

Как мы защищаем критическую инфраструктуру

Наша цель — обеспечить бесперебойное функционирование киберфизических систем на объектах критической инфраструктуры и в промышленности с помощью современных технологий, знаний и опыта.

Защищены решениями «Лаборатории Касперского»

>130

завершенных проектов
в нефтегазовом секторе

>40

компаний энергетической
и коммунальной отраслей

12%

мировой добычи
нефти

>80

завершенных проектов
в электроэнергетике
(атомная, тепловая, ВИЭ)

Топ-5

глобальных
производителей ВИЭ

>60

нефтегазовых
компаний

Критическая инфраструктура (КИ) — это технологические системы, от которых напрямую зависит устойчивое функционирование экономики, государства и общества.

Примеры КИ



Энергетика



Водоснабжение



Транспорт



Добыча
полезных
ископаемых



Металлургия



Машиностроение



Пищевая
промышлен-
ность



Химическая
промышленность



Фармацевтическая
промышленность



ЖКХ



Логистика



Производство
электроники и др.

Почему это важно

Современные системы промышленной автоматизации становятся все более цифровыми, связанными и умными — они используют облака, ИИ, интернет вещей и цифровые двойники. Это повышает эффективность производства, но и увеличивает риски: возрастает поверхность атаки, а сами объекты КИ превращаются в привлекательную цель для злоумышленников. При этом многие критически важные системы изначально создавались для работы в изолированной среде, а сейчас вынуждены функционировать в условиях высокой открытости и связанности.

Сегодня мир сталкивается с растущим числом кибератак на критически важные объекты, и эти атаки становятся все более изощренными.

Ключевые инциденты 2024–2025 годов

- Служба военной разведки Дании 18 декабря 2025 года опубликовала заявление, в котором утверждалось, что группа Z-Pentest провела разрушительную атаку на Датский водоканал в 2024 году. Атакующие изменили давление в насосной станции недалеко от города Кёге, что привело к прорыву трех труб.

- Атака вымогателей на Jaguar Land Rover вызвала пятидневный простой производства, ставший прямой причиной убытков, оцениваемых в десятки миллионов долларов. Инцидент стал фатальным для нескольких поставщиков автопроизводителя — им пришлось прибегнуть к процедуре банкротства. Атака сказалась на работе около 5 000 британских организаций, нанеся суммарный ущерб британской экономике в \$2,5 млрд.
- Атака вымогателей на платформу онлайн-регистрации ARINC cMUSE американского разработчика Collins Aerospace привела к сбоям в работе нескольких крупнейших европейских аэропортов, в очередной раз демонстрируя, насколько авиатранспортный сектор уязвим к атакам на цепочку поставок.
- Крупнейшая российская авиакомпания «Аэрофлот» также стала жертвой злоумышленников. Атака хактивистов на системы авиакомпании вынудила отменить множество рейсов.
- Неизвестные злоумышленники в апреле 2025 года атаковали плотину на озере Рисеватнет в коммуне Бремангер на западе Норвегии и дистанционно открыли затвор. Он был полностью открыт в течение четырех часов, прежде чем несанкционированное вмешательство обнаружили и локализовали.

Все чаще уязвимыми оказываются энергетика, водоснабжение и транспорт — отрасли, от которых напрямую зависят повседневная жизнь людей и устойчивое развитие страны.

В то же время основной мишенью злоумышленников остается именно производственный сектор. Согласно нашим ежеквартальным [обзорам](#) основных инцидентов промышленной кибербезопасности, подавляющее большинство атакованных в 2024–2025 годах организаций относятся к производству.

Наш подход к защите критической инфраструктуры

Мы рассматриваем кибербезопасность как непрерывный цикл: подготовка — мониторинг и своевременное обнаружение — реагирование — быстрое восстановление работы.

