DOI 10.58351/2949-2041.2023.3.3.008

Васильева Анна Валентиновна,
магистрант 3 курса Юридического факультета,
Санкт-Петербургского института (филиала)
ВГУЮ (РПА Минюста России)

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ, АКТУАЛЬНЫЕ ВОПРОСЫ ПРЕДУПРЕЖДЕНИЯ ПРАВОНАРУШЕНИЙ

Аннотация: статья посвящена новым видам мошенничества с использованием информационных технологий. Рассмотрены актуальные технические и законодательные новации по предупреждению данных видов правонарушений. Вынесены предложения по дальнейшему совершенствованию законодательства и профилактике мошенничества.

Ключевые слова: мошенничество; фишинг; дипфейк; киберпреступность, антифрод.

Abstract: the article is devoted to new types of fraud using information technology. The current technical and legislative innovations on the prevention of these types of offenses are considered. Proposals were made for further improvement of legislation and fraud prevention.

Keywords: fraud, phishing, deepfake, cybercrime, anti-fraud.

В XXI веке с бурным развитием информационных технологий появляются все новые и новые виды преступлений.

Погруженность в информационное пространство современного общества представляет собой интеграцию повседневной жизни человечества с новейшими цифровыми технологиями С одной стороны - глобально люди сегодня подчиняются информационному пространству и транслируемому им контенту. [1] С другой стороны – граждане по причинам возраста, или каким-либо иным, не разбираются в технологиях и не вовлечены в глобальную сеть, но обладают современными средствами связи, владеют банковскими счетами и привязанными к ним картами и, таким образом, являются потенциальными жертвами преступников.

Вышеуказанные факторы способствовали развитию и появлению различных видов мошенничества.

Перечислим и кратко опишем самые распространенные на сегодняшний день и (или) представляющие наибольшую опасность:

- телефонные (реже через мессенджеры) звонки, мошенники представляются работниками банков (сотрудниками правоохранительных органов и т.п.). Суть данных манипуляций заключается в склонении граждан к денежным переводам на банковскую карту злоумышленников. Особенно подвержены данному виду мошенничества пожилые граждане;

- фишинг - завладевание персональными данными с помощью рассылок: СМС, электронная почта, мессенджер-рассылки с вредоносными ссылками, использование поддельных VPN-сервисов. Голосовой фишинг, или вишинг (vishing) предполагает разговор по телефону. Одна из вариаций почтового фишинга — клон-фишинг. Мошенники определяют, какими программами и магазинами пользуется жертва, а затем отправляют письма якобы от этих брендов. В смишинге (smishing) вместо звонков используют СМС-сообщения с вредоносными ссылками, которые маскируют под купоны и розыгрыши. Фишинг представляет собой одну из разновидностей социальной инженерии, которая базируется на незнании пользователями основ сетевой безопасности. [2]

- фарминг– нарушение навигационной структуры браузера с целью скрытного перенаправления жертвы на ложный IP-адрес для завладевания её персональными данными о логинах и паролях;

- дипфейк – новая технология генерации поддельного видео и аудио контента;

- взламывание страниц в социальных сетях и аккаунтов в мессенджерах.

Основными проблемами профилактики и раскрытия преступлений в сфере информационных технологий являются:

- высокая латентность;
- технические и интеллектуальные возможности мошенников,
- свободный доступ и анонимность пользователя в сети Интернет,
- широкая аудитория и скорость реагирования,
- недостаточная квалификация специалистов в правоохранительных органах;
- отсутствие на данный момент законодательной поддержки пострадавших граждан.

Правительством Российской Федерации и IT- организациями в последние годы были предприняты следующие инициативы, направленные на профилактику и минимизацию последствий данных видов преступлений.

1. В начале года 2023 Роскомнадзор запустил платформу для борьбы с телефонным мошенничеством и для блокировки звонков и СМС-сообщений с подменных номеров под названием «Антифрод». Разработкой и внедрением системы на базе площадок операторов связи занимались специалисты ГРЧЦ Главного радиочастотного центра.

Единая платформа верификации телефонных вызовов (ЕПВВ) «Антифрод» обрабатывает информацию об абонентских номерах и уникальных кодах идентификации абонентов, инициирующих вызовы (включая звонки, СМС, передачу голосовых сообщений), информацию о номерах абонентов, которым поступил вызов; информацию о дополнительных номерах, используемых при переадресации соединений, данные о дате и времени установления соединения, информацию о сетях связи, задействованных при пропуске трафика,

К платформе подключены четыре основных оператора связи — «Мегафон», «МТС», «Билайн» и Tele2. Платформа «Антифрод» с момента запуска заблокировала 135 млн звонков с подменных номеров.

