АССОЦИАЦИЯ ФИНТЕХ

ТРЕНДЫ КИБЕРБЕЗОПАСНОСТИ ФИНАНСОВОЙ ОТРАСЛИ РОССИИ В 2026 ГОДУ

Совместное исследование
Positive Technologies и Ассоциации ФинТех

Содержание

Денис Баранов
Генеральный директор
Positive Technologies

«Финансовая отрасль, которая традиционно была важной мишенью для киберпреступников, одной из первых научилась им противостоять. Однако в последнее время мотивация злоумышленников меняется: их атаки все чаще нацелены на подрыв киберустойчивости как отдельных игроков, так и всей индустрии. В то же время меняется и инструментарий: технологии искусственного интеллекта сегодня доступны и защитникам, и атакующим. Поэтому критически важно сохранять темпы строительства киберзащиты с учетом более деструктивных мотивов преступников и их доступа к современным технологиям. Наше исследование призвано помочь адаптироваться к новому ландшафту киберугроз и заглянуть в безопасное цифровое будущее отрасли».

Максим Григорьев
Генеральный директор
Ассоциации ФинТех

«Тренды ИБ в финтехе на 2026 год отражают системный сдвиг в характере рисков. Атаки все чаще развиваются по каскадному сценарию, затрагивая одновременно ИТ-сервисы, цепочки поставок, дочерние структуры и критически важные бизнес-процессы. Использование ИИ дополнительно усиливает давление: снижается порог входа для злоумышленников, растет качество социальной инженерии и масштабируемость атак. В этих условиях классический периметр больше не является достаточной точкой опоры для защиты.

Поэтому ключевая задача сегодня — не просто фиксировать эти сигналы, а превращать их в конкретные управленческие решения. Тренды имеют ценность только тогда, когда они помогают расставлять приоритеты: куда инвестировать, что проверять в первую очередь, какие сценарии считать недопустимыми. В 2026 году выигрывать будут те компании, которые умеют быстро переводить понимание угроз в действия — в процессы, метрики, ответственность и практическую киберустойчивость».

Введение

Финансовая отрасль России выступает фундаментом экономической устойчивости государства, обеспечивая непрерывность платежей, кредитование, расчеты на финансовых рынках и доверие населения к денежной системе. Тот факт, что 87% платежей приходится на безналичную форму оплаты и Россия входит в топ-5 стран по этому показателю, является свидетельством высокого уровня доверия населения к финансовым институтам. С другой стороны, именно финансовые организации остаются одними из наиболее приоритетных целей для киберпреступников, в том числе хактивистских групп и высокоорганизованных APT-группировок. Рост геополитической напряженности, цифровизация финансовых сервисов, активное внедрение API-банкинга, облачных и платформенных решений, а также ускоренное использование искусственного интеллекта качественно меняют ландшафт киберугроз.

Традиционный фокус информационной безопасности на предотвращении инцидентов и формальном выполнении регуляторных требований перестал быть достаточным. Практика последних лет показывает: даже организации с высоким уровнем зрелости ИБ, сертифицированными процессами и значительными инвестициями остаются уязвимыми для сложных многошаговых атак, усиленных искусственным интеллектом, для компрометации цепочек поставок, атак через доверенных подрядчиков и злоупотреблений легитимными цифровыми механизмами. В этих условиях ключевым становится не вопрос «произойдет ли инцидент?», а вопрос «как минимизировать ущерб и быстро восстановить деятельность организации в условиях инцидента?».

Именно поэтому в центре настоящего исследования находится концепция киберустойчивости — способности финансовой системы продолжать выполнение системно значимых функций при реализованных киберугрозах, минимизируя масштаб деградации, экономический ущерб и социальные последствия. Такой подход согласуется с эволюцией регуляторной логики Банка России и международными практиками перехода от prevent-only security ① к модели resilience–driven security ②.

Совместное исследование Positive Technologies и Ассоциации ФинТех направлено на формирование целостного взгляда на ключевые изменения сфере кибербезопасности финансового сектора на горизонте 2026–2027 годов. Документ адресован руководителям ИБ и ИТ, архитекторам цифровых платформ, риск-менеджерам, а также представителям регуляторных и отраслевых структур.

① Prevent-only security — это подход в кибербезопасности, ориентированный исключительно на блокирование угроз до того, как они смогут причинить ущерб.

② Resilience-driven security — подход к обеспечению кибербезопасности, основанный на способности организаций предвидеть, выдерживать, восстанавливаться и адаптироваться к неблагоприятным условиям, атакам или компрометациям ИТ-систем.

Подход и методология исследования

Исследование проводилось в несколько этапов. В рамках первого этапа была сформирована база более чем из 20 российских и международных материалов, на основе которой сформирован длинный перечень трендов (лонг-лист).

Тренд — это устойчивое и воспроизводимое изменение рынка, подтверждаемое совокупностью эмпирических данных, отраслевого опыта, которое в краткосрочной перспективе (1–2 года) оказывает существенное влияние на профиль рисков, архитектуру решений и управленческие модели защиты финансовых организаций.

Далее перечень трендов был сокращен и вынесен на экспертное обсуждение. По итогам обсуждения, а также по итогам качественных интервью с участниками Ассоциации ФинТех сформирован итоговый перечень из 9 трендов информационной безопасности.

Структура и логика исследования

Тренды кибербезопасности объединены в группы, отражающие три взаимосвязанных уровня:

- три тренда, отражающих изменение подходов атакующих группировок (#атака);
- три тренда, отражающих изменения защитных действий организаций (#защита);
- три технологических тренда, которые влияют на кибербезопасность организаций (#технологии).

Каждый тренд рассматривается с точки зрения:

- источников и драйверов;
- потенциальных векторов атак;
- влияния на киберустойчивость финансовых организаций.

ТРЕНДЫ КИБЕРБЕЗОПАСНОСТИ ФИНАНСОВОЙ ОТРАСЛИ В 2026 ГОДУ

#АТАКА

1. Рост числа каскадных комбинированных атак на экосистемы организаций
2. Хактивизм, усиленный финансовой поддержкой
3. Эпидемия киберпреступности, усиленная искусственным интеллектом

#ЗАЩИТА

4. Экосистемная киберустойчивость и централизованное управление информационной безопасностью
5. Развитие национальной инфраструктуры противодействия кибератакам
6. Фокус на измеримой защите и управлении киберрисками

#ТЕХНОЛОГИИ

7. Проактивная кибербезопасность
8. Неконтролируемое применение недоверенного ИИ
9. Развитие платформ безопасности искусственного интеллекта

pt

АССОЦИАЦИЯ ФИНТЕХ

#АТАКА

1. Рост числа каскадных комбинированных атак на экосистемы организаций

2. Хактивизм, усиленный финансовой поддержкой

3. Эпидемия киберпреступности, усиленная искусственным интеллектом

Тренды, отражающие изменение подходов атакующих группировок в 2026 году

#АТАКА

В 2026 году действия атакующих группировок все меньше укладываются в модель одиночных, изолированных атак. Злоумышленники переходят **к каскадным комбинированным сценариям,** выстроенным вокруг экосистем организаций: подрядчиков, дочерних ИТ-компаний, аутсорсеров, облачных сервисов и цепочек поставок. Цель таких атак — не просто компрометация периметра, а остановка критически значимых бизнес-процессов, создание эффекта домино и максимизация совокупного ущерба, включая операционные, финансовые и репутационные потери.