Сегодня киберустойчивость выходит за рамки классической кибербезопасности. Это означает, что уже недостаточно просто блокировать атаки — нужно обеспечивать устойчивость всей ОТ-инфраструктуры¹ даже в условиях инцидентов.

Поэтому мы строим платформу безопасности киберфизических систем, где решения «Лаборатории Касперского» защищают ИТ-, ОТ- и IIoT-среды², помогают организациям внедрять цифровые технологии, не ставя под угрозу стабильность бизнеса, безопасность людей и окружающей среды.

¹ ОТ-инфраструктура (Operational Technology) — совокупность систем, оборудования и ПО, которые напрямую управляют физическими процессами в промышленности и на объектах критической инфраструктуры.

² Industrial Internet of Things или промышленный интернет вещей — многоуровневая система, включающая в себя датчики и контроллеры, установленные на узлах и агрегатах промышленного объекта, средства передачи собираемых данных и их визуализации, мощные аналитические инструменты интерпретации получаемой информации и многие другие компоненты.

Помогаем минимизировать риски и оценивать выгоды от инвестиций в защиту КИ

Как наши решения помогают бизнесу экономить и принимать взвешенные решения

Нарушения в работе промышленных предприятий из-за кибератак могут обернуться серьезными убытками — от простоя оборудования до потери продукции и репутационного ущерба. Чтобы помочь компаниям точнее оценивать риски и эффективность инвестиций в кибербезопасность, мы провели международное [исследование](#) совместно с аналитическим агентством VDC Research.

Что в результате

Совместное исследование показало, что внедрение комплексного решения (защита промышленных узлов и мониторинг сетевого трафика) может снизить потенциальный ущерб от киберинцидентов:

- до 45% — для предприятий энергетики и ЖКХ;
- до 76% — для производственного сектора.

Обеспечиваем защиту на всех уровнях

Платформа промышленной безопасности KOTCS

Kaspersky OT CyberSecurity — это специализированная XDR-платформа, которая защищает все уровни систем и сетей промышленных предприятий и объектов критической инфраструктуры.



Уровень 2

Мониторинг и управление

- IIoT¹, защита периметра и верхнего уровня автоматизации (SCADA)
- Контроль доступа, аудит и повышение видимости OT-систем
- Экспертная поддержка на стороне заказчика

Уровень 3

Корпоративные системы

- Конвергенция IT и OT, корреляция данных из всех доступных источников
- Унифицированные процессы и подходы к обеспечению безопасности с помощью технологии расширенного обнаружения и реагирования на угрозы гибридного типа (Hybrid XDR)
- Обучающие программы, консалтинг и расширенная аналитика угроз

Уровень 1

Контроллеры и защита

- Обнаружение вторжений, попыток взлома и компрометации микропроцессорного оборудования нижнего уровня автоматизации
- Глубокая инспекция промышленных протоколов (DPI), защита встроенных ОС от сетевых угроз и попыток изменения параметров технологического процесса
- Обнаружение аномалий в техпроцессах с помощью машинного обучения

Уровень 0

Технологический процесс

- Мониторинг киберфизических угроз для основного оборудования
- Обеспечение безопасности подключенных транспортных средств и других физических объектов

¹ Industrial Internet of Things или Промышленный интернет вещей — многоуровневая система, включающая в себя датчики и контроллеры, установленные на узлах и агрегатах промышленного объекта, средства передачи собираемых данных и их визуализации, мощные аналитические инструменты интерпретации получаемой информации и многие другие компоненты.

