УДК 343. 3/.7

А. А. Блинов, А. А. Чичендаева
Кузбасский государственный технический университет им. Т.Ф. Горбачева, Кемерово, Россия

ФИШИНГ КАК НОВЫЙ СПОСОБ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

научный руководитель: к.п.н, доцент кафедры Истории, философии и социальных наук Съедина Н.В.

В статье рассматриваются вопросы относительно новых способов совершения мошенничества в сфере компьютерной информации, в частности фишинг, затронут анализ статистических данных применительно к существующим киберугрозам, раскрыта сущностная характеристика внедрения цифровых технологий в процесс производства и управления, а также в жизнь общества.

Ключевые слова: мошенничество, компьютерная информация, фишинг, информационные технологии, средства массовой информации.

С развитием информационных технологий изменяются способы передачи, обмена и хранения информации. Многие процессы подвергаются влиянию данных обстоятельств, включая электронный документооборот, цифровые подписи, дистанционное образование, а также финансово-экономические аспекты.

В наши дни компьютеризация затронула почти все области жизни общества, что помимо положительных сторон, имеет и неблагоприятные последствия – частности, появление совершенно новых преступлений, совершенных с использованием информационных технологий. Последнее находит подтверждение через попытки создание безопасных условий в цифровое среде [Золотухин, Золотухин, 2022; Золотухин, 2023 Золотухин, Михайлов, 2023; Якунина, Скрипко, Тинтин, 2023] в социологических опросах, например, по данным ВЦИОМа «т**олько 14% россиян абсолютно уверены в своей способности защитить компьютер или смартфон от таких угроз.** Еще 34% «скорее уверены» в этом. Достаточно большая часть наших сограждан (44%) признались, что они не смогут обезопасить свои гаджеты от вредоносных программ или кибератак. Чем старше россияне, тем чаще они так думают: если среди молодежи 18-24 года показатель составляет 26%, то в группе старше 60 лет — 52%.» [Цифровая, 2024].

Мошенничество в сфере компьютерной информации является относительно новым составом хищения, не связанным с основным составом мошен-

ничества [Бахов, Беккер, 2020; Булыгин, 2022; Потапова, Старостина, Съедина, 2022 Слонов, Козырева, 2022; Золотухин, Козырева, 2023]. Так, Федеральным законом «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» № 207-ФЗ от 29.11.2012 г. в действующий УК РФ была включена статья 159.6 «Мошенничество в сфере компьютерной информации». Отметим, что внесение указанной статьи в уголовное законодательство способствует конкретизации компьютерных преступлений, выделяя преступления, осуществляемые с использованием именно компьютерных технологий в отельную категорию [УК РФ, 1996; О внесении, 2012].

В соответствии с Примечанием 1. статьи 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [УК РФ, 1996]. При этом, в юридической литературе справедливо отмечается, что главное отличие мошенничества в сфере компьютерной информации это сложность данной формы хищения, как для квалификации, так и для расследования [Щур, 2021]. Часто жертвами мошенников в сфере компьютерной информации становятся пользователи и организации, а современные средства защиты не всегда способны противостоять меняющейся тактике злоумышленников, так как их механизмы основаны не на технических уязвимостях, а на человеческих слабостях и доверчивости пользователей, не говоря уже о специфике российской ментальности и правоприменения [Zolotukhin, Bikmetov, Shiller, Tarasenko, 2021; Zolotukhin, Yazevich, Zolotukhina, Kozyreva, 2023].

