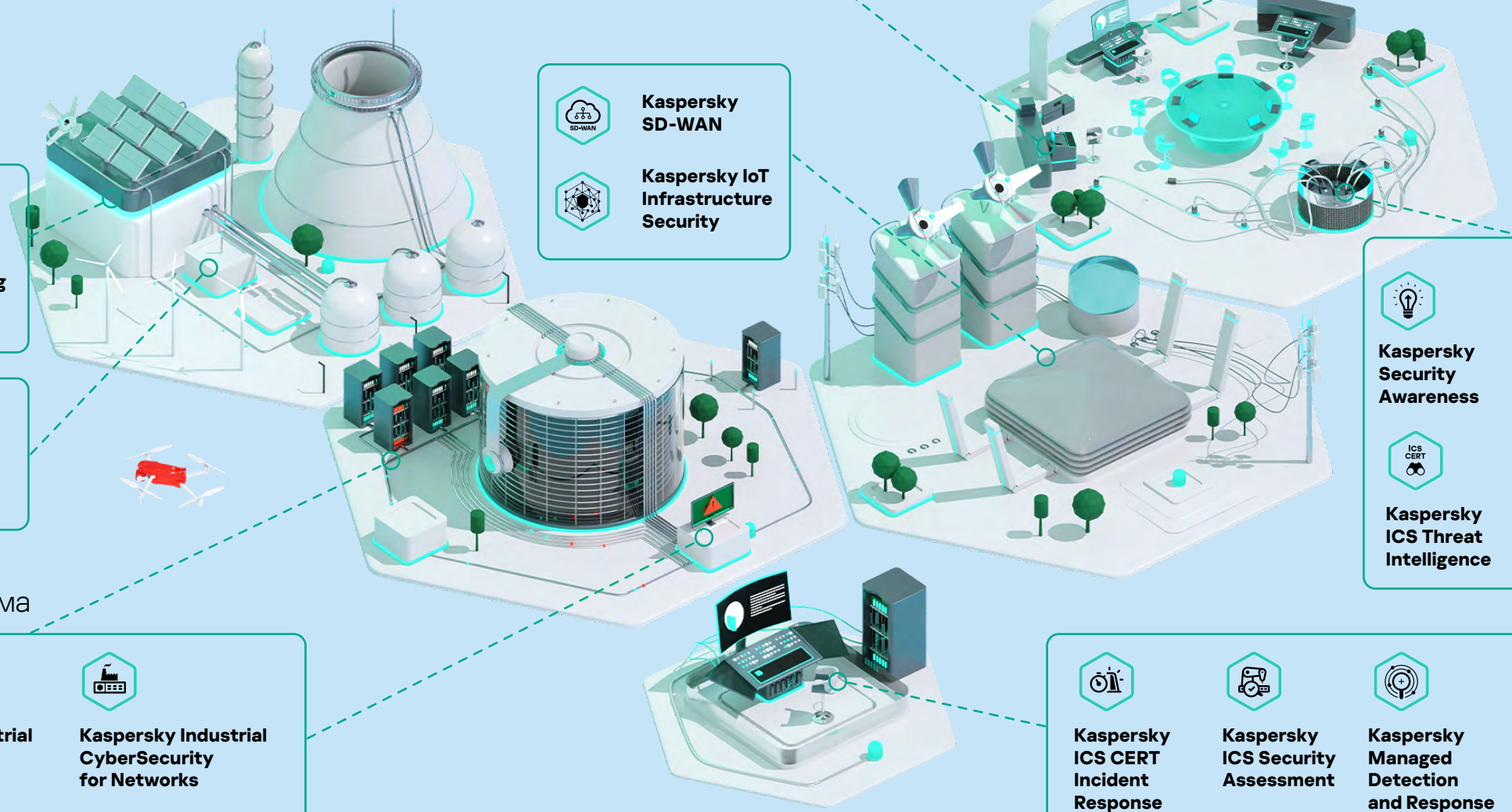
Экосистема промышленной безопасности



Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Secure Remote Workspace

Kaspersky SD-WAN

Kaspersky IoT Infrastructure Security

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Antidrone

Kaspersky Security Awareness

Kaspersky Ask the Analyst

Kaspersky ICS Threat Intelligence

Kaspersky ICS CERT Training

XDR-платформа

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Kaspersky ICS CERT Incident Response