Ключевые отрасли применения

- Нефтегазовая и химическая отрасли
- Электроэнергетика, включая атомную, и ЖКХ
- Металлургия и добыча полезных ископаемых
- Промышленное производство, в том числе микроэлектроника

Перспективные направления применения Kaspersky OT CyberSecurity

- Фармацевтика и медтехника
- Транспорт и логистика, включая аэропорт
- Телекоммуникации
- Крупные объекты инфраструктуры (стадионы, бизнес-центры, торговые центры, жилые комплексы)

Специализированные решения



Kaspersky SD-WAN



Kaspersky Machine Learning for Anomaly Detection



Kaspersky Antidrone



Kaspersky Industrial CyberSecurity

Нативный XDR



KICS for Nodes

Защита конечных точек, обнаружение и реагирование



KICS for Networks

Анализ сетевого трафика, обнаружение и реагирование

Решения на базе KasperskyOS



Kaspersky Thin Client



Kaspersky Automotive Secure Gateway

Знания

Кибергигиена



Kaspersky Security Awareness

Аналитика угроз



Kaspersky ICS Threat Intelligence

Обучение



Kaspersky ICS CERT Training

Экспертиза

Диагностика



Kaspersky ICS Security Assessment

Реагирование



Kaspersky Incident Response

Управляемый сервис



Kaspersky Managed Detection and Response

KICS — основа платформы Kaspersky OT CyberSecurity

Сегодня
под защитой
KICS

10%
нефтехимического производства

15%
коммерческой атомной генерации

Ядром платформы киберфизической безопасности является Kaspersky Industrial CyberSecurity (KICS). Решение обеспечивает ситуационную осведомленность, киберустойчивость, видимость событий в промышленных сетях и мощную защиту основных автоматизированных систем, не влияя на доступность технологических процессов.

12%
общемировой добычи нефти и газа

до 15–25%
добычи и переработки различных металлов

20%
производства азотных и фосфорных удобрений

KICS помогает предотвратить дорогостоящие простои, инциденты безопасности, кражу данных и саботаж, вызванные массовыми угрозами, целевыми атаками, программами-вымогателями или действиями инсайдеров. Она также позволяет защитить устаревшее оборудование и продлить срок его эксплуатации, помогает соблюдать национальные и международные

стандарты и лучшие практики информационной безопасности промышленных инфраструктур.

Состав платформы:

- KICS for Nodes — защита серверов, рабочих станций, панелей оператора на базе Linux и Windows;
- KICS for Networks — анализ сетевого трафика, инвентаризация активов, выявление аномалий и вторжений, реагирование на сетевые угрозы.

География распространения KICS

За отчетный период мы существенно укрепили отношения с компаниями, которые специализируются на системах хранения энергии, производстве электротранспорта и солнечных панелей. Среди наших клиентов пять производственных компаний, каждая из которых, по независимым оценкам, входит в топ-5 мировых лидеров в этих отраслях.

Такое взаимодействие придало бизнесу дополнительный импульс, результатом которого стала организация в 2025 году конференции [KICS Con China 2025](#) в Шэньчжэне — одном из инновационных регионов, известном своим технологическим кластером. Эта конференция собрала более 100 участников. Также были проведены отраслевые круглые столы для нефтегазового сектора в регионе МЕТА¹.

Мы последовательно развиваем программу технологического партнерства. Платформа KICS прошла испытания на совместимость с решениями производителей промышленной автоматизации из Латинской Америки, Восточной Азии и Китая, включая Altus, Chint, Consen, Supcon и HollySys, помогая заказчикам выстраивать устойчивые цепочки поставок и ответственно подходить к выбору технологий.

В настоящее время KICS — лидер по числу публичных историй успеха как в портфолио «Лаборатории Касперского», так и среди конкурентов.

Наши новые клиенты, защищенные KICS:

- Nuevo Hospital de Toledo (Испания) — самый большой госпиталь в регионе Иберия;
- Birla Sugar Group — крупнейший в Индии производитель сахара;
- Holy Stone — один из лидеров цементной отрасли в Китае;
- Atlas Tapes (Греция) — крупнейший в Евросоюзе производитель изолянт;
- OLED — крупнейший в Китае производитель OLED-дисплеев.

Платформа KICS совместима
со множеством АСУ ТП от

70+ вендоров

>50
успешных историй внедрения KICS

¹ Ближний Восток, Турция, Африка.

