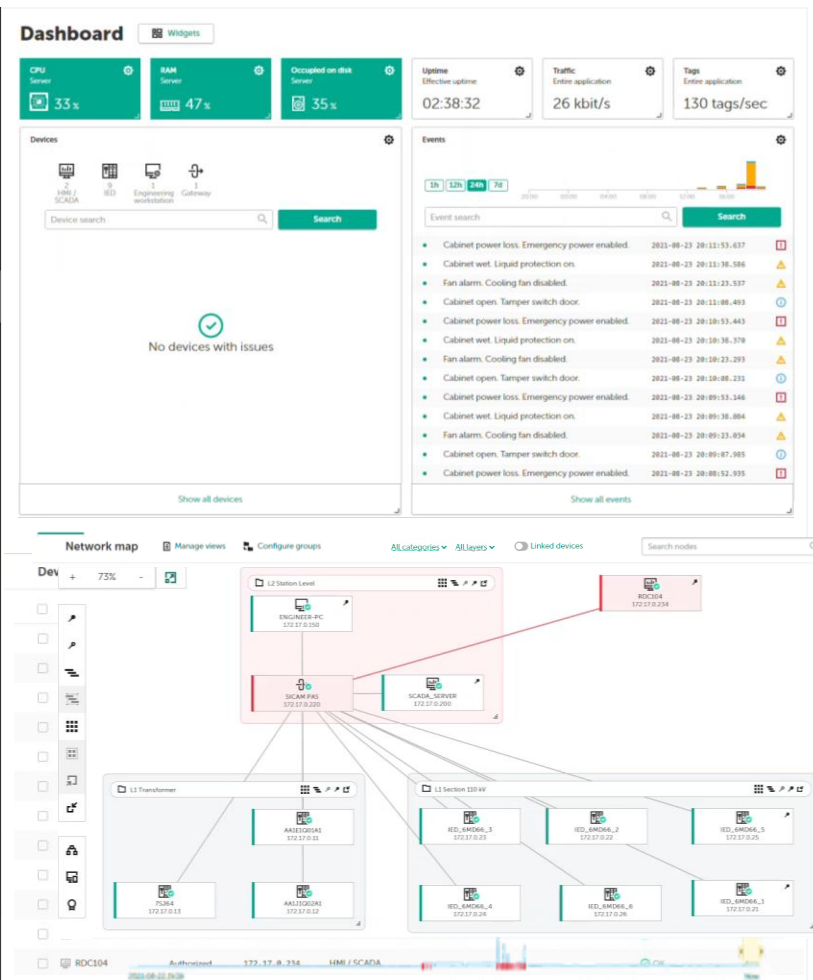
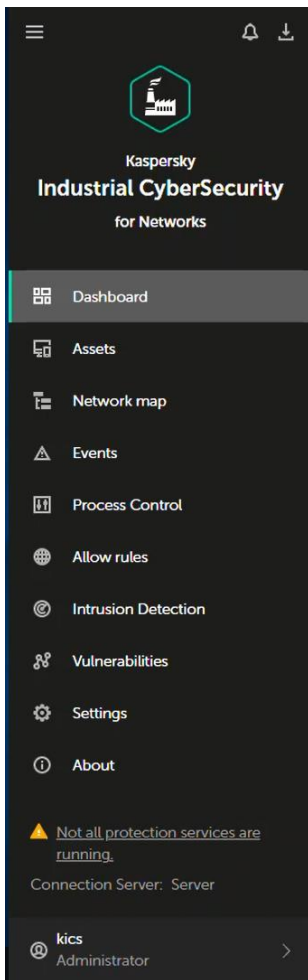
Новый дашборд

