Индекс УДК 004.056
Код ГРНТИ 81.93.29
DOI: 10.22204/2410-4639-2026-129-01-88-102

С.В. ЛЕБЕДЬ*

Киберугрозы и безопасность банковской инфраструктуры: анализ в контексте обеспечения цифрового суверенитета России

В статье рассматриваются современные киберугрозы, влияющие на устойчивость банковской инфраструктуры Российской Федерации в контексте обеспечения цифрового суверенитета страны. Анализируется информационная инфраструктура крупных финансовых организаций, включая серверные парки, сети банкоматов, автоматизированные рабочие места, сетевое оборудование и системы кибербезопасности. Особое внимание уделяется регуляторным требованиям, предъявляемым к кредитным организациям, включая Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры», Федеральный закон № 161-ФЗ «О национальной платёжной системе», а также нормативным актам Банка России. Систематизированы основные киберриски, представлена типология современных угроз, включая фишинг, APT-атаки, программы-вымогатели, DDoS-атаки, а также новые вызовы, связанные с применением технологий искусственного интеллекта, больших языковых моделей и мультиагентных систем. Сделан вывод о необходимости комплексного подхода к обеспечению кибербезопасности банковского сектора как важнейшего элемента цифрового суверенитета России.

Ключевые слова: кибербезопасность, банковская инфраструктура, цифровой суверенитет, киберугрозы, критическая информационная инфраструктура, APT-атаки, искусственный интеллект, мультиагентные системы, регуляторные требования, финансовый сектор

Введение

Цифровой суверенитет представляет собой способность государства контролировать и защищать свою информационную среду, включая данные, системы связи, программное обеспечение и другие информационные ресурсы и технологии таким образом, чтобы обеспечить независимость от внешних факторов, включая иностранных поставщиков программного обеспечения, оборудования и услуг.

Современный этап развития глобальной цифровой экономики характеризуется активным внедрением цифровых технологий практически во все сферы жизни общества. Особое значение приобретает сфера финансовых услуг, где цифровизация привела к кардинальным изменениям в моделях оказания банковских услуг, появлению новых продуктов и сервисов. Однако наряду с преимуществами цифровизации возникли серьёз-

* **Лебедь Сергей Владимирович** — вице-президент по кибербезопасности ПАО Сбербанк.
E-mail: svlebed@sberbank.ru

ные вызовы в области кибербезопасности, ставящие под угрозу стабильность функционирования всей финансовой системы.

Стабильность финансовой системы напрямую влияет на обеспечение национального суверенитета и безопасность страны. Проблемы в сфере денежного обращения и функционирования финансовых рынков способны приводить к серьёзным социальным потрясениям и оказывать разрушительное воздействие на экономику в целом, затрагивая такие чувствительные сферы, как ВПК. Подобные негативные явления могут быть использованы заинтересованными сторонами для дестабилизации обстановки в отдельных регионах и в стране в целом.

Несмотря на усилия регуляторов и надзорных органов, направленные на повышение уровня информационной безопасности, российские банки сталкиваются с множеством серьёзных угроз, таких как фишинг, целенаправленные атаки типа Advanced Persistent Threat (APT), инсайдерская деятельность, промышленный шпионаж, кибервандализм, переходящий в последнее время к вандализму в физическом мире.

Проблематика информационной безопасности становится важнейшим фактором устойчивости всей банковской системы государства. Банковская отрасль сталкивается с такими трудностями, как недостаток эффективных механизмов раннего предупреждения угроз, сложность эффективного реагирования на киберинциденты, трудности оперативного выявления попыток мошенничества и недостаточная интеграция разнородных информационных систем. Поэтому создание надёжной и устойчивой системы защиты от компьютерных угроз приобретает первостепенное значение.

В настоящей статье рассматривается современное состояние цифровой экономики и финансовых рынков, характеризующее динамику появления новых типов атак и рост опасности цифровых угроз. Основной целью автора статьи является установление контекста глобальных изменений и выявление ключевых факторов риска для финансовых организаций.

Типовая банковская инфраструктура

Информационная инфраструктура современной финансовой организации представляет собой разветвлённую и технически сложную гетерогенную систему, включающую широкий спектр элементов: центры обработки данных, телекоммуникационное оборудование, глобальные сети передачи данных, распределённую сеть банкоматов, автоматизированные рабочие места (АРМ) сотрудников, мобильные приложения и web-сервисы для взаимодействия с клиентами, а также интеграционные сервисы с внешними партнёрами. Растущий масштаб и многообразие этой инфраструктуры неизбежно увеличивают поверхность возможных атак, создавая дополнительные точки проникновения.

Серверная инфраструктура

Крупные финансовые организации эксплуатируют десятки и сотни тысяч серверов, размещая их преимущественно в центрах обработки данных (ЦОД). Внутри каждого ЦОД обеспечивается надёжная организация бесперебойной работы, дублирование критически важных узлов и данных, а также строгое соблюдение норм кибербезопасности и физической охраны.

Значительное количество серверов объясняется необходимостью обеспечения масштабируемых экосистем, охватывающих разнообразные сегменты рынка, не только финансовые, но и такие как: розничная торговля, логистика, автомобильные услуги, индустрия развлечений, туристические сервисы, медицинское обслуживание и другие. В результате крупнейшие российские банки управляют одним из самых мощных серверных парков в стране.

Одной из заметных тенденций последних лет стало расширение использования отечественных серверных решений. Такой подход увеличивает независимость

отечественной IT-инфраструктуры от зарубежных поставщиков комплектующих и ПО, что служит укреплению цифрового суверенитета России.

Тем не менее остаётся открытым ряд стратегических задач, связанных с повышением операционной независимости и самостоятельности финансовых организаций в части серверной инфраструктуры. Дальнейшая модернизация парка серверов должна сопровождаться постоянным мониторингом мировых технологических достижений и разработкой принципиально новых решений, гарантирующих конкурентоспособность национальных игроков на международном рынке.