Платформа XDR для промышленности



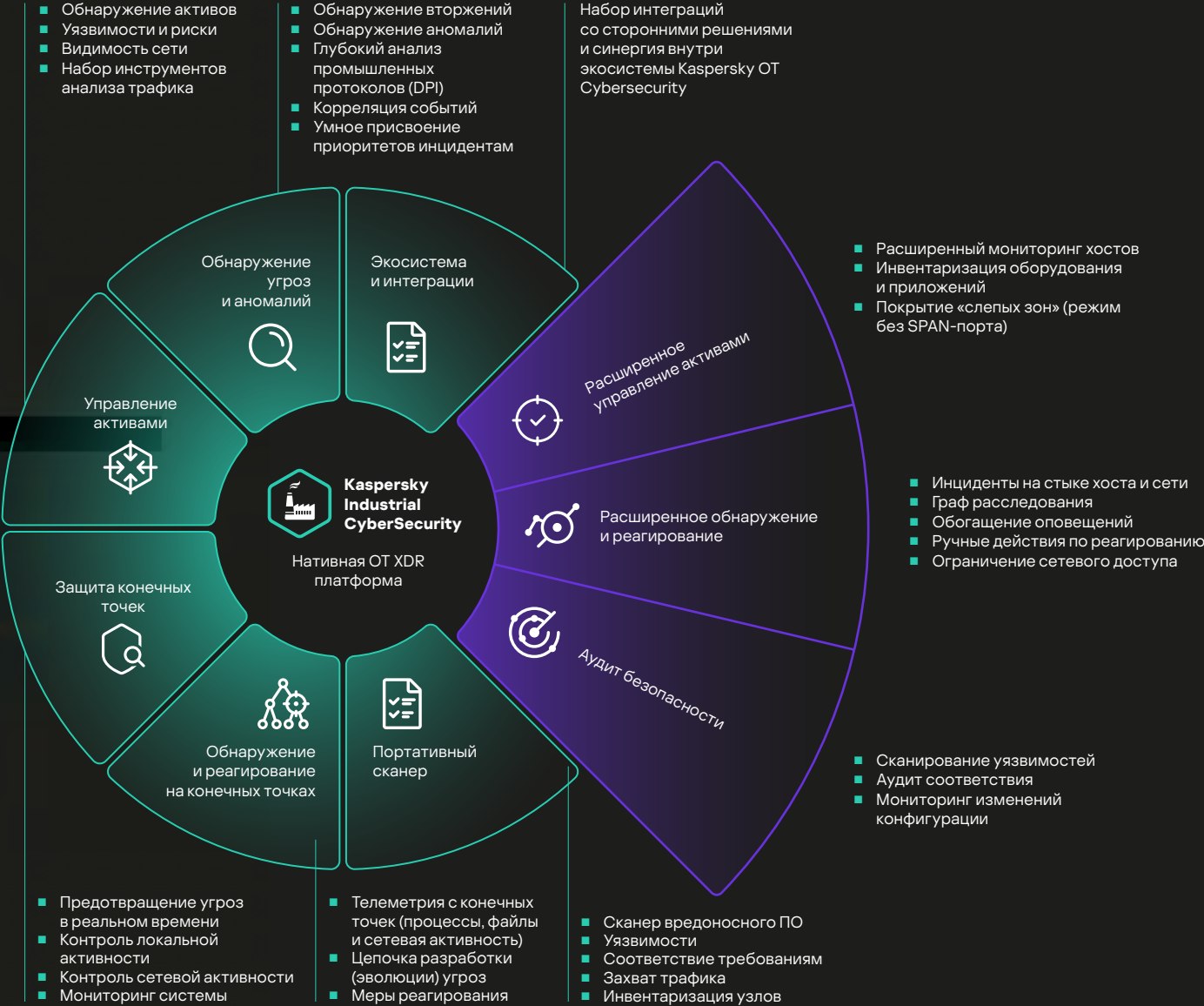
Kaspersky Industrial CyberSecurity for Networks

