

kaspersky

АКТИВИРУЙ
БУДУЩЕЕ

Kaspersky OT CyberSecurity

Экосистема промышленной
кибербезопасности



Единая концепция промышленной кибербезопасности во главе с центральным компонентом – индустриальной XDR-платформой.



Kaspersky
OT CyberSecurity

Ответ на актуальные вызовы в области промышленной кибербезопасности

Устойчивое развитие промышленных предприятий и объектов критической инфраструктуры напрямую зависит от стабильности производственных и бизнес-процессов, надежной защиты важных активов и безопасности операционной (OT) и IT-инфраструктуры. Постоянный рост количества и сложности киберугроз в эпоху четвертой промышленной революции, глобализация информационной среды и необходимость соответствия требованиям регулирующих органов – все это побуждает организации задуматься о комплексном подходе к обеспечению кибербезопасности.

Тренды промышленной кибербезопасности:

Увеличение количества точек входа злоумышленников в инфраструктуру, которая находится на пересечении OT- и IT-сред

Усиление регуляторных требований в отношении защиты КИИ и массовое импортозамещение

Рост количества атакованных компьютеров АСУ

Основные источники угроз для компьютеров в технологической инфраструктуре – интернет, съемные носители и электронная почта

Наши ключевые отличия

С «Лабораторией Касперского» у организаций есть все необходимое для отражения кибератак любого масштаба и сложности.

1

Надежность

и безупречная
репутация в ИБ-сфере

2

Технологии

с охватом защиты
IT- и OT-сред

3

Знания

о киберугрозах и передача
практических навыков

4

Экспертиза

международного уровня

Почему выбирают нас

Почему промышленные предприятия могут положиться на «Лабораторию Касперского» в вопросе киберзащиты?



Глобальный охват
и международное
сотрудничество



Доказанная эффективность
технологий



Опыт и знания мирового
уровня



Высокий статус в индустрии
безопасности IT/OT-систем

1

Надежность



«Лаборатория Касперского» – наш доверенный партнер в киберпространстве, и мы рады возможности развивать наше сотрудничество в сфере защиты промышленных объектов.

Алексей Беспалов,
Начальник управления информационных технологий и заместитель главного инженера ПАО «Татнефть»

Комплексный подход от глобального поставщика в области IT/OT-безопасности

Сегодня производственным организациям необходима поддержка надежного партнера, обладающего многолетним опытом, глобальной экспертизой и пониманием современных кибервызовов на пересечении корпоративного и промышленного пространства. «Лаборатория Касперского» обеспечит инструментарием и аналитикой, необходимыми для отражения угроз, поможет в экстренной ситуации и поделится опытом и знаниями.





Глобальный охват и международное сотрудничество



Мы считаем «Лабораторию Касперского» одним из мировых лидеров в области информационной безопасности. Сотрудничество с этой компанией позволяет нам наиболее эффективно защищать наши системы от киберугроз. На данный момент мы протестировали на совместимость и безопасную работу с нашим ПО KICS for Nodes и KICS for Networks. В рамках использования решений «Лаборатории Касперского» мы можем обеспечить бесперебойную работу внутренних процессов промышленных предприятий – продукты компании не оказывают негативного влияния на технологические процессы наших заказчиков.

Михаил Карпенко,
Менеджер по продажам сервисных услуг
ООО «Йокогава Электрик СНГ» (Yokogawa)

Подписано более 10 OEM-соглашений с производителями АСУ ТП, такими как Yokogawa Electric Corporation, Siemens, Schneider Electric, Emerson, Honeywell и другими



Бренд, известный во всем мире.
Одна из крупнейших частных компаний в сфере кибербезопасности

34 офиса по всему миру



лет
опыта

Более 10 лет «Лаборатория Касперского» разрабатывает и предлагает решения для защиты промышленных предприятий



лидеров
ИБ-индустрии

Более 120 лидеров ИБ-индустрии доверяют «Лаборатории Касперского» защиту своих клиентов через технологическое и OEM-партнерство



Решения компании защищают критические IT-инфраструктуры крупнейших российских банков, промышленных предприятий, федеральных органов власти и госкорпораций



Сегодня технологии «Лаборатории Касперского» по всему миру защищают:

400+ миллионов пользователей

240+ тысяч корпоративных клиентов



«Лаборатория Касперского» вкладывает значительные инвестиции в исследования и разработку (R&D) — до 30% своей прибыли



«Лаборатория Касперского» является доверенным партнером государственных организаций по всему миру, в том числе Интерпола, Европола и различных подразделений CERT



«Лаборатория Касперского» обладает проектным опытом внедрения в разных отраслях: добыча полезных ископаемых, электроэнергетика, промышленность, транспорт и др.



