ВТБ

Безопасность в банке будущего

Центр технологических исследований ВТБ

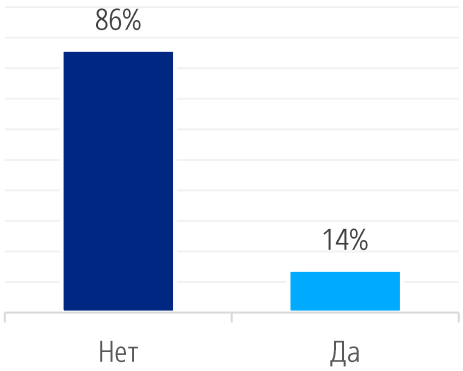
Февраль 2026 г.

Атаки на банки и их клиентов: мнение россиян

В декабре 2025 г. ВТБ провел среди россиян опрос об атаках на банки и на их клиентов. В исследовании приняли участие 1500 респондентов в возрасте 18-65 лет, жители российских городов с населением свыше 100 тыс. человек.

Исследователи четко разделяли два типа атак – на инфраструктуру банков и на их клиентов.

Становились ли вы жертвой атаки непосредственно на банк?

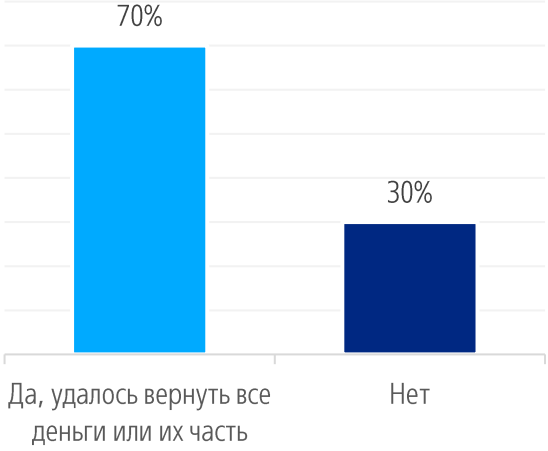


Большинство респондентов (86%) заявили, что никогда не становились жертвами атак злоумышленников непосредственно на банк, когда из-за действий хакеров становятся недоступными сервисы банка и др.

Из тех 14% россиян, кто сталкивался с атаками на банк, половина респондентов сообщили, что потеряли деньги из-за этих атак – либо из-за того, что вовремя не могли воспользоваться своими средствами в банке, либо из-за того, что злоумышленники получили доступ к их счетам в банке.

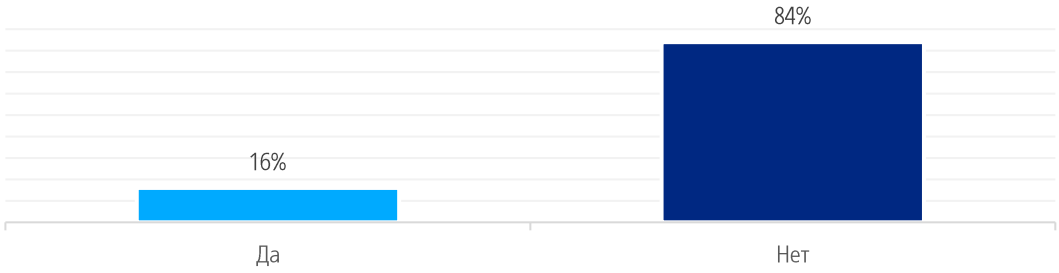
При этом если клиенты банков теряли средства, в большинстве случаев им удавалось их вернуть – так ответили 70% респондентов.

Если из-за атаки вы теряли деньги, удалось ли вам их вернуть?

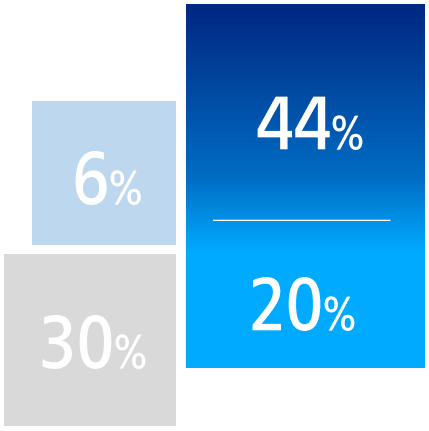


Атаки на банки и их клиентов: мнение россиян

Сталкивались ли вы когда-либо с атаками на вас как на клиента банка – при помощи взлома вашего личного кабинета?



Аналогичная статистика прослеживается и при атаках непосредственно на пользователей – когда злоумышленники атакуют не сам банк, а его клиентов, например, при помощи взломов их личных кабинетов. Большинство россиян (84%) сообщили, что не сталкивались с такими атаками



Вы теряли деньги в результате этой атаки?

- Нет, злодеям не удалось меня провести
- Нет, меня вовремя убедили в мошенничестве сотрудники банка
- Я потерял деньги, вернуть их не удалось
- Я потерял деньги, но их удалось вернуть

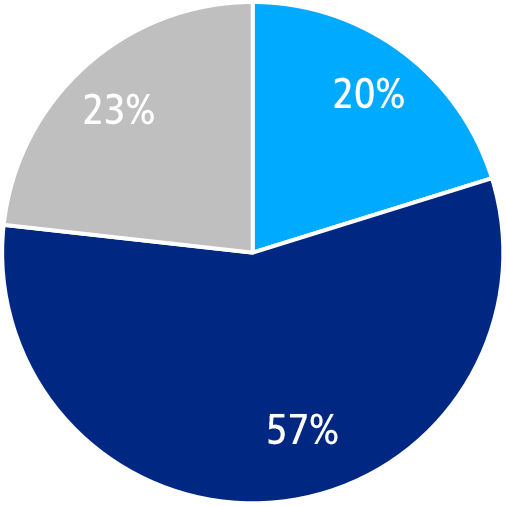
Участники опроса также ответили на вопрос, становились ли они жертвами мошенничеств в случаях, когда злоумышленники пытаются украсть средства обманным путем. Из тех, кто сталкивался с такими атаками, 64% сообщили, что не потеряли своих денег. Либо они сами «раскусили» мошенников (44%) и не поддались на их уловки, либо их убедили в мошенничестве сотрудники банка (20%). Перевели свои деньги злоумышленникам 36% пострадавших (примерно 6% россиян в целом).

