Социальная инженерия как метод финансового мошенничества в кредитно-финансовой сфере: техники и факторы уязвимости

Павел Владимирович РЕВЕНКОВ
доктор экономических наук,
профессор кафедры информационной безопасности,
Финансовый университет при Правительстве Российской Федерации,
4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия.
E-mail: PVRevenkov@fa.ru
https://orcid.org/0000-0002-0354-0665

Марина Дмитриевна Шуликова,
студентка 3-го курса, Финансовый университет при Правительстве Российской Федерации, Российская Федерация, Москва, 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456
E-mail: 230867@edu.fa.ru
https://orcid.org/0009-0005-8113-3167

Аннотация. В статье рассматривается социальная инженерия как доминирующий метод осуществления финансового мошенничества в кредитно-финансовой сфере. Проанализированы предпосылки роста атак и этапы их реализации. Раскрыт механизм эксплуатации когнитивных искажений, на которых строятся техники манипулятивного воздействия. Особое внимание уделено современным гибридным схемам, сочетающим социальную инженерию с использованием технологий искусственного интеллекта и вредоносного программного обеспечения. Рассматриваются правовые аспекты квалификации таких преступлений и проблема возврата похищенных средств.

Ключевые слова: социальная инженерия, кибермошенничество, претекстинг, когнитивные искажения

Social engineering as a method of financial fraud in the credit and financial sector: techniques and vulnerability factors

Pavel V. Revenkov
Doctor of Economics, Professor, Department of Information Security,
Financial University under the Government of the Russian Federation,
4th Veshnyakovsky Proezd, Building 4, Bldg. 2, Moscow, 109456, Russia.
E-mail: PVRevenkov@fa.ru
https://orcid.org/0000-0002-0354-0665

Marina D. Shulikova,
Third-year student, Financial University under the Government of the Russian Federation, Russian Federation, Moscow, 4th Veshnyakovsky Proezd, Building 4, Bldg. 2, Moscow, 109456
E-mail: 230867@edu.fa.ru
https://orcid.org/0009-0005-8113-3167

Abstract. The article considers social engineering as the dominant method of financial fraud in the credit and financial sector. The drivers behind the growth of attacks and the stages of their implementation are analyzed. The mechanism of exploiting cognitive biases, which form the basis of manipulative techniques, is revealed. Particular attention is paid to modern hybrid schemes that combine social engineering with artificial intelligence technologies and malicious software. The legal aspects of qualifying such crimes and the problem of recovering stolen funds are also examined.

Keywords: social engineering, cyber fraud, pretexting, cognitive biases

Введение / Introduction

На сегодняшний день социальная инженерия является одной из наиболее серьезных угроз для кредитно-финансовой сферы. По данным Банка России, в первом квартале 2026 года 96,5% всех операций по переводу денежных средств без добровольного согласия клиентов было совершено с использованием методов социальной инженерии [1].

Социальная инженерия представляет собой метод финансового мошенничества, основанный на манипулировании людьми с целью получения конфиденциальной информации или побуждения к совершению определенных действий. В его основе лежит эксплуатация доверия: злоумышленник выстраивает взаимодействие таким образом, чтобы жертва добровольно раскрыла запрашиваемые сведения, выполнила необходимое ему действие либо осознанно отступила от установленных правил безопасности.

Рост числа атак с использованием социальной инженерии обусловлен несколькими факторами, среди которых в первую очередь следует выделить массовый переход банков на дистанционные каналы обслуживания [2]. С развитием новых сервисов и ростом объемов безналичных операций закономерно увеличивается и количество угроз. Удаленное оказание услуг подразумевает, что коммуникация между банком и клиентом все чаще разворачивается в среде, которую банк не контролирует. В этих условиях кредитной организации объективно сложнее отследить, какие именно действия совершаются на стороне пользователя и кем они инициированы.

