



Kaspersky Symphony

Системный подход к защите
вашего бизнеса



**Kaspersky
Symphony**



**Системный
подход к кибер-
безопасности
вашего бизнеса**

Виртуозный ответ на современные вызовы

Усложнение ландшафта киберугроз, цифровизация информационной среды, постоянная оптимизация бизнес-процессов, изменение ситуации на рынке ИБ-решений и необходимость соответствовать законодательным требованиям – все это формирует у организаций понимание важности системного подхода к защите своего бизнеса.

Kaspersky Symphony поможет выстроить комплексную киберзащиту в соответствии с задачами компании и ее ростом и позволит сохранить время ИБ-специалистов.

Вызовы в сфере ИБ



Рост числа кибератак и усложнение тактик, техник и процедур, используемых злоумышленниками



Увеличение количества точек входа злоумышленников в инфраструктуру



Уход с рынка иностранных ИБ-производителей и усиление регуляторных требований



Уменьшение числа квалифицированных ИБ-специалистов на рынке труда и рост спроса на них

Ключевые преимущества

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

Почему выбирают нас

Почему предприятия могут рассчитывать на «Лабораторию Касперского» в вопросе киберзащиты своего бизнеса?

1

Технологии
для всесторонней
защиты бизнеса



Доказанная
эффективность
технологий

2

Аналитика
и экспертиза
мирового уровня



Международный
опыт

3

Единая
платформа
для усиления
возможностей
каждого
компонента XDR
защиты



Единый партнер
по кибер-
безопасности

Варианты защиты

Помимо фундаментальной защиты рабочих мест (Kaspersky Symphony Security), в рамках всей линейки решений Kaspersky Symphony «Лаборатория Касперского» предлагает два варианта создания надежной защиты от сложных киберугроз:

- Выстраивание собственной передовой защиты с помощью продвинутых инструментов ИБ (Symphony EDR и Symphony XDR)
- Делегирование задач по мониторингу и реагированию экспертом «Лаборатории Касперского» (Symphony MDR)

Продвинутые технологии защиты

Линейка решений Kaspersky Symphony **содержит 4 уровня защиты**, которые включают такие технологии, как EPP, EDR, MDR и XDR, для всесторонней защиты компаний как от массовых угроз, так и от целевых атак.

Kaspersky Symphony	Security	MDR	EDR	XDR
Уровень защиты	Базовая собственная защита	Передовая управляемая защита	Передовая собственная защита	Расширенная собственная защита
Автоматическая защита физических и виртуальных конечных точек от массовых угроз	●	●	●	●
Передовое обнаружение сложных угроз на уровне конечных точек и реагирование на них		●	●	●
Детектирование с помощью песочницы и реагирование на обнаружения				●
Мониторинг и корреляция событий ИБ (+модуль ГосСОПКА)				●
Централизованное управление инцидентами с единым графом расследования				●
Управление аналитическими данными о киберугрозах и встроенные потоки данных				●
Защита электронной почты и веб-трафика				●
Глубокий анализ сетевого трафика и реагирование на уровне шлюзов				●
Повышение киберграмотности				●

XDR Core



Kaspersky Symphony Security

Endpoint Protection Platform

Фундаментальная защита физических и виртуальных конечных точек, а также мобильных устройств