Опрос ВТБ: большинство пользователей не сталкивается с атаками злоумышленников – как на сам банк, так и на его клиентов.

В случае, если такие атаки происходят, чаще всего пользователи не теряют деньги, или им удается вернуть свои средства (70%).

Атаки на банки и их клиентов: мнение россиян

В случаях, когда злоумышленники атакуют инфраструктуру банков или клиентов банков, вы вините в этом сами банки?

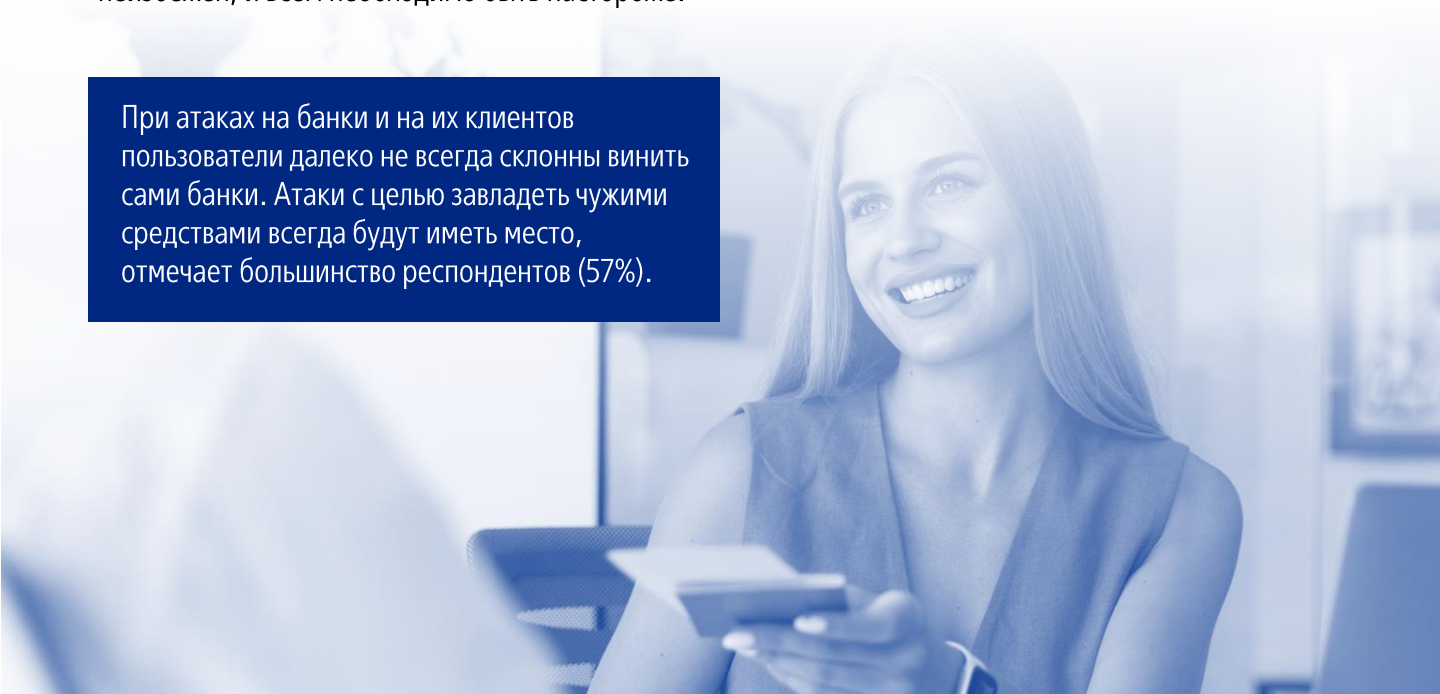


- Нет. У банков огромная инфраструктура, и закрыть все уязвимости невозможно. Атаки же с целью завладеть чьими-либо средствами всегда будут
- Каждый случай следует рассматривать по отдельности: где-то виноват банк с несовершенствами его инфраструктуры, а где-то клиент, который беспечно относится к защите финансов, а где-то атаки хакеров неизбежны
- Ответственность в любом случае лежит на банке, которому доверился клиент

Каждый пятый россиянин (20%) считает, что инфраструктура банков и банковских сервисов настолько огромна, что закрыть абсолютно все уязвимости невозможно, злоумышленники же всегда будут пытаться что-либо украсть – у банка или у его клиентов.

Большинство россиян (57%) уверены, что каждый случай следует рассматривать отдельно. Где-то может быть виноват сам клиент, который невнимательно относится к защите своих финансов, или банк, который вовремя не выявил ту или иную уязвимость, а в каких-то случаях наплыв хакеров неизбежен, и всем необходимо быть настороже.

При атаках на банки и на их клиентов пользователи далеко не всегда склонны винить сами банки. Атаки с целью завладеть чужими средствами всегда будут иметь место, отмечает большинство респондентов (57%).



«В 2020-2022 годах фиксировались явные атаки на клиентов от имени банков, когда злоумышленники представлялись "службой безопасности банка"», — отмечает Дмитрий Ревякин, вице-президент ВТБ, начальник управления защиты корпоративных интересов департамента по обеспечению безопасности. Для этих атак применялись недочеты в банковской инфраструктуре, например, мошенники могли подменить телефонный номер банка и позвонить или отправить с него СМС, говорит эксперт.

