УМВД России по Кировской области
Общественный совет при УМВД России по Кировской области

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ТЕЛЕФОННОМУ МОШЕННИЧЕСТВУ В ФИНАНСОВОЙ СФЕРЕ

Методические материалы

Киров
2024

Методические материалы рекомендованы к распространению на заседании научно-практической секции УМВД России по Кировской области 20.12.2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Телефонное мошенничество получило широкое распространение в России начиная с 2017 года. В настоящее время эта проблема стала особенно острой. Можно сказать, что России объявлена негласная «информационно-психологическая война», в ходе которой граждане несут значительный имущественный ущерб, лишаясь своих накоплений и взятых в кредит денежных средств.

Глава ЦБ России Эльвира Набиуллина, выступая в рамках панельной дискуссии «Противодействие мошенничеству и социальной инженерии» на форуме «Кибербезопасность в финансах» в феврале 2023 года, отметила, что «перелома в борьбе с телефонным мошенничеством не произошло, а значит, звонки будут поступать россиянам и дальше» [Набиуллина, 2023]. Но, как считает Э. Набиуллина, перелома в ситуации можно добиться, если скоординировать усилия всех заинтересованных участников. Поскольку мошенники «креативны и очень сфокусированы», необходимо усиливать меры противодействия, в частности, необходимо повышать устойчивость граждан к мошенническим действиям [там же].

Несмотря на предпринимаемые УМВД России профилактические меры, кировчане все чаще становятся жертвами телефонных мошенников. Одной из причин такого положения дел является то, что мошенники применяют специально разработанные технологии, оказывая психологическое воздействие на сознание потенциальных жертв. Мошенники чаще всего имеют специальную подготовку, умеют налаживать контакты, могут расположить к себе, а в нужный момент прибегают к запугиванию и шантажу.

К настоящему времени граждане России перевели мошенникам десятки миллиардов рублей. В Кировской области только за 2023 год зарегистрировано 5126 случаев краж и мошенничества, совершенных с использованием информационно-телекоммуникационных технологий. Это на 38,4% больше, чем за 2022 года. Общий материальный ущерб от данныхпреступлений в 2023 году составил более 1 млрд 101 млн рублей.

Мошеннические действия отрицательно влияют на психологическое здоровье и благополучие людей, лишившихся своих

сбережений [Мешкова с соавт., 2022]; подрывают веру граждан в эффективность деятельности правоохранительных органов.

В этой ситуации актуальной становится задача специальной подготовки сотрудников полиции к организации и проведению работы по противодействию телефонному мошенничеству в финансовой сфере.

Брошюра предназначена для сотрудников полиции и других лиц, занимающимися просветительской и профилактической работой в сфере финансовой грамотности населения. Предпочтительными формами плановой программной деятельности являются лекции, семинары, практикумы. Возможно выделение темы «Психология противодействия телефонному мошенничеству в финансовой сфере» в качестве специального модуля повышения квалификации соответствующих служб.

Вместе с тем сотрудники правоохранительных и других государственных органов и служб могут изучать данные методические материалы самостоятельно, используя их при взаимодействии с населением.

Материалы брошюры будут полезны также для подготовки лекторов-инструкторов, и для самостоятельного прочтения представителями самых широких аудиторий.

Цель методических материалов: содействовать сотрудникам правоохранительных и других служб в организации эффективной защиты граждан от телефонного мошенничества, а также повышать грамотность и психологическую устойчивость самих граждан.

Авторы-составители методических рекомендаций:
Баранцев Сергей Павлович, начальник отдела информации и общественных связей УМВД России по Кировской области.
Медяник Ольга Викторовна, кандидат психологических наук, доцент кафедры управления рисками и страхования факультет психологии Санкт-Петербургского государственного университета.
Низовских Нина Аркадьевна, доктор психологических наук, доцент кафедры психологии ФГБОУ ВО «Вятский государственный университет»
Николаева Оксана Анатольевна, оперуполномоченный 5 отдела Управления уголовного розыска УМВД России по Кировской области.

1. АНАЛИЗ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ, НАПРАВЛЕННЫХ НА ХИЩЕНИЕ ДЕНЕЖНЫХ СРЕДСТВ ГРАЖДАН

Телефонное мошенничество реализуется в настоящее время методами «социальной инженерии», которая определяется как *способ обманом заставить кого-либо раскрыть информацию или предоставить доступ к данным* [Социальная инженерия]. Мошенники манипулируют людьми в своих преступных целях, используя человеческие слабости, низкий уровень финансовой грамотности и отсутствие у населения выработанных способов противодействия. Производится так называемый «взлом» человеческого сознания с использованием психологических приемов.

Методы социальной инженерии основываются на знании психологических закономерностей финансового поведения человека [Моисеева, 2022]. При определенных психологических воздействиях человек становится управляемым и склонным передавать сведения о доступе к его финансовым ресурсам без учета своей безопасности [Приложение 2].

Приемами социальной инженерии являются: фишинг (вишинг), претекстинг, «дорожное яблоко», «кви про кво», «Троянский конь» [Зотина, 2923, с. 32]. Одним из основных способов обмана является претекстинг (действия по заранее подготовленному сценарию) [там же].

Сущность претекстинга заключается в том, что преступник использует заранее подготовленный коммуникативный сценарий, прорабатывает речевые стратегии и тактики, основная интенция которых – осуществление деструктивного манипулятивного психологического воздействия на жертву, выведение ее из состояния душевного равновесия, понуждение к совершению добровольной передачи денежных средств мошеннику [там же].

Специалисты в области кибербезопасности отмечают, что в 2023 году получили распространение **«пристрелочные» звонки,** предшествующие реализации мошеннической схемы претекстинга. Их суть заключается в том, что телефонные мошенники совершают несколько подготовительных звонков, в том числе и с

разницей в несколько дней, общаются с потенциальной жертвой, выясняя таким образом ее психотип, особенности речевого поведения, подверженность влиянию нейролингвистического программирования [Зотина, 2923, с. 33].

РАСПРОСТРАНЕННЫЕ СПОСОБЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА[1]

К наиболее распространенным способам телефонного мошенничества в настоящее время относятся следующие:

• Мошенник представляется сотрудником правоохранительных органов (сотрудником ФСБ РФ, прокуратуры, следственного комитета) и сообщает, что группа лиц использовала лицевой счет клиента для распоряжения денежными средствами, полученными преступным путем; далее снова предлагаются действия по снятию наличных денежных средств или их переводу на «безопасный счет». Один из вариантов войти в доверие к потерпевшему – направить сообщение в мессенджере якобы от руководителя организации с просьбой о содействии сотрудникам ФСБ, «который сейчас перезвонит». Естественно, что аккаунт руководителя является клоном настоящей его страницы с фотографией, либо просто используется его фотография, взятая в сети Интернет.

• Мошенник представляется специалистом портала «Госуслуги» или оператором сотовой связи и под предлогом получения писем, информации, справок (о перерасчете пенсии, о доходах..., штрафах... иной интересующей информации клиента) на электронную почту клиента, а также смены абонентского номера телефона, окончания действия сим-карты (которая зачастую привязана к банковской карте в качестве услуги в мобильном банке) просит граждан сообщить ему код (пароль), который поступит в смс-сообщении на мобильное устройство и, получая данные сведения, в последующем мошенник получает свободный доступ в

[1] Подробный перечень распространенных направлений кибермошенничества приводится в Приложении 1.

приложения клиента (оператора связи, банковское приложение), после чего зная персональные данные лица, оформляет от его имени кредиты в различных учреждениях, банках, микрофинансовых организациях.

• Мошенник представляется сотрудником банка и сообщает о том, что некто пытается оформить кредит от лица клиента, либо совершить манипуляции с личными накоплениями на счете последнего, и клиенту настоятельно предлагается для защиты от несанкционированного оформления кредита, как можно быстрее первому оформить кредит или взять кредит на сумму аналогичную той, которая уже оформлена посторонним лицом, обналичить деньги и передать их для сохранения якобы сотрудникам банка или перевести денежные накопления на «безопасный счет» («зеркальный счет», «в безопасную ячейку»), т. е. совершить действия по предупреждению оформления несанкционированного кредита на имя потерпевшего посторонним лицом (самому клиенту вперед быстрее оформить новый кредит, чтобы Банк более не смог выдать иных кредитов на имя клиента посторонним лицам) и тем самым, переведя только что взятые в кредитные денежные средства, аннулировать кредит.

Схемы мошенничества являются многоэтапными и растянутыми во времени. Диалог с клиентом может продолжаться в течение нескольких часов или дней. При общении с гражданами используются психологические приемы воздействия путем уговоров, угроз (содействие террористам, вооруженным силам недружественных государств), повышение тона, перекладывания вины и ответственности при потере денежных средств на самого гражданина в случае отказа следовать указаниям звонящих. Зачастую злоумышленники возвращаются к обманутым гражданам, чтобы обмануть их повторно и/или вовлечь их в противоправные антиобщественные действия (совершить поджог отделов полиции, военкоматов, транспортных средств, отделений банков).

Клиенту под угрозой уголовной ответственности предъявляется требование о сохранении всех переговоров в тайне; сообщается, что разглашать информацию нельзя никому, даже соседям или близким родственникам. Мошенники полностью контролируют действия граждан, требуют постоянно находиться с ними в

режиме телефонного общения, при направлении гражданина в отделении банка для оформления и получения кредита, указывают лицу при общении с сотрудником банка называть надуманные цели для получения кредита (срочная покупка, медицинское лечение, строительство), якобы для понимания того, кто из сотрудников банка замешан в совершении мошенничества и дальнейшей его поимке.

Появляются и дополнительные способы телефонного мошенничества:

• *Махинации со счетами мобильных телефонов*. Клиенту поступает сообщение или звонок об ошибочном переводе денег на счёт мобильного телефона и формулируется просьба вернуть их владельцу. При этом могут осуществляться угрозы обращения в полицию или оператору мобильной связи с требованием блокировки телефона.

• *Сообщение о попавшем в беду родственнике (чаще это представлено как виновник при совершении ДТП) с просьбой о финансовой помощи «для решения вопроса»*. Звонок о попавшем в беду родственнике, как правило,поступает на стационарный телефон среди ночи, когда полусонной жертве сообщают об автомобильной аварии, наезде на пешехода, крушении поезда или любых других происшествиях, случившихся с детьми, внуками или просто друзьями. Далее следует просьба о срочной помощи в виде перевода немалой суммы на электронный кошелек или счёт мобильника. Метод крайне жестокий, известны случаи инфарктов от подобных новостей. Потерпевшими выступают чаще всего лица в возрасте 40-60 лет. Есть примеры, когда телефонные звонки поступали малолетним детям с требованиям найти деньги, так как их родители якобы виновны в совершении дорожно-транспортных происшествий.

• *Сообщения о выигрыше в лотерею, получении бонусов в виде денежного приза от банка в честь дня рождения, иного события*. Новость сопровождается требованием перевода на покрытие технических издержек самой лотереи, либо сообщении реквизитов банковской карты и кода из смс-сообщения для перевода денежного приза. Мошенники здесь рассчитывают на незнание гражданами законодательства РФ, согласно которому

все расходы организаторов лотерей ложатся на них самих, а также отсутствия в банках подобных ситуаций – выплат в качестве призов.

Для усыпления бдительности клиентов мошенники используют различные современные технологии и мошеннические схемы.

ОБМАН ПРИ ПОМОЩИ ЧАТ-БОТОВ

О новом способе обмана россиян при помощи чат-ботов рассказал руководитель отдела продвижения продуктов компании «Код безопасности» Павел Коростелев [Коростелев, 2023]. По мере того как чат-боты стали набирать популярность у обычных людей, ими стали пользоваться и мошенники. Например, они взламывают легитимные чат-боты различных компаний и организуют рассылку-опрос, с помощью которой собирают личную информацию: номера телефонов, геопозицию и т.д. Также хакеры могут создавать собственные чат-боты, что придает фишинговому сайту большую правдоподобность: люди доверяют чат-ботам и не подозревают, что «сливают» им свои данные.