Вместе с тем кредитно-финансовая сфера традиционно рассматривается как сфера с наиболее зрелыми техническими системами защиты информации, включающими криптографическую защиту данных при передаче и хранении, системы обнаружения вторжений и многофакторную аутентификацию. Однако при этом остается неизменным тот факт, что в любой информационной системе самым незащищенным звеном был и остается человек. Никакие технические средства не способны полностью исключить риск

манипулятивного воздействия на пользователя. Именно этот разрыв — между надежно выстроенной инфраструктурой и уязвимостью конечного пользователя — и создает условия, в которых социальная инженерия является одним из основных способов осуществления финансового мошенничества.

Привлекательность социальной инженерии для злоумышленников объясняется рядом особенностей, выгодно отличающих этот метод от технического взлома. К ним относятся простота реализации, доступность — для применения большинства техник не требуется специальных знаний, кроме нескольких психологических приемов. Также метод отличается малозатратностью и низкой степенью риска для атакующего. Кроме того, социальная инженерия демонстрирует высокую экономическую эффективность: даже если воздействию поддается лишь малая часть потенциальных жертв, это приносит злоумышленникам немалую прибыль [3].

Кредитно-финансовая сфера выступает приоритетной целью для применения методов социальной инженерии. Здесь злоумышленник получает не только конфиденциальные сведения о клиенте, но и прямой доступ к денежным средствам жертв. В отличие от многих других отраслей, где похищенные данные требуется дополнительно монетизировать, в финансовой сфере результат атаки достигается непосредственно: успешное применение методов социальной инженерии завершается прямым хищением денежных средств жертвы [4].

Материалы и методы / Materials and Methods

Теоретическую основу исследования составили труды российских и зарубежных ученых в области кибербезопасности, социальной инженерии, виктимологии и когнитивной психологии. Технологические и системные аспекты реализации атак социальной инженерии в кредитно-финансовой сфере раскрыты в работах П.В. Ревенкова и А.А. Бердюгина [2], а также А.А. Менщикова и М.Ю. Федосенко [4]. Психологические механизмы уязвимости человека перед методами социальной инженерии рассматриваются в работах В.А. Зорина [5], А.С. Унукович [3], Е.В. Зотиной [6], а также О.В. Медяник и Н.А. Низовских [7]. Теоретической основой для анализа манипулятивного воздействия послужили также рассмотренные Р.Б. Чалдини принципы социального влияния [8].

Нормативно-правовую базу исследования составили положения Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» [9].

Эмпирическую базу исследования составили статистические и аналитические материалы Центрального банка Российской Федерации [1], доклад Аналитического центра НАФИ [10], а также данные Ассоциации российских банков [11].

Методологическую основу исследования составили сравнительный анализ, классификация, систематизация, а также синтез психологических и технологических подходов к анализу механизмов социальной инженерии.

Обсуждение / Discussion

Атака социальных инженеров состоит из нескольких этапов. На первом этапе мошенники определяют вид и объем информации, необходимой им для совершения атаки, а также выбирают методы социальной инженерии, посредством которых эта информация будет получена.

После этого злоумышленники переходят к выбору потенциальной жертвы — лица, действия в отношении которого приведут к желаемой цели. Наиболее уязвимыми для манипулятивного воздействия оказываются люди, обладающие повышенной гипнабельностью, находящиеся в состоянии стресса либо имеющие хорошее воображение — именно эти характеристики облегчают социальному инженеру задачу по установлению контроля над жертвой [5].

Следующий этап — сбор информации из открытых источников (OSINT). Это один из самых распространенных стартовых этапов атаки. Злоумышленники изучают социальные сети, профессиональные сообщества, корпоративные сайты, объявления и форумы. Из профилей можно извлечь значительный объем данных: имя и фамилию, дату рождения, место жительства или работы, увлечения, имена коллег и членов семьи, фотографии. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя значительную часть информации в свободном доступе, что облегчает злоумышленникам сбор данных.