Kaspersky ICS Security Assessment

Kaspersky Managed Detection and Response

Kaspersky Industrial Emergency Kit

Kaspersky Industrial CyberSecurity

Ключевые отрасли применения экосистемы

- Нефтегазовая и химическая отрасли
- Энергетика, в том числе атомная
- Металлургия и добыча полезных ископаемых
- Промышленное производство

Перспективные направления применения KOTCS

- Фармацевтика и медтехника
- Транспорт и логистика
- Телекоммуникации

Ключевым элементом экосистемы KOTCS является платформа Kaspersky Industrial CyberSecurity (KICS), предназначенная для защиты промышленных предприятий и объектов КИ и не оказывающая негативного влияния на непрерывность технологических процессов.

KICS

Нативная XDR-платформа KICS работает в самой глубине АСУ ТП[1], проводит глубокий анализ трафика и телеметрии узлов, активно реагирует на угрозы или просто информирует о них. Она помогает защищать от атак любой сложности современные цифровые и подключенные системы промышленной автоматизации, а также контролировать безопасность эксплуатации программно-технических комплексов прошлых поколений.

KICS обеспечивает полную видимость происходящего на всех уровнях технологического процесса: на уровне физических устройств, контроллеров, серверов SCADA[2] и системы управления производством. Платформа протестирована на совместимость с продуктами ведущих вендоров систем промышленной автоматизации, включая Siemens, Honeywell, B&R (ABB Group), Yokogawa, Emerson, Schneider Electric, Baker Hughes, GE и других.

Платформа KICS совместима со множеством АСУ ТП от 50+ вендоров

В составе платформы два тесно взаимосвязанных и дополняющих друг друга компонента: KICS for Nodes для защиты промышленных панелей оператора, рабочих станций и серверов и KICS for Networks — для мониторинга безопасности промышленнй сети.

