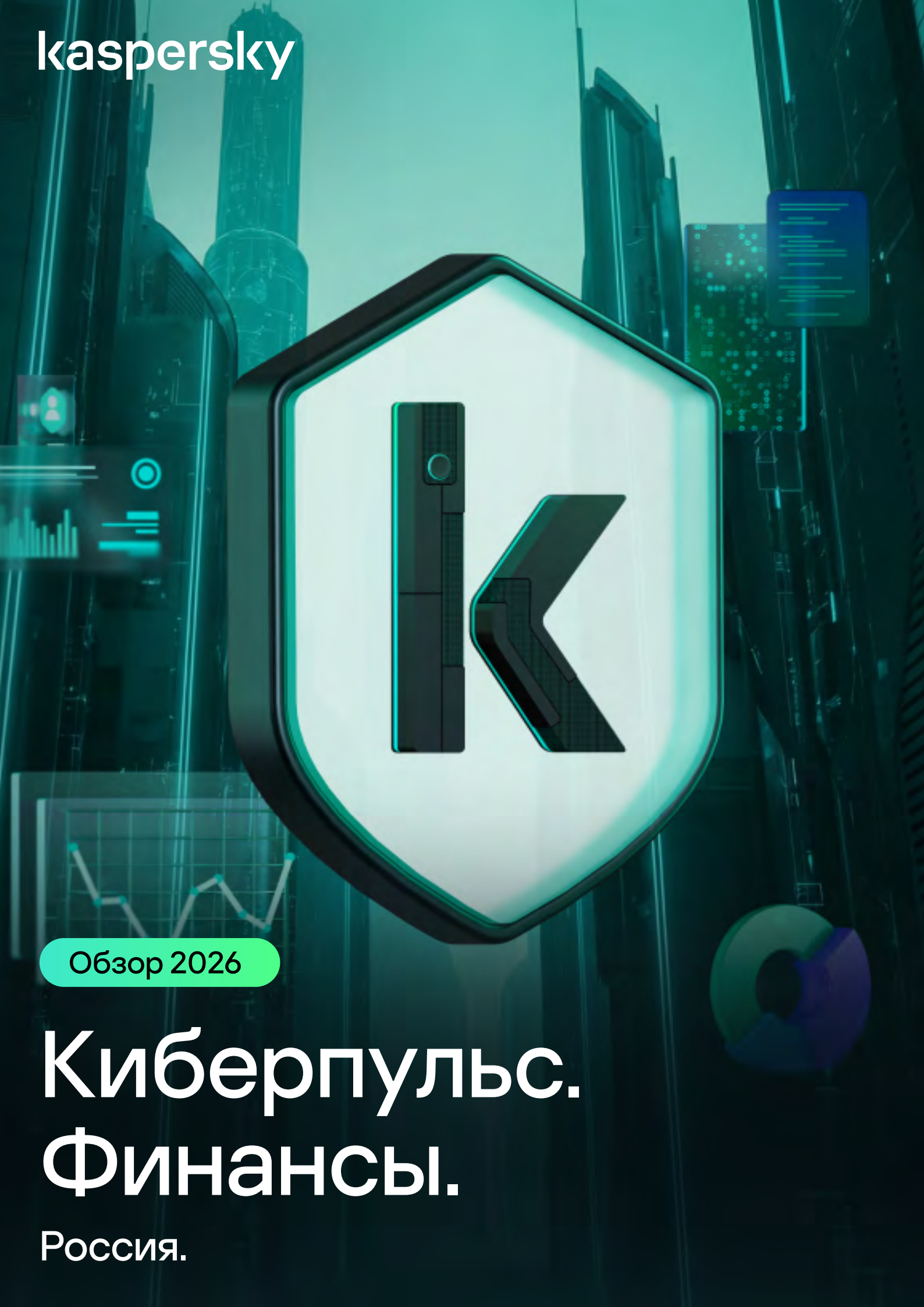
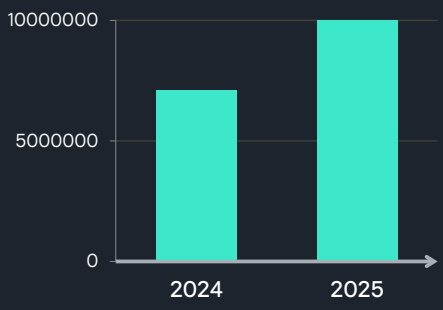

kaspersky
Обзор 2026
Киберпульс.
Финансы.
Россия.

