

Kaspersky Security для ПОЧТОВЫХ серверов

Надежная
многоуровневая защита
корпоративной почты

kaspersky активируй
будущее



Статистика угроз в 2025 году

81%

организаций столкнулись с атаками
через электронную почту

>144 миллиона

атак с использованием вредоносных
вложений обнаружено
и заблокировано решениями
«Лаборатории Касперского»

>554 миллиона

попыток фишинговых атак обнаружено
и заблокировано решениями
«Лаборатории Касперского»

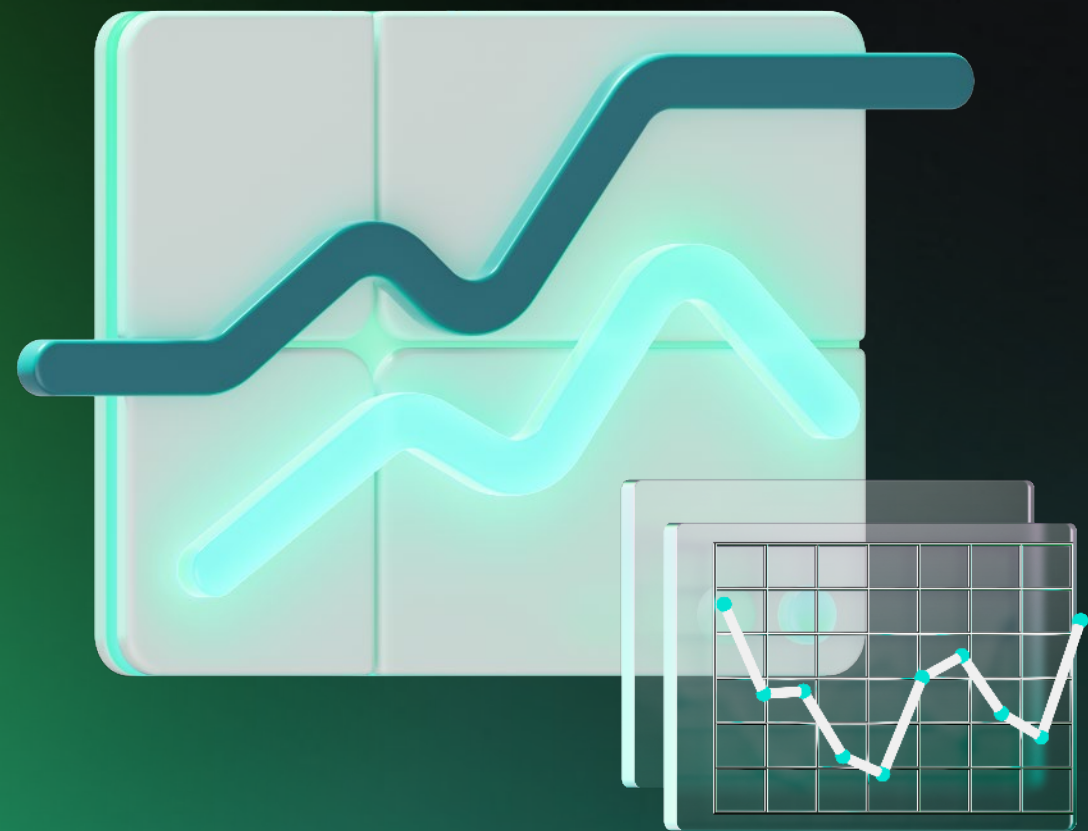


Независимо от размера
организации, базовых
встроенных средств
защиты электронной
почты уже недостаточно
для противодействия
современным угрозам.



Сегодня для надежной защиты
электронной почты требуется
решение с расширенными
возможностями безопасности.

Ключевые тенденции и вызовы современного рынка



Развитие киберугроз и появление новых методов и сценариев атак



Сложные почтовые атаки с применением искусственного интеллекта



Рост числа кибератак через сервисы совместной работы и средства корпоративных коммуникаций

Обзор продукта

01



01 Обзор продукта

02 Ключевые технологии

03 Интеграция

04 Лицензирование

05 Преимущества
«Лаборатории Касперского»

О решении



Kaspersky Security для ПОЧТОВЫХ серверов

Защищает от спама, вредоносных вложений, фишинга, компрометации корпоративной электронной почты (BEC), атак с QR-кодами и других киберугроз.

Решение также обеспечивает контроль над передачей информации, помогая предотвратить нарушения бизнес-процессов, финансовые потери от мошенничества и утечки данных.

Возможности



Защита от массовых атак и сложных угроз



Простое масштабирование и адаптация к растущему объему почтового трафика



Защита любой почтовой инфраструктуры



Снижение рисков атак через электронную почту

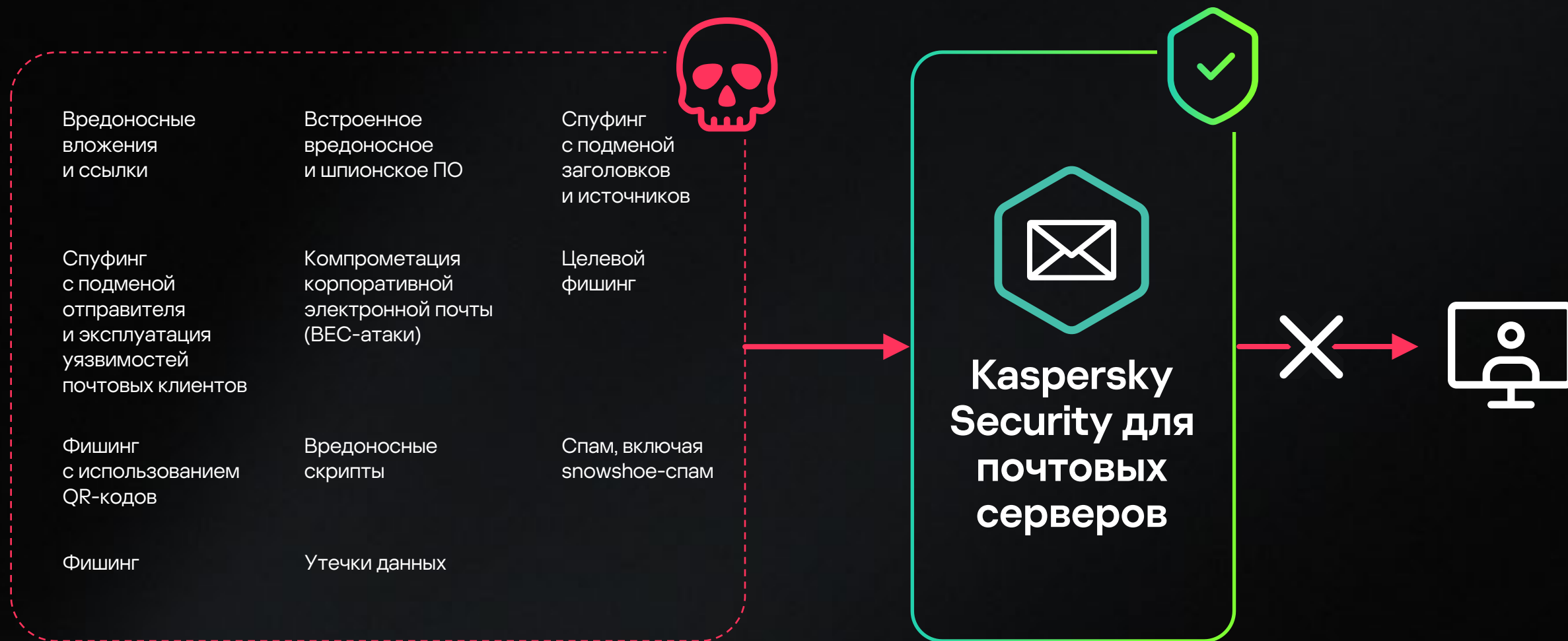


Интеграция с почтовой инфраструктурой и текущими решениями для защиты



Экономическая эффективность и максимальная безопасность в рамках одной лицензии

Надежная защита от массовых атак и сложных угроз, распространяемых по электронной почте



Преимущества для бизнеса



Усиление защиты почтовой инфраструктуры

Единый продукт для надежной защиты от актуальных угроз, который создан на базе запатентованных технологий машинного обучения, используемых для обнаружения и реагирования.



