# Непрерывная киберзащита

одного из крупнейших
региональных банков России

kaspersky активируй будущее

На рынке более
**30 лет**

**2 млн**
частных клиентов

**60 000**
корпоративных клиентов

число сотрудников
**> 5000**

# О заказчике

Крупный универсальный банк, сильный игрок в финансовом секторе с фокусом на северо-западный регион, предоставляющий полный спектр банковских услуг для физических и юридических лиц.

Банк демонстрирует устойчивость и стабильность на всех основных рынках финансовых услуг и сохраняет репутацию надежного партнера уже более 30 лет. Банк занимает 17 место по объему активов среди российских банков (более 1 млрд ₽ в 2023 г.), а также располагает долей рынка в 6–10% по активам, преимущественно в сегментах ипотеки и розничных депозитов.

## Приоритетные направления деятельности:

1. Кредитование
2. Расчетно-кассовое обслуживание корпоративных и розничных клиентов
3. Операции на валютном рынке и рынке межбанковских кредитов
4. Операции с ценными бумагами

### Многолетнее партнерство

Региональный банк и «Лаборатория Касперского» поддерживают плодотворное сотрудничество уже более 10 лет. Организация использует широкий спектр продуктов и услуг «Лаборатории Касперского», включая решение по управляемой защите Kaspersky MDR.

# Курс на кибербезопасность в режиме 24/7

В современном мире кибератаки становятся все более многочисленными и сложными, таким критически важным для общества объектам как банкам, важно сохранять непрерывность бизнес-процессов и иметь все необходимые инструменты для защиты конфиденциальной информации. Для банка резкое увеличение объема цифровых данных и изменения в инфраструктуре создали новые риски, которые послужили стимулом к поиску ИБ-решения, позволяющего проактивно отвечать на современные вызовы. Как организации, которая ставит в приоритет доверие клиентов, заказчику было важно найти ИБ-решение, которое позволило бы обеспечить круглосуточную защиту корпоративных бизнес-процессов и сохранить стабильность банковских операций.

Kaspersky
Managed Detection
and Response

## Преимущества Kaspersky MDR

Уверенность в том, что компания находится под постоянной защитой даже от самых сложных и изощрённых угроз

Возможность направить внутренние ИБ-ресурсы компании на решение других важных задач

Возможность пользоваться ключевыми преимуществами международного центра SOC

Сокращение расходов на безопасность из-за отсутствия необходимости нанимать новых ИБ-специалистов

Благодаря стабильной работе решения и оперативной поддержке со стороны «Лаборатории Касперского», банк получил уверенность в долгосрочной эффективности своей защиты и значимости выбранного ИБ-решения

# Расширение сотрудничества

Выбор «Лаборатории Касперского» в качестве стратегического партнера по кибербезопасности стал естественным и обоснованным шагом для обеспечения комплексной киберзащиты банка. Ряд значимых факторов в принятии решения о расширении взаимодействия включал: безупречную репутацию надежного вендора ИБ-решений, обширное портфолио продуктов и услуг, обеспечивающих эффективную защиту от современных киберугроз, непрерывные инновации и высокий уровень поддержки. Однако многофункциональность и легкость интеграции ИБ-решений сыграли решающую роль в выборе «Лаборатории Касперского».

Несмотря на наличие собственного SOC, региональный банк нуждался в дополнительном взгляде в свою инфраструктуру и мнении международных экспертов, поэтому заказчиком было принято решение о внедрении Kaspersky MDR — решения по обеспечению круглосуточного мониторинга и обнаружения киберугроз, способных обойти автоматические средства безопасности. Благодаря передовым технологиям защиты, Kaspersky MDR предоставил банку возможность работать только с реальными инцидентами ИБ, сохраняя тем самым ценное время специалистов на совершенствование внутренних процессов.

# Внедрение Kaspersky MDR

На момент подключения MDR банк уже использовал решения «Лаборатории Касперского», включая Kaspersky Security для бизнеса, KEDR Expert и Kaspersky Anti Targeted Attack, с которыми предварительно были настроены все необходимые интеграции, поэтому внедрение решения по управляемой защите прошло без осложнений. Значимым преимуществом стало то, что для Kaspersky MDR наличие внутреннего SOC — стандартный сценарий работы в инфраструктурах зрелых заказчиков. При этом, Kaspersky MDR рассматривается командой внутреннего SOC как один из источников данных об инцидентах, управление которыми далее производится во внутренних системах в соответствии с корпоративными нормативными документами. Для целей интеграции Kaspersky MDR с внутренними системами управления инцидентами предусмотрен хорошо документированный API.

