и обработки сведений о состоянии здоровья и диагнозах граждан». URL: http://publication.pravo.gov.ru

6. Скрипкин Ю. К., Мордовцева В. Н. Кожные и венерические болезни: рук. для врачей. Т. 2. М., 1999. С. 24–30.

7. Кванина В. В., Громова Е. А., Спиридонова А. В. К вопросу о системе принципов предпринимательского права // Бизнес, менеджмент и право. 2018. № 4. С. 18–21. EDN: XWHGMX.

8. Mayba J., Gooderham M. J. Review of atopic dermatitis and topical therapies // J Cutan Med Surg. 2017. Vol. 21, № 3. Pp. 227–236.

З. М. Бешукова,
доктор юридических наук, доцент,
Адыгейский государственный университет

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: МЕХАНИЗМ СОВЕРШЕНИЯ И ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ

Аннотация. В статье рассматриваются наиболее популярные и распространенные схемы мошенничества с использованием методов социальной инженерии. Определен механизм совершения данного вида преступлений, который включает четыре этапа: подготовка, проникновение, эксплуатация и отключение. Сформулированы рекомендации, которые могут быть использованы в целях повышения эффективности профилактики мошенничества с использованием методов социальной инженерии.

Ключевые слова: мошенничество, социальная инженерия, телефонное мошенничество, предупреждение, профилактика, фишинг, смишинг, вишинг, претекстирование

FRAUD USING SOCIAL ENGINEERING METHODS: MECHANISM OF COMMITMENT AND BASIC METHODS OF PROTECTION

Abstract. The article discusses the most popular and widespread fraud schemes using social engineering methods. The mechanism for committing this type of crime has been determined, which includes four stages: preparation, penetration, exploitation and shutdown. Recommendations are formulated that can be used to increase the effectiveness of fraud prevention using social engineering methods.

Keywords: fraud, social engineering, telephone fraud, warning, prevention, phishing, smishing, vishing, pretexting

Введение. В последние годы наблюдается значительный рост телефонного мошенничества, которое реализуется методами социальной инженерии.

В 2022 г. по официальной информации Центрального банка РФ российские граждане в результате телефонного мошенничества потеряли 14,2 млрд рублей [1].

При этом кредитными организациями жертвам данного вида преступлений было возвращено всего 4,4 % от похищенных средств, или 618,4 млн руб. Приведем аналогичные данные из обзора Центрального банка России об инцидентах информационной безопасности при переводе денежных средств за предыдущие годы. В 2021 г. жертвам было возмещено 6,8 % от похищенных средств, или 920,5 млн руб., в 2020 г. – 11,3 %, или 1,1 млрд руб., в 2019 г. – 15 %, или 935 млн руб. Как видим, самый низкий уровень возмещения денежных средств жертвам мошенничества приходится на 2022 г. Это является следствием высокой доли мошенничества, реализуемого методами социальной инженерии, т. е. когда граждане самостоятельно осуществляют переводы денежных средств преступникам или раскрывают конфиденциальную информацию [2].

В связи с этим особую актуальность приобретает анализ механизма совершения мошенничества с использованием методов социальной инженерии, а также проблема определения возможных способов защиты от него.

Основная часть. В настоящее время наиболее популярными и распространенными схемами мошенничества с использованием методов социальной инженерии являются:

1. Фишинг и смишинг. Суть фишинга заключается в использовании преступниками электронных писем и сообщений в социальных сетях с важной информацией. Смишинг предполагает использование текстовых сообщений (SMS-сообщений) в качестве механизма доставки для запуска эксплойта. Важно отметить, что текстовые сообщения имеют более высокий уровень открываемости, чем электронная почта, поэтому этот метод используется преступниками очень активно.

2. Вишинг ((от англ. «voice» и «phishing»), иными словами, голосовой фишинг) – это телефонный эквивалент фишинга. Вишинг представляет собой метод, произошедший от фрикинга, который был широко распространен в эпоху до появления сети «Интернет». Используя эту технику, преступники манипулируют жертвами в процессе телефонного разговора. При этом им порой удается усыпить бдительность даже самого внимательного человека.

Мошеннические схемы подвергаются регулярному обновлению. Например, после того как словосочетание «Здравствуйте, звонок из службы безопасности» фактически превратилось в мем (преступники часто представлялись сотрудниками банка), жертвы стали получать звонки от «представителей» других учреждений. Из последних трендов – звонки от имени федеральных министров. В контексте этого, важно отметить, что преступники практически всегда обладают так называемыми установочными данными, т. е. они владеют достоверной информацией о фамилии, имени, отчестве жертвы, месте ее работы, роде профессиональной деятельности, наличии ученой степени и др. Например, в 2023 г. жертвами мошенников стали преподаватели ВУЗов, которым преступники звонили в мессенджерах от имени ректоров, кураторов из Минобрнауки РФ и т. д.[3].