Снижение рисков атак через электронную почту

Защита от всех видов угроз, распространяемых по электронной почте, и снижение рисков остановки бизнес-процессов, финансового и репутационного ущерба, а также утечек данных.



Оптимизация расходов

Три приложения с расширенными возможностями защиты для различных почтовых инфраструктур в рамках одной лицензии. Гибкая модель подписки обеспечивает прогнозируемость и контроль расходов на безопасность.



Kaspersky Security для почтовых серверов

Комплексное решение для защиты электронной почты и сервисов для совместной работы, обеспечивающее полную безопасность корпоративных коммуникаций

Три ключевых приложения в составе Kaspersky Security для почтовых серверов



**Kaspersky
Secure Mail
Gateway**

Виртуальное
или standalone-решение



**Kaspersky
Security
для Microsoft
Office 365**

SaaS



**Kaspersky
Security для Microsoft
Exchange Servers**

Локальная версия
(on-premise)

- Подходит для любой почтовой инфраструктуры — локальной, облачной или гибридной на базе Windows или Linux
- Обеспечивает защиту на уровне шлюза и почтовых ящиков

Kaspersky Secure Mail Gateway



Kaspersky
Secure Mail
Gateway



Kaspersky
Security
для Microsoft
Office 365



Kaspersky
Security
для Microsoft
Exchange Servers

Блокируйте угрозы
до того как они
ДОСТИГНУТ СВОЕЙ ЦЕЛИ

Готовый шлюз электронной почты (SEG) для выявления и блокирования опасных писем на ранних этапах атаки — еще до того, как они попадут на устройство пользователя и причинят ущерб.

Виртуальное решение

Standalone-решение

Компоненты приложения:



Операционная
система



Почтовый агент
(MTA)



Приложение
для защиты
электронной
почты



Удобный
веб-интерфейс

Kaspersky Security для Microsoft Office 365



Kaspersky
Secure Mail
Gateway



Kaspersky
Security
для Microsoft
Office 365



Kaspersky
Security
для Microsoft
Exchange Servers

Будьте на шаг впереди сложных угроз,
распространяемых по электронной почте
и через сервисы для совместной работы

Облачное решение, обеспечивающее защиту
сервисов Microsoft Office 365 для почты,
общения и совместной работы — Exchange
Online, OneDrive, SharePoint Online и Teams —
от угроз безопасности.

SaaS



Интеграция через API



Облачное решение —
не требует дополнительного
оборудования и ПО



Надежные технологии
безопасности

Kaspersky Security для Microsoft Exchange Servers



Kaspersky
Secure Mail
Gateway



Kaspersky
Security
для Microsoft
Office 365



Kaspersky
Security
для Microsoft
Exchange Servers

Защитите почтовую инфраструктуру Microsoft Exchange с помощью надежных технологий безопасности



Мониторинг входящего,
исходящего
и внутрисетевого
почтового трафика



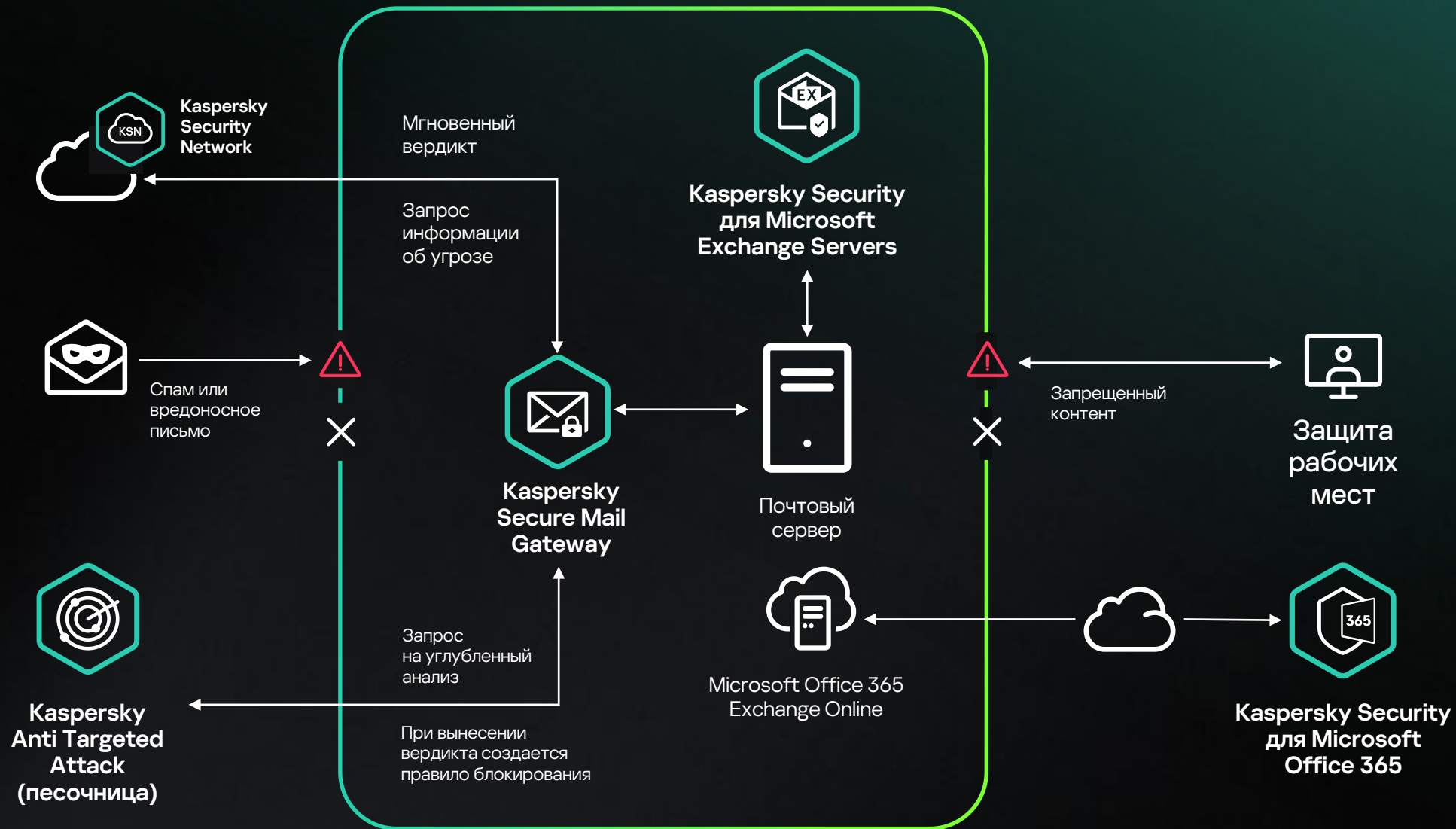
Защита почтовой
инфраструктуры Microsoft
Exchange как на уровне шлюза,
так и на уровне почтовых ящиков



Интеграция
с Microsoft Exchange
Server через API

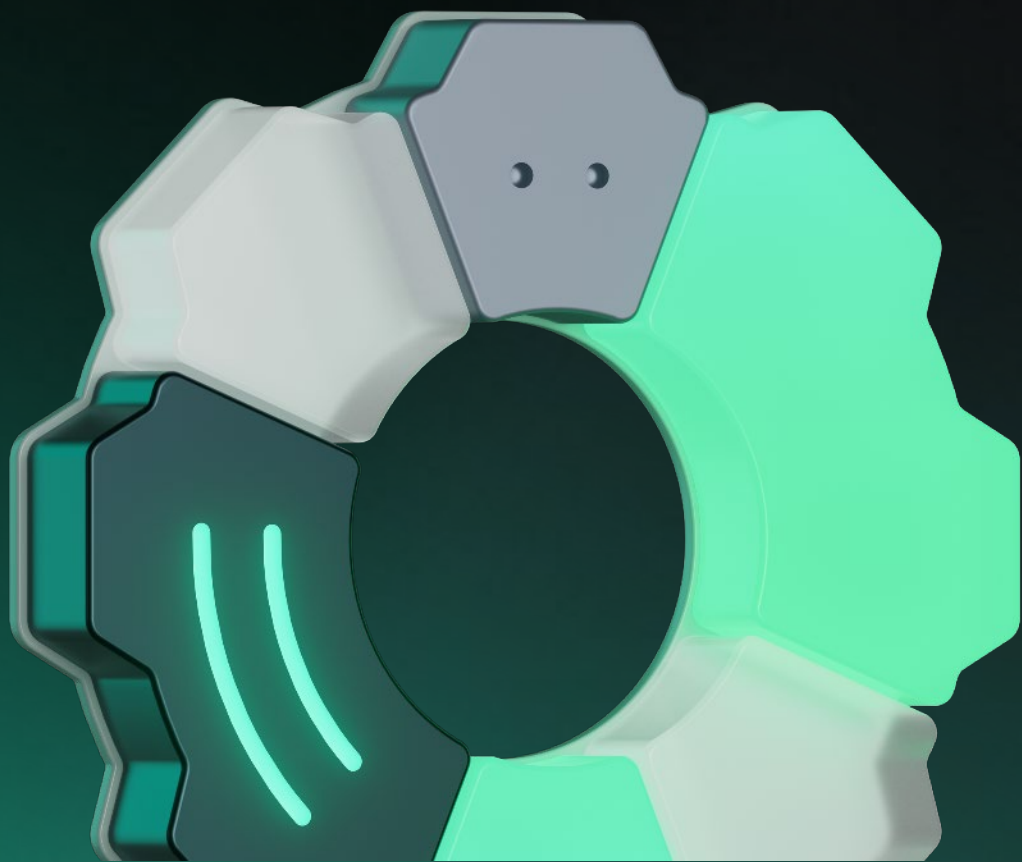
Локальная версия
(On-premise)