Еще одним источником данных выступают приобретенные или похищенные базы данных. Мошенники покупают на черном рынке либо добывают самостоятельно базы данных, содержащие персональные сведения клиентов интернет-магазинов, банков, мобильных операторов, социальных сетей, сервисов доставки. Нередко утечки происходят вследствие кибератак, а иногда — по вине сотрудников организаций или в результате случайных ошибок.

Собранная информация нужна для персонализации атаки. Анализ полученных сведений позволяет понять, какие темы интересуют человека, и составить его

психологический портрет. Располагая детализированным досье, мошенник может обратиться к жертве по имени, упомянуть близких, сослаться на реальную покупку или недавнюю поездку. Это позволяет вызвать доверие либо, напротив, спровоцировать панику — и в том, и в другом случае критическое мышление жертвы оказывается подавленным, что открывает злоумышленнику дорогу к завершающему этапу атаки.

В дальнейшем злоумышленники могут разработать претекст — заранее подготовленный сценарий, по которому злоумышленник будет взаимодействовать с жертвой [6]. Претекстинг предполагает конструирование ложной истории или легенды, с помощью которых мошенник сможет воздействовать на жертву и получить от нее конфиденциальную информацию.

Все техники социальной инженерии основаны на когнитивных искажениях. Когнитивные искажения — это систематические и повторяющиеся ошибки в мышлении человека, как правило, возникающие по определенным шаблонам в одних и тех же ситуациях на основе неверных суждений [7]. Когнитивные искажения становятся причиной искаженных интерпретаций и иррационального поведения.

Существует ряд исследований, которые делают попытку классифицировать наиболее распространенные механизмы психологического воздействия, эксплуатируемые в том числе в целях совершения противоправных действий. В частности, американским социальным психологом Робертом Чалдини были выделены и описаны шесть классических принципов влияния, которые лежат в основе многих техник манипуляции [8]. Хотя данные принципы не являются специфически «мошенническими» и широко применяются в маркетинге, рекламе и политике, именно они активно используются злоумышленниками в схемах социальной инженерии.

К числу таких принципов относятся:

Принцип авторитета. Люди склонны подчиняться или доверять тем, кого они воспринимают как авторитетов (руководство, представители правоохранительных органов, эксперты). Социальные инженеры часто выдают себя за таких лиц, чтобы вызвать безусловное доверие.

Принцип дефицита и срочности. Человеку свойственно ценить то, что является редким или доступно в ограниченное время. Угроза потери чего-либо или необходимость быстрого реагирования подталкивают к необдуманным действиям.

Принцип последовательности и обязательства. Люди стремятся быть последовательными в своих действиях и словах. Если жертва однажды согласилась на небольшую уступку, ее легче склонить к более значительному шагу.

Принцип взаимного обмена. Если кто-то сделал нам добро, мы чувствуем внутреннюю потребность ответить тем же. Злоумышленник может «помочь» жертве решить небольшую проблему, а затем попросить «взаимную услугу» в виде конфиденциальной информации.

Принцип благорасположения. Мы более склонны доверять и соглашаться с теми, кто нам нравится, кто похож на нас или кто делает нам комплименты. Поэтому зачастую эффективность действий мошенника зависит от того, смог ли он создать у потенциальной жертвы ощущение «своего».

Принцип социального доказательства. Люди склонны поступать так, как поступает большинство, особенно в неопределенных ситуациях. Если человек видит, что окружающие его люди поступают определенным образом, он склонен считать это правильным.

Существуют схемы мошенничества, в которых злоумышленники используют детей в качестве промежуточного звена для доступа к финансовым средствам родителей. Выбор ребенка в роли посредника не случаен: в силу возраста дети еще не обладают развитым критическим мышлением, хуже распознают попытки манипуляции и при этом имеют физический доступ к устройствам взрослых членов семьи.

Коммуникация с ребенком начинается в знакомой и психологически комфортной для него среде — как правило, это игровая платформа или мессенджер, где мошенник выдает себя за такого же игрока или сверстника. Установив контакт, преступник меняет тактику и переходит к запугиванию — теперь он выступает уже от имени «службы безопасности» или «правоохранительных органов», сообщая ребенку, что его родителям грозит серьезная опасность, избежать которой можно только немедленно выполнив все инструкции. Здесь злоумышленники эксплуатируют сразу два принципа влияния: эффект авторитета и эффект срочности, которые ограничивают способность ребенка критически оценить ситуацию.