Kaspersky Industrial CyberSecurity имеет оптимизированный набор компонентов защиты по сравнению с другими решениями, а также обеспечивает сниженную нагрузку на вычислительные ресурсы, благодаря чему наши технологические процессы остаются непрерывными.

Марат Халфин,
Начальник отдела управления
корпоративными сервисами ЦИКТ
ПАО «КАМАЗ»

Передовые технологии защиты АСУ ТП

Для обеспечения кибербезопасности промышленных предприятий «Лаборатория Касперского» предлагает различные решения как ключевые, так и ориентированные на решения специфических задач на производстве. Kaspersky Industrial CyberSecurity — это специализированное решение для мониторинга сети АСУ ТП и защиты конечных узлов промышленной среды. Представляет собой специализированную промышленную платформу класса XDR.

Ключевые решения

Защищает рабочие станции и серверы
в рамках промышленной сети

Подробнее



Kaspersky
Industrial CyberSecurity
for Nodes

Анализирует трафик на уровне
промышленных протоколов

Подробнее

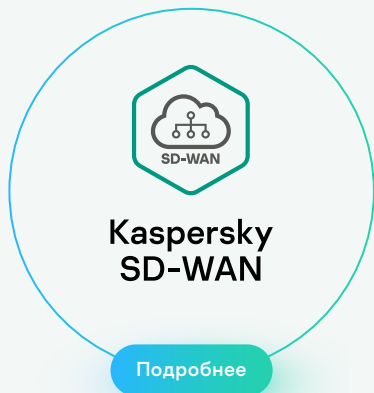


Kaspersky
Industrial CyberSecurity
for Networks



Команда экспертов

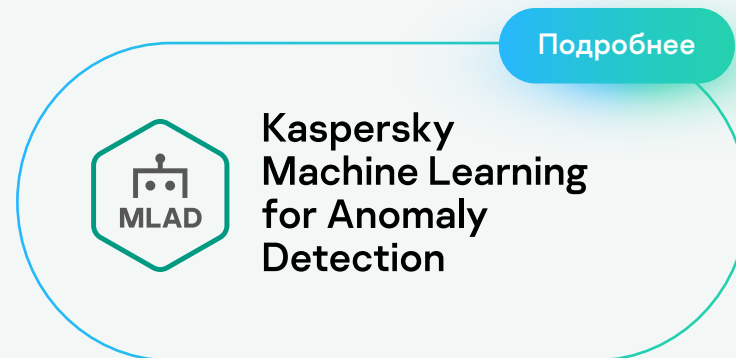
Уникальная команда ИБ-экспертов «Лаборатории Касперского» помогает обеспечивать кибербезопасность промышленной инфраструктуры предприятий разных отраслей. Эксперты создают эффективные решения с учетом исследований угроз для технологической сети, особенностей каждой индустрии и требованиям к ее защите.



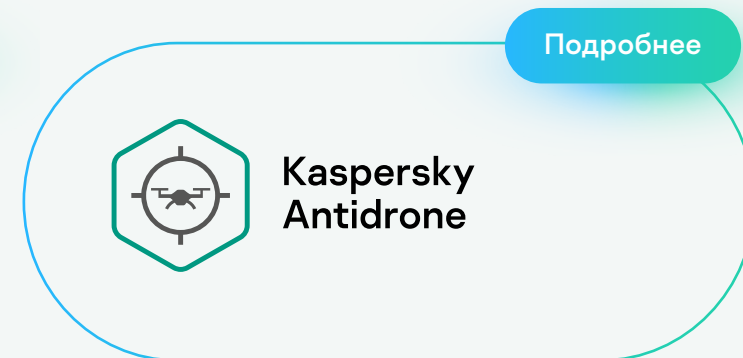
Решение позволяет построить отказоустойчивую территориально распределенную сеть с централизованным управлением

