Kaspersky Security

для почтовых серверов и для интернет-шлюзов

Ландшафт угроз

Доступ в Интернет и электронная почта являются основными векторами проникновения угроз.

Электронная почта – самый распространенный способ компрометации пользователей.

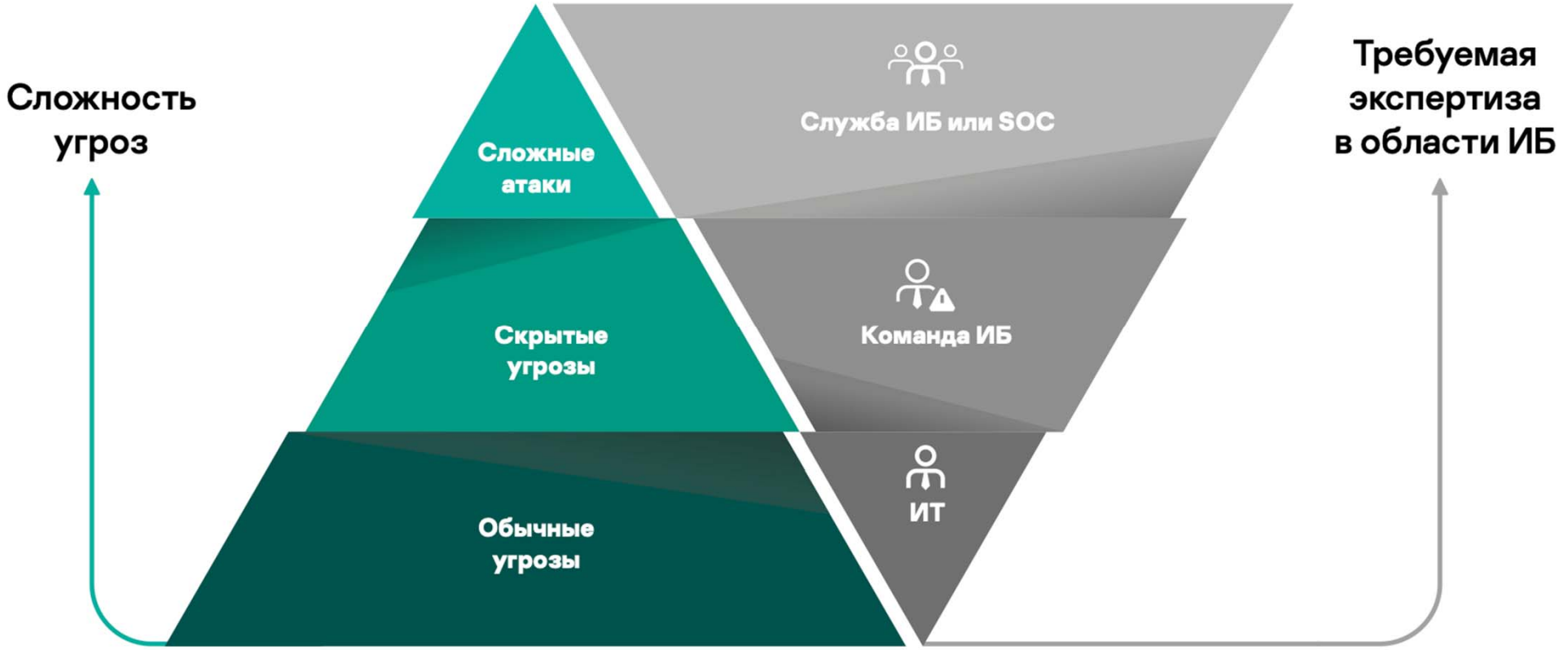
Примеры включают ответ на фишинговое электронное письмо, переход по небезопасной ссылке и запуск вложенных вредоносных документов.

37% инцидентов информационной безопасности крупного бизнеса (Enterprise) в 2021 году связано с фишингом и атаками с использованием социальной инженерии *

Средний размер транзакции от компрометации бизнес-переписки (Business Email Compromise - BEC) вырос с $30,000 до $60,000 с 2021 по 2022 год **

Многие почтовые клиенты блокируют запуск исполняемых вложений, в то время как количество вложенных вредоносных офисных документом выросло почти в два раза с 2021 по 2022 год ***

Виды угроз и уровень экспертизы



ИБ-задачи при защите корпоративной сети

35% компаний крупного бизнеса (Enterprise) не уверены в своей способности предотвратить следующий большой инцидент

40% компаний малого и среднего бизнеса (SMB) не имеют достаточно информации чтобы своевременно обнаруживать и быстро останавливать угрозы

Ограничены в бюджете, персонале и времени

Подход к обеспечению кибербезопасности

Уровень	ИБ-задачи	Исполнитель	Продукты
1-й обычные угроза	Защита конечных точек Защита почты и web-доступа Защита данных Поддержка	ИТ-специалисты Kaspersky Security Foundations	Kaspersky Security (для бизнеса, для виртуальных и облачных сред) Kaspersky Security для почтовых серверов и интернет-шлюзов Kaspersky Security для систем хранения MSA и профессиональные сервисы
2-й скрытые угрозы	Обнаружение и реагирование Расширенная защита Обогащение данными Киберграмотность	Команда ИБ, HR Kaspersky Optimum Security	Kaspersky EDR Оптимальный Kaspersky Sandbox Kaspersky Threat Intelligence Portal Kaspersky Security Awareness
3-й сложные атаки	Повышение экспертизы Аналитика угроз Расширенное обнаружение и реагирование Анализ защищенности Реагирование на угрозы	Служба ИБ или SOC Kaspersky Expert Security	Kaspersky Cybersecurity Training Kaspersky Threat Intelligence Kaspersky Endpoint Detection and Response, KUMA, KATA Kaspersky Security Assessment Kaspersky Security Incident Response

Kaspersky Security
для почтовых серверов

Kaspersky Security для почтовых серверов

Kaspersky Security для почтовых серверов

- Предотвращает угрозы, распространяемые по электронной почте, не позволяя вирусам, шифровальщикам, фишинговым письмам и спаму достигнуть рабочего места.
- Решение показывает высокий уровень обнаружения угроз и низкое количество ложных срабатываний.
- Позволяет эффективно противостоять изощренным атакам по электронной почте.