Банкоматная сеть

Российские банки обслуживают одну из крупнейших в мире сетей банкоматов, обеспечивая население удобством и доступностью наличных расчётов и базовых банковских операций. Лидером в этой области традиционно выступает Сбербанк, чья банкоматная сеть насчитывает 46 тысяч устройств, что составляет значительную долю от общероссийского показателя [17]. Другие крупные игроки рынка, такие как ВТБ, Альфа-Банк, Газпромбанк и Т-банк, также поддерживают значительные объёмы собственной сети. Российские банки уделяют большое внимание равномерному покрытию территорий страны, особенно регионов с низкой плотностью отделений и офисов банков.

Особую тревогу вызывает сценарий длительного и масштабного сбоя в сети банкоматов, который способен вызвать волну паники среди населения и представителей бизнеса, спровоцировав резкий всплеск спроса на снятие наличных. В случае неспособности банков оперативно удовлетворить этот повышенный спрос даже в отдельно взятом регионе, ситуация может перерасти в серьёзные социальные беспорядки, ставящие под угрозу стабильность всей страны.

Банкоматы оборудованы специализированным ПО для повышения уровня безопасности и надёжности обслуживания клиентов. Дополнительную надёжность обслуживанию придают эффективные системы мониторинга и удалённого технического обслуживания. Все устройства оснащены современными датчиками и видеокамерами, способными мгновенно фиксировать попытки неправомерного вмешательства или повреждения оборудования [4]. Во многих случаях применяется технология автономного режима работы банкомата, позволяющая продолжить оказание стандартных услуг даже при кратковременных перебоях связи или электропитания.

Широкая география распространения банкоматов вкупе с продуманными техническими и организационными мерами безопасности превращает российскую банкоматную сеть в один из важнейших элементов системы оказания качественных банковских услуг. Она удовлетворяет потребности граждан и малого бизнеса в быстром доступе к своим средствам и поддерживает экономический рост страны.

Автоматизированные рабочие места

Российский рынок банковских услуг представлен большим числом организаций, каждая из которых оснащена значительным количеством АРМ, масштабы инфраструктуры требуют особого внимания к решению вопросов безопасности АРМ.

Одной из центральных задач российских банков в последнее десятилетие стало импортозамещение ПО и ИТ. Осознавая стратегическую важность независимости от зарубежных компаний-разработчиков, банки предпринимают шаги по переводу сотрудников на отечественную инфраструктуру. Показательным примером является инициатива Сбербанка, начатая в сентябре 2024 года, когда банк приступил к поэтапному переводу около 150 тысяч сотрудников на новую российскую платформу виртуальных рабочих мест Termidesk, заменяя ранее использовавшееся иностранное ПО Citrix [18].

Переход на собственную инфраструктуру имеет важное значение для укрепления

цифрового суверенитета России и снижения рисков санкционного давления со стороны западных государств.

Сетевое оборудование и коммуникационные каналы

Российские банки представляют собой мощные цифровые экосистемы, соединённые высокоскоростной и надёжной сетевой инфраструктурой. Количество единиц сетевого оборудования ведущих банков, таких как Сбербанк, ВТБ, Альфа-Банк и другие, превышает десятки тысяч устройств, что позволяет организовать бесшовное подключение многочисленных подразделений, филиалов и офисов, расположенных по всей стране. Сети охватывают региональные подразделения, многочисленные филиалы, расположенные в городах и посёлках, а также внешние точки подключения, доступные миллионам клиентов через интернет-банки и мобильные приложения.

Сегодня ёмкость скоростных каналов достигает пропускной способности в несколько Тбит/с, что позволяет быстро передавать огромные массивы данных, обеспечивая высокое качество обслуживания [22].

Ещё одна важная особенность сетевых каналов российских банков — обеспечение высокого уровня безопасности. Современные системы защиты включают шифрование передаваемых данных, глубокую фильтрацию пакетов и интеллектуальные системы обнаружения вторжений, что препятствует возможным атакам и снижает риски компрометации ценных данных.

Благодаря развитию сетевой инфраструктуры банки России готовы не только качественно обслуживать миллионы клиентов ежедневно, но и предлагать надёжные сервисы другим участникам финансовой экосистемы. Таким образом, российская банковская отрасль, инвестируя значительные средства в развитие сетевой инфраструктуры, смогла создать единую высокоэффективную информационную магистраль, поддерживающую интероперабельность их систем, обеспечивающую быстрое и безопасное перемещение огромных объёмов данных по всей стране.

Система кибербезопасности

Современная финансовая система России функционирует в условиях повышенной угрозы со стороны киберпреступников, поэтому вопрос кибербезопасности выходит на первый план для всех крупных кредитных учреждений. Учитывая огромный масштаб проводимых операций и объём обрабатываемых данных, именно хорошо организованные системы защиты обеспечивают безопасность как самого банка, так и его клиентов.

Высокий уровень защиты возможен благодаря современному программному обеспечению, новейшему оборудованию и высококвалифицированным специалистам, которые круглосуточно контролируют ситуацию и реагируют на малейшее подозрение. Автоматизированные системы обнаружения и реагирования на инциденты позволяют оперативно идентифицировать и нейтрализовать любую попытку несанкционированного доступа или другой вид атаки.

Стоит отдельно подчеркнуть, что ведущую роль в борьбе с кибератаками на финансовый сектор играет Центр мониторинга и реагирования на компьютерные инциденты в кредитно-финансовой сфере (ФинЦЕРТ). Под руководством Банка России, ФинЦЕРТ осуществляет сбор, анализ и распространение информации о киберугрозах, помогая банкам своевременно выявлять и устранять инциденты.

Это коллективное усилие, подкреплённое бюджетом и самыми современными инструментами, позволяет российским банкам вести успешную борьбу с киберпреступностью: защищать собственную цифровую инфраструктуру, предпринимать действия для защиты клиентов и в итоге способствовать обеспечению национального цифрового суверенитета.

