In order to improve the economic position of a construction company in the market, it should increase its assets, which thereby improve its liquidity. This can help a company stay in the construction market for a long time.

Thus, the change in the construction market, to a large extent, involves correctly chosen strategies for further development of the construction companies so that the new residential areas could meet all the requirements of consumers. In the current business environment, there is a number of external and internal risks affecting the construction market. If companies assess their risks before starting construction, they can avoid problems in the future and build quality and new dwellings for their customers. The proposed methodology enables to assess the current risk factors that may affect the business. It can be applied by other construction companies operating in Russia.

References

1. Place of the construction industry in the country's economy [Electronic resource]. URL: https://studref.com/304747/marketing/mesto_stroitelnoy_otrasli_ekonomike_strany (Accessed: 20.12.2022).

2. Simkin L., Pride W., Ferrell O., Dibb S. Marketing concepts and strategies. 8th edition, Cengage Learning EMAE, 2019.

3. Program «Young family» [Electronic resource]. URL: https://realty.rbc.ru/news/5bf68c3e9a79475a8f12a80d (Accessed: 20.12.2022).

4. Reducing the demand for housing [Electronic resource]. URL: https://mir24.tv/news/16525795/snizhenie-sprosa-na-kvartiry-nablyudaetsya-v-rossii (Accessed: 20.12.2022).

5. Official website of the construction company [Electronic resource]. URL: https://gk-dom-stroy.ru (Accessed: 20.12.2022).

Юридические науки

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ ПРИ ИСПОЛЬЗОВАНИИ ФИНАНСОВЫХ ТЕХНОЛОГИЙ НА ПРИМЕРЕ ФИШИНГА

Власов А.В.

ФГБОУ ВО «Финансовый университет при Правительстве РФ», Москва, e-mail: kimurkastyle@gmail.com

Развитие сетей связи производит серьёзное преобразующее влияние на общественные отношения. Деловое общение, общение с банками и даже государством все больше переходит в удаленный и электронный формат, преимущественно по средством сети Интернет. Отдельно стоит отметить развитие финансовых (информационных) технологий, или коротко финтеха. На сегодняшний день уже почти невозможно представить современную жизнь без интернет-банкинга, онлайн-шоппинга, средств «электронного государства». Однако увеличение объема удаленных операций так же увеличивает риски их противоправного использования.

Уже достаточно богатая история развития всемирной сети Интернет содержит опыт выявления и классификации различных способов неправомерного доступа к информации. Среди наиболее популярных классов неправомерных действий в сети интернет особое место занимает фишинг (от англ. fishing – рыбачить).

Принцип данного класса неправомерных действий состоит в получении необходимой информации или денежных средств от жертвы, используя вполне легальные действия и методы, но по средством введения в заблуждение. Как правило злоумышленники пользуются приемами социальной инженерии. Самый распространенный из используемых приемов – злоупотребление доверием, как правило к известному бренду. Так жертве в виде письма может прийти приглашение, например от популярного интернет-магазина, которое будет содержать информацию о больших «скидках» на товары и ссылку. Однако эта ссылка уже будет вести не на страницу магазина, о котором думает жертва, а на страницу мошенников, которая мимикрирует под официальную. Если жертва вовремя не заметит подмены ресурсов, то проведенный платеж с такой страницы или оставленные платежные данные оказываются в руках мошенников. Стоит отметить, что фишинг-ссылки могут приходить не только по электронной почте. Ввиду распространения смартфонов фишинг ссылку можно так же получить из смс, сообщений в социальных сетях и торговых площадках, а также мессенджерах.

Стоит отметить, что с точки зрения уголовного законодательства при достаточном количестве материального ущерба фишинг это мошенничество, поскольку он построен на механизме злоупотребления доверием. С другой стороны, сам факт создания и рассылки фишинговых ссылок и страниц не является уголовно наказуемым деянием.

Согласно статистическим сводкам МВД [1] в 2021 году процент преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации превысил 26% от общего числа, причем две трети таких преступлений происходит по средством использования сети Интернет. Дополнительно отмечается увеличение как общего количества таких преступлений, так и их доля в общем количестве преступлений. Дополнительно стоит отметить, что статистически число расследованных случаев мошенничества, совершенного с использованием информационных технологий, не превышает 10% процентов. Такой процент раскрываемости стал результатом выделения двух специальных статей УК РФ по мошенничеству. Первая из специальных статей УК 159.3 «Мошенничество с ис-

пользованием электронных средств платежа» изначально содержащая во второй половине названия «платежных карт». Причиной изменения послужило расширение термина на все доступные платежные инструменты в РФ. По данному составу необходимо наличие умышленного злоупотребления доверием потерпевшего. Как правило обман происходит в результате прямого общения с потерпевшим, либо при разговоре/переписке по средствам информационно-телекоммуникационных сетей.