Это решение идеально подойдет вам ,чтобы

- Усилить свою защиту как против массовых ,так и против целевых атак ,в которых электронная почта используется для доставки вредоносного ПО .
- Реализовать подходящие сценарии защиты электронной почты для различных платформ и схем развертывания .

Преимущества для бизнеса

- Уменьшение ущерба, финансовых и репутационных потерь от атак с использованием фишинга и социальной инженерии.
- Повышение производительности труда благодаря блокированию спама, отвлекающего сотрудников.
- Снижение нагрузки на ИТ- и ИБ- специалистов, сокращение операционных затрат благодаря простоте внедрения, администрирования и автоматическому блокированию угроз, распространяемым по электронной почте.

Практическое применение

- Защита инфраструктуры усиливается на уровне почтового сервера.
- Предоставление имеющимся системам обнаружения сложных угроз дополнительные данные и возможности.

Kaspersky Security для почтовых серверов

способы развертывания

Kaspersky Secure Mail Gateway
Шлюз безопасности электронной почты

- Полностью интегрированное решение, объединяющее систему электронной почты и средства её защиты.
- Виртуальное устройство для VMware ESXi и Microsoft Hyper-V (ISO образ).

Kaspersky Security для Linux Mail Server

- Интеграция с почтовыми серверами Postfix, Sendmail, Exim и qmail на базе дистрибутивов Linux: CentOS, Red Hat, SUSE, Ubuntu, Debian и ОС FreeBSD.
- TXZ, TXZ, DEB, и RPM пакеты.

Kaspersky Security для Microsoft Exchange Servers

- Устанавливается непосредственно на серверы Microsoft Exchange с ролями Mailbox или Edge Transport.
- Перехватывает и осуществляет проверку почтовых сообщений.

Kaspersky Security для Microsoft Office 365

- Комплексная защита служб Microsoft Office 365 с использованием API.
- Защита электронной почты Exchange Online и облачного хранилища OneDrive, SharePoint Online, включая файлы в Teams.

Kaspersky Security для почтовых серверов

ключевые возможности

Защита от спама и контентная фильтрация

- Антиспам ядро с использованием машинного обучения.
- Обнаружение подмены символов в почтовых и URL-адресах (юникод-спуфинг).
- Централизованный анти-спам карантин.
- Данные о репутации из Kaspersky Security Network.
- Обнаружение массовых рассылок.
- Сканирование ссылок и тегирование сообщений по категориям Malicious | Adware | Legitimate.
- Контентная фильтрация вложений (имя, тип, размер).
- Персональные списки разрешенных / запрещенных адресатов.

Защита от фишинга

- Использует анализ нейронной сети.
- Использует более 1000 критериев, включая анализ изображений, языковые проверки и скрипты, данные о URL и IP-адресах.

Многоуровневая защита от вредоносного ПО

- Антивирус Касперского для почтовых серверов.
- Глобальная аналитика угроз Kaspersky Security Network (KSN).
- Эмуляция и поведенческий анализ в песочнице для защиты от целевых, APT-угроз и атак нулевого дня.
- Репутационный фильтр вредоносных URL и IP-адресов.
- Обнаружение вредоносных макросов в документах Microsoft Office.
- Проверка архивов.

Защита от компрометации бизнес-переписки или Business Email Compromise (BEC) атак

- Основана на машинном обучении.
- Обнаруживает атаки с использованием похожих доменов, подмену адреса отправителя.
- Механизмы аутентификации SPF/DKIM/DMARC.

Kaspersky Security для почтовых серверов

ключевые возможности

Управление

- Централизованное управление с использованием веб-интерфейса.
- Широкий набор правил для управления почтовым трафиком и функциями безопасности.
- Ролевое управление и аутентификация пользователей с использованием Active Directory, Kerberos и NTLM Single Sign-On (SSO).

Мониторинг и гибкая система отчетности

- Информационная панель (Dashboard) со сведениями о статусе безопасности и обнаруженных угрозах.
- Отчеты в формате PDF.
- Система уведомлений SMTP и SNMP.

Интеграция

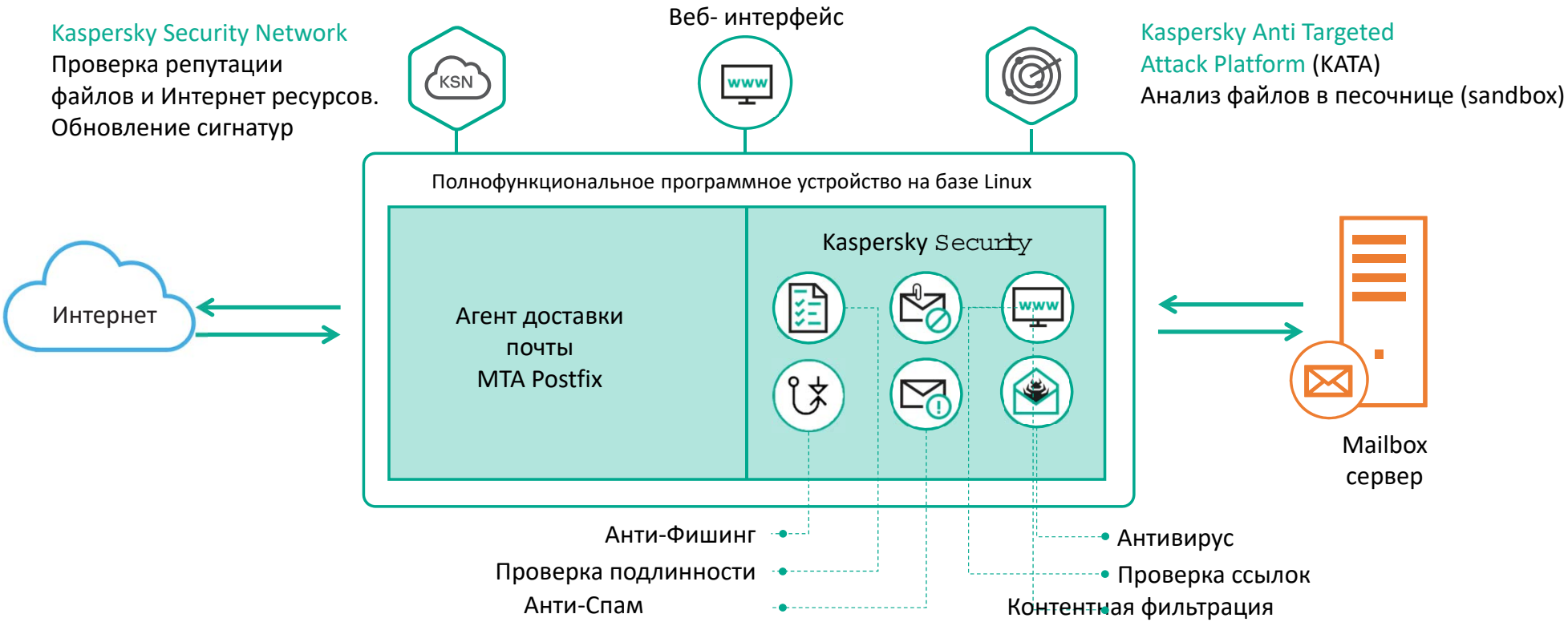
- Kaspersky Anti Targeted Attack Platform (KATA) sandbox для защиты от целевых, APT- угроз и атак нулевого дня.
- Kaspersky Private Security Network (KPSN) для организаций, предъявляющих высокие требования к конфиденциальности.
- Поддержка syslog в формате CEF для отправки событий в SIEM решения, например, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Масштабируемая архитектура