Фокусные решения

Обнаруживает отклонения в технологическом процессе на самом раннем этапе



Защищает воздушное пространство производств от беспилотных летательных аппаратов



Решения на базе KasperskyOS

Обеспечивает защищенное подключение к виртуальным рабочим столам, базируется на операционной системе KasperskyOS



Обеспечивает мониторинг систем интернета вещей и защищает их от кибератак, базируется на операционной системе KasperskyOS



Сотрудничество НЛМК и «Лаборатории Касперского» не ограничивается пилотными и коммерческими внедрениями, а скорее является перспективным технологическим партнерством.

Сергей Слаута,
Директор дирекции по автоматизации
технологических процессов, НЛМК



Киберугрозы способны нанести огромный ущерб предприятию. Речь идет как о репутационных и экономических потерях в результате сбоев технологического процесса, так и о возможном ущербе от действий киберпреступников в корпоративной среде. Сейчас нам удалось выстроить комплексную систему защиты нашей организации от киберугроз во всех сегментах нашего бизнеса, и все это благодаря тесному и продуктивному сотрудничеству с «Лабораторией Касперского».

Владимир Федотов,
Генеральный директор АЭМЗ

Единая киберзащита промышленного и корпоративного сегментов одного предприятия

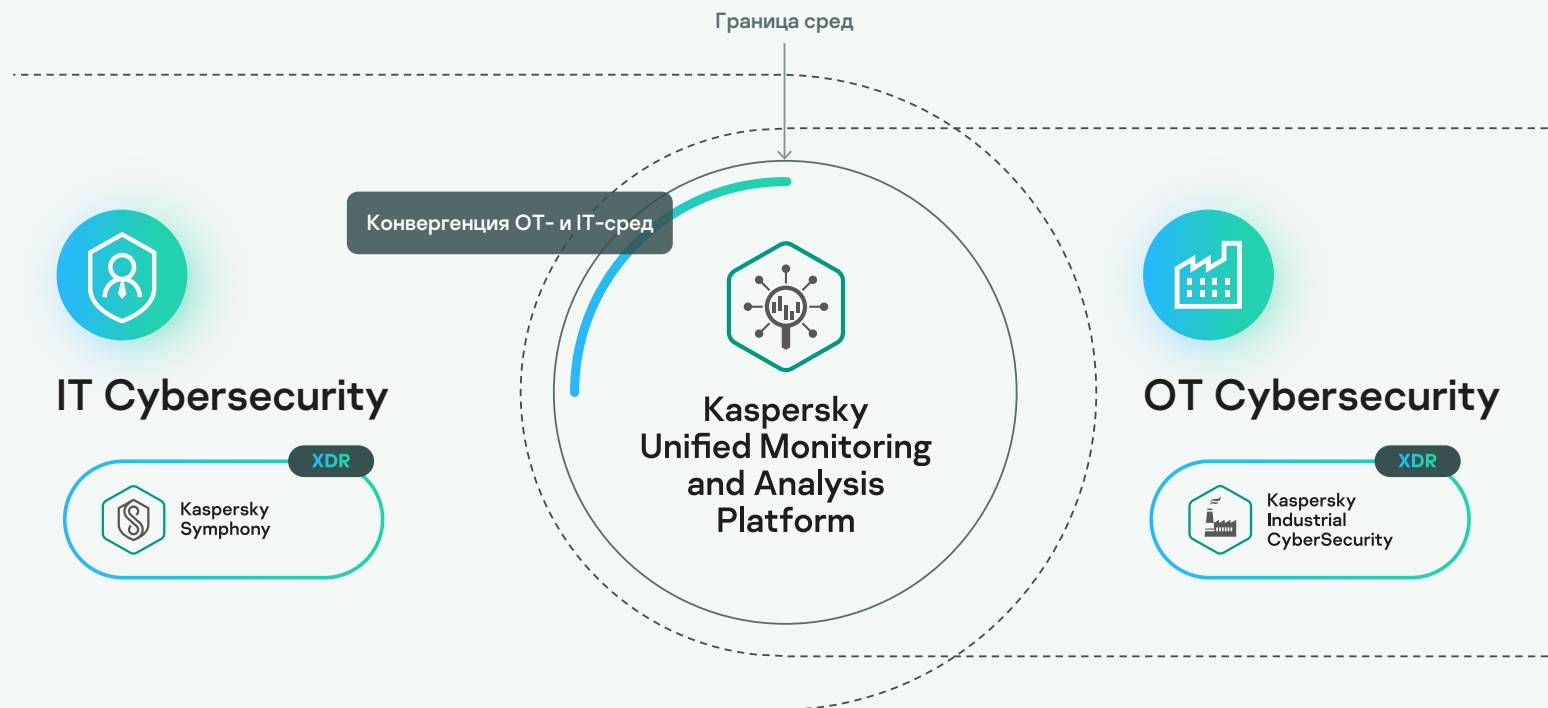
Одним из ключевых компонентов экосистемы кибербезопасности как промышленного, так и корпоративного сегмента является **Kaspersky Unified Monitoring and Analysis Platform** — решение класса SIEM, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и своевременной их нейтрализации.