ТЕХНОЛОГИЯ ПОДМЕНЫ ТЕЛЕФОННЫХ НОМЕРОВ

Злоумышленники применяют технологию подмены номера, когда в качестве номера звонящего подставляется официальный телефон банка, различных правоохранительных ведомств (сведения о которых в свободном доступе находится в сети Интернет, данные руководителей указанных структур).

В январе-феврале 2023 года мошенники, как правило, звонили с номеров, начинающихся с кодов 495/499, то есть использовали подмену абонентского номера на российскую нумерацию, хотя на самом деле они звонили из другой страны из специальных call-центров. Но поскольку в настоящее время операторы мобильной связи за пропуск из-за границы подменных номеров привлекаются к административной ответственности, а виновным представителям компаний назначаются крупные денежные штрафы, операторы, начиная с марта 2023 года, не пропускают либо крайне редко пропускают такие звонки.В последнее время

«подменные» звонки проходят с номеров различных операторов связи, при этом возможна принадлежность абонентов-мошенников к любому региону РФ.

СВЯЗЬ КИБЕРМОШЕННИЧЕСТВА С ФИНАНСОВОЙ СУГГЕСТИЕЙ

Финансовая суггестия[2] – это процесс, при котором потребителям делаются предложения или рекомендации относительно их финансовых решений [Медяник, 2024]. Финансовая суггестия является важным инструментом для привлечения новых клиентов и обеспечения устойчивости финансовых систем. Однако, в условиях все возрастающего количества кибермошенничества, эффективность таких предложений ставится под сомнение. Злоумышленники все более активно используют уязвимости в финансовых системах, чтобы манипулировать людьми и организациями для своей выгоды. Использование различных техник позволяет им создавать ложные представления о возможности получения дохода или о минимальных рисках при инвестировании, кредитовании, страховании и других видах финансовой деятельности.

Одной из основных проблем финансовой суггестии в условиях кибермошенничества является сложность обнаружения мошеннических действий. Злоумышленники постоянно адаптируются и разрабатывают новые методы, чтобы оставаться незаметными для систем безопасности. Мошенническая финансовая суггестия имеет серьезные последствия как для отдельных лиц, так и для организаций. Люди могут потерять свои деньги или стать жертвами кражи личной информации.

---

[2] Суггестия (внушение) – процесс воздействия на психическую сферу человека, связанный со снижением сознательности и критичности при восприятии и реализации внушаемого содержания. В сознании человека, подвергшегося суггестии отсутствуют целенаправленное и активное понимание внушенного содержания, его логический анализ. Содержанию сознания, усвоенному по механизму суггестии, присущнавязчивый характер, оно с трудом поддается коррекции [Большая психологическая энциклопедия. внушение | это... Что такое внушение? (academic.ru)].

Различные виды кибермошенничества могут распространяться через социальные сети, электронную почту и SMS-рассылки. Для каждого вида мошенничества характерны тот или иной эффект социальной инженерии, суггестивные атаки (или коды манипулятивного воздействия) и когнитивные искажения, которые используются мошенниками для убеждения жертв в своей правоте [Приложение 3]. Например, для мошенничества с использованием кредитных карт или банковских счетов характерны следующие эффекты: **профайлинг[3] и эффект авторитета.** Мошенники выдают себя за представителей банков или других авторитетных организаций, чтобы убедить жертву предоставить им свои личные данные или совершить финансовую операцию.

Когнитивные искажения могут использоваться мошенниками для убеждения жертв в своей правоте. Например, для мошенничества с предложением быстрого и легкого заработка без особых усилий указан **эффект подтверждения**, который может привести к тому, что жертва поверит обманчивым обещаниям мошенников. Так, к примеру, мошенники во время разговора со своей жертвой представляются аналитиками или трейдерами Московской биржи и предлагают совершить инвестиции в акции российских и международных компаний под высокие проценты. После этого они стараются узнать информацию о банковских картах гражданина или просят провести платеж по своим реквизитам [Мошенники стали представляться трейдерами Московской биржи – Рамблер/финансы (rambler.ru)]. Но, заметим, потерпевшие не знают, что сотрудники биржи не звонят гражданам, не имеют права просить данные платежных карт и не предоставляют никаких инвестиционных рекомендаций [там же].

Мошенники часто манипулируют такими когнитивными искажениями, **как фантомная фиксация и предвзятость подтверждения,** чтобы использовать доверие людей и их стремление к быстрой финансовой выгоде. Примером может служить реклама мошеннической компании «Газпром Инвест», которая к реальной государственной корпорации никакого отношения не имеет. Доверить им свои деньги – это гарантированно потерять вложения.

---

[3] Профайлинг – составление профиля личности человека.

Еще одним видом кибермошенничества являются атаки с внушением, которые связаны с ложными обещаниями высоких доходов от инвестиций. Мошенники используют психологические приемы, чтобы убедить жертву в том, что их схема принесет значительную прибыль при минимальных рисках.

Скрытые платежи и условия – распространенная форма кибермошенничества при оформлении кредита или займа. Мошенники пользуются доверием людей к банкам или финансовым организациям, скрывая дополнительные платежи или условия, которые могут поставить клиента в невыгодное положение. Эта тактика, известная как **ландшафтный дизайн,** также использует когнитивные искажения и может заставить жертву неосознанно согласиться на невыгодные финансовые предложения.

Анализ видов кибермошенничества, а также связанных с ними эффектов социальной инженерии, суггестивных атак и когнитивных искажений, показывает разнообразие методов, используемых злоумышленниками для манипулирования пользователями [Приложение 3; Медяник, 2023].

КОДЫ МАНИПУЛЯЦИЙ, ПРИМЕНЯЕМЫХ МОШЕННИКАМИ [Медяник, 2024]

1. Создание эмоциональной зависимости. Эти коды используются для того, чтобы вызвать у другого человека чувство вины, страха или обязательства.

2. Создание иллюзии необходимости. Эти коды используются для того, чтобы заставить другого человека думать, что он обязан что-то сделать.

3. Создание иллюзии важности. Эти коды используются для того, чтобы заставить другого человека думать, что то, что манипулятор хочет, является очень важным.

4. Создание иллюзии выбора. Эти коды используются для того, чтобы заставить другого человека думать, что он имеет выбор, хотя на самом деле выбора нет.

5. Создание иллюзии согласия. Эти коды используются для того, чтобы заставить другого человека думать, что он согласен на что-то, хотя на самом деле он этого не хочет.

6. Создание иллюзии справедливости. Эти коды используются для того, чтобы заставить другого человека думать, что то, что манипулятор хочет, является справедливым или правильным.

7. Создание иллюзии единства. Эти коды используются для того, чтобы заставить другого человека думать, что он и манипулятор находятся в одной команде или имеют общую цель.

8. Создание иллюзии контроля. Эти коды используются для того, чтобы заставить другого человека думать, что манипулятор контролирует ситуацию или имеет большую власть.

ОТКУДА ИСХОДИТ ОПАСНОСТЬ?

По данным Сбера на долю Украины приходится до 90% всех мошенническихcall-центров, работающих против граждан РФ, остальные располагаются на территории России и стран СНГ. Основные call-центры находятся в настоящее время в г. Днепр (бывшем Днепропетровске), который неофициально считается столицей телефонного мошенничества.

Деятельностью call-центров управляют организованные преступные группы, а контроль и поддержку им оказывают региональные управления СБУ. Можно говорить о криминальной индустрии, в которую помимо непосредственных сотрудников call-центров вовлечены тысячи людей.

На похищенные денежные средства преступники скупают недвижимость внутри страны и заграницей, открывают легальный бизнес, а также финансируют украинские вооруженные силы. Так, по данным Сбера, все чаще мошенники, успешно обманув свою жертву, добавляют в конце разговора «благодарность» за финансирование ВСУ.

ЧТО ИЗ СЕБЯ ПРЕДСТАВЛЯЮТ CALL-ЦЕНТРЫ?

Call-центрывыглядят как обычные офисы со столами и компьютерами, в которых за высокие денежные вознаграждения «трудятся» мошенники. Зарплата таких сотрудников от 1500 $ в месяцс еженедельными выплатами.

Начинающих телефонных мошенников здесь же в call-центрах обучают «профессионалы». На преступников работают десятки психологов, которые обучают сотрудников call-центров основам НЛП (нейро-лингвистического программирования) и грамотному построению речи. Для психологической подготовки в г. Днепр существует специальный «учебный call-центр» на 250 рабочих мест.

На работу в call-центры нанимают, как правило, молодых (до 35 лет) людей с навыками работы в коллективе, активно пользующихся персональными компьютерными, с хорошими речевыми навыками. Если удается привлечь работника без характерного южнорусского или украинского акцента, то это считается большой удачей, заработки такого сотрудника на порядок выше, чем у сотрудников с акцентом.

На первое время работникам предоставляется оплачиваемое жилье – хостел, который, как правило, находится в пешей доступности от call-центра. Связь с кандидатом по вакансии обычно происходит через мессенджер «Telegram», где обговариваются условия работы, в частности рекрутеры не скрывают, что работают по клиентам российских банков.

Во время первого разговора с кандидатом наниматель из call-центра просит перезвонить с украинского номера телефона; особенности вакансии стараются обсуждать только лично при встрече. Также требуется предоставить скан украинского паспорта. Последнее связано, в частности, с репортажем о работе телефонных мошенников на Украине (передача «Андрей Малахов. Прямой эфир»), когда корреспондент устроился на работу в call-центр в рамках журналистского расследования.

После общения и уточнения всех особенностей работы кандидата, если он подходит, приглашают непосредственно в офис. Кандидата уверяют, что с правоохранительными органами «все подвязано». Все собеседования, как правило, проходят в несколько этапов, что обеспечивает конфиденциальность работы сотрудников данного call-центра. Сотрудники call-центров входят в разные группы.

ГРУППЫ	***ЗАДАЧИ***
«Холодники[4]»	Обзванивают людей по базам телефонов. Основные задачи: • установить контакт с клиентом; • получить информацию о его счетах, картах и банковских операциях; • встревожить, напугать, заставить сотрудничать. Человеку сообщают о подозрительном снятии денег с его банковских карт, говорят о возбуждении уголовного дела и т.д. Информацию, полученную от потенциальной жертвы, холодник фиксирует в CRM[5], затем клиент передается на вторую линию «клосерам»
«Клосеры»[6]	Клосеры – это мошенники с большим стажем и опытом. Они разными путями (уговорами, психологическим давлением, шантажом) добиваются от жертвы перевода денег на счета владельцев call-центра. Клосеры бывают двух типов: • *тип 1* – работают с личными деньгами жертвы; • *тип 2* – специализируются на попытках вынудить обманываемого взять в банке кредит и перечислить его мошенникам. ***Если на счетах жертвы имеется значительная сумма,*** то мошенники вынуждают обналичить средства. Для этого используются сценарии «Безопасный счет» или «Страховая ячейка». Жертву убеждают внести средства наличными якобы на специально созданный для спасения от мошенников «безопасный» счет. В действительности это мошеннические реквизиты банковских счетов или карт, полученные от дроп-сервиса. Как правило, для

[4] «Холодник» или «холоднозвонящий» - это сотрудник, осуществляющий «холодный» обзвон потенциальных жертв. Холодный звонок – одна из форм телемаркетинга, когда менеджер звонит клиенту, с которым не имел дела ранее.

[3] Customer relationship management (CRM) переводится как управление взаимоотношениями с клиентами. Это программа, которая помогает регулировать бизнес-процессы, выстраивать долгосрочные отношения с клиентами и способствует повышению эффективности продаж.

[6] Клосеры или «клоузеры» - от английского to close – закрывать.

