# Kaspersky NGFW

kaspersky активируй будущее

# Глобальная экспертиза и передовые технологии для защиты от сетевых угроз и контроля активности приложений

**95%**

Показатель обнаружения и предотвращения сетевых угроз с помощью IDPS (Detection Rate)*

**до 200 Гбит/с**

Производительность Kaspersky NGFW в режиме L4 FW + Application control**

**6 000+**

Распознаваемых приложений с помощью собственного DPI

**9 000+**

Поддерживаемых сигнатур IDPS

**до 100 000**

Поддерживаемых правил Firewall

Межсетевой экран нового поколения на основе глобальной экспертизы и передовых технологий. Продукт защищает корпоративную сеть компаний от широкого спектра киберугроз, контролирует активность приложений и сервисов, позволяет эффективно управлять трафиком и оптимизирует производительность инфраструктуры.

## Архитектура

Под капотом Kaspersky NGFW собственные технологии безопасности и архитектура, которая поддерживает многопоточную обработку трафика с минимизацией количества копирований

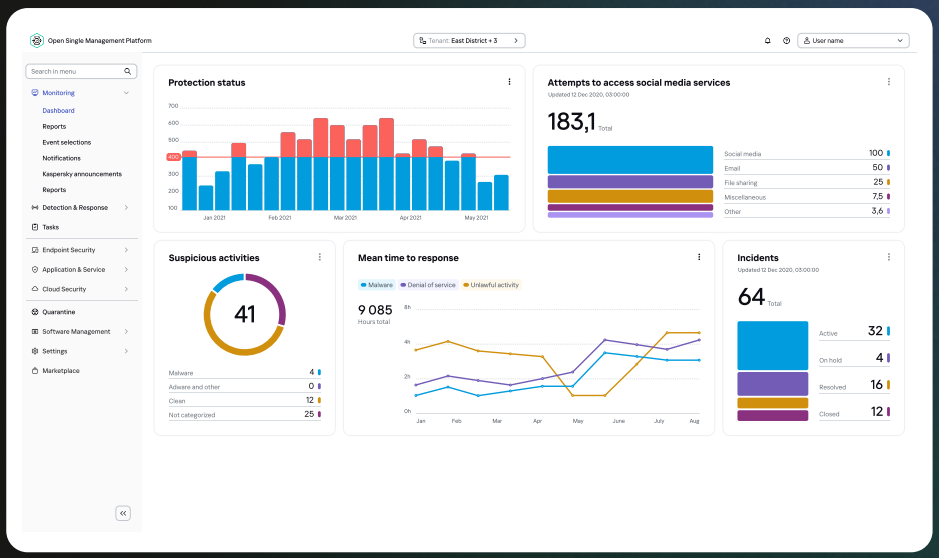
- Эффективное использование ресурсов
- Оптимизация производительности продукта
- Высокие показатели производительности на x86 процессорах
- Возможность кластеризации на базе собственного протокола Kaspersky High-availability Cluster Protocol

**Open Single Management Platform**

## Экосистемный подход и централизованное управление

Open Single Management Platform — консоль мониторинга и управления всеми развёрнутыми NGFW и другими продуктами Kaspersky упрощает рутинные операции и администрирование

- Возможность реагирования на киберугрозы с помощью Kaspersky Symphony XDR
- Полная картина кибербезопасности компании в рамках единого окна




* Тестирование проводилось с помощью IXIA BreakingPoint, Strike Level 3 и 5, 2521 попытка атак

** Тестирование проводилось с 20 000 правил Firewall и включенным логированием

# Ключевые технологии

## Контроль сетевых соединений

**Высокотехнологичный Stateful Firewall**

- Отслеживает состояния активных соединений и возможные угрозы в них
- Принимает решения на основе контекста трафика
- Возможность блокировки установленных сессий
- Контроль трафика конкретных стран и регионов с помощью GeoIP-политик

**User-aware политики**

- Позволяют контролировать доступы, как разрешать, так и запрещать, для отдельных пользователей или целых групп
- Обеспечивают более полный контроль сети и упрощают работу специалистов ИТ / ИБ с инфраструктурой

**Производительный DPI**

- Определяет в трафике более 6 000 приложений и сервисов
- Собственный центр экспертизы по распознаванию приложений

## Защита от сетевых угроз

**Гибкий IDPS**

- Выявляет и предотвращает атаки в режиме реального времени
- Поддержка более 9 000 сигнатур
- Показатель обнаружения и предотвращения сетевых угроз (Detection Rate) превышает 95%*

**Продвинутая SSL/TLS-инспекция**

- Расшифровывает трафик любых протоколов
- Поддержка исключений из расшифровки на основе веб-категорий
- Подключает к анализу все движки безопасности