Параллельно меняется и **мотивационная модель атакующих.** Граница между хактивизмом и финансово мотивированными группировками размывается: идеологически окрашенные атаки все чаще получают устойчивое финансирование, а классическая киберпреступность заимствует риторику и тактики хактивистов. В результате организации сталкиваются с более агрессивными, более публичными и разрушительными кампаниями, в которых давление оказывается не только через ИТ-системы, но и через медиаэффекты, утечки и дестабилизацию доверия.

Отдельным ускорителем эволюции атак становится **массовое применение искусственного интеллекта.** Генеративные модели позволяют злоумышленникам кратно масштабировать фишинг, автоматизировать разведку, создавать реалистичные дипфейки и быстро адаптировать сценарии под конкретные организации и сотрудников. Это формирует эффект эпидемии киберпреступности, когда порог входа снижается, скорость атак растет, а традиционные защитные меры все чаще оказываются реактивными и запаздывают.

Дмитрий Машков
Руководитель Центра
кибербезопасности
АО «Россельхозбанк»

«В условиях геополитической напряженности значительно возросла нагрузка на кибер-пространство. Изменилась и роль специалиста по информационной безопасности в организациях: сейчас от него ожидается в первую очередь не комплаенс и соответствие всех документов регуляторным требованиям „на бумаге“, а именно прикладной кибербез, так как руководству организаций важно понимать состояние реальной защищенности. Во многих организациях развитию ИБ стало уделяться серьезное внимание, но все еще зачастую это происходит после реализованного компьютерного инцидента с эксфильтрацией или шифрованием инфраструктуры.

Современная кибератака — это, как правило, детально продуманная кампания, которая намеренно растягивается во времени для снижения вероятности обнаружения и затрагивает сразу несколько уровней организации: от ИТ-систем до бизнес-процессов и репутации.

В сложившихся условиях выстраивание контура защиты подразделениями кибербезопасности на основе процесса отслеживания применимого к организации ландшафта киберугроз и адекватной модели угроз становится необходимостью, как и доскональный анализ всех аномалий, фиксируемых в информационной инфраструктуре».

Дмитрий Миклухо
Старший вице-президент-руководитель блока информационной безопасности ПАО «БАНК ПСБ»

«Тренды атак показывают: чем умнее ИИ в защите, тем изощреннее социальная инженерия. Развитие ИИ в средствах защиты резко снизило эффективность классических техник атакующих, при этом одновременно повысило ценность человеческого фактора. Когда алгоритмы успешно отслеживают аномалии в коде, трафике и поведении систем, злоумышленники смещают акцент на манипуляцию доверием, контекстом и привычками сотрудников. Социальная инженерия становится более персонализированной и правдоподобной, часто неотличимой от легитимных рабочих коммуникаций. В результате ИИ усиливает технологическую безопасность, но делает человека ключевой и самой сложной для автоматизации точкой защиты.

Сегодня самый популярный эксплойт — доверие к тому, что система „уже защищена“. Современные атаки все чаще эксплуатируют не уязвимости в технологиях, а уверенность организаций в достаточности уже внедренных мер безопасности. Наличие средств защиты создает иллюзию контроля, за которой скрываются устаревшие настройки, неиспользуемые учетные записи, исключения в политиках и отсутствие регулярной проверки реальной эффективности защиты. Злоумышленники используют именно это доверие — не ломая систему, а работая в ее допустимых границах. Таким образом, ключевая уязвимость находится не в инфраструктуре, а в предположении, что защита по умолчанию означает безопасность».

Рост числа каскадных комбинированных атак на экосистемы организаций

#АТАКА

Суть тренда

В результате регулярного мониторинга киберугроз в финансовом секторе выявлено, что фокус злоумышленников сместился с нанесения прямого материального ущерба на оказание деструктивного воздействия (например, выведение из строя критически значимых информационных систем), а также на причинение репутационного вреда. Все чаще хакеры атакуют не только головной офис предприятия, но и менее защищенные филиалы, дочерние компании или вендоров. Цель — скомпрометировать инфраструктуру, чтобы таким образом вызвать каскадные сбои и нарушить критически важные процессы организации или целой отрасли.

Специфика тренда

Злоумышленники проводят комбинированные атаки для воздействия на операционную деятельность организации: например, выводят ресурсы из строя, генерируя множество запросов к ним, или шифруют данные с помощью вируса. Затем выдвигают требования о выкупе для остановки атаки, расшифровки данных или предотвращения их публикации.

Так как уровень защищенности крупных финансовых организаций высок, растет число атак на цепочки поставок. Злоумышленники компрометируют инфраструктуру филиалов, дочерних организаций, подрядчиков и партнеров, защита которых может быть слабее. Это позволяет внедрить вредоносный код в разрабатываемое ПО и инфраструктуру, похитить конфиденциальные данные или парализовать работу поставщика, что отражается на деятельности головных или клиентских организаций.

Предложения

Рекомендуется регулярно проверять реальное состояние защищенности как собственной организации, так и дочерних компаний, поставщиков и подрядчиков. На основании полученной информации следует разрабатывать компенсирующие меры и внедрять лучшие практики для устранения выявленных уязвимостей. Следующий шаг — выход на платформы bug bounty и проведение кибериспытаний для проверки критически значимых процессов и инфраструктуры.

На что обратить внимание

Бизнесу

- Непрерывность деятельности
- Доверие к бренду
- Управление рисками
- Надежность цепочки поставок

Специалистам по ИБ

- Двойное мошенничество
- Рост числа DDoS-атак на API
- Атаки на поставщиков и партнеров
- Киберустойчивость критически важных процессов

Факты

Ноябрь 2025 года. Из-за атаки на ИТ-инфраструктуру ресурсы Страхового Дома ВСК были недоступны на протяжении недели. По заявлениям генерального директора, организация была не готова к угрозам такого масштаба.

2025 год. В топ-3 последствий кибератак на финансовые организации вошли утечка конфиденциальных данных, нарушение основной деятельности и прямые финансовые потери. По информации StormWall, число DDoS-атак во втором квартале 2025 года увеличилось на 42% по сравнению с тем же периодом 2024 года.