KICS сегодня

~230 000
проданных лицензий KICS for Nodes

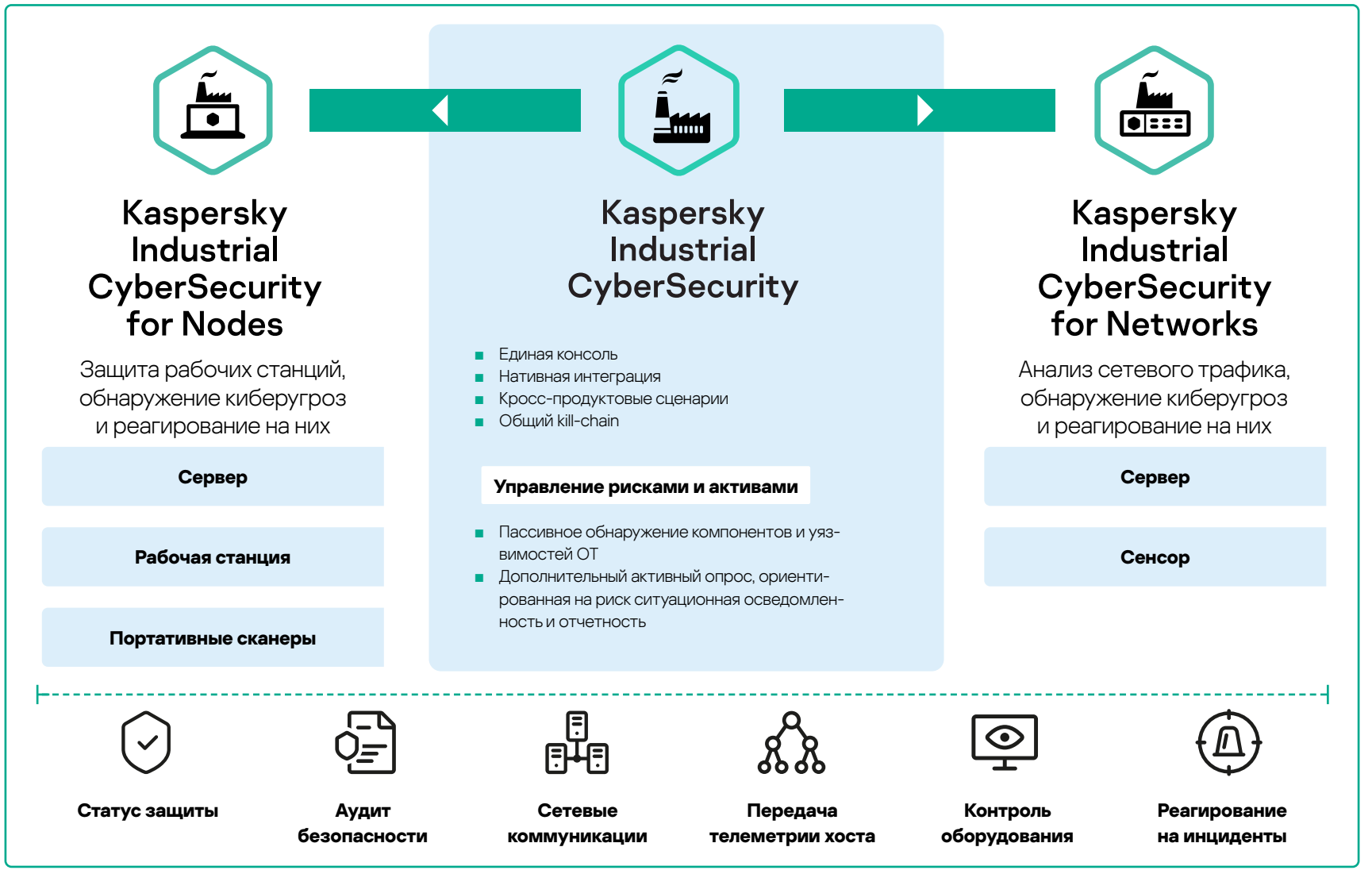
>1 000
промышленных клиентов используют решения KICS

430
промышленных сетей крупных клиентов защищено по всему миру

+20%
средний доход на одного клиента

[1] Автоматизированная система управления технологическим процессом.
[2] Диспетчерское управление и сбор данных (Supervisory Control and Data Acquisition).

Платформа XDR для промышленности



KICS защищает все ныне эксплуатируемые системы АСУ ТП:

- brown field (более 90%) — это системы, создававшиеся с 2005 по 2020 год. Как правило, распределенные системы управления (РСУ), состоящие из микропроцессорных контроллеров разных типов (ПЛК[1], ИЭУ[2], РЗА[3] и др.), компьютерных человеко-машинных интерфейсов (ЧМИ) на старых ОС Windows и промышленных Ethernet-based сетей;

- перспективные проекты, популярные направления (5–10%) — различные виды цифровизации, подключенные площадки, облачные технологии, IIoT, цифровые двойники, виртуализация промышленных систем, ИИ / машинное зрение, СППР[4], аддитивные технологии и т. п.

В процессе работы платформа KICS обеспечивает полную наблюдаемость и контроль над тем, что происходит в системах управления ключевым технологическим процессом промышленного предприятия. Она обнаруживает и блокирует сетевые угрозы, аномалии трафика и технологического процесса, предотвращает заражения компьютерного оборудования вредоносным ПО и обнаруживает нарушение политики безопасной эксплуатации установок персоналом. В дополнение к этому платформа помогает производить инвентаризацию промышленных активов, аудит безопасности, а также позволяет обнаруживать уязвимости и управлять рисками.

1 Программируемые логические контроллеры.
2 Интеллектуальные электронные устройства.
3 Релейная защита и автоматика.
4 Системы поддержки принятия решений.