- Поддержка кластеризации для масштабирования и отказоустойчивости.
- Балансировка нагрузки с использованием MX записей или балансировщиков нагрузки, например HAProxy.

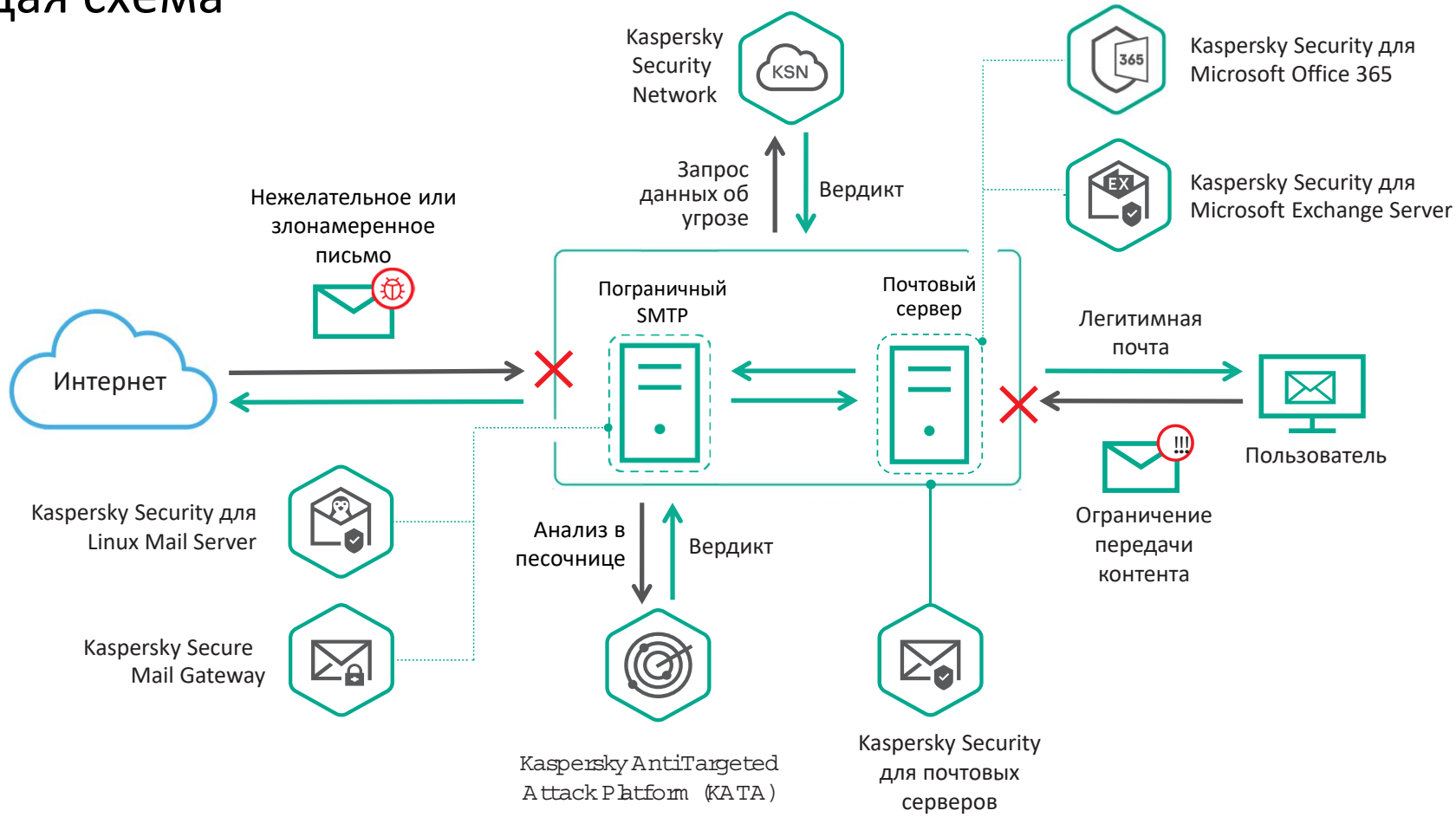
Kaspersky Secure Mail Gateway (KSMG)