Июнь 2024 года. В результате DDoS-атаки на протяжении нескольких часов наблюдались сбои в работе СБП и других связанных с ней сервисов. НСПК подтвердила инцидент, отметив его кратковременный характер и ограниченное влияние.

Недопустимые события

Прерывание деятельности

- Остановка работы финансовых сервисов
- Простой в работе корпоративной инфраструктуры
- Перебои в работе цифровой экосистемы (организации или ее партнеров)

Утечка конфиденциальной информации

- Кража информации, составляющей банковскую тайну
- Кража персональных данных клиентов банка

Финансовые потери

- Вывод денежных средств с корреспондентского счета банка
- Вывод денежных средств со счетов клиентов банка

«Обзор основных типов компьютерных атак в финансовой сфере в 2024 году» — Банк России

«CODE RED 2026: актуальные киберугрозы для российских организаций» — Positive Technologies

«Киберугрозы финансовой отрасли: прогноз на 2025–2026 годы» — Positive Technologies

Хактивизм, усиленный финансовой поддержкой

#АТАКА

Суть тренда

Анализ ландшафта киберугроз за 2025 год указывает на трансформацию тактик злоумышленников: часть хактивистов начала применять методы вымогательства, ранее характерные для деятельности финансово мотивированных группировок. Сохраняя векторы атак, они шифруют и похищают данные, после чего требуют выкуп за восстановление доступа или за предотвращение их публикации.

Специфика тренда

В России 30 мая 2025 года увеличились штрафы за утечки данных: взыскания за повторные утечки могут достигать 500 млн ₽, что усиливает давление на организации.

В описанных условиях злоумышленники рассматривают инциденты с данными как эффективный инструмент монетизации. В рамках одной кампании преступники могут сначала украсть чувствительную информацию, затем нарушить работу инфраструктуры жертвы, использовать похищенные сведения для шантажа и получения выкупа, а после — множество раз продать базу третьим лицам и сохранить данные для повторного применения в целевых или массовых атаках.

Кроме того, часть данных попадает на рынки обогащенных баз — агрегированных массивов, в которых сведения, полученные из разных утечек, объединяются и дополняются.

Ожидается, что в 2026 году хактивистские группировки все чаще будут прибегать к раскрытию украденных данных, используя их публикацию как инструмент давления на организации для нанесения репутационного и финансового ущерба.

Предложения

- **Провести харденинг ИТ-инфраструктуры:** настроить параметры безопасности сетей, систем и сервисов.
- **Провести обучение практикам кибербезопасности:** правильные действия сотрудников, точно знающих, как не стать жертвами хакеров, снижают количество успешных кибератак на организацию.
- **Обеспечить мониторинг и своевременное реагирование на инциденты:** чем раньше будет обнаружена атака, тем меньший ущерб она нанесет.
- **Обеспечить непрерывность бизнеса:** следует подготовить и проверить системы резервного копирования.

На что обратить внимание

Бизнесу

- Санкции за утечки информации
- Репутационный ущерб
- Двойное вымогательство

Специалистам по ИБ

- Рост числа DDoS-атак и атак с применением вирусов-шифровальщиков, вайперов ①
- Защита чувствительной информации и персональных данных
- Повышение осведомленности сотрудников организации в части ИБ

① Вайперы — это класс ВПО, предназначенный для стирания данных.

Факты

2025 год. По данным Минцифры, озвученным в марте, прямой ущерб, нанесенный хакерами российской экономике за предыдущий год, составил от 160 до 250 млрд рублей.

Согласно исследованию BI.ZONE, в первом полугодии 2025 года каждая пятая кибератака на российские организации была совершена хактивистскими группировками.

«Лаборатория Касперского» отмечает, что с 2022 года Россия является одной из самых атакуемых стран в киберпространстве, а хактивизм остается основной угрозой для российских организаций.

Недопустимые события

Прерывание деятельности

- Остановка работы финансовых сервисов
- Простой в работе корпоративной инфраструктуры
- Перебои в работе цифровой экосистемы (организации или ее партнеров)

Утечка конфиденциальной информации

- Кража информации, составляющей банковскую тайну
- Кража персональных данных клиентов банка

«CODE RED 2026: актуальные киберугрозы для российских организаций» — Positive Technologies

«Хактивисты стоят за 20% атак на российские компании в 2025 году» — Anti-Malware.ru

«Ландшафт угроз в 2026-м: внимание на Россию» — Хабр

«Киберугрозы-2025: F6 назвала основные тренды вымогателей, утечек и фишинга» — F6

«Записки цифрового ревизора: три кластера угроз в киберпространстве» — «Лаборатория Касперского»

Эпидемия киберпреступности, усиленная искусственным интеллектом

#АТАКА

Суть тренда

① Искусственный интеллект (ИИ) — комплекс технологических средств, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их.

Искусственный интеллект ① существенно расширил возможности киберпреступников, упростив создание фишинговых сообщений, подделку голоса и видео, а также разработку вредоносного ПО. В результате порог входа в киберпреступную деятельность снизился, а сложность, число и масштаб атак заметно возросли. Ситуация усугубляется тем, что механизмы контроля применения ИИ, включая инструменты выявления сгенерированного контента и ограничения использования ИИ для потенциально чувствительных задач, недостаточно зрелые. В ближайшие годы эта тенденция будет только усиливаться.

Специфика тренда

Несмотря на ограниченное применение ИИ в кибератаках, потенциальные возможности технологии огромны. Киберпреступники активно используют новые методы и не оставляют попыток повысить свою продуктивность за счет внедрения искусственного интеллекта.

Большие языковые модели могут помочь киберпреступнику-новичку разобраться в основах: они способны представить необходимую информацию в сжатом виде и быстро ответить на базовые вопросы. Помимо этого, ИИ помогает составить профиль жертвы и сформировать сценарии для атак с применением социальной инженерии.

Злоумышленники генерируют фишинговые сообщения и дипфейки, автоматизируют работу мошеннических аккаунтов, эксплуатацию уязвимостей, сбор и анализ информации о жертве.

Киберпреступники могут использовать ИИ в качестве цифрового ассистента, а также генерировать с помощью него вредоносный контент. Искусственный интеллект способен как подсказывать оптимальные действия человеку, так и выполнять за него простые операции. К примеру, ИИ уже используется для генерации скриптов и проверки кода при подготовке вредоносного ПО.

Предложения

Для противодействия атакам с использованием ИИ организациям необходимо:

- Встраивать процессы подтверждения личности в критически значимых процессах.
- Обучать сотрудников распознавать фишинг и дипфейки.
- Использовать решения для автоматического выявления и блокировки подозрительных операций в целях борьбы с мошенниками.
- Автоматизировать обнаружение и противодействие хакерской активности, поиск уязвимостей в инфраструктуре, а также применять СЗИ, в которые внедрены технологии ИИ.