Архитектура продукта



Ключевые технологии

02



01 Обзор продукта

02 Ключевые технологии

03 Интеграция

04 Лицензирование

05 Преимущества
«Лаборатории Касперского»

Анализ почтового трафика и основные технологии



Электронное письмо

Извлечение заголовков, текста письма, вложений, ссылок, изображений и других объектов



Защита от вредоносного ПО

- Углубленная проверка вложений
- Поддержка KSN и KPSN

Проверка отправителя

- Продвинутые механизмы проверки на базе SPF, DKIM, DMARC
- Сопоставление доменов отправителя

Проверка ссылок

Обнаружение вредоносных ссылок, рекламных приложений и потенциально опасного ПО

Защита от спама

- Интеллектуальные технологии обнаружения спама и массовых рассылок
- Антиспам-карантин
- Защита от спуфинга
- Анализ репутации IP-адресов и доменов

Защита от фишинга

Расширенные технологии на базе машинного обучения для обнаружения целевого фишинга, фишинга с использованием QR-кодов, спуфинга, BEC-атак и т. д.

Content Disarm and Reconstruction (CDR)

Удаление потенциально вредоносных объектов из электронных писем и вложений и восстановление их содержимого в безопасном файле

Контентная фильтрация и защита от утечек данных

- Фильтрация с использованием регулярных выражений
- Фильтрация вложений

Облачные технологии для репутационного анализа

Репутационный анализ доменов, IP- и URL-адресов

Анализ в песочнице

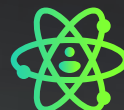
Динамический анализ вложений в изолированной среде

Защита от вредоносного ПО

Надежная многоуровневая система, которая с высокой точностью обнаруживает вредоносные программы и проактивно блокирует их с помощью технологий на базе машинного обучения.



Технологии на базе нейросетей
глубокого обучения



Технологии машинного обучения
для повышения безопасности



Защита от вредоносных программ, в том
числе шпионского ПО, банковских троянцев,
шифровальщиков, криптомайнеров,
вайперов и других

Защита от спама

Надежные антиспам-технологии

- Выявление нежелательных писем по атрибутам отправителя, IP-адресам, размеру сообщения и заголовкам
- Интеллектуальные методы, такие как уникальные сигнатуры изображений, и анализ содержимого и вложений

Анτισпам-карантин

Подозрительные сообщения могут помещаться на карантин и затем проверяться повторно по обновленным данным об угрозах. Пользователи могут настраивать параметры карантина и длительность хранения писем.

Репутация IP-адресов и доменов

Фильтр вредоносных URL- и IP-адресов получает обновления из глобальной облачной базы данных KSN в режиме реального времени и блокирует электронные письма, содержащие ссылки на зараженные сайты и вредоносные файлы, а также письма с адресов, ранее замеченных в рассылке спама.

Технология обновления MOEBIUS

Технология обновления антиспам-баз в режиме реального времени постоянно синхронизируется с серверами обновлений «Лаборатории Касперского», поддерживая актуальность сигнатур для обнаружения спама и обеспечивая максимальную защиту даже от новейших типов атак.

Технология обновления MOEBIUS

Moebius — технология
обновления
антиспам-баз
в режиме реального
времени



Обеспечивает более оперативную доставку критически важных обновлений приложения



Постоянно синхронизируется с серверами обновлений «Лаборатории Касперского», поддерживая актуальность сигнатур для обнаружения спама и обеспечивая максимальную защиту даже от новейших типов атак

Антиспам-карантин с использованием машинного обучения



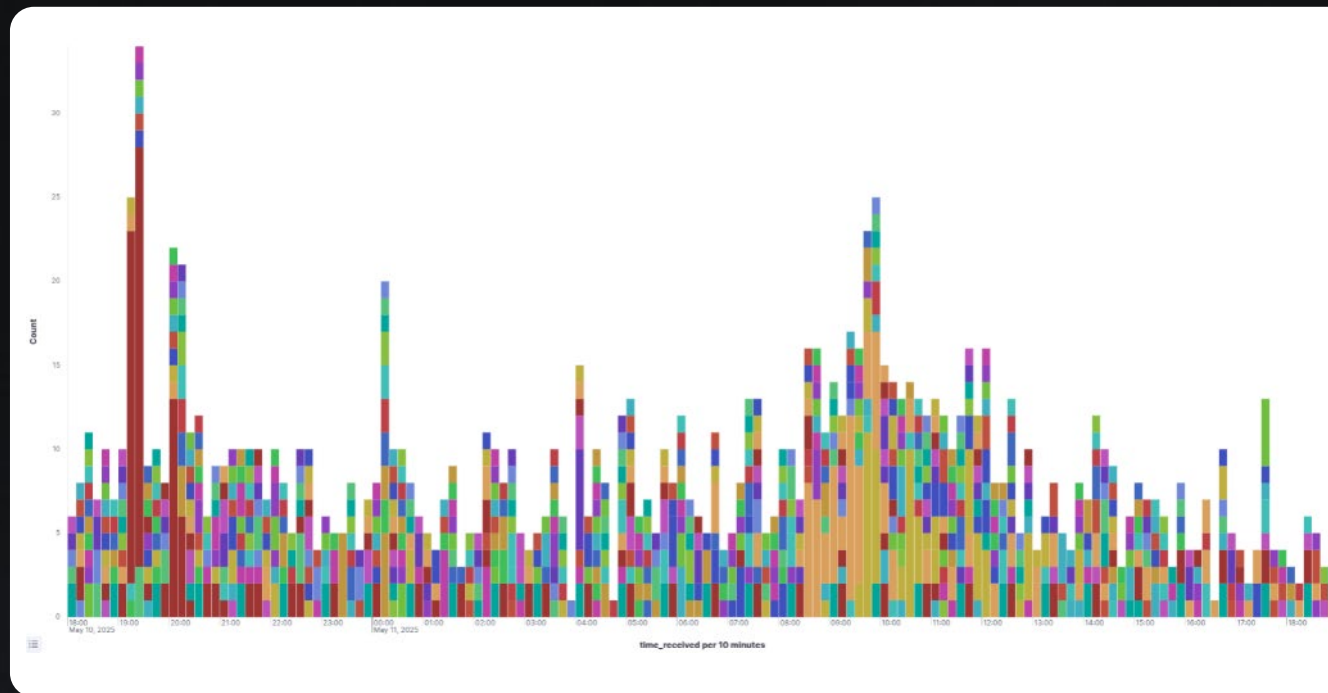
Потенциально нежелательные сообщения могут временно помещаться в карантин с последующей повторной проверкой на основе актуализированных баз данных об угрозах



Технология классификации сообщений использует нейросети для анализа MIME-заголовков и повышения точности обнаружения спама



Настройка критериев попадания сообщений в карантин, сроков их хранения и других параметров доступна через веб-интерфейс



Визуализация сообщений, помещенных в карантин, с цветовой маркировкой по доменам отправителей

Удобное управление карантинном без портала

- Управление сообщениями в карантине в один клик **прямо из дайджеста пользователя**
- **Не требуется заходить на портал персонального карантина** для удаления или получения сообщения

You have received **3 new messages** since the previous digest.

