Автономное инфобезопасное



Кибербезопасность в банковском секторе в 2025 году, безусловно, вышла на новый качественный уровень. Об этом можно с уверенностью говорить, анализируя кейсы внедрения защитных решений и заявления ключевых участников ИБ-рынка



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Очевидно, что в 2025 году ИИ стал полноценным участником рынка кибербезопасности. Знаковым в этом вопросе явилось выступление вице-президента по кибербезопасности СберБанка **Сергея Лебедя** на X Международной конференции AI Journey в ноябре 2025 года. Эксперт заявил: «Будущее киберзащиты — за мультиагентными системами на основе ИИ. В банке уже разработана и внедрена подобная система, которая позволяет сократить время анализа киберугроз, ускорить разработку мер противодействия, выявлять новые типы кибератак и повысить скорость реагирования на инциденты. В будущем система сможет работать автономно, без участия человека».

Кроме того, в СберБанке сообщили, что его антифрод-системы на базе ИИ помогли в 2025 году предотвратить хищения у клиентов на сумму свыше 360 млрд рублей.

Вредоносное ПО чаще всего попадает в IT-инфраструктуру банков по-прежнему благодаря «старому доброму» фишингу, поскольку, хоть технологии и меняются, суть заражения остается прежней

С чем пришлось бороться?

Какие угрозы были актуальны для финансовой сферы? В сегменте вредоносного ПО, как следует из доклада **Анастасии Понкратовой,** заместителя начальника 2-го отдела (организации расследования дистанционных хищений) Следственного департамента МВД, сделанного в декабре 2025 года в ходе форума «АнтиФрод Россия 2025», приложение для захвата, мониторинга и анализа NFC-трафика NFCGate заняло 52,4% по распространенности среди «профильного» вредоносного ПО.

Эксперты в области ИБ крайне осторожно дают комментарии касательно NFCGate. Тем не менее **Георгий Дорофеев,** заместитель директора операционно-технологического департамента НСПК, в интервью «Б.О» посчитал необходимым дать участникам антифрод-рынка некоторую информацию по этому поводу.

Проблема достигла такого уровня, что в июне на ПМЭФ-2025 **Дмитрий Дубынин,** генеральный директор НСПК, сообщил в интервью каналу «Россия-24», что НСПК совместно с ВТБ начала тестирование и внедрение новой технологии, способной выявлять банковские операции, совершаемые под влиянием мошенников с зараженных устройств.

Анастасия Понкратова в своем выступлении назвала и второе по распространенности вредоносное ПО: банковский троян Mamont с «долей рынка» в 38,7%. По данным «Лаборатории Касперского», троян может получить доступ к SMS и push-уведомлениям на зараженном Android-смартфоне для кражи средств через SMS-банкинг. Mamont способен и «угнать» аккаунт в мессенджерах. Для борьбы с угрозой ИБ-эксперты настоятельно рекомендуют включить двухфакторную аутентификацию в банковских приложениях. А в МВД признали, что в области защиты мобильных платформ есть над чем поработать.

Как вредоносное ПО чаще всего попадает в IT-инфраструктуру банков? Ответ специалистов прозвучал на форуме «Финополис 2025» в рамках сессии «Кибербезопасность — стратегический актив финтеха»: в основном благодаря «старому доброму» фишингу, поскольку, «хоть технологии и меняются, суть заражения остается прежней».

Сергей Голованов, главный эксперт «Лаборатории Касперского», помимо фишинга назвал топ-3 причины киберинцидентов в финансовом секторе: «уязвимости в IT-системах, кража паролей, а также атаки через подрядчиков». По мнению спикера, с технологической точки зрения единственным способом комплексно противостоять перечисленным угрозам является применение платформенных ИБ-решений, постепенно приближая IT-инфраструктуру к концепции Security by Design, требующей минимального участия служб ИБ в функционировании банка.

Андрей Выборнов, заместитель директора департамента ИБ Банка России, отметил: «Набор рисков — один и тот же на протяжении 10 лет», после чего подробно расшифровал сказанное: «Во-первых, это хищение средств у клиентов — физических лиц. Во-вторых, обеспечение операционной надежности и киберустойчивости, ведь помимо всего прочего инциденты и недоступность сервисов у крупных банков неизбежно вызывают напряженность в обществе. В-третьих, обеспечение контроля над утечками персональных данных. Четвертое, это хищение собственных средств банков и других финансовых организаций».