Общая защита конечных
точек всех платформ

Мощные инструменты
контроля

Экономия ресурсов за счет
унифицированного управления



Kaspersky Symphony MDR

Managed Detection
and Response

Управляемая экспертная защита мирового уровня

Знания и опыт экспертов
международного уровня

Передовая защита
от киберугроз

Эффективное
использование ресурсов

Поддержка базовых возможностей EDR
для собственного контроля



Kaspersky Symphony EDR

Endpoint Detection
and Response

Расширение собственной защиты

Передовое обнаружение угроз
и зрелый процесс расследования

Высокий уровень
автоматизации

Точное и быстрое реагирование
на сложные инциденты



Kaspersky Symphony XDR

Extended Detection
and Response

Верхний уровень – мощная платформа класса XDR

Передовые
технологии

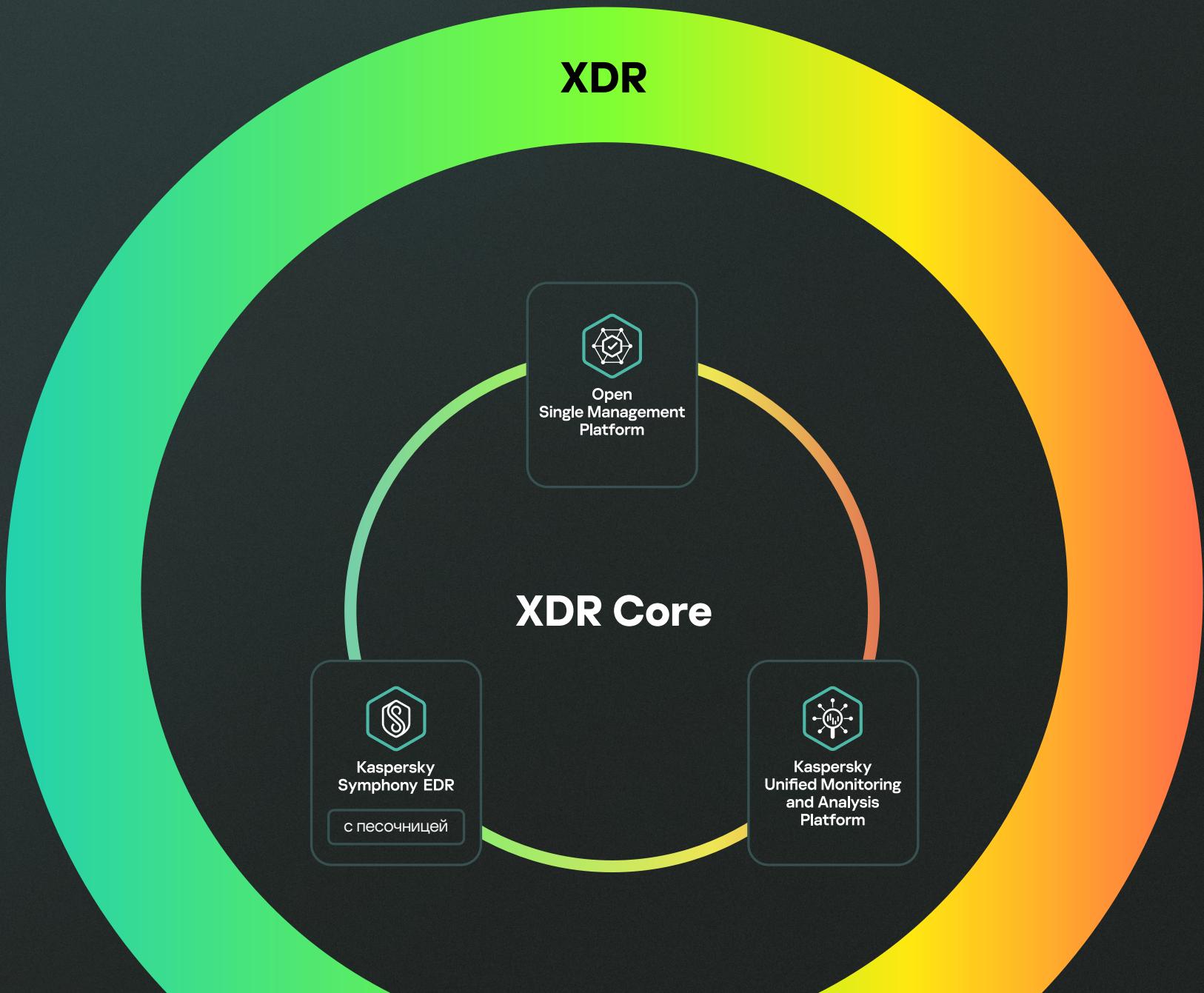
Кросс-продуктовое
взаимодействие

Единое представление
информации

Соответствие
требованиям

Kaspersky Symphony XDR Core

Базовый уровень лицензирования платформы Kaspersky Symphony XDR, который включает в себя ключевой набор продуктов для выстраивания защиты класса XDR. Решение идеально подходит организациям, для которых важна гибкость и поэтапность в построении мощной XDR-защиты: как на базе как на базе решений «Лаборатории Касперского», так и на основе продуктов других производителей.