The most recent of them are shown in the table below:

Sender	Recipients	Subject	Date	Action
master@company.local	blablabla@gmail.com	test Mon, 16 Mar 2026 14:38:56 +0000	16/03/2026 14:38	Delete Send
master@company.local	blablabla@gmail.com	test Mon, 16 Mar 2026 14:38:55 +0000	16/03/2026 14:38	Delete Send
master@company.local	blablabla@gmail.com	test Mon, 16 Mar 2026 14:38:55 +0000	16/03/2026 14:38	Delete Send

Click on the **Delete** link to have the message removed from your Backup.

Click on the **Send** link to have the message sent to your inbox.

The table is limited to 10 lines.

[View all messages in my account](#)

This message is generated by Kaspersky Secure Mail Gateway on 16/03/2026 14:41.

To unsubscribe from Backup digest, click [here](#).

Продвинутые правила сложных и маскирующихся угроз

Доступно в KSMS Plus

Динамические правила обнаружения распознают угрозы, которые маскируются под обычные письма и могут оставаться незамеченными для базовых антиспам-движков

- Письма, созданные с помощью искусственного интеллекта
- Защита от атак с массовой регистрацией — когда злоумышленник автоматически регистрирует пользователя на сотнях веб-сайтов
- Проверка и анализ репутации, а также срока существования домена отправителя
- Выявление подозрительной активности в деловой переписке между компаниями (B2B)

Гибкая настройка: предоставление **отдельным группам пользователей** доступа к рекламным сообщениям, которые обычно блокируются для остальных сотрудников организации.

Изменить правило

Общие

Информация о правиле

Отправители и получатели

Модули проверки

AV

 Антивирус

LS

 Проверка ссылок

AP

 Анти-Фишинг

AS

 Анти-Спам

CF

 Контентная фильтрация

MA

 Проверка подлинности

KT

 Защита KATA

CD

 Обезвреживание содержимого

MF

 Фильтрация некорректных сообщений

Дополнительные параметры

Скрытая копия

Действия над заголовками

Примечание к сообщению

Анти-Спам

Статус

Вкл

Спам Предполагаемый спам Массовая рассылка Расширенные эвристики Дополнительные параметры

Расширенные эвристики

Актуальный список эвристик с пояснениями см. в [справке](#).

+ Добавить

Удалить

☐	Название эвристики	Действие	Статус
☐	B2B	Пропустить	Вкл
☐	List-linking	Отклонить	Вкл
☐	BEC-AI	Удалить сообщение	Вкл
☐	recently-registered-domain	Удалить сообщение	Вкл
☐	first-seen-domain	Пропустить	Вкл
☐	first-seen-and-recently-registered-domain	Удалить сообщение	Вкл

Модуль обнаружения писем, созданных с помощью искусственного интеллекта

Доступно в KSMS Plus

Распознает письма, написанные с помощью ИИ (языковые модели, например ChatGPT)

Специализируется на выявлении финансового мошенничества и ВЕС-атак

Не требует наличия ссылок или вложений для срабатывания

Поддерживает 8 языков, список постоянно расширяется

From: halim.ahmed@gmail.com

Subject: Urgent business

Hello,

I am Halim Ahmed from Niger Republic presently living in Accra Ghana, I have something important to discuss with you on investment in your country.

Let me have your WhatsApp number and your full name so that I can call you on WhatsApp and explain things to you in detail.

Waiting for your urgent response.

Halim Ahmed

Это письмо создано с помощью ИИ в качестве примера и было обнаружено системой

Продвинутые правила обнаружения атак: массовая регистрация

Доступно в KSMS Plus

Атаки с массовой регистрацией на веб-сайтах

Злоумышленники используют скрипт, чтобы подписать ваш почтовый адрес на сотни сайтов, в результате чего вы получаете шквал писем с подтверждением регистрации

Обычные спам-фильтры не блокируют такие письма — все они выглядят легитимными



**Переполненный
почтовый ящик**
999+ писем

Обнаружение массовой регистрации

Мгновенное распознавание и блокировка типичных писем-подтверждений регистрации

Атака останавливается — почтовый ящик остается чистым



**Чистый
почтовый ящик**

Новый или неизвестный домен

Доступно в KSMS Plus

Блокировка фишингового письма до того, как оно попадет к пользователю

- Определение репутации и возраста домена отправителя
- Злоумышленники используют новые, но формально «легитимные» почтовые домены, чтобы обойти проверки SPF, DKIM, DMARC
- Даже если все технические проверки пройдены, сам домен может быть подозрительным



Проверка архивов, защищенных паролем

Проверка архивов, защищенных паролем, во вложениях писем.
В KSMS доступны **три варианта работы**:



Решение пытается подобрать пароль к архиву, используя слова, найденные в тексте письма



Используется встроенный словарь самых популярных паролей для попытки разблокировать защищенные архивы



Пользователи самостоятельно проверяют архивы, защищенные паролем, через специальный веб-портал

Технологии продвинутой контентной фильтрации

Простой контроль информации для защиты конфиденциальных данных от утечки



Продвинутая фильтрация и блокировка писем по правилам на основе регулярных выражений и масок



Надежная фильтрация и блокировка вложений на основе настроенных правил



Шаблоны конфиденциальных документов для снижения риска утечки данных



Удобные словари для управления правилами фильтрации

Фильтрация писем возможна по следующим параметрам

- Размер сообщения
- Размер MIME-части
- Тип вложения (независимо от расширения файла)
- Имя вложения
- Заголовки
- Текст сообщения
- Тема сообщения
- Получатель
- Отправитель
- Скрытая копия
- Ключевые слова

Фильтрация вложений возможна по следующим параметрам

Размер сообщения

Имя вложения

Тип вложения

Проверка архивов, защищенных паролем, через веб-портал

Доступно в KSMS Plus

Используйте безопасный портал в интерфейсе KSMS для проверки зашифрованных архивов:

1

Выберите электронные письма, содержащие архивы, защищенные паролем

2

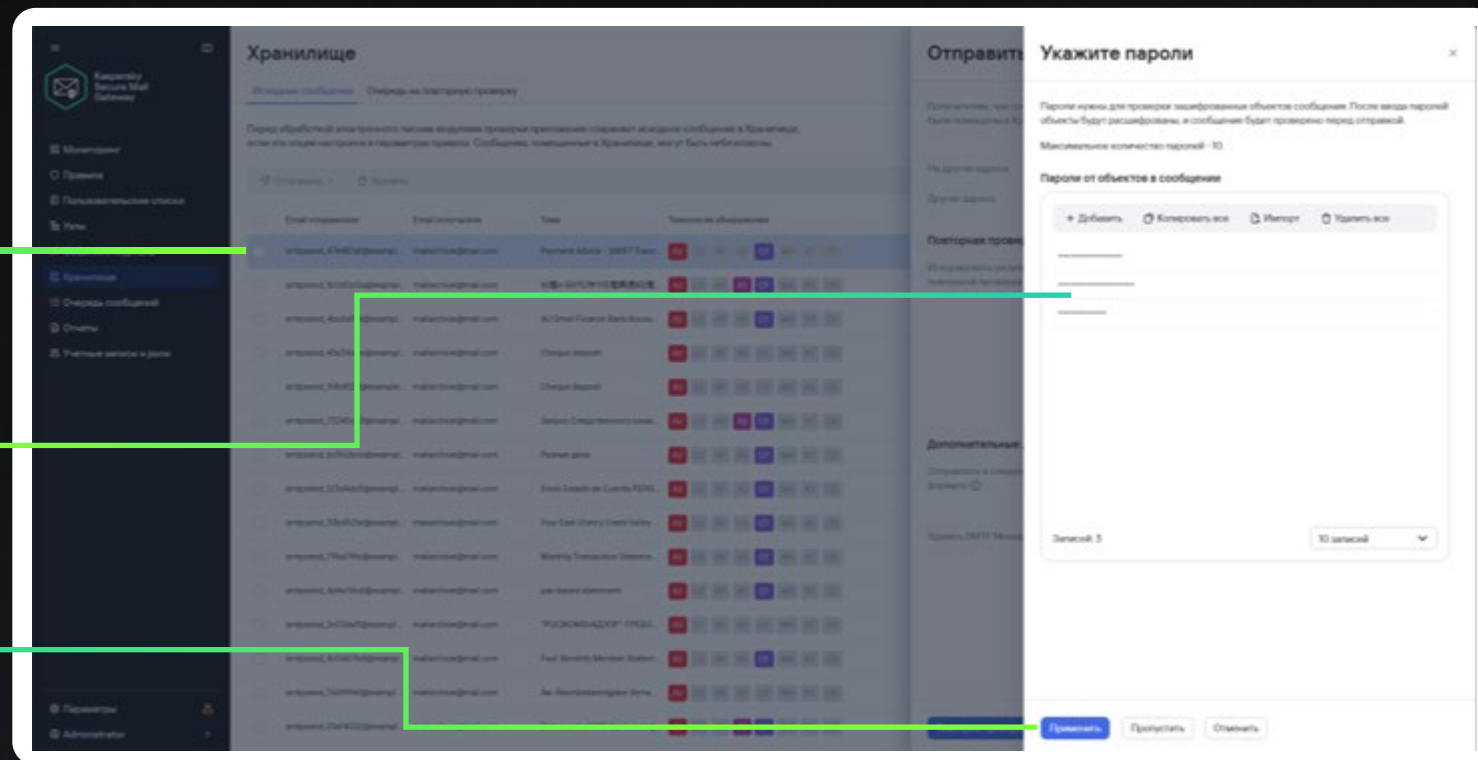
Введите пароль

3

Отправьте вложения из архивов на анализ

4

Получите исходное электронное письмо с безопасным вложением



Функция Content Disarm and Reconstruction (CDR)

Доступно в KSMS Plus



Входящие
электронные
письма
с вложениями



CDR удаляет угрозы
и восстанавливает
файлы

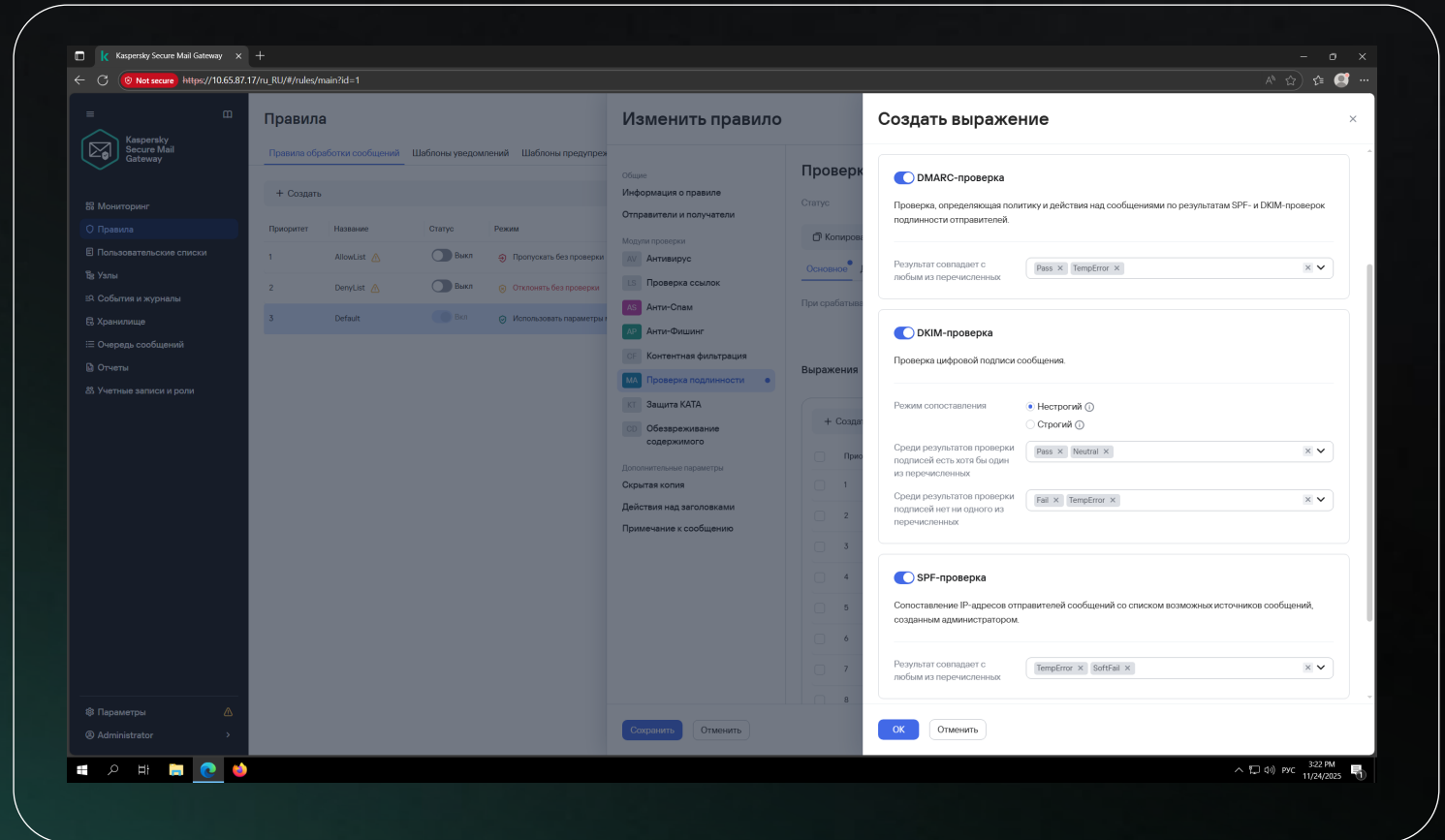


Пользователь
получает
безопасный
файл

- Мгновенное удаление скрытых угроз
- Расширение возможностей других модулей, обеспечивающих защиту на уровне шлюза

Проверка отправителя: SPF, DKIM, DMARC

- Надежные механизмы проверки отправителя: SPF, DKIM, DMARC
- Эффективная защита от спуфинга и BEC-атак — проверяйте надежность отправителя
- Тонкая настройка действий при всех возможных результатах проверок SPF, DKIM и DMARC



Проверка отправителя: сопоставление доменов отправителя



Для компаний
с развитой
экспертизой в области
аутентификации
отправителей почты:

Уникальный уровень гибкости
настройки правил на основе
результатов проверок
SPF/DKIM/DMARC



Для компаний, у которых
нет специалистов по
безопасности и опыта
в настройке
аутентификации
отправителей:

Предустановленные параметры
и действия, рекомендованные
специалистами Kaspersky на основе
лучших практик использования
технологий аутентификации
отправителей

Проверка подлинности

Статус ☒ Вкл

☐ Копировать параметры из другого правила ☒ **Использовать рекомендуемые значения**

Основное Действия при ошибке проверки Действия, если выражения не сработали

При срабатывании выражений

- ☒ Применить действие выражения с высшим приоритетом, остальные выражения игнорировать
- ☐ Применить самое строгое среди действий сработавших выражений

Создать выражение

Тип логической связи

☒ **DMARC-проверка**

Проверка, определяющая политику и действия над сообщениями по результатам SPF- и DKIM-проверок подлинности отправителей.

Результат совпадает с любым из перечисленных

☒ **DKIM-проверка**

Проверка цифровой подписи сообщения.

Режим сопоставления ☒ Нестрогий ☐ Строгий

Среди результатов проверки подписей есть хотя бы один из перечисленных

Среди результатов проверки подписей нет ни одного из перечисленных

☒ **SPF-проверка**

☒ **Сопоставление доменов отправителя**

Сопоставление адресов отправителя сообщения, указанных в SMTP-сессии (команда MAIL FROM) и в теле сообщения (MIME-заголовок From).

Результат совпадает с любым из перечисленных

Защита от фишинга

Антифишинговая система «Лаборатории Касперского» использует новейшие достижения науки о данных и алгоритмы машинного обучения для блокирования всех типов фишинговых атак.

Она задействует **более 1000 критериев**, включая анализ изображений, языковые проверки и специфические скрипты, и использует собираемые по всему миру данные о вредоносных и фишинговых URL-адресах для защиты от известных и новых фишинговых угроз.