> **«Но за последние годы кредитные организации вместе с сотовыми операторами усилили меры безопасности, в том числе исключили возможность подмены телефонного номера и создали защищенные чаты для общения с пользователями. В ВТБ также была внедрена двухфакторная аутентификация для обращений клиентов. Учитывая эволюцию средств защиты, мошенникам теперь очень сложно представляться сотрудниками банков для обмана клиентов. Теперь чаще встречаются схемы, когда злоумышленники звонят от имени правоохранительных органов, а их жертвы переводят им деньги со счетов в нескольких разных банках или вовсе продают имущество и отдают наличные деньги. Поэтому потерпевшие даже не могут сказать, какой банк виноват в том, что у них украли деньги. Наоборот, на банки люди стали чаще жаловаться в контексте того, что они блокируют операции, а не потому что не защитили их денежные средства», — отметил эксперт.**

По словам Дмитрия Ревякина, с попытками мошенничества уже столкнулось почти все трудоспособное население России. «Однако доля реализованных случаев хищения денежных средств в общем объеме попыток крайне мала. В каких-то случаях сами люди понимают, что имеют дело с мошенниками и не дают себя обмануть, в каких-то ситуациях реагируют банки», — добавил он.

Основная цель злоумышленников при атаках на банки и их клиентов — это получение денег. Часто мошенники пытаются оформить кредиты на крупные суммы при предоставлении недостоверных документов и информации о своих финансовых возможностях. «Однако нам известно и единичных случаях на рынке с поддельными паспортами. Но бывают и более изощренные атаки. Например, хакеры используют вирусы-шифровальщики, с помощью которых стараются испортить инфраструктуру банков с целью вымогательства денежных средств. В целом мошенники стараются использовать какие-то уязвимости кредитных организаций, но во всех этих случаях ущерб наносится только банку, а не его клиентам», — отмечает Дмитрий Ревякин.

По оценке Международного союза электросвязи (МСЭ, ITU, International Telecommunication Union, одной из наиболее авторитетных организаций в мире в сфере связи, ИТ и технологий), Россия входит в число стран с наиболее высоким уровнем развития кибербезопасности. Союз регулярно составляет Мировой индекс кибербезопасности (Global Cybersecurity Index). По данным этого индекса за 2020 год, Россия занимала пятое место в мире по развитию кибербезопасности, наряду с Объединенными Арабскими Эмиратами. Более высокий уровень кибербезопасности МСЭ зафиксировал в США, Великобритании, Корее, Сингапуре и ряде других стран. Россия обходила такие страны, как Франция, Германия, Япония и др.

В 2024 году МСЭ изменил методологию индекса, разделив все проанализированные страны на пять групп (tiers) по уровню развития кибербезопасности:

- образцовые (role-modelling);
- передовые (advancing);
- устоявшиеся (establishing);
- развивающиеся (evolving);
- страны, в которых отрасль кибербезопасности только формируется (building).

Россия оказалась во второй группе наряду с Китаем, Канадой, Австрией и Израилем. Среди role-modeling стран в МСЭ назвали США, Великобританию, ОАЭ, Корею, Турцию, Катар и др.

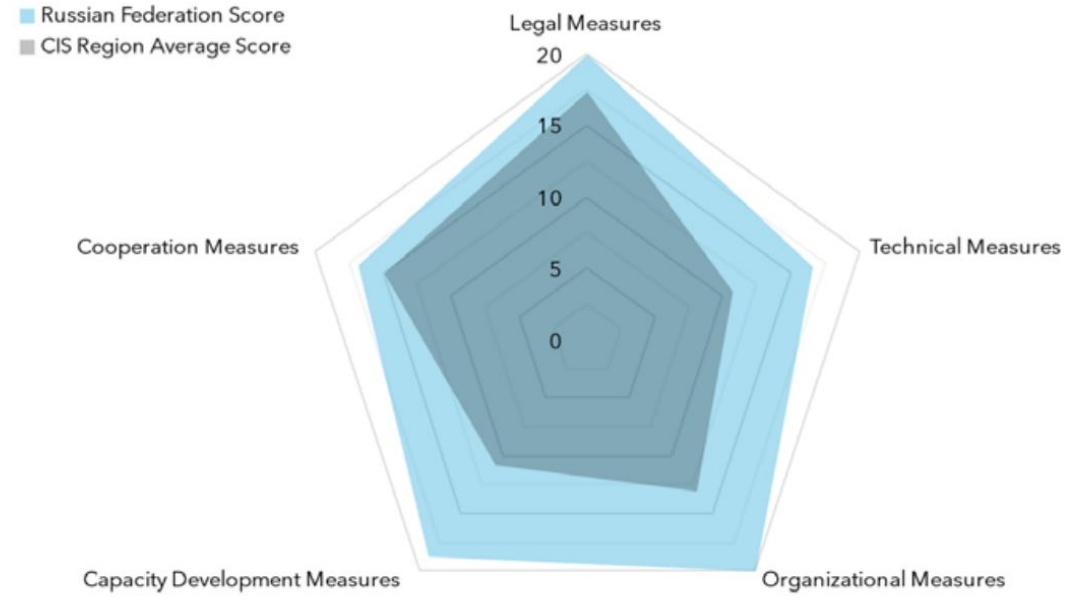
Уровень развития кибербезопасности в странах мира МСЭ анализировал по критериям в пяти разных областях:

- Регуляторные меры (legal measures) — наличие правового регулирования кибербезопасности и киберпреступности;
- Меры по технологическому развитию (technical measures) — наличие организаций, стандартов и фреймворков, регулирующих вопросы кибербезопасности;
- Организационные меры (organization measures) — наличие координирующих органов, политик и стратегий развития кибербезопасности на национальном уровне;
- Меры по развитию потенциала (capacity-development measures) — наличие научных исследований и разработок, образовательных и обучающих программ, сертифицированных специалистов и государственных органов, способствующих развитию потенциала;
- Меры по развитию сотрудничества (cooperation measures) — наличие партнёрств и сетей обмена информацией на национальном, региональном и глобальном уровнях.

По критериям в каждой из областей аналитики присваивали до 20 баллов. По совокупности всех оценок исследователей в индексе МСЭ 2020 года Россия набирала 98,06 баллов, а в индексе 2024 года – 92,13. Из топ-10 экономик мира по ВВП максимальные оценки по всем критериям получили США, Великобритания и Италия и ряд других стран. Китай набрал 91,64 балла, Канада – 93,18.

В России, по оценке МСЭ, хорошо развита регуляторика, принимаются организационные шаги и меры по развитию потенциала. А областями для дальнейшего роста эксперты назвали технологическое развитие и меры по развитию сотрудничества.