**Высокоскоростной потоковый антивирус**

- Выявляет вредоносные активности на самых ранних этапах
- Высокое соотношение качества детектирования и производительности

Возможность выбора наиболее подходящего варианта

**AI-powered антивирус**

- Разработан на базе технологий Kaspersky Endpoint Security, специально оптимизированных для Kaspersky NGFW
- Эвристический анализ файлов на базе механизмов Machine Learning (ML) и Artificial Intelligence (AI)
- Проверка архивов с любыми расширениями и возможность отправки файлов на дополнительную проверку в сторонние системы через ICAP-клиент

## Контроль веб-трафика

**Высокоточный веб-категоризатор**

- Точное определение категории URL
- Собственные категории с гибкими сценариями реагирования
- Возможность исключения конкретных URL-адресов

**Проверка репутации URL-адресов**

- Ограничение доступа к опасным и потенциально опасным веб-ресурсам и IP-адресам
- Блокировка рекламных ресурсов

**DNS Security**

- Проверяет принадлежность доменных имен к потенциально опасным
- Позволяет оптимизировать производительность за счет фильтрации на уровне доменов

* Тестирование проводилось с помощью IXIA BreakingPoint, Strike Level 3 и 5, 2521 попытка атак

# Актуальные данные об угрозах и обогащение аналитикой

## Threat Intelligence

- Встроенное автоматическое обогащение актуальной информацией об угрозах
- Уникальные тактические данные на основе опыта экспертов «Лаборатории Касперского»

Высокоскоростной потоковый антивирус

Объектный антивирус

Высокоточный веб-категоризатор

Проверка репутации URL-адресов

**Kaspersky Security Network**

Обогащение информацией с помощью глобальной сети обмена сведениями об угрозах

**343 млн**
отражено атак с различных ресурсов*

**50 млн**
обнаружено уникальных вредоносных ссылок*

**15 млн**
заблокировано нежелательных объектов*

# Интеграционные сценарии

Kaspersky NGFW поддерживает интеграцию с другими решениями «Лаборатории Касперского» в рамках экосистемного подхода.

**Kaspersky Symphony XDR**

Автоматизация управления безопасностью и реагирование

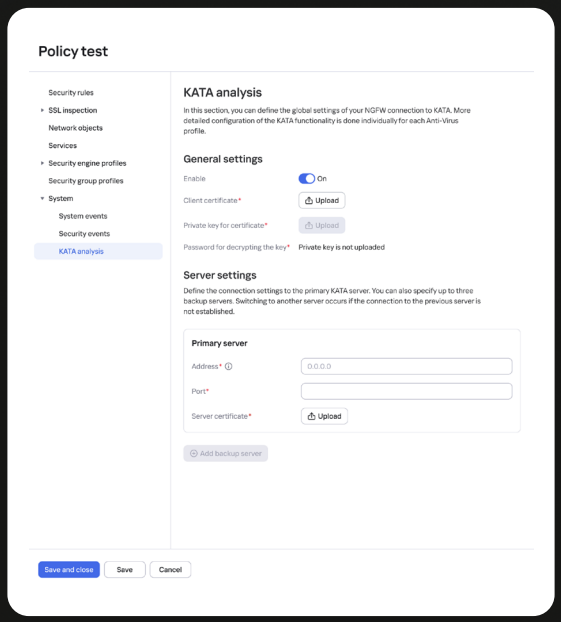
**Kaspersky Unified Monitoring and Analysis Platform**

Сбор и корреляция событий безопасности

**Kaspersky Anti Targeted Attack**

Предотвращение сложных атак и угроз нулевого дня с помощью проверки подозрительных файлов в специальной среде — Sandbox

- Интеграция по API для достижения максимальной скорости получения вердикта
- Кеширование вердиктов для оптимизации скорости обработки запросов на повторную проверку файлов




* Развитие информационных угроз в первом квартале 2026 года. «Лаборатория Касперского»

# Возможности продукта

## Функции управления и мониторинга

Централизованная система управления (Kaspersky Security Center (KSC) + Kaspersky Unified Monitoring and Analysis Platform (KUMA))

Комплексное управления продуктами экосистемы Kaspersky для XDR-сценария через централизованную консоль управления Open Single Management Platform (OSMP)

Аналитические панели мониторинга и отчеты по результатам работы решения в OSMP или KUMA

Возможность предварительного просмотра внесенных в политику изменений перед ее применением

Централизованное управление сетевой конфигурацией при помощи шаблонов

Мониторинг состояния решения в режиме реального времени

Экспорт событий в SIEM-системы через Syslog

Zabbix-шаблон для мониторинга NGFW

Ролевая модель доступа (RBAC)

Командная строка (CLI)

Поддержка виртуальных контекстов (VSS)

Подключение через SSH

Поддержка обновления ПО NGFW

Интеграция по LDAP (MS AD)