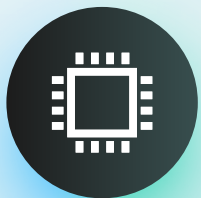
Благодаря тесной интеграции с SIEM-системой платформа Kaspersky Industrial CyberSecurity позволяет реализовывать больше сценариев взаимодействия с решениями сторонних поставщиков и расширять действия по расследованию и реагированию. Это также позволяет защищать бизнес не только в промышленной среде, но и в той части, где промышленная среда пересекается с корпоративной, тесно взаимодействуя с корпоративной XDR-платформой Kaspersky Symphony XDR.



Соответствие законодательству

Решение помогает организациям соответствовать действующему законодательству РФ в сфере безопасности объектов КИИ.





Доказанная эффективность технологий

FORRESTER®

Экономическая эффективность и рентабельность инвестиций от внедрения Kaspersky Industrial CyberSecurity были подтверждены ведущим аналитическим агентством Forrester в рамках проведенного исследования

[Подробнее](#)

FORRESTER®

 **THE RADICATI GROUP, INC.**
A TECHNOLOGY MARKET RESEARCH FIRM



Эффективность технологий и экспертных знаний «Лаборатории Касперского» подтверждена ведущими аналитическими агентствами (Gartner, Forrester, Radicati Group, Frost & Sullivan и другими)

[Подробнее](#)



**MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION**

*kaspersky.com/top3

Продукты «Лаборатории Касперского» ежегодно участвуют в широком наборе независимых тестов и исследований. С 2013 по 2021 год они приняли участие в 741 независимом тесте/обзоре. Они заняли **первое место в 518 случаях**

[Подробнее](#)

 **ТАТЭНЕРГО**



 **НОВОСТАЛЬ-М**

 **ҚазМұнайГаз**
ПАВЛОДАР МҮНАЙХИМИЯ ЗАУМТЫ

 **РОСАТОМ**

Более 100 успешных проектов по всему миру в промышленном сегменте и десятки публичных историй успеха

[Подробнее](#)



Сертификаты и соответствие стандартам



80+ сертификатов

Более 80 сертификатов о совместимости с оборудованием вендоров АСУ ТП

[Подробнее](#)



По результатам проведения аудита SDL сравнительная оценка реализации практик SDL в «Лаборатории Касперского» относительно выборки отечественных компаний составляет 10/10 баллов

[Подробнее](#)



Решения «Лаборатории Касперского» помогают организациям соответствовать требованиям законодательства РФ в области безопасности КИИ, в том числе к построению центров ГосСОПКА

[Подробнее](#)



Некоммерческая организация MITRE Corporation присвоила «Лаборатории Касперского» статус CVE Numbering Authority (CNA)

Сертификация ФСБ и ФСТЭК

Продукты «Лаборатории Касперского» сертифицированы ФСБ и ФСТЭК России и входят в единый реестр отечественного ПО

[ФСТЭК 4027](#)

[ФСТЭК 3907](#)

Стандарт SSAE 18

«Лаборатория Касперского» успешно прошла аудит SOC 2 Type 1 в соответствии со стандартом SSAE 18, проводимый компаниями из «большой четверки»

Global Transparency Initiative

«Лаборатория Касперского» поддерживает глобальную инициативу по информационной открытости (Global Transparency Initiative)

[Подробнее](#)

3

Знания



Сотрудничество с «Лабораторией Касперского» в рамках сервисов Kaspersky Threat Intelligence предоставило нам возможность по-новому взглянуть на современный ландшафт киберугроз.