ГРУППЫ	ЗАДАЧИ
«Клосеры»	взноса средств используются банкоматы банков, позволяющих вносить средства на счета без дополнительной идентификации вносителя. ***При отсутствии значительной суммы у клиента*** оператор использует сценарий «Кредит» и пытается подвести клиента к осуществлению заёма денежных средств в нескольких банках. Это так называемая «кредитная карусель». У мошенников есть информация, какие суммы и в каких банках чаще всего оформляются в кредитах без дополнительных проверок со стороны служб безопасности. Чем больше денег сумеют вытащить из жертвы мошенники, тем больший бонус вся команда звонивших получит по итогу «закрытия» разводки. Обычно главари call-центров оставляют своим работникам до 20% от суммы похищенного.
«Мены»	«Мены» это люди, хорошо знающие определённый регион страны, владеющие информацией о структуре власти области или края, ключевых региональных фигурах, именах начальников отделений банков, управлений МВД, знающие географию города жертвы, они всегда в курсе последних городских новостей и т.д. У каждого из них есть телефоны с подменным номером, который для жертвы выглядит как совпадающий с номером учреждения, якобы из которого звонит «мен». Задача этой группы мошенников – помочь своим подельникам убедить в реальности происходящего засомневавшуюся жертву, они засыпают её своими знаниями о том, на какой улице находится тот или иной банк, как туда пройти или проехать, называют реальные фамилии. Попытки жертвы подловить звонящую «банковскую шишку», «следователя» или «трейдера из венчурной компании» на лжи упираются в детальное знание «меном» региональной реальности. При этом «мены» могут вообще никогда не бывать в данном регионе – они скрупулёзно изучают область или республику через Интернет.

ЭТАПЫ РАБОТЫ МОШЕННИКОВ

1 этап. *Организационные мероприятия.* Настройка оборудования, SIP-телефонии[7], подготовка баз данных и распределение их между сотрудниками.

2 этап. *Холодный звонок клиенту.* Фиксация информации в CRM и передача клиента на «вторую линию». Оператор вносит полученную во время разговора информацию об операциях, счетах и вкладах клиента в CRM.

3 этап. *«Закрытие» клиента.* Оператор «второй линии» звонит клиенту и, используя информацию, полученную на предыдущем этапе, убеждает клиента совершить перевод на мошеннический счет. Оператор «второй линии» связывается с сервисом «обнала», передает информацию о сумме средств и получает в ответ мошеннические реквизиты (например, номер банковской карты) для вывода украденных денежных средств.

4 этап. *Вывод денежных средств.* Обнал-сервис организует обналичивание переведенных жертвой средств с дроперского счета, забирает свою комиссию (около 20%), а оставшаяся сумма переводится сервисом на подконтрольные руководителям call-центра BTC-кошельки.

КАК ОСУЩЕСТВЛЯЕТСЯ СБОР ДАННЫХ О ПОТЕНЦИАЛЬНЫХ ЖЕРТВАХ
(на примере call-центра, действовавшего в г. Бердянске)

Выделенный сотрудник покупает украденные базы данных в теневом сегменте сети Интернет (даркнет). «Закупщик» использует специально созданные одноразовые Telegram-аккаунты, которые удаляются после сделки. Покупаются базы данных мобильных операторов связи, банков, онлайн-магазинов и т.д. Стоимость таких баз данных составляет от 100 до 500 долларов США за 1000 строк.

---

[7] Способ голосовой связи через интернет на основе протокола SIP (англ. Session Initiation Protocol, Протокол установления сеанса — протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи).

Базы данных распределяются между конкретными сотрудниками, которые осуществляют обзвон. Во избежание повторных звонков каждый сотрудник работает по своей базе. Для хранения и обработки данных, полученных от клиента во время телефонного разговора сотрудник вносит информацию по каждой жертве в CRM.

Сотрудник, отвечающий за базы данных, рассылает «звонарям» подготовленные файлы с данными для обзвона. Файлы представляют из себя таблицы, содержащие от 50 до 100 записей с ФИО, адресами, номерами телефонов и прочими персональными данными потенциальных жертв.

Если информации в базах данных недостаточно, то сотрудники группы «пробива клиентов» осуществляют дополнительный сбор сведений о потенциальной жертве. Основным инструментом поиска являются специализированные Telegram-боты. Такие боты объединяют информацию из различных украденных из организаций баз данных и предоставляют возможность получить по номеру телефона различную исчерпывающую информацию о его владельце.

Так, через Telegram-бот можно заказать «расширенный поиск» по требуемому субъекту: найти по номеру телефона дополнительную информацию о клиенте в социальных сетях и коммерческих сервисах ВКонтакте, Skype, Одноклассники, WhatsApp, Telegram, GetContact, NumBuster, TrueCaller, объявления на Avito, Youla, Auto, Cian и др. Некоторые сервисы позволяют отправить анонимное SMS-сообщение, получить образец голоса абонента. При выборе подобной услуги абоненту поступает звонок, определяющий доступность телефона, и в случае, если абонент принял вызов, включается диалог с голосовым роботом. Файл с записью голоса поступает инициатору запроса сразу после завершения диалога, длительность составляет 10 секунд. При этом можно выбрать сценарий звонка: «мужчина», «девушка», «грубый», «наглый», «школьник», «курьер» и др.

Таким образом, имея минимальный набор первичной информации о клиенте (например, только номер телефона), с помощью специальных Telegram-групп злоумышленники получа-

ют исчерпывающую информацию о своей жертве и совершают эффективные адресные атаки на конкретную жертву, создавая у нее ощущение, что с ней действительно разговаривает сотрудник банка или правоохранительных органов.

Поэтому злоумышленникам для совершения атак изначально не требуется широкий набор персональных данных. Фактически достаточно только номера телефона, имени и отчества его владельца.

СЦЕНАРИИ РАЗГОВОРА С ПОТЕНЦИАЛЬНЫМИ ЖЕРТВАМИ

Мошенники используют сотни заранее разработанных сценариев разговора. Но существует несколько основных сценариев: 1) звонки от имени службы безопасности банка, 2) звонки от имени правоохранительных органов; 3) сообщение в мессенджере от имени портала «Госуслуги»; 4) сообщение в мессенджере от имени оператора телефонной связи.

Каждый звонящий мошенник, в зависимости от опыта работы, добавляет в сценарий (скрипт) телефонного разговора или сообщения в мессенджере некоторые дополнительные детали, помогавшие войти в доверие к клиенту. Обзвонщик представляется, например, сотрудником того или иного конкретного банка в зависимости от информации о клиенте, которой он располагает.

Для сомневающихся клиентов существует специальный скрипт «ломаем заборы», в котором описывается какими терминами должны оперировать сотрудники call-центра и как строить разговор, если клиент усомнился в правдоподобности звонка:

– мошенники убеждают клиентов, что звонки банка могут быть не только с короткого номера «900», но и с других номеров «с защищенной линии технического отдела службы безопасности», а также могут поступать через сообщения в мессенджерах;

– для убедительности клиенту называется сумма и время его последних проведенных операций. Интересно, что эту информацию мошенники узнают от самого клиента во время первой линии его разговора.

Иллюстрацией сценарности может служить запись телефонного разговора юриста Смбата Алиханяна с мошенниками [Мошенники из сбербанка попали на юриста! Полный разговор! - YouTube].

Общая модель мошеннических действий приводится в Приложении 2 [по: Моисеева, 2022].

В телефонном разговоре мошенники поэтапно применяют психологические технологии [Моисеева]:

1. Создание проблемы.
2. Погружение в стресс.
3. Управление действиями жертвы, которая находится в измененном состоянии сознания:

– выяснение баланса по счетам;
– выяснение конфиденциальных данных;
– слом сопротивления жертвы;
– перевод денег (через код в смс или через банкомат)

На первом этапе мошенники имеют целью ввести человека в заблуждение, посредством чего создать в субъективном восприятии якобы проблемную финансовую ситуацию.

На втором этапе мошеннические действия направлены на погружение человека в глубокое эмоциональное состояние (стресс, измененное состояние сознания), в котором для жертвы затруднено критическое мышление и способность контролировать свои действия и благодаря которому жертвой становится легче управлять.

Мошенники стремятся предупредить попытки жертвы разрешить ситуацию, прибегнув к посторонней помощи. Им важно замкнуть процесс решения проблемы на себя, т. е. показать, что только они способны решить возникшие трудности клиента и вывести его из сложившейся ситуации с минимальными потерями, все остальные этого сделать не смогут. Для этих целей мошенники применяют широкий арсенал методов психологического воздействия: от примитивного информационного манипулирования до прямых угроз уголовной ответственностью или шантажа потерей денежных средств [Моисеева, 2022].

На третьем этапе мошенники переходят к непосредственному управлению действиями жертвы. Для этого используется

процедура идентификации, в ходе которой жертва, осознавая безвыходность ситуации и опасаясь за свои финансы, сообщает данные своей банковской карты. Здесь мошенники используют директивные высказывания – четкие указания к действиям. В ходе дальнейшего разговора мошенники под предлогом проведения процедуры возврата денежных средств или страхования всех счетов выясняют баланс по имеющимся банковским картам, наличие кредитов и вкладов, секретную информацию в виде CVC-кодов и другие данные, позволяющие удаленно управлять денежными средствами.

ПРИЕМЫ РАБОТЫ МОШЕННИКОВ С СОПРОТИВЛЕНИЕМ КЛИЕНТОВ

Пользуясь низким уровнем финансовой грамотности населения:

– мошенники используют специфическую терминологию,

– создают иллюзию срочности или безотлагательности конкретных действий,

– угрожают мнимой уголовной ответственностью за разглашение банковской тайны, блокированием счета, арестом денежных средств при отказе сообщать личные сведения.

Любые способы преодоления опасной ситуации, которые предлагаются жертвой, мошенники искусно обесценивают.

Например, мошенники убеждают жертву, что перевод денежных средств на карту другого человека приведет к списанию всех денежных средств с его карты, а в случае звонка в банк возникшая проблема не решится, поскольку его службы не обладают нужными инструментами, при этом потраченное на такой звонок время, как и любое прерывание мобильного соединения, приведет к потере денег.

На этапе перевода и получения денежных средств мошенники призывают клиента к помощи. Они предлагают принять активное участие в поимке сотрудника, по вине которого были скомпрометированы личные данные, отключено СМС-информирование или произошли еще какие-либо изменения персональной информации.

Эта ситуация позволяет мошенникам развивать два основных сценария.

Первый сценарий будет реализовываться, если жертва демонстрирует высокий уровень владения средствами электронного платежа. В этом случае мошенники сообщают, что нужно создать специальный защищенный счет, куда жертва должна будет перевести все свои денежные средства или продиктовать специальные коды из смс-уведомления.

Второй сценарий разрабатывается для тех, кто не обладает такими техническими возможностями – им предлагается посетить отделение банка и совершить перевод через банкомат.

В навязанном телефонном разговоре необходимо обращать внимание на психологические признаки использования методов социальной инженерии или иного воздействия.

Признаки использования методов социальной инженерии:

– ведение диалога по типу «суфлера»,

– использование заученных фраз,

– смена ролей от представителей кредитных организаций до сотрудников правоохранительных органов,

– призывы к помощи поймать преступников.

При выражении жертвой недоверия или отказе предоставить какие-либо сведения потенциальная жертва сталкивается с прямым раздражением или наигранным удивлением.

Преступников могут выдавать говор, акцент, безграмотная речь, низкая общая осведомленность или сниженная интеллектуальная функция, угрозы или шантаж. Мошенник в телефонном разговоре может перейти на крик, нецензурную брань, раздражение, оскорбление.

Для оказания сопротивления распознанному психологическому воздействию нельзя доверять полученной информации и выполнять директивные указания. Не стоит также стремиться «переиграть» мошенников – гораздо безопаснее прекратить диалог под любым предлогом и связаться с сотрудниками банка для предотвращения списания денежных средств.

ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ МОШЕННИЧЕСКИХ ЗВОНКОВ

В статье, подготовленной в рамках государственного задания правительства Российской Федерации Финансовому университету на 2022 год по теме «Модели и методы защиты текстов в рамках противодействия телефонному мошенничеству» (ВТК-ГЗ-ПИ-30-2022), авторский коллектив представляет разработанный ими метод выявления мошенничества в телекоммуникационных системах на основе анализа содержания телефонного разговора, основанного на использовании нейросетевых методов распознавания эмоций речи. Точность данного метода составила порядка 92%. Предполагается создание приложения для мобильных телефонов, которое позволит использовать предложенный метод для онлайн-обнаружения факта мошенничества до момента, когда будет нанесен ущерб вызываемому абоненту [Филимонов А.В. с соавт., 2022, с. 90].

