Руденок Василий Петрович
канд. полит. наук, профессор
Магамедрасулова Эмилия Закировна
руководитель
Москаленко Максим Александрович
студент

НОУ ВО «Московский технологический институт»
г. Москва

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЕ МОШЕННИЧЕСТВО В ЦИФРОВУЮ ЭПОХУ: МЕТОДЫ, РИСКИ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Аннотация: *в условиях форсированной цифровизации финансового сектора наблюдается экспоненциальный рост киберпреступности. В статье исследуется проблематика имущественных преступлений, совершаемых дистанционным способом. С применением методов системного анализа и поведенческой психологии рассматривается эволюция мошеннических схем – от классического фишинга до использования нейросетей. Выявлена корреляция между уровнем цифровой грамотности населения и степенью виктимизации. Результатом исследования стала классификация актуальных психологических триггеров, используемых злоумышленниками, а также обоснование необходимости внедрения концепции «нулевого доверия» как базового элемента защиты граждан в информационном пространстве.*

Ключевые слова: *ИТТ-мошенничество, киберпреступность, социальная инженерия, фишинг, вишинг, дипфейки, цифровая гигиена, финансовая грамотность, антифрод-системы, виктимология.*

В последние годы глобальное общество столкнулось с кардинальной трансформацией структуры имущественной преступности. Классические виды хищений стремительно уступают место правонарушениям, совершаемым в вир-

туальной среде. Мошенничество с использованием информационно-телекоммуникационных технологий (ИТТ) превратилось в одну из главных угроз экономической безопасности граждан. Развитие онлайн-банкинга, внедрение электронных государственных услуг и цифровизация торговли создали беспрецедентные удобства для пользователей, но одновременно сформировали обширную базу для криминальных структур.

Фундаментальной проблемой противодействия ИТТ-мошенничеству является смещение фокуса атаки. Современные информационные системы банков обладают высокой степенью криптографической защиты, взломать которые техническим путём крайне сложно. Поэтому преступники выбирают путь наименьшего сопротивления: главным объектом взлома становится сам человек. Этот подход базируется на методах социальной инженерии – комплексе психологических манипуляций, направленных на то, чтобы жертва добровольно передала злоумышленникам конфиденциальные данные (пароли, коды) или самостоятельно осуществила перевод средств.

Системный анализ показывает, что современное ИТТ-преступление состоит из двух компонентов: высокотехнологичной базы (IP-телефония, вредоносное ПО) и глубокого психологического воздействия. Наиболее массовым методом сегодня является вишинг (vishing) – телефонное мошенничество. Используя технологию подмены номера (Caller ID spoofing), злоумышленники добиваются того, что на экране смартфона жертвы высвечивается официальный номер реального банка или правоохранительного ведомства, что создаёт первичный уровень доверия.

Анализ типовых мошеннических скриптов (сценариев разговора операторов криминальных колл-центров) показывает, что психологическое давление базируется на нескольких базовых триггерах. Во-первых, это страх и паника: жертве сообщают о несанкционированном доступе к её счетам или попытке оформления кредита, блокируя рациональное мышление. Во-вторых, создаётся искусственный дефицит времени – человеку не дают возможности остановиться и перезвонить в банк. В-третьих, используется апелляция к авторитету: мо-

шенники представляются «следователями ФСБ» или «специалистами Центробанка», используя строгий тон и специфическую терминологию. Наконец, жертву запугивают уголовной ответственностью за разглашение «тайны следствия», изолируя её от помощи реальных сотрудников банка и родственников.

Помимо вишинга, колоссальную угрозу представляет фишинг (phishing) и взлом аккаунтов в мессенджерах (Telegram, WhatsApp). Преступники рассылают по списку контактов взломанного пользователя сообщения с просьбой срочно одолжить денег или проголосовать в конкурсе по прикреплённой ссылке, ведущей на сайт для кражи учётных данных. Доверие к «знакомому» контакту усыпляет бдительность.

Новым, стремительно развивающимся вектором ИТТ-мошенничества стало применение технологий искусственного интеллекта. Используя нейросети, злоумышленники генерируют дипфейки (deepfakes) – аудио- и видеоподделки. Получив образец голоса жертвы из социальных сетей, алгоритм синтезирует речь с идеальной имитацией интонации. Схема «Fake Boss», при которой сотруднику звонит или пишет голосовые сообщения мнимый «генеральный директор» с требованием срочно перевести средства, уже наносит значительный ущерб бизнесу.

Виктимологические исследования опровергают миф о том, что жертвами мошенников становятся исключительно пожилые люди. Сегодня от социальной инженерии страдают люди с высшим образованием, государственные служащие и IT-специалисты. Это доказывает, что уровень академического интеллекта не защищает от профессиональных манипуляций. Единственным фактором, определяющим уязвимость, является отсутствие специфических навыков цифровой гигиены.

Для эффективного противодействия этой криминальной эпидемии необходим многоуровневый подход. На технологическом уровне требуется внедрение операторами связи и банками продвинутых антифрод-систем (Anti-Fraud), использующих машинное обучение для блокировки подменных номеров и приостановки аномальных транзакций. Однако любые технические решения бес-

сильны, если жертва сама снимает наличные в банкомате и переводит их мошенникам.

Ключевым рубежом обороны является когнитивный уровень. В обществе необходимо сформировать парадигму «нулевого доверия» (Zero Trust) к любым неинициированным контактам в цифровой среде и по телефону. Базовые правила цифровой гигиены должны стать нормой поведения:

− категорический отказ от сообщения кому-либо паролей, CVC-кодов и кодов из SMS, пуш-уведомлений;

− мгновенное прерывание телефонного звонка при первых словах о «подозрительной активности на счёте» и самостоятельный перезвон в банк по официальному номеру;

− обязательное использование двухфакторной аутентификации (2FA) для защиты социальных сетей, мессенджеров и портала государственных услуг;

− критическая проверка любой информации о просьбах финансовой помощи от друзей или родственников путём установления альтернативного канала связи (личный созвон).

Подводя итоги, следует констатировать, что ИТТ-мошенничество представляет собой высокотехнологичную, адаптивную индустрию. Цифровые технологии сами по себе нейтральны, а главным звеном, определяющим надёжность системы информационной безопасности, всегда остаётся человек. Преодоление угрозы кибермошенничества невозможно исключительно техническими или уголовно-правовыми методами; оно требует непрерывного просвещения граждан, развития критического мышления и внедрения культуры безопасного поведения в современном цифровом пространстве.

Список литературы

1. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры / В.С. Овчинский, Э.Г. Жмудь; ред. В.С. Овчинский. – М.: Норма: Инфра-М, 2018. – 352 с.

2. Противодействие мошенничеству в финансовой сфере. – URL: https://www.cbr.ru/information_security/pmp/ (дата обращения: 26.07.2026).

3. Виды мошенничества в интернете и как не стать жертвой. – URL: https://www.kaspersky.ru/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim (дата обращения: 26.07.2026).