Юрий Шеховцов,
Директор по информационным технологиям, Череповецкий металлургический комбинат

FORRESTER®

The Forrester Wave™:
External Threat Intelligence Services Q1, 2021

«Лаборатория Касперского»
признана лидером в области
сервисов оперативного
информирования о киберугрозах

Аналитика о киберугрозах для АСУ ТП

Противодействие современным киберугрозам тесно связано с пониманием полной картины тактик, техник и процедур, используемых злоумышленниками. Обладая петабайтами подробных данных об угрозах, «Лаборатория Касперского» предоставляет организациям достоверные аналитические данные об угрозах со всего мира в разных форматах, что помогает обеспечивать защиту даже от ранее неизвестных кибератак. Все исследования, связанные с аналитикой угроз для АСУ ТП, проводятся командой Kaspersky ICS CERT.

Отчеты об угрозах для АСУ ТП

Доступ по подписке к portalу с регулярными отчетами об атаках, угрозах и уязвимостях, характерных для АСУ ТП

Консультации с аналитиком

Индивидуальные консультации по угрозам АСУ ТП, уязвимостям, трендам и индустриальным стандартам

[Подробнее](#)

Kaspersky
ICS CERT Services

Потоки данных о ВПО для АСУ ТП

Индикаторы компрометации (IoC) и метаданные для интеграции с SIEM-системами

Потоки данных об уязвимостях АСУ ТП

Точная и актуальная информация для выявления уязвимостей в сетях АСУ ТП

Тренинги в области промышленной кибербезопасности



Kaspersky Security Awareness

Подробнее

Повышение киберграмотности сотрудников

Внедрение технических средств обеспечения безопасности — это лишь часть стратегии защиты промышленных сред. Повышение осведомленности сотрудников столь же важно, так как всего одна ошибка сотрудника, не знакомого с основами кибербезопасного поведения, может привести к серьезному инциденту. «Лаборатория Касперского» предлагает короткие, но интенсивные обучающие курсы для рядовых сотрудников предприятий, для IT/OT-операторов, инженеров АСУ ТП, а также игровые тренинги по промышленной кибербезопасности для руководителей.



Kaspersky ICS CERT Training

Подробнее

Получение экспертных знаний

Специалистам в области безопасности IT/OT следует постоянно повышать свой уровень знаний и оттачивать профессиональные навыки. Постоянное развитие — залог успешной борьбы с киберугрозами. Организации могут повысить экспертизу своих экспертов с помощью тренингов Kaspersky ICS CERT Training.

“ В ходе тренинга мы получили много полезной информации и практических навыков, применимых в работе. Хочется отдельно отметить, что тренинг проводят эксперты с реальным практическим опытом, готовые ответить на любой возникающий вопрос. Методология криминалистики, которую мы получили, апробирована под производственные системы и с легкостью будет внедрена в наши процессы.

Сергей Повышев,
Старший менеджер группы защиты
производственных систем Управления
информационной безопасности
ПАО «Северсталь»



Опыт и знания мирового уровня

4500+

специалистов

В «Лаборатории Касперского» работает более 4500 высококвалифицированных специалистов, половина из которых — **R&D-эксперты**.

GREAT

В основе решений и сервисов «Лаборатории Касперского» лежат знания об аналитических данных о масштабных АPT-атаках, полученных глобальным центром исследования и анализа угроз «Лаборатории Касперского» (GREAT)

Штатные эксперты обладают международными сертификатами: OSCP, OSCE, GREM, GCFA, GCFE, GRID, GCIH, CEH, CREST CPSA, CCNA (Discovery, R&S), GIAC (GPEN, GXPN, GNFA, GCIH), CCNP R&S, ICSI CNSS, CISSP, CISM, CISA и др.