SNMPv2, SNMPv2c, SNMPv3

Многофакторная аутентификация TOTP (RFC 6238)

SNMP trap

Языки интерфейса — русский, английский

## Сетевые функции

Статическая маршрутизация IPv4

Поддержка VRF

BGPv4

Поддержка DNS-клиента

OSPFv2

Поддержка DHCP-клиента

BFD

Поддержка NTP-клиента

Поддержка агрегированных интерфейсов (LACP)

Policy-Based Routing (PBR)

Поддержка L2 (bridge) интерфейсов

Поддержка Multi-WAN на базе IP SLA

Поддержка L3-интерфейсов

DHCP Relay

Поддержка VLAN (802.1q) и саб-интерфейсов

## Site-to-Site VPN

Policy-Based IPSec

Route/GRE-Based IPSec

IKEv2

Алгоритмы шифрования

- AES-CBC-128
- AES-CBC-192
- AES-CBC-256
- AES-GCM-128
- AES-GCM-192
- AES-GCM-256

NAT Traversal

## Трансляция сетевых адресов

Source NAT

Destination NAT

Статический NAT

Динамический NAT

PAT

NAT oversubscription

## Отказоустойчивость

Поддержка отказоустойчивого кластера active-passive на базе собственного протокола KHCP (Kaspersky High-availability Cluster Protocol)

Синхронизация сессий

Синхронизация маршрутной информации (RIB)

Синхронизация ARP-таблиц

Мониторинг интерфейсов в кластере

Поддержка виртуальных MAC и IP-адресов

GARP

Режимы автоматического и ручного переключения на резервный узел кластера

Режим автоматического переключения на резервный канал связи в случае нарушения параметров IP SLA (задержка, потери, доступность)

Поддержка отказоустойчивости системы управления

Возможность использования нескольких Sync-интерфейсов для кластера

Возможность агрегирования management-интерфейсов

Выделенный control plane

## Межсетевой экран

Поддержка Stateful Packet Inspection

Поддержка использования зон

Поддержка фильтрации трафика по:

- IP-адресам (host, подсеть, диапазон)
- Зонам
- Пользователям и группам пользователей
- FQDN
- GeoIP
- Сервисам (L3/L4 протокол + порт)
- Приложениям и категориям приложений

Распознавание при помощи DPI более 6 000 приложений

Интеграция с внешними каталогами пользователей (MS AD)

Поддержка групп объектов и вложенных групп

Логирование начала и конца сессии

Время жизни и/или расписание работы для правил

Использование групповых профилей модулей безопасности в правилах

## Функции безопасности

- Антивирусная проверка по протоколам: HTTP(S), SMTP(S), POP3(S) и IMAP(S)
- Антивирусная проверка архивов с любыми расширениями
- Проверка репутации URL-адресов (malware, phishing, c&c, adware и т.п.)
- Инспектирование SSL/TLS-трафика с поддержкой TLS 1.1, 1.2 и 1.3
- Система обнаружения и предотвращения вторжений (IDPS) с поддержкой более 9 000 собственных сигнатур
- Возможность исключений в SSL/TLS-инспекции по веб-категориям и конкретным доменам
- Отправка расшифрованного трафика на анализ всеми модулями безопасности
- Отображение страниц блокировок и предупреждения при попытке доступа на веб-ресурс
- Поддержка проверки DNS-трафика (DNS Security) по репутационным базам
- Возможность настройки периода и источника обновления локальных баз NGFW
- Нативная интеграция с Threat Intelligence для обогащения баз модулей антивируса и веб-фильтрации
- Менеджер сессий для просмотра и контроля установленных сессий
- Возможность настройки таймаутов сессий для устройств и VSS
- Потоковый антивирус
- AI-powered антивирус
- Возможность блокировки Partial Content
- Интеграция с песочницей KATA по API
- ICAP клиент
- Возможность указания минимальной версии TLS
- Валидация сертификата сервера
- Категоризация и контроль веб-трафика по SNI или URL
- Более 90 предустановленных веб-категорий
- Поддержка пользовательских веб-категорий
- Возможность исключения сигнатур IDPS
- Захват трафика при сработках сигнатур IDPS
- IDPS проверка по неклассифицированным сессиям
- Поддержка исключений для веб-фильтрации
- Поддержка работы правил фильтрации по расписанию
- Поддержка DNS-redirect
- Защита от IP Spoofing
- Защита от сетевого сканирования

## Поддержка гипервизоров

- KVM
- VMware ESXi

## Интеграция с продуктами от Лаборатории Касперского

- Kaspersky Symphony XDR (посредством плейбуков)
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Anti Targeted Attack (по API для проверки файлов с помощью Sandbox)

# Аппаратные и виртуальные платформы

Линейка KX (Kaspersky Extension) — семейство сетевых аппаратных платформ, разработанных специально для решения Kaspersky NGFW. Эти устройства обеспечивают высокую производительность, надежную защиту от киберугроз и масштабируемость для различных сценариев использования.