Под диктовку мошенников ребенок совершает требуемые действия и помогает злоумышленникам осуществить перевод денежных средств со счетов родителей. При этом с точки зрения банка, операция является полностью легитимной — она совершена с устройства, которое регулярно используется клиентом, и подтверждена корректной аутентификацией (рисунок 1).[1]

[1] Рис. 1 Схема мошенничества «Ночные дети». Источник: составлено авторами

Рис.1. Схема мошенничества «Ночные дети»

Социальная инженерия стирает грань между ролями жертвы и соучастника, превращая человека, ставшего объектом манипуляции, в невольного участника преступного замысла. Именно эта особенность — добровольная передача жертвой конфиденциальной информации и совершение ею требуемых мошенником операций при отсутствии следов технического взлома или вмешательства в работу системы — служит причиной, по которой возврат похищенных средств крайне затруднен. Более того, не во всех случаях жертва догадывается о том, что стала участником мошеннической схемы, поскольку ее действия выглядят как обычные и легитимные банковские операции.

При этом банк как оператор по переводу денежных средств обязан возместить клиенту сумму операции, совершенной без его добровольного согласия, в случаях, которые установлены статьями 8 и 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» [9]. К ним относятся: неинформирование клиента о совершенной операции; осуществление операции после получения от клиента уведомления об утрате электронного средства платежа (ЭСП — средство, используемое для безналичных расчетов: банковская карта, мобильное приложение, электронный кошелек) или его использовании без согласия; неосуществление должного контроля и неприостановление подозрительной операции. Если же банк докажет, что клиент нарушил порядок использования электронного средства платежа — в частности, добровольно сообщил мошеннику конфиденциальные данные или коды подтверждения, — обязанность по возмещению не наступает.

В соответствии с данными, публикуемыми Банком России, доля возмещенных потерь на протяжении последних лет практически не поднимается выше 10%, и жертвы большинства эпизодов мошенничества не могут рассчитывать на компенсацию похищенных средств [1].

В последнее время широкое распространение получила мошенническая схема с так называемым «безопасным счетом». Жертву убеждают, что ее средства находятся под угрозой, и для их сохранности необходимо временно перевести деньги на специальный защищенный счет. В классическом варианте схема сводится к тому, что потерпевший под диктовку мошенника осуществляет перевод на счета дропов. Однако в последнее время данный сценарий все чаще дополняется этапом токенизации банковской карты через приложение Mir Pay.

При этом важно отметить, что технология токенизации является удобным и безопасным способом осуществления платежа. Она позволяет проводить офлайн-платежи простым прикладыванием смартфона к терминалу, а при онлайн-оплате исключает передачу реквизитов карты продавцу: вместо них используется зашифрованный цифровой токен, который генерируется для конкретного устройства и не может быть использован на другом.

Мошенники, однако, не пытаются взломать эту технологию — они воздействуют на ее пользователя. Действуя в рамках легенды о «безопасном счете», злоумышленники получают от жертвы реквизиты ее карты и коды из СМС-сообщений, после чего выпускают токен на собственном смартфоне. С этого момента они могут снимать наличные в банкоматах с NFC и оплачивать покупки от имени держателя карты (рисунок 2).[2]

[2] Рис. 2 Схема мошенничества «Mir Pay: токенизация карты жертвы». Источник: составлено авторами

Рис. 2. Схема мошенничества «Mir Pay: токенизация карты жертвы»

Стоит также отметить, что социальная инженерия на сегодняшний день распространяется через различные каналы коммуникации, которые не ограничиваются лишь телефонным мошенничеством. Мошенники могут взаимодействовать с потенциальными жертвами и в цифровом пространстве посредством электронной почты или мессенджеров. Расширение поля атаки происходит на фоне роста цифровой вовлеченности населения, которая, однако, не сопровождается сопоставимым повышением уровня цифровой грамотности пользователей.