Инфраструктура российских банков демонстрирует высокую степень готовности к различным сценариям и позволяет решать самые сложные задачи. Накопленный опыт и отработанные технологии находят

применение не только внутри организаций, но и распространяются на государственные проекты и коммерческие структуры, оказывая позитивное влияние на национальную кибербезопасность и технологическую независимость страны.

Регуляторные требования и риск-ориентированный подход

ФЗ № 187 «О безопасности критической информационной инфраструктуры РФ» (с 01.01.2018г.) установил ряд обязательных требований для различных объектов критической информационной инфраструктуры (КИИ), включая банковские организации. Эти требования направлены на минимизацию рисков нарушения доступности, целостности и конфиденциальности важных ИС и обеспечивают повышенную защиту государственных и корпоративных структур от внешних и внутренних угроз.

Банки, будучи важнейшим элементом национальной экономики, попадают под действие этого закона.

Закон № 187-ФЗ предусматривает обязательные требования для участников банковской системы:

- установку сертифицированных средств защиты информации;
- ограничение физического доступа к серверам и устройствам;
- регулярное обновление программного обеспечения и операционных систем;
- ведение журналов регистрации событий безопасности;
- проведение регулярных проверок и аудитов систем безопасности.

Российские банки активно внедряют централизованные системы мониторинга событий безопасности (SIEM), позволяющие оперативно реагировать на любые подозрительные активности в информационной системе. Данная мера способствует раннему выявлению угроз и снижает риск успешной кибератаки.

Законом установлено требование обязательного резервирования и дублирования информационных систем и каналов связи (статья 10 Закона № 187-ФЗ).

Организация обязана осуществлять подготовку специалистов, занимающихся вопросами информационной безопасности (Приказ ФСТЭК № 235). Сотрудники, работающие с системой КИИ, проходят специальную аттестацию и периодически подтверждают свою квалификацию.

Исполнение этих требований положительно сказывается на повышении общей устойчивости банковской системы и гарантирует эффективную защиту важной государственной инфраструктуры от любых воздействий, что укрепляет позиции российского государства в области информационной безопасности.

ФЗ № 161 «О национальной платёжной системе» вступил в силу в июне 2011 года и регулирует деятельность операторов платёжных систем, организаторов расчётов и банковских организаций. Закон закрепляет правовой статус НПС и вводит важные положения, касающиеся информационной безопасности:

1. Регистрация и лицензирование операторов платёжных систем, включая оценку соответствия утверждённым критериям безопасности и надёжности.
2. Банки обязаны принять меры по защите информации, содержащейся в платёжных сервисах, от несанкционированного доступа, утраты или искажения.
3. Банки обязаны хранить и обрабатывать личные данные клиентов исключительно в предусмотренных законом целях и в соответствии с требованиями законодательства РФ о защите персональных данных.
4. Граждане имеют право на возмещение средств в случае необоснованного списания, ошибок в платежах или сбоев в системе. Банки обязаны незамедлительно уведомлять клиентов обо всех операциях и возвращать деньги в установленный срок.
5. Банки, осуществляющие международные расчёты, обязаны соблюдать действующие в России законы и нормативные акты, регулирующие международные платежи и операции.

6. Выявление нарушений влечёт наложение административных взысканий, вплоть до приостановления лицензии на проведение платёжных операций.

Одним из важных эффектов введения Федерального закона № 161-ФЗ стало укрепление позиций России в вопросах цифрового суверенитета. Национальная платёжная система, регулируемая на законодательном уровне, уменьшает зависимость от зарубежных платёжных систем и повышает управляемость процессом электронных платежей. Закон стимулирует развитие отечественного программного обеспечения и аппаратных решений, что снижает риски санкций и форс-мажорных обстоятельств, связанных с зависимостью от иностранных поставщиков.

Постановление Правительства РФ от 8 февраля 2018 г. № 127 категорирует объекты критической информационной инфраструктуры (КИИ) Российской Федерации, устанавливает показатели критериев значимости. Поскольку банковская система признана объектом КИИ, данное постановление распространяется и на банки.

Благодаря установлению единых требований и механизмов контроля российские банки улучшают свои системы защиты, снижают риски кибератак и обеспечивают защиту информации, находящейся в их распоряжении. Нормативные акты действуют как инструменты государственного регулирования, формирующие необходимую правовую базу для полноценного функционирования банковской системы России в условиях повышенного риска информационных угроз.

В ответ на резкое увеличение числа кибератак на российские организации после начала СВО российское государство предприняло ряд законодательных инициатив, направленных на укрепление технологического суверенитета и информационной безопасности.

Указ Президента РФ № 166 от 30 марта 2022 года:

- запрещает закупку иностранного ПО для значимых объектов критической информационной инфраструктуры без согласования с уполномоченными органами;
- устанавливает поэтапный переход на отечественные решения, завершившийся полным запретом на использование иностранного ПО с 1 января 2025 года;
- поручает правительству создать систему мониторинга и контроля, а также наладить подготовку кадров в сфере разработки и сопровождения отечественных решений [20].

Основной целью Указа является обеспечение технологической независимости и безопасности критической информационной инфраструктуры РФ.

Указ Президента РФ № 250 от 1 мая 2022 года:

- определяет порядок реагирования на кибератаки и привлечения к мероприятиям по кибербезопасности только аккредитованных и лицензированных организаций;
- вводит запрет на использование средств защиты информации из недружественных иностранных государств [13].

Эти меры направлены на снижение зависимости от зарубежных технологий и повышение устойчивости российской инфраструктуры к внешним угрозам.

Риск-ориентированный подход представляет собой комплексное сочетание методов управления киберрисками и сбалансированного применения мер защиты, что позволяет свести к минимуму остаточный киберриск. Процесс управления рисками начинается с их тщательного выявления и качественной оценки, после чего формируются планы по минимизации рисков в зависимости от их критичности. Далее осуществляется постоянный мониторинг существующих рисков и своевременное выявление новых угроз.