Аудиозапись переводится в текстовое представление разговора с предполагаемым мошенником и далее осуществляются две взаимодополняющие проверки: проверка на эмоциональное давление со стороны одного из участников разговора (модуль анализа эмоций) и проверка на характерные шаблоны построения фраз (модуль анализа стоп-слов). Результаты работы обоих модулей сопоставляются в модуле анализа динамики разговора, на основании чего принимается решение, является ли вызывающий абонент мошенником или нет [Филимонов А.В. с соавт., 2022].

Манера ведения разговора со стороны злоумышленника укладывается в несколько типовых схем.

ЭМОЦИОНАЛЬНОЕ ДАВЛЕНИЕ

Структура информационного текста принципиально отличается от структуры внушающего (манипулирующего) текста и характеризуется отсутствием намеренной ритмизации его лексических и фонетических единиц [Филимонов А.В. с соавт., 2022, с. 86].

На практике это означает, что некоторые звукосочетания способны не только вызывать определенные эмоции, но и могут восприниматься в качестве определенных образов. Например, в сочетаниях буква «и» с указанием предмета обладает свойством «уменьшения» объекта, перед которым (или в котором) она явно доминантно присутствует. Также, звук «о» производит впечатление мягкости и расслабленности. Преобладание звуков «а», «э», как правило, ассоциируется с эмоциональным подъемом. Логика выделения знаков соответствует физиологии человека. Например, когда человек волнуется, то ему требуется больше кислорода для дыхания, и поэтому он широко открывает рот. Соответственно, в его речи будут преобладать «кричащие» звуки: а, о, э и т.п. Даже когда человек использует письменную речь, а не устную, то все равно копирует звуковые диспропорции в соответствии со своим эмоциональными состояниями [там же].

Эмоциональное давление в разговоре может указывать на попытку манипуляции.

ИСПОЛЬЗОВАНИЕ ШАБЛОННЫХ СЛОВ

Одна из последних схем мошенничества, которая появилась сравнительно недавно: «Здравствуйте. Меня зовут ... ». Делается звонок с произвольного мобильного телефона. Молодой человек произносит следующую фразу: «Здравствуйте. Меня зовут Александр. Алло, вас плохо слышно. Вы меня слышите?». Потом происходит сброс вызова. Здесь осуществляется прямая манипуляция собеседником, когда человека вынуждают произнести слово «Да». Цель – сбор образцов голоса с привязкой к номеру мобильного телефон, что очень опасно.

Опасность состоит в том, что в настоящий момент наблюдается бум голосовых помощников от разных сервисов, включая банковские.

Если в телефонном разговоре встретилось сочетание слов «вы меня слышите? (или каких-то других фраз, требующих ответа: «да!»), то данный разговор можно считать подозрительным.

Подозрительными должны рассматриваться и такие наборы слов, как «служба безопасности», «CVC-код», «прокуратура», «счет», «зеркальный кредит», «безопасная ячейка» и т.д.

НЛП-ТЕХНИКИ КАК ИНСТРУМЕНТ ТЕЛЕФОННЫХ МОШЕННИКОВ

Мошенник в ходе общения с потенциальной жертвой осуществляет направленное манипулирование собеседником. Для этого он использует различные техники.

Наиболее распространенная среди них – техника перегрузки. Данная техника основана на превышении лимита восприятия поступающей информации.

В ходе телефонного разговора мошенники оказывают эмоциональное давление и используют характерное построение фраз, специфические шаблонные слова.

Основная задача мошенника – воздействие на когнитивное поле потенциальной жертвы, изменение его сознания, что приводит к иррациональности в поведении.

Каждый человек время от времени впадает в непроизвольный транс, каждый имеет такую же потребность в трансе, как и во сне (Коуплан, 2001) [по: Сергеева, Кубекова, 2019, с. 279]. Микродинамика наведения гипнотического транса и внушения состоит из следующих стадий: 1) фиксация внимания; 2) депотенциализация установок сознания (изменение психического функционирования в сторону гипнотического, т. е. правополушарного); 3) бессознательный поиск; 4) гипнотический отклик [там же].

ОСОБЕННОСТИ ТРАНСОВОГО СОСТОЯНИЯ ЖЕРТВ

Переход в трансовое состояние является переходом в арефлексивность. Трансовое состояние сходно с состоянием засыпания, некоторой «потерей себя».

Для наведения трансового состояния мошенники создают у жертвы чувство опасности, применяют эффект неожиданности, используют угрозы.

РЕЧЕВЫЕ МАНИПУЛЯЦИИ, ИСПОЛЬЗУЕМЫЕ ТЕЛЕФОННЫМИ МОШЕННИКАМИ [Макаров, Шумилина, 2021]

– использование образа авторитетного лица, которое не позволяет безразлично относиться к его словам;

– использование образов попавших в беду близких людей, что вызывает у потерпевших сильные эмоции, чувство сопереживания;

– использование эффекта неожиданности, что создает ощущение растерянности;

– прямое или косвенное указание на ограниченность времени для принятия решения;

– использование конструкции «или-или» («или вы переводите средства, или ваш внук будет посажен в тюрьму» и т.д.);

– «перетасовка» как упоминание только положительных или отрицательных фактов и умалчивание противоположных.

2. СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ТЕЛЕФОННОМУ МОШЕННИЧЕСТВУ

	Признаки действий мошенников	***Что нужно знать и как нужно действовать***
1.	Звонящие, представляясь сотрудниками банка, государственных или правоохранительных органов, предлагают сообщить сведения о ваших счетах, картах	Сотрудники банков, госорганов и правоохранительных органов никогда не запрашивают по телефону или через мессенджеры подобную информацию. Положите трубку.
2.	Запрашивают сведения об оформлении кредита	Положите трубку.
3.	Предлагают отвечать на вопросы односложно: «да», «нет»	Положите трубку.
4.	Требуют перечислений денег с одного счета на другой, оформления кредитов	В банках нет «безопасных счетов», «безопасных ячеек», «зеркальных счетов». Положите трубку.

5.	Оставляют мало времени на раздумья, требуют быстрого выполнения операций	Скажите: «Я не могу сейчас говорить!» Положите трубку.
6.	Кричат, настаивают, угрожают	Положите трубку.
7.	Требуют установить в мобильных устройствах или компьютерах какие-либо приложения, программы (предназначенные для защиты от несанкционированного оформления кредитов, списания личных накоплений со счетов, а также оказаний иной помощи в защите средств клиента), создать виртуальные карты, скайпы и т.д.	Положите трубку.
8.	Предлагают назвать коды и пароли из смс-сообщений	Положите трубку.
9.	Звонки поступают в мессенджерах: «Вайбер», «Ватсап», «Телеграмм» от имени сотрудников банков или правоохранительных органов.	Положите трубку.
10.	Сотрудники банков или правоохранительных органов в мессенджерах направляют Вам фотоизображения своих служебных удостоверений, иных документов с фото, личными данные работника, справок из банков об оформлении на Ваше имя кредита, о погашении Вами кредита после перевода денежных средств.	Ни при каких обстоятельствах сотрудники банков или правоохранительных органов не будут направлять Вам указанные личные, служебные документы! Положите трубку.

ПРИЕМЫ ПРОТИВОДЕЙСТВИЯ, КОТОРЫЕ СЛЕДУЕТ РЕКОМЕНДОВАТЬ ГРАЖДАНАМ В СЛУЧАЕ ЗВОНКА С НЕЗНАКОМОГО НОМЕРА ТЕЛЕФОНА

1.	Любой звонок с незнакомого номера должен насторожить
2.	Особенно необходимо насторожиться, если вам звонят со слишком короткого номера, состоящего из трех или четырех цифр, или звонок поступает со скрытого номера
3.	«Сбрасывающие» звонок почти всегда мошенники
4.	Не перезванивайте на незнакомые номера, если звонок оказался слишком коротким или, когда вы заметили пропущенный незнакомый вызов
5.	Если звонок поступил со знакомого вам номера, но во внеурочное время, стоит отнестись к нему с настороженностью. Мошенники могут сгенерировать любой номер телефона
6.	Разговор лучше начинать со слов «Слушаю» или «Алло»
7.	Не вступайте в беседу, если у вас срочно требуют деньги или данные банковской карты. Просто положите трубку
8.	Если вы начали разговор, включите громкую связь
9.	Спросите ФИО звонящего, запишите
10.	Скажите, что вы перезвоните в банк и в полицию
11.	Положите трубку, сделайте паузу
12.	Не принимайте быстрых решений
13.	Не сообщайте информацию, которую у вас просят
14.	Сообщите о звонке родственнику, другу, соседу, которому вы доверяете
15.	*Если вы разволновались, для того, чтобы успокоиться примените простые психологические техники:* • отвлекитесь от разговора и начинайте считать: пять, четыре, три, два, один; • мысленно перечислите пять предметов, которые вы видите, потом четыре цвета, потом три мысли, пришедшие в голову, два звука и один запах
16.	При повторных звонках отключите телефон
17.	Если есть сомнения в сохранности имеющихся на счетах денежных средств, обратитесь в банк, позвоните в полицию
18.	• Если вы распознали мошенника, не следует в телефонном разговоре пытаться «подколоть» их, вывести «на чистую воду», «развес-

18.	ти», вначале подыгрывая им, чтобы потом обругать, посмеяться или угрожать. Это может привести к мести с их стороны. *«Месть» от мошенников может быть организована так:* • звонки с незнакомых номеров учащаются; • мошенник работает из-под программы, которая подменяет номер телефона. Он просто заменяет свои цифры на ваши из мести. Другие люди пытаются дозвониться на ваш номер, хотя вы лично никому не звонили. Они видят пропущенный и набирают номер спустя время; • после подмены номера некоторые жертвы думают, что это вы занимаетесь подобной авантюрой. Им звонит преступник с «вашего» номера. Людей разводят, после чего звонят по номеру, который у них высветился. Вы берете трубку, и слушаете много новой информации о своей персоне; • преступники звонят от вашего имени в полицию. Они заявляют, например, о заложенной в школе бомбе. Стоит ли объяснять, что полицейские быстро вычислят человека по номеру телефона. То есть, вас. Разбираться: кто на самом деле и кому звонил – будут, но много позже; • ваш телефон указывают на сайтах знакомств в приватных чатах. Вам начинают поступать предложения непристойного характера. Если вы живете один или одна – это не страшно. Состоя в браке, объяснить такие смс или сообщения в мессенджере довольно сложно; • хорошо, если человек просто перезвонил вам. Совсем другое дело, когда люди все-таки попадают на развод. Их сложно переубедить, что ваш номер просто заменили. И вы ничего такого не совершали. В некоторых случаях потерпевшие могут указать ваш номер телефона, составляя заявление в полицию. Вот тут и придется долго и упорно доказывать собственную непричастность
19.	*Защитить себя от мести мошенников можно так:* • просто не брать трубку, когда вам звонят с незнакомых номеров. Если вас действительно хотят найти важные или близкие люди – они напишут смс или отправят сообщение в мессенджер; • не конфликтовать и не отшучиваться. Чувствуете с первых строк, что вас разводят – просто положите трубку, пожалейте свое время; • установите приложения для фильтра телефонного спама. Так вы уже сможете себя уберечь от львиной доли мошеннических звонков; • просто переждать, если вы подшутили над жуликом, а он запустил механизм мести. Как показывает практика, волна звонков со временем спадает. Мошенники не тратят много времени на месть. У них есть много других задач; • сохраняйте спокойствие. Вы всегда можете показать журнал звонков или взять выписку по истории звонков у мобильного оператора

3. ПСИХОЛОГИЧЕСКИЙ ПОРТРЕТ ЖЕРТВ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Согласно результатам исследования [Мешкова с соавт., 2022] группу риска, подверженную манипулятивному воздействию телефонных мошенников, составляют люди:

– возраста 50+ ,
– с выраженными ценностями безопасности,
– с образом мышления наивного оптимиста,
– с высоким самоконтролем,
– ставящие интересы группы выше собственных,
– склонные к сотрудничеству.

Исследователи констатируют, что основная доля звонков от мошенников в последнее время основана на страхе жертвы потерять, что имеешь, а не на стремлении обогатиться [Мешкова с соавт., 2022, с.142].

