



Комплексная защита корпоративных сетей от современных угроз для факторинговой компании

kaspersky

 **СБЕР ФАКТОРИНГ**



Компания СберФакторинг

Данные за 2025 год

(на 01.01.2026)

960 млрд ₽

портфель компании

2 650 млрд ₽

выплаченное
финансирование

2 914

активных клиентов

1 945 294

количество
профинансированных
поставок

СберФакторинг — один из крупнейших российских факторов.

С 2014 года компания предоставляет комплекс услуг для предприятий, ведущих торговую деятельность на условиях отсрочки платежа. Решения и сервисы по управлению дебиторской и кредиторской задолженностью компании доступны поставщикам и покупателям в любом регионе России. Для финансирования экспортных и импортных поставок СберФакторинг реализует сделки международного факторинга.

Важным направлением деятельности компании является развитие интегрированных сервисов и собственной онлайн-платформы СберФакторинг. Онлайн-платформа обеспечивает полностью бесконтактный путь реализации сделки: от заявки на факторинг до финансирования и мониторинга клиентом статусов по поставкам. СберФакторинг входит в Ассоциацию факторинговых компаний России, участвует в развитии финансовых услуг для малого и среднего предпринимательства.

Основные факторинговые продукты компании:

Для поставщиков:



Быстрое финансирование



Сервис возврата дебиторской задолженности

Для покупателей:



Деньги на закупку



Финансирование поставщиков

Предыстория

Компания СберФакторинг в рамках стратегии импортозамещения приняла решение заменить текущую сетевую инфраструктуру российским решением. Ранее в компании эксплуатировались межсетевые экраны нового поколения Cisco FTD, но из-за ухода вендора из России дальнейшее использование решения ставило под угрозу безопасность работы всей компании.

Помимо замены на решение, которое соответствует требованиям регулятора, входит в реестр российского ПО и работает на отечественных аппаратных платформах, у компании были и другие требования:



Высокий уровень обнаружения и предотвращения сетевых угроз



Развитая функциональность для нового решения



Широкие возможности сегментации корпоративной сети



Бесперебойная работа во время миграции



Бесшовная миграция текущей инфраструктуры



**Kaspersky
NGFW**

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

Kaspersky NGFW — межсетевой экран нового поколения, обеспечивающий глубокую фильтрацию трафика на прикладном уровне, превентивный анализ поведения пользователей и приложений, а также проактивное блокирование известных уязвимостей на основе глобальных данных об угрозах.



**Kaspersky
Professional
Services**

Kaspersky Professional Services — комплекс услуг от экспертов «Лаборатории Касперского», созданный для того, чтобы компании могли максимально эффективно использовать свои решения по кибербезопасности, не отвлекая собственных IT-специалистов от основных задач.

Услуги охватывают весь жизненный цикл решений безопасности и группируются по нескольким направлениям:

- Оценка и аудит;
- Внедрение, развертывание и миграция;
- Обслуживание и оптимизация;
- Помощь с обновлением продуктов «Лаборатории Касперского» и переходом с других решений.

Реализация проекта

Перед реализацией проекта компания СберФакторинг сравнивала несколько отечественных NGFW-решений. После глубокого анализа функциональных возможностей и успешной и положительной истории взаимодействия по другим продуктам было принято решение о закупке межсетевого экрана нового поколения от «Лаборатории Касперского», который к тому же в наибольшей степени соответствовал требованиям заказчика.

Для реализации такого амбициозного проекта со стороны «Лаборатории Касперского» были вовлечены эксперты **Kaspersky Professional Services**, которые сопровождали проект от начала и до конца: от аудита текущей сетевой архитектуры заказчика до помощи в настройке и миграции решения.

Весь проект был поделен на несколько этапов:

1 Подготовка программно-аппаратных комплексов (ПАК) к тестированию на трафике заказчика

Эксперты «Лаборатории Касперского» провели первичную настройку и конфигурацию политик безопасности для тестовых сегментов сети заказчика, чтобы проверить, как отрабатывается трафик и работает отказоустойчивый кластер. На этом этапе оборудование находилось в лаборатории компании СберФакторинг.

2 Глубокое продуктовое обучение

Эксперты **Kaspersky Professional Services** провели несколько обучающих сессий для специалистов заказчика для более глубокого понимания особенностей работы с продуктом и его функциональными возможностями.

3 Практическая проверка решения заказчиком в изолированной сети

После завершения обучения специалисты СберФакторинг приступили к практической проверке решения в своей внутренней изолированной сети. На этом этапе эксперт «Лаборатории Касперского» выполнил полную предварительную настройку кластера **Kaspersky NGFW**: на основе требований заказчика разработаны и применены политики безопасности, настроены правила контроля доступа по приложениям, обеспечены антивирусная проверка трафика и фильтрация веб-контента, а также собран, сконфигурирован и подключен к тестовой среде кластер.



Затем заказчик подключил к кластеру свои сегменты сети и приступил к генерации трафика. Специалисты СберФакторинг воспроизводили различные сценарии работы сервисов, имитировали разные подключения и анализировали результат. В ходе тестирования проверялись протоколы HTTPS, DNS, SSH, RDP, NTP и другие — при этом ни один из стандартных портов не использовался, что позволило убедиться в корректном распознавании приложений и категорий трафика вне зависимости от порта.

Все тесты проводились силами заказчика на заранее сконфигурированном экспертом «Лаборатории Касперского» оборудовании. В качестве SIEM-системы использовалась **Kaspersky Unified Monitoring and Analysis Platform (KUMA)** — через нее специалисты могли наблюдать сработки правил и переход трафика с одной ноды Kaspersky NGFW на другую, что подтверждало корректную работу отказоустойчивого кластера.

4

Миграция на Kaspersky NGFW

После успешного прохождения всех тестов было принято решение о начале процесса миграции трафика на решение от «Лаборатории Касперского». Все оборудование было настроено и отправлено на площадки заказчика. Начало миграции совпало с выходом новой версии 1.2, поэтому обновление продукта было выполнено уже на площадке заказчика. Преднастроенные кластеры **Kaspersky NGFW** были размещены и подключены на площадках ЦОДов заказчика. В настоящее время кластеры обрабатывают трафик, продолжается процесс перевода остальных сервисов на новое решение.

★
ANGARA
SECURITY

Angara Security — партнер проекта.

Ведущий российский ИБ-интегратор и провайдер более 80 услуг в сфере информационной безопасности.

Результаты

СберФакторинг в лице как специалистов по информационной безопасности, так и сетевой инфраструктуры остался полностью доволен продуктом Kaspersky NGFW, его функциональными возможностями, высоким уровнем детектирования угроз и отказоустойчивостью, а также качеством сервиса **Kaspersky Professional Services**.

В результате проекта заказчик заменил геораспределенные кластеры active-passive на своих площадках: основных и резервных ЦОДах. Были установлены ПАКи **Kaspersky NGFW**, централизованная система управления решением Kaspersky NGFW (KSCL) и Log Analyzer (модуль аналитики).

Отдельно стоит отметить, что заказчик остался особенно доволен качественным распознаванием трафика по категориям приложений и нестандартным портам. Kaspersky NGFW с помощью технологии DPI определяет прикладные протоколы, поддерживаемые решением, на основе сигнатур, а не только по номерам портов.

Сейчас проект находится на финальном этапе миграции: специалисты СберФакторинг переводят все сегменты сети на **Kaspersky NGFW**. После ввода в эксплуатацию партнер проекта Angara Security возьмет на себя дальнейшее сопровождение и обслуживание аппаратных платформ.

Заказчик также ждет новых версий продукта в следующих релизах, чтобы пользоваться дополнительными возможностями решения, в частности, высокий интерес представляет Remote Access VPN.



Анна Кулашова

Вице-президент по развитию
бизнеса «Лаборатории Касперского»
в России и странах СНГ

Финансовый сектор остается одной из главных целей для злоумышленников: по нашим данным, в 2025 году число кибератак на финансовые организации в России выросло на 43%, и в 2026-м их активность сохраняется на высоком уровне. В таких условиях финансовым организациям особенно важно выстраивать комплексную защиту, способную адаптироваться к меняющемуся ландшафту угроз.

Для нас особенно ценно, что по итогам комплексного тестирования СберФакторинг выбрал Kaspersky NGFW, доверив защиту своей инфраструктуры нашим технологиям. Это важное подтверждение качества и зрелости нашего решения. За этим результатом стоит большая совместная работа наших команд на всех этапах проекта. Полученный опыт станет еще одним ориентиром для развития продукта. Мы продолжим совершенствовать Kaspersky NGFW, усиливая его возможности с учетом новых киберугроз и потребностей рынка.



Константин Панченко

Главный инженер отдела
кибербезопасности СберФакторинг

Сегодня надежная киберзащита для финансовой компании — это не просто опция, а фундамент бизнеса. Методы киберпреступников эволюционируют, поэтому нам принципиально важно иметь систему, которая работает на опережение и мгновенно адаптируется к новым угрозам. Именно такой технологический периметр мы выстроили, внедрив Kaspersky NGFW в нашу сетевую инфраструктуру. По сути, мы получили интеллектуальный центр управления трафиком, который обеспечивает глубокий контроль и защиту всех цифровых потоков компании.

Интеграция решений такого класса — самый сложный процесс, но благодаря тому, что команда вендора сделала проект под ключ, внедрение прошло оперативно и бесшовно для наших бизнес-процессов. Специалисты продемонстрировали высочайший уровень экспертизы, и сегодня мы абсолютно уверены в безопасности наших данных и защищенности бизнеса в долгосрочной перспективе.

95%

Показатель обнаружения и предотвращения сетевых угроз с помощью IDPS*

6 000+

Распознаваемых приложений с помощью DPI

до 100 000

Поддерживаемых правил движком Stateful Firewall

до 200 Гбит/с

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

9 000+

Поддерживаемых сигнатур гибким IDPS

Бескомпромиссная защита от сетевых угроз и контроль активности приложений

Kaspersky NGFW — межсетевой экран нового поколения на основе глобальной экспертизы и передовых технологий. Под капотом решения собственная архитектура и движки безопасности.

Преимущества Kaspersky NGFW для российских компаний:



Собственная архитектура и движки безопасности, основанные на лидерских технологиях



Полный контроль и эффективное управление сетевым трафиком и активностью приложений



Экосистемный подход к защите корпоративной инфраструктуры и централизованное управление



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



Прозрачное лицензирование без дополнительных модулей и расширений



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

* Данные IXIA BreakingPoint, Strike Level 3 и 5, 2521 попытка атак

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



Kaspersky NGFW

Подробнее

www.kaspersky.ru

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

#kaspersky
#активируйбудущее