На что обратить внимание

Бизнесу

- Рост ущерба, наносимого киберпреступлениями
- Репутационные и регуляторные риски.
- Повышение осведомленности сотрудников о новых видах мошенничества

Специалистам по ИБ

- ИИ-фишинг и скам ②
- Новые сценарии социальной инженерии
- Автоматизация киберпреступных кампаний
- Автоматизация контура защиты

② Скам — вид интернет-мошенничества, чаще всего связанный с использованием социальной инженерии для кражи денежных средств или данных жертвы.

Факты

2025 год. Киберпреступления составляют почти половину (45,8%) от всех преступлений в Москве. Наиболее распространенным видом ИТ-преступлений остаются мошенничество и кражи (76%).

За третий квартал 2025 года общий объем операций без добровольного согласия клиентов составил 8176 075,88 тыс. руб. (статистика Банка России).

2024 год. Злоумышленники, используя дипфейк-технологию, ввели сотрудника в заблуждение и под видом одного из руководителей вынудили его перевести на подставной счет 25 млн $.

Недопустимые события

Финансовые потери

- Вывод денежных средств со счетов клиентов банка
- Вывод денежных средств с корреспондентского счета банка

Утечка конфиденциальной информации

- Кража информации, составляющей банковскую тайну
- Кража персональных данных клиентов банка

«Искусственный интеллект в кибератаках» — Positive Technologies

«Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. III квартал 2025 года» — Банк России

Microsoft Digital Defense Report 2025 — Microsoft

#ЗАЩИТА

4 Экосистемная киберустойчивость и централизованное управление информационной безопасностью

5 Развитие национальной инфраструктуры противодействия кибератакам

6 Фокус на измеримой защите и управлении киберрисками

Тренды, отражающие изменения защитных действий организаций в 2026 году

#ЗАЩИТА

В 2026 году организации все отчетливее осознают ограниченность классической модели кибербезопасности, ориентированной исключительно на предотвращение атак и выполнение формальных требований регуляторов. На фоне усложнения сценариев атак, роста межорганизационных рисков и зависимости от цифровых экосистем фокус защиты смещается в сторону **киберустойчивости** — способности сохранять и быстро восстанавливать критически важные функции даже при успешных атаках. Это приводит к переходу от фрагментированной защиты отдельных систем к централизованному управлению безопасностью на уровне процессов, цепочек поставок и отраслевых экосистем.

Параллельно развивается **национальная и отраслевая инфраструктура противодействия кибератакам,** обеспечивающая обмен данными о киберинцидентах, координацию реагирования и единые подходы к оценке угроз. Организации все чаще рассматривают кибербезопасность не как сугубо внутреннюю функцию, а как элемент коллективной защиты — с участием регуляторов, отраслевых центров, вендоров и операторов критической информационной инфраструктуры. Это в совокупности с политикой технологического суверенитета повышает защищенность российских финансовых организаций.

Ключевым сдвигом становится переход **к измеримой и управляемой защите,** основанной на анализе рисков и недопустимых событий, а не на перечнях средств и чек-листах. В 2026 году все больше организаций стремятся отвечать не на вопрос «соответствуем ли мы требованиям?», а на вопрос «что именно мы не можем себе позволить потерять и насколько готовы к этому сценарию?». Это трансформирует ИБ из затратной функции в управляемый элемент бизнес-устойчивости, непрерывности деятельности организации и стратегического управления.

Дмитрий Никишов
Вице-президент по информационной безопасности АО «Банк ДОМ.РФ»

«Новые вызовы, с которыми мы сталкивались в этом году — от распределенных атак до атак на цепочки поставок, — требуют от нас оперативного ответа и действий на опережение. Мы активно модернизируем классическую экосистему защиты: отказываемся от «веры в технологии» в пользу доказуемой эффективности. Наш фокус заострен на прозрачных, измеримых мерах, ценность которых понятна бизнесу, а результат виден невооруженным взглядом. Мы сверяем наши шаги с актуальной картой угроз и свежими бенчмарками, чтобы обеспечить действительно качественную отдачу от вложенных в защиту ресурсов. Наш новый принцип: защита должна быть обоснованной, подотчетной и результативной».

Сергей Крамаренко
Руководитель департамента
кибербезопасности
АО «АЛЬФА-БАНК»

«В 2025 году наиболее заметной тенденцией, на наш взгляд, стал каскад сложных комбинированных кибератак через внешних партнеров, подрядчиков, дочерние структуры и доверенные интеграции организаций. Атаки все реже направлены на преодоление фронтальных защитных мер и воздействие на отдельные системы и сервисы, но все чаще сфокусированы на остановке деятельности или коллапсе критичных бизнес-процессов. В текущих условиях полное восстановление бизнес-деятельности после успешной реализации хакерами таких атак может занимать существенное время и требовать значительных затрат и усилий. Не можем не отметить влияния на киберсреду факта использования злоумышленниками ИИ. В частности, генеративные технологии позволяют атакующим создавать эффективные фишинговые сценарии, искать уязвимости, разрабатывать и отлаживать вредоносный код, проводить разведку и многое другое, снижая порог необходимых навыков и компетенций.

В результате ключевыми факторами успешного противостояния хакерам становятся скорость обнаружения и эффективного реагирования на кибератаки, быстрое и скоординированное принятие решений в условиях высокой неопределенности, повышение уровня киберграмотности персонала, ответственное выстраивание партнерских отношений, превентивное планирование, организация и реализация комплекса мероприятий, направленных на противодействие актуальным киберугрозам с использованием ИИ как средства защиты активов компаний».

Экосистемная киберустойчивость и централизованное управление информационной безопасностью

#ЗАЩИТА

Суть тренда

Тренд отражает переход от локального обеспечения ИБ к управлению рисками на уровне всей группы компаний. Киберустойчивость рассматривается как свойство единой экосистемы, где сбой в одном звене способен привести к каскадным последствиям: к остановке бизнес-процессов, нарушению цепочек поставок, финансовым потерям и реализации регуляторного риска для всего холдинга. В таких условиях эффективная защита возможна только при централизованном управлении безопасностью. Этого можно добиться либо большими инвестициями в создание своего центра противодействия киберугрозам, либо путем обращения к масштабируемым сервисным моделям безопасности и облачным решениям.

Специфика тренда

Крупные группы компаний переходят к централизованной модели управления кибербезопасностью: она предусматривает формирование единых стандартов и требований для всех организаций холдинга, совместный мониторинг и реагирование на инциденты. Особое внимание уделяется защите общих ИТ-платформ и внешних сервисов, от которых зависят ключевые бизнес-процессы.