Анализ сетевого трафика, обнаружение и реагирование



Kaspersky Industrial CyberSecurity for Nodes

Защита конечных точек, обнаружение и реагирование



Формируем кибериммунитет

Почему это важно

Кибериммунитет — свойство системы, при котором стоимость атаки на нее превышает потенциальный ущерб или выгоду злоумышленников. Мы считаем, что подобные системы можно создавать с помощью KasperskyOS. Для этого в KasperskyOS комбинируются лучшие практики разработки информационных систем с опорой на безопасную архитектуру, принципы и паттерны проектирования безопасных систем, контроль качества, методологию разработки безопасного ПО, отраслевые стандарты и обязательное тестирование на проникновение. Так мы приближаем прекрасное будущее, в котором системы решают задачи безопасности «из коробки».

Мы предлагаем строить системы так, чтобы они были безопасны по умолчанию благодаря разделению на изолированные части и контролю взаимодействий между ними.

В результате, даже если злоумышленнику удастся преодолеть одну линию защиты, остальные части системы продолжают работать безопасно. Это особенно важно для промышленной автоматизации, носимых устройств, интернета вещей и удаленного доступа к критической инфраструктуре.

Новые стратегические альянсы

- [Соглашение с ОАО «РЖД»](#) о тестировании и внедрении решений на базе KasperskyOS и технологий защиты контейнерных сред
- [Соглашение с Институтом системного программирования РАН](#) о создании Центра конструктивной информационной безопасности

KasperskyOS

Платформой для построения кибериммунных решений является микроядерная KasperskyOS. Это собственная разработка «Лаборатории Касперского», которая не основывается на каком-либо существующем открытом проекте.

Комбинация микроядерной архитектуры и концепций MILS (Multiple Independent Levels of Security) и FLASK (Flux Advanced Security Kernel) в KasperskyOS формирует принципиально новый уровень киберзащиты, позволяющий значительно повысить устойчивость системы к кибератакам.

В 2024–2025 годах мы сделали значительный шаг в развитии KasperskyOS: скорректировали стратегический фокус и начали расширять границы ее применения в качестве полноценной операционной системы общего назначения.



Флагманский релиз: Kaspersky Thin Client 2.3

[Ключевым продуктом](#) отчетного периода стала новая коммерческая версия [Kaspersky Thin Client 2.3](#), которая объединила разработки 2024 и новые функции 2025 года:

- расширенную поддержку периферии (веб-камер, гарнитур, сканеров);
- централизованное управление настройками мониторов через Kaspersky Security Center;
- техподдержку удаленного администратора;
- режим Secure Boot.

Это первый релиз, сертифицированный на платформе Dell Wyse 3040, что стало важным шагом к расширению аппаратной совместимости.

Примеры успешного внедрения Kaspersky Thin Client

- [Российская компания «КрасЭко»](#) построила на базе этого решения безопасную инфраструктуру рабочих мест с единой консолью управления и поддержкой отечественных операционных систем.
- [Международный партнер Aswant Distribution](#) стал эксклюзивным дистрибьютором Kaspersky Thin Client в Малайзии и Индонезии. За 2024–2025 годы он поставил кибериммунные тонкие клиенты госорганам, промышленным предприятиям, финансовым и образовательным учреждениям региона.
- В муниципальном совете Кулима внедрение системы снизило операционные затраты на 20% и повысило киберустойчивость инфраструктуры.



Создаем продукты, позволяющие отслеживать ESG-показатели



Kaspersky Automotive Secure Gateway

Kaspersky Automotive Secure Gateway — это [решение](#) для защиты подключенных транспортных средств, включающее шлюз безопасности, бортовую систему обнаружения и предотвращения вторжений (In-Vehicle IDPS), сервисы телеметрии, дистанционного управления и навигационную систему.