Система «Антифрод» состоит из центрального узла, узлов верификации и узлов взаимодействия. За центральный узел и узлы взаимодействия отвечают напрямую специалисты ГРЧЦ. Узлы верификации подключаются непосредственно к операторам связи. Создавать и эксплуатировать эту часть системы будут сами операторы. ГРЧЦ будет потом обслуживать их удалённо. Каналы связи между узлами системы обеспечивает Роскомнадзор. Ведомство также будет хранить и анализировать информацию о соединениях, получая её от операторов. Штраф за пропуск вызовов с подменных номеров составит около 500 тыс. рублей.

Телефонные мошенники с начала года начали менять номера мобильных телефонов на международные для обхода систем блокировок операторов связи и платформы «Антифрод» от Роскомнадзора. Представители операторов связи рассказали СМИ, что российским пользователям стали чаще поступать нежелательные звонки с номеров, использующих коды Японии, Кореи, Казахстана, Турции и Лихтенштейна. Злоумышленники адаптировались под новые блокировки и начали систематически звонить пользователям через визуально схожие с российскими номерами телефонов наборы цифр, полученные через зарубежных провайдеров связи.

«В настоящий момент к системе подключились четыре крупных оператора. До конца этого года планируется подключение всех оставшихся операторов телефонной связи в России. Порядка 90% вызовов должно быть верифицировано». Планируется, что после этого подключения к системе «Антифрод» всех операторов связи подменить номер в России будет невозможно технологически. [5]

2. Группа исследователей из Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета создала модель графовой нейронной сети, которая способна отличать подозрительные транзакции от безопасных, а мошенников — от честных пользователей.

Для создания новой модели учёные проанализировали сотни транзакций и подробную информацию о них, начиная с номера операции и заканчивая типом устройства, с которого

производился перевод. В частности, банковские операции и пользователей представили в виде графов, а затем разделили их на мошенников и людей, которые осуществляют легитимные денежные переводы.

Модель ориентирована на решение проблемы больших объёмов данных о транзакциях, повышение скорости анализа операций на предмет безопасности и обнаружение новых способов банковского мошенничества. Графовая нейронная сеть также справится с выявлением в социальных сетях пользователей, распространяющих дезинформацию, или с обнаружением сетевых атак в сетях передачи данных, считают ученые. [7]

3. Российские программисты разработали приложение, способное распознавать мошенников в самом начале телефонной беседы. После того, как разработка вычисляет злоумышленников, она предупреждает об этом пользователя, а если тот не обращает внимания и продолжает общение, программа прерывает звонок самостоятельно.

Помимо этого, в систему входят и другие модули, которые проверяют переписку и обнаруживают странности в дизайне сайтов.

«Приложение определяет, что диалог мошеннический, на первых этапах разговора. Например, если скрипт злоумышленника рассчитан на одну минуту, детектирование произойдет примерно на 20-й секунде разговора. Ожидаемая эффективность работы программы - 90%, как показала аналитика проведенных исследований».

Второй модуль - для выявления мошенников по переписке - будет действовать таким же образом, но минуя стадию перевода разговора в текст. Помимо этого, программисты намереваются дополнить систему методами анализа фишингового контента с помощью искусственного интеллекта. Третий модуль будет заниматься анализом дизайна сайтов на вредоносность. [4]

4. МВД заключило контракт на научную разработку способов борьбы с дипфейками. Она получила шифр «Зеркало (Верблюд)». Это следует из данных в системе госзакупок. Результат должен быть уже в 2023 году. Победителем тендера стала научно-промышленная компания «Высокие технологии и стратегические системы». Исполнителю заказа предстоит исследовать возможные способы выявления внутрикадрового монтажа в роликах, который сделан с помощью нейронных сетей. [3]

5. Принята разработанная на основании поручения Президента РФ В. В. Путина Стратегия развития информационного общества до 2030 г., отражающая необходимость повышения безопасности информационной сферы на основе популяризации ресурсов, способствующих распространению традиционных духовно-нравственных ценностей. [8]

6. Банк России ведет работу по выявлению мошеннических схем, информирует о них правоохранительные органы, которые занимаются расследованием хищений денежных средств. [9]

7. Президент Владимир Путин поручил правительству совместно с Банком России до 1 июля 2023 рассмотреть возможность создания механизма выплаты банками и кредитными организациями компенсаций гражданам, у которых мошенники украли деньги со счетов. Об этом говорится в одном из поручений, сформулированных после заседания Совета по развитию гражданского общества и правам человека 7 декабря 2022 года. Перечень поручений опубликован на сайте Кремля.

"Правительству Российской Федерации совместно с Банком России рассмотреть вопрос о создании механизма выплаты банками и иными кредитными организациями компенсаций клиентам, денежные средства которых были похищены в результате мошеннических действий, и при необходимости представить предложения по внесению соответствующих изменений в законодательство РФ", - говорится в документе. Создан Законопроект № 197920-8 об обязанности банков и операторов по переводу средств возмещать клиентам деньги, которые сняли с их счетов мошенники, в сентябре внес в Госдуму председатель думского комитета по финансовому рынку Анатолий Аксаков. Для переводов внутри России компенсация должна быть выплачена за 30 дней, для трансграничных - за 60 дней.