ТАСС пишет о том, что одним из наиболее опасных видов киберугроз, по словам специалистов, остается фишинг. Количество фишинговых сайтов в доменных зонах .ru и .рф за январь-сентябрь 2022 года увеличилось на 15% в сравнении с аналогичным периодом прошлого года. Фишинговые сайты составляют 98-99% заблокированных ресурсов киберпреступников [Статистика, 2023]. Борсученко С. А. и Амосов Е. А. в предложенной им классификации способов интернет-мошенничества, особую роль отводит фишингу, который выступает значимым инструментом мошенничества в сфере компьютерной ин-

формации. Целью мошенника в таком случае становится возможность завладеть банковскими реквизитами, данными электронных платежных карт либо данными от электронных интернет-кошельков пользователей. Фишинговый сайт сложно распознать ввиду того, что он полностью копирует оригинальный сайт, например, может быть полностью скопирован интерфейс какого-либо клиент-банка (в основном, актуально для физических лиц, так как клиент-банки у юридических лиц защищены средствами крипто-шифрования и усиленных цифровых подписей). Технология фишинга заключается в рассылке писем на электронную почту владельцам денежных средств о том, что они якобы стали победителями какой-либо акции. Если владелец переходит по ссылке, отраженной в этом письме, данные его банковской карты (электронного кошелька) отсылаются злоумышленникам. Далее денежные средства потерпевшего без его ведома перемещаются на счета, подконтрольные хакерам, причем нередко производится коррекция страниц с историей доступного баланса с целью скрыть хищение [Борсученко, Амосов, 2020].

В 2022 году чаще всего подвергались кибератакам сайты и приложения – «Сбер», «Авито», «Ozon», «Додо Пицца», «Красное и Белое», «Альфа-банк» «ВТБ», «BlaBlaCar», «Столото», «М.Видео» и «Эльдорадо». Именно от их имени киберпреступники пытались вымогать у граждан их личные данные и денежные средства [Статистика, 2023]. По данным Координационного центра доменов число мошеннических сайтов, мимикрирующих под российские маркетплейсы растет год от года. Если за первое полугодие 2022 года в доменных зонах .ru и .рф заблокировали 5 тыс. фишинговых сайтов, то в первом полугодии 2023 года – уже более 18 тыс. [Координационный, 2024].

При этом для маркетплейсов и площадок подобных «Юла» и «Авито» ситуация является просто критической. Так, в первом полугодии заблокировано 329 мошеннических доменов, так или иначе, связанных с торговлей на «Авито», 94 – с «Юла» и 89 – с «Ozon». Основной схемой мошенничество является поддельная продажа – пользователь вводит данные карты на сайте мошенников, после чего последние похищают деньги. Ссылки на такие ресурсы распространяются в первую очередь через мессенджеры. Маркетплейсы стали первооче-

редной целью потому, что они имеют большие обороты и огромную аудиторию «подготовленных» пользователей, при этом легко клюющих на удочку злоумышленников [Координационный, 2024].

Банковский сектор, сектор продаж, предпринимательство, бизнес, здравоохранение, все эти сферы уже давно автоматизировали процессы хранения и обработки данных. Но с развитием технологий возникают и новые способы мошенничества, предупреждение и предотвращение которых требуют развития криминалистических приемов и методов. При этом отметим, что в связи с популяризацией внедрения в жизнь человека компьютерных технологий возрастает риск несвоевременного раскрытия преступления, такая ситуация связана с тем, что за единицу времени совершается несколько фактов мошенничества.

Библиографический список

1. Бахов К.А., Беккер А.Э. Мошенничество с использованием платежных карт. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. Посвящается 300-летию Кузбасса и 70-летию КузГТУ. Под редакцией В.М. Золотухина, В.Г. Михайлова. – Кемерово, 2020. – С. 144–149.

2. Борсученко С.А., Амосов Е.А. Мошенничество в сфере компьютерной информации: вопросы теории и практики // в сборнике: Цифровизация рыночных отношений: вопросы экономики и права. – 2020. // [Электронный ресурс] – Режим доступа : URL: https://www.studentlibrary.ru/ru/doc/ISBN9785998811838-SCN0000.html (дата обращения 15.03.2024).

3. Булыгин И.А. Мошенничество с использованием электронных средств платежа. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сб. статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 191–196.

4. Золотухин В. М. Социально-философский и культурологический аспекты устойчивого развития цифровых экосистем. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сб. статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2023. – С. 89–99.

5. Золотухин М. В., Золотухин В. М. Проблемы цифровой безопасности в условиях развития технологий. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сб. статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 76–86.