Russian Federation



Country Score
out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures
20	16.59	20	18.77	16.77

Источник: Global Cybersecurity Index 2024 стр.102

Отдельный рейтинг по уровню защищенности различных компаний от киберугроз представили исследователи из SecurityScorecard. Среди наиболее защищенных банков и финансовых компаний оказались финансовые организации из стран Европы, Азии и США.

Исследователи опирались на внешние данные — общие показатели активности злоумышленников на рынке присутствия того или иного банка, наличие обнародованных данных об утечках и внимание к организации в хакерских сообществах в даркнете, а также доступные в открытых источниках данные о показателях надежности ИТ-инфраструктуры.

Результаты показали, что при сочетании различных факторов в топе по киберзащищенности могут быть как крупнейшие банки различных стран, так и относительно небольшие организации:

Alpha Bank S.A. (Греция)	Один из крупнейших банков Греции, предоставляет розничные, корпоративные и инвестиционные банковские услуги в Европе.
CTBC Bank (Тайвань)	Крупнейший частный банк Тайваня, предлагает корпоративные, розничные, инвестиционные и международные финансовые услуги.
State Bank of India (Индия)	Крупнейший государственный банк Индии, обслуживает миллионы клиентов, предоставляя универсальные банковские и финансовые услуги.
Provident Credit Union (США)	Региональный кредитный союз, ориентированный на сообщества, предлагает сберегательные счета, кредиты и цифровые банковские сервисы.
S&T Bancorp, Inc (США)	Финансовая холдинговая компания, предоставляющая банковские, ипотечные и инвестиционные услуги частным и корпоративным клиентам.
Bank Syariah Indonesia (Индонезия)	Крупнейший исламский банк Индонезии, обслуживает розничных и корпоративных клиентов.
UBSI, Inc. (США)	Американская финансовая компания, предоставляющая банковские и инвестиционные решения для бизнеса и частных клиентов.
Tangerine (Канада)	Цифровой банк Канады, ориентированный на онлайн-обслуживание, сберегательные продукты и простые финансовые решения.
Forte Payment Systems (США)	Платёжная финтех-компания, предоставляющая решения для электронных платежей, ACH, карт и банковских переводов.
First Abu Dhabi Bank (FAB) (ОАЭ)	Крупнейший банк ОАЭ, предоставляет универсальные банковские, инвестиционные и корпоративные финансовые услуги в регионе MENA.

$12 трлн

в 2026 году составит добыча хакеров по всему миру

$20 трлн

в 2030 году

В 2026 году, по прогнозу аналитиков Proxyrack, эта цифра должна составить почти $12 трлн, а к 2030 году приблизиться к $20 трлн. В 2015 году этот показатель оценивался на уровне $3 трлн.

Одним из самых крупных и известных хищений за последние годы стала серия атак кибербанды Carbanak в 2013-2014 гг., о которой сообщала «Лаборатория Касперского». Деятельность злоумышленников затронула более 100 банков в России, США, Германии, Китае и др. странах, а также платежных систем и других финансовых организаций из 40 стран. В каждом случае добычей злоумышленников становились суммы от $2,5 млн до $10 млн. По оценке антивирусной компании, общий объем финансовых хищений пострадавших составил $1 млрд, что сделало Carbanak одной из самых успешных кибербанд в истории.

Как были устроены атаки

Преступники рассылали фишинговые письма сотрудникам компаний с вредоносными вложениями. Если работник открывал вложение, компьютер заражался вирусом, который незаметно собирал информацию о работе устройства. В дальнейшем вирус распространялся и по другим устройствам организации. В среднем на ограбление каждого из банков уходило от двух до четырех месяцев — от заражения первого компьютера до вывода средств.

$1 трлн

По прогнозам американской аналитической компании Cybersecurity Ventures, к 2031 году мировые расходы на продукты и сервисы в сфере кибербезопасности в B2B и B2C сегментах достигнут $1 трлн. В 2025 году, по подсчетам аналитиков, эта цифра составила $454 млрд, увеличившись с $220 млрд в 2021 г.