Состав Kaspersky Symphony XDR

Мощная защита на уровне сети

-  Kaspersky Anti Targeted Attack
-  Kaspersky Security для почтовых серверов
-  Kaspersky Security для интернет-шлюзов

Платформа обучения киберграмотности

-  Kaspersky Automated Security Awareness Platform

Kaspersky Symphony XDR

Kaspersky Symphony XDR Core

-  Open Single Management Platform
-  Kaspersky Unified Monitoring and Analysis Platform
-  Kaspersky Symphony EDR + песочница

Интеграция с ИБ-решениями



Сторонние решения



Решения Kaspersky

Потоковое обогащение данными

-  Kaspersky Threat Data Feeds
 - Malicious URL
 - Malicious Hashes
 - Phishing URL
 - Botnet C&C URL
 - IP Reputation

-  Kaspersky CyberTrace

Поисковый портал о киберугрозах и взаимосвязях

-  Kaspersky Threat Lookup

Сильные стороны Kaspersky Symphony XDR



Общепризнанная защита конечных точек

Протестированное MITRE решение класса EDR в синергии с EPP, которое защищает более 60 млн корпоративных рабочих мест по всему миру



Повышение уровня киберграмотности

Онлайн-тренинги, повышающие уровень киберграмотности сотрудников, что снижает число успешных атак, связанных с человеческим фактором (например, использующих социальную инженерию)



Взаимодействие элементов системы ИБ

Тесная интеграция включенных элементов с поддержкой различных кросс-продуктовых сценариев. Возможность взаимодействия с решениями сторонних поставщиков



Обогащение аналитическими данными

Аналитика об угрозах, признанная лучшей в мире (по результатам исследования SPARK Matrix™: Digital Threat Intelligence Management в 2024 году)



Гибкость сетевой защиты

Защита электронной почты и доступа в интернет, анализ сетевого трафика и Netflow, песочница, а также возможность загрузки фидов с данными об угрозах в сторонние сетевые инструменты



Соответствие требованиям регуляторов

Соответствие требованиям регуляторов (например, в сфере безопасности объектов КИИ), в том числе благодаря встроенному модулю ГосСОПКА

Доказанная эффективность технологий



БОЛЬШЕ ТЕСТОВ*
БОЛЬШЕ НАГРАД*
БОЛЬШЕ ЗАЩИТЫ

*kaspersky.ru/top3

Продукты и технологии «Лаборатории Касперского» ежегодно участвуют в широком наборе независимых тестов и исследований. С 2013 по 2023 год они приняли участие в 927 независимом teste/обзоре. В 680 случаях они заняли первое место

Подробнее



FORRESTER®

IDC

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Эффективность технологий и качество экспертных знаний «Лаборатории Касперского» подтверждены ведущими аналитическими агентствами

Подробнее

MITRE
ENGENUITY™ | ATT&CK® Evaluations



AVTEST

AV
comparatives

ICSA labs
CERTIFIED ADVANCED THREAT DEFENSE

Качество обнаружения киберугроз решениями «Лаборатории Касперского» подтверждено оценками MITRE ATT&CK, SE Labs, AV-Test, AV-Comparatives и другими независимыми тестовыми лабораториями

Подробнее

МКБ РТИ

ВБРР РОСАТОМ

Десятки реализованных проектов по всему миру – это истории успеха, которыми делятся наши клиенты и партнеры

Подробнее



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



2024 SPARK Matrix™: Digital Threat Intelligence Management by Quadrant Knowledge Solutions

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

Передовая аналитика о киберугрозах

Противодействие современным киберугрозам тесно связано с пониманием тактик, техник и процедур, которые используются злоумышленниками по всему миру. «Лаборатория Касперского» обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Информация от собственных аналитиков и исследователей мирового уровня аккумулируется в платформе **Kaspersky Threat Intelligence**.

Ее функциональность включена в верхний уровень линейки – Kaspersky Symphony XDR.



Kaspersky Threat Lookup

Поисковый портал о киберугрозах и взаимосвязях

Портал получает результаты анализа угроз, детализированные по веб-адресам, доменам, IP-адресам, хешам файлов, названиям угроз, статистическим и поведенческим данным, данным WHOIS/DNS, атрибутам файлов, данным геолокации, цепочкам загрузки, временным меткам и др.



Kaspersky CyberTrace

Платформа консолидации потоков данных о киберугрозах

Платформа дает возможность интегрировать потоки данных об угрозах с различными системами безопасности для их дальнейшего эффективного использования. Продукт позволяет работать с любым потоком аналитических данных в форматах JSON, STIX, XML и CSV



Kaspersky Threat Data Feeds

Потоки данных об угрозах

Malicious URL
(URL-адреса вредоносных ссылок)

IP Reputation
(данные о репутации IP-адресов)

Malicious Hashes
(хеши вредоносных объектов)

Phishing URL
(URL-адреса фишинговых ссылок)

Botnet C&C URL
(URL-адреса командных серверов ботнетов)

Международный опыт

5000+ специалистов

В «Лаборатории Касперского» работает более 5000 высококвалифицированных специалистов, 1/3 из которых — R&D-эксперты

30% прибыли

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

CERT

«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

MITRE

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



«Лаборатория Касперского» открыто делится информацией обо всех нашумевших вредоносных кампаниях, попавших в зону пристального внимания экспертов «Лаборатории Касперского» (в том числе с помощью проекта «Хроника целевых кибератак»)

[Подробнее](#)

Эксперты «Лаборатории Касперского»

Не просто защищают мир от существующих угроз, но и ежедневно исследуют и изобретают новые направления борьбы с ними. Полученные знания об атаках, группировках и зловредах со всего мира лежат в основе решений и сервисов «Лаборатории Касперского».