Как говорится в пояснительной записке, предлагается обязать не только банк плательщика, как это установлено сейчас, но и банк получателя средств проверять операции на признаки мошенничества, включая сверку с базой данных о случаях и попытках переводов денежных средств без согласия клиента, которую ведет Банк России. Кроме того, предлагается предоставить банкам право не принимать к исполнению распоряжения по явно мошенническим операциям в течение двух дней, даже несмотря на согласие клиента. [6]

Выводы и предложения:

Если обратиться к вопросу законодательного регулирования ответственности за мошенничество, то надо вспомнить о том, что дискуссионным является вопрос о необходимости дальнейших внесений в Уголовный кодекс уточнений, конкретизирующих ответственность за различные виды мошенничества. По нашему мнению, не следует дифференцировать ответственность исходя из сферы совершения преступления, применяя общую норму для всех видов правонарушений, связанных с хищением чужого имущества или приобретением права на чужое имущество путем обмана или злоупотребления доверием. Если идти по пути дальнейшей дифференциации, ближайшие годы и десятилетия с развитием технологий и появлением все новых и новых видов мошенничества придется регулярно менять уголовный закон. Также следует обратить внимание на проблемы квалификации преступлений следователями, прокурорами и судами на местах.

Необходимо активизировать работу правоохранительных органов с гражданами, используя средства массовой информации. Производить наглядные социальные ролики и демонстрировать их на телевидении, также на радиоканалах делать регулярные объявления, публиковать статьи в газетах и журналах, предназначенных для пожилых людей, печатать и размещать плакаты с предупреждающей информацией, привлекающей внимание фокусной аудитории граждан.

Жестким, но эффективным методом профилактики преступлений может быть регистрация в сети интернет в целом, и также в социальных сетях, в частности, по паспорту, с присвоением личного кода и дальнейшей возможности отслеживания по данному коду всех действий гражданина.

Важнейшими в борьбе с данным видом правонарушений, безусловно, являются технические методы. Следует более активно совершенствовать технологии, повышать степень зашиты информации в банковских сервисах, обновлять и поддерживать на соответствующем уровне техническую базу в правоохранительных органах, внедрять на законодательном уровне разработанные новации.

Список литературы:

1. Ордоков М.Х., Карданова Д.А. О способах совершения мошенничеств в глобальном информационном пространстве // «Журнал прикладных исследований». - 2021. - № 4-1. - С.93-97.

2. Табак И.С. Мошенничество с банковскими картами // Современные инновации. 2018. № 5. С. 33.

3. Открытый конкурс в электронной форме. № 0373100088721000002. Выполнение научно-исследовательской работы «Исследование возможных способов выявления признаков внутрикадрового монтажа видеоизображений, выполненного с помощью нейронных сетей». Шифр «Зеркало (Верблюд)» (в рамках ГОЗ) // [Электронный ресурс] Официальный сайт государственных закупок РФ. URL: https://zakupki.gov.ru/epz/order/notice/ok504/view/event-journal.html?regNumber=0373100088721000002 (дата обращения: 05.01.2023).

4. Специальная инженерия: нейросеть опознает мошенника во время разговора. Как искусственный интеллект научили отличать звонки, сообщения и сайты злоумышленников. // [Электронный ресурс] Официальный сайт газеты «Известия». URL: https://iz.ru/1192463/olga-kolentcova/spetcialnaia-inzheneriia-neiroset-opoznaet-moshennika-vo-vremia-razgovora (дата обращения: 10.04.2023).

5. Система Роскомнадзора "Антифрод" заблокировала 135 млн звонков с подменных номеров. // [Электронный ресурс] Официальный сайт Интерфакс. URL: https://www.interfax.ru/russia/895801 (дата обращения: 10.05.2023).
6. Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека // [Электронный ресурс] Официальный сайт Президента РФ. URL: http://www.kremlin.ru/acts/assignments/orders/copy/70349 (дата обращения: 15.01.2023).
7. Ученые Политеха Петра Великого научили нейросеть бороться с мошенничеством в интернете. // [Электронный ресурс] Официальный сайт Правительства Санкт-Петербурга Комитет по науке и высшей школе. URL: http://knvsh.gov.spb.ru/news/view/5684/ (дата обращения: 10.05.2023).
8. Указ Президента РФ от 9 мая 2017 г. № 203 “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы” // [Электронный ресурс] https://www.garant.ru/products/ipo/prime/doc/71570570/ (дата обращения: 05.01.2023).
9. Информационная безопасность. Противодействие мошенническим практикам/ [Электронный ресурс] Официальный сайт Центрального банка Российской Федерации URL: https://cbr.ru/information_security/pmp/ (дата обращения: 05.01.2023).