архитектура



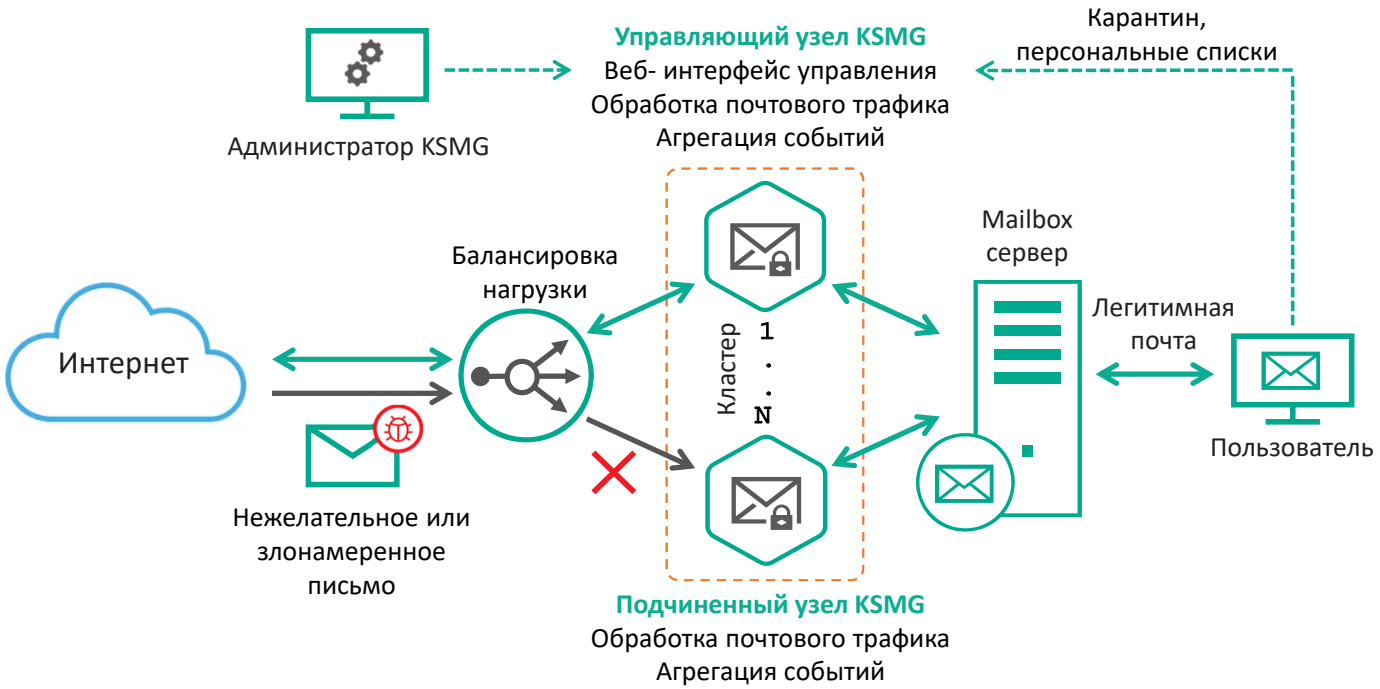
Kaspersky Security для почтовых серверов

общая схема



Kaspersky Secure Mail Gateway (KSMG)

Кластеризация: масштабирование и отказоустойчивость



Кластер - это группа серверов KSMG, объединенных для задач балансировки нагрузки и отказоустойчивости.

Управляющий узел выполняет синхронизацию конфигурации с подчиненными узлами; предоставляет централизованное управление через веб- интерфейс, централизованную отчетность, централизованный доступ к анти-спам карантину и управление персональными списками разрешенных и запрещенных адресатов.

Балансировка нагрузки может выполняться с использованием MX записей или с помощью отдельного балансировщика нагрузки, например, HAProxy.

Kaspersky Security для почтовых серверов

защита всех почтовых доменов компании

Один узел или кластер Kaspersky Security для почтовых серверов может использоваться для защиты всех почтовых доменов компании.

Маршрутизация электронной почты выполняется с использованием MX записей или транспортной таблицы.

Kaspersky Security для почтовых серверов

преимущества

Предотвращение ущерба от инцидентов нформационной безопасности

- Эффективная защита корпоративной почты от вредоносного контента, программ-вымогателей, спама, фишинга и специализированных Business Email Compromise (BEC) атак. Обнаруживает и перехватывает атаки в самом начале цепочки поражения.
- В 2021 году продукты «Лаборатории Касперского» приняли участие в 75 независимых тестах и обзорах, заняли первое место в 57 случаях и 63 раза вошли в ТОП-3.

Повышение производительности труда пользователей

- Блокируя больше спама, решение помогает сотрудникам не отвлекаться от работы.
- Ложные срабатывания минимальны, безопасные сообщения крайне редко попадают в спам.
- Независимые тесты постоянно подтверждают высокое качество наших технологий фильтрации спама.

Сокращение расходов и снижение нагрузки на ИТ- и ИБ- специалистов

- «Лаборатория Касперского» предлагает полностью интегрированный продукт, объединяющий в себе почтовый шлюз и средства защиты электронной почты, который не требует подбора совместимых решений.
- Снижение нагрузки на ИТ- и ИБ- специалистов, и сокращение операционных затрат благодаря простоте внедрения, администрирования и автоматическому блокированию почтовых угроз.

Kaspersky Security для интернет-шлюзов

Kaspersky Security для интернет-шлюзов

Kaspersky Security для интернет-шлюзов

- Обеспечивает надежную защиту от множества веб-угроз, включая вредоносное ПО, шифровальщики, криптомайнеры, онлайн-фишинг и вредоносные веб-ресурсы.
- Позволяет контролировать доступ к Интернет, ограничивая доступ к определенным веб-ресурсам в соответствии с корпоративной политикой.
- Включает такие URL –категории, как Защита детей (139-ФЗ, 436-ФЗ), Федеральный список экстремистских материалов (114-ФЗ) и Единый реестр Роскомнадзора.

Это решение идеально подойдет вам, чтобы

- Защитить инфраструктуру и сотрудников от веб-угроз.
- Ограничить доступ к ресурсам, заблокированным законодательством Российской Федерации.
- Реализовать подходящие сценарии защищенного доступа к сети Интернет с использованием различных платформ и схем развертывания.

Преимущества для бизнеса

- Уменьшение ущерба, финансовых и репутационных потерь от интернет-угроз.
- Повышение производительности труда сотрудников благодаря контролю доступа к веб- ресурсам.
- Снижение нагрузки на ИТ- и ИБ- специалистов, и сокращение операционных затрат благодаря простоте внедрения, администрирования и автоматическому блокированию веб-угроз.

Практическое применение

- Усиление защиты рабочих мест на уровне интернет-шлюза.
- Предотвращение заражения корпоративной сети, утечки ценных данных и использования Интернет в нерабочих целях.
- Предоставление имеющимся системам обнаружения сложных угроз дополнительные данные и возможности.

Kaspersky Security для интернет шлюзов

Способы развертывания

Kaspersky Web Traffic Security (KWTS) —корпоративное решение для защиты HTTP-, HTTPS- и FTP- трафика, проходящего через прокси-сервер.

