

Секция «Инновации в государственном управлении на современном этапе»

Спецкнопка: инновационное решение в борьбе с кибермошенничеством

Научный руководитель – Мельник Сергей Васильевич

Понтелеева Мария Александровна

Студент (специалист)

Орловский юридический институт МВД России имени В. В. Лукьянова, Факультет
подготовки следователей, Орел, Россия

E-mail: mariaponteleeva@icloud.com

По банковской отчетности за 2024 год мошенники похитили у граждан более 27,5 млрд рублей, из которых только 1,2 млрд рублей похищено со счетов юридических лиц, вся остальная сумма – со счетов физических лиц. По сравнению с 2023 годом, сумма увеличилась на 74,4% [1].

Наиболее распространенным видом кибермошенничества является использование вредоносного вируса с удаленным доступом, который устанавливается на устройства жертв злоумышленников под видом безвредных приложений, а на самом деле собирает все необходимые данные, которые помогут для осуществления переводов денежных средств на счета мошенников.

Согласно опросам, проводимым Центральным банком (далее по тексту – ЦБ) России, только третья часть всех пострадавших фактически обращаются в банк или правоохранительные органы [2]. Остальные не считают нужным этого делать в силу отсутствия смысла, а также затруднительности самой процедуры обращения и получения юридической помощи. Для этого сперва необходимо предоставить факты совершения мошенничества: следует сохранить всю переписку, а также собрать платёжные документы. Далее либо непосредственно через обращение в отделение полиции или банка, либо онлайн подать заявление, введя при этом необходимые данные, и предоставить доказательства мошенничества.

По нашему мнению, основной же причиной преступности в банковской сфере является слабая система безопасности данных граждан. Именно поэтому денежные средства являются частым объектом посягательства мошенников. В современных реалиях активно развиваются дистанционные услуги, в т.ч. по обслуживанию банками своими клиентов. Прослеживается тенденция увеличения случаев кибермошенничества, можно сказать, что оно «идет в гору».

Уголовное законодательство содержит правовые нормы, которые включает в себя составы преступлений касаясь сферы мошенничества, ключевым из которых является хищение денежных средств со счетов посредством использования современных компьютерных программ, которые позволяют преступникам осуществлять свою незаконную деятельность дистанционно, получая доступ ко всем сведениям граждан.

Связи с цифровой трансформацией общества не только законопослушные граждане имеют возможность использовать в своей жизни искусственный интеллект, но и злоумышленники. Остается неизменным и использование ими методов социальной инженерии – психологического воздействия на жертв путем принуждения их к переводу денежных средств или предоставления необходимых личных данных для незаконных целей. Уязвимыми участниками данных правоотношений по-прежнему являются пожилые люди, которые в основном отдалены от современных тенденций развития общества. Однако Банк России составил портрет пострадавшего от кибермошенников в 2024 году – ими оказались женщины в возрасте от 25 до 44 лет, которые, как правило, являются городскими жительницами [3].

Актуальность данной проблемы также объясняется тем, что рост случаев мошенничества в банковской сфере влечет за собой недоверие граждан к банковским организациям и их деятельности, что впоследствии может привести к возможности дестабилизации всей финансовой системы России.

В июле 2024 года была предложена идея о приостановлении выдачи кредитов в случае, если возникла угроза или предположение об участии мошенников в данной операции. Данное преобразование коснулось также осуществления переводов со счетов.

В текущий момент времени само государство, а также банковские организации заинтересованы в борьбе с данным видом преступлений. Помимо установленной Уголовным кодексом РФ ответственности, а также размещенной на сайтах российских банков информации об угрозах и способах мошенничества для предостережения граждан от возможности совершения ошибок, 19 февраля 2025 года Председатель ЦБ РФ Эльвира Набиуллина на форуме «Кибербезопасность в финансах» обратила свое внимание на возможность введения в октябре текущего года «спецкнопки» в мобильных приложениях российских банков. С ее помощью можно будет сообщать о случаях мошенничества, в том числе ответить на запрос из МВД о факте преступления.

Для упрощения процедуры подачи заявления в банк была создана специальная кнопка, встроенная в мобильное приложение банка, которая позволяет путем ее нажатия сообщить банк о посягательстве на денежные средства предполагаемой жертвы. В приложении также можно будет получить необходимую информацию о том, как обратиться в полицию с тем же обращением. В том числе и сам банк клиента пришлет ему запрос о совершенной операции, чтобы подтвердить является или не является она мошеннической. Данное нововведение ожидает, в первую очередь, крупные банки, которые играют немаловажную роль в финансовой системе нашей страны. «Спецкнопка» будет способствовать:

- Упрощению самой процедуры подачи заявлений на злоумышленника;
- Изменению процесса сбора документов для сообщения о мошенничестве в правоохранительные органы (без посещения отделения полиции);
- Обеспечению увеличения данных обращений, что, в свою очередь, увеличит показатели раскрытия случаев мошенничества, а также непосредственно сократит случаи нераскрытия данного вида преступления;
- Блокированию счета злоумышленника, на который были переведены денежные средства клиента банка.

Касаемо механизма работы «спецкнопки», банки обязаны в том числе предостеречь клиентов от случайного нажатия, например, требовать неоднократного подтверждения обращения в случае угрозы мошенничества через всплывающее окно. Кроме того могут возникнуть случаи, когда гражданин специально пожалуется на какого-либо другого человека, который ни в чем не виноват, но в силу личной неприязни пострадает. Данный момент нужно урегулировать, например, путем установления ответственности за необоснованное сообщение о факте мошенничества.

Источники и литература

- 1) Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций [Электронный ресурс]. https://cbr.ru/analytics/ib/operations_survey/2024/
- 2) Портрет пострадавшего от кибермошенников в 2024 году [Электронный ресурс]. <https://cbr.ru/press/event/?id=23367>

- 3) ЦБ обяжет крупные банки создать «спецкнопки» для жалоб на мошенников [Электронный ресурс]. <https://rbc-ru.turbopages.org/rbc.ru/s/finances/19/02/2025/67b597b39a79474831535e80>