УДК 343.72

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО И СПОСОБЫ ЗАЩИТЫ ОТ НЕГО

Набатова Валерия Александровна, *студентка 3 курса специалитета института экономики и управления АПК, ФГБОУ ВО РГАУ – МСХА имени К.А.Тимирязева, valeri.nabatova@gmail.com*
Никитина Ирина Денисовна, *студентка 3 курса специалитета института экономики и управления АПК, ФГБОУ ВО РГАУ – МСХА имени К.А.Тимирязева, irinavolkova212@mail.ru*
Комарова Дарья Владимировна, *студентка 3 курса специалитета института экономики и управления АПК, ФГБОУ ВО РГАУ – МСХА имени К.А.Тимирязева, dasha_32@icloud.com*

Научный руководитель - Рахаева Виктория Владимировна, *к.э.н., доцент, доцент кафедры экономической безопасности и права, ФГБОУ ВО РГАУ – МСХА имени К.А.Тимирязева, v_rahaeva@rgau-msha.ru*

Аннотация. *В статье рассматриваются современные формы телефонного мошенничества и основные методы, используемые мошенниками для обмана граждан и компаний. Подробно анализируются психологические и технические приемы, которые позволяют злоумышленникам завоевывать доверие жертв и добиваться передачи им денежных средств или конфиденциальной информации. Особое внимание уделено практическим способам защиты от телефонного мошенничества, включая использование технологий для блокировки нежелательных звонков, рекомендации по безопасности общения, а также примеры сценариев, по которым действуют мошенники. Статья предназначена для широкого круга читателей, стремящихся повысить свою осведомленность и защитить себя и свои данные.*

Ключевые слова: *телефонное мошенничество, способы защиты, безопасность данных, обман по телефону, мошеннические схемы, технологии блокировки звонков, психологические уловки, противодействие мошенничеству.*

TELEPHONE FRAUD AND WAYS TO PROTECT YOURSELF FROM IT

Nabatova Valeria Aleksandrovna, *3rd year student of the specialty program of the Institute of Economics and Management of the Agro-Industrial Complex, Russian State Agrarian University-Moscow Timiryazev Agricultural Academy, valeri.nabatova@gmail.com*
Nikitina Irina Denisovna, *3rd year student of the specialty program of the Institute of Economics and Management of the Agro-Industrial Complex, Russian State Agrarian University-Moscow Timiryazev Agricultural Academy, irinavolkova212@mail.ru*

Komarova Darya Vladimirovna, *3rd year student of the specialty program of the Institute of Economics and Management of the Agro-Industrial Complex, Russian State Agrarian University-Moscow Timiryazev Agricultural Academy, dasha_32@icloud.co*

Rakhaeva Victoria Vladimirovna*, Ph.D in Economics, Associate Professor, Associate Professor of the Department of Economic Security and Law, Russian State Agrarian University-Moscow Timiryazev Agricultural Academy, v_rahaeva@rgau-msha.ru*

Annotation. The article examines modern forms of telephone fraud and the main methods used by fraudsters to deceive individuals and companies. It analyzes in detail the psychological and technical techniques that allow attackers to gain the trust of victims and achieve the transfer of money or confidential information to them. Particular attention is paid to practical methods of protection against telephone fraud, including the use of technologies for blocking unwanted calls, recommendations for communication security, as well as examples of scenarios by which fraudsters operate. The article is intended for a wide range of readers seeking to increase their awareness and protect themselves and their data.

Key words: telephone fraud, protection methods, data security, telephone deception, fraudulent schemes, call blocking technologies, psychological tricks, counteraction

Согласно статье 159 УК РФ, мошенничество – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Телефонным мошенничеством называют аналогичное деяние – это форма преступной деятельности, при которой злоумышленники используют телефонные звонки или текстовые сообщения для обмана и получения личной, финансовой или другой конфиденциальной информации у жертвы. Оно может быть направлено как на физических лиц, так и на организации [2].

Мошенники используют различные предлоги: необходимость переоформить договор об оказании услуг связи, изменить тарифный план на более выгодный, отключить платную услугу и другие.