KWTS виртуальный шлюз:

- Полностью интегрированное решение, объединяющее прокси сервер и средства защиты.
- Настройка параметров прокси-сервера через веб-интерфейс.
- Виртуальное устройство для VMWare ESXi, Microsoft Hyper-V (ISO образ).

KWTS приложение:

- ICAP-сервер для сканирования объектов прокси-сервера HTTP(S) с поддержкой ICAP-протокола и служб REQMOD / RESPMOD, например, Squid.
- Пакеты RPM и DEB для дистрибутивов Linux: RHEL, CentOS, Debian, Ubuntu и SUSE.

Kaspersky Security для интернет-шлюзов

Ключевые возможности

Многоуровневая защита:

- Защита от вредоносных программ, шифровальщиков с использованием алгоритмов машинного обучения и технологии эмуляции.
- Защита от целевых, APT- угроз и атак нулевого дня с использованием песочницы Kaspersky Anti Targeted Attack Platform (KATA).
- Блокирование доступа к зараженным и фишинговым сайтам.
- Проверка репутации файлов и веб-ресурсов в режиме реального времени в Kaspersky Security Network (KSN) или Kaspersky Private Security Network (KPSN).

Мониторинг и контроль доступа:

- Контентная фильтрация по URL; имени файла, MIME-типу, размеру, хеш- сумме; направлению трафика для предотвращения утечки важных документов.
- Гранулированный контроль доступа по URL- категориям.
- Мониторинг состояния работы виртуального устройства / приложения KWTS, обрабатываемого веб- трафика пользователей и обнаруженных угроз, отчеты в формате PDF.

Управление и интеграция:

- Широкий набор правил для управления веб-трафиком и функциями безопасности.
- Интеграция с Active Directory, ролевое управление, аутентификация пользователей, Kerberos и NTLM Single Sign-On (SSO).
- Рабочие области для настройки индивидуальных правил обработки трафика подразделений или управляемых организаций (для поставщиков услуг).
- Поддержка syslog в формате CEF для отправки событий в SIEM решения, например, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Масштабируемая архитектура:

- Поддержка кластеризации для масштабирования и отказоустойчивости.
- Балансировка нагрузки с использованием балансировщиков нагрузки, например HAProxy.

Kaspersky Security для интернет-шлюзов

Архитектура виртуального устройства безопасности Kaspersky Web Traffic Security

1. Запрос веб-ресурса.
2. Прокси-сервер отправляет запрос на проверку в приложение Kaspersky Web Traffic Security (KWTS).
3. Если веб-ресурс разрешен, прокси-сервер направляет запрос к веб-серверу в Интернет.
4. Веб-сервер отвечает.
5. Прокси-сервер отправляет ответ веб-сервера в KWTS для сканирования содержимого в соответствии с политикой безопасности.
6. Пользователь получает запрошенный на первом этапе веб-ресурс или страницу блокировки с объяснением причины.

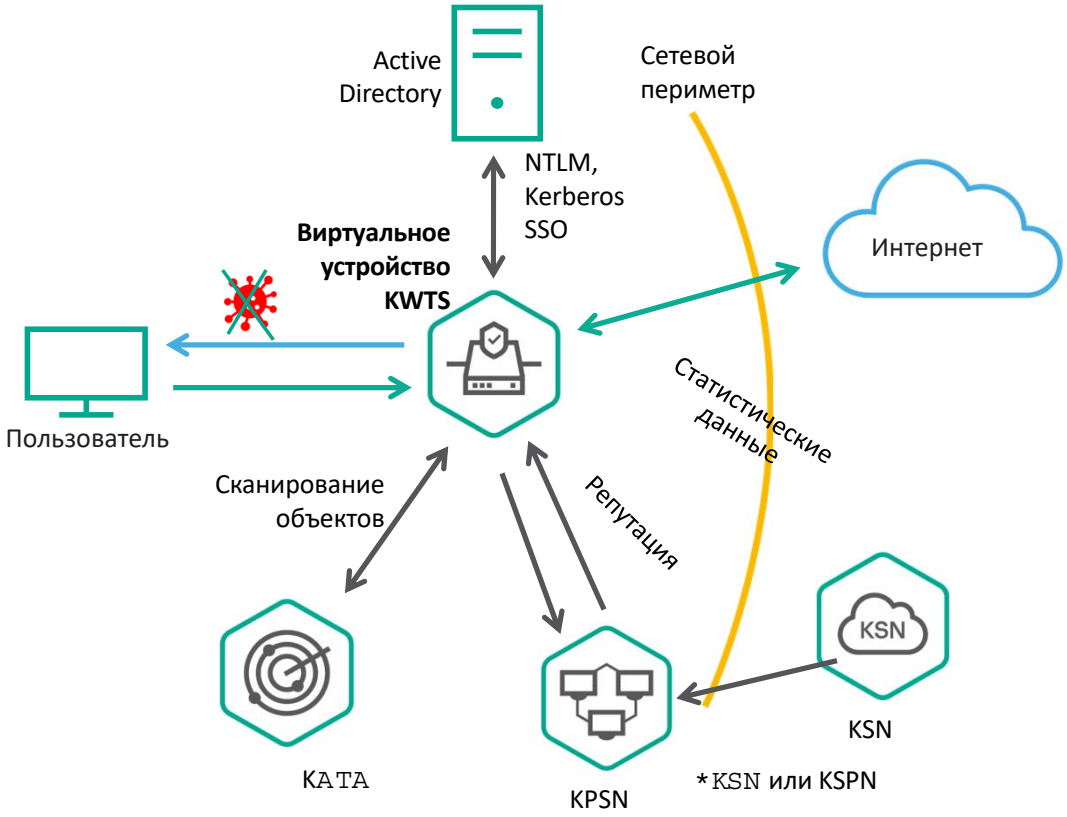
Kaspersky Security для интернет-шлюзов

Развертывание KWTS в режиме ICAP вместе с существующим сторонним прокси-сервером

Приложение Kaspersky Web Traffic Security (KWTS) может использоваться как внешнее решение для защиты веб- трафика с существующим сторонним прокси-сервером с поддержкой протокола Internet Content Adaptation Protocol (ICAP).

Kaspersky Security для интернет-шлюзов

Развертывание виртуального устройства безопасности KWTS, интеграция с KATA, KSN / KPSN



При использовании Kaspersky Security Network (KSN) определенная статистика, полученная в результате работы Kaspersky Web Traffic Security (KWTS), автоматически отправляется в «Лабораторию Касперского».