Инфраструктура банковской отрасли должна соответствовать ряду нормативных требований, но дополнительно к этому эффективно реализовывать риск-

ориентированный подход. Это означает, что все составляющие банковской инфраструктуры — от серверных ферм и сетевого оборудования до автоматизированных рабочих мест и банковских приложений — нуждаются в постоянной модернизации и мониторинге для обеспечения необходимого уровня защиты, что приводит к повышению уровня киберустойчивости банковской отрасли, которая является одной из важнейших составляющих цифрового суверенитета нашей страны.

Основные киберриски типовой банковской инфраструктуры

Важнейшими факторами риска банковской инфраструктуры являются:

- масштаб клиентской базы: большой круг клиентов, обладающих доступом к крупным финансовым ресурсам, делает банковскую инфраструктуру привлекательной целью для преступников;
- постоянное обновление технологий и устройств: быстрое развитие новых технологий и устройств создаёт дополнительную поверхность для атак. Банки вынуждены оперативно реагировать на новые виды угроз, внедряя передовые решения по защите данных и систем;
- интеграция физических и виртуальных элементов инфраструктуры: современная банковская инфраструктура сочетает физические активы (офисы, банкоматы, дата-центры) и виртуальные компоненты (интернет-банкинг, мобильные приложения, облака). Такое переплетение создаёт дополнительные уязвимости и увеличивает сложность управления рисками. Рост доли онлайн-взаимодействий и расширение дистанционного обслуживания приводят к увеличению числа возможных объектов атак.

Несмотря на значительное улучшение качества и скорости обслуживания клиентов, цифровая трансформация сопровождается появлением новых рисков, среди которых выделяют:

- финансовую уязвимость: увеличение доли цифровых операций ведёт к росту числа мошеннических операций. По данным Банка России, в 2025 году объём похищенных мошенниками средств составил 29,3 млрд рублей [12];
- операционные сбои: нарушение работоспособности цифровых каналов способно приводить к значительным экономическим убыткам и потере доверия клиентов;
- утечку данных: масштабное накопление больших объёмов данных создаёт предпосылки для массовых утечек персональной информации;
- правовые и регуляторные риски: быстрое развитие цифровых технологий опережает темпы формирования адекватного правового регулирования, создавая правовую неопределённость и затрудняя эффективное реагирование на инциденты [8].

Таким образом, цифровая трансформация, являясь мощным драйвером экономического роста, одновременно порождает комплекс новых рисков. Риск-ориентированный подход необходим для эффективного управления киберрисками в банковской сфере. Он позволяет банкам лучше подготовиться к возможным угрозам, заблаговременно выявлять новые риски и грамотно распределять ресурсы на их минимизацию. Только комплексный подход, основанный на сочетании мониторинга, анализа и постоянных улучшений, способен обеспечить высокий уровень киберустойчивости и надёжно защитить банковскую инфраструктуру от атак.

Типология современных угроз

Геополитические потрясения, начавшиеся в феврале 2022 года, оказали радикальное влияние на состояние кибербезопасности в России. Эти изменения привели к возникновению новой реальности, в рамках которой традиционные угрозы многократно усилились, а также появились совершенно новые вызовы, требующие немедленной реакции и переосмысления существующих практик защиты.

Сразу после начала специальной военной операции (СВО) наблюдается резкое увеличение числа кибератак на российские организации, включая финансовые. По данным Банка России, число кибератак на российские банки в первом полугодии 2022 года увеличилось в три раза по сравнению с аналогичным периодом прошлого года. Всего за указанный период было зафиксировано более 1 миллиона кибератак различной направленности, что сопоставимо с объёмом атак за предшествующие семь лет.

Необходимо отметить ограничение взаимодействия с западными поставщиками. Ряд российских организаций попали в список Specially Designated Nationals (SDN), введённый Министерством финансов США. Это означает полное ограничение возможностей взаимодействия с американскими компаниями, включая поставщиков решений в области кибербезопасности. Фактически более 85% зарубежных вендоров прекратили свою деятельность на территории России, оставив многие организации без необходимого оборудования и программного обеспечения для защиты от киберугроз.

Российские компании столкнулись с рядом непредвиденных трудностей, вызванных уходом западных поставщиков:

- рост числа таргетированных атак и усложнение используемых злоумышленниками техник;
- ограничение поставок импортного IT-оборудования;
- удаление российских приложений из мировых магазинов мобильных приложений;
- полный отказ от технической поддержки и прекращение выпуска обновлений, включая патчи безопасности;
- угроза отзыва сертификатов международных удостоверяющих центров;
- проблемы с использованием открытого ПО (OpenSource) для организаций, попавших под санкции.

Все перечисленные факторы привели к деградации средств защиты информации (СЗИ) многих организаций, что выразилось в отключении или полном выходе из строя межсетевых экранов, прекращении подписки на базы уязвимостей, отсутствии актуальной аналитики по киберугрозам и прекращении работы сервисов динамического анализа почтового трафика.

Международные группировки начали организованную кампанию против российских организаций. Было выявлено более 45 активных хакерских объединений, преимущественно проукраинской и прозападной ориентации, объединивших более 1 миллиона участников. Среди наиболее заметных группировок:

- IT Army of Ukraine (Украина);
- Кибер-Партизаны (Беларусь);
- Head Mare (Украина);
- BO Team (Украина);
- Anonymous (международное объединение).

Эти группы проводили скоординированные атаки на критически важные объекты инфраструктуры, включая банки, медиахолдинги и логистические компании. Среди наиболее громких инцидентов пострадали такие известные бренды, как RuTube, CDEK, Delivery Club, ivi и Первый канал. Эти атаки вызвали временное прекращение работы сервисов, утечку данных и потерю доверия со стороны клиентов.