Мошенники быстро вычисляют в разговоре уязвимые точки собеседника и начинают на них давить. Страх за собственные сбережения, за близких, за собственную репутацию – вот на что они делают ставку [На их уловки ведутся даже профессора...].

«Страх потери» может являться более сильным фактором манипулирования, чем желание обогатиться. Доверчивая жертва загоняется в безальтернативную ситуацию при страхе потерять, тогда как обогащение предполагает «вилку возможностей»: от готовности рисковать дальше и, в итоге, оказаться (или не оказаться) жертвой мошенничества – до сдерживания рисков («вовремя выйти») и полного отказа контактировать с мошенниками» [Мешкова с соавт., 2022, с. 143].

ВИКТИМНОЕ ПОВЕДЕНИЕ ЛИЦ ПОЖИЛОГО ВОЗРАСТА КАК ПОТЕНЦИАЛЬНЫХ ЖЕРТВ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

Очень часто жертвами мошеннических действий с использованием средств мобильной связи становятся лица пожилого возраста. В силу возрастных психофизических особенностей онив значительной степени подвержены психологическому манипулированию. Исследователи в области социальной психо-

логии отмечают, что ухудшение социо-когнитивных способностей, необходимых для обработки подозрительной социальной информации, является одним из определяющих факторов снижения социального функционирования, в результате чего лица пожилого возраста более подвержены рискам стать жертвами мошенничества [Зотина, 2923, с. 33–34]. Несмотря на информационную пропаганду в отношении противодействия телефонным мошенникам, пожилые граждане продолжают вступать с ними коммуникацию, а обращение со стороны «представителя правоохранительных органов» вызывает у них чувство доверия, защищенности, выступает дискурсивным маркером установления и поддержания речевого контакта. Кроме этого, большое значение имеет недостаточный уровень финансовой грамотности пожилых граждан, отсутствие базовых навыков обеспечения информационной безопасности в сети Интернет, их неспособность распознавать приемы психологического (нейро-лингвистического) манипулирования и оказывать им эффективное противодействие [Зотина, 2023, с. 34].

В 2022 году был проведен опрос, в котором приняли участие 1043 россиянина (465 мужчин и 578 женщин) [Медяник, Легостаева, 2022].

В результате было выделено четыре психотипа финансового поведения людей: тревожный, рациональный, недоверчивый, доверчивый (табл.).

Тревожный тип финансового поведения содержит следующие признаки: сложности с концентрацией внимания, раздражительность,неспособность расслабиться, беспокойство и др. Рациональный тип финансового поведенияотличается недоверием ощущениям и интуиции при принятии важных решений,недоверием чувствам и инстинктивным чувствам, взвешенным принятием решений и др. Недоверчивый тип финансового поведения содержит следующие признаки: доверие маркетплейсам, недоверие к кредитам, недоверие рисковым проектам, экономное финансовое поведение и др. Доверчивому типу финансового поведения соответствуютследующие признаки: доверие с опорой на внутреннее чутье, отсутствие финансовой безопасности, доверие первому впечатлению и др.

Тревожный	***Рациональный***	***Недоверчивый***	***Доверчивый***
Распространенные симптомокомплексы в условиях финансовой тревоги			
• Яркие характеристики финансовой тревожности. • Сложности в концентрации внимания. • Внутренняя скованность. • Бессонница. • Головокружение. • Раздражительность. • Скованность мышц и тяжелое дыхание	Отсутствие ярких характеристик финансовой тревожности	Отсутствие ярких характеристик финансовой тревожности	Отсутствие ярких характеристик финансовой тревожности
Психологические риски			
• Длительная концентрация на проблеме. • Беспокойство. • Неспособность расслабиться. • Отсутствие уверенности в завтрашнем дне. • Склонен к внушению	• Недоверие чувствам и ощущениям при принятии решений. • Недоверие интуиции при любых ситуациях. • Недоверие инстинктам при решении жизненных проблем	• Не склонен к экстриму. • Недоверчив	• Доверие с опорой на внутреннее чутье. • Доверие первому впечатлению. • Склонен к внушению
Финансовые риски			
• Страх невозврата кредита. • Отсутствие страха перевода денег в интернете	• Взвешенное чувство при принятии финансовых решений.	• Недоверие маркетплейсам и финансовым платформам.	• Финансовая доверчивость. • Неуверенность в финансовом будущем

Финансовые риски			
	• Расчетливость и финансовое планирование. • Нежелание зависеть от чужого мнения. • Сниженное финансовое доверие	• Недоверие кредитам. • Недоверие рисковым проектам. • Экономное финансовое поведение	• Отсутствие финансовой безопасности. • Риск оказаться жертвой финансовых мошенников
Код психологической уязвимости			
• Воздействие ролью друга	• Отсутствие кодов финансовой уязвимости	• Воздействие авторитетом. • Воздействие взаимностью. • Воздействие экспертностью	• Воздействие инструктажем. • Воздействие обязательством. • Воздействие страхом. • Воздействие профайлингом. • Воздействие сравнением. • Воздействие экспертностью
Рекомендации			
• Рационализация страхов. • Контроль финансовой безопасности. • Переключение эмоций. Положительный настрой. • Приятие финансовых решений «здесь и сейчас». • Снижение отклика на рекомендации друзей	• Ограничение рационализации финансового поведения. • Ограничение волюнтаризма. • Снижение переоценки своих знаний в области финансов	• Способность принять помощь от другого, не только авторитетного и статусного источника. • Актуализация доверия к окружающим. • Снижение финансовой избирательности и бдительности	• Рационализация финансового поведения. • Финансовая грамотность. • Финансовая активность. Готовность брать на себя ответственность за свои финансовые действия. • Снижение патернализма

ИНДИКАТОР ПСИХОЛОГИЧЕСКИХ РИСКОВ ДЛЯ ТИПОВ СТРАТЕГИЙ ФИНАНСОВОГО ПОВЕДЕНИЯ В УСЛОВИЯХ ФИНАНСОВОЙ СУГГЕСТИИ

Кластеры	*Стратегии финансового поведения*	*Склонность к суггестии*	*Пол*	*Материальное положение*	*Возраст*	*Проценты (%)*	*«Светофор рисков»*
1	Интуитивный	да	Мужчины и женщины	Низкое и среднее	26-45	32,2	
2	Ситуативный	да	Женщины	Среднее	25-45	16,7	
3	Рациональный	нет	Женщины	Среднее	25-45	25,5	
4	Недоверчивый	нет	Мужчины	Среднее	25-45	5,8	
5	Осторожный	да	Женщины	Среднее	25-35	19,8	
Всего:						100,0	

Наиболее высокорисковыми типами (темно-серый цвет) в ситуации финансового мошенничества будут Интуитивный и Ситуативный типы стратегий финансового поведения. Эти психотипы склонны к финансовой суггестии. Они могут быть более подвержены манипуляции и обману со стороны мошенников, использующих их тревогу и интуицию для привлечения внимания и совершения финансовых ошибок. Из предоставленных данных можно сделать вывод, что наиболее низкорисковыми типами (среднесерый цвет) (31,3%) в ситуации финансового мошенничества являются Недоверчивый и Рациональный типы. Осторожному психотипу (почти 20%) от выборки помогает финансовая тревожность, как личностное свойство психики. Они находятся в осторожной позиции, но эмотивность может помещать им принять правильное решений в условиях дефицита времени.

ВЛИЯНИЕ ЛИЧНОСТНЫХ ОСОБЕННОСТЕЙ НА ВЫБОР ПСИХОЛОГИЧЕСКИХ СТРАТЕГИЙ [Программа для ЭВМ, 2022 / О. В. Медяник, И. В. Зеленчук]

Кластер 1 (32,3 % от всей выборки). Интуитивная стратегия финансового поведения.

Кластер 1 представляет собой группу людей с интуитивной стратегией финансового поведения. У выборки этого кластера лидирует интуитивный и тревожный профиль финансового поведения. Они предпочитают полагаться на свои внутренние ощущения и предыдущий опыт, а не на анализ фактов и цифр.

Психологический профиль. Люди интуитивного типа часто принимают финансовые решения на основе своей интуиции и внутреннего голоса, не обращая особого внимания на анализ фактов и цифр. Они могут быть склонны к риску и переживать по поводу будущих финансовых проблем, даже если такие проблемы не имеют объективных оснований. Люди этого типа могут проявлять недоверие к финансовым советам и рекомендациям, особенно если они исходят от незнакомых или непроверенных источников. Они предпочитают принимать финансовые решения самостоятельно, основываясь на своей интуиции и собственном анализе. Некоторые из них могут испытывать сомнения и беспокойство по поводу своих финансовых решений, даже если они уже доказали свою эффективность в прошлом. В результате, они могут часто менять свою финансовую стратегию и испытывать неуверенность в своих действиях.

В целом, люди с интуитивным типом финансового поведения могут испытывать сложности в управлении своими финансами из-за своей эмоциональной реакции и недоверия к окружающим. Однако, с помощью правильной подготовки и обучения, они могут научиться контролировать свои эмоции и принимать более обдуманные финансовые решения.

Прогноз. Мошенники могут использовать различные методы, чтобы привлечь и обмануть людей с интуитивным психотипом. Эти люди могут быть более склонны к доверчивости и верить в то, что им говорят, особенно если они улавливают какие-то интуитивные сигналы или чувства. Они могут быть менее подозри-

тельными и более склонными к риску, что может сделать их более уязвимыми перед мошенниками.

Склонность к суггестии. Люди, которые принимают финансовые решения на основе интуиции и эмоций, могут быть более подвержены финансовой суггестии. Использование эмоциональных стимулов и психологических техник может помочь убедить их совершить определенные финансовые действия вопреки своему желанию.

Кластер 2 (16,7%). Ситуативная стратегия финансового поведения.

Кластер 2 представляет лиц с профилем финансового поведения, характеризующимся как вызывающий беспокойство. Этот кластер в основном состоит из женщин, и в нем преобладают лица старше 35 лет. Большинство людей в этой группе находятся в возрастном диапазоне от 26 до 45 лет, без экономического образования, занятые в негосударственном и коммерческом секторе.

Психологический профиль. Что выделяется в этом кластере, так это профиль их финансового поведения. Индивиды в этом кластере более склонны принимать рациональные решения, в то же время полагаясь в своих действиях на интуицию. Они проявляют более высокую склонность не доверять другим и часто испытывают финансовые затруднения. Они также с большей вероятностью доверяют другим в зависимости от ситуации.Люди с таким типом поведения принимают финансовые решения в зависимости от конкретной ситуации, в которой они находятся. Они могут адаптироваться к изменяющимся обстоятельствам и принимать решения на основе доступной информации и своих целей.

Люди этой группы часто принимают решения, основываясь на своих эмоциях и ощущениях. Они, как правило, испытывают высокий уровень беспокойства и опасений по поводу своих финансовых решений и общей финансовой ситуации. Для них характерно беспокоиться о финансовых проблемах и колебаться при принятии важных финансовых решений.

Люди с ситуационным типом поведения могут быть гибкими в своих финансовых решениях и уметь анализировать ситуацию, чтобы выбрать наиболее выгодное решение. Они могут учиты-

вать факторы, такие как уровень дохода, расходы, возможные риски и потенциальную прибыль. Однако они также могут быть подвержены влиянию внешних факторов, таких как эмоции или мнения окружающих. Несмотря на свою тревожность, люди этой группы обладают высокой степенью доверия к другим. Эта склонность к доверию к другим может быть объяснена их склонностью принимать решения, основанные на эмоциях и интуиции.

Прогноз. Из-за высокой тревожности и склонности к спонтанным решениям, люди с этим психотипом могут быть более уязвимыми для мошеннических схем. Они могут быть склонными доверять другим людям, что может привести к тому, что они становятся жертвами финансовых мошенников.

Склонность к суггестии. Финансовое поведение может сильно зависеть от конкретной ситуации или контекста. Люди могут быть более склонны к суггестии, когда они находятся под воздействием определенных факторов, таких как социальное давление, авторитетные источники информации или временные ограничения.

Кластер 3 (25,5%).Рациональный тип финансового поведения.