Вторая из таких статей УК РФ 159.6 «Мошенничество в сфере компьютерной информации» наиболее интересна при рассмотрении фишинга. Учитывая постановления Верховного Суда № 48 от 2017 года [2] и 37 от 2022 года [3], мошенничество в сфере компьютерной информации требует так же квалификации по статьям 272-274.1 УК РФ. При этом сам смысл указанных статей не предполагает какого-либо взаимодействия с потерпевшим, что делает «злоупотребление доверием», как обязательный признак мошенничества» в данном случае невозможным либо маловероятным.

Учитывая вышесказанное, фишинг, как способ мошенничества в сети интернет, можно было бы квалифицировать по статье 159.6 УК РФ в совокупности со статьей 273 УК РФ. Однако в данном случае могут возникнуть проблемы квалификации. Если саму фишинговую страницу/ссылку можно подвести под термин «иной компьютерной информации», то при наличии прямого онлайн эквайринга на этой странице, перечисленные в статье запрещенные действия «уничтожения, блокирования, модификации, копирования» не описывают произведенное деяние – «передачу» данных.

Оценив общий объем операций без согласия клиента платежных систем в 13.6 миллиардов рублей только в 2021 году Банк России инициировал более 6 тысяч блокировок фишинговых страниц [4]. Стоит отметить, что скорость блокировки резко возросла в декабре 2021, поскольку был принят Федеральный закон от 01.07.2021 N 250-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», позволяющий проводить Центральному Банку досудебную блокировку ресурсов подобного содержания. Дополнительно Банком России была произведена блокировка 179 тысяч мошеннических телефонных номеров. С целью продолжить деятельность в этом направлении Банком России был инициирован законопроект о создании единой системы телефонных номеров, которая позволяла бы подключившимся организациям получать точные сведения о текущем держателе номера [5]. Однако, проанализировав данный законопроект, можно прийти к выводу, что он больше служит для упрощения работы банков и несет серьезные риски утечки персональных данных граждан.

Как можно заметить, деятельность государственных органов и Банка России в области борьбы с фишингом не предполагает расследования. Предупреждение фишинга сводится к информированию населения, либо к предложению отключения инструментов удаленной оплаты у наиболее подверженной мошенническим действиям прослойки населения – пенсионеров [4]. Наиболее активные усилия прилагаются государством в области пресечения подобной деятельности. Причем о блокировке скомпрометированных банковских счетов речи не идет. Получив блокировку одного из своих фишинговых сайтов злоумышленнику, не стоит особого труда перенести его на другое доменное имя. Указанное положение дел может только служить почвой для роста самой проблемы.

Современные исследователи, анализируя проблему фишинга и мошенничества в информационно-телекоммуникационных сетях в целом приходят к выводам о необходимости повышения квалификации сотрудников следственных органов и необходимости обучения и информирования населения о проблеме [6]. Другим распространенным мнением является введение юридической ответственности для провайдеров связи, которые не ограничивают доступ к ресурсам, содержащим запрещенную информацию, и запрет на технологии, способствующие анонимности в информационно-телекоммуникационных сетях [7].

Стоит отметить, что данные подходы несколько не адекватны ситуации. Рассматривая вопрос повышения квалификации следователей до уровня, необходимого для эффективного противостояния фишингу не стоит упускать факт того, что фишинг, как и преступления, связанные с информационными технологиями и современными средствами телекоммуникации в целом – не единственное направление в работе следователя, с которым у него могут возникнуть вопросы ввиду низкого уровня знаний предмета. Изучая, например, вопрос финансовых преступлений авторы более склонны к формированию методик и тактик связанных с использованием компетенций специалистов. Предлагается придерживаться указанного подхода и в рассматриваемом вопросе.

Вопрос об ответственности провайдера за контент в интернете кажется излишним, в текущей ситуации все провайдеры обязаны иметь оборудование СОРМ, которое осуществляет блокировку по спискам Роскомнадзора. Вопрос о не полном или некорректном срабатывании таких блокировок должен быть отнесен к юридическим лицам, обслуживающим данное оборудование по договору с провайдерами. Обязать провайдеров превентивно блокировать информацию приведет к переходу механизмов цензуры от государства к частным компаниям. Запрет «анонимайзеров» выглядит тоже как избыточ-

ная мера. Под общим соловом «анонимайзер» как правило понимают сервисы VPN и Proxy. Оба этих сервиса в первую очередь используются для усиления безопасности работы в интернет и создания безопасных соединений между филиалами компаний или их сотрудниками на удаленном режиме работы.