Наш вклад в безопасное производство чистой энергии

Защищаем энергообъекты с помощью современных информационных и операционных технологий и сервисов

Усть-Каменогорская и Шульбинская ГЭС — крупные стратегические объекты, поставляющие чистую энергию из возобновляемых источников жителям и предприятиям Восточного Казахстана. Руководители электростанций искали наилучшее решение для обеспечения их безопасной и бесперебойной работы.

Сложность проекта по защите инфраструктуры ГЭС была в том, что при выборе подходящего решения нужно было учитывать следующие важные критерии:

- требования в архитектуре;
- требования по совместимости с другими решениями;
- требования к системам АСУ ТП.

В итоге наиболее подходящей для защиты производственных процессов станций оказалась платформа KICS. Это решение было внедрено в технологические системы ГЭС, расположенные в разных городах и связанные только VPN-каналом.

Что в результате?

Наше решение KICS обеспечивает безопасность промышленной инфраструктуры двух ГЭС на всех уровнях — от серверов АСУ ТП и автоматизированных рабочих мест до программируемых логических контроллеров и сетевого оборудования, — не нарушая взаимодействия информационных систем и промышленного оборудования. KICS позволяет выявлять разные типы угроз на ГЭС: человеческие ошибки, нарушение коммуникаций между устройствами, появление сотрудника, выполняющего работы без согласования, атаки и вредоносное ПО.

Формируем кибериммунитет

Задача

Обеспечение надежной и прогнозируемой работы промышленных систем, снижение рисков инцидентов и связанных с ними аварий

Число подключенных к интернету устройств с каждым днем увеличивается, а вместе с этим повышается и уровень киберпреступности. Киберугрозы могут стать причиной значительного физического ущерба, если речь идет, например, о промышленных предприятиях, объектах энергетики, автомобилях или системах «Умного города». Индустрия информационной безопасности создает все новые технологии и продукты, но часто оказывается, что они лишь догоняют злоумышленников. Необходимо найти способ опередить их и защититься от киберугроз.

Решения

Предотвращаем кибератаки с помощью собственной операционной системы KasperskyOS

Кибериммунитет — это подход, позволяющий создавать программно-аппаратные IT-системы со встроенной защитой от кибератак. Это один из определяющих факторов развития в области промышленной автоматизации, носимых промышленных устройств, интернета вещей, удаленного доступа к критически важным объектам. Например, уже сейчас нам доступны такие кибериммунные устройства, как шлюзы промышленного интернета вещей, тонкие клиенты, контроллеры для «Умного города», шлюзы для автомобилей.

В рамках кибериммунного подхода мы разработали собственную операционную систему KasperskyOS — платформу для создания продуктов и решений, защищенных на уровне архитектуры.

Кибериммунитет обеспечивается благодаря разделению системы на изолированные части и контролю взаимодействий между ними. При таком подходе большинство возможных атак на систему будут бесполезны — она продолжает выполнять критически важные функции даже в условиях агрессивной среды и не позволяет злоумышленнику развить атаку.

Важными особенностями KasperskyOS являются собственное микроядро и монитор безопасности — подсистема Kaspersky Security System. Это обеспечивает более высокий уровень безопасности и удовлетворяет требованиям кибериммунности «из коробки». Эти решения практически невозможно скомпрометировать, а число возможных уязвимостей в них сведено к минимуму.

Помогаем промышленным компаниям реализовывать ESG-стратегию

Задача

Мониторинг и анализ показателей устойчивого развития

Крупные промышленные компании ведут деятельность, руководствуясь принципами устойчивого развития, и разрабатывают собственные ESG-стратегии. Они устанавливают целевые показатели в области изменения климата и планируют постепенно снижать углеродный след до минимума. Чтобы отслеживать свой прогресс в этой сфере, компании в реальном времени и ретроспективно отслеживают и анализируют значения показателей выбросов парниковых газов и загрязняющих веществ. В подобной системе учета особенно заинтересованы предприятия, деятельность которых сопровождается существенными выбросами парниковых газов, в том числе транспортные и добывающие компании.