Сбор, обработка и хранение персональных данных пользователя не осуществляется.

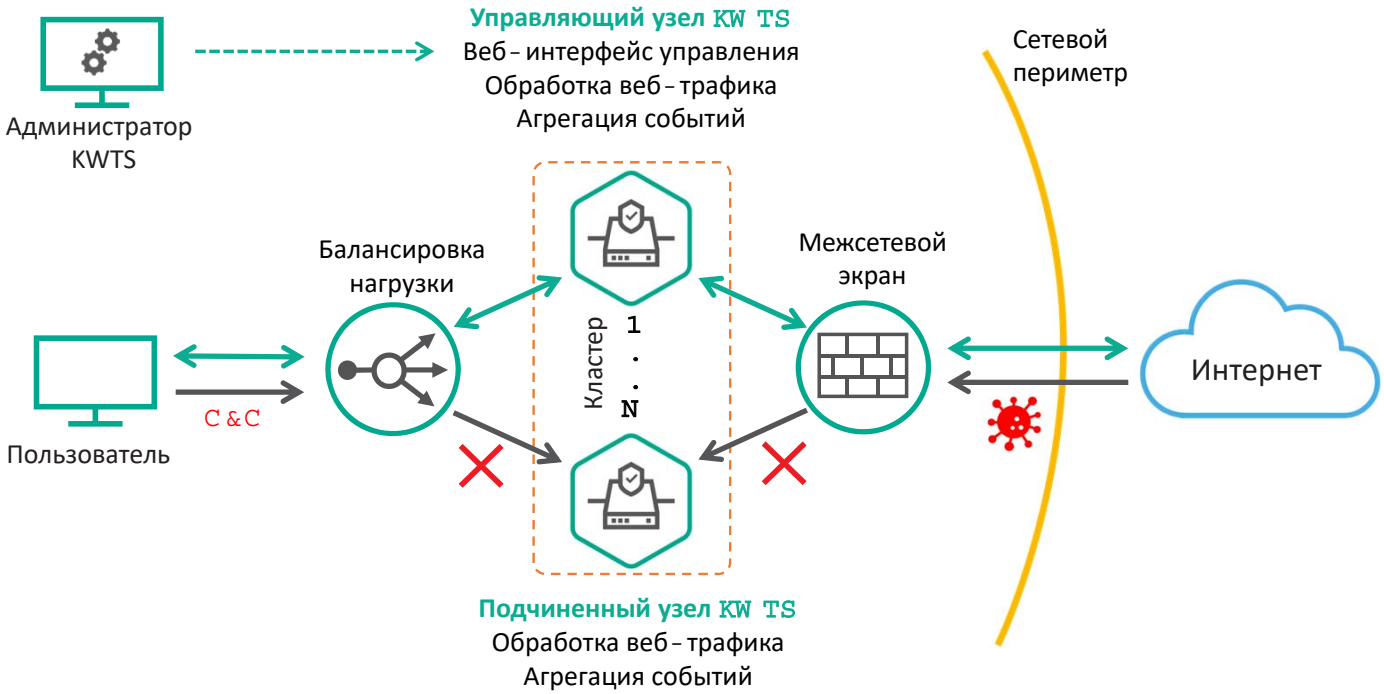
Kaspersky Private Security Network (KPSN) — это решение, позволяющее пользователям получать доступ к репутационным базам данных Kaspersky Security Network (KSN), а также к другим статистическим данным без отправки данных в KSN.

Интеграция с Kaspersky Anti Targeted Attack Platform (KATA):

- Отправка файлов, URL и IP на сервер KATA, Scan API.
- Получение обнаруженных KATA объектов с использование технологий Sandbox и YARA, Alerts API.

Kaspersky Security для интернет-шлюзов

Кластеризация: масштабирование и отказоустойчивость



Кластер — это группа виртуальных устройств Kaspersky Web Traffic Security (KWTS), объединенных для балансировки нагрузки и отказоустойчивости.

Управляющий узел выполняет синхронизацию конфигурации с подчиненными узлами; предоставляет централизованное управление через веб- интерфейс и централизованную отчетность.

Балансировка нагрузки может выполняться с использованием отдельного балансировщика нагрузки, например, HAProxy.

Kaspersky Security для интернет-шлюзов

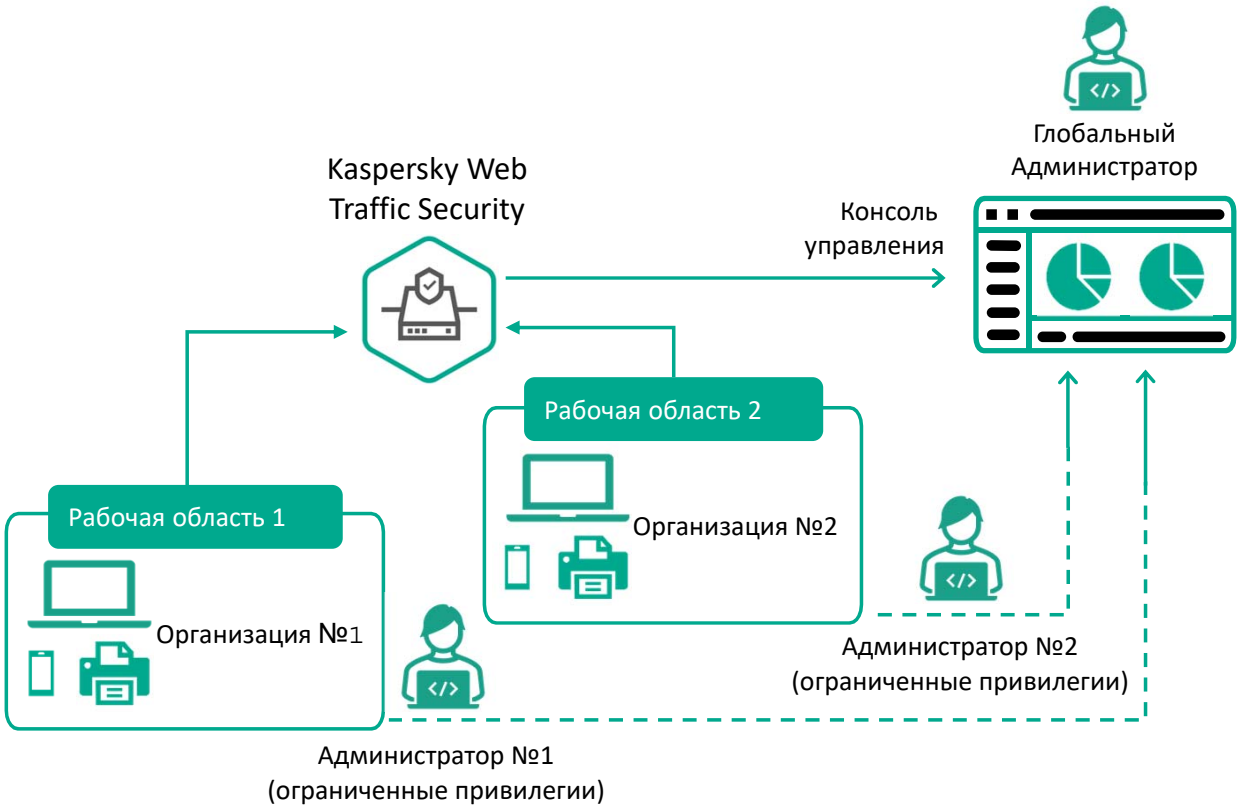
Мультиарендная (multitenancy) архитектура