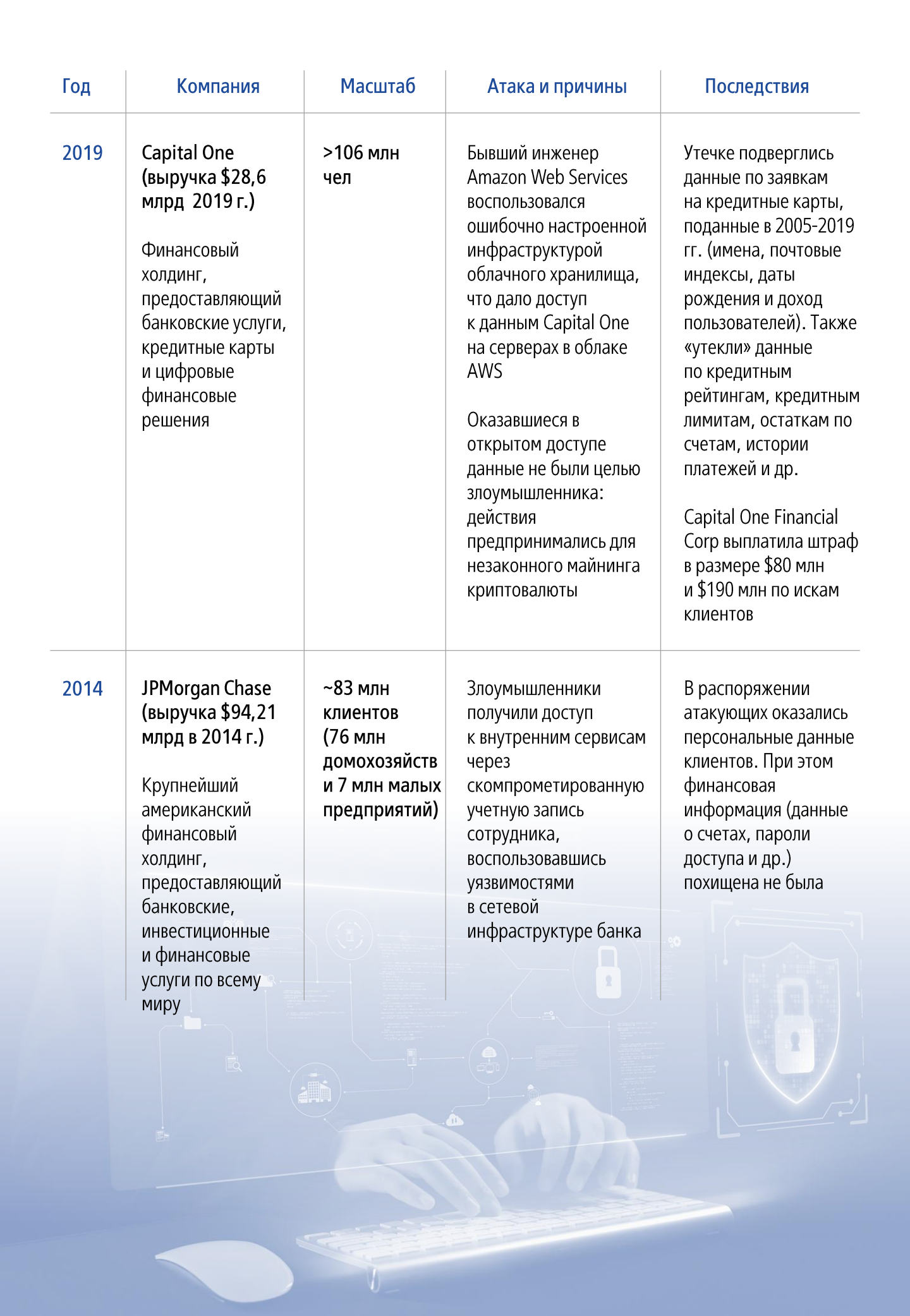
Эксперты Statista же прогнозируют, что совокупная выручка компаний в сфере кибербезопасности по всему миру превысит $265 млрд к 2030 году. Рынок кибербезопасности будет расти на 6,18% в период 2025-2030 гг.

Среди крупнейших утечек

Помимо денежных средств, объектом атаки могут быть данные клиентов, что также несет значительный ущерб как самим клиентам, так и финансовым организациям, допустившим утечку.

Год	Компания	Масштаб	Атака и причины	Последствия
2019	**First American Financial (выручка $6,2 млрд в 2019 г.)** Компания по страхованию прав собственности, сопровождения сделок и обработки ипотечных данных	**~885 млн записей**	Утечка произошла из-за ошибки в информзащите: переход по ссылке на страницу с конфиденциальными данными не требовал аутентификации	В открытый доступ попали номера социального страхования, банковские реквизиты, ипотечные и налоговые документы клиентов компании
2017	**Equifax (выручка $3,4 млрд в 2017 г.)** Бюро кредитных историй	**~147–148 млн чел.**	Наличие уязвимостей в системе защиты данных Скрытое течение атаки	В открытом доступе оказались персональные и платежные данные клиентов, к компании были поданы многочисленные иски клиентов
2008 - 2009	**Heartland Payment Systems (выручка $1,5 млрд в 2008 г.)** Поставщик услуг по обработке платежей и платежных решений для бизнеса	**~130 млн карт**	Атака на процессинг Heartland началась с SQL-инъекции на корпоративном сайте, после чего инструменты злоумышленников попали в платёжную сеть. Вредоносное ПО перехватывало данные карт во время транзакций, что оставалось незамеченным в течение месяцев	Были скомпрометированы персональные и платежные данные клиентов, а также их пароли доступа к финансовым сервисам

Год	Компания	Масштаб	Атака и причины	Последствия
2019	**Capital One (выручка $28,6 млрд 2019 г.)** Финансовый холдинг, предоставляющий банковские услуги, кредитные карты и цифровые финансовые решения	**>106 млн чел**	Бывший инженер Amazon Web Services воспользовался ошибочно настроенной инфраструктурой облачного хранилища, что дало доступ к данным Capital One на серверах в облаке AWS Оказавшиеся в открытом доступе данные не были целью злоумышленника: действия предпринимались для незаконного майнинга криптовалюты	Утечке подверглись данные по заявкам на кредитные карты, поданные в 2005-2019 гг. (имена, почтовые индексы, даты рождения и доход пользователей). Также «утекли» данные по кредитным рейтингам, кредитным лимитам, остаткам по счетам, истории платежей и др. Capital One Financial Corp выплатила штраф в размере $80 млн и $190 млн по искам клиентов
2014	**JPMorgan Chase (выручка $94,21 млрд в 2014 г.)** Крупнейший американский финансовый холдинг, предоставляющий банковские, инвестиционные и финансовые услуги по всему миру	**~83 млн клиентов (76 млн домохозяйств и 7 млн малых предприятий)**	Злоумышленники получили доступ к внутренним сервисам через скомпрометированную учетную запись сотрудника, воспользовавшись уязвимостями в сетевой инфраструктуре банка	В распоряжении атакующих оказались персональные данные клиентов. При этом финансовая информация (данные о счетах, пароли доступа и др.) похищена не была



Безопасность и искусственный интеллект

$28,5 млрд

объем рынка ИИ-решений в отрасли кибербезопасности в 2025 г., оценивают аналитики Research and Markets (эксперты включают сюда программные продукты и оборудование, а также сервисные услуги, в которых в той или иной степени используются технологии искусственного интеллекта)

$136 млрд

объем этого рынка в 2032 г., согласно оценке аналитиков

Использование технологий искусственного интеллекта в обеспечении информационной безопасности является одним из ключевых приоритетов для ИБ-руководителей в разных странах мира, отмечается в масштабном исследовании 2026 Global Digital Trust Insights, проведенном аналитиками PricewaterhouseCoopers (PwC). Исследование основано на интервью свыше 3 тыс. ИТ-руководителей из более чем 70 стран мира.

