УДК 343.72

СОВРЕМЕННЫЕ СПОСОБЫ МОШЕННИЧЕСТВА И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ИМ

Рощин А.С.

магистрант 2 курса юридического института

ФГБОУ ВО «МГУ им. Н.П. Огарёва»

г. Саранск, Россия

Аннотация. В статье рассматриваются актуальные виды мошеннических схем в цифровой и офлайн-среде, анализируются их механизмы, оценивается масштаб ущерба. Представлены современные методы противодействия мошенничеству на уровне государства, финансовых организаций и рядовых пользователей. Обозначены перспективные направления развития систем защиты.

Ключевые слова: мошенничество, киберпреступность, фишинг, социальная инженерия, антифрод-системы, цифровая грамотность.

MODERN METHODS OF FRAUD AND METHODS OF COUNTERING THEM

Roshchin A.S.

2nd year Master's student at the Law Institute

Ogarev Mordovian State University,

Saransk, Russia

Annotation. The article examines the current types of fraudulent schemes in the digital and offline environment, analyzes their mechanisms, and assesses the scale of damage. Modern methods of countering fraud at the level of the state, financial organizations and ordinary users are presented. Promising directions for the development of protection systems are outlined.

Keywords: fraud, cybercrime, phishing, social engineering, anti-fraud systems, digital literacy.

В эпоху стремительной цифровизации мошенничество эволюционировало в высокоорганизованную преступную деятельность, использующую передовые технологии и психологические приёмы. По данным МВД РФ, в 2025 году зарегистрировано свыше 450 тысяч преступлений, связанных с мошенничеством, причём более 40 % из них совершены с применением информационно-коммуникационных технологий [1]. Масштаб ущерба заставляет искать комплексные решения на всех уровнях, от государственного регулирования до личной бдительности граждан.

Современные мошеннические схемы демонстрируют поразительную изобретательность. В киберпространстве доминируют фишинг, фарминг, смишинг и вишинг. Фишинг предполагает рассылку поддельных писем от имени банков или госорганов с целью кражи платёжных данных, например, через имитацию уведомлений о «блокировке счёта» или фальшивые квитанции ЖКХ. Фарминг перенаправляет пользователей на фальшивые сайты через взломанные DNS-серверы, а смишинг использует SMS-сообщения с вредоносными ссылками (например, о «выигрыше»). Вишинг реализуется через телефонные звонки от «сотрудников банка», требующих сообщить CVV-код или перевести деньги на «безопасный счёт».

Особую опасность представляют схемы в социальных сетях и мессенджерах: поддельные аккаунты знаменитостей для сбора пожертвований, сообщения о «друзьях в беде», требующие срочной финансовой помощи, или фейковые розыгрыши с требованием предоплаты за «приз». В финансовой сфере распространены инвестиционные мошенничества, псевдобиржи с гарантированной доходностью и криптоскамы (фальшивые ICO, «майнинг-фермы»), а также кредитные аферы с предложениями «кредитов без проверок» за предоплату. Не теряют

актуальности и офлайн-схемы: «целители», требующие денег за «снятие порчи», автоподставы, обман при купле-продаже с авансами за несуществующие товары и т.д.

Противодействие мошенничеству требует многоуровневого подхода. На государственном уровне ключевую роль играет совершенствование законодательства, ужесточение наказаний по ст. 159 УК РФ и введение ответственности за создание фишинговых ресурсов [2]. Важна координация МВД, Центробанка и операторов связи для оперативного блокирования мошеннических номеров и сайтов, а также международное сотрудничество с правоохранительными органами зарубежных государств.

Технологические решения становятся основой превентивной защиты. Банки внедряют антифрод-системы, анализирующие поведенческие паттерны (время, сумма, место транзакций), используют двухфакторную аутентификацию и блокировку подозрительных операций в реальном времени. Искусственный интеллект помогает выявлять фишинговые письма через NLP-анализ и распознавать голосовой фишинг. Перспективны блокчейн-технологии для верификации транзакций, биометрическая аутентификация (распознавание лица, голоса, отпечатков) и квантовое шифрование.