В связи с этим в ближайшее время ожидается усиление фокуса на обеспечении ИБ не только собственной инфраструктуры, но и инфраструктуры всех участников цепочки поставок и дочерних организаций. Для реализации такого подхода компании будут все активнее внедрять следующие меры:

- Расширенное применение практик управления рисками третьих лиц.
- Внедрение единых стандартов ИБ для всех дочерних и партнерских организаций.
- Создание единых центров противодействия киберугрозам для непрерывного и централизованного мониторинга.
- Использование сервисной модели безопасности.
- Обеспечение защищенности облачных сервисов.
- Регулярная оценка уровня защищенности.
- Выход организаций с наиболее значимыми процессами на публичные платформы для поиска уязвимостей.

Предложения

Для поддержания киберустойчивости рекомендуется:

- Внедрять и тиражировать лучшие практики ИБ для филиалов, партнеров и клиентов.
- Обеспечить централизованный мониторинг событий безопасности на уровне холдинга.
- Проводить регулярные аудиты, оценивать зрелость процессов ИБ дочерних и партнерских организаций.
- Проводить киберучения для оценки эффективности защитных мер.

На что обратить внимание

Бизнесу

- Управление рисками третьих лиц (TPRM)
- Сервисная модель обеспечения безопасности (MSSP)
- Учет киберинцидентов как бизнес-риска

Специалистам по ИБ

- Тиражирование лучших практик ИБ для филиалов, партнеров и клиентов
- Централизованный мониторинг событий безопасности
- Регулярные аудиты безопасности дочерних и партнерских организаций

Факты

2025 год. Toppan Next Tech, компания, отвечавшая за печать клиентских документов для Development Bank of Singapore и Bank of China, стала жертвой атаки программы-вымогателя. Под угрозой оказались данные более 11 000 клиентов.

2024 год. Согласно отчету Банка России о кибератаках в финансовой сфере за 2024 год, компрометация подрядчиков стала самым частым способом получения первоначального доступа к финансовым организациям страны.

Атака группировки вымогателей RansomEXX на поставщика банковских технологических систем C-Edge Technologies привела к сбою в предоставлении финансовых услуг примерно в 300 небольших банках в Индии.

«Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года» — Positive Technologies.

«Обзор основных типов компьютерных атак в финансовой сфере в 2024 году» — Банк России.

Развитие национальной инфраструктуры противодействия кибератакам

#ЗАЩИТА

Суть тренда

Наиболее часто встречающийся формат совместной деятельности по предотвращению инцидентов — создание единых центров реагирования, позволяющих своевременно выявлять масштабные атаки и минимизировать их ущерб. Подобные центры существуют в рамках как отдельных компаний, так и целых отраслей. ФинЦЕРТ — показательный пример для финансового сектора. Иные методы взаимодействия включают обмен данными об атаках и акторах, индикаторами компрометации и унификацию стандартов в сфере менеджмента инцидентов.

Специфика тренда

Работу в части совместного отражения атак и обмена знаниями активно продвигают государственные структуры (ФСТЭК, ФСБ, Банк России, Минцифры России и другие регуляторы). Более того, при их поддержке создаются единые хранилища данных об угрозах, доступные и для государственных, и для частных организаций.

Со стороны государства также прослеживается тренд на предоставление компаниям общих ресурсов для противодействия кибератакам. В рамках такого подхода реализуются и развиваются следующие инициативы:

- Интеграция инфраструктуры организаций с ГосСОПКА.
- Создание ГИС «Антифрод» (цель — объединить операторов связи, банки и государственные органы для борьбы с мошенничеством).
- Разработка отраслевых стандартов информационной безопасности.
- Проведение киберучений национального уровня.
- Создание программ для повышения осведомленности в области ИБ, а также для формирования базовых навыков кибергигиены.

Описанная активность коррелирует с ростом инвестиций в отечественные технологии в рамках концепции технологического суверенитета. Все эти действия позволяют добиться более высокого уровня защищенности и независимости от внешних поставщиков и параллельно дают возможность развития отечественным игрокам рынка ИБ. В условиях геополитической напряженности и стремительного усложнения угроз коллективная безопасность становится первым приоритетом.

На что обратить внимание

Бизнесу

- Своевременное информирование регуляторов об инцидентах
- Развитие каналов коммуникаций с регуляторами
- Отслеживание новых требований регуляторов

Специалистам по ИБ

- Обмен опытом в части практик защиты организаций
- Участие регулятора в работе группы реагирования на инциденты
- Проведение совместных учений

Факты

2025 год. Переход от реактивной модели реагирования к проактивной кооперации — расширение обмена данными с НКЦКИ о кибератаках и инцидентах.

В настоящее время к системе ГосСОПКА подключено более 90 организаций, осуществляющих взаимодействие в рамках выявления, предупреждения и реагирования на компьютерные атаки.

С 1 сентября микрофинансовые организации должны подключиться к АСОИ ФинЦЕРТ. Это позволит МФО получать доступ к данным о подозрительных операциях и использовать их для выявления признаков мошенничества.

Принят федеральный закон о создании ГИС «Антифрод», позволяющей госорганам, банкам, операторам связи и другим компаниям автоматически обмениваться данными о мошеннических схемах.

Указ Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации»

«Обзор основных типов компьютерных атак в финансовой сфере в 2024 году» — Банк России

Фокус на измеримой защите и управлении киберрисками

#ЗАЩИТА

Суть тренда

Рост последствий атак приводит к тому, что по значимости киберриски все чаще становятся в один ряд с финансовыми и операционными угрозами. Атаки не только затрагивают данные и ИТ-системы — они приводят к остановке бизнес-процессов, нарушению цепочек поставок, влекут за собой штрафы и прямые финансовые потери, которые могут измеряться миллионами рублей в сутки.

Помимо этого, из-за высокой стоимости денег акционеры организаций считают инвестиции и экономические метрики на обеспечение информационной безопасности.

Специфика тренда

Большой бюджет на кибербезопасность сам по себе не гарантирует киберустойчивости. В условиях растущего числа киберугроз компании переходят от формального подхода к обеспечению ИБ к измеримой модели, при которой важно не просто наличие средств защиты, а их реальная эффективность и способность снижать ущерб.

Чтобы измерить эффективность защиты, оценить реальную устойчивость инфраструктуры и работу SOC, организации выбирают разные способы: например, **проведение пентестов и киберучений, выход на площадки багбаунти.** Результаты подобных проверок позволяют определить возможные векторы атак и посчитать такие показатели, как **time to attack (TTA) и time to response (TTR).**

Все больше компаний стремится к тому, чтобы время, необходимое для успешной атаки, превышало время реагирования и остановки хакеров. Это свидетельствует о росте зрелости рынка и более осознанным инвестициям в кибербезопасность.