Ключевая статистика киберугроз для финансовой отрасли в России

Количество кибератак на финансовые организации в России, 2025 vs 2024*



+43%

Почтовые угрозы

83%

компаний финансового сектора подверглись почтовым кибератакам в 2025 г. *

Данные по основным типам угроз для финансового сектора в России, 2025 vs 2024

+42%

рост количества атак с **помощью шпионского ПО***

-17%

снижение количества атак с помощью **бэкдоров***

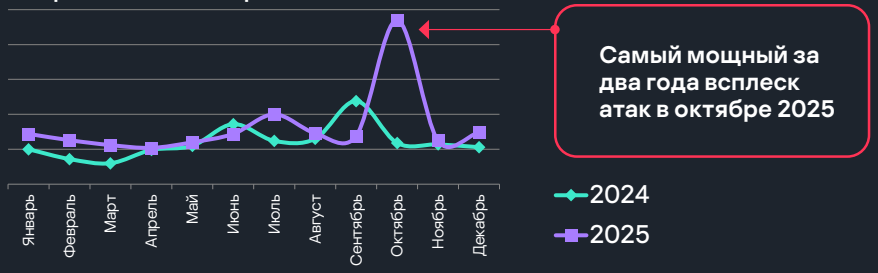
x4

рост количества атак с помощью **банкеров** (ВПО для кражи денежных средств через онлайн доступ к банковским счетам)*

+32%

рост количества атак с помощью **программ-вымогателей** (ransomware)*

Сезонность атак с использованием программ-вымогателей на финансовые организации в России**



Самый мощный за два года всплеск атак в октябре 2025

Дмитрий Галов
Руководитель Kaspersky GReAT в России

Октябрь 2025 года ознаменовался **крупнейшим за два года всплеском количества кибератак** с использованием программ-вымогателей на российские организации, включая компании финансового сектора. Программы-вымогатели остаются главной киберугрозой для бизнеса. В 2025 году они продемонстрировали устойчивость, адаптивность и готовность эволюционировать. Доминировала **модель «программа-вымогатель как услуга»** (RaaS), которая облегчает злоумышленникам получение как самого вредоносного ПО, так и первоначального доступа в систему. Кроме того, обычной практикой стало двойное и тройное вымогательство.

Также особенностями прошедшего года стали активное использование **шпионского ПО**, кратный рост количества и интенсивности **атак на цепочки поставок**, повышенное внимание злоумышленников к поиску и эксплуатации уязвимостей.

APT-кампании, нацеленные на российский финансовый сектор в 2025 году**

- Angry Likho
- GOFFEE
- Lazarus
- Horned Ghouls
- TWELVE
- Crypt Ghouls
- Hive0117
- BlueNoroff
- OldGremlin
- Forum Troll

* По данным Kaspersky Global Research and Analysis Team (GReAT)
** По данным Kaspersky Cyber Threat Intelligence Team

Актуальные угрозы для финансовой сферы конца 2025 – начала 2026 года

Форумный тролль

В 2025 году эксперты Kaspersky GReAT обнаружили сложную целевую кампанию, в которой использовалась уязвимость нулевого дня в Chrome. Злоумышленники рассылали по российским организациям, в том числе финансовым учреждениям, персонализированные фишинговые письма с приглашением на форум «Примаковские чтения». Если жертва переходила по ссылке и открывала браузер Chrome (или другой браузер на движке Chromium), устройство сразу заражалось, никаких дополнительных действий от пользователя не требовалось. Целью сложного вредоносного ПО, использованного в атаке, был шпионаж.