Еще одним из важных аспектов устойчивого развития являются производственная безопасность и охрана труда. Промышленные предприятия включают цели по сокращению травматизма в свои ESG-стратегии. Чтобы отслеживать свой прогресс в достижении целей, определять уязвимые места и принимать меры для предотвращения несчастных случаев на производстве, они собирают и анализируют данные об условиях труда и травматизме. Для этого используются IT-решения, позволяющие автоматически контролировать соблюдение техники безопасности, фиксировать нарушения и передавать эти данные в систему учета.

Решения

Создаем продукты, позволяющие отслеживать целевые ESG-показатели

Чтобы помочь нашим клиентам не только защитить автомобили от взлома, но и контролировать потребление топлива, строить оптимальные логистические маршруты и учитывать выбросы от автомобильного транспорта, мы создали решение Kaspersky Automotive Secure Gateway. Оно работает на базе операционной системы KasperskyOS и собирает все необходимые цифровые данные о работе транспортного средства, делает их видимыми, прозрачными и понятными, отправляет на серверы для анализа и оценки возможности улучшения показателей, предлагает новые пути для этого. Наше решение позволяет клиентам достигать своих целей в области устойчивого развития в реальности, а не только на бумаге. Кроме того, оно проводит безопасное обновление шлюза и помогает в обновлении других электронных блоков автомобиля, собирает события внутренней сети автомобиля и отправляет их в центр мониторинга безопасности, обеспечивая единое место управления и реагирования и минимизируя расходы на обслуживание.

Помогаем соблюдать требования в области защиты КИ

Задача

Обеспечение соблюдения законов разных стран пользователями наших решений

Промышленные предприятия и операторы КИ обязаны соблюдать местные законодательные и отраслевые требования по управлению рисками и отчетности об инцидентах. «Лаборатория Касперского» гарантирует соответствие своих продуктов стандартам и законодательным требованиям к промышленной кибербезопасности в разных странах мира.

Подробнее о законодательных и отраслевых требованиях, которые мы учитываем при разработке наших продуктов и решений, читайте в Приложении 4 на стр. 151

Решения

Учитываем требования и стандарты при разработке продуктов для промышленных предприятий

KICS — первая в мире XDR-платформа, сертифицированная по промышленному стандарту IEC 62443–4-1

Оба продукта, входящие в платформу KICS, — KICS for Nodes и KICS for Network — прошли сертификацию по основным международным стандартам в области кибербезопасности, а также учитывают или помогают выполнять требования других международных законов и отраслевых стандартов:

- ISO/IEC 27 001 IEC 27 002 (DIN 2008 в Германии) — стандарт, устанавливающий требования к созданию, внедрению, поддержанию и постоянному совершенствованию системы управления информационной безопасностью в контексте организации;
- ISO/IEC 27 019 (DIN 2011 в Германии) — стандарт, использующийся для обеспечения информационной безопасности в энергетике;
- ISO/IEC 27 032 — стандарт, который касается вопросов обеспечения безопасности в интернете и содержит рекомендации по устранению наиболее распространенных угроз в этой сфере (социальная инженерия, атаки нулевого дня, шпионское ПО и т. д.);
- ISO/IEC 15 408 — стандарт, который имеет исторически сложившееся название «Общие критерии» и представляет собой обобщенный опыт различных государств по разработке и практическому использованию критериев оценки безопасности информационных технологий;
- IEC 62 443 (ANSI/ISA99) — серия этих стандартов содержит требования к проектированию систем управления кибербезопасностью АСУ ТП и SCADA;
- IEC 62 351 — стандарт, который охватывает вопросы информационной безопасности энергетических систем;
- NIST CSF — рекомендации по обеспечению безопасности промышленных систем управления, разработанные Национальным институтом стандартов и технологий США (NIST);
- NERC CIP — свод стандартов кибербезопасности для критической инфраструктуры и защиты энергосистемы США, на которые также ориентируются некоторые страны Латинской Америки;
- NIS 2 Directive (EU) 2022/2555) — новая директива ЕС о кибербезопасности[1];
- IMO MSC.428(98) — резолюция Комитета по безопасности на море, которая регулирует управление киберрисками в морской отрасли в рамках систем управления безопасностью;
- ICAO — стратегия кибербезопасности в авиации[2];
- IAEA Nuclear Security Series No. 17-T (Rev. 1) — методы обеспечения компьютерной безопасности для ядерных установок.