Тёмная тема

Версии для CentOS и Astra Linux

Рост производительности

Vulnerability management



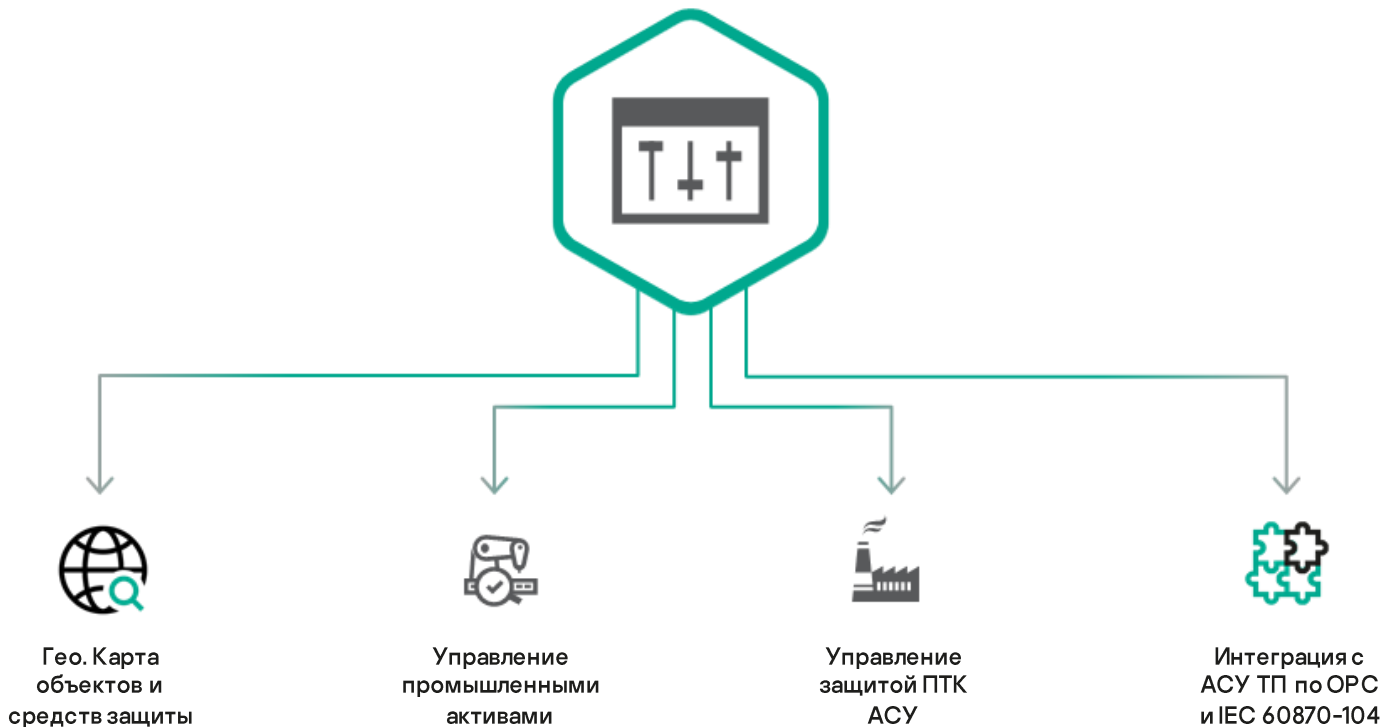
Данные об уязвимостях
Позволяют контролировать риски предприятия

Лучшие источники
Точные данные об уязвимостях - исследования Kaspersky ICS-CERT. Дополнительно - NVD и US ICS-CERT, БДУ

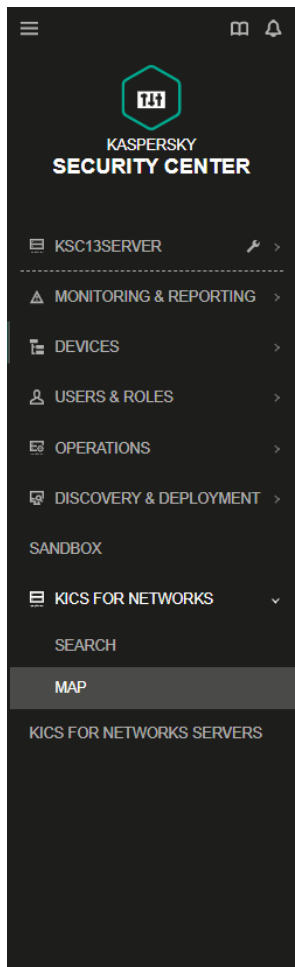
Наглядное информирование
Позволяет своевременно планировать меры противодействия

Центральное управление для крупных предприятий

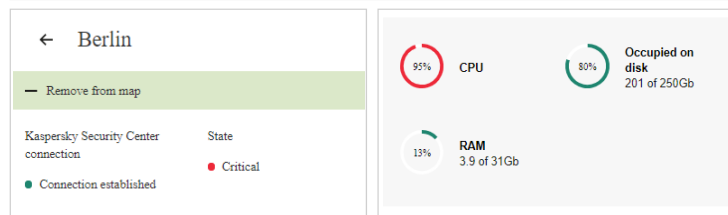
KASPERSKY SECURITY CENTER



KSC: для географически распределённых объектов



MONITORING & REPORTING / DASHBOARD



Мониторинг и управление

Kaspersky Security Center позволяет собирать данные с группы промышленных объектов

Навигация

Расположение СЗИ и объектов на карте с мгновенным переходом к детальным настройкам без дополнительного ввода пароля