Всего в компании действуют пять центров уникальной экспертизы:

- Глобальный центр исследований и анализа угроз (Kaspersky GREaT)
- Kaspersky Threat Research (Центр исследования угроз)
- Kaspersky AI Technology Research (Центр исследования технологий искусственного интеллекта)
- Центр сервисов по кибербезопасности (Kaspersky Security Services)
- Центр исследования безопасности промышленных систем (Kaspersky ICS CERT)

[Подробнее](#)





Решение помогает организациям соответствовать

Требованиям законодательства РФ. Решение позволяет выполнить требования законодательства в части обнаружения, предупреждения кибератак и ликвидации их последствий, информирования о компьютерных инцидентах, а также установления причин и условий их возникновения. Встроенный модуль ГосСОПКА позволяет напрямую обмениваться данными об инцидентах с НКЦКИ.

Единая платформа кибербезопасности

Линейка решений Kaspersky Symphony – это комплекс тесно интегрированных технологий и решений, основанных на экспертизе и многолетнем практическом опыте. Благодаря единой платформе компании увеличивают эффективность системы безопасности и прозрачность инфраструктуры и готовы успешно отражать атаки любого масштаба и сложности. Кроме того, обеспечивается соответствие требованиям регулирующих органов.

Наиболее полно платформенный подход воплощен в уровне **Kaspersky Symphony XDR**. Это решение, которое защищает многочисленные точки входа в организацию, в том числе сеть, почту и конечные устройства, от потенциальной угрозы, обогащено знаниями признанной лучшей в мире глобальной системы информирования об угрозах Kaspersky Threat Intelligence, оберегает компанию от ошибок рядовых сотрудников (например, в результате фишинговой атаки) и готово легко встроиться в существующую систему безопасности.

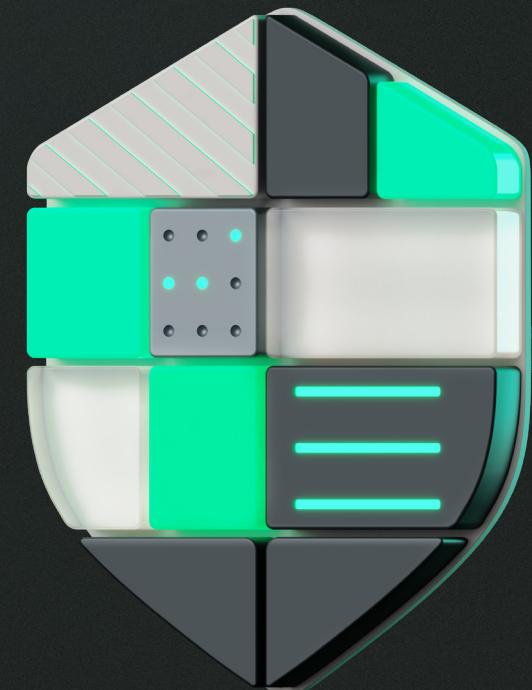
Снижение издержек за счет:

Единой схемы
лицензирования

Единой службы
поддержки

Единой точки
взаимодействия

Единого поставщика
по кибербезопасности



Глобальный охват и международное сотрудничество

Сегодня организациям необходима поддержка надежного партнера, обладающего многолетним опытом, глобальной экспертизой и пониманием современных кибер вызовов. «Лаборатория Касперского» готова обеспечить инструментарием и аналитикой, необходимыми для отражения угроз, помочь в экстренной ситуации и поделиться опытом и знаниями.

Единый партнер по кибербезопасности



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

30+ офисов по всему миру
Деятельность более чем в **200 странах мира**

27

Более 27 лет «Лаборатория Касперского» разрабатывает и предлагает решения для защиты предприятий



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



Сегодня технологии «Лаборатории Касперского» защищают во всем мире:

400+ миллионов пользователей
240+ тысяч корпоративных клиентов



«Лаборатория Касперского» обладает проектным опытом внедрения в разных отраслях:

- Банки и финансы
- Строительство
- Государственный сектор
- Пищевая промышленность
- Здравоохранение
- СМИ
- Транспортная инфраструктура
- Добыча полезных ископаемых
- Электроэнергетика
- Тяжелая промышленность и др.