С 8 февраля 2022 года область сертификации распространяется на сервисы обработки данных «Лаборатории Касперского» (KSN). Многие клиенты KICS активируют KSN при установке. Для них крайне важно, что Компания использует лучшие мировые практики в своих дата-центрах в Цюрихе, Франкфурте-на-Майне, Торонто, Москве и Пекине. Подробнее об этом читайте здесь.

Наша платформа KICS полностью сертифицирована европейской сертификационной TUV Austria на соответствие международному стандарту в части жизненного цикла разработки ПО для обеспечения кибербезопасности промышленных предприятий. Уровень доверия — 3 из 4.

«Лаборатория Касперского» проходит аудиты Service Organization Controls (SOC 2). В рамках сертификации Type 2 проверялась эффективность средств контроля, используемых с целью обезопасить процесс разработки и выпуска антивирусных баз от несанкционированного вмешательства. Работоспособность механизмов контроля, принятых в Компании, оценивалась не на определенную дату, как при аудите первого типа, а за шесть месяцев.

Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks имеют также сертификаты государственных органов Российской Федерации (ФСТЭК и ФСБ). В декабре 2023 года успешно прошли сертификационные испытания версии 3.2.0.273 (для Windows) и 1.3.0.1 206 (для Linux). Помимо этого, решения «Лаборатории Касперского» включены в Единый реестр российских программ для электронных вычислительных машин и баз данных, который был создан в начале 2023 года Минцифры России.

В октябре 2023 года «Лаборатория Касперского» запустила регуляторный хаб знаний в области информационной безопасности, который включает все нормативные правовые акты в области ИБ, действующие в России. Центр знаний призван помочь пользователям ориентироваться в законодательстве в сфере ИБ, понимать текущие требования и рекомендации для конкретной отрасли.

[1] Государства — члены Евросоюза должны принять и опубликовать меры по кибербезопасности, необходимые для соблюдения новой директивы, до 17 октября 2024 года.

[2] FAA Advisory Circular 119-1 — Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP).

Наш вклад в создание стандартизированного подхода к кибербезопасности

Разрабатываем российские ИБ-стандарты в области кибербезопасности

При разработке операционной системы KasperskyOS мы обнаружили, что в российских документах и учебниках по информационной безопасности не хватает терминов, определений и понятий, с помощью которых можно описать проектные архитектурные решения. Чтобы решить эту проблему, мы начали разработку двух национальных стандартов. Они определяют базовые понятия и основные архитектурные принципы, заложенные в системы с разделением доменов, в том числе в KasperskyOS.

Что в результате?

В апреле 2023 года оба стандарта были приняты Техническим комитетом «Киберфизические системы» (ТК 194) и вступили в действие.

- Информационные технологии. Интернет вещей. Системы с разделением доменов. Термины и определения
- Информационные технологии. Интернет вещей. Системы с разделением доменов. Базовые компоненты

Наши результаты

KICS

Продажи платформы KICS существенно увеличились на всех основных рынках решений для промышленной кибербезопасности. Российский рынок, оставаясь ключевым для Компании, генерирует около 80% бизнеса и показывает рост более 50%. Это объясняется стремительным импортозамещением решений иностранных вендоров, а также возросшим спросом на защиту из-за роста количества атак на российскую инфраструктуру.

В 2023 году направление промышленной кибербезопасности показало следующие результаты.