Снижение рисков

Атаки влияют на деятельность организации, могут нарушить бизнес-процессы и привести к крупным финансовым потерям.

В этих условиях измеримая кибербезопасность становится основой для развития страхования киберрисков. Страховые компании оценивают не наличие мер защиты, а зрелость процессов ИБ, устойчивость к инцидентам и потенциальный масштаб ущерба. Условия и стоимость покрытия напрямую зависят от управляемости киберрисков, подтвержденной результатами тестов, сценариев атак и показателями реагирования.

На что обратить внимание

Бизнесу

- Управление и страхование киберрисков
- Прогнозируемость инвестиций в кибербезопасность
- Бенчмаркинг и оценка эффективности

Специалистам по ИБ

- Подтверждение киберустойчивости: проведение киберучений, выход на платформы багбаунти
- Анализ эффективности процессов ИБ
- Практико-ориенированное подтверждение защиты организации

Факты

2025 год. «Т-Технологии» первыми среди финтех-компаний запустили новую программу в формате кибериспытаний

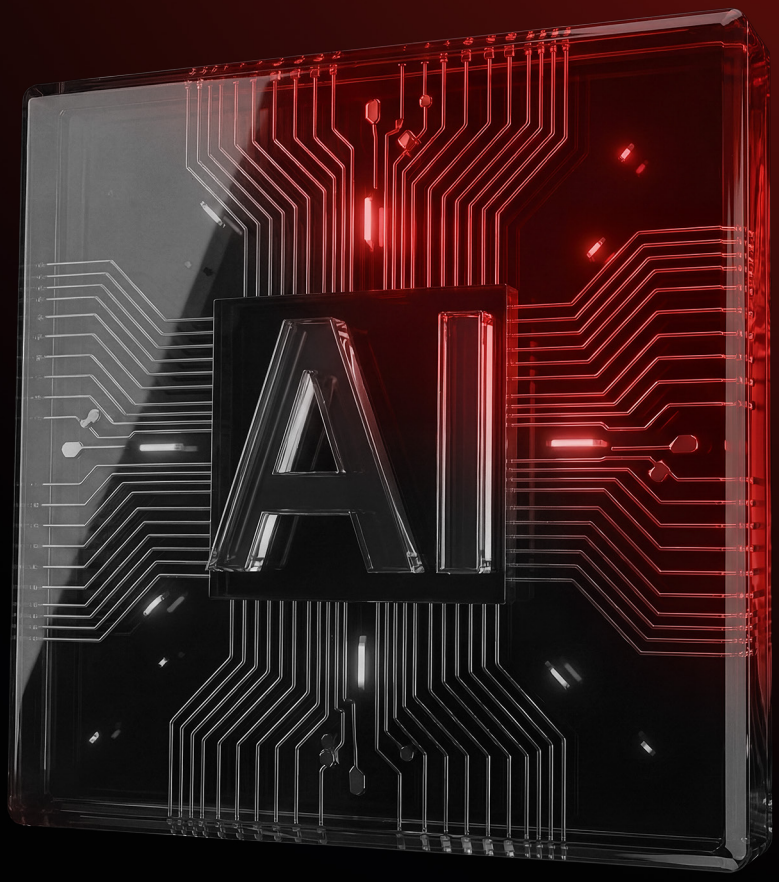
Дополнительный индикатор развития рынка — рост выплат исследователям: по итогам года совокупный объем вознаграждений на платформах Standoff Bug Bounty и BI.ZONE Bug Bounty превысил 300 млн руб.

«Анатомия цифровых бурь: как превратить хаос в киберустойчивость» — Positive Technologies

«Зачем нужны метрики работы с инцидентами в security operations center» — Хабр

«Обзор программ и площадок баг-баунти в России: практика, кейсы, суммы гонораров» — Anti-Malware.ru

#ТЕХНОЛОГИИ



7 Проактивная кибербезопасность

8 Неконтролируемое применение недоверенного ИИ

9 Развитие платформ безопасности искусственного интеллекта

Технологические тренды, которые влияют на кибербезопасность организаций

#ТЕХНОЛОГИИ

В 2026 году технологические изменения становятся одним из ключевых драйверов трансформации кибербезопасности — как с точки зрения возможностей защиты, так и с точки зрения появления новых классов рисков. Рост сложности ИТ-ландшафтов, активное внедрение ИИ и автоматизации, а также ускорение цифровых процессов приводят к ситуации, в которой традиционные реактивные модели ИБ перестают справляться с масштабом и скоростью происходящих изменений. Формируется запрос **на проактивную кибербезопасность,** основанную на прогнозировании, моделировании сценариев и опережающем выявлении уязвимостей.

Одновременно усиливается проблема **неконтролируемого применения недоверенного искусственного интеллекта** внутри организаций. Генеративные модели и ИИ-сервисы все чаще используются сотрудниками без формализованных правил, оценки рисков и встроенных механизмов контроля. Это создает новые векторы утечек данных, риск подмены решений и скрытых уязвимостей, смещая фокус ИБ с внешнего противника на внутренние технологические риски и управляемость цифровых инструментов.

Ответом на эти вызовы становится **развитие платформ безопасности искусственного интеллекта,** объединяющих контроль жизненного цикла ИИ-моделей, мониторинг их поведения и интеграцию с корпоративными средствами защиты. В 2026 году ИИ все чаще рассматривается не только как объект защиты, но и как активный элемент самой системы кибербезопасности, способный усиливать аналитику, автоматизировать реагирование и поддерживать принятие решений в условиях высокой неопределенности.

Дмитрий Гадарь
Руководитель департамента
информационной безопасности
АО «Т-Банк»

«Ключевой тренд 2026 года — переход от точечной защиты ИИ к платформенному и продуктовому подходу. Безопасность закладывается непосредственно в AI-платформы и жизненный цикл продуктов: на уровне обучения моделей, инференса, RAG-сценариев и интеграций с бизнес-системами. Используются единые политики доступа, изоляция сред, контроль данных и цепочек поставок, а также встроенные security guardrails, ограничивающие недопустимое поведение ИИ.

Отдельным направлением станет применение ИИ для защиты ИИ. В 2026 году этот вектор будет развиваться: атакующие ИИ-агенты будут использоваться для поиска уязвимостей, а ИИ-ассистенты (такие как Safeliner) будут помогать в разработке — анализировать исходный код, находить потенциальные уязвимости и помогать устранять их до выхода продукта в продакшен.

В итоге угрозы, связанные с ИИ, перестанут рассматриваться как отдельная тема. Они станут частью общей продуктовой безопасности, реализуемой по принципу defense in depth, когда устойчивость обеспечивается архитектурой, платформами и процессами, а не отдельными защитными инструментами».

