Научная статья
Original article

Интернет-мошенничество как угроза экономической безопасности

Гончарова М.Н.*, Перевалов А.М., Геймбихнер В.Р.
Уральский государственный экономический университет, Екатеринбург, Россия
**Автор-корреспондент: gonchmn@usue.ru*

Аннотация: В статье представлены результаты анализа статистических данных, характеризующие изменения динамики случаев интернет-мошенничества, приведена характеристика «фишинга» как современного вида обмана в сети, особое внимание уделено дейтинговым ресурсам, как площадкам для осуществления фишингового мошенничества. Также рассмотрены методы, используемые мошенником для заполучения персональной информации жертвы. Киберпреступность рассматривается как фактор угрозы экономической безопасности личности. Выдвинута гипотеза возможных о мерах государственной политики, направленных на решение рассмотренной проблемы.

Ключевые слова: интернет-мошенничество, киберпреступность, фишинг, дейтинг, экономическая безопасность.

Для цитирования: Гончарова М.Н., Перевалов А.М., Геймбихнер В.Р. Интернет-мошенничество как угроза экономической безопасности. Умная цифровая экономика. 2022. Т.2, №2, с. 116-121

Internet fraud as a threat to economic security

Goncharova M.N.*, Perevalov A.M., Geymbikhner V.R.
Ural State University of Economics, Yekaterinburg, Russia
** Corresponding author: gonchmn@usue.ru*

Abstract: The article presents the results of the analysis of statistical data characterizing changes in the dynamics of cases of Internet fraud, characterizes "phishing" as a modern type of deception on the network, special attention is paid to dating resources as platforms for phishing fraud. The methods used by the fraudster to obtain the victim's personal information are also considered. Cybercrime is considered as a threat to the economic security of the individual. A hypothesis of possible measures of state policy aimed at solving the considered problem has been put forward.

Keywords: Internet fraud, cybercrime, phishing, dating, economic security.

For citaion: Goncharova M.N., Perevalov A.M., Geymbikhner V.R. Internet fraud as a threat to economic security. Smart Digital Economy. 2022. T.2, №2, pp. 116-121

Современные компьютерные и информационные технологии имеют как положительные, так и отрицательные последствия для экономики. С одной стороны, они дают преимущества: технологии онлайн-платежей, возможность коммуникации из любых точек мира, а также большое количество информации в отрытом доступе. С другой же стороны,

потенциальные возможности могут выступать как угроза экономической безопасности личности. Это происходит тогда, когда действующими лицами выступают с одной стороны – мошенники, а с другой – доверчивые люди с низким уровнем интернет-грамотности.

За период ограничений, вызванных коронокризисом, в Российской Федерации был зафиксирован резкий рост числа зарегистрированных случаев мошенничества. За второй квартал 2020 года прокуратурой было зафиксировано 82,5 тысяч случаев мошенничества, из которых 71% – по телефону или через интернет. Согласно статистике генпрокуратуры, за первое полугодие 2020 года количество дел о телефонном и интернет-мошенничестве выросло на 76% в сравнении с аналогичным периодом 2019 года [3]. Суммарно за 2020 год телефонные и онлайн-мошенники заработали на россиянах около 150 миллиардов рублей [1].

Новый вид мошенничества, реализуемого посредством глобальной сети, определяется как «фишинг» и характеризуется как «вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям» [4]. Сущность метода заключается в умышленном обмане жертвы с целью заполучения персональных данных. Целью обмана является заполучение таких личных данных, как логин и пароль пользователя от определённого аккаунта, идентификационные данные банковского кабинета или ПИН-код с номером карточки [6]. Имея эту информацию, мошенник может получить доступ к соцсетям жертвы, вывести на свой счёт его деньги, а также использовать для иных противоправных целей.

Пострадавший предоставляет фишеру личные данные добровольно под влиянием психологических воздействий. Фишер использует персональную информацию для совершения противоправных действий.

В научной статье М. М. Могунова выводит следующее определение фишинга: «получение путем обмана или методов социальной инженерии (хакерства с использованием человеческого фактора) персональных данных для использования в корыстных, преступных целях». С повышением опытности и недоверчивости людей у мошенников появилась необходимость в модернизации и совершенствовании схем обмана. Был разработан такой способ фишингового мошенничества, как «социальная инженерия». Его отличительной чертой является добровольный характер действий жертвы. В данном случае получение персональных данных осуществляется посредством психологических приёмов мошенника [5].

На протяжении последних лет количественная динамика жертв мошенников в сфере интернет знакомств сохраняет стабильную возрастающую тенденцию. Сайты и приложения для знакомств носят название «Дейтинг» (Dating с англ. – свидание, встреча). Рынок онлайн-дейтинга в России начал формироваться в начале 2000-х. Тогда сайты знакомств динамично росли, но испытывали серьезные проблемы с репутацией. Однако на сегодняшний день онлайн-сервисы по поиску знакомств получили широкое распространение, в открытом доступе представлено множество сайтов и приложений. Более 30% пользователей сервисов знакомств сталкиваются с мошенничеством, например, получают ссылки с вредоносным программным обеспечением или попадаются в хитросплетенные сети шантажистов