Внешний вид моделей

KX-100-KA1

KX-100-KB1

Внешний вид моделей

KX-400
KX-1000
KX-3500

| | KX-100-KA1 | KX-100-KB1 | KX-400 | KX-1000 | KX-3500 |
|---|---|---|---|---|---|
| Производительность в режиме L4 FW + Application Control* | До 10 Гбит/с | До 10 Гбит/с | До 40 Гбит/с | До 100 Гбит/с | До 200 Гбит/с |
| Производительность в режиме NGFW (L4 FW + Application Control + IDPS)* | До 3 Гбит/с | До 3 Гбит/с | До 15 Гбит/с | До 40 Гбит/с | До 140 Гбит/с |
| Интерфейсы | • 6 × 10/100/1000 Ethernet RJ45<br>• 2 × SFP+ | • 14 × 10/100/1000 Ethernet RJ45<br>• 2 × SFP+ | • 4 × 10/100/1000 Ethernet RJ45<br>• 8 × 25G SFP28<br>• 4 × 100G QSFP28 | • 4 × 10/100/1000 Ethernet RJ45<br>• 8 × 25G SFP28<br>• 4 × 100G QSFP28 | • 4 × 10/100/1000 Ethernet RJ45<br>• 8 × 25G SFP28<br>• 4 × 100G QSFP28 |

В рамках линейки KX-Series доступны также виртуальные исполнения — vKX. Они предназначены для развертывания Kaspersky NGFW на собственных ресурсах заказчика без необходимости использования аппаратных платформ. В данный момент доступно виртуальное исполнение Kaspersky NGFW vKX-8.

| | vKX-8 |
|---|---|
| Производительность в режиме L4 FW + Application Control* | До 5 Гбит/с |
| Производительность в режиме NGFW (L4 FW + Application Control + IDPS)* | До 4 Гбит/с |
| Гипервизоры | KVM и VMware ESXi |

Для аппаратных платформ также доступна Расширенная гарантия Hardware MSA

Подробнее

Более подробно изучить линейку KX-Series можно в нашем каталоге оборудования

Подробнее

## Узнать подробнее о методике тестирования производительности

Подробнее

* Тестирование проводилось с 20 000 правил Firewall и включенным логированием

# Лицензирование

Решение Kaspersky NGFW представлено в двух вариантах: Standard и Advanced.

**Kaspersky NGFW**

Standard

Предоставляет все необходимые инструменты управления и мониторинга, контроля сетевых соединений и защиты от сетевых угроз.

**Kaspersky NGFW**

Advanced

Предлагает расширенные возможности для контроля веб-ресурсов и построения комплексной защиты корпоративной сети.

Каждый вариант решения включает в себя техническую поддержку в соответствии с выбранным уровнем обслуживания: Premium или Premium Plus.

## Лицензия

1. Выбранная аппаратная платформа
2. Необходимый вариант решения: Standard или Advanced
3. Подходящий уровень технической поддержки: Premium или Premium Plus

+ Kaspersky NGFW Log Analyzer — модуль аналитики на базе OSMP с подходящим количеством событий в секунду (EPS, Events Per Second)

Скидка 95% в течение года

## Пример

1. KX-3500
2. В варианте Advanced
3. С включенной технической поддержкой уровня Premium

Подробнее о лицензировании

Подробнее

# Почему Kaspersky NGFW

Полностью российский продукт, соответствующий стратегии движения к импортонезависимости (сертификация ФСТЭК России)

Полный контроль и эффективное управление сетевым трафиком и активностью приложений

Экосистемный подход к защите корпоративной инфраструктуры и централизованное управление

Собственная архитектура и механизмы безопасности, основанные на лидерских технологиях

Прозрачное лицензирование без дополнительных модулей и расширений

Глобальная экспертиза в борьбе с киберугрозами, разработке продуктов и поддержке клиентов

Подробнее

# Уникальный опыт экспертов в основе решения

### Глобальный центр исследований и анализа угроз

Исследование сложных угроз и расследование финансово мотивированных киберпреступлений

### Центр исследования угроз

Исследование угроз, создание детектирующей логики, контентная фильтрация, безопасная разработка

### Центр исследования технологий искусственного интеллекта

Обнаружение угроз с помощью ИИ / усиление ИБ решений алгоритмами ИИ

### Центр исследования безопасности промышленных систем*

Анализ угроз в индустриальных инфраструктурах

Исследование угроз  Расследование инцидентов

* В рамках разработки решения для промышленных инфраструктур, с 2027 года

Kaspersky
NGFW

Узнать больше

www.kaspersky.ru

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

#kaspersky
#активируйбудущее