6. Золотухин В.М., Козырева М.В. Юридически значимые сделки: действия, совершаемые заключенными к лишению свободы. // Теория и практика социогуманитарных наук. 2023. – № 2 (22). – С. 109–118.

7. Золотухин М. В., Михайлов В. Г. Цифровизация экономики: проблемы, тенденции и перспективы. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сб. статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2023. – С. 420–425.

8. Координационный центр доменов .ru /.рф (КЦ) // [Электронный ресурс] – Режим доступа : URL: https://cctld.ru/service/ (дата обращения 15.03.2024).

9. Скрипко В. Е. Формирование концепций сетевой трансформации экономики и ее цифровой платформы. // Экономика и управление инновациями. 2023. – № 4 (27). – С. 4–10.

10. «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Федеральный закон № 207-ФЗ от 29.11.2012 // Российская газета. – 02.12.2012. [Электронный ресурс]. – Режим доступа : URL: https://rg.ru/documents/2012/12/03/moshennichestvodok.html?ysclid=lotxvienbf447510927 (дата обращения 15.03.2024).

11. Потапова А. А., Старостина В. Е., Съедина Н. В. Недобросовестная конкуренция как механизм повышения уровня продаж в социальных сетях. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сб. статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 475–481.

12. Слонов Е. А., Козырева М. В. Проблема наследования цифровых активов: социокультурный и правовой аспекты. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сб. статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 482–491.

13. Статистика и аналитика. Министерство Внутренних дел Российской Федерации. // [Электронный ресурс] – Режим доступа URL: https://xnb1aew.xnp1ai/dejatelnost/statistics?ysclid=lotyapgvs2473673242 (дата обращения 15.03.2024).

14. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 14.02.2024) // [Электронный ресурс]. – Режим доступа: URL: http://pravo.gov.ru/proxy/ips/?docbody&nd= 102041891&ysclid=loty2f903s958769412 (дата обращения 15.03.2024).

15.Цифровая самооборона. ВЦИОМ. 12. Марта 2024. // [Электронный ресурс]. – Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/cifrovaja-samooborona (дата обращения 15.03.2024).

16. Щур, Д. Г. Мошенничество в сфере компьютерной информации как состав преступления: проблемы квалификации и правоприменения. // Молодой ученый. – 2021. – № 25 (367). – С. 357-360. – [Электронный ресурс]. – Режим доступа :URL: https://moluch.ru/archive/367/82639/ (дата обращения 15.03.2024).

17. Якунина Ю. С., Скрипко В. Е., Тинтин Ху. К вопросу о сетевизации экономики в контексте ее устойчивости к внешним шокам. // Экономика и предпринимательство. 2023. – № 2 (151). С. 152–154.

18. Zolotukhin V.M., Bikmetov R.S., Shiller V.V., Tarasenko A.A. Sociocultural aspect of criminal lam enforcement the russian mentality . Rudn conference on legal theory, methodology and regulatory practice (RUDN LTMRP conference 2021/ SHS Web of Conferences (см. в книгах). 2021. № 118. С. 02009.

19. Zolotukhin, V., Yazevich, M., Zolotukhina, N., Kozyreva, M. The problems of legal regulation of the environmental policy of the resource-producing region. E3S Web of Conferences, 2023, 376, 05052

A. A. Blinov., A. A. Chichendaeva

B. *Kuzbass State Technical University them. T.F. Gorbachev, Kemerovo, Russia*

PHISHING AS A NEW WAY OF FRAUD IN THE FIELD OF COMPUTER INFORMATION

Scientific adviser: PhD in Pedagogy, Associate Professor at the Department of History, Philosophy and Social Sciences Sedina N.V.

The article discusses issues regarding new ways of committing fraud in the field of computer information, in particular phishing, touches on the analysis of statistical data in relation to existing cyber threats, reveals the essential characteristics of the introduction of digital technologies in the production and management process, as well as in the life of society.

Key words: fraud, computer information, phishing, information technology, mass media.