разработчиков

Команда разработчиков решений для защиты промышленных объектов насчитывает 400 человек



«Лаборатория Касперского» открыто делится информацией обо всех нашумевших вредоносных кампаниях, попавших в зону внимания наших экспертов (в том числе с помощью проекта «Хроника целевых кибератак»). Каждое полугодие публикуются отчеты об угрозах как для всего мира, так и отдельно по России.

[Подробнее](#)

MITRE | ATT&CK®

«Лаборатория Касперского» является контрибьютером аналитики о киберугрозах для различных мировых сообществ, в том числе для компании MITRE с целью повышения качества их матрицы тактик и техник злоумышленников ATT&CK

ICS
CERT

«Лаборатория Касперского» имеет собственное международное подразделение Kaspersky Industrial Control Systems Cyber Emergency Response Team (ICS CERT), которое нацелено на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных объектов критически важных инфраструктур.

[Подробнее](#)

4

Экспертиза



Важнейшим приоритетом для нас является вопрос защищенности АО «МОСГАЗ» от киберугроз, поэтому мы обратились к экспертам «Лаборатории Касперского», которые провели детальный анализ нашей промышленной инфраструктуры и безопасно интегрировали специализированное решение по кибербезопасности АСУ ТП.

Александр Кузин,
Заместитель начальника Управления
информатизации, АО «МОСГАЗ»

Экспертные сервисы

Привлекая внешних экспертов, вы сможете просчитать возможные векторы сложных атак и получить практические рекомендации по борьбе с ними. «Лаборатория Касперского» — это надежный партнер, обладающий глубокой экспертизой и опытом оказания сервисов, который поможет в экстренной ситуации, оценит текущее состояние защищенности систем и поможет эффективно прореагировать на сложные инциденты.



Каждая промышленная
среда уникальна, поэтому мы
адаптируем наши сервисы
под конкретную отрасль

[Подробнее](#)

Kaspersky
ICS CERT Services

Сервисы «Лаборатории Касперского»

Экспертные сервисы Kaspersky OT CyberSecurity помогают усилить кибербезопасность организаций и включают анализ защищенности, тестирование на проникновение, реагирование на инциденты и цифровую криминалистику. Эксперты «Лаборатории Касперского» располагают обширным международным опытом в области обеспечения кибербезопасности промышленных предприятий различных отраслей и используют единый структурированный подход к идентификации актуальных промышленных угроз, исследованию и предотвращению киберинцидентов.



Высокий статус в индустрии безопасности IT/OT-систем

F R O S T  S U L L I V A N

«Лаборатория Касперского» признана международной компанией года на рынке промышленной кибербезопасности в 2020 году по данным Frost & Sullivan

VDC|Research

«Лаборатория Касперского» стала обладателем платиновой награды VDC Research 2020 в категории «Промышленная безопасность» за решения для промышленного интернета вещей



«Лаборатория Касперского» — член консорциума промышленного интернета (Industrial Internet Consortium)



«Лаборатория Касперского» — постоянный участник в расследованиях и операциях по противодействию киберугрозам совместно с международными организациями, такими как Интерпол и Европол и центрами CERT по всему миру



«Лаборатория Касперского» поддерживает сообщество экспертов в области промышленной безопасности и ежегодно проводит конференцию [Kaspersky Industrial Cybersecurity Conference](#), где собирает ведущих экспертов со всего мира

[Подробнее](#)

Заключение

Число атак на промышленные системы, в частности на системы АСУ ТП и SCADA, продолжает расти. При этом традиционные решения не способны защитить промышленные среды от специализированных киберугроз. Именно поэтому сегодня как никогда важен выбор надежного партнера, который обладает экспертизой в корпоративной и промышленной среде кибербезопасности и готов предложить комплексный подход, способный обезопасить индустриальную и корпоративную среду от актуальных киберугроз.



Kaspersky OT CyberSecurity — это сплав технологий и экспертизы для промышленной кибербезопасности. Во главе с центральным компонентом индустриальной XDR-платформой — Kaspersky Industrial CyberSecurity.



Kaspersky
OT CyberSecurity

Подробнее

Защитите вашу промышленную инфраструктуру с помощью Kaspersky OT CyberSecurity

www.kaspersky.ru

© 2022 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.