По данным Аналитического центра НАФИ, который проводит ежегодный мониторинг цифровой грамотности россиян, 75% населения обладают базовым уровнем цифровых навыков, уверенно пользуясь цифровыми сервисами для решения повседневных задач. Вместе с тем исследование выявило и проблемные зоны: одна из наиболее выраженных трудностей связана с оценкой достоверности информации — этим навыком обладают лишь 59% россиян [10]. Таким образом, значительная часть пользователей, активно взаимодействуя с цифровой средой, остается недостаточно подготовленной к распознаванию попыток манипуляции, что создает благоприятные условия для применения методов социальной инженерии.

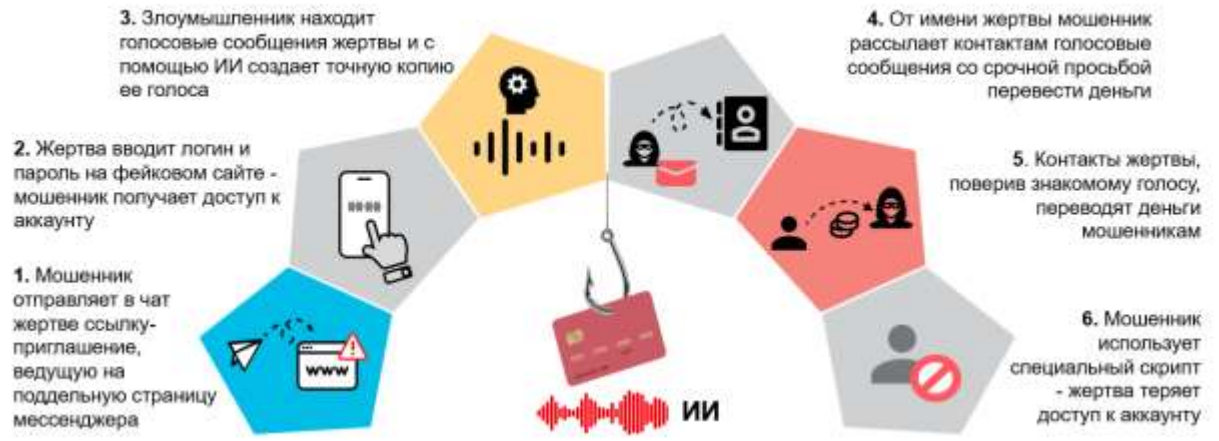
В настоящее время мошенники активно применяют технологии искусственного интеллекта, которые позволяют генерировать правдоподобный контент — грамматически корректный и стилистически адаптированный под конкретную ситуацию или получателя. Искусственный интеллект дает возможность создавать сообщения, практически

неотличимые от тех, которые могли бы исходить от известных компаний, государственных учреждений или знакомых людей.

Примером схемы мошенничества с использованием искусственного интеллекта является атака, при которой злоумышленники получают доступ к аккаунту жертвы в мессенджере и используют хранящиеся в нем данные для генерации фейкового голосового контента. Это позволяет обманывать контакты жертвы, а также получать ее личные данные. Подобные схемы несут риски не только финансовых потерь, но и кражи личности — продвинутые технологии используются здесь для повышения кредита доверия и эффективности традиционных атак социальной инженерии.

На первом этапе мошенникам необходимо получить доступ к аккаунту пользователя. Для этого они направляют ему фишинговую ссылку в мессенджере, которая выглядит как приглашение вступить в чат. Однако данная ссылка перенаправляет жертву на мошеннический ресурс, копирующий внешний вид формы авторизации мессенджера. Введенные на этой странице логин и пароль передаются на сервер злоумышленников. После этого мошенники получают возможность собрать все необходимые для успешной атаки данные — аудио- и видеосообщения, отправленные жертвой ранее, — на основе которых генерируют новый аудио- и видеоконтент, неотличимый от голоса и манеры общения владельца аккаунта.