Требования регуляторов



Реестр российского ПО

«Лаборатория Касперского» является отечественным разработчиком средств информационной безопасности, и ее решения внесены в единый реестр российского ПО

Сертификаты ФСБ и ФСТЭК России

Основные решения «Лаборатории Касперского» имеют сертификаты ФСТЭК и ФСБ России

Безопасная разработка

«Лаборатория Касперского» первой в России прошла сертификацию процессов безопасной разработки и получила сертификат №1 в ФСТЭК России о соответствии процессов безопасной разработки программного обеспечения требованиям ГОСТ Р 56939. Сегодня требование соответствию ГОСТ Р 56939 уже включается во все проводимые заказчиками тендеры, оно прописано в документах всех значимых отраслей, таких как банковская сфера, КИИ, транспорт, медицина

Единая концепция кибербезопасности



Корпоративная ИТ-безопасность

FSTЭK FСБ

ЦБ РФ СТО БР ИББС

GDPR PCI DSS

Соответствие

Необходимость следования рекомендациям и требованиям действующего законодательства порождает вопрос: причем здесь возврат инвестиций? Все просто: определенные требования регуляторов обязательны для выполнения, и им необходимо следовать во избежание проблем и возможных убытков, связанных с несоответствием таким требованиям.

Ключевые аспекты современных законодательных требований

Сертифицированное ПО

Использование решений, присутствующих в Реестре российского ПО Минцифры РФ и имеющего сертификаты ФСБ и ФСТЭК России, в т. ч. в цепочке поставок.

Сбор и централизованное хранение данных,

вердиктов и иной информации, связанной с произошедшими инцидентами, которые позволяют оказывать содействие специалистам ФСБ, предоставляя им необходимую информацию об обнаруженных угрозах.

Только отечественные решения

Полный запрет для ряда организаций использования СЗИ и сервисов по информационной безопасности, происходящих из недружественных стран.

Указ Президента РФ от 01.05.2022 N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Защита персональных данных

Соблюдение требований по сбору, хранению ПДн, обращению с ними и их защите.

Проверка инфраструктуры

на наличие получаемых от регуляторов (в т. ч. отраслевых) индикаторов компрометации, проведение оперативных мер по реагированию и пр.

Обязательства по информированию

об инцидентах через передачу информации о кибератаках на КИИ в ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак).

SDL

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

[Подробнее](#)

Информационная открытость и соответствие требованиям

Сертификация ФСБ и ФСТЭК

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

[Подробнее](#)

Global Transparency Initiative

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

[Подробнее](#)


Решения «Лаборатории Касперского» помогают организациям соответствовать требованиям регуляторов, в том числе в области безопасности КИИ

[Подробнее](#)

Стандарт SSAE 18

«Лаборатория Касперского» успешно прошла аудит SOC 2 Type 1 в соответствии со стандартом SSAE 18, проводимый компанией из «большой четверки». Процесс разработки и выпуска антивирусных баз защищен от неавторизованного вмешательства благодаря сильным механизмам контроля безопасности

[Подробнее](#)

Аудиты от TÜV AUSTRIA

По результатам проведенных аудитов компанией TÜV AUSTRIA «Лаборатория Касперского» подтвердила соответствие требованиям международного стандарта систем менеджмента информационной безопасности ISO/IEC 27001

[Подробнее](#)


Некоммерческая организация MITRE Corporation присвоила «Лаборатории Касперского» статус CVE Numbering Authority (CNA), то есть «Лаборатория Касперского» вошла в состав CNA как исследователь уязвимостей и стала шестой компанией в мире с таким статусом

[Подробнее](#)

Заключение

Сегодня как никогда важен именно комплексный системный подход к кибербезопасности бизнеса, который включал бы взаимодополняющие друг друга классы технологий – EPP, EDR, MDR и XDR – и при этом соответствовал бы требованиям регулирующих органов. «Лаборатория Касперского» уже следует такому подходу, воплощая его в новой линейке решений Kaspersky Symphony.



Заштите свой бизнес от кибератак любой сложности



Kaspersky Symphony

Киберзащита как искусство

Запросить демо решения или задать
вопросы вы можете, написав письмо
на symphony@kaspersky.com

Подробнее

Написать