Цель мошенников – получить у человека код для входа в его личный кабинет мобильного оператора и установить переадресацию, либо убедить абонента подключить ее самостоятельно. Это позволит им получить доступ к дистанционному управлению банковским счетом и похитить деньги.

На сегодняшний день, по разным оценкам более 90% афер в нашей стране совершается именно по телефону.

Социальная инженерия – это метод манипуляции людьми, используемый злоумышленниками для обмана людей и получения доступа к конфиденциальной информации или ценным ресурсам. В отличие от технических взломов, которые фокусируются на уязвимостях программного обеспечения, социальная инженерия использует человеческий фактор – наши эмоции, доверие и

склонность к поспешным решениям, это искусство манипуляции, основанное на глубоком понимании психологии жертвы и умелом использовании различных приемов [1].

Основные методы социальной инженерии включают в себя:

1) Создание срочности: мошенники создают иллюзию неотложности, заставляя жертву действовать быстро, не задумываясь о последствиях. Например, они могут сообщать о блокировке банковской карты, требуя немедленного подтверждения данных для разблокировки. Срочность подавляет критическое мышление, заставляя человека реагировать инстинктивно, минуя здравый смысл. Более изощренные схемы могут включать подделку уведомлений от банковских приложений, имитируя настоящие push-уведомления.

2) Использование авторитета: злоумышленники притворяются представителями организаций – банков, правоохранительных органов, технической поддержки, ИТ-компаний или государственных служб. Они используют официальный тон, профессиональную лексику и поддельные документы (часто подделывая фирменные бланки и логотипы), чтобы убедить жертву в своей легитимности. Этот метод особенно эффективен, поскольку люди склонны доверять представителям власти или уважаемых организаций, не проверяя информацию из независимых источников.

3) Эмоциональные манипуляции: мошенники играют на эмоциях жертвы, используя страх, чувство вины, жалость, жадность или радость. Например, могут сообщать о выигрыше в лотерее, требуя оплаты налога или комиссии для получения выигрыша, или же угрожать серьезными последствиями в случае невыполнения требований. Страх перед юридическими проблемами, потеря денег или репутацией является мощным инструментом манипуляции. Более продвинутые схемы могут включать предварительное изучение жертвы в социальных сетях для выявления ее интересов и уязвимостей, которые затем используются для более эффективной эмоциональной манипуляции.

Спуфинг – это технология, позволяющая подделывать идентификационную информацию, в том числе номера телефонов, email-адреса и IP-адреса. В контексте телефонного мошенничества, подмена номера телефона делает звонок практически не отслеживаемым. Злоумышленники могут отображать на экране жертвы номер, принадлежащий банку, госучреждению или другой доверенной организации. Это увеличивает вероятность того, что жертва ответит на звонок и поверит мошеннику.

Технологии, используемые для спуфинга, постоянно развиваются. Помимо простых программ для изменения номера на вызове, активно используется VoIP (Voice over Internet Protocol) – технология, позволяющая совершать звонки через интернет, обходя традиционные телефонные сети. VoIP-сервисы часто предлагают анонимность и позволяют подменять номера из разных стран, что затрудняет идентификацию злоумышленника. Более того, развитие технологий глубокой подделки голоса (deepfake) открывает новые возможности для создания убедительных подлогов, имитирующих голос конкретного человека.

Вишинг – это телефонный аналог фишинга. Мошенники звонят жертве, представляясь сотрудниками банка, технической поддержки или других организаций, и пытаются получить конфиденциальную информацию, такую как номера банковских карт, пароли, PIN-коды, данные паспорта или номера социальных страховок. Они используют сложные сценарии, часто комбинируя несколько методов социальной инженерии, чтобы убедить жертву в необходимости предоставить личные данные.

Злоумышленники могут использовать информацию, которую они уже знают, для создания иллюзии легитимности и доверия. Например, они могут назвать имя и фамилию жертвы, последние четыре цифры номера ее банковской карты или другие детали, чтобы убедить ее в своей подлинности.