Созданные при помощи искусственного интеллекта аудиосообщения обычно содержат просьбу о срочном переводе денежных средств. Контакты жертвы, слыша знакомый голос, не сомневаются в подлинности просьбы и переводят деньги мошенникам (рисунок 3).[3]



[3] Рис. 3. Схема мошенничества «Мошенничество в мессенджере с помощью сгенерированного голоса». Источник: составлено авторами

Рис. 3. Схема мошенничества «Мошенничество в мессенджере с помощью сгенерированного голоса»

В августе 2024 года в России впервые были зафиксированы успешные атаки на клиентов банков с применением технологии NFCGate. Данная мошенническая схема представляет собой гибридный метод, сочетающий использование вредоносного программного обеспечения (ВПО) и приемы социальной инженерии.

Приложение NFCGate изначально разрабатывалось как легитимный инструмент: в 2015 году студенты Дармштадтского технического университета создали его в качестве учебного проекта для анализа и отладки NFC-трафика, а также для проведения экспериментов в области бесконтактных технологий. Приложение является программным обеспечением с открытым исходным кодом и предоставляет возможности захвата, мониторинга и воспроизведения NFC-сигнала. Однако впоследствии модифицированные версии NFCGate стали использоваться злоумышленниками в противоправных целях. При этом злоумышленникам удалось совершить значительный объем хищений, используя подобные атаки: только за первые десять месяцев 2025 года у россиян было похищено 1,6 миллиарда рублей [11].

Мошенническая схема на базе NFCGate реализуется в двух сценариях — прямом и обратном. В первом случае жертва прикладывает свою карту к NFC-датчику зараженного смартфона, а перехваченные данные ретранслируются на устройство злоумышленника у банкомата, позволяя ему снять наличные. Во втором случае вектор передачи данных меняется на противоположный: устройство злоумышленника считывает карту дропа, после чего ее данные передаются на смартфон жертвы и эмулируются им для последующего использования при транзакции. Наибольшее распространение получил именно обратный сценарий, так как он хуже распознается банковскими антифрод-системами.

В случае реализации злоумышленниками обратного сценария атака на пользователей банковских карт проводится в два этапа. Вначале преступники, используя приемы социальной инженерии, пытаются убедить потенциальную жертву в необходимости установки вредоносного APK-файла на устройство под видом полезной программы. Злоумышленники используют различные легенды и могут связывать необходимость установки приложения с необходимой мерой для «защиты» банковского счета или получения более выгодных условий обслуживания. После загрузки вредоносного приложения, функционал которого позволяет перехватывать и подменять NFC-трафик, злоумышленники переходят к следующему этапу атаки и убеждают жертву

направиться к банкомату и совершить необходимые для зачисления средств действия. Когда жертва прикладывает свое устройство к NFC-датчику банкомата, происходит авторизация банковского счета злоумышленника, в результате чего пользователь, полагая, что зачисляет деньги на свой счет, фактически переводит их на счет мошенника (рисунок 4).[4]

Рисунок 4. Схема мошенничества «Обратный NFCGate»

Данная схема мошенничества похожа на другой распространенный сценарий, описанный выше, а именно на схему мошенничества с безопасным счетом. Принципиальное отличие состоит в том, что злоумышленники не пытаются выведать у клиента банка конфиденциальную информацию: жертву не просят продиктовать коды из СМС-сообщений, не запрашивают данные ее карты. Напротив, пользователю могут сообщить «новый» ПИН-код — якобы от его же карты, что создает иллюзию безопасности проводимой операции.

Результаты / Results

Проведенный анализ позволяет выделить ряд устойчивых характеристик, присущих социальной инженерии в кредитно-финансовой сфере. Выявлено, что атаки кибермошенников представляют собой многоэтапный, хорошо спланированный процесс, в ходе которого злоумышленники предварительно собирают информацию о потенциальной жертве, разрабатывают сценарий атаки (претекст) и с использованием современных

[4] Рис. 4. Схема мошенничества «Обратный NFCGate». Источник: составлено авторами

технологий, в частности искусственного интеллекта, персонализируют атаку, адаптируя ее под конкретную жертву.