Среди основных ИИ-инструментов аудиторы PwC выделяют ИИ-агентов (Agentic AI) — их используют в качестве одного из основных ИИ-элементов защиты от киберугроз. ИИ-агенты превращаются в полноценных цифровых помощников, которые могут действовать автономно, сотрудничать с командами специалистов и инициировать самостоятельные решения по кибербезопасности для защиты инфраструктуры от ИБ-угроз.

В 2026 г. опрошенные аналитиками PwC ИБ-руководители планируют применять ИИ-агентов в облачных решениях, при защите данных, операций, управлении доступом и др.

При этом областью для дальнейшего роста аналитики PwC называют дальнейшую работу по анализу и обработке данных для более эффективного использования технологий искусственного интеллекта.

Внедрение искусственного интеллекта приводит к ощутимой финансовой выгоде. Согласно отчету IBM, благодаря внедрению ИИ-решений, впервые за пять лет глобальные затраты из-за утечек данных снизились на 9% в годовом выражении до $4,4 млн. По данным компании, организации, которые использовали IT-решения на базе ИИ, смогли снизить среднюю стоимость ущерба на $1,9 млн.

Использование ИИ-агентов стало характерно не только для защиты от киберугроз, но и при осуществлении хакерских атак. Это привело к тому, что в 2025 году отрасль кибербезопасности перешла так называемый ИИ-рубикон, отмечает международный эксперт по кибербезопасности Дэн Лорманн (Dan Lohrmann). По его словам, прошедший год характеризовался активным развитием автономных ИИ-систем, агентов, которые могут планировать и выполнять действия без участия человека. Это, отмечает Лорманн, составляет одну из новых киберугроз, связанную с появлением сложных автоматизированных атак на ИТ-инфраструктуру. Такие атаки становятся адаптивными — благодаря ИИ атакующие системы могут менять тактику «в моменте», обходя защитные механизмы. Помимо этого, развитие больших языковых моделей и генеративного ИИ позволяет создавать персонализированные фишинговые письма и все более совершенные дипфейки, что выводит подобные атаки на беспрецедентный уровень.

Развитие базовых больших языковых моделей обеспечивает автономность ИИ-агентов и их способность взаимодействовать между собой в мультиагентных системах. Уже сегодня известны случаи, когда атака на IT-инфраструктуру осуществлялась практически в автономном режиме сетью из множества ИИ-агентов. Например, осенью 2025 года о такой атаке сообщала американская ИТ-компания Anthropic.

«Совершенствование мультиагентных систем будет способствовать кратному росту скорости поиска уязвимостей хакерами. Высвобождение ресурсов приведет к тому, что в среде хакеров в перспективе ближайших лет появятся «великие комбинаторы», которые будут создавать стратегии атак, планировать ключевые сценарии и др., тогда как всю рутину возьмут на себя ИИ-агенты. На стороне защищающихся организаций ситуация будет развиваться аналогично: будут специалисты, выстраивающие периметр защиты на стратегическом уровне, а вся механическая работа, в том числе написание кода, будет автоматизирована с помощью ИИ-агентов», — отмечает Вадим Кулик, заместитель президента – председателя правления ВТБ.

Работа сервисов, основанных на технологиях искусственного интеллекта, тесно сопряжена с анализом большого числа разных по своим типам данных. будучи одним из крупнейших социально-значимых банков, ВТБ строит свою работу с данными в соответствии с самыми строгими нормами информационной безопасности.

«Для работающих в банке LLM мы используем, например, различные AI-файерволы, которые отслеживают и обрабатывают как входные данные, пользовательские запросы (промпты), так и ответы модели, — отмечает Максим Коновалихин, старший вице-президент, руководитель департамента анализа данных и моделирования ВТБ. — Подобные решения предназначены для предотвращения угроз, связанных с особенностями работы ИИ-моделей, например, вредоносных инъекций, когда злоумышленники могут “обмануть“ модель, внеся в качестве пользовательского запроса некий вредоносный код, который может приводить как к кражам данных, так и выведению модели из строя».

«Я бы не стала говорить, что искусственный интеллект сейчас доминирует в решениях по информационной безопасности, но рост использования этих технологий в ИБ, конечно, есть. ИИ, безусловно, делает какие-то вещи проще. Например, он может быстро просматривать огромные массивы информации и искать в них какие-то корреляции, может искать ошибки и уязвимости в коде или может давать какие-то подсказки "безопаснику" по тому или иному продукту, на документации по которому он, как помощник, обучился», — отметила президент группы компаний InfoWatch, председатель правления АРПП «Отечественный софт» Наталья Касперская в подкасте ВТБ «Деньги любят техно». Перспективы использования технологий на базе ИИ эксперт видит в развитии цифровых помощников, когда такие решения обучаются на больших массивах данных и предоставляют подсказки квалифицированным специалистам.

«Но необходимо помнить, что такие подсказки будут всегда носить вероятностный характер, иногда выдавая неправильные ответы. И задачей специалиста по ИБ будет вовремя найти ту или иную ошибку, перепроверив нужный раздел документации», – добавила Наталья Касперская

Увеличение использования искусственного интеллекта в решениях по информационной безопасности происходит по всему миру, соглашается бизнес-консультант по информационной безопасности Positive Technologies Алексей Лукацкий. По его словам, это происходит в ответ на рост популярности использования ИИ и среди злоумышленников.

«Уже сейчас ИИ берет на себя большую часть рутины в SOC (центр мониторинга и реагирования на инциденты информационной безопасности – прим.). Это, например, анализ телеметрии, выявление аномалий, группировка событий, приоритезация инцидентов, суммирование больших объемов данных и подготовка рекомендаций по действиям аналитиков SOC», — отмечает Алексей Лукацкий. Такой подход повышает скорость реакции и уменьшает нагрузку на специалистов, дефицит которых становится критическим, объясняет эксперт.

По его мнению, при правильной архитектуре ИИ становится не угрозой, а «усилителем» киберзащиты. «Мир движется к автономным SOC на базе роевого ИИ, который закрывает до 80% операций, а человек остается сосредоточен на расследованиях и принятии решений», — поясняет эксперт.

В настоящее время также часто говорят об использовании ИИ для создания дипфейков, но эта угроза на данный момент сильно преувеличена, отмечает Дмитрий Ревякин, вице-президент ВТБ, начальник управления защиты корпоративных интересов департамента по обеспечению безопасности.