Сергей Демидов

Заместитель Председателя Правления
по информационной безопасности
ПАО «Московская Биржа»

«Сегодня технологии меняют саму логику кибербезопасности. Искусственный интеллект и автоматизация перестали быть просто вспомогательными инструментами: они становятся базой, на которой строятся и атаки, и защита. В результате борьба все чаще идет не за периметр, а за скорость обнаружения, качество аналитики и умение работать с данными.

Ключевая задача для организаций — удержать баланс между внедрением новых технологий и управляемостью рисков. Недостаточно просто „добавить ИИ“ в процессы безопасности: компании вынуждены пересматривать архитектуру ИТ, модели реагирования и подходы к управлению инцидентами, чтобы технологии действительно усиливали защиту, а не создавали новые точки уязвимости.

Поэтому стратегия информационной безопасности сегодня — это уже не набор регламентов, а часть технологического развития бизнеса. Тот, кто заранее адаптирует свои подходы ИБ под изменения в технологиях, получает не только более высокий уровень защиты, но и устойчивость к тем рискам, которые еще только формируются».

Проактивная кибербезопасность

#ТЕХНОЛОГИИ

Суть тренда

Технологии искусственного интеллекта повышают эффективность как атакующих, так и защитников. Применение ИИ значительно расширило ландшафт киберугроз: злоумышленники получили возможность быстро автоматизировать и масштабировать атаки. Вместе с тем использование искусственного интеллекта для защиты способствует автоматизации обнаружения и блокировки подозрительной активности, снижает нагрузку на команды кибербезопасности и повышает скорость реагирования на инциденты.

Специфика тренда

В сфере ИБ технологии искусственного интеллекта дополняют и расширяют возможности классических решений для защиты:

- **Первичная обработка событий и снижение нагрузки на SOC:** сортировка событий, обогащение их контекстом, снижение доли информационного шума.
- **Поведенческий анализ пользователей:** построение профиля нормальной активности пользователей и систем, выявление аномалий, которые могут указывать на атаку.
- **Анализ аномалий в потоках данных:** поиск признаков вредоносной активности, в том числе ранее неизвестных угроз, в трафике, журналах и поведении процессов.
- **Чат-бот — помощник:** ответы на вопросы, объяснение срабатываний и помощь в принятии решений.
- **Автоматическое реагирование:** обучение на конкретных действиях команды защиты при определенных типах инцидентов и повторение этих действий, генерация плейбуков в зависимости от действий хакера и атакуемых ресурсов.
- **Автопентест:** автоматизация отдельных шагов тестирования на проникновение.
- **OSINT и предиктивная аналитика:** определение трендовых уязвимостей и угроз по открытым источникам, предложение мер по их устранению.
- **Контроль утечек и конфиденциальности:** анализ больших объемов информации, распознавание в них чувствительных данных и предотвращение утечек.

Предложения

Интеграция ИИ в процессы и системы обеспечения кибербезопасности возможна как на базе решений вендоров, так и за счет собственных разработок, при этом на практике выделяются два ключевых сценария его применения.

- **Автоматизация.** Направлена на снижение ручной нагрузки и на ускорение реагирования. При наличии качественных данных ML-алгоритмы способны выявлять аномалии и векторы атак, выполнять корреляцию событий, приоритизировать инциденты и автоматически на них реагировать.
- **Аугментация.** Предполагает использование ИИ-ассистентов, развернутых во внутренней инфраструктуре и обученных на данных организации. Они облегчают работу специалистов по ИБ и других команд, помогают анализировать данные, обогащают сведения об инцидентах дополнительной информацией и предлагают разные варианты решений.

На что обратить внимание

Бизнесу

- Инвестиции в СЗИ на основе технологий ИИ
- Подготовка инфраструктуры для ИИ
- Повышение качества данных для использования ИИ

Специалистам по ИБ

- Использование ИИ для обнаружения аномалий в поведении пользователей и систем
- Снижение нагрузки на аналитиков SOC
- Автоматизация систем защиты

Факты

2025 год. На российском рынке сформировался отдельный сегмент СЗИ с применением ИИ, включающий более 20 решений от ведущих отечественных вендоров, таких как **Positive Technologies, R-Vision, BI.ZONE, «Лаборатория Касперского», «СерчИнформ»** и других. Эти решения направлены на проактивное выявление угроз, прогнозирование атак и повышение киберустойчивости организаций.

Хотя специализированный сегмент защиты ИИ еще формируется, уже фиксируется рост инвестиций в ключевые технологии ИИ-безопасности в России, включая:

- разработку ИИ-алгоритмов для обнаружения угроз и автоматизации реагирования;
- создание инструментов контроля и защиты ИИ-систем и данных;
- интеграцию ИИ-компонентов в отечественные СЗИ.

«Искусственный интеллект в киберзащите» — Positive Technologies.

Staying Ahead of Threat Actors in the Age of AI — Microsoft Threat Intelligence.

Russia AI-Enabled Cyber Defense Platforms Market — Ken Research

Неконтролируемое применение недоверенного ИИ

#ТЕХНОЛОГИИ

Суть тренда

Теневой ИИ (shadow AI) — это явление, при котором сотрудники организаций используют внешние ИИ-сервисы и модели без согласования с ДИТ и ДИБ. В процессе работы сотрудники могут выгружать в такие сервисы конфиденциальные сведения, защищенные законодательством, исходный код разрабатываемого ПО, API-ключи, персональные данные, результаты интеллектуальной деятельности и иную чувствительную информацию. Подобная практика приводит к утрате контроля над данными, к нарушению требований по их защите и к компрометации ресурсов организации.

Специфика тренда

Финансовая отрасль относится к числу наиболее уязвимых к проявлениям недоверенного ИИ из-за высокой концентрации структурированных и чувствительных данных, используемых в операционной, аналитической и клиентской деятельности.

В последние годы наблюдается стремительное распространение генеративных ИИ-сервисов. Многие организации признают их практическую ценность, развертывая корпоративные ИИ-решения внутри собственной инфраструктуры.

В то же время такие модели нередко имеют функциональные ограничения, ограничения по части производительности и доступности и требования к согласованию запросов. В результате сотрудники обращаются к внешним ИИ-сервисам, доступ к которым может быть ограничен корпоративными политиками безопасности. Для обхода подобных ограничений могут использоваться специальные средства. Кроме того, иногда сотрудники копируют рабочие данные на личные устройства для последующего анализа вне корпоративного периметра.

В обоих случаях информация выводится за пределы контролируемой среды организации — это приводит к потере прозрачности обработки данных, повышает риск их компрометации или искажения и напрямую нарушает требования ИБ.

Предложения

- Разработать политику применения ИИ в организации.
- Адаптировать существующие политики кибербезопасности к рискам, связанным с использованием ИИ.
- Обучить сотрудников правилам обращения с ИИ в корпоративной среде.
- Провести инвентаризацию и категорирование информационных активов.