Последние годы отмечены серией масштабных кибератак на российские организации, среди которых особо выделяются:

- Аэрофлот (2025) — атака украинского объединения Silent Crow и Belarus Cyber-Partisans, приведшая к отмене более 100 рейсов, сбоям в бронировании и выводу из строя около 7 тыс. серверов [7, 11];
- Винлаб (2025) — крупная атака программ-вымогателей, временно нарушившая работу более 2 тыс. магазинов [11];
- СДЭК (2024) — сбой в работе сайта и пунктов выдачи, вызванный внешним воздействием [6];
- ВГТРК (2024) — кратковременный сбой онлайн-вещания и внутренних сервисов [6].

Эти инциденты не только нанесли прямой экономический ущерб, но и проде-

монстрировали уязвимость критически важной инфраструктуры перед лицом современных киберугроз.

Значительная часть атак носила ярко выраженный политический характер. Перечисленные выше международные группировки проводят скоординированные кампании, направленные на дестабилизацию российской инфраструктуры. Политически мотивированные кибератаки становятся инструментом гибридных войн, что требует от государства принятия незамедлительных мер по укреплению цифрового суверенитета.

В ответ на указанные вызовы российское государство предприняло ряд законодательных инициатив, направленных на укрепление технологического суверенитета и информационной безопасности. Основные из них были перечислены выше.

Одной из ключевых проблем на пути к достижению полноценного цифрового суверенитета является острейший дефицит квалифицированных специалистов в области информационной безопасности. Нехватка специалистов по ИБ в России — порядка 50 тысяч человек. Не хватает экспертов, чтобы закрыть половину всех имеющихся на рынке вакансий. Особенно востребованы специалисты в ИТ-компаниях, банках и розничной торговле [15]. Дефицит объясняется несколькими причинами:

- большая часть опытных специалистов уже трудоустроена;
- выпускники вузов требуют дополнительного обучения и адаптации;
- молодые специалисты предпочитают профессии, связанные с разработкой и аналитикой, оставляя сферу кибербезопасности с меньшим интересом;
- быстрый рост потребностей рынка опережает возможности образовательной системы, которая выпускает всего 10-15 тыс. специалистов ежегодно, что покрывает лишь малую часть спроса [3, 14, 16, 19, 23].

Несмотря на имеющиеся трудности, существует позитивная динамика в увеличении числа занятых в сфере кибербезопасности. С 2016 по 2023 год количество специалистов удвоилось и достигло 110 тыс. человек. Эксперты прогнозируют дальнейший рост до 181-196 тыс. к 2027 году, хотя дефицит кадров останется значительным — около 54-65 тыс. специалистов [16, 23].

Геополитические изменения, произошедшие в 2022 году, создали абсолютно новую реальность для российских организаций, включая финансовые. Возросшая интенсивность атак, ограничение доступа к технологиям и разрыв связей с иностранными поставщиками поставили перед российским бизнесом беспрецедентные вызовы. Решение этих проблем требует срочной мобилизации ресурсов, перехода на отечественные разработки и формирования новых подходов к обеспечению кибербезопасности, способных выдержать давление внешней агрессии и сохранить устойчивость национальной финансовой системы.

Типология современных угроз типовой банковской инфраструктуры

Современные кибератаки отличаются высоким уровнем организованности, профессионализмом и разнообразием техник. Анализируя современную ситуацию в сфере кибербезопасности, эксперты выделяют ряд наиболее опасных типов атак, направленных против банков и финансовых учреждений.

1. **Фишинг и социальная инженерия**

Фишинговые атаки продолжают оставаться одним из самых распространённых способов похищения конфиденциальной информации. Преступники применяют высокотехнологичную социальную инженерию, маскируясь под официальных представителей банков и вынуждая пользователей раскрывать личные данные. Под угрозой находятся личные счета, карты и персональные данные клиентов [2, 24].

2. **Целевые атаки (Advanced Persistent Threats, APT)**

Это самые опасные и технически сложные виды атак, организованные профессиональными группами с финансированием государств или преступных синдикатов. Такие атаки нацелены на длительную скры-

тую эксплуатацию уязвимостей с целью систематического сбора ценных данных, включая исходные коды и внутреннюю документацию компаний, а также нанесения максимального ущерба [9].

3. **Программы-шпионы и вымогатели (Ransomware)**

Программные вирусы, крадущие данные или шифрующие файлы, требуют выкуп за восстановление работоспособности системы. Масштаб заражения настолько велик, что даже государственные ведомства подвергаются подобным атакам.

4. **Ботнеты и распределённые атаки отказа в обслуживании (DDoS)**

DDoS-атаки направлены на перегрузку серверов банков и сетей связи, что приводит к временной утрате доступности сервисов. Подобные атаки наносят серьёзный репутационный и экономический ущерб, вызывая недовольство клиентов и потерю конкурентоспособности [9]. Создаются ботнеты — сети заражённых компьютеров, способные генерировать мощные потоки запросов, приводящие к перегрузкам и остановке работы важнейших систем банков.

5. **Угроза искусственного интеллекта (ИИ), включая LLM и мультиагентные системы**

Совершенствование технологий искусственного интеллекта и возникновение больших языковых моделей (Large Language Models, LLM) привело к появлению новых классов угроз, представляющих особую опасность для банковской инфраструктуры. В последние годы наибольшую озабоченность вызывают две разновидности угроз:

- генеративный ИИ;
- агенты на основе LLMs;
- мультиагентные системы.

Развитие технологий ИИ открывает широкие перспективы для автоматизации процессов и повышения эффективности, но одновременно создаёт дополнительные риски. Хакеры активно осваивают технологии генеративного ИИ для создания сложных вредоносных программ, способных адаптироваться к защитным механизмам и избегать обнаружения традиционными средствами защиты, а также дипфейков и персонализированных фишинговых писем, используемых для подделывания личности сотрудников банка или клиентов.