Кроме того, исследователи обнаружили ранее неизвестный зловред — коммерческое шпионское ПО Dante, созданное итальянской компанией Memento Labs (ранее Hacking Team), впервые замеченное в реальных атаках. Чтобы избежать обнаружения, Dante использовало уникальный метод анализа среды, чтобы определить, может ли он скрытно выполнять свои функции. Обнаружить такое ПО можно только с помощью комплексных продвинутых решений.

Цепочка атаки «Форумный тролль»

Подробнее

Бэкдор CoolClient. Посвящение в шпионы

Последние несколько лет мы отслеживаем активность APT-группы HoneyMyte, которая использует сложные инструменты, в том числе для шпионажа по всему миру. В 2025 году группа добавила новые функции в бэкдор CoolClient. Одно из ключевых обновлений — функция мониторинга буфера обмена. Эта функция позволяет получать всё его содержимое. Таким образом злоумышленники могут отслеживать поведение пользователя, определять, какие он использует приложения, а также получать контекст для похищенных данных.

Подробнее

Галя, у нас подмена!

DLL Hijacking — техника подмены DLL-файлов (Dynamic Link Library – библиотек), которые загружает и выполняет легитимное ПО в процессе своей работы, на вредоносные с таким же именем. Это позволяет злоумышленникам обойти защиту на устройстве жертвы и совершить атаку. Подмену библиотек используют как создатели массового вредоносного ПО, например банковских троянцев, так и APT-группы в процессе целевых атак. Например, подобным образом распространяется Lumma, один из наиболее активных стилеров в 2025 году. По данным «Лаборатории Касперского», число кибератак с подменой DLL в России в первом полугодии 2025 года по сравнению с аналогичным периодом в 2024 году увеличилось в 4 раза.

Подробнее

Возвращение PassiveNeuron

Эксперты Kaspersky GReAT выявили новую волну заражений PassiveNeuron, которая длилась практически весь 2025 год. Отличительная черта кампании — нацеленность преимущественно на операционные системы Windows Server. У злоумышленников появились новые инструменты, например Neursite — модульный бэкдор, который может собирать системную информацию, управлять запущенными процессами и направлять сетевой трафик через скомпрометированные хосты, обеспечивая перемещение по сети. Были обнаружены образцы, обменивающиеся данными как с внешними командными серверами, так и со скомпрометированными внутренними системами. Почему именно серверы? Серверы, особенно доступные из интернета, часто привлекают внимание APT-групп, поскольку служат точками входа в целевые организации.

Подробнее

Блокчейн под прицелом

Эксперты Kaspersky GReAT выявили новые целевые атаки группы BlueNoroff — GhostCall и GhostHire, активные с апреля 2025 года и нацеленные на криптовалютные и Web3-организации. В обеих кампаниях задействованы инструменты социальной инженерии: злоумышленники выдают себя за венчурных инвесторов (GhostCall) или рекрутеров (GhostHire). В процессе общения они под разными предлогами просили жертв загрузить вредоносный файл или скрипт — якобы для устранения проблем со звуком или скачивания файла с тестовым заданием. Загрузка вредоносного скрипта приводила к заражению устройств и последующим атакам, включая компрометацию цепочек поставок и распространение новых видов зловредов. BlueNoroff активно использует генеративный ИИ, что позволяет ускорять разработку вредоносного ПО и повышать эффективность атак.

Подробнее

Приоритеты ИБ в финансовых организациях на 2026 год

Игорь Кузнецов

Директор
Kaspersky GReAT

О Kaspersky GReAT

Глобальный центр исследования и анализа угроз Kaspersky GReAT основан в 2008 году. В его задачи входит поиск и исследование наиболее сложных атак, кампаний кибершпионажа, новых методов заражения, эксплойтов, использующих уязвимости нулевого дня. Сегодня в команде центра более 30 экспертов, работающих по всему миру: в Европе, России, Южной Америке, Азии, на Ближнем Востоке. Они известны своими достижениями в расследовании наиболее сложных атак, включая кампании кибершпионажа и киберсаботажа.