Многоуровневая защита от угроз:

1

Распространенные
фишинговые
сценарии

2

Целевой фишинг
(включая
BEC-атаки)

3

Фишинг
с использованием
QR-кодов

4

Спуфинг

И другие сложные угрозы

Защита от фишинга с использованием QR-кодов

Проверка различных типов QR-кодов

- Черно-белые и цветные
- Под углом
- Несколько QR-кодов в одном изображении
- Размытые коды
- Коды с логотипами
- Коды в GIF- и других файлах

Анализируемые объекты

- Вложения с изображением внутри, в том числе в PDF-файлах
- Изображения, встроенные в HTML-код

Функция доступна во всех приложениях Kaspersky Security для почтовых серверов

- Kaspersky Secure Mail Gateway
- Kaspersky Security для Microsoft Office 365
- Kaspersky Security для Microsoft Exchange Servers



Пн 14.08.2023 15:18

Outlook Authenticator

Urgent Access Expiration Notice - Action Required

Кому



Your password to **Outlook Authenticator** expires today Monday, August 14, 2023,
Please do the following to keep using your mailbox without any issues and to receive incoming emails.

Scan the QR code with your phone's camera to fix this problem.



Once you've scanned the QR code, the app will guide you through the process of keeping your account..
Please ensure you follow the instructions carefully.

This email was sent to you because you indicated that you'd like to receive email notifications from microsoft. If you don't want to receive such emails in the future, please update your [email notification settings](#). Microsoft LLC
1600 Amphitheatre Parkway
Mountain View CA 94043 USA

Облачные технологии для репутационного анализа



**Kaspersky
Security Network**

Kaspersky Security Network (KSN)

Облачная глобальная база данных об угрозах, которая пополняется за счет сведений, добровольно предоставляемых более 100 млн пользователей из почти 200 стран

Интеграция с **Kaspersky Private Security Network** позволяет использовать локальные репутационные базы и глобальную аналитику угроз без передачи данных за пределы организации.

Фильтр вредоносных URL- и IP-адресов получает репутационные данные и обновления из KSN/KPSN в режиме реального времени и блокирует электронные письма, содержащие ссылки на зараженные сайты и вредоносные файлы.

Проверка ссылок



Выявляет и отслеживает:

- Вредоносные веб-сайты
- Рекламные ссылки
- Ссылки на легитимное программное обеспечение, которое может быть использовано злоумышленниками для нанесения ущерба корпоративной сети

Технология обнаружения:



Автоматически
проверяет все ссылки
в сообщениях
электронной почты

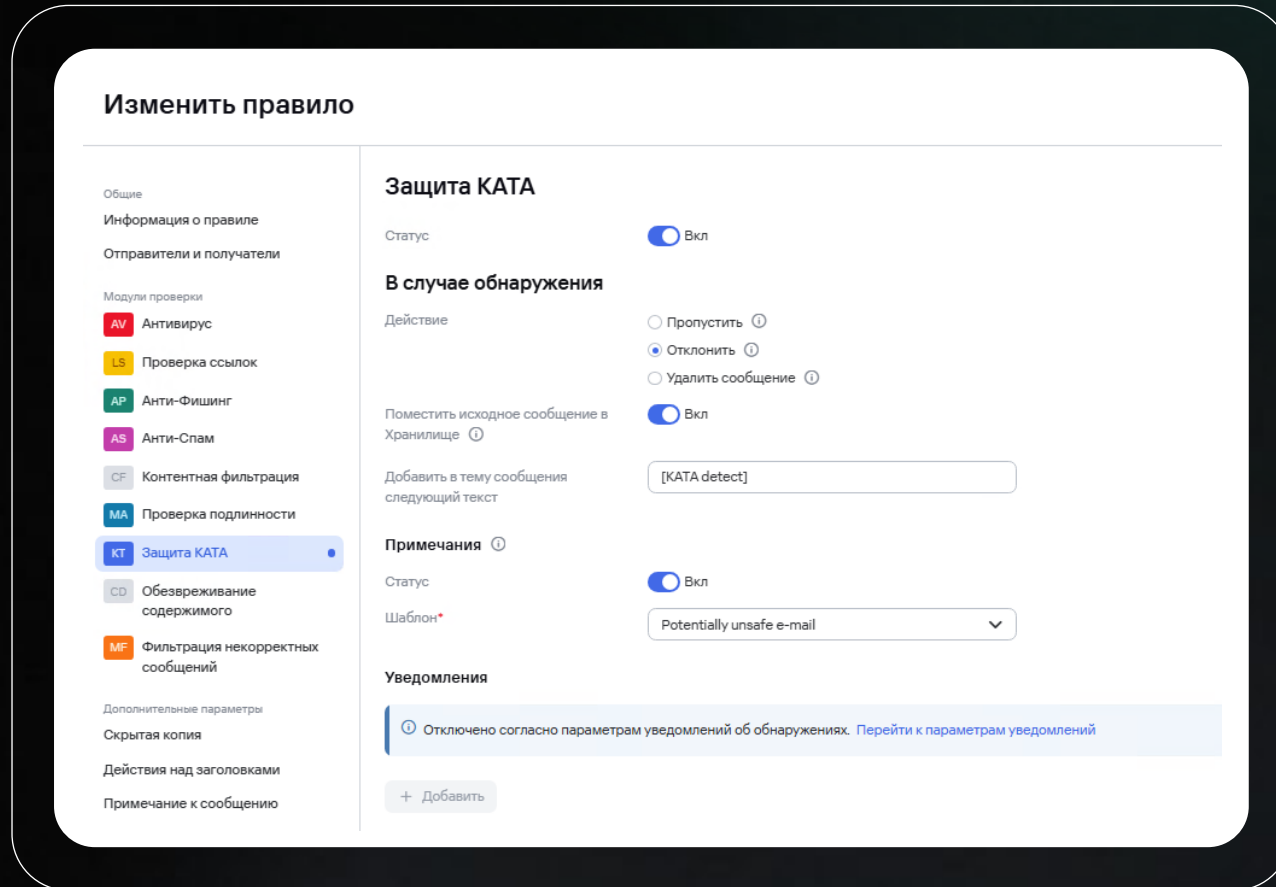


Выявляет вредоносные
и фишинговые веб-
сайты



Блокирует или помечает подозрительные и опасные
ссылки и веб-сайты до того, как они достигнут
пользователей

Динамический анализ вложений в песочнице



Удобная интеграция
с сетевой песочницей
Kaspersky Anti
Targeted Attack



Пользователи
получают
подробный отчет
по результатам
анализа



Во время проверки в песочнице запуск
вложений производится в безопасной
изолированной среде без риска для
основной инфраструктуры

Виджет «Пользователи в зоне риска». Подход к защите на основе оценки человеческого фактора

< 30% сотрудников организации получают большую часть спама и вредоносных сообщений

Сосредоточьте усилия на сотрудниках из группы риска и повысьте эффективность обучения по кибербезопасности

Выявляйте пользователей группы риска и снижайте риски, связанные с почтовыми угрозами

Топ-10 получателей вредоносных ссылок

Получатель	Сообщения
ivanov@sales.lab	7
bob@sales.lab	7
sobolev@sales.lab	5
Всего в топ-10:	19

Топ-10 получателей спама

Получатель	Сообщения
bob@sales.lab	19
sobolev@sales.lab	17
ivanov@sales.lab	12
Всего в топ-10:	48

Топ-10 получателей фишинга

Получатель	Сообщения
sobolev@sales.lab	7
bob@sales.lab	6
ivanov@sales.lab	3
Всего в топ-10:	16

Топ-10 получателей вредоносного ПО

Получатель	Сообщения
bob@sales.lab	2
ivanov@sales.lab	1
Всего в топ-10:	3

Поиск и фильтрация журналов почты в веб-интерфейсе

Все ключевые события доступны непосредственно в интерфейсе продукта, что делает администрирование и анализ быстрее и удобнее.

- Мониторинг
- Правила
- Пользовательские списки
- Узлы
- События и журналы
- Хранилище
- Очередь сообщений
- Отчеты
- Учетные записи и роли

События и журналы

События почтового трафикаСобытия приложенияСобытия аудитаЖурналы

На этой вкладке вы можете просмотреть события из системных журналов. Поиск ведется по всему текущему файлу выбранного журнала, не только по отображаемым ниже строкам. При изменении параметров поиска нажмите на кнопку Показать, чтобы увидеть результат.