Kaspersky Web Traffic Security (KWTS) поддерживает рабочие области для настройки индивидуальных правил обработки трафика подразделений или управляемых организаций (для поставщиков услуг).

Рабочая область – набор параметров и прав доступа, применимых к выделенной группе пользователей.

Возможности:

- разграничение прав доступа к каждой рабочей области между разными администраторами;
- создание правил обработки трафика, действующих только для пользователей отдельной рабочей области;
- настройка индивидуальной страницы блокировки



Kaspersky Security для Интернет шлюзов

Преимущества

Предотвращение ущерба от инцидентов информационной безопасности

- Эффективная защита от множества веб-угроз, включая вредоносное ПО, шифровальщики, криптомайнеры, онлайн-фишинг и вредоносные веб-ресурсы. Обнаруживает и перехватывает атаки в самом начале цепочки поражения.
- В 2021 году продукты «Лаборатории Касперского» приняли участие в 75 независимых тестах и обзорах, заняли первое место в 57 случаях и 63 раза вошли в ТОП-3.

Преимущества для бизнеса

- Уменьшение ущерба, финансовых и репутационных потерь от Интернет угроз.
- Повышение производительности труда сотрудников благодаря контролю доступа к веб-ресурсам.
- Ограничение доступа к ресурсам, заблокированным законодательством Российской Федерации.

Сокращение расходов и снижение нагрузки на ИТ- и ИБ- специалистов

- «Лаборатория Касперского» предлагает полностью интегрированный продукт, объединяющий в себе прокси сервер и средства защиты от веб-угроз, не требует подбора совместимых решений.
- Снижение нагрузки на ИТ- и ИБ-специалистов, и сокращение операционных затрат благодаря простоте внедрения, администрирования и автоматическому блокированию Интернет-угроз.

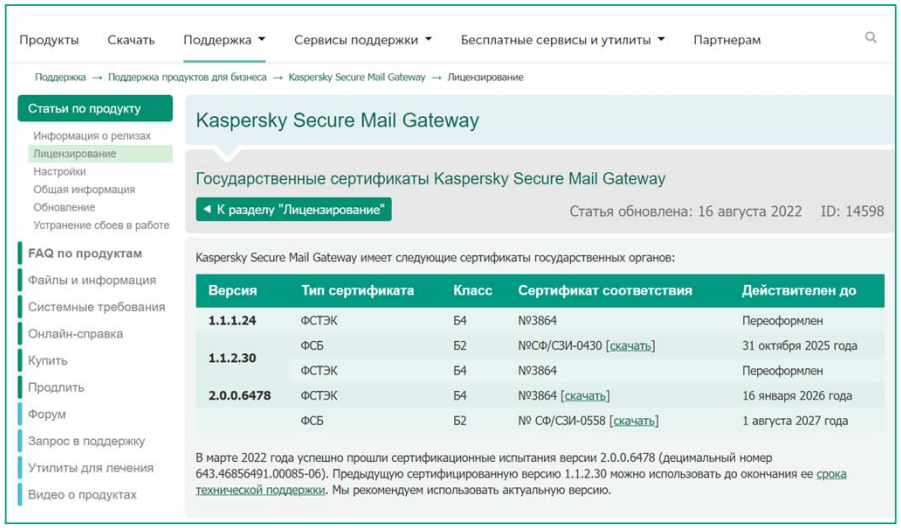
Лицензирование
Сертификаты
Пилотные проекты