Кластер 3 представляет людей, характеризующихся своим финансовым поведением, которое можно охарактеризовать как недоверчивое. Этот кластер преимущественно состоит из женщин, причем значительное большинство составляют лица старше 25 лет, наиболее заметной является возрастная группа от 26 до 45 лет.

Что делает этот кластер уникальным, так это его разнообразие с точки зрения статуса занятости. Здесь есть как работающие люди, так и те, кто не работает или является студентом, включая студентов, временно безработных, незанятых, лиц, занятых в домашнем хозяйстве, лиц, находящихся в декретном отпуске, и пенсионеров. Что касается уровня образования, то преобладают лица с высшим или незаконченным высшим образованием.

Психологический профиль. Этот кластер демонстрирует рациональный профиль финансового поведения. Люди с таким профилем финансового поведения, как правило, проявляют высокую степень недоверия к другим людям и финансовым вопросам. Они

подходят к финансовым предложениям и решениям с осторожностью и подозрением, тщательно проверяя их на надежность и прибыльность. Этот осторожный характер распространяется и на их финансовые решения, поскольку они отдают предпочтение стабильности и часто избегают рисков. Они, как правило, более консервативны в выборе инвестиций, предпочитая надежные, но потенциально менее прибыльные методы управления финансами.

Более того, недоверчиво-рациональное финансовое поведение проявляется в повышенном уровне осторожности при трате денег. Эти люди, как правило, экономны, придерживаются строгого финансового планирования и бережливы, избегая ненужных расходов и полагаясь на внешнюю финансовую помощь. Они предпочитают решать финансовые проблемы самостоятельно, не полагаясь на поддержку других людей или внешние источники.

Прогноз. Профиль рационального финансового поведения может ограничивать возможности получения дохода и инвестиций, но он служит защитой от финансовых рисков и обеспечивает финансовую независимость и самодостаточность. Эти люди демонстрируют уникальное сочетание осторожности, независимости и сильной зависимости от интуиции при принятии финансовых решений.

Склонность к суггестии. Для этого кластера рационального психотипа финансовое суггестивное воздействие может быть эффективным, если оно представлено в виде убедительных аргументов и доказательств.

Кластер 4 (5,8%). Недоверчивый тип финансового поведения.

В этом кластере преобладают мужчины, люди в возрасте 18-45 лет. Также в этом кластере незначительно преобладают работающие люди в коммерческом секторе, бюджетной сфере и студенты. Преобладают люди со средним общим, средним профессиональным и средним специальным образованием.

Психологический профиль. По всем профилям представители этого кластера имеют значения ниже среднего по всем профи-

лям (рационального поведения, доверчивого поведения, недоверчивого поведения, интуитивного и тревожного поведения). Это может указывать на то, что эти люди менее склонны в своих поступках полагаться на интуицию, а также менее склонны к принятию рациональных решений. Они менее склонны не доверять и тревожиться. При этом эти группы людей менее склонны доверять окружающим.

Исходя из этого, можно сделать вывод, что данный кластер еще можно назвать «осторожным», низко социализированным в финансовой жизни. Люди из этого кластера не склонны к экстремальным решениям и действиям, они в большей степени руководствуются логикой, не доверяют на слово, и чаще подозревают всех вокруг в плохих намерениях. Такой психотип финансового поведения будет взвешенно оценивать свои действия и не будет поддаваться на уговоры или манипуляции в условиях мошенничества.

Прогноз. В целом, прогноз для недоверчивого типа финансового поведения включает в себя более взвешенное принятие финансовых решений, осторожное отношение к риску и низкий интерес к финансовой активности. Но недоверчивый психотип может быть более подвержен из-за своего скептицизма и недоверия, если на них воздействуют с помощью манипулятивных кодов.

Склонность к суггестии. Совсем немногочисленная часть потребителей может быть склонна к недоверию к финансовым предложениям и рекламе. Однако, с помощью правильной коммуникации и использования доверия, финансовое суггестивное воздействие может быть эффективным даже для них.

Кластер 5 (19,8%). Осторожный (тревожный) тип финансового поведения.

Кластер 5 представляет людей с профилем финансового поведения, характеризующимся как недоверчивый, интуитивный и тревожный. Этот кластер преимущественно состоит из женщин, в основном в возрасте от 18 до 45 лет, с более высокой концентрацией в возрасте от 26 до 45 лет.В этом кластере доминируют работающие люди. Уровень образования тяготеет к высшему или незаконченному высшему образованию.

Психологический профиль. Профиль финансового поведения этого кластера отличается доверием ниже среднего, в то время как все остальные профили оцениваются выше среднего.

Люди в этой группе в выборе стратегии финансового поведения опираются на тревожность как личностную особенность. Этот психотип указывает на то, что люди в этой группе осторожны в своих финансовых операциях и более скептически относятся к намерениям других. Они часто принимают решения, основанные на сочетании рационального анализа и внутреннего беспокойства. Такой осторожный и сбалансированный подход может быть выгоден, поскольку помогает им ориентироваться во времени, сделать паузу в принятия финансовых решений. Однако их повышенная тревожность и недоверие иногда могут привести к ненужному беспокойству по инвестиционным финансовым вопросам.

Таким образом, осторожный профиль финансового поведения характеризуется уникальным сочетанием осторожности, скептицизма и опоры как на интуицию, так и на логику при принятии финансовых решений.

Прогноз. Люди этого типа будут проявлять осторожность и скептицизм в своих финансовых операциях. Они будут полагаться на сочетание интуиции и логики при принятии решений и будут стараться избегать финансовых обманов или мошенничества. Однако, из-за их повышенной тревожности и недоверия, они могут испытывать беспокойство по финансовым вопросам даже в отсутствие реальных угроз. Важно, чтобы они научились различать между реальными рисками и назначенными ими. В целом, этот психотип может быть выгодным, поскольку помогает людям ориентироваться в сложностях принятия финансовых решений и избегать потенциальных обманов.

Склонность к суггестии. Некоторые люди проявляют осторожность и предпочитают избегать рисковых финансовых решений. Для таких людей финансовое суггестивное воздействие может быть эффективным, если оно представлено в виде безопасных и надежных финансовых возможностей.

4. СОТРУДНИЧЕСТВО С ГРАЖДАНАМИ

В организации работы по противодействию телефонным мошенникам важно сотрудничать с гражданами, поощрять их за это.

Пример 1.

1. Сотрудники УМВД России по городу Кирову поблагодарили работницу офиса коммерческого банка Е. К. за проявление чуткости и гражданской позиции. Благодаря ее действиям было своевременно предотвращено дистанционное мошенничество, совершаемое в отношении 71-летней жительницы областного центра.

В офис финансовой организации пенсионерка обратилась с требованием обналичить 500 тысяч рублей с ее счета. Банковская карта заблокировалась, а деньги, по ее словам, срочно нужны на лечение. При этом женщина нервничала, разговаривала на повышенных тонах.

Менеджер Е. К., к которой обратилась пенсионерка, попыталась ее успокоить. Посетительница ответила на телефонный звонок – на связь с ней якобы вышел «врач», который, судя по поведению кировчанки, торопил с выполнением денежного перевода. Работница банка попросила пенсионерку перевести разговор в режим громкой связи, а по репликам собеседника и манере его общения поняла, что это мошенник.

Как выяснилось, накануне кировчанке позвонил незнакомец, представившийся «сотрудником службы безопасности» банка: кто-то якобы пытается похитить 500 тысяч рублей с ее счета. Для защиты от хищения их нужно перевести на «безопасный счет». В процессе выполнения женщиной телефонных инструкций банк заблокировал карту, а собеседник потребовал обналичить деньги, придерживаясь легенды необходимости лечения.

Е. К. отговорила пожилую женщину от выполнения требований звонившего, разъяснив схему обмана и предложив обратиться в полицию, где по факту покушения на мошенничество в дальнейшем было возбуждено уголовное дело.

Пример 2.

Жительнице одного из поселков Оричевского района поступил звонок на стационарный домашний телефон. Неизвестный 80-летней пенсионерке мужчина представился следователем и сообщил о якобы совершенном по вине ее дочери дорожно-транспортном происшествии. Для возмещения ущерба мошенник потребовал передать курьеру 500 тысяч рублей. Потерпевшая поверила в этот обман и приготовила деньги.

На счастье, потерпевшей в качестве курьера злоумышленники решили использовать водителя местного такси, оформив заказ на его поездку дистанционно. Прибыв по указанному адресу, водитель пообщался с женщиной, увидел признаки совершаемого в отношении нее мошенничества и убедил ее обратиться в полицию. В результате проведенной разъяснительной работы крупная сумма денежных средств – полмиллиона рублей – была сохранена. Возбуждено уголовное дело по ч. 3 ст. 159 УК РФ (Мошенничество в крупном размере).

Начальник межмуниципального отдела МВД России «Оричевский» подполковник полиции Николай Дресвянников поблагодарил водителя такси за честность, порядочность и активную гражданскую позицию, которые позволили предотвратить хищение крупной суммы у жительницы района и вручил ему благодарственное письмо.

Пример 3.

В межмуниципальный отдел МВД России «Кикнурский» обратился водитель такси, который сообщил, что, по-видимому, его наняли мошенники. Из Яранска он должен был отвезти молодого человека в Кикнур. Но по пути таксист догадался, что они едут забирать деньги у жертвы, высадил пассажира из машины, а сам обратился в полицию.

Яранские полицейские установили личность и местонахождение злоумышленника – им оказался 21-летний житель Республики Татарстан. По указаниям кураторов ночью он прибыл в Яранск, чтобы, переночевав, отправиться за деньгами. Однако передачи денег не случилось.

Полицейские опросили потенциальную жертву – жительницу Кикнура, 1953 года рождения. Пенсионерка рассказала, что накануне ей позвонил «следователь», сообщивший, что якобы ее внук виновен в ДТП. «За спасение его от уголовного дела» с женщины потребовали миллион рублей. Таких денег у пенсионерки не оказалось, но она выразила готовность отдать все имеющиеся средства. К прибытию курьера она подготовила около 200 тысяч рублей, банку варенья и постельное белье.

В отношении подозреваемого возбуждено уголовное дело по статье «Покушение на мошенничество». Проводятся следственные действия.

Пример 4.

В г. Кирсе на домашний телефон местной жительницы, 1943 года рождения, поступил телефонный звонок. Мужской голос в телефонной трубке назвал себя «сотрудником полиции» и предложил женщине за определенную сумму решить вопрос о не привлечении к уголовной ответственности ее родственницы. Якобы та совершила дорожно-транспортное происшествие и за это она неминуемо сядет в тюрьму, если только не будет заплачено 250 тысяч рублей.

Пожилая женщина восприняла угрозу в адрес своей родственницы серьезно, нашла необходимую сумму наличными деньгами и передала подъехавшему на ее адрес молодому человеку. Через какое-то время выяснилось, что с родственницей все в порядке, никаких проблем у нее нет, действовали мошенники. Потерпевшая обратилась в полицию.

Тем временем сотрудники отдела полиции «Верхнекамский» получили сигнал от граждан о нахождении в городе Кирсе явно не местного молодого человека, поведение которого вызывало подозрения в недобропорядочности его намерений. Предварительный анализ показал, что схожий по приметам мужчина приезжал к потерпевшей. Подозреваемый вызвал такси для поездки в г. Омутнинск.

Отрабатывая поступившую от коллег из Верхнекамского района информацию, сотрудники МО МВД России «Омутнинский» выставили на подъезде к городу патруль Госавтоинспекции. Как

только такси подъехало, находившийся в нем пассажир был задержан сотрудниками дорожно-патрульной службы. Им оказался гражданин одной из республик Средней Азии, находящийся на территории Российской Федерации на законных основаниях. При нем были похищенные денежные средства. С его слов предложение о заработке он нашел в сети Интернет, согласился на предложенные условия, в которые входил и разъездной характер деятельности.

Возбуждено уголовное дело по статье Уголовного кодекса «Мошенничество». Полицейскими установлен еще один факт мошенничества в Кировской области, к которому причастен задержанный.

Пример 5.

В межмуниципальный отдел МВД России «Котельничский» обратилась жительница районного центра, 1956 года рождения. Вернувшись из банка, где она перевела «на безопасный счет» 1 миллион 122 тысячи, она поняла, что ее обманули преступники.

