

Шерстяных А.С.,

кандидат технических наук, доцент

Сибирский юридический институт МВД России (г. Красноярск)

Цифровая виктимология: психологические тактики в современных схемах кибермошенничества

В последнее время все увеличивающаяся скорость внедрения IT-технологий в повседневную жизнь человека является серьезным испытанием не только для новичков в цифровой среде, но и для опытных специалистов. Для России форсированный переход на отечественное программное обеспечение и инфраструктуру, являющийся обязательным государственным требованием, создает дополнительную угрозу кибербезопасности персональных данных в виде потенциальных уязвимостей в новых, недостаточно проверенных решениях. Киберпространство становится новым стратегическим полем, где сталкиваются интересы государства, бизнеса и кибермошенников.

Для усиления мер защиты населения от мошенников, в 2025 году были приняты два федеральных закона. Первый касается создания единой государственной информационной системы противодействия киберпреступлениям¹, второй – создания многофункционального сервиса обмена информацией, который является «...инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения госу-

дарственных и муниципальных функций в электронной форме»².

Введенные законодательные инициативы имеют три основных приоритета: обеспечение целостности и конфиденциальности данных, противодействие цифровому мошенничеству и создание безопасной среды для функционирования цифровых сервисов.

Благодаря значительному повышению эффективности защитных мер в 2025 году, удалось снизить успешность мошеннических атак. Так, в 2024 году каждая 55-я попытка мошенников заканчивалась успехом, в 2025 – лишь каждая 146-я³. Что также подтверждается статистическими данными МВД России: количество преступлений, совершенных в 2025 году с использованием информационно-телекоммуникационных технологий, «...зарегистрировано на 11,8 меньше, чем в 2024 году, в том числе категории тяжких и особо тяжких – на 4,6 %. Количество дистанционных краж снизилось на 23,6 %, дистанционных мошенничеств – на 9 %, а преступлений в сфере компьютерной информации – на 42,2 %»⁴. С другой стороны, общий объем потерь граждан от кибермошенничества продолжает увеличиваться, что указывает на увеличение масштаба и изощренности атак.

1 О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 01.04.2025 №41-ФЗ.

2 О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 24.06.2025 № 156-ФЗ.

3 Какие схемы мошенничества будут распространены в 2026 году и как не потерять свои деньги // финансовый маркетплейс Банки.ру. URL: <https://www.banki.ru/news/daytheme/?id=11020662> (дата обращения: 01.02.2026).

4 Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2025 года // МВД.РФ : официальный сайт. URL: <https://мвд.рф/reports/item/77848182/> (дата обращения: 01.02.2026).

В 2025 году злоумышленники активно использовали несколько распространённых схем, адаптируя их под актуальные события и технологические изменения. Среди наиболее популярных можно выделить следующие.

Имитация сообщений от служб ЖКХ, операторов связи, доставки (почтового отправления и т.п). Мошенники звонят от имени соответствующей службы и просят подтвердить действие, назвав код из СМС (который в процессе диалога мошенники сами и присылают). После получения кода стараются создать у жертвы впечатление, что они передали важную информацию мошенникам и теперь они якобы смогут взломать аккаунт в банке, «Госуслугах» и пр. Целью такого поведения является напугать человека, ввести его в состояние стресса. При этом связь обрывается и почти сразу следует новый звонок (или присылается текстовое сообщение) от лиц, представляющих сотрудниками Роскомнадзора или правоохранительных органов. Они информируют о якобы произошедшем взломе учетной записи на портале «Госуслуг», оформлении на имя жертвы доверенностей или кредитов. В случае текстового сообщения, жертве предлагается самой позвонить на телефон якобы горячей линии «Госуслуг» или Роскомнадзора. И вот тут уже действительно начинается работа мошенников по получению конфиденциальной информации под видом помощи.

По-прежнему у злоумышленников актуальны схемы, связанные с финансовыми махинациями, такие как предложения инвестиций и «быстрого заработка». Жертва, откликнувшись на рекламу высокодоходных вложений, переведя деньги, остается, как правило, ни

с чем. В этой схеме, как правило, используются фишинговые ресурсы, очень похожие по дизайну на настоящие. При этом все чаще используются дипфейки для создания правдоподобных образов государственных или публичных личностей, рекламирующих несуществующие «выгодные предложения».

Отдельного внимания заслуживают целенаправленные атаки на несовершеннолетних. Мошенники могут звонить от имени учителей, завучей или директоров школ под предлогом обновления данных в электронных дневниках. Другой распространенный сценарий – сообщения от «сотрудников военкоматов» или «деканатов» вузов по вопросам медосмотра, поступления или сдачи экзаменов. Целью таких обращений является получение персональных данных подростков или денежных средств от них или их родителей.

Параллельно сохраняют актуальность традиционные, но оттого не менее эффективные методы: массовые рассылки фишинговых писем от имени банков и госорганов, а также создание фальшивых сайтов, например, для оплаты якобы выписанных штрафов за нарушение ПДД.

Ключевыми признаками, указывающими на мошеннический характер общения, остаются: создание искусственной спешки и давления, чтобы не дать время жертве спокойно обдумать ситуацию; стремление перевести диалог из официальных каналов в мессенджеры; потребовать произвести перевод необычным способом – в криптовалюте, по заранее подготовленным фишинговым ссылкам, на карту физического лица и пр.