Забота об экологии

Наше решение может осуществлять постоянный мониторинг систем автомобиля (батарея, электроника, параметры движения и прочее), что позволяет, например, оптимизировать зарядные операции и продлить срок службы аккумуляторов, а также сократить пробег сервисных машин и, соответственно — выбросы CO₂, используя данные предиктивной диагностики.

Безопасность людей

Наше решение — первое в России, процессы разработки которого и отдельные программные компоненты сертифицированы по ISO 26262 (ASIL B). Этот стандарт функциональной безопасности для автопрома минимизирует риски ущерба жизни и здоровью людей в результате сбоев автомобильных систем.

Учет требований информационной (security) и функциональной (safety) безопасности открывает путь к удаленным бизнес-сценариям (дистанционное обслуживание, автономные перевозки, гибкие рабочие модели доступа к транспортным средствам) без компромиссов в области безопасности людей и киберрисков.

Качество управления

Kaspersky Automotive Secure Gateway помогает автопроизводителям соблюдать требования международных стандартов кибербезопасности для транспортных средств, в том числе обеспечивая мониторинг событий ИБ и их передачу в Vehicle Security Operations Center (VSOC) для своевременного реагирования и расследования инцидентов.

Такие свойства Kaspersky Automotive Secure Gateway способствуют реализации ESG-принципов в транспортной отрасли.



Соблюдаем требования и стандарты при разработке решений

«Лаборатория Касперского» гарантирует соответствие своих продуктов стандартам и законодательным требованиям к промышленной кибербезопасности в разных странах.

Подробнее о законодательных и отраслевых требованиях, которые мы учитываем при разработке наших продуктов и решений, читайте в [приложении 5](#) на с. 136

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 исполнить требования других международных законов и отраслевых стандартов.

Наши результаты

Kaspersky OT CyberSecurity
в 2024–2025 годах

Платформа промышленной безопасности Kaspersky OT CyberSecurity и входящее в нее решение Kaspersky Industrial CyberSecurity в отчетном периоде показали уверенный рост продаж. Повышение интереса к этим решениям было обусловлено:

- рыночными факторами, включая рост числа атак на промышленные предприятия, усиление региональных регуляторных норм, импортозамещение, фокус на киберсуверенитет и диверсификацию поставщиков средств защиты, рост зрелости заказчиков;
- долгосрочной стратегией «Лаборатории Касперского» по закреплению позиций на домашних рынках и геоэкспансии;
- стратегическим подходом к кросс-продуктовым экосистемным продажам для заказчиков государственного сектора и объектов критической инфраструктуры.

2-е место

в портфеле Kaspersky
по суммарным продажам
всех продуктов экосистемы

KICS в 2025 году

Платформа KICS показала стабильный 30%-ный годовой рост бизнеса, продемонстрировав хорошую динамику на всех ключевых рынках, включая регионы, затронутые геополитическими проблемами.

- Российский рынок остается ключевым для KICS, генерируя 75% бизнеса и сохраняя снизившиеся по сравнению с предыдущими периодами, но все еще высокие темпы роста в 25%. Это обусловлено ужесточением законодательства в разрезе защиты КИИ, продолжающимися тенденциями импортозамещения и большим числом атак на инфраструктуру.
- Международные продажи растут более чем на 50% год к году благодаря реализуемой Компанией стратегии геоэкспансии.

+20%

CAGR (среднегодовой
совокупный темп
роста) год к году

KasperskyOS

В 2024–2025 годах экосистема KasperskyOS продемонстрировала устойчивый рост и выход на новые рынки. Портфель решений на ее базе расширился, охватив корпоративный, транспортный и встраиваемый сегменты. В этот период платформа показала двухзначный по миру и трехзначный в России рост инсталляционной базы (в процентном выражении).