LLM обладают огромной мощностью и широким спектром способностей, включая умение имитировать поведение людей, создавать убедительные тексты и взламывать системы с минимальным вмешательством человека. В руках злоумышленников эти технологии могут стать эффективным оружием для реализации широкомасштабных атак:

- имитация легитимных персон — подделка электронных писем, голосовых сообщений и чат-ботов, для убеждения сотрудников банков раскрыть конфиденциальную информацию;
- генерация контента, в том числе персонифицированного, для атак — агенты LLMs способны создавать качественные материалы для фишинга, социальной инженерии и дезинформации;
- автоматизация атак — атаки могут происходить в массовом масштабе, при этом агент LLM сможет точно выбирать жертвы и подбирать индивидуальные сценарии нападения.

Появились мультиагентные системы, в которых агенты скоординированно выполняют отдельную роль/функцию в рамках единой миссии, усиливая совокупную мощность атак:

- распределённая атака на систему — несколько агентов могут одновременно атаковать разные участки инфраструктуры банка, отвлекая ресурсы защиты и увеличивая шансы успеха атаки;
- совместная разведка и эксплуатация уязвимостей — мультиагенты могут параллельно искать уязвимости и совместно вырабатывать стратегию их эксплуатации;
- самообучение и адаптация — мультиагентные системы способны учиться на предыдущих действиях и адаптироваться к изменениям в инфраструктуре банка, что значительно осложняет усилия по их нейтрализации.

6. **Угроза внутреннего нарушителя (инсайды)**

Проблема инсайдерских угроз заключается в действиях сотрудников, имеющих легитимный доступ к информационным системам банка. Ранее исследования показывали, что такие нарушители занимали бóльшую долю в проводимых атаках. Недовольство персонала, халатность или корысть могут привести к серьёзным инцидентам, связанным с утечкой данных или нанесением ущерба инфраструктуре [10].

7. **Финансовые мошенничества**

Классические мошеннические схемы, такие как подделка электронных писем, фальсификация реквизитов и социальная инженерия, продолжают представлять значительную угрозу. Эксперты отмечают, что в 2025 году вероятность значительных инцидентов информационной безопасности составляет от 12% до 20%, а к 2026 году этот показатель может увеличиться до уровня выше 25% [5].

8. **Взлом API-интерфейсов**

API-интерфейсы являются неотъемлемой частью архитектуры современных банковских приложений. На совместных открытых API построены сервисы открытого банкинга (Open banking), когда банки обмениваются информацией о счетах и транзакциях, а также предоставляются сервисы сторонних организаций через поверхность банка [1]. Это позволяет клиентам в одном приложении видеть счета и балансы разных банков, а также получать услуги сторонних сервисов. Компрометация API способна привести к массовым утечкам данных и финансовым потерям, затрагивающим большое количество клиентов [21]. Актуальность данной атаки возрастает в связи с выходом финансовых организаций в облака, наращиванием взаимодействия, началом развития ИИ помощников и AI агентов, которые просто не смогут работать без открытых API.

В современном ландшафте угроз всё более доминирующую позицию занимают сложные, многогранные атаки, основанные на использовании AI, LLMs и мультиагентных систем. Эти технологии серьёзно усложняют традиционные подходы к обеспечению информационной безопасности и требуют радикально новых подходов к построению систем защиты.

Заключение

Рассмотрены основные тенденции и угрозы, влияющие на устойчивость финансовых учреждений, а также проанализированы регуляторные требования и законодательные инициативы, направленные на укрепление защиты данных и инфраструктуры банков.

Современная цифровая среда диктует необходимость выработки комплексной стратегии кибербезопасности, сочетающей технические, организационные и правовые меры. Банковская отрасль сталкивается с широким спектром угроз, начиная от традиционного фишинга и заканчивая высокоорганизованными APT-операциями, реализуемыми в реальном времени мультиагентными системами. Эффективное противостояние этим вызовам возможно только при условии тесного сотрудничества между государством, бизнесом и научным сообществом, направленного на формирование устойчивой и надёжной системы защиты национальных экономических интересов.

Представленный обзор показывает, насколько важны современные СЗИ и умение предвидеть угрозы для устойчивого функционирования банков. Основными выводами статьи являются:

- высокая степень зависимости финансовой системы от надёжности информационных сетей и коммуникаций;
- необходимость постоянного мониторинга текущих угроз и адаптации систем защиты к новым технологиям;
- рост влияния регуляторов и законодателей на политику безопасности банков.

Цифровой суверенитет является необходимым условием для сохранения национальной безопасности и независимости в условиях современных геополитических вызовов. Российская Федерация предпринимает активные шаги по укреплению тех-

нологического суверенитета, однако существующие проблемы в области кадрового обеспечения и технологической независимости требуют скорейшего разрешения.

Текущий тренд развития систем защиты должен быть направлен на кардинальное повышение эффективности борьбы с новыми поколениями угроз, вызванных появлением таких технологий, как агенты ИИ и мультиагентные атакующие системы. Сегодня количество ежедневно регистрируемых киберсобытий измеряется триллионами, и с активным внедрением агентов ИИ это число увеличится на порядки. Следовательно, новое поколение систем защиты должно уметь не только оперативно обрабатывать и анализировать миллиарды событий в реальном времени, но и выявлять скрытую корреляцию между отдельными инцидентами, происходящими в гетерогенных системах и сетях.