Внедрение и постоянное развитие многоуровневой системы защиты. В том числе укрепление архитектуры сетевой защиты. Внедрение многоуровневой сегментации сети, использование комплексной платформы сетевой безопасности с инструментами NGFW, IDS/IPS, сетевой анализ трафика (NTA) и SIEM для корреляции событий безопасности, контроль доступа к корпоративным системам по принципу Zero Trust.

Защита от угроз с использованием ИИ и новых технологий. Обеспечение передовой защиты от продвинутых угроз типа DLL Hijacking, горизонтального перемещения и других, способных обходить базовые защитные решения.

Повышенное внимание к защите конечных точек (Endpoint Security). Использование продвинутых EDR/XDR на всех рабочих местах и серверах. Актуальная защита от новейших стилеров, бэкдоров, банковских троянов и ransomware, основанная на последних данных Threat Intelligence. Контроль запуска, запрет локальных администраторских прав пользователям.

ИБ-гигиена: управление уязвимостями, обновлениями, правами доступа. Организация эффективного процесса патч-менеджмента, инвентаризация уязвимостей и мониторинг эксплуатируемых CVE на основе фидов Threat Intelligence. MFA для администраторов, удалённого доступа (VPN, RDP), критичных бизнес-систем (АБС, ДБО, процессинг). Принцип минимальных привилегий и регулярный (не реже 1 раза в квартал) пересмотр прав, особенно по отношению к подрядчикам.

Обучение и повышение культуры безопасности. Регулярное обучение сотрудников ИТ-подразделений и всего персонала методам защиты, реагирования на фишинг и инциденты. Внедрение политик безопасности и процедур, понятных и обязательных для всех. Оценка эффективности обучения через реальные фишинг-тесты и контроль соблюдения процедур.

Взгляд вперёд: на что обратить внимание уже сейчас

Рост количества атак на NFC-платежи
В третьем квартале 2025 количество атак с применением вредоносных утилит для работы с NFC в России составило более 44 тыс. (**x1.5 vs Q2 2025**)

Появление «агентных шифровальщиков» — вредоносного ПО, способного с помощью технологий ИИ динамически изменять поведение в процессе выполнения, адаптируясь к атакуемой инфраструктуре

Рост количества **предварительно заражённых устройств**, включая заражённые банковскими троянами

Рост использования ИИ для кибератак: от создания дипфейков для социальной инженерии до самописных зловредов

Дальнейший рост количества **атак на цепочку поставок**

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

Развитие цифровых сервисов и технологий создает новые возможности для роста бизнеса, но вместе с тем расширяет поверхность потенциальных кибератак. Наблюдается рост количества и сложности этих атак, и на этом фоне построение комплексной системы кибербезопасности становится не просто необходимостью, а конкурентным преимуществом бизнеса. Информационная безопасность стала по-настоящему стратегическим активом.

Компаниям необходимо включать киберугрозы в общую систему оценки и управления рисками, поскольку инциденты информационной безопасности могут привести к серьезным последствиям: от прямых денежных потерь и репутационных издержек до угрозы жизни и здоровью людей. Кибербезопасность требует комплексного подхода, объединяющего три ключевых элемента: люди, процессы и технологии.

Возможности портфолио «Лаборатории Касперского» для финансовой отрасли

Kaspersky Symphony XDR

Платформа комплексной кибербезопасности

Внедрение комплексных платформ кибербезопасности помогает сэкономить до 40% ресурсов команд ИБ за счет автоматизации, а также повысить скорость и эффективность реагирования на 35% и 50% соответственно

Kaspersky Anti Targeted Attack

Платформа анализа сетевого трафика и комплексной защиты от сложных угроз и целевых атак с модулем NDR

Kaspersky Unified Monitoring and Analysis Platform

Высокопроизводительная SIEM-платформа

Kaspersky Threat Intelligence

Комплекс сервисов информирования об угрозах, обогащения защитных решений и повышения экспертизы ИБ-команд