Потерпевшая рассказала сотрудникам полиции, что несколько часов назад ей поступил звонок из «Центрального банка России». Неизвестные по телефону предупредили, что якобы постороннее лицо оформляет на нее кредит в 100 тысяч. Испугавшись за свои сбережения, она согласилась действовать по указаниям телефонного собеседника, предложившего «обезопасить накопления». Ее проинструктировали, что когда в банке она будет делать перевод со вклада, то должна будет сказать оператору, что деньги ей нужны для покупки квартиры. Она все выполнила.

Получив информацию, сотрудники котельничской полиции немедленно связались с местным отделением банка и проинформировали о совершенном в отношении их клиента преступлении. Работники финансовой организации оперативно отреагировали. Они связались с банком-получателем, транзакция денег заморозили, накопления пенсионерки не дошли до получателя. В ближайшее время они будут ей возвращены.

По факту мошенничества в особо крупном размере возбуждено уголовное дело.

Пример 6.

В Богородском районе водитель такси помог полицейским задержать подозреваемого в мошенничестве. Вечером на домашний телефон жительницы Богородского района поступил звонок. Пенсионерка, как ей показалось, по голосу в трубке опознала свою дочь. Далее последовала многократно описанная схема обмана: неизвестный представился сотрудником полиции, стал рассказывать о ДТП, о возможности избежать для ее дочери привлечения к уголовной ответственности.

Как и было предложено, предметы личной гигиены и деньги – 574 тысячи рублей (все, что имелось) – женщина передала подъехавшему на такси к ее дому мужчине.

Как уже потом рассказывал задержанный полицейскими 54-летний кировчанин, предложение о заработке он нашел в одном из популярных мессенджеров. С каждой поездки неизвестные ему обещали по 5 тысяч рублей. Ездил по указанным адресам неоднократно, получал и пересылал через терминалы деньги, однако в этот раз дело до перевода денег не дошло.

Водителем такси оказался мужчина с активной гражданской позицией. Еще по дороге ему показалось подозрительным содержание телефонных переговоров, которые вел его пассажир. А когда пожилая женщина передала ему на улице два пакета с вещами и деньгами, сомнений не оставалось.

Водитель позвонил по телефону 112, рассказал стражам правопорядка о своих обоснованных подозрениях и привез пассажира к зданию пункта полиции «Богородское». У задержанного были изъяты похищенные деньги, а сам он во всем сознался.

Возбуждено уголовное дело по статье «Мошенничество», установлена причастность задержанного к другим преступлениям, совершенным на территории как минимум еще трех районов Кировской области.

Полицейские благодарят водителя такси за его неравнодушие, смелость и решительность при пресечении противоправного деяния.

ЗАКЛЮЧЕНИЕ

Авторы-составители настоящей брошюры выражают надежду, что представленные в ней методические материалы являются полезными, расширяя представления сотрудников полиции и других заинтересованных лиц о возможностях и способах противодействия мошенничеству, совершаемому с использованием информационно-телекоммуникационных технологий.

Дистанционные мошенники постоянно совершенствуют манипулятивные тактики воздействия на сознание граждан с целью хищения их денежных средств. Преступники изобретательны и циничны. Это означает для нас только одно: необходимость проведения широкой просветительской и профилактической работы среди населения. Знание о методах мошенников поможет защитить граждан от финансовых потерь, будет способствовать повышению их психологической устойчивости.

Важно содействовать развитию у людей критического мышления, укреплять в их сознании мысль, что никогда не следует доверять незнакомым собеседникам в телефонных разговорах и при общении в мессенджерах, особенно если речь идет о деньгах. Все финансовые решения следует принимать вдумчиво и осмотрительно, подозрительные звонки и сообщения следует сразу же отклонять или тщательно проверять, проявляя бдительность.

Профилактическая работа с населением по предотвращению случаев телефонного мошенничества должна организовываться планомерно, неформально и строиться на основе специальных знаний. Важно привлекать к сотрудничеству с правоохранительными органами самих граждан.

Желаем эффективной работы на благо российских граждан!

ЛИТЕРАТУРА

Абрамовский А.А.Профайлинг: понятие и основные направления его развития в криминалистике // Известия ТулГУ. Экономические и юридические науки. 2020. №4.

Зотина Е.В. Криминологические детерминанты телефонного мошенничества, совершаемого с использованием приемов социальной инженерии // Ученые записки Казанского юридического института МВД России. 2023. Т. 8. № 1 (15). С. 31–35.

Интервью с полковником полиции Михаилом Скочиловым https://kirov-portal.ru/news/svoi-lyudi/ilon-mask-filipp-iz-turcii-podarki-i-brillianty-kak-obmanyvayut-kirovchan-distancionnye-moshenniki-intervyu-s-sotrudnikom-policii-31761/

Кудаева В. «Приезжайте, отдам деньги»: 73-летняя женщина перехитрила мошенников, встретив их курьера с полицией | КП Иркутск | Дзен (dzen.ru)

Капориков И.Обмануть обманщиков. Таксист спас бабушку от мошенников и придумал гениальный способ проучить их | РЕН ТВ | Дзен (dzen.ru)

КовалевскийВ.Какателефонныемошенникивзламываютнашесознание:интервьюспсихотерапевтом(xn--b1aew.xn--p1ai)Источник: Амурскаяправдаот27.05.2021

Коростелев П. Красивые слова: мошенники стали обманывать россиян при помощи текстов от чат-ботов | Известия | Дзен (dzen.ru)

Кубекова А.С., Мамина В.П. Техники эриксоновского гипноза в деятельности психолога // Психология служебной деятельности: достижения и перспективы развития. Санкт-Петербург, 2020. С. 879-880. .К. Кулиева. – СПб.: Скифия-принт, 2020. – 1052 с.

Макаров К.В., Шумилина В.Г. Речевые манипуляции в телефонном мошенничестве // Трибуна ученого. 2021. Выпуск 05. С. 397–405.

Медяник О.В. Исследования когнитивных искажений в цифровой экономике и праве // Юридическая мысль. 2023. № 3 (131).

Медяник О.В. Социоинженерные механизмы использования финансовой суггестии в кибермошенничестве //Журнал социологии и социальной антропологии. СПБ, 2024. №1.

Медяник О.В., Легостаева Н.И.Финансовое поведение россиян: факторы, типы, коды уязвимости//Телескоп: журнал социологических и маркетинговых исследований. 2022. № 4. С. 50–55.

Мешкова Н.В., Кудрявцев В.Т., Ениколопов С.Н. К психологическому портрету жертв телефонного мошенничества // Вестник Московского университета. Серия 14. Психология. 2022. № 1. С. 138–157. doi: 10.11621/vsp.2022.01.06

Моисеева И.Г. Психологические аспекты противодействия телефонному мошенничеству // Калужский экономический вестник. 2022. № 1. С.70–74.

Мошеннический колл-центр «Бердянск» (отчет правоохранительных органов).

Набиуллина Э.С.«Противодействие социальной инженерии и мошенничеству». Уральский форум 2023 - поиск Яндекса по видео (yandex.ru) Время выступления: 26.00 - 31.00.

На их уловки ведутся даже профессора...: чем подкупают телефонные мошенники и как от них защититься | Комсомольская Правда - Уфа | Дзен (dzen.ru)

Никитин П.В. Распознавание эмоций по аудио сигналам как один из способов борьбы с телефонным мошенничеством / П. В. Никитин, А. В. Осипов, Е. С. Плешакова, С. А. Корчагин, Р. И. Горохова, С. Т. Гатауллин // Программные системы и вычислительные методы. 2022. № 3. URL: https://cyberleninka.ru/article/n/raspoznavanie-emotsiy-po-audio-signalam-kak-odin-iz-sposobov-borby-s-telefonnym-moshennichestvom (дата обращения: 01.03.2023).

Онищенко, Ольга Романовна. Манипулирование сознанием и поведением жертв при мошенничестве : автореферат дис. ... кандидата психологических наук : 19.00.06 / Акад. права и упр. Федерал. службы исполнения наказаний. – Рязань, 2005. - 25 с.

Программа для ЭВМ. Свидетельство о государственной регистрации программы для ЭВМ № 2022667946 Российская Федерация. «Программа для определения типов финансового поведения пользователей» (FinTech User Behavior) : № 2022667319 : заявл. 22.09.2022 : опубл. 29.09.2022 / О. В. Медяник, И. В. Зеленчук ; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет».

Рябинина Ю. Доцент Тимофеев: Мошенники чаще звонят с номеров, состоящих из трех или четырех цифр - Российская газета (rg.ru)

Сергеева М.А., Кубекова А.С. Техники эриксоновского гипноза при работе с эмоциональным выгоранием у студентов медицинского вуза // Психология. Историко-критические обзоры и современные исследования. 2019. Т. 8. № 6А. С. 279-285. DOI: 10.34670/AR.2020.46.6.180

Социальная инженерия – защита и предотвращение (kaspersky.ru)

Телефонные мошенники «мстят» тем, кто не попался — вот как они это делают | Mr. Android – эксперт по гаджетам | Дзен (dzen.ru)

Тукаев Р.Д. Эволюция гипнотерапии: методические аспекты // Вестник психотерапии. 2020. № 76 (81). С. 7-29.

Филимонов А.В., Осипов А.В., Плешакова Е.С., Гаттауллин С.Т. Нейросетевые методы распознавания эмоций речи для противодействия мошенничеству в телекомукационных системах // Вопросы кибербезопасности. 2022. № 6(52). С. 83–92. DOI:10.21681/2311-3456-2022-6-83-92

Юрист из будущего Смбат Алиханян / Мошенники из сбербанка попали на юриста! Полный разговор! (dzen.ru)

Яджин Н. В. Психология мошенничеств, совершаемых с использованием средств сотовой связи // Научно-методический электронный журнал «Концепт». – 2015. – Т. 13. – С. 4261–4265. – URL: http://e-koncept.ru/2015/85853.htm.

ПРИЛОЖЕНИЕ 1

РАСПРОСТРАНЕННЫЕ НАПРАВЛЕНИЯ КИБЕРМОШЕННИЧЕСТВА [Медяник, 2023]

Мошенничество с онлайн-играми: это включает в себя различные схемы, в которых мошенники обманывают игроков, предлагая им фальшивые предметы, валюту или аккаунты в обмен на реальные деньги или ценности.

Афера с «бесплатными подарками»: мошенники обманывают людей, предлагая им якобы бесплатные подарки или призы, но затем требуют оплату за доставку или другие услуги, оставляя жертву без подарка и потерянных денег.

Афера с неполной занятостью: мошенники предлагают работу или возможность заработка, требующую минимальных усилий или времени, но в конечном итоге требуют оплату за регистрацию, обучение или доступ к информации, которая оказывается бесполезной или несуществующей.

Фальшивые инвестиционные проекты, пирамидальные схемы или схемы «продажи воздуха», где мошенники обещают высокие доходы или инвестиционные возможности, но на самом деле просто обманывают людей.

Мошенничество с кредитами: мошенники предлагают людям легкий доступ к кредитам или финансовой помощи, но требуют предварительную оплату или предоставление личной информации, которая затем используется для кражи личных данных или денег.

Мошенничество с романтическими отношениями в интернете: мошенники создают фальшивые профили на сайтах знакомств или социальных сетях и устанавливают эмоциональную связь с жертвами, чтобы потом обмануть их, попросив деньги или предоставив фальшивые истории.

Мошенничество с онлайн-покупками: мошенники создают фальшивые интернет-магазины или объявления о продаже товаров по низким ценам, но после получения платежа не отправляют товары или отправляют поддельные или некачественные товары.

Мошенничество с виртуальной валютой: мошенники обманывают людей, предлагая им покупку или инвестиции в виртуальные валюты, которые оказываются фальшивыми или несуществующими.

Инвестиционные аферы: мошенники предлагают людям высокодоходные инвестиционные возможности, но на самом деле используют их деньги для собственной выгоды или просто исчезают с деньгами.

Выдача мошенника за чиновников: мошенники представляются государственными чиновниками или предлагают помощь в разрешении юридических или финансовых проблем, но в итоге требуют оплату или предоставление личной информации.