Деловой журнал «Банковское обозрение», в свою очередь, на протяжении 10 лет не раз выделял значимые ИБ-проекты, которые

Качество работы антифрод-систем банков из списка системно значимых кредитных организаций составляет около 99,7%

минимизировали своими результатами хотя бы часть рисков, называемых регулятором, а самые достойные номинировались на получение премии FINAWARD. Среди победителей оказывались и некоторые приведенные в данном анализе компании и банки, что доказывает высокую квалификацию экспертного жюри, осуществлявшего выбор лучшего из лучших.

Значимые ИБ-проекты

Собственно говоря, приведенные мнения экспертов и регулятора определили не только организационно-методическую составляющую кибербеза, но и список приоритетных ИБ-проектов, которые были осуществлены в банках в 2025 году.

- **ОТП Банк** в ноябре 2025 года внедрил платформу «Лаборатории Касперского» Kaspersky Anti Targeted Attack (KATA) и систему Kaspersky EDR Expert. Связка KATA и Kaspersky EDR Expert представляет собой решение класса XDR нативного типа с широкими возможностями обнаружения и исследования сложных инцидентов, а также реагирования на них. Решение позволило банку защитить свою корпоративную инфраструктуру от сложных кибератак (APT) без привлечения дополнительных ресурсов.
- **УБРиР** при содействии «Софтлайн Решений» в декабре запустил комплексную отечественную ASOC-платформу Hexway Vampy ASPM, которая входит в состав продуктового портфеля группы компаний «Солар». Платформа реализует процесс безопасной разработки программного обеспечения (DevSecOps).
- **«Индо Банк»** построил систему сетевой безопасности на базе UserGate NGFW. Интегратор «Нева-Автоматизация» создал кластер, в состав которого вошли два ПАК UserGate D500. Они были дополнены модулями антивирусной защиты, почты и расширенной защиты от угроз (APT). Это же решение в мае было инсталлировано в **Сибсоцбанке** и выбрано в том числе за возможность обеспечить экосистемный подход к обеспечению контура безопасности кредитной организации.
- **Сбер** весной перешел с IBM Security Identity Manager (ISIM) и IBM Security Access Manager (ISAM) на отечественные решения Platform V IDM и Platform V IAM SE от «СберТеха». Инструменты предназначены для обеспечения полного жизненного цикла учетных записей, поддержки управления пользователями и их полномочиями. В самом конце года СберБанк сообщил, что средства компании «КриптоПро» стали основой криптографической защиты биометрических сервисов.

Интересен и проект МТС Банка, который усилил киберзащиту своей IT-инфраструктуры благодаря внедрению решения Threat Intelligence от компании BI.ZONE. Подробнее этот кейс описан в публикации «Б.О» «Пандорино горе и черный ящик».

И криптография, и антифрод

О каких направлениях развития говорят ИБ-эксперты? В каких сферах ожидаются массовые внедрения средств кибербезопасности в 2026 году? Топ-3 идей выглядит так.

1. «Качество работы антифрод-систем банков из списка системно значимых кредитных организаций составляет около 99,7%. Вместе с тем суммы хищений говорят сами за себя, и в основном это — последствия социальной инженерии», — заявил **Вадим Уваров,** директор департамента ИБ Банка России, на втором Форуме «АНТИФРОДУМ-2025». А 5 января 2026 года премьер-министр **Михаил Мишустин** поручил создать единую платформу сбора и анализа данных по цифровым преступлениям на базе ГИС «Антифрод», масштабные контуры которой на упомянутом выше форуме «АнтиФрод Россия 2025» презентовал замминистра Минцифры **Олег Качанов.**
2. В ходе XIII Технологической конференции НСПК **Игорь Голдовский** дал старт масштабному проекту: «К 1 января 2031 года необходимо, чтобы на нашем рынке появились терминалы и пластиковые карты, работающие на базе в том числе и отечественной постквантовой криптографии». Вычислительные возможности криминала растут, и для обеспечения безопасности финансовых операций требуется перейти на новые криптографические алгоритмы, имеющие криптостойкость не меньше 128 бит.
3. Вернемся к мнению Сергея Лебедя: «Необходимо активно строить системы киберзащиты с агентскими ИИ-системами, которые смогут автономно обнаруживать уязвимости, быстро адаптироваться, исходя из угроз, и успешно противостоять им». **Б.О**