ЛИТЕРАТУРА

1. База знаний Открытого банкинга в России [Электронный ресурс]. URL: https://wiki.openbankingrussia.ru
2. Юдина О. Бизнес под защитой: как интернет-банк СберБизнес обеспечивает безопасность данных [Электронный ресурс]. URL: https://sberbusiness.live/publications/biznes-pod-zaschitoi-kak-internet-bank-sberbiznes-obespechivaet-bezopasnost-dannih
3. В России дичайший дефицит ИБ-специалистов. Все хорошие уже заняты, а вузы выпускают «сырых» [Электронный ресурс]. URL: https://www.cnews.ru/news/top/2025-02-04_v_rossii_dichajshchij_defitsit
4. Чернов А. В Сбере рассказали о развитии своего банкоматного сервиса [Электронный ресурс]. URL: https://www.gazeta.ru/business/news/2023/06/27/20754836.shtml
5. Пославская Ю., Буйлов М. Вероятность ИБ-инцидентов в финансовой сфере может превысить 25% [Электронный ресурс]. URL: https://www.kommersant.ru/doc/8006168
6. Ясакова Е. Винлаб, ВГТРК, СДЭК: какие ещё компании пострадали от хакерских атак [Электронный ресурс]. URL: https://hi-tech.mail.ru/review/131095-vinlab-vgtrk-sdek-kakie-eshe-kompanii-postradali-ot-hakerskih-atak/
7. Пашкова Л. Власти дали рекомендации перевозчикам после хакерской атаки на «Аэрофлот» [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/09/09/2025/68bfa9a99a794763c9f0bf05
8. Информационная безопасность в банках [Электронный ресурс]. URL: https://www.tadviser.ru/a/314707
9. Какие угрозы информационной безопасности наиболее опасны в 2025 году и как бизнесу защититься от утечек, атак и сбоев [Электронный ресурс]. URL: https://www.kt-team.ru/blog/cybersecurity-threats-2025
10. Кибератаки 2025: что нового готовят злоумышленники [Электронный ресурс]. URL: https://www.computerra.ru/312655/kiberataki-2025-chto-novogo-gotovyat-zloumyshlenniki
11. Миллионные убытки: почему от хакеров страдают даже компании-гиганты и как защитить свой бизнес от кибератак [Электронный ресурс]. URL: https://incrussia.ru/share/letnie-vzlomy-2025
12. Болотов С. Мошенники поставили рекорд по хищениям со счетов россиян в банках в 2025 году [Электронный ресурс]. URL: https://rg.ru/2026/02/16/moshenniki-postavili-rekord-po-hishcheniiam-so-schetov-rossiian-v-bankah-v-2025-godu.html?utm_referrer=https%3A%2F%2Fwww.google.com%2F
13. Заведенская А. Разъяснения к Указу Президента о дополнительных мерах по обеспечению ИБ (№ 250 от 01.05.2022) [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/President-Decree-250-Clarifications

14. Катковская Ю. Российский IT-рынок 2025: парадокс кадрового голода на фоне рекордной безработицы [Электронный ресурс]. URL: https://tproger.ru/articles/rossijskij-it-rynok-2025--paradoks-kadrovogo-goloda-na-fone-rekordnoj-bezraboticy
15. Быстрова Е. Рынок ИБ в 2025: нехватка кадров и рост зарплат до миллиона рублей [Электронный ресурс]. URL: https://www.anti-malware.ru/news/2025-05-27-111332/46173
16. Рынок труда в информационной безопасности в России в 2024–2027 гг.: прогнозы, проблемы и перспективы [Электронный ресурс]. URL: https://ptsecurity.com/research/analytics/rynok-truda-v-informaczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy
17. Соловьев И. Сбербанк лидирует по числу банкоматов и качеству их обслуживания [Электронный ресурс]. URL: https://www.newsinfo.ru/news/2015-09-28/bankomats/778845
18. Сбербанк удаляет ПО Citrix и переводит 150 тыс. сотрудников на российскую инфраструктуру виртуальных рабочих мест [Электронный ресурс]. URL: https://www.tadviser.ru/a/829352
19. Спрос рождает удаление [Электронный ресурс]. URL: https://www.kommersant.ru/doc/7478242
20. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента РФ от 30.03.2022 № 166 [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/47688
21. Минаев И. Цифровизация в банковской сфере [Электронный ресурс]. URL: https://boostra.ru/pages/articles/tsifrovizatsiya-bankovskikh-uslug-vozmozhnosti-i-vyzovy
22. ЦОДы Сбербанка [Электронный ресурс]. URL: https://www.tadviser.ru/a/469027
23. ЦСР «Северо-Запад» и Positive Technologies представили исследование по дефициту кадров на рынке кибербезопасности РФ [Электронный ресурс]. URL: https://habr.com/ru/news/820237
24. Петрова Ю. Эксперты назвали главные киберугрозы для банков и их клиентов в 2025 году [Электронный ресурс]. URL: https://www.forbes.ru/finansy/528907-eksperty-nazvali-glavnye-kiberugrozy-dla-bankov-i-ih-klientov-v-2025-godu

Cyberthreats and Banking Infrastructure Security: an Analysis in the Context of Ensuring Russia's Digital Sovereignty

Sergei Vladimirovich Lebed — Vice President for Cybersecurity at Sberbank PJSC.
E-mail: svlebed@sberbank.ru

This article examines modern cyberthreats affecting the resilience of the Russian Federa-tion's banking infrastructure in the context of ensuring the country's digital sovereignty. It analyzes an information infrastructure of large financial institutions, including server farms, ATM networks, automated workstations, network equipment, and cybersecurity systems. Par-ticular attention is paid to regulatory requirements imposed on credit institutions, including Federal Law No. 187-FZ "On the Security of Critical Information Infrastructure", Federal Law No. 161-FZ "On the National Payment System", as well as regulatory acts of the Bank of Russia. The author systematizes the main cyber risks and presents a typology of modern threats, including fishing, APT attacks, ransomware, DDoS attacks, as well as new challenges associated with the use of artificial intelligence technologies, large-scale language models, and multi-agent systems. The author concludes that a comprehensive approach to ensuring the cybersecurity of the banking sector is essential as a crucial element of Russia's digital sovereignty.