3. Использование претекста. Претекстирование включает в себя изощренную имитацию надежного источника или создание сфабрикованного сценария с единственной целью убедить жертву выполнить определенное действие. Преступники часто выбирают комбинацию цифр номера телефона, электронной почты, текстовых сообщений или социальных сетей, чтобы завоевать доверие жертвы.

Что же такое социальная инженерия? В первую очередь необходимо отметить, что целью настоящего исследования не является выработка определения данного термина. В связи с этим отметим только то, что в специальной литературе имеются различные определения понятия «социальная инженерия». В настоящем исследовании социальная инженерия понимается как манипулятивное воздействие на психику с целью совершения жертвами определенных действий или разглашения конфиденциальной информации, в том числе с использованием современных информационных технологий.

Мошенничество с использованием методов социальной инженерии происходит в основном в четыре этапа:

1. Подготовка. Преступник, как было отмечено ранее, всегда заблаговременно собирает информацию о жертве различными способами (через социальные сети; открытые данные, размещенные на сайтах различных организаций и учреждений; даркнет или другие источники).

2. Проникновение. Преступник «приближается» к жертве, обычно маскируясь под доверенные контакты или представителей органов власти, и использует при этом информацию, собранную о ней, чтобы завоевать доверие.

3. Эксплуатация. Преступник «убеждает» жертву предоставить ему конфиденциальную информацию, которую он использует для достижения своей преступной цели.

4. Отключение. Преступник прекращает общение с жертвой, осуществляет вредоносную деятельность и исчезает.

В связи с этим возникает вопрос, что необходимо сделать, чтобы люди не верили мошенникам? К основным способам защиты от мошенничества с использованием методов социальной инженерии относится предупредительная деятельность, которая должна включать в себя:

– повышение уровня осведомленности населения об особенностях мошеннических схем, о функционировании тех или иных финансовых механизмов, как и финансовой грамотности в целом [4. С. 357–361];

– специальное обучение вопросам информационной безопасности, позволяющее выработать у населения навыки безопасного поведения в различных ситуациях. Именно такая задача должна быть поставлена перед всеми субъектами профилактики правонарушений [4. С. 357–361];

– использование лицензионного антивирусного программного обеспечения и регулярное его обновление.

Заключение. Аккумулируя все ранее изложенное, можно сделать вывод, что эффективное противодействие мошенничеству с использованием методов социальной инженерии возможно только при использовании комплексного подхода. Причем ключевую роль в борьбе с мошенничеством играет именно критическое мышление потенциальной жертвы.

Список литературы

1. Бевза Д. В 2022 году телефонные мошенники похитили более 14 млрд рублей. URL: https://rg.ru/2023/03/03/v-2022-godu-telefonnye-moshenniki-pohitili-bolee-14-mlrd-rublej.html

2. Россияне сдали мошенникам рекордные 14 млрд. URL: https://www.rbc.ru/newspaper/2023/02/15/63eb5da89a794701b759621f

3. Медведева О., Тихонова Н. Телефонные мошенники переключились на медиков и преподавателей вузов. URL: https://rg.ru/2023/09/13/rektor-nikomu-ne-pishet.html

4. Трахов А. И., Бешукова З. М. Предупреждение телефонного мошенничества: российский и зарубежный опыт // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. Казань: Изд-во «Познание» Казанского инновационного университета, 2022. С. 357–361.

А. Л. Бурова,
помощник судьи,
Восемнадцатый арбитражный апелляционный суд

ПРАВОВОЙ СТАТУС ПРОЕКТА СУДЕБНОГО АКТА АРБИТРАЖНОГО СУДА, ПОДГОТОВЛЕННОГО ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Аннотация. Цель работы состоит в исследовании актуальных проблем и перспектив правового статуса проекта судебного акта арбитражного суда, созданного искусственным интеллектом. Анализируется правовой статус проекта судебного акта арбитражного суда, подготовленного помощником судьи, представленного стороной арбитражного процесса, а также созданного искусственным интеллектом. В заключении приводится вывод о необходимости внесения изменений в Арбитражный процессуальный кодекс Российской Федерации и Инструкцию по делопроизводству в арбитражных судах Российской Федерации в целях закрепления правового статуса проекта судебного акта, разработанного искусственным интеллектом.

Ключевые слова: судья, арбитражный суд, арбитражное судопроизводство, электронное правосудие, искусственный интеллект, системы на основе искусственного интеллекта, проект судебного акта

LEGAL STATUS OF THE DRAFT JUDICIAL ACT OF THE ARBITRATION COURT PREPARED BY ARTIFICIAL INTELLIGENCE

Abstract. The purpose of the work is to study the current problems and prospects of the legal status of the draft judicial act of the arbitration court created by artificial intelligence. The legal status of the draft judicial act of the arbitration court, prepared by an assistant judge, submitted by a party to the arbitration process, as well as created by artificial intelligence, is analyzed. In conclusion, it is concluded that it is necessary to amend the Arbitration Procedural Code of the Russian Federation and the Instructions on Office Work in the arbitration courts of the Russian Federation in order to consolidate the legal status of the draft judicial act developed by artificial intelligence.