Поиск

Управляющий узел

maillog

100

Показать

Найдено более 100 событий. Уточните критерии поиска

Копировать

Скачать

1 Jun 23 11:02:26 ksmg postfix/qmgr[302028]: 324B8260003: removed

2 Jun 23 11:02:26 ksmg postfix/smtp[303064]: 324B8260003: to=<bob@sales.lab>, relay=sales.lab[10.68.85.2]:25, delay=0.08, delays=0.03/0/0.04/0.01, dsn=2.0.0, status=sent (250 Queued (0.000 seconds))

3 Jun 23 11:02:26 ksmg postfix/smtpd[303045]: disconnect from unknown[10.68.85.185] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5

4 Jun 23 11:02:26 ksmg postfix/smtpd[303045]: proxy-accept: END-OF-MESSAGE: 250 2.0.0 Ok: queued as 324B8260003; from=<chr@corp-demo.local> to=<bob@sales.lab> proto=ESMTP helo=<[127.0.1.1]>

5 Jun 23 11:02:26 ksmg postfix/smtpd[303062]: disconnect from localhost[127.0.0.1] ehlo=1 xforward=1 mail=1 rcpt=1 data=1 quit=1 commands=6

6 Jun 23 11:02:26 ksmg postfix/qmgr[302028]: 324B8260003: from=<chr@corp-demo.local>, size=1926, nrcpt=1 (queue active)

7 Jun 23 11:02:26 ksmg postfix/cleanup[303063]: 324B8260003: message-id=<>

8 Jun 23 11:02:26 ksmg postfix/smtpd[303062]: 324B8260003: client=localhost[127.0.0.1], orig_client=unknown[10.68.85.185]

9 Jun 23 11:02:26 ksmg postfix/smtpd[303062]: connect from localhost[127.0.0.1]

10 Jun 23 11:02:26 ksmg klms-smtp_proxy: Message from <chr@corp-demo.local> to <bob@sales.lab> replaced by 1 new message(s)

11 Jun 23 11:02:24 ksmg postfix/smtpd[303045]: NOQUEUE: client=unknown[10.68.85.185]

12 Jun 23 11:02:24 ksmg postfix/smtpd[303045]: connect from unknown[10.68.85.185]

13 Jun 23 11:02:24 ksmg postfix/smtpd[303045]: disconnect from unknown[10.68.85.185] ehlo=1 mail=1 rcpt=1 data=1 iset=1 quit=1 commands=5/6

14 Jun 23 11:02:24 ksmg postfix/smtpd[303045]: proxy-reject: END-OF-MESSAGE: 550 5.7.1 This message is blocked due to security reason; from=<news@mx-sender.demo> to=<bob@sales.lab> proto=ESMTP helo=<[127.0.1.1]>

15 Jun 23 11:02:24 ksmg klms-smtp_proxy: Message from <news@mx-sender.demo> to <bob@sales.lab> rejected

16 Jun 23 11:02:21 ksmg postfix/smtpd[303045]: NOQUEUE: client=unknown[10.68.85.185]

17 Jun 23 11:02:21 ksmg postfix/smtpd[303045]: connect from unknown[10.68.85.185]

18 Jun 23 11:02:21 ksmg postfix/qmgr[302028]: A12B8260003: removed

19 Jun 23 11:02:21 ksmg postfix/smtp[303064]: A12B8260003: to=<bob@sales.lab>, relay=sales.lab[10.68.85.2]:25, delay=0.08, delays=0.02/0/0.02/0.05, dsn=2.0.0, status=sent (250 Queued (0.000 seconds))

20 Jun 23 11:02:21 ksmg postfix/smtpd[303045]: disconnect from unknown[10.68.85.185] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5

21 Jun 23 11:02:21 ksmg postfix/smtpd[303045]: proxy-accept: END-OF-MESSAGE: 250 2.0.0 Ok: queued as A12B8260003; from=<billing@partner-lab.test> to=<bob@sales.lab> proto=ESMTP helo=<[127.0.1.1]>

22 Jun 23 11:02:21 ksmg postfix/smtpd[303062]: disconnect from localhost[127.0.0.1] ehlo=1 xforward=1 mail=1 rcpt=1 data=1 quit=1 commands=6

23 Jun 23 11:02:21 ksmg postfix/qmgr[302028]: A12B8260003: from=<billing@partner-lab.test>, size=2473, nrcpt=1 (queue active)

24 Jun 23 11:02:21 ksmg postfix/cleanup[303063]: A12B8260003: message-id=<>

25 Jun 23 11:02:21 ksmg postfix/smtpd[303062]: A12B8260003: client=localhost[127.0.0.1], orig_client=unknown[10.68.85.185]

Получено 23.06.2026 16:26:55

Балансировка трафика между несколькими IP-адресами

- **Балансировка нагрузки** между несколькими IP-адресами непосредственно через веб-интерфейс KSMG
- **Более надежная архитектура**, поскольку не требует:



балансировщика
нагрузки



DNS-сервера

Изменить домен

Общие

DKIM-подписи

Тип записи

Домен

Имя записи

email.net

Локальный домен

☒ Вкл

Режим TLS-безопасности для исходящих сообщений

☒ Использовать режим
[Проверить возможность TLS-шифрования](#)
☐ Изменить режим TLS-безопасности для этого домена

Не использовать TLS-шифрование

Подробнее о настройке режима TLS-безопасности см. в [справке](#).

Маршрутизация

☒ Вкл

Адрес назначения сообщений

☐ Поиск MX-записей DNS для указанного домена назначения
☒ Пользовательские почтовые серверы

Протокол

SMTP

Порт

25

Пользовательские почтовые серверы

+ Добавить

Удалить

☐	Приоритет	Формат	Адрес назначения
☐	1	IPv4	10.0.0.2
☐	1	IPv4	10.0.0.3
☐	2	IPv4	10.0.0.50

Сохранить

Отменить

Удалить

Интеграция

03



- 01 Обзор продукта
- 02 Ключевые технологии
- 03 Интеграция
- 04 Лицензирование
- 05 Преимущества
«Лаборатории Касперского»

Возможности интеграции



Kaspersky Anti Targeted Attack

Интеграция с песочницей в Kaspersky Anti Targeted Attack для динамического анализа объектов и ссылок в изолированной среде



Kaspersky Security Network

Интеграция с глобальной репутационной базой для получения актуальных данных об угрозах в режиме реального времени



Kaspersky Unified Monitoring and Analysis Platform

Интеграция с SIEM для расширенного экспорта событий и централизованного управления



Kaspersky Security Center

Интеграция с консолью управления продуктами для управления лицензиями и распространения обновлений безопасности



Kaspersky Symphony XDR

Интеграция с XDR-решением для обмена результатами анализа и их использования для создания правил корреляции и сценариев реагирования на инциденты безопасности



И другие
решения

Основные преимущества Kaspersky Security для почтовых серверов



Ведущая аналитика угроз

Эффективное детектирование атак благодаря ведущей системе threat intelligence и глобальным данным о киберугрозах, которыми KSMS обогащается в режиме реального времени.



Одно решение для любой почтовой инфраструктуры

Широкий выбор сценариев внедрения в рамках одной лицензии — от развертывания безопасного шлюза электронной почты до интеграции локальных и облачных решений для защиты электронной почты через API — в инфраструктурах на базе Windows и Linux.