На что обратить внимание

Бизнесу

- Политика и контроль использования ИИ
- Создание корпоративной культуры использования ИИ и обучение сотрудников
- Обработка чувствительных данных во внутреннем контуре организации

Специалистам по ИБ

- Утечки конфиденциальных данных
- Контроль использования мобильных устройств
- Адаптация каналов мониторинга систем для контроля утечек

Факты

2025 год. Согласно исследованию LayerX, 45% сотрудников организаций используют инструменты генеративного ИИ, 77% этих пользователей копируют данные в чат-боты.

2024 год. По результатам опроса, проведенного Gartner, 30% респондентов столкнулись с утечкой данных в результате использования генеративных моделей ИИ.

Исследование Harmonic Security выявило, что 8,5% всех запросов к популярным генеративным моделям содержали конфиденциальные данные:

- 46% — данные клиентов.
- 27% — данные о сотрудниках.
- 15% — сведения о сделках, стратегиях и инвестициях.
- 12% — исходный код приложений, API-ключи, отчеты о состоянии безопасности.

2023 год. Сотрудники Samsung систематически выгружали в ChatGPT корпоративные данные, а также исходный код разрабатываемого ПО с целью анализа и оптимизации.

Enterprise AI & SaaS Data Security Report 2025 — LayerX

AI Apps in the Enterprise: 2024 — Netskope Threat Labs

From Payrolls to Patents: The Spectrum of Data Leaked into GenAI Copy — Harmonic Security

Развитие платформ безопасности искусственного интеллекта

#ТЕХНОЛОГИИ

Суть тренда

Массовое внедрение ML-моделей, в том числе LLM, формирует риски, которые не покрываются традиционными средствами ИБ. В ответ рынок смещается в сторону платформенных решений для безопасности искусственного интеллекта, обеспечивающих централизованный контроль, защиту и управление как внешними ИИ-сервисами, так и внутренними корпоративными моделями и приложениями.

Специфика тренда

Все чаще ИИ рассматривается не только как технологический актив, но и как самостоятельный источник угроз. Ошибки и галлюцинации моделей могут приводить к ложным выводам и решениям, манипуляции входными запросами — к обходу этических ограничений и утечкам данных, а компрометация обучающих наборов — к системным сбоям и масштабированию рисков на всю цифровую экосистему организации. В результате системы, основанные на ИИ, требуют не только защиты как ИТ-компоненты, но и постоянного контроля их поведения, результатов работы и соответствия регуляторным и этическим требованиям.

С ростом числа уязвимостей и сценариев атак возрастает потребность в платформенных решениях для безопасности ИИ, обеспечивающих централизованное управление рисками использования искусственного интеллекта, включая:

- контроль использования внешних ИИ-сервисов и внутренних корпоративных моделей,
- мониторинг изменений параметров, поведения и деградации моделей,
- оценку безопасности, качества и происхождения используемых данных,
- применение единых политик безопасности, доверия и этики на всем жизненном цикле ИИ.

Предложения

Хотя платформы безопасности ИИ только начинают появляться, организациям, использующим искусственный интеллект, необходимо заранее обеспечить контроль и сформировать меры защиты для снижения негативного влияния ИИ-систем на устойчивость бизнеса:

- Сформировать политику использования ИИ.
- Провести анализ используемых датасетов и дополнительных компонентов.
- Выстроить процесс журналирования и анализа входящих и исходящих промптов.
- Тестировать применяемые модели перед запуском.

На что обратить внимание

Бизнесу

- Определение и контроль метрик качества работы ИИ
- Анализ бизнес-рисков, связанных с применением ИИ
- Обучение сотрудников этичному и безопасному применению ИИ

Специалистам по ИБ

- Формирование доверия, безопасности и этичности применения ИИ
- Анализ используемых датасетов и других компонентов
- Контроль входящих и исходящих запросов для LLM-моделей
- Контроль соблюдения этических принципов

Факты

За последний год на российском рынке сформировался набор решений для защиты ИИ-систем, включая инструменты контроля и фильтрации запросов, обнаружения аномалий и защиты LLM-моделей: Jay Guard, HiveTrace, LLM Firewall, Kaspersky AIST и др.

По данным Ассоциации ФинТех, 25% финансовых организаций уже столкнулись с киберинцидентами, связанными с применением ИИ.

Объем инвестиций финансового сектора в технологии ИИ достиг **56,8 млрд рублей**, при этом рынок ИИ демонстрирует ежегодный рост на уровне около 30%.

«Рекомендации по безопасному внедрению ИИ-систем» — «Лаборатория Касперского»

AI Security в Финтехе — Ассоциация ФинТех, Swordfish Security

Gartner Identifies the Top Strategic Technology Trends for 2026 — Gartner

The Rise of Agentic AI Security — Reco

Краткие выводы

Результаты исследования показывают, что в 2026 году кибербезопасность финансовой отрасли России все в меньшей степени определяется формальным соответствием требованиям и все в большей — способностью организаций управляемо действовать в условиях реализованных киберинцидентов. Ключевым фактором устойчивости становится не предотвращение всех атак как таковое, а готовность предвидеть критически опасные сценарии, выявлять недопустимые события и сохранять работоспособность ключевых финансовых сервисов при их наступлении. Это требует перехода от фрагментированных мер защиты к системному управлению киберрисками, подкрепленному регулярными кибериспытаниями, практическими проверками и измеримыми метриками эффективности ИБ.

Финансовые организации, которые уже сегодня смещают фокус с защиты периметра на управление устойчивостью критически важных функций и интеграцию ИБ в бизнес-контуры и процессы принятия решений, получают долгосрочное стратегическое преимущество. Такое преимущество выражается не только в снижении операционных и системных рисков, но и в повышении доверия со стороны клиентов, партнеров и регуляторов. Настоящее исследование призвано служить практическим ориентиром для этого перехода — от реактивной модели кибербезопасности к управляемой и доказуемой киберустойчивости финансовой отрасли.

Над исследованием работали

Алексей Сидорюк
Отраслевой технический директор Positive Technologies

Алексей Выборнов
Аналитик группы международной аналитики Positive Technologies

Дарья Исламетдинова
Руководитель проектов Positive Technologies

Марианна Данилина
Руководитель управления стратегии, исследований и аналитики Ассоциации ФинТех

Александр Товстолип
Руководитель управления информационной безопасности Ассоциации ФинТех

Сергей Лапин
Эксперт по информационной безопасности Ассоциации ФинТех

Мария Чернышева
Ведущий бизнес-аналитик Ассоциации ФинТех

ptsecurity.com

fintechru.org

pt

АССОЦИАЦИЯ ФИНТЕХ

2026