Осведомлённость

Состояние защиты и полный контроль над ситуацией для крупных предприятий

Kaspersky ICS

5y Vision



Требования к защите

Промышленные
предприятия

Регулятор

Корп. центр

Сервисный
центр

Вендор

Региональный центр

Объект

Требования к защите

Промышленные предприятия

КОРПОРАТИВНЫЙ, ГОСУДАРСТВЕННЫЙ ИЛИ СЕРВИСНЫЙ ЦЕНТР МОНИТОРИНГА

 Predict

 Prevent

 Detect

 Respond

РЕГИОНАЛЬНАЯ
СЛУЖБА ИБ

КОРПОРАТИВНЫЕ
СИСТЕМЫ И СЕТИ

ТЕЛЕМЕХАНИКА И
УДАЛЁННОЕ
ОБСЛУЖИВАНИЕ

УПРАВЛЕНИЕ
АКТИВАМИ И
РИСКАМИ

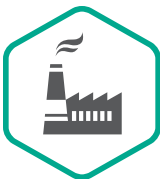
Автоматизация технологического процесса

Промышленный интернет
вещей

Технологии безопасности в промышленности



Сертифицированная защита Windows и Linux в КИИ



Мониторинг сети АСУ: обнаружение вторжений, сетевых атак и аномалий



Сервисы и пакеты экспертизы



Центры управления, мониторинга и реагирования



Машинное обучение и цифровые двойники



Контроль рисков, отчёты о соответствии требованиям



Инвентаризация АСУ, уязвимостей и цифровые двойники



Защита периметра и сегментация сети



Безопасное удалённое подключение

Создаём **экосистему** решений для
промышленных компаний любой
величины

CyberImmunity



Дмитрий Лукиян

Руководитель отдела управления корпоративными продуктами на базе KasperskyOS

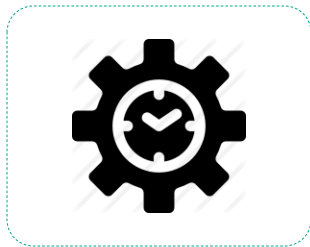
Лаборатория Касперского

Новые технологии – это новые возможности и новые вызовы

Дроны



Предиктивная аналитика



Роботизация



Автономный транспорт



Новые возможности



Новые вызовы ИБ



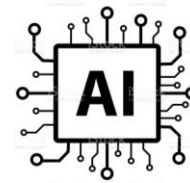
Интернет вещей



Сети 5G



Машинное обучение



Искусственный интеллект

Кибериммунитет



KasperskyOS

ОС нового поколения

Не является клоном Linux

Реализует концепции:
Microkernel, MILS, FLASK



Кибериммунные системы

системы, способные выполнять
определенный набор функций
под активной атакой, как уже
известной так и не известной