Keywords: cybersecurity, banking infrastructure, digital sovereignty, cyber threats, critical information infrastructure, APT attacks, artificial intelligence, multi-agent systems, regulatory requirements, financial sector

REFERENCES

1. Baza znaniy Otkrytogo bankinga v Rossii [Electronic resource]. URL: https://wiki.openbanking-grussia.ru (in Russian).
2. Yudina O. Biznes pod zashchitoy: kak internet-bank SberBiznes obespechivaet bezopasnost dannykh [Electronic resource]. URL: https://sberbusiness.live/publications/biznes-pod-zaschitoi-kak-internet-bank-sberbiznes-obespechivaet-bezopasnost-dannih (in Russian).
3. V Rossii dichayshiy defitsit IB-spetsialistov. Vse khoroshie uzhe zanyaty, a vuzy vypuskayut «syrykh» [Electronic resource]. URL: https://www.cnews.ru/news/top/2025-02-04_v_rossii_dichajshchij_defitsit (in Russian).
4. Chernov A. V Sbere rasskazali o razvitii svoego bankomatnogo servisa [Electronic resource]. URL: https://www.gazeta.ru/business/news/2023/06/27/20754836.shtml (in Russian).
5. Poslavskaya Yu., Buylov M. Veroyatnost IB-intsidentov v finansovoy sfere mozhet prevysit 25% [Electronic resource]. URL: https://www.kommersant.ru/doc/8006168 (in Russian).
6. Yasakova E. Vinlab, VGTRK, SDEK: kakie eshche kompanii postradali ot khakerskikh atak [Electronic resource]. URL: https://hi-tech.mail.ru/review/131095-vinlab-vgtrk-sdek-kakie-eshe-kompanii-postradali-ot-hakerskih-atak/ (in Russian).
7. Pashkova L. Vlasti dali rekomendatsii perevozchikam posle khakerskoy ataki na «Aeroflot» [Electronic resource]. URL: https://www.rbc.ru/technology_and_media/09/09/2025/68bfa9a99a794763c9f0bf05 (in Russian).
8. Informatsionnaya bezopasnost v bankakh [Electronic resource]. URL: https://www.tadviser.ru/a/314707 (in Russian).
9. Kakie ugrozy informatsionnoy bezopasnosti naibolee opasny v 2025 godu i kak biznesu zashchititsya ot utechek, atak i sboev [Electronic resource]. URL: https://www.kt-team.ru/blog/cybersecurity-threats-2025 (in Russian).
10. Kiberataki 2025: chto novogo gotovyat zloumyshlenniki [Electronic resource]. URL: https://www.computerra.ru/312655/kiberataki-2025-chto-novogo-gotovyat-zloumyshlenniki (in Russian).
11. Millionnye ubytki: pochemu ot khakerov stradayut dazhe kompanii-giganty i kak zashchitit svoy biznes ot kiberatak [Electronic resource]. URL: https://incrussia.ru/share/letnie-vzlomy-2025 (in Russian).
12. Bolotov S. Moshenniki postavili rekord po khishcheniyam so schetov rossiyan v bankakh v 2025 godu [Electronic resource]. URL: https://rg.ru/2026/02/16/moshenniki-postavili-rekord-po-hishcheniiam-so-schetov-rossiian-v-bankah-v-2025-godu.html (in Russian).
13. Zavedenskaya A. Razyasneniya k Ukazu Prezidenta o dopolnitelnykh merakh po obespecheniyu IB (№ 250 ot 01.05.2022) [Electronic resource]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/President-Decree-250-Clarifications (in Russian).
14. Katkovskaya Yu. Rossiyskiy IT-rynok 2025: paradoks kadrovogo goloda na fone rekordnoy bezrabotitsy [Electronic resource]. URL: https://tproger.ru/articles/rossijskij-it-rynok-2025--paradoks-kadrovogo-goloda-na-fone-rekordnoj-bezraboticy (in Russian).
15. Bystrova E. Rynok IB v 2025: nekhvatka kadrov i rost zarplat do milliona rubley [Electronic resource]. URL: https://www.anti-malware.ru/news/2025-05-27-111332/46173 (in Russian).
16. Rynok truda v informatsionnoy bezopasnosti v Rossii v 2024–2027 gg.: prognozy, problemy i perspektivy [Electronic resource]. URL: https://ptsecurity.com/research/analytics/rynok-truda-v-informaczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy (in Russian).
17. Solovyev I. Sberbank lidiruet po chislu bankomatov i kachestvu ikh obsluzhivaniya [Electronic resource]. URL: https://www.newsinfo.ru/news/2015-09-28/bankomats/778845 (in Russian).
18. Sberbank udalyaet PO Citrix i perevodit 150 tys. sotrudnikov na rossiyskuyu infrastrukturu virtualnykh rabochikh mest [Electronic resource]. URL: https://www.tadviser.ru/a/829352 (in Russian).

19. Spros rozhdaet udalenie [Electronic resource]. URL: https://www.kommersant.ru/doc/7478242 (in Russian).
20. O merakh po obespecheniyu tekhnologicheskoy nezavisimosti i bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Ukaz Prezidenta RF ot 30.03.2022 № 166 [Electronic resource]. URL: http://www.kremlin.ru/acts/bank/47688 (in Russian).
21. Minaev I. Tsifrovizatsiya v bankovskoy sfere [Electronic resource]. URL: https://boostra.ru/pages/articles/tsifrovizatsiya-bankovskikh-uslug-vozmozhnosti-i-vyzovy (in Russian).
22. TsODy Sberbanka [Electronic resource]. URL: https://www.tadviser.ru/a/469027 (in Russian).
23. TsSR «Severo-Zapad» i Positive Technologies predstavili issledovanie po defitsitu kadrov na rynke kiberbezopasnosti RF [Electronic resource]. URL: https://habr.com/ru/news/820237 (in Russian).
24. Petrova Yu. Eksperty nazvali glavnye kiberugrozy dlya bankov i ikh klientov v 2025 godu [Electronic resource]. URL: https://www.forbes.ru/finansy/528907-eksperty-nazvali-glavnye-kiberugrozy-dla-bankov-i-ih-klientov-v-2025-godu (in Russian).