Секция «Уголовное право и криминология, уголовно-исполнительное право»

Актуальные вопросы противодействия мошенничествам, совершаемым с использованием методики социальной инженерии

Научный руководитель – Вихляев Александр Александрович

Трофимов Егор Алексеевич
Студент (специалист)
Московский университет Министерства внутренних дел Российской Федерации, Факультет подготовки сотрудников полиции по охране общественного порядка, Москва, Россия
E-mail: egorfootbol99@mail.ru

В условиях современных экономических преобразований процесс цифровой трансформации поглотил многие сферы общественных отношений. Банковская сфера не стала исключением.

Государственными и частными банками активно пропагандируется использование сервисов, позволяющих совершать многочисленные финансовые операции удаленно с использованием смартфонов, мессенджеров и информационно-телекоммуникационной сети Интернет (дистанционное банковское обслуживание).

Наибольшую популярность указанные сервисы в нашей стране, как и во всем мире, приобрели в период карантинных мер, вызванных пандемией коронавирусной инфекции нового типа (COVID-19), что, в свою очередь, повлияло на рост мошеннических действий.

Объем всех операций, совершенных мошенническим путем в банковской сфере к 2020 году составлял 5 723,5 млн. рублей, а их количество - 571 957 случаев.

В первом полугодии 2020 года, в период активной фазы пандемии, количество противоправных действий в сфере дистанционного банковского обслуживания, совершенных мошенническим путем, превысило показатели предыдущего года за аналогичный период на 35%. Общая сумма материального ущерба составила 1 287 млн. рублей. При этом, примерно 70% мошеннических действий совершались с использованием методики социальной инженерии.

Под социальной инженерией понимается метод получения необходимого доступа к информации или персональным данным граждан, основанный на особенностях психологии людей.

Выделим основные факторы, влияющие на распространение указанного вида мошенничества:

1) социальная инженерия не требует от злоумышленников каких-либо специальных познаний в технике, а также больших финансовых затрат при подготовке к противоправным действиям, либо непосредственно при их совершении;

2) доступность персональных данных граждан, с помощью которых мошенники входят в доверие и предрасполагают к себе (при этом одну информацию злоумышленники могут получить в открытом доступе (например, в социальных сетях, на сайтах знакомств); другую - в следствие нарушений условий конфиденциальности как самими пользователями информационных ресурсов, так и со стороны персонала различных компаний и организаций кредитно-банковской сферы);

3) низкая финансовая и техническая грамотность населения, позволяющая вводить жертв в заблуждение и получать доступ к их персональным аккаунтам мобильных банков.

Другими словами, мошеннику проще совершить звонок возможной жертве и получить необходимый доступ к денежным средствам с помощью нее, чем разрабатывать какое-

либо вредоносное программное обеспечение с целью взлома финансовых систем, защита которых в данный момент осуществляется на высоком уровне.

Проведенный анализ позволяет сделать вывод, что вопрос противодействия мошенничеству с использованием социальной инженерии в настоящее время стоит наиболее остро.

При этом банковские организации не располагают реальными возможностями фактически контролировать действия клиентов, которые, подвергаясь манипулированию со стороны мошенников, сами отдают свои деньги злоумышленникам.

Отметим одну из наиболее распространенных схем мошеннических действий с использованием методов социальной инженерии, по которой злоумышленник, связываясь с пользователем онлайн-банкинга, используя фишинг-методику, сообщает, что по его счетам производится подозрительная операция, которую сама жертва противоправных действий фактически не осуществляла, и, как результат, запугивая ее, получает от нее все необходимые для снятия денежных средств сведения (номер банковской карты, CVV2/CVC2 код, кодовые слов или образец голоса). Для совершения противоправных действий могут также использоваться подставные копии популярных сайтов либо SMS-сообщений с номеров, внешне схожих с номерами, используемыми кредитными организациями (например, создание реплики номера Сбербанка «900» путем внесения в реестр буквенных символов OO вместо цифрового ряда - «9OO»).

Выделим наиболее приоритетные способы противодействия мошенническим действиям, совершаемым с использованием методов социальной инженерии, к которым можно отнести:

1) повышение финансовой и технической грамотности населения в части основных используемых им финансовых технологий, применяя для этого все доступные каналы коммуникации;

2) развитие, распространение и широкое внедрение антифрод-систем, позволяющих оценивать финансовые транзакции на предмет возможного мошенничества;

3) жесткий контроль в области использования субъектами финансовых отношений персональных данных клиентов с исключением возможности их утечки «на сторону»;

4) совершенствование нормативно-правового регулирования [1] в сфере информационной безопасности, в частности, - принятие закона, позволяющего Банку России во взаимодействии с Роскомнадзором производить внесудебную блокировку мошеннических (фишинговых) сайтов.

Предложенные пути по противодействию методике социальной инженерии не являются исчерпывающими, однако их реализация, доработка и доступность в краткосрочной перспективе позволят осуществлять действенную профилактику мошенничеств в условиях проводимой государством политики цифровизации общественных отношений.

Источники и литература

1) Мартыненко Н.Н., Овчаренко А.В. Мошенничество в сфере дистанционного банковского обслуживания и методы борьбы с ним в условиях пандемии // Инновации и инвестиции. 2020. №12.

2) Система обеспечения законодательной деятельности. Законопроект № 605945-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации» [Электронный ресурс]. – URL: https://sozd.duma.gov.ru/bill/605945-7 (дата обращения 01.03.2021)