В современном цифровом мире, где киберпреступность приобретает все более изощренные формы, защита от социальных инженеров и мошенников становится критически важной. Социальная инженерия — это манипулятивное искусство, направленное на обман людей с целью получения доступа к конфиденциальной информации или ресурсам. В отличие от технических атак, которые полагаются на уязвимости программного обеспечения, социальная инженерия использует психологические уловки, играя на человеческих слабостях, таких как доверие, жадность и страх. Мошенники мастерски используют эти слабости, создавая убедительные сценарии, чтобы заставить жертву совершить нежелательные действия.

Образовательные и информационные меры играют ключевую роль в профилактике телефонного мошенничества. Когда люди знают о распространённых схемах мошенников, они менее подвержены обману. Основные направления включают просвещение о типах мошенничества, поскольку многие люди не знают о популярных схемах обмана. Регулярное распространение информации о новых схемах, которые используют мошенники (например, ложные звонки от «банков» или «госслужб»), помогает людям распознавать опасные ситуации. Также эффективны тренинги по информационной безопасности. Специальные тренинги или вебинары для сотрудников компаний и пожилых людей, которые являются основной мишенью мошенников, обучают защите личных данных и правильной реакции на подозрительные звонки. Важную роль играют медиа и социальные сети, которые используются для размещения информационных материалов на телевидении, в Интернете и социальных сетях. Платформы, такие как Facebook, Instagram, YouTube, и мессенджеры, например, WhatsApp и Telegram, подходят для распространения материалов по безопасности и предупреждений о новых методах мошенничества [2].

Современные технологии помогают распознавать и блокировать мошеннические звонки, предупреждая пользователей о потенциальной угрозе. Например, блокировщики звонков — многие мобильные операционные системы (например, Android и iOS) имеют встроенные функции для блокировки нежелательных вызовов. Эти системы могут автоматически распознавать звонки с подозрительных номеров и предупреждать пользователя о возможном

мошенничестве. Также популярны приложения для распознавания номеров, такие как Truecaller, Kaspersky Who Calls, GetContact и другие, которые собирают базу данных мошеннических номеров. Если с этого номера поступает звонок, приложение выдает предупреждение, а пользователи могут сами сообщать о мошенниках, добавляя номера в базу данных. Ещё одна мера — интеллектуальные фильтры и спам-фильтры: некоторые мобильные операторы предлагают услуги по автоматической блокировке спам-звонков на основе данных от пользователей, что снижает количество нежелательных вызовов и предупреждает о подозрительных звонках.

Соблюдение нескольких простых рекомендаций может значительно снизить риск стать жертвой телефонного мошенничества. Во-первых, важно никогда не сообщать конфиденциальные данные по телефону. Это правило должно быть строго соблюдено — никогда не передавайте по телефону свои паспортные данные, номера карт, PIN-коды и CVV-коды, даже если звонящий представляется сотрудником банка или госслужбы. Настоящие сотрудники банков и служб безопасности никогда не запрашивают такие данные. Во-вторых, всегда следует проверять информацию и не реагировать на угрозы и эмоциональные уловки. Мошенники часто пытаются запугать или заставить человека действовать импульсивно, утверждая, что банковский счёт заблокирован или грозит штраф. В таких случаях нужно прервать разговор и самостоятельно связаться с организацией, от имени которой звонили, по официальному номеру. В-третьих, рекомендуется использовать двухфакторную аутентификацию и следить за активностью банковских счетов. Двухфакторная аутентификация создаёт дополнительный барьер для мошенников, а регулярная проверка активности по банковским счетам помогает вовремя обнаружить подозрительные транзакции [4].

Государство занимает важное место в борьбе с телефонным мошенничеством, разрабатывая и принимая законы и нормативные акты, направленные на предотвращение таких преступлений и защиту граждан. В ряде стран внедряются специальные законы и ужесточаются существующие нормативные требования, чтобы бороться с телефонным мошенничеством. Эти меры охватывают различные схемы обмана, такие как ложные звонки от имени государственных структур или банков, продажа личных данных и прочее. В некоторых случаях для банков и операторов вводятся обязательные требования по усилению защиты данных клиентов и повышению безопасности коммуникаций. За телефонное мошенничество предусмотрены как административные, так и уголовные санкции, причем степень наказания зависит от тяжести преступления и нанесенного ущерба. Законы предусматривают штрафы, тюремные сроки и иные санкции для лиц, вовлеченных в мошенничество, чтобы сдерживать и предотвращать распространение подобных преступлений. Защита персональных данных также является одной из ключевых задач в борьбе с мошенниками. Законы, такие как GDPR в Европе, ограничивают доступ к личной информации и требуют от компаний высокого уровня защиты

данных клиентов, что снижает вероятность утечек, которые могут использоваться злоумышленниками [5].