Мошенничество с выдачей себя за другого человека: мошенники создают фальшивые профили или используют чужие личные данные, чтобы получить доступ к чужим счетам или информации.

Мошенничество с выдачей себя за представителя какой-нибудь компании: мошенники представляются сотрудниками компаний или организаций и используют это для получения личной информации или денег от жертв.

Мошенничество с иностранной валютой: мошенники предлагают людям возможность покупки или продажи иностранной валюты по выгодному курсу, но на самом деле обманывают их, получая деньги без предоставления услуги или предоставляя фальшивые валютные операции.

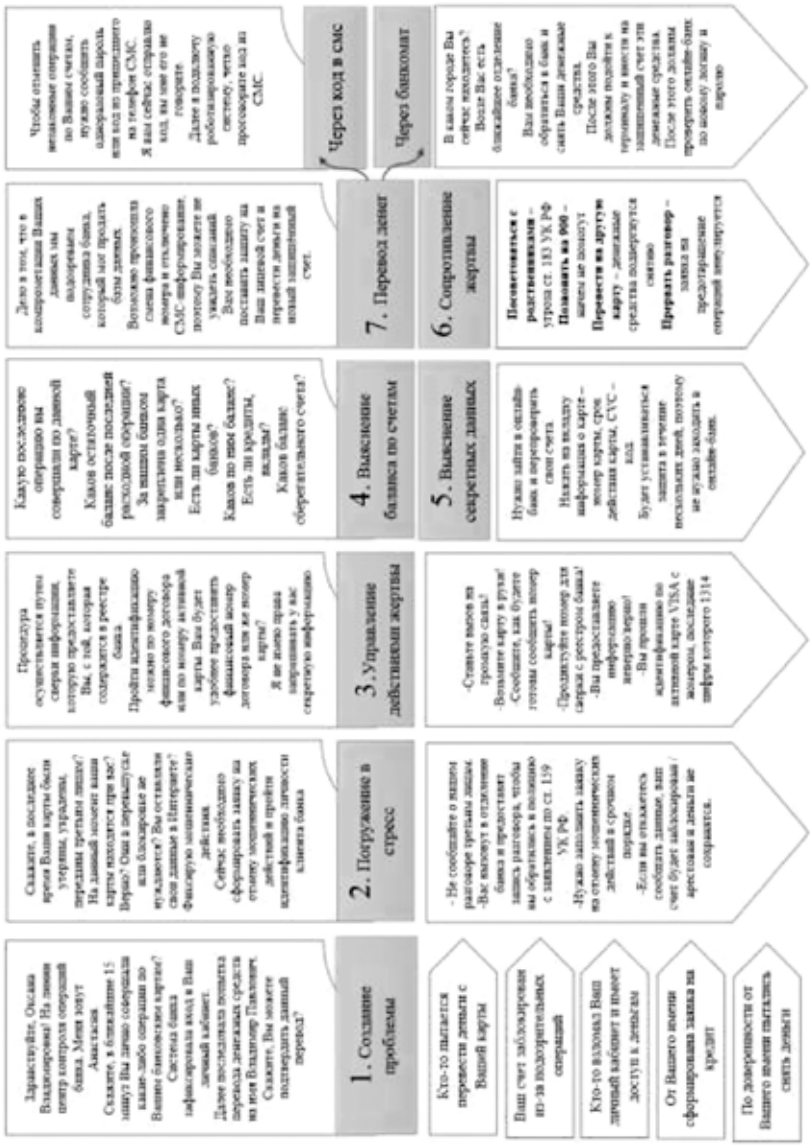
Взлом аккаунта в соцсетях: мошенники получают доступ к аккаунту пользователя в социальных сетях, чтобы отправлять фальшивые сообщения или размещать вредоносные ссылки, а также получать доступ к личной информации.

Мошенничество с доставкой посылок: мошенники предлагают услуги доставки товаров или посылок, требуя оплату заранее, но не выполняют услугу или отправляют пустые или фальшивые посылки.

Религиозные аферы: мошенники используют религиозные убеждения или обещания духовного просветления, чтобы обмануть людей, требуя пожертвования или предоставления личной информации.

ПРИЛОЖЕНИЕ 2

ОБЩАЯ МОДЕЛЬ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ
[приводится по: Моисеева, 2022]



ПРИЛОЖЕНИЕ 3

25 ВИДОВ МОШЕННИЧЕСТВА И КОГНИТИВНЫХ ИСКАЖЕНИЙ (каналы распространения: социальные сети, электронная почта, SMS-рассылки)

№	*Виды кибермошенничества*	*Эффект социальной инженерии*	*Суггестивные атаки*	*Когнитивные искажения*
1.	Предложение быстрого и легкого заработка без особых усилий.	Мошенники используют обманчивые обещания и убеждения, чтобы убедить людей вложить деньги в непроверенные или недостоверные схемы заработка.	Фантомная фиксация	«эффект подтверждения» (confirmation bias)
2.	Ложные обещания о высокой доходности инвестиций	Мошенники используют психологические методы, чтобы убедить жертву вложить деньги в их схему, обещая высокую доходность и минимальные риски.	Фантомная фиксация	«эффект доверия» (trust effect)
3.	Скрытые комиссии и скрытые условия при оформлении кредита или займа	Мошенники могут использовать доверие клиента к банку или финансовой организации, чтобы скрыть дополнительные расходы или условия, которые могут быть невыгодны для клиента.	Ландшафтный дизайн	«эффект доверия» (trust effect)
4.	Фальшивые лотереи и конкурсы, требующие оплаты за участие	Мошенники используют этот эффект, чтобы убедить людей платить за участие в фальшивых лотереях и конкурсах, которые на самом деле не существуют или не предоставляют обещанных выигрышей.	Ландшафтный дизайн	«эффект доверия» (trust effect)

№	Виды кибермошенничества	Эффект социальной инженерии	Суггестивные атаки	Когнитивные искажения
5.	Навязывание ненужных услуг или продуктов при оформлении кредита или займа.	Мошенники могут использовать страх и угрозы, чтобы заставить людей принимать решения в их пользу, угрожая отказом в выдаче кредита или займа.	Страх	«эффект авторитета» (authority bias)
6.	Мошенничество с использованием кредитных карт или банковских счетов.	Мошенники могут выдавать себя за представителей банков, правительственных органов или других авторитетных организаций, чтобы убедить жертву предоставить им свои личные данные или совершить финансовую операцию.	Профайлинг	«эффект авторитета» (authority bias)
7.	Подделка документов для получения кредита или займа.	Мошенники могут подделывать документы, чтобы создать впечатление, что они имеют высокий социальный статус или имеют доступ к конфиденциальной информации.	Экспертность	«эффект авторитета» (authority bias)
8.	Ложные обещания о снижении процентной ставки по кредиту или займу	Ложные обещания о снижении процентной ставки на кредит или займ могут убедить людей взять кредит или займ, которые они не могут позволить себе, что приведет к финансовым проблемам.	Ландшафтный дизайн	«эффект обещаний» (promise effect)
9.	Навязывание дополнительных услуг при оформлении страховки или кредитной карты.	Продавец предлагает клиенту дополнительные товары или услуги, которые могут быть необязательными или не совсем необходимыми.	Страх	«эффект подталкивания» (nudge effect)

№	*Виды кибермошенничества*	*Эффект социальной инженерии*	*Суггестивные атаки*	*Когнитивные искажения*
10	Ложные обещания о возможности получения кредита или займа без проверки кредитной истории.	Злоумышленник использует различные методы и техники, чтобы обмануть свою жертву и получить от нее нужную информацию или выполнить определенное действие.	Профайлинг	«эффектом доверия»
11.	Навязывание недвижимости или инвестиционных продуктов, которые не соответствуют потребностям клиента.	Продавец создает искусственную ситуацию, при которой клиенту кажется, что он должен срочно принимать решение о покупке, не давая ему достаточно времени на обдумывание и анализ.	Дефицит	«эффект дефицита» (scarcity effect)
12.	Предложение работы с высокой зарплатой без опыта и образования, которая оказывается нелегальной или мошеннической.	Злоумышленник может распространять ложную информацию или представлять себя как надежный источник, чтобы убедить людей в своей правоте и получить доступ к их личным данным или деньгам	Экспертность	"эффект подтверждения" (confirmation bias)
13.	Мошенничество при продаже товаров через интернет, например, продажа поддельных товаров или неисправных устройств.	Мошенники могут создавать видимость надежности и доверия, например, путем использования фальшивых отзывов или подделки сертификатов качества, чтобы убедить покупателей в том, что они покупают настоящий и качественный товар.	Экспертность	"эффект подтверждения" (confirmation bias)

№	Виды кибермошенничества	Эффект социальной инженерии	Суггестивные атаки	Когнитивные искажения
14.	Мошенничество с использованием криптовалюты, например, фейковые ICO или пирамиды	Мошенники создают ложное чувство доверия и убеждают людей вложить деньги в фейковые проекты, обещая высокую доходность.	Фантомная фиксация	«эффектом доверия» (trust effect)
15.	Навязывание услуг по ремонту или обслуживанию техники, которые не требуются или являются переплатой.	Мошенники выдают себя за экспертов или представителей компаний и убеждают людей в необходимости оплаты услуг, которые на самом деле не нужны.	Экспертность	«эффект авторитета» (authority bias)
16.	Ложные обещания о получении государственных пособий или льгот	Мошенники используют ложные обещания о получении государственных пособий или льгот, чтобы обмануть людей и получить от них деньги или личные данные.	Фантомная фиксация	«эффект обещаний» (promise effect)
17.	Мошенничество при продаже товаров через интернет, например, продажа поддельных товаров или неисправных устройств	Мошенники используют ложную информацию о товаре и обманывают покупателей, чтобы получить от них деньги.	Экспертность	"эффект подтверждения" (confirmation bias)
18.	Навязывание услуг по установке программного обеспечения, которые не нужны или могут быть установлены бесплатно.	Мошенники убеждают покупателя в том, что им необходимы дополнительные услуги, которые на самом деле не нужны или могут быть получены бесплатно.	Страх	«эффект дефицита» (scarcity effect)
19.	Ложные обещания о возможности заработка на онлайн-опросах или кликах на рекламу	Этот случай относится к эффекту манипуляции обещаниями, так как ложные обещания о возможности заработка создают у людей ожидание вознаграждения и стимулируют их к выполнению задания	Фантомная фиксация	«эффект обещаний» (promise effect)

20.	Мошенничество при продаже билетов на мероприятия, например, продажа поддельных билетов или переплата за билеты	Мошенники используют обманчивые методы, чтобы убедить людей в том, что они получат настоящие билеты или получат их по низкой цене.	Дефицит	«эффект иллюзия контроля» (Illusion of control)
21.	Навязывание услуг по продвижению сайтов или брендов, которые не являются эффективными или не нужны клиенту.	Пользователю создается ложное ощущение того, что он может контролировать ситуацию и принимать решения, когда на самом деле он попадает под влияние маркетинговых приемов и манипуляций.	Сравнение	«эффект иллюзии контроля» (Illusion of control)
22.	Навязывание услуг по оформлению документов, которые можно оформить самостоятельно или за меньшую плату.	Пользователю предлагается услуга, которая кажется ему более надежной и профессиональной, чем самостоятельное оформление документов.	Экспертность	«эффект авторитета» (authority bias)
23.	Ложные обещания о возможности снижения долгов или улучшения кредитной истории.	Злоумышленник предлагает жертве ложные обещания, чтобы получить доступ к ее финансовым ресурсам.	Авторитет	"эффект подтверждения" (confirmation bias)
24.	Навязывание услуг по оформлению виз или гражданства, которые могут быть получены только через официальные каналы	Данный случай соответствует эффекту авторитетности, когда злоумышленник выступает под видом официального представителя и убеждает жертву в необходимости использования его услуг.	Экспертность	"эффект подтверждения" (confirmation bias)
25.	Ложные обещания о возможности получения бесплатных услуг или товаров, которые требуют оплаты.	Злоумышленник использует различные методы обмана и манипуляции, чтобы получить доступ к конфиденциальной информации или денежным средствам.	Дефицит	«эффект дефицита» (scarcity effect)

Для заметок

Для заметок