Не менее значимы образовательные меры. Программы цифровой грамотности в школах и вузах, информационные кампании Центробанка и МВД, тренинги для пенсионеров по безопасному использованию онлайн-банкинга формируют «человеческий щит» против мошенников. Гражданам рекомендуется: не передавать коды из SMS третьим лицам; проверять реквизиты сайтов (HTTPS, доменное имя); использовать сложные пароли и менеджеры паролей; избегать переводов по просьбам из соцсетей без личной верификации; регулярно мониторить выписки по счетам.

Перспективные направления борьбы включают децентрализованные системы идентификации на базе блокчейна и автоматизированные платформы

для подачи заявлений о мошенничестве. Ключевой тренд переход от реактивных методов (расследование совершённых преступлений) к проактивным, основанным на ИИ и анализе больших данных.

Таким образом, эффективность противодействия мошенничеству зависит от синергии правовых, технологических и образовательных мер. Только комплексный подход, сочетающий государственное регулирование, инновации в кибербезопасности и повышение осведомлённости граждан, способен снизить риски в условиях постоянной эволюции преступных схем.

В современном мире мошенничество остаётся одной из наиболее острых проблем, угрожающих как финансовой стабильности, так и психологическому комфорту людей. Стремительное развитие цифровых технологий даёт злоумышленникам всё новые инструменты для обмана, что делает особенно важным формирование у каждого человека навыков осознанного поведения в цифровой среде. Статистика свидетельствует: жертвами мошенников могут стать представители любых возрастных и социальных групп, а общий объём ущерба ежегодно достигает многомиллиардных сумм [3].

Тем не менее существует ряд эффективных способов минимизировать риски попадания в мошеннические схемы. Прежде всего необходимо развивать критическое мышление, умение анализировать информацию, выявлять подозрительные признаки и не поддаваться на эмоциональные манипуляции. Важнейшим правилом становится обязательная проверка любых сомнительных предложений, будь то финансовые операции, сообщения от «знакомых» или уведомления от якобы официальных организаций.

На техническом уровне защита строится на нескольких ключевых принципах: использовании надёжных, уникальных паролей для каждого сервиса, обязательной активации двухфакторной аутентификации и своевременном обновлении программного обеспечения. Эти меры

существенно усложняют злоумышленникам доступ к личным данным и финансовым средствам.

Помимо индивидуальных действий, важную роль играют государственные и корпоративные инициативы по защите граждан. Так, через портал «Госуслуги» доступна функция самозапрета на оформление кредитов, которая эффективно предотвращает мошеннические займы [4]. Операторы мобильной связи внедряют системы фильтрации спам-звонков и подозрительных SMS, снижая вероятность контакта с аферистами.

Дополнительным уровнем защиты может стать страхование от мошенничества. Специальные страховые продукты позволяют частично компенсировать финансовые потери в случае успешной атаки злоумышленников, что особенно актуально при крупных денежных операциях.

Таким образом, эффективная защита от мошенничества складывается из комплекса мер: личной бдительности, технических средств безопасности и институциональных механизмов. Только системный подход, объединяющий индивидуальные навыки и внешние защитные инструменты, способен обеспечить надёжную преграду перед современными мошенническими схемами.

Библиографический список

1. Состояние преступности в Российской Федерации [Электронный ресурс] / МВД Росссии. – URL: https://мвд.рф/reports/item/64450541/ – Режим доступа: сеть Интернет. – Текст : электронный.

2. Российская Федерация. Законы. Уголовный кодекс Российской Федерации: УК: текст с изменениями и дополнениями на 6 апреля 2024 года: [принят Государственной Думой 24 мая 1996 года: одобрен Советом Федерации 5 июня 1996 года]. – Текст: электронный // Консультант Плюс:

[сайт информ.-правовой компании]. – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ – Режим доступа: сеть Интернет. – Текст : электронный.

3. Данилова Е. П. Финансовое мошенничество в современном мире / Е. П. Данилова, Е. М. Портняга // Siberian Socium. 2023. Том 7. № 2 (24). С. 67-97. – Режим доступа: сеть Интернет. – Текст : электронный.

4. Самозапрет на заключение договоров потребительских кредитов (займов) [Электронный ресурс] / Банк России. – URL: https://cbr.ru/ckki/self-prohibition_credit/ – Режим доступа: сеть Интернет. – Текст : электронный.