kaspersky АКТИВИРУЙ БУДУЩЕЕ

# Kaspersky Security для интернет-шлюзов

## Первая линия защиты корпоративной сети

**Бизнес-задачи большинства предприятий сегодня уже невозможны без использования интернета. Однако, будучи удобным инструментом в работе и источником информации, интернет при этом является одним из основных источников угроз корпоративной интернет-безопасности.**

- **Веб-угрозы растут не только количественно, но и качественно и становятся более изощренными.**
- **Злоумышленники используют методы социальной инженерии, чтобы вводить в заблуждение пользователей и добиваться желаемого без помощи вредоносного ПО.**
- **С виду безвредный, но содержащий эксплойты веб-сайт может незаметно заразить корпоративную сеть.**

**Безусловно, эффективная защита рабочих мест имеет решающее значение для повышения их устойчивости к веб-угрозам. Но логичнее бороться с угрозами до того, как они попадут на рабочие места пользователей корпоративной сети.**


## Блокируйте атаки до того, как они достигнут цели

### Защита пользователей и конечных устройств от веб-атак

Как правило,веб-угрозы приводятся в действие на конечных устройствах. Kaspersky Security для интернет-шлюзов обнаруживает и нейтрализует угрозы на ранней стадии — прежде чем они проникнут внутрь периметра сети.

### Снижение рисков, связанных с интернет-ресурсами

Решение ограничивает доступ к отдельным веб-ресурсам и их категориям в соответствии с политиками безопасности компании. Решение блокирует потенциально опасные и зараженные сайты (например, фишинговые или содержащие вредоносное ПО).Kaspersky Security для интернет-шлюзов позволяет значительно снизить риск заражения вашей сети, утечки ценных данных и использования интернета в нерабочих целях.

### Повышение устойчивости к продвинутым атакам

Kaspersky Security для интернет-шлюзов интегрируется с другими решениями «Лаборатории Касперского», предоставляет дополнительные данные для углубленного анализа угроз и позволяет разрушать цепочки целевых атак при попытке пересечения периметра.

# Ключевые возможности

## Многоуровневая защита от вредоносного ПО

Надежная многоуровневая защита обнаруживает, анализирует и блокирует различные угрозы, такие как шпионское ПО, банковские троянцы, программы- вымогатели, криптомайнеры и вайперы.

## Передовая защита от фишинга

Антифишинговые компонетны используют облачную защиту от известных и неизвестных фишинговых угроз и угроз «нулевого часа» на базе нейросетевого анализа более чем по 1000 критериев. Они включают анализ изображений, языковые проверки и специфические скрипты, а также собираемые со всего мира данные о вредоносных и фишинговых веб и IP- адресах.

## Репутационная фильтрация

Решение фильтрует подозрительные и нежелательные веб и IP-адреса, нарушая сценарии веб-атак. Его база пополняется за счет вердиктов, Kaspersky Security Network, и результатов анализа (на основе машинного обучения) большого объема данных, получаемых в режиме реального времени от десятков миллионов пользователей, а также на основе опыта экспертов «Лаборатории Касперского».

## Веб-Контроль с категоризацией

Доступ к нежелательным, неуместным и вредоносным веб-сайтам можно заблокировать или ограничить на основании предварительно заданных категорий.

## Управление и прозрачность

Простой веб-интерфейс позволяет администратору контролировать уровень защиты корпоративного прокси-сервера и осуществлять настройку системы безопасности.

В 2021 году 82% нарушений были связаны с человеческим фактором. Люди продолжают играть очень большую роль в инцидентах кибербезопасности.

По данным Verizon Data Breach Report 2022

## Предотвращение нежелательной передачи файлов

Загрузка одних типов файлов может привести к заражению, а отправка других – к утечке данных. Предотвращение загрузки и передачи таких файлов значительно снижает риски.

## Гибкое развертывание

Kaspersky Security для интернет-шлюзов может быть интегрирован в корпоративную сеть в качестве системы защиты существующего прокси-сервера. Второй вариант поставки позволяет развернуть полноценное программное устройство безопасности, включающее готовый к использованию прокси-сервер и систему его защиты.

# Защита от сложных угроз и целевых атак

Интеграция Kaspersky Security для интернет шлюзов с платформой защиты от целевых атак Kaspersky Anti Targeted Attack позволяет получать дополнительные данные для более глубокого анализа, автоматически блокировать компоненты атак и связь с серверами злоумышленников через интернет, например передачу команд, вредоносного кода и извлечение украденных данных. Они разработаны на единой технологической базе и отлично дополняют друг друга, обеспечивая комплексную и надежную защиту.

**15,45%***

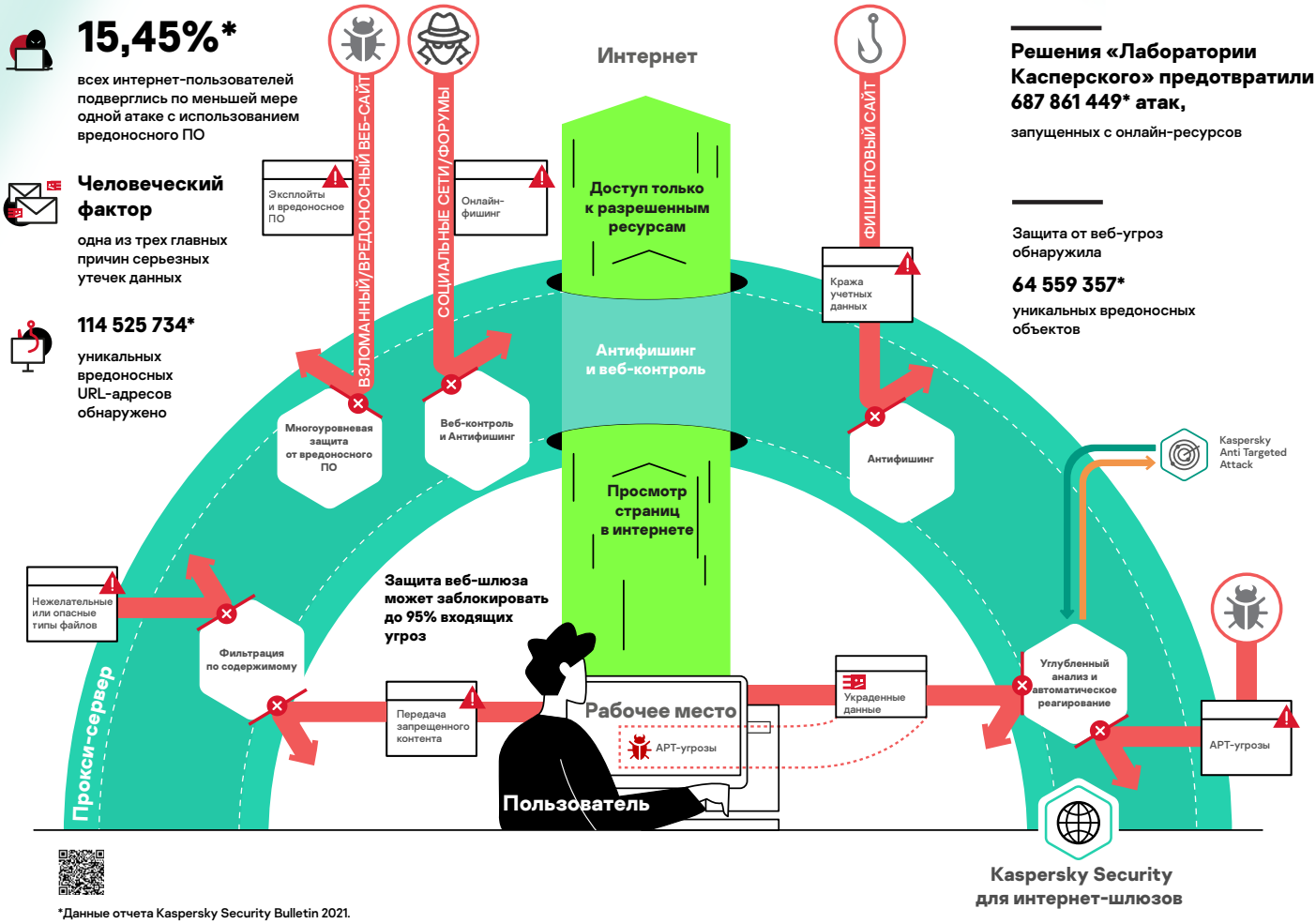
всех интернет-пользователей подверглись по меньшей мере одной атаке с использованием вредоносного ПО

**Человеческий фактор**

одна из трех главных причин серьезных утечек данных

**114 525 734***

уникальных вредоносных URL-адресов обнаружено




**Решения «Лаборатории Касперского» предотвратили 687 861 449* атак,**

запущенных с онлайн-ресурсов

Защита от веб-угроз обнаружила

**64 559 357***

уникальных вредоносных объектов

**Kaspersky Security для интернет-шлюзов**

*Данные отчета Kaspersky Security Bulletin 2021.

**Также рекомендуем:**

**Kaspersky Security для почтовых серверов** – отличное дополнение защиты интернет-шлюзов системой безопасности электронной почты, одного из ключевых путей распространений угроз.

**Kaspersky Security для бизнеса** – флагманская линейка решений для построения системы многоуровневой защиты рабочих станций и серверов от всех видов киберугроз.

## Как приобрести

Kaspersky Security для интернет-шлюзов можно приобрести в составе Kaspersky Total Security для бизнеса или как отдельное решение..

## Состав продукта

Kaspersky Web Traffic Security

**www.kaspersky.ru**