Кибериммунные продукты

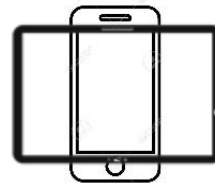
Шлюзы для
Интернет вещей



Тонкие клиенты
для VDI



Профессиональные
мобильные устройства



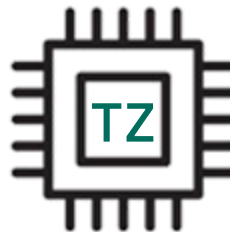
Транспорт



АСУ ТП



In Chip ИБ



Кибериммунные продукты

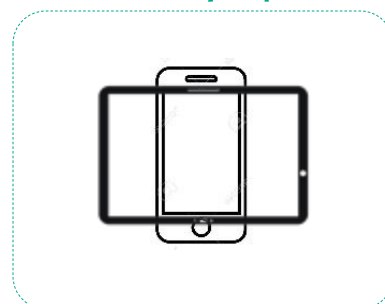
Шлюзы для
Интернет вещей



Тонкие клиенты
для VDI



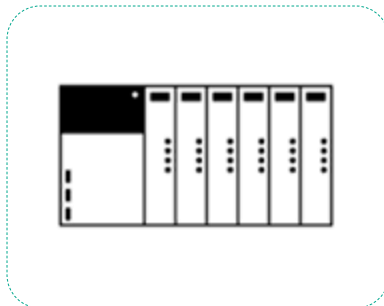
Профессиональные
мобильные устройства



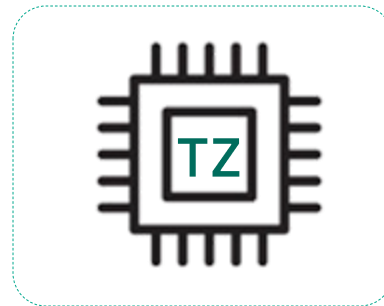
Транспорт



АСУ ТП



In Chip ИБ



Кибериммунные продукты

Шлюзы для
Интернет вещей



Тонкие клиенты
для VDI



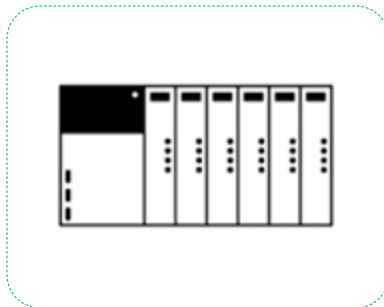
Профессиональные
мобильные устройства



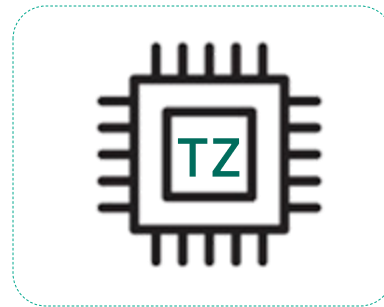
Транспорт



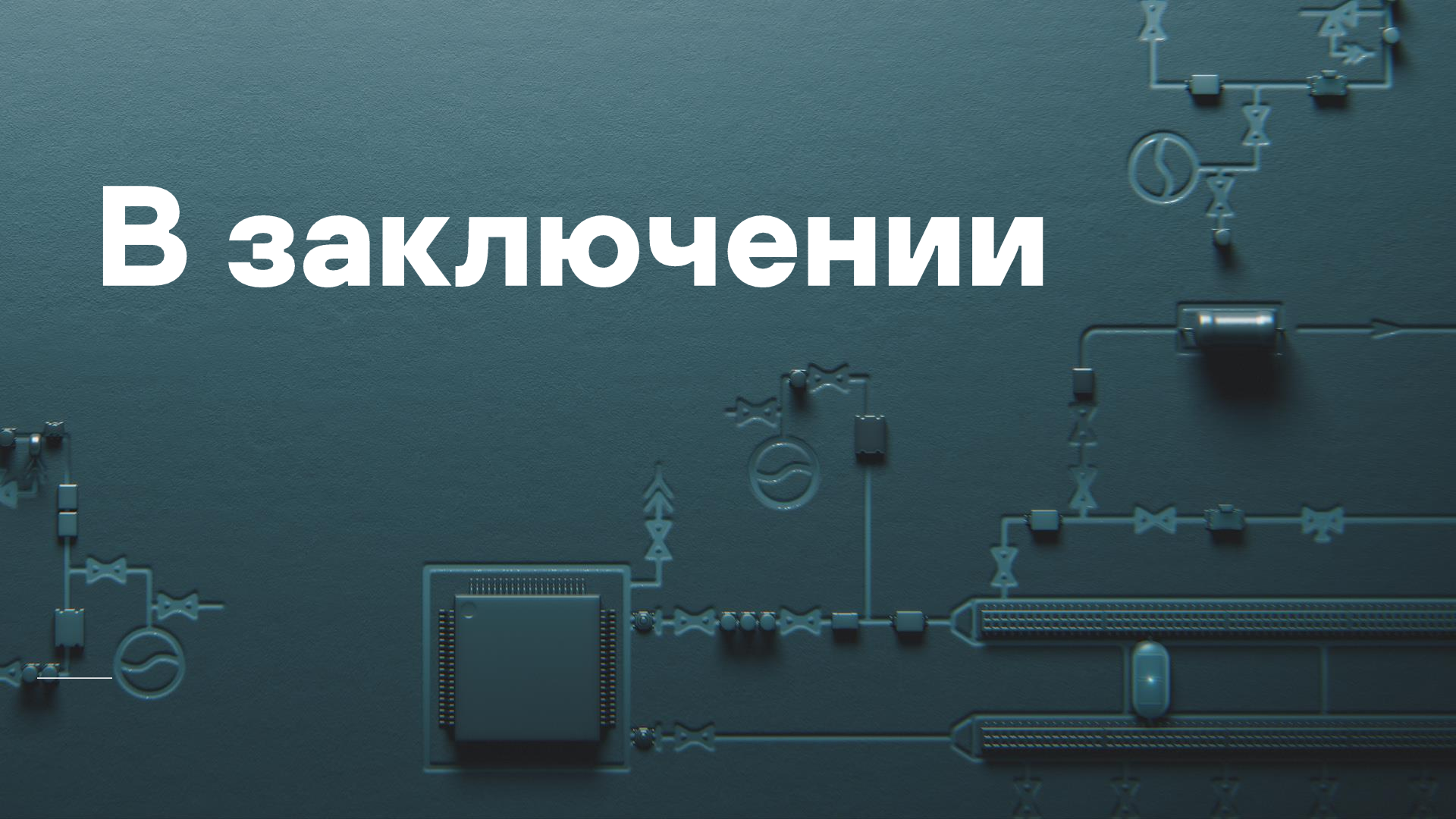
АСУ ТП



In Chip ИБ



В заключении



Thank you!

Let's bring on the future



Kirill Naboyshchikov

KICS Business Development

@LinkedIn

Dmitry Lukiyan

Head of KOS Enterprise products

@Kaspersky.com

kaspersky