Установлено, что все атаки социальных инженеров эксплуатируют особенности психики человека и когнитивные искажения, такие как склонность к подчинению авторитету, подверженность эффекту срочности и дефицита, а также доверчивость в ситуациях неопределенности.

Вместе с тем социальная инженерия зачастую является лишь частью более сложной мошеннической схемы. Ее применение позволяет получить от жертвы конфиденциальные данные, коды подтверждения операций и добровольное согласие на совершение требуемых злоумышленнику действий, после чего в атаку могут включаться иные средства, в частности вредоносное программное обеспечение, поддельные сайты и платформы, а также средства перехвата и подмены NFC-трафика.

Проведенное исследование позволяет сделать вывод о необходимости совершенствования механизмов возврата похищенных денежных средств. Действующее законодательство связывает обязанность банка по возмещению с фактом нарушения клиентом порядка использования электронного средства платежа, что в большинстве случаев социальной инженерии оставляет потерпевшего без компенсации. В этой связи актуальной задачей становится повышение прозрачности и эффективности процедуры оспаривания транзакций для пострадавших, в том числе путем уточнения критериев добровольности согласия и распределения ответственности между ОКФС и клиентом с учетом конкретных обстоятельств атаки.

Заключение / Conclusion

На сегодняшний день основной вектор атак мошенников на кредитно-финансовую сферу сместился с банковской инфраструктуры на клиента. Банки последовательно усиливали технологическую защиту, и злоумышленники нашли иной путь: вместо попыток обхода технологических барьеров они используют психологические манипуляции, заставляя самого пользователя совершить нужные им действия. Таким образом, социальная инженерия в кредитно-финансовой сфере является не техническим, а поведенческим феноменом, эксплуатирующим устойчивые особенности человеческого восприятия и принятия решений.

Из этого следует, что основные меры по предотвращению подобных атак должны быть направлены прежде всего на самого человека — на формирование у него критического мышления и повышение финансовой грамотности. Развитие технологий

искусственного интеллекта, появление сервисов, упрощающих подготовку и проведение атак, а также распространение средств генерации синтетического медиаконтента ведут к повышению убедительности мошеннических схем, что, в свою очередь, требует роста подготовленности пользователей. Способность критически оценивать поступающую информацию становится не просто желательным навыком, а необходимым условием финансовой безопасности.

На уровне кредитно-финансовых институтов одним из приоритетных направлений должно стать дальнейшее развитие антифрод-систем, ориентированных на противодействие социальной инженерии. Современные решения уже способны анализировать не только корректность аутентификационных данных, но и контекст операции: поведенческие паттерны пользователя, типичность параметров сессии, фоновую активность приложений. Углубленная интеграция поведенческой аналитики будет во многом определять способность банков выявлять операции, совершаемые клиентом под влиянием манипуляции, даже в тех случаях, когда формальные признаки легитимности соблюдены.

Список источников

1. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств (I квартал 2026 г.) [Электронный ресурс] // Банк России. — 2026. — URL: https://cbr.ru/statistics/ib/review_1q_2026/ (дата обращения: 08.07.2026).
2. Ревенков П.В., Бердюгин А.А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. — 2017. — Т. 13, № 9. — С. 1747–1760.
3. Унукович А.С. Социальная инженерия и кибербезопасность: виктимологический аспект // Психопедагогика в правоохранительных органах. — 2021. — Т. 26, № 3(86). — С. 346–351.
4. Менщиков А.А., Федосенко М.Ю. Возможности использования методов социальной инженерии в организации телефонного мошенничества // Экономика и качество систем связи. — 2021. — № 4. — С. 38–50.
5. Зорин В.А. Информационная безопасность и нейробиология социальной инженерии: когнитивные искажения, эмпатия // Труды Института проблем управления РАН. — 2024.
6. Зотина Е.В. Претекстинг как прием социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему // Вестник

Казанского юридического института МВД России. — 2022. — Т. 13, № 4(50). — С. 93–99.