Банки и мобильные операторы оказываются на переднем рубеже борьбы с мошенничеством, поскольку именно через них мошенники часто обращаются к гражданам. Поэтому компании в этих секторах внедряют различные меры для защиты своих клиентов. Банки используют системы мониторинга, которые выявляют подозрительные операции и помогают предотвратить мошенничество. Например, при обнаружении неожиданного перевода банк может заблокировать транзакцию и связаться с клиентом для подтверждения. Также банки уведомляют клиентов о попытках входа в аккаунт и изменениях, связанных с учетной записью. Операторы связи применяют алгоритмы для распознавания подозрительных звонков и блокировки номеров, с которых массово совершаются мошеннические звонки, и могут предупреждать пользователей о возможной опасности. Кроме того, банки и операторы активно информируют своих клиентов о различных схемах телефонного мошенничества через уведомления, информационные материалы, видеоролики и регулярные SMS-сообщения с советами по безопасности [3].

Совместные усилия государственных и частных структур могут значительно усилить борьбу с телефонным мошенничеством, обеспечивая обмен данными, ресурсами и координацию действий. Компании и государственные органы могут обмениваться информацией о подозрительных номерах, случаях мошенничества и новых схемах, что позволяет быстрее выявлять угрозы. Например, банки, операторы связи и государственные агентства могут вести общие базы данных мошенников и подозрительных номеров, что повышает эффективность предотвращения преступлений. Государственные и частные структуры могут также разрабатывать совместные программы информирования и обучения граждан. Совместные вебинары, социальные кампании и обучающие материалы помогают повысить осведомленность населения и защитить их от телефонного мошенничества. В некоторых странах создаются горячие линии, на которые можно сообщать о мошеннических звонках. Такие службы, организованные совместно государством и частными компаниями, собирают и анализируют информацию о случаях мошенничества и быстро реагируют на угрозы. Совместная работа операторов, банков и правоохранительных органов помогает быстрее выявлять и пресекать действия мошенников. Операторы могут определить местоположение злоумышленника, банки — предоставить данные о подозрительных операциях, а полиция — задержать преступников [2].

В заключение, телефонное мошенничество остается серьезной угрозой, требующей комплексного подхода для эффективного противодействия. Современная борьба с этим явлением основывается на тесной координации между государственными органами, частным сектором и гражданским обществом. Законы, регулирующие защиту данных и предусматривающие наказания для мошенников, создают законодательную основу, способствующую сдерживанию преступников. Банки и операторы связи играют критически важную роль, внедряя технологии мониторинга и предупреждая клиентов о

рисках. Обмен информацией и совместные программы повышения осведомленности населения позволяют быстрее выявлять и устранять угрозы, обеспечивая более высокий уровень безопасности. Развитие интегрированных решений и продолжение сотрудничества между всеми заинтересованными сторонами позволит укрепить систему защиты и минимизировать распространение телефонного мошенничества в будущем.

Библиографический список

1. Иванов, И.В. Борьба с телефонным мошенничеством: правовые и технологические аспекты // Журнал права и безопасности. — 2023. — № 4. — С. 56–68.
2. Петров, А.А. и Сидоров, Б.Б. Влияние законодательства на эффективность противодействия телефонному мошенничеству // Современные исследования в сфере безопасности. — 2022. — Т. 14. — С. 102–115.
3. Смирнов, В.В. Роль банков и операторов связи в борьбе с мошенничеством // Финансовая безопасность. — 2021. — № 2. — С. 45–58.
4. Министерство внутренних дел Российской Федерации. Методические рекомендации по предотвращению телефонного мошенничества. — М., 2023.
5. Официальный сайт Роскомнадзора. Защита персональных данных и предотвращение мошенничества [Электронный ресурс]. — URL: https://rkn.gov.ru (дата обращения: 03.11.2024).