Kaspersky Container Security

Специализированное решение для сред разработки и эксплуатации приложений

Kaspersky Fraud Prevention

Проактивное обнаружение схем мошенничества в режиме реального времени в цифровых каналах

Kaspersky NGFW

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

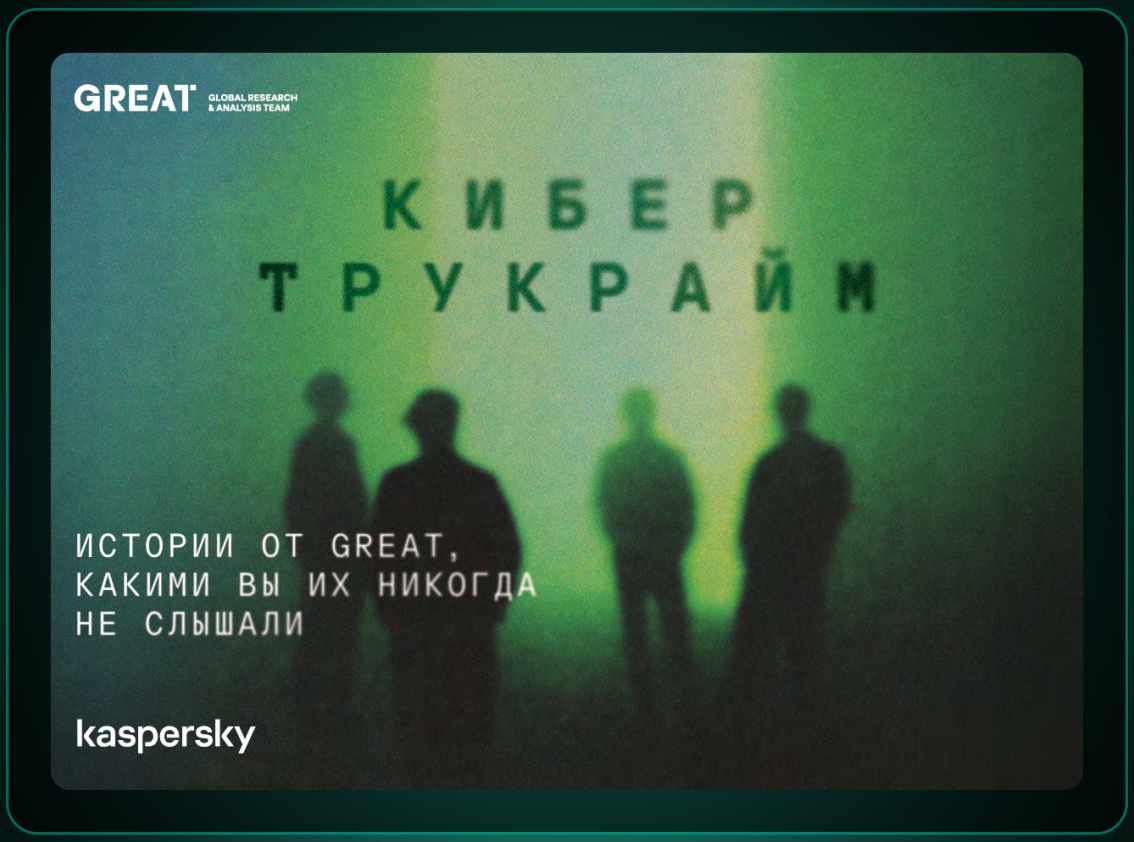
Кибербезопасность – стратегический актив финансовых организаций

Банки, страховые компании и финтех-стартапы внедряют новые сервисы и строят цифровые экосистемы. Это открывает возможности для роста, но одновременно повышает риски: от кибератак на платежные системы до мошенничества и утечек данных. Мы готовы предложить фокусные решения, которые отвечают вашим бизнес-приоритетам.

Комплексное предложение «Лаборатории Касперского» для финансовых организаций:

Получить

Больше интересных кейсов – в новом подкасте от Kaspersky GReAT



Слушать

www.kaspersky.ru

#kaspersky
#активируйбудущее