7. Медяник О.В., Низовских Н.А. Общение с жертвами финансового внушения: учебно-методические рекомендации и практикум для банковских сотрудников. — Москва : Литрес, 2025. — 118 с.
8. Чалдини Р.Б. Психология влияния / пер. с англ. Е. Бугаева [и др.]. — 5-е изд. — СПб. : Питер, 2012. — 294 с. — (Мастера психологии).
9. Российская Федерация. Законы. О национальной платежной системе : Федеральный закон от 27.06.2011 № 161-ФЗ : последняя редакция // КонсультантПлюс : справочно-правовая система. — URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 08.07.2026).
10. Индекс цифровой грамотности — 2025 [Электронный ресурс] // НАФИ. — 2025. — URL: https://nafi.ru/ratings/ (дата обращения: 08.07.2026).
11. У клиентов российских банков в 2025 году с помощью NFCGate похитили не менее 1,6 млрд рублей [Электронный ресурс] // Ассоциация российских банков. — 2025. URL: https://arb.ru/b2c/scrammers/u_klientov_rossiyskikh_bankov_v_2025_godu_s_pomoshchyu_nfcgate_ne_menee_1_6_mlrd-10694345/ (дата обращения: 08.07.2026).

1. Review of Reporting on Information Security Incidents During Funds Transfers (Q1 2026) [Electronic resource] // Bank of Russia. — 2026. — URL: https://cbr.ru/statistics/ib/review_1q_2026/ (date of access: 07/08/2026).
2. Revenkov P.V., Berdyugin A.A. Social Engineering as a Source of Risks in the Context of Remote Banking Services // National Interests: Priorities and Security. — 2017. — Vol. 13, No. 9. — Pp. 1747–1760.
3. Unukovich A.S. Social Engineering and Cybersecurity: Victimological Aspect // Psychopedagogy in Law Enforcement Agencies. — 2021. — Vol. 26, No. 3(86). — P. 346–351.
4. Menshchikov A.A., Fedosenko M.Yu. Possibilities of Using Social Engineering Methods in Organizing Telephone Fraud // Economics and Quality of Communication Systems. — 2021. — No. 4. — P. 38–50.

5. Zorin V.A. Information Security and the Neurobiology of Social Engineering: Cognitive Biases, Empathy // Proceedings of the Institute of Control Sciences of the Russian Academy of Sciences. — 2024.

6. Zotina E.V. Pretexting as a Social Engineering Technique Used by Telephone Fraudsters: A Criminological Approach // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. — 2022. — Vol. 13, No. 4(50). — P. 93–99.

7. Medyanik O.V., Nizovskikh N.A. Communicating with Victims of Financial Hypothesis: Training and Methodological Recommendations and a Workshop for Bank Employees. Moscow: Litres, 2025. 118 p.

8. Cialdini, R.B. Psychology of Influence / translated from English by E. Bugaeva [et al.]. 5th ed. St. Petersburg: Piter, 2012. 294 p. (Masters of Psychology).

9. Russian Federation. Laws. On the National Payment System: Federal Law of June 27, 2011, No. 161-FZ: latest edition // ConsultantPlus: legal reference system. URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (accessed July 8, 2026).

10. Digital Literacy Index — 2025 [Electronic resource] // NAFI. — 2025. — URL: https://nafi.ru/ratings/ (date of access: 07/08/2026).

11. At least 1.6 billion rubles were stolen from clients of Russian banks using NFCGate in 2025 [Electronic resource] // Association of Russian Banks. — 2025. URL: https://arb.ru/b2c/scrammers/u_klientov_rossiyskikh_bankov_v_2025_godu_s_pomoshchyu_nfcgate_ne_menee_1_6_mlrd-10694345/ (date of access: 07/08/2026).