«До сих пор не зафиксировано качественных дипфейков. Чтобы создать ложный образ человека, необходим большой объем аудиофайлов и видеофайлов о нем – запись голоса длительностью минимум десять минут и видео человека со всех ракурсов. У мошенников нет информации в таком объеме об обычных пользователях. Это сложная атака, которую зачастую создавать и проводить нецелесообразно. Однако мы видим, что мошенники пытаются подделать голоса людей — для этого используются специальные сервисы, которые могут изменять голос и делать его похожим на конкретного человека. Но если такие атаки будут проводиться в отношении банка, то антифрод системы без проблем их обнаружат».

«Основную опасность в работе с искусственным интеллектом, как это ни странно, составляют не ошибки, допущенные машиной, не бреши, оставленные в контурах информационной безопасности, а именно иррациональные страхи самих пользователей, которые могут приводить, как следствие, к иррациональным действиям», — отметил Вадим Кулик, заместитель президента — председателя правления ВТБ.

Криптоанклав: изолировать угрозу

Криптоанклав – это решение для безопасного объединения больших данных. Это аппаратно изолированная среда, в которой выполняются операции с ключами и чувствительными данными, недоступные даже администраторам. Информация в нем хранится и обрабатывается в зашифрованном виде. Задача системы —извлечение из общего массива данных прогнозов и построения с помощью AutoML-алгоритмов.

Криптоанклавы уже выходят в мире на уровень отраслевого стандарта, говорит бизнес-консультант по информационной безопасности Positive Technologies Алексей Лукацкий. «Сегодня криптоанклавы активно используют JP Morgan Chase (AWS Nitro Enclaves для защиты ключей), ING и Rabobank (Intel SGX для безопасных вычислений), а также финтех-компании в Сингапуре и ОАЭ, строящие свои облачные платформы с конфиденциальными вычислениями», – перечисляет он.

По его словам, технология эффективна там, где критичны риски инсайдеров и атак на инфраструктуру. Анклавы защищают данные в процессе вычисления – то, чего классическая криптография пока не делает, уточняет эксперт. Но у этого решения есть свои ограничения: side-channel-атаки (атаки по сторонним каналам – прим.), сложность интеграции и необходимость строгого инженерного дизайна. Тем не менее, это уже не эксперимент, а практический инструмент защиты платежей, биометрии и ключевой криптографии, говорит Лукацкий. В России законодательная база еще не до конца сформирована под беспрепятственный обмен данными между организациями для корректной работы технологии криптоанклавов, добавляет эксперт.

В 2023 г. ВТБ совместно с МФТИ разработали первый российский криптоанклав. Банк активно участвует в дальнейшем развитии этой технологии – совместно со своим технологическим партнером, ИТ-холдингом Т1.

Открытый банкинг

Еще одним направлением, в котором сегодня активно развиваются банковские сервисы, и где одним из основных вопросов является обеспечение безопасности — это развитие открытого банкинга.

Открытый банкинг (англ. Open banking) — это концепция взаимной интеграции продуктов и сервисов от разных финансовых поставщиков в едином интерфейсе. Такой подход позволяет строить обмен данными о клиенте с его согласия с помощью технологии открытых API (Open API, универсальных программных интерфейсов). Таким образом, при помощи открытого банкинга клиент может видеть свои счета в разных банках, управлять ими, переводить средства со счета на счет и др. — из наиболее удобного для клиента приложения какого-либо одного банка.

Технологии открытого банкинга в России сегодня развиваются в пилотном режиме. Крупнейшие российские банки участвуют в различных пилотах по интеграции клиентских счетов в едином интерфейсе: тестируется отображение счетов, а также их управление. Например, используя приложение ВТБ, входящий в пилотную группу клиент может видеть свои счета в других банках, в некоторых случаях управлять ими. Это может быть актуально для пользователей физических лиц или компаний — располагающими большим количеством счетов в различных банках.

Важным аспектом здесь является обеспечение безопасности — как самих операций, так и передачи персональных данных пользователей, их финансовой информации между различными банками. Для этого ВТБ применяет целый комплекс мер.

«Использование алгоритмов ГОСТ для шифрования данных, то есть шифрование данных, подтвержденное государственными стандартами, обеспечивает высокий уровень сохранности данных на этапе их передачи. Также для этого используется системы, относящиеся к значимым объектам критической информационной инфраструктуры (ЗО КИИ). К данному классу систем предъявляются повышенные требования безопасности и отказоустойчивости», — отмечает Игорь Бессчастный, лидер Платформы API ВТБ.

Банк ВТБ обеспечивает комплексный подход для обеспечения безопасного обмена данными в Open API, включая системы защиты от DDoS-атак и др.

Аналогичные системы и оборудование для защиты в Open API сегодня применяют и другие банки, участвующие в пилотных проектах по открытому банкингу. Но для полноценного развития открытого банкинга, а также следующих после него стадий – открытых финансов и открытых данных, когда в обмене данными при помощи Open API участвует все большее число игроков из различных сфер (страховые компании, интернет-сервисы и др. компании), необходимо распространение требований по информационной безопасности, которые сейчас применяются к ВТБ и другим крупнейшим банкам, на всех остальных участников рынка. Без этого процесс безопасного обмена данными будет невозможен.

«Развитие открытого банкинга и в дальнейшем концепций открытых финансов и открытых данных позволит крупным банкам аккумулировать и анализировать все новые пласты информации о пользователе – включая его цифровой профиль в интернете (какие страницы он смотрит, какие покупки совершает, оплачивая их со счетов любых банков, и др.). Это, в свою очередь, будет помогать банку оказывать услуги клиентам все более адресно. Также новая информация о пользователе позволит банку еще более эффективно защищать его от мошенничеств – вовремя идентифицируя нетипичное поведение клиента, выявляя случаи, когда он попадает под влияние мошенников. Таким образом, безопасность и совершенствование банковского сервиса станут одними из основных драйверов развития открытого банкинга и в дальнейшем концепций открытых финансов и открытых данных» – Игорь Бессчастный, лидер Платформы API ВТБ.