Отвергая предложенные пути решения проблемы хочется обратиться к имеющимся насущным проблемам. Как можно видеть из анализов результатов борьбы государства с фишингом главная проблема состоит в идентификации владельца фишингового ресурса. Данная проблема вызвана полным отсутствием регулирования на государственном уровне как хостинга (англ. hosting) так и выделения доменных имен что порождает возможность анонимного создания страниц противоправного содержания. Стоит отметить, что хостинг, как деятельность по предоставлению технической возможности размещать страницы с общим доступом в сети интернет не трактуется Роскомнадзором как деятельность, требующая лицензирования, поскольку имеющийся Федеральный закон «О связи» предполагает необходимость факта передачи информации, который в понятие хостинг не входит [8].

Так один из крупнейших регистраторов доменных имён в РФ осуществляет свою деятельность на основе договора, в котором прописываются данные достаточные для однозначной идентификации клиента [9]. С другой стороны, на рынке присутствуют организации, которые предоставляют эти услуги на условиях публичной оферты [10]. Аналогичная ситуация наблюдается с хостингом. Очевидно, что имея злонамеренный умысел преступник обратится к услугам фирм, не требующим подписания полноценного контракта и идентификации личности. Учитывая изложенную выше информацию, становится очевидной необходимость модернизации законодательства в части обязывания компаний, предоставляющих услуги хостинга и выделения доменных имен, регистрировать и заключать договора со своими клиентами, только при полной и однозначной идентификации. Можно предположить, что введение таких мер заставит мошенников перейти на зарубежный хостинг. С целью предупреждения обхода ограничения таким образом необходимо ввести запрет для эквайринговых организаций на работу с сайтами, каким-либо образом зарегистрированным или работающим за пределами Российской Федерации. Учитывая санкционную ситуацию на конец 2022 года, в частности недоступности сервиса SWIFT, данная мера не будет избыточной или критически ограничивающей.

В дополнение стоит организовать на базе Роскомнадзора реестр доверительных сайтов с подключенными механизмами удаленной оплаты, содержащий достоверные и полные данные о получателе денежных средств. С другой стороны, под надзором Минцифры разработать приложения для разных операционных систем ПК и смартфонов, которые позволяли бы проверять наличие открытой на устройстве ссылки или страницы в упомянутом ранее реестре, с указанием информации о получателе платежа или данных пользователя.

Список литературы

1. Состояние преступности (январь-октябрь по годам). Министерство Внутренних Дел Российской Федерации. Официальный сайт. [Электронный ресурс]. URL: https://мвд.рф/folder/101762 (дата обращения: 12.12.2022).

2. Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате». СПС «КонсультантПлюс».

3. Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». СПС «КонсультантПлюс».

4. Киберустойчивость финансового сектора и противодействие кибермошенничеству // офиц. сайт Банка России. [Электронный ресурс]. URL: https://cbr.ru/about_br/publ/results_work/2021/obespechenie-ustoychivosti-finansovogo-rynka (дата обращения: 12.12.2022).

5. Законопроект № 514780-7 О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма» и иные законодательные акты Российской Федерации (о создании информационной системы проверки сведений об абоненте) // Система обеспечения законодательной деятельности. [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/514780-7 (дата обращения: 12.12.2022).

6. Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. Т. 13. № 2. DOI 10.17150/2411-6262.2022.13(2).36.

7. Озеров И.Н., Озеров К.И. Проблемы предупреждения мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий // Проблемы правоохранительной деятельности. 2021. № 1. С. 30-34.

8. Разъяснения Роскомнадзора по вопросу лицензирования деятельности провайдеров хостинга. Официальный сайт Роскомнадзора. [Электронный ресурс]. URL: https://rkn.gov.ru/it/control/p852/ (дата обращения: 12.12.2022).

9. Форма договора для физического лица. RUCenter. [Электронный ресурс]. URL: https://www.nic.ru/help/forma-dogovora-dlya-fizicheskogo-lica_3641.html (дата обращения: 12.12.2022).

10. Справочная информация. A100.RU. [Электронный ресурс]. URL: https://a100.ru/131-2/ (дата обращения: 12.12.2022).

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ФИНАНСОВОЙ СФЕРЕ

Голодрыга Л.В.

ФГБОУ ВО «Финансовый университет при Правительстве РФ», Москва, e-mail: www.msluiza.com@mail.ru

Искусственный интеллект это сочетание новых технологий, процессов и методов, имеющих все большее значение для текущего и будущего развития экономики. Искусственный интеллект сегодня применяется в различных отраслях, таких как медицинская диагностика, оптическое