16%

выручки Компании
генерируют промышленные
заказчики (второе место
после госсектора)

+20%

рост продаж в России

Топ-5

доменов среди B2B-
продуктов Компании

>540

защищенных сетей крупных
структурообразующих
для экономики заказчиков

+20%

рост ARPC (среднего
дохода на одного клиента)
за счет cross-sell и up-sell
решений (кросс-продаж
и увеличения объема продаж
существующим клиентам)

>330 000

проданных лицензий

Наши планы на 2026–2027 годы

Промышленная кибербезопасность

Промышленные компании по всему миру переходят от закрытых (проприетарных) решений к открытым архитектурам и программно-определяемой автоматизации. Например, в России уже создана [Межотраслевая рабочая группа](#) по вопросу разработки открытой автоматизированной системы управления технологическими процессами (АСУ ТП).

В связи с этим наши планы в сфере промышленной кибербезопасности на 2026–2027 годы включают:

1. Интеграцию и развитие KICS. В рамках развития Kaspersky OT CyberSecurity мы планируем продолжать интеграцию KICS с решением для защиты облачных и контейнерных сред Kaspersky Cloud Workload Security, параллельно расширяя ее функциональность и интеграцию с другими продуктами. В KICS уже применяются технологии ИИ для мониторинга (профилирование устройств, анализ процессов) и разрабатываются средства защиты от будущих кибератак с использованием ИИ.

2. Развитие кибериммунных устройств и новых технологий. Еще одно направление развития KOTCS — разработка на базе KasperskyOS кибериммунных устройств — тонких клиентов и защищенных мобильных устройств. Также в планах — развитие от шлюзов подключенных автомобилей к устройствам контроля данных V2X¹ для высокоавтоматизированных транспортных средств. Они не требуют экстренных обновлений безопасности и служат дольше.

3. Подготовку специалистов. Совместно с Kaspersky Academy мы планируем развивать сотрудничество с ведущими техническими вузами, в которых есть кафедры или учебные лаборатории АСУ ТП или информационной безопасности. Предлагая студентам возможность получить актуальный практический опыт, мы уже сейчас формируем кадровый резерв инженеров, которые будут защищать критически важные предприятия в течение будущих десятилетий.

Развитие KasperskyOS

KasperskyOS в ближайшие годы сфокусируется на выходе за рамки ниши встроенных решений и превращении в полноценную технологическую основу для безопасных цифровых экосистем нового поколения.

Основные направления развития экосистемы

1. Расширение областей применения.

KasperskyOS станет универсальной защищенной платформой для цифровых экосистем компаний, государственных структур и промышленных организаций.

2. Технологическое развитие ядра и SDK.

Улучшение микроядерной архитектуры, оптимизация производительности и расширение инструментов для разработчиков (KasperskyOS SDK) — это позволит партнерам и разработчикам быстрее создавать новые решения на базе ОС.

3. Рост экосистемы. Формирование сообщества интеграторов и разработчиков, использующих KasperskyOS, расширение образовательных программ и акселераторов по кибериммунной безопасности.

4. Международное продвижение.

Масштабирование внедрения KasperskyOS в странах Азии, Ближнего Востока, Латинской Америки и Турции, создание региональных центров компетенций и развитие локализованных версий продуктов.

5. Регуляторное и отраслевое признание.

Продолжение совместной работы с регуляторами и промышленными ассоциациями над формированием стандартов нового класса — устройств и систем со встроенной кибериммунной защитой, подтвержденной архитектурно.

6. Вклад в ESG-повестку. Использование KasperskyOS как основы для построения безопасных и энергоэффективных решений в транспорте, промышленности, энергетике и IT, чтобы помочь снизить углеродный след и повысить эффективность использования оборудования.

¹ Vehicle-to-Everything — обмен информацией в реальном времени между подключенным транспортным средством и любым другим объектом (другие транспортные средства, объекты дорожной инфраструктуры: светофоры, пешеходы, сети и др.) посредством технологий беспроводной связи.