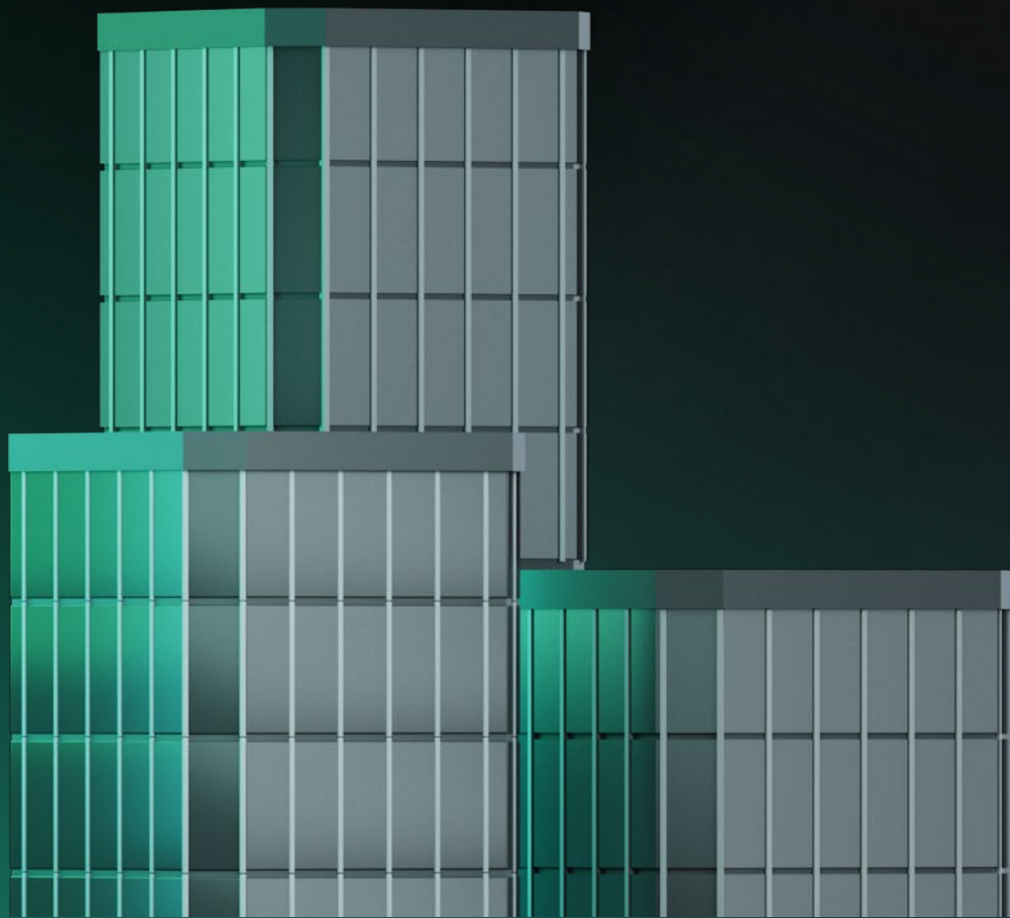


Эффективная защита от угроз

Комплекс проверенных запатентованных технологий для многоуровневой защиты электронной почты с использованием алгоритмов машинного обучения для противодействия любым видам фишинговых атак, спама, BEC-атак и другим угрозам.

Лицензирование

04



- 01 Обзор продукта
- 02 Ключевые технологии
- 03 Интеграция
- 04 **Лицензирование**
- 05 Преимущества
«Лаборатории Касперского»

Лицензирование: KSMS и KSMS Plus

Ключевые ВОЗМОЖНОСТИ	KSMS	KSMS Plus (NEW)
Антивирус, антиспам, антифишинг	•	•
Проверка подлинности отправителя (SPF, DKIM, DMARC, сопоставление домена отправителя)	•	•
Интеграция с песочницей KATA Sandbox, с глобальной репутационной базой Kaspersky Security Network (KSN / KPSN)	•	•
Фильтрация контента	•	•
Проверка зашифрованных архивов		•
Проверка документов, защищенных паролем		•
Динамические правила обнаружения		•
Content Disarm and Reconstruction (CDR)		•



KSMS Plus —
новая лицензия
с расширенными
ВОЗМОЖНОСТЯМИ
для защиты почты.

Преимущества «Лаборатории Касперского»

05



- 01 Обзор продукта
- 02 Ключевые технологии
- 03 Интеграция
- 04 Лицензирование
- 05 Преимущества
«Лаборатории Касперского»

В чем преимущество решений «Лаборатории Касперского»



Инновационные
решения на базе
экспертных знаний
и искусственного
интеллекта



Международное
присутствие
и уникальные
источники данных



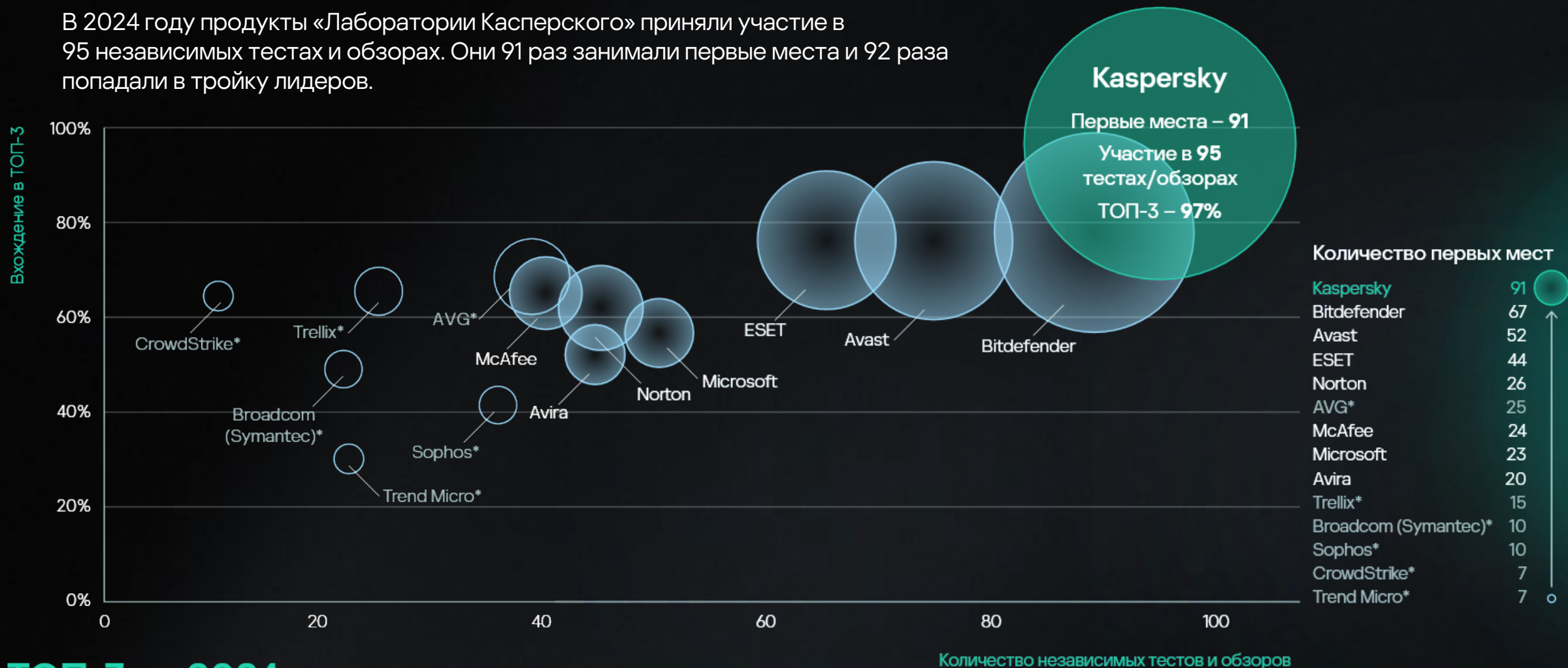
Признание
независимых
экспертов
и прозрачность



Активный вклад
в развитие
индустрии

Больше тестов. Больше наград. Больше защиты*

В 2024 году продукты «Лаборатории Касперского» приняли участие в 95 независимых тестах и обзорах. Они 91 раз занимали первые места и 92 раза попадали в тройку лидеров.



ТОП-3 за 2024 г.



MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION

[*kaspersky.com/top3](https://kaspersky.com/top3)

* Примечания.

- По результатам независимых тестов корпоративных, потребительских и мобильных продуктов за 2024 год.
- В обзор вошли тесты, проведенные следующими независимыми лабораториями: AV-Comparatives, AV-TEST, MRG Effitas, SE Labs, Testing Ground Labs, Virus Bulletin.
- Тестировались все доступные технологии защиты против известных, неизвестных и комплексных угроз.
- Диаметр круга соответствует числу занятых первых мест.
- Производители с пометкой «*» участвовали менее чем в 35% от общего числа тестов и были добавлены в таблицу для общего контекста.



Kaspersky
Security для
почтовых серверов

Запросить
пробную
версию



Подробнее



Подробнее
о продукте



Подробнее



Спасибо!

2026



www.kaspersky.ru

© 2026 АО «Лаборатория Касперского»
Зарегистрированные товарные знаки и знаки обслуживания
являются собственностью их правообладателей.

#kaspersky
#активируйбудущее