- Платформа KICS уверенно вошла в пятерку лучших по выручке среди всех B2B-продуктов Компании.
- Направление Industrial Cybersecurity в очередной раз показало трехзначный рост выручки в процентном соотношении относительно прошлого года.
- Перевыполнение плана продаж составило 128%.
- Показатели Gross EBITDA margin; Operating EBITDA margin и EBITDA margin лежат в диапазоне от 20 до 40%.

Основные драйверы развития платформы Kaspersky Industrial CyberSecurity

- Возрастающие угрозы и возникающие инциденты информационной безопасности, с которыми промышленные компании, к сожалению, все чаще сталкиваются на практике.
- Потребность в решении, способном защищать гетерогенную инфраструктуру, состоящую одновременно из технологических процессов, управляемых как устаревшими системами автоматизации, так и современными решениями на основе сетей с продвинутой архитектурой, актуальных операционных систем и версий промышленного ПО.
- Активное внедрение подключенных интеллектуальных устройств и устройств промышленного интернета вещей в рамках процесса цифровизации, а также широкого использования IT-, программного, аппаратного и сетевого технологического стека на промышленных объектах.

В ближайшие 4 года мы ожидаем двукратный рост в этом бизнес-сегменте. Для этого мы продолжим инвестировать в развитие технологических возможностей KICS и ее продвижение в ключевых регионах.

KasperskyOS

В отчетном периоде мы начали развивать региональный бизнес по защите виртуальных рабочих мест. Это направление стало особенно актуальным в постпандемийный период, когда многие компании перешли на гибридную модель работы сотрудников.

В частности, в августе 2023 года мы подписали соглашение с корпорацией Centerm, согласно которому специализированные рабочие места (тонкий клиент на KasperskyOS) могут поставляться по заказам из любых стран. Мы уже получили первые заказы из Швейцарии и Малайзии.

В 2023 году наши специалисты детально изучили вопрос расширения аппаратных платформ уникальными решениями, построенными на принципах кибериммунитета, и начали экспертную работу для получения необходимых заключений и разрешений регуляторов.

Наши планы на 2024 год

Промышленная кибербезопасность

Предложение глубокой и всесторонней защиты

во всех сегментах инфраструктуры наших клиентов с помощью технологий, знаний и экспертизы, входящих в нашу OT-экосистему. Развитие кросс-продуктовых сценариев использования наших нативно интегрированных технологий в ответ на новые запросы заказчиков, а также включение в нашу открытую экосистему решений наших партнеров.

- Инвестиции в Linux-функционал и в развитие технологических возможностей платформы KICS.
- Расширение поддерживаемых аппаратных платформ, протоколов промышленной передачи данных и развитие экспертной базы данных промышленных устройств.
- Отработка сценариев использования носимых устройств, безопасного обмена данными, а также создание инструментария аудита информационной безопасности и плановой проверки даже изолированных систем и сетей.

Расширение

на новые вертикальные рынки, участникам которых необходимо четко отслеживать ESG-показатели.

- Сотрудничество с клиентами из таких отраслей, как транспорт, логистика, полупроводники, автомобильная промышленность и производство комплектующих.
- Партнерство с лидерами в OT-интеграции, а также создание технологических альянсов с региональными чемпионами среди вендоров систем промышленной автоматизации[1].

Геоэкспансия

в регионы с меньшим присутствием Компании. Для этого мы адаптируем экосистему под особенности каждого региона.

- Сохранение инвестиций в исторические рынки — Россия, СНГ, Европа.
- Расширение сотрудничества с региональными партнерами в области защиты КИ: Бразилия, Китай, Индия, Индонезия, Саудовская Аравия, ОАЭ, Алжир, ЮАР.

KasperskyOS

Развитие

бизнес-сообщества партнеров, участники которого используют киберриммунные продукты в вертикальных отраслевых решениях.

Запуск

пилотных проектов с ключевыми заказчиками в различных отраслях для разработки сценария с эффективным применением кибериммунных решений.

Проработка

требований регуляторов для создания описания нового класса устройств со встроенной (кибериммунной) защитой.

[1] Региональные лидеры, производители промышленного оборудования и систем автоматизации.