Шифрование: потенциал фотона

Среди перспективных технологий киберзащиты выделяется и технология квантового шифрования, которая основана на законах квантовой механики. При данном виде криптографии информация кодируется в виде состояний квантовых частиц, чаще всего фотонов. Они передаются по оптоволоконному кабелю, а любая попытка измерения приводит к изменению их состояния. Таким образом, всегда можно отследить попытку вмешательства в сеть.

«Технология квантового шифрования обеспечивает возможность быстрой смены ключей шифрования. Каждая компрометация сразу же становится видна владельцу системы, банку. Злоумышленники теряют возможность попасть в канал, украсть из него какую-либо информацию, оставаясь при этом незамеченными. Квантовое шифрование можно сравнить с охранной сигнализацией: как только она срабатывает, запускается процесс замены ключей шифрования. Ключи шифрования могут заменяться со скоростью сотен, тысяч ключей в минуту — в зависимости от используемого оборудования и длины канала», — говорит Николай Шуткин, заместитель руководителя департамента развития инфраструктуры ВТБ.

При помощи квантового шифрования организации могут защищать крупные каналы связи. В контексте банка можно говорить о каналах, например, крупных зарплатных клиентов, продолжил Николай Шуткин. По ним передаются персональные данные получателей средств, суммы перечисления и др. «Соответственно, если кто-либо захочет эти данные украсть, он попытается подобрать ключ шифрования, скомпрометировать его, перехватить данные. С квантовым шифрованием это сразу же будет обнаружено, ключи мгновенно заменены, что исключает возможность взлома», — отметил Николай Шуткин.

Квантовое распределение ключей теоретически обеспечивает абсолютную стойкость к перехвату, но пока остается технологией ограниченного применения, отмечает Алексей Лукацкий.

Масштабные пилоты по внедрению квантового шифрования есть в Китае (проект Пекин–Шанхай длиной более 2000 км, где участвуют Bank of China и ICBC), в Швейцарии (SwissQuantum, тестировавшийся совместно с банками и операторами связи), а также в Южной Корее, где квантовое распределение ключей встроили в защищенные каналы для финансовых транзакций, напоминает эксперт.

«В ВТБ мы тестируем квантовое шифрование в рамках пилотных проектов. Технология перспективна, но пока остается дорогостоящей, зависящей от целого ряда технологических аспектов», — отмечает Николай Шуткин. Помимо высокой стоимости использования, технология чувствительна к помехам и ограничена расстояниями, согласен с Шуткиным Лукацкий. Без усилителей технология работает всего на несколько сотен километров. «При этом при включении в модель усилителей они могут стать слабым звеном всей схемы. Поэтому банки внедряют модель точечно — в каналах между своими ЦОДами или на инфраструктуре уровня центрального банка», — добавляет Лукацкий.

Тестирование технологии квантового шифрования связано с развитием квантовых суперкомпьютеров. Например, в ноябре 2025 г. компания Quantinuum представила новое поколение ионного квантового компьютера Helios с увеличенным числом кубитов — с 56 до 96. «Пока массового использования квантовых компьютеров нет, но с его началом такие машины могут стать одним из инструментов злоумышленников при атаках на банковскую инфраструктуру. И крупные банки должны быть к этому готовы. Поэтому ВТБ как социально ответственный бизнес активно тестирует технологию квантового шифрования», — отметил Николай Шуткин.

Развитие этого направления может пойти и по пути постквантового шифрования. Эта технология также активно тестируется в ВТБ с 2023 года, добавляет Николай Шуткин. Работа алгоритмов постквантового шифрования не требует такого мощного оборудования, как квантовое шифрование, но может противостоять воздействию квантовых компьютеров. Сертификация алгоритмов постквантового шифрования сейчас продолжается в разных странах мира, в том числе в России. По мнению Алексея Лукацкого, квантовое шифрование останется нишевой технологией, а широкую защиту банковских данных обеспечат именно постквантовые алгоритмы.

Вадим Кулик

Заместитель президента – председателя правления ВТБ

«Развитие современных технологий, таких как, например, технологий открытого банкинга, искусственного интеллекта, криптоанклавов и квантового шифрования, создадут банки нового поколения. С еще более персонализированными сервисами, прогнозированием потребностей клиентов, удобными интерфейсами, позволяющими максимально быстро получать как непосредственно банковские услуги, так и оплачивать различные товары и услуги.

В то же время, это приведет к появлению мошенников нового поколения, которые будут пытаться использовать эти же технологии в своих целях. Например, технологии искусственного интеллекта – для проведения более автоматизированных и персонализированных атак. Хакеры будут все чаще использовать ИИ-агентов в качестве атакующих ботов, что может кратно увеличить объем атак при сохранении того же уровня затрат злоумышленников.»

Одним из ключевых трендов в развитии банков и обеспечении безопасности в их ИТ-инфраструктуре будет развитие ИИ-агентов.

Сейчас мы видим тренд ускорения цикла совершенствования ИИ-моделей и ИИ-агентов. Это период, когда выходит новая версия базовой модели и затем вокруг нее появляется агентская инфраструктура. Сейчас это занимает около года, но через год этот цикл будет составлять уже полгода, а потом и вовсе квартал. В результате такого ускорения развития ИИ-агентов на горизонте пары лет может не остаться ни одного банка, у которого не будет своих ИИ-агентов, при этом большинство хакерских атак также будут совершаться при помощи ИИ-агентов.

Будет появляться все больше ИИ-агентов – как на стороне бизнеса, для оказания услуг клиентам и пользователям, так и на стороне самих клиентов и пользователей – для получения ими качественных услуг от различных поставщиков.

Соответственно, с развитием ИИ в каналах для общения возникнут цепочки, в которые будут встроены ИИ-агенты. В этом случае уже не клиенты будут напрямую взаимодействовать с приложением банка, а сначала клиент будет обращаться к своему агенту, а уже пользовательский агент будет контактировать с агентом бизнеса.

Это, в свою очередь потребует адаптации ИТ-систем всех сервисов.