Kaspersky Security для почтовых серверов

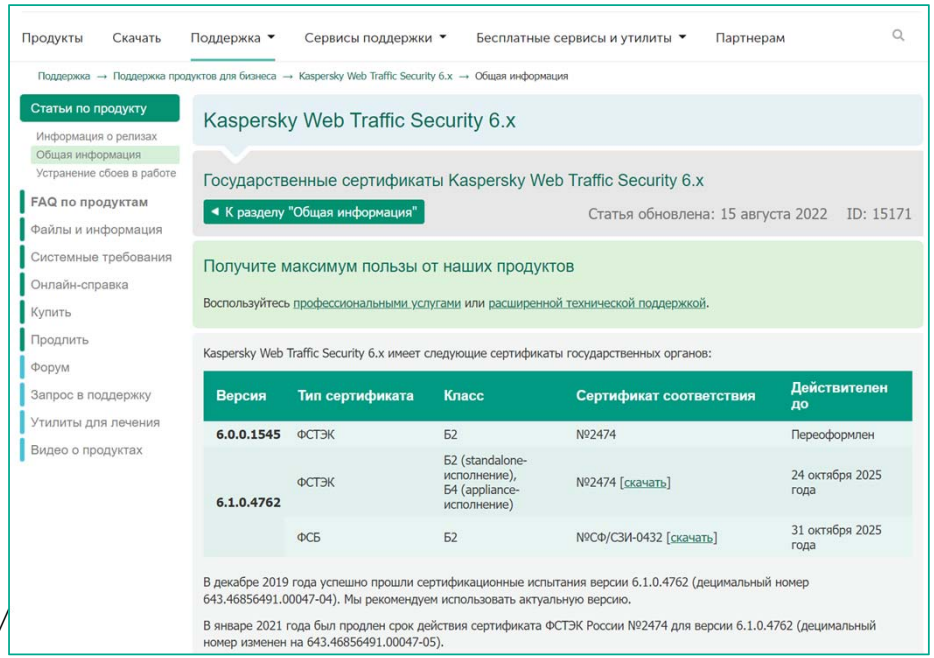
Лицензирование

Продукт	Объекты лицензии / количество
Kaspersky Security для почтовых серверов: • Виртуальный шлюз безопасности электронной почты Kaspersky Secure Mail Gateway (KSMG) • Kaspersky Security для Linux Mail Server • Kaspersky Security для Microsoft Exchange Servers	1) Лицензирование по количеству защищаемых почтовых ящиков; служебные и адреса рассылок не учитываются. 2) 150% почтовых ящиков от количества лицензий Add-on SKU для Kaspersky Endpoint Security for Business (KESB). 3) В составе Kaspersky Total Security for Business (KTSB). Доверительная модель лицензирования.
Kaspersky Security для Интернет шлюзов: • Виртуальное устройство безопасности Kaspersky Web Traffic Security (KWTS) • Kaspersky Web Traffic Security (KWTS) приложение для Linux	1) Лицензирование по количеству защищаемых Интернет пользователей. 2) 110% Интернет пользователей от количества Add-on SKU для KESB. 3) В составе Kaspersky Total Security for Business (KTSB). Доверительная модель лицензирования.
Kaspersky Security для Microsoft Office 365	Лицензирование по количеству защищаемых почтовых ящиков; адреса рассылок не учитываются.

Государственные сертификаты ФСТЭК и ФСБ

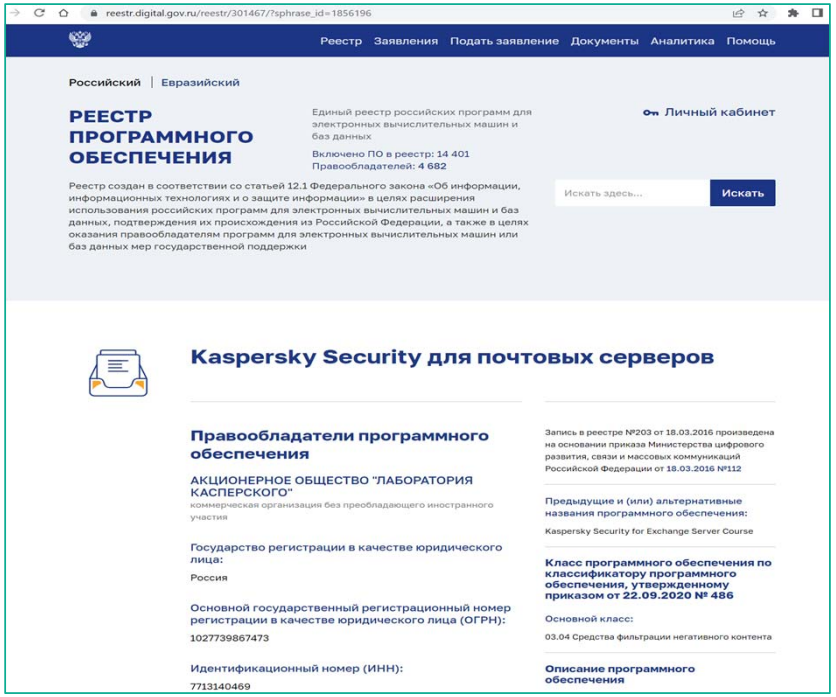


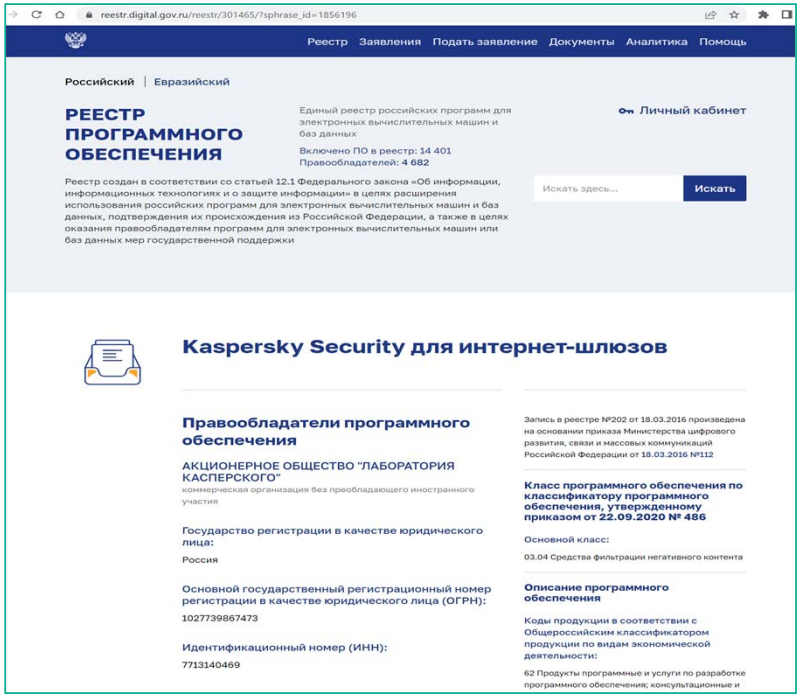
Государственные сертификаты Kaspersky Secure MailGateway:https://support.kaspersky.ru/



Государственные сертификаты Kaspersky Web Traffic Security 6.x:https://support.kaspersky.ru/15171

Решения «Лаборатории Касперского» в реестре Российского ПО





https://reestr.digital.gov.ru/reestr/301467/?sphrase_id=1856196

https://reestr.digital.gov.ru/reestr/301465/?sphrase_id=1856196

Продукты и решения «Лаборатории Касперского» — в реестре Российского ПО: https://www.kaspersky.ru/small-to-medium-business-security/registry

Для принятия решения предлагаем

Узнать! Увидеть! Попробовать!

- Развернутая презентация с привлечением технических специалистов ответит на важные вопросы
- Демонстрация решения покажет все особенности *(в тестовом или рабочем варианте)*
- Самый точный ответ на все вопросы даст пилотный проект