Помимо двусторонней связи с IRP, которая получает полную информацию об инциденте и передает результаты его обработки обратно в MDR, также настроена интеграция с SIEM KUMA, где коррелируются инциденты от MDR с событиями других средств защиты информации, снижая нагрузку на аналитиков внутренней команды SOC.

Важнейшим преимуществом Kaspersky MDR является отсутствие дополнительных инфраструктурных затрат на внедрение: весь функционал поставщика телеметрии MDR включен в Kaspersky Security для бизнеса. Такая тесная интеграция агента MDR с Kaspersky Security для бизнеса обеспечивает оптимальную производительность конечной точки при наиболее глубоком анализе тактик, техник и инструментов атакующих.

# Результаты и отзывы

Внедрение Kaspersky MDR стало для банка одним из самых значимых ИБ-проектов последних лет. Высокая эффективность системы обнаружения угроз выделяется как важнейший аспект реализованного проекта, в результате которого значительно снизилась вероятность успешных атак на организацию. Регулярные обновления баз данных об угрозах позволили внутренней ИБ-команде оперативно адаптироваться к динамично меняющейся среде. Благодаря стабильной работе решения и оперативной поддержке со стороны экспертов «Лаборатории Касперского», банк получил уверенность в долгосрочной эффективности своей защиты и значимости выбранного ИБ-решения.

Руководитель SOC заказчика

Для нас Kaspersky MDR — не просто инструмент. Это целая философия безопасности, которая сочетает в себе непрерывный мониторинг, анализ поведения и мгновенное реагирование на угрозы. В наше время наличие доступа к опыту и ресурсам кибербезопасности — вопрос первостепенной важности, и Kaspersky MDR помогает нам этого достичь. На данный момент мы уже используем различные продукты и сервисы «Лаборатории Касперского» и открыты к дальнейшему расширению нашего сотрудничества.

Анна Кулашова

Управляющий директор в России и странах СНГ, АО «Лаборатория Касперского»

Выбор крупнейшего регионального банка в пользу Kaspersky MDR — это подтверждение того, что наши решения соответствуют высоким стандартам безопасности в финансовой индустрии — одной из самых атакуемых отраслей в России и СНГ. Мы рады быть частью инноваций, которые банк внедряет для защиты своих клиентов, и готовы вместе преодолевать новые вызовы киберпространства.

# Усиление киберзащиты

Банк расширил сотрудничество с «Лабораторией Касперского», внедрив SIEM-систему Kaspersky Unified Monitoring and Analysis Platform (KUMA) и Kaspersky Anti Targeted Attack (KATA).

KATA обеспечивает контроль над ключевыми точками входа атаки (сетью, веб-трафиком и электронной почтой) и позволяет анализировать подозрительные файлы в изолированной среде, снижая риски заражения. Встроенный модуль NDR расширяет возможности KATA в части поиска сетевых угроз, детально исследуя сетевые данные, выявляя атаки через индикаторы взлома и проводя ретроспективный анализ данных. Решение эффективно противодействует кибератакам на каждом этапе: оно не только обнаруживает уже происходящие атаки и смягчает их воздействие, но и предотвращает возможные угрозы благодаря оценке уязвимостей в текущей системе безопасности.

Для банка внедрение SIEM-системы KUMA имеет стратегическое значение, так как позволяет осуществлять централизованный сбор и анализ логов безопасности со всех информационных систем. Это дает возможность оперативно выявлять даже сложные многоэтапные атаки, которые могут угрожать финансовым операциям и клиентским данным. Кроме того, решение помогает банку соответствовать строгим требованиям регуляторов, включая ЦБ РФ и законодательство о персональных данных.

## Комплексный мониторинг

KUMA обеспечивает мониторинг всех критически важных систем банка, включая платежные сервисы, онлайн-банкинг и корпоративные сети. Платформа проводит анализ угроз в режиме реального времени и позволяет проверять подозрительные объекты в изолированной среде, что значительно повышает уровень безопасности. Особенностью решения являются максимальная гибкость системы и мощные инструменты корреляции событий безопасности, которые обеспечивают проактивный поиск угроз.

## Kaspersky Managed Detection and Response

Подробнее

## Kaspersky Anti Targeted Attack

Подробнее

## Kaspersky Unified Monitoring and Analysis Platform

Подробнее

www.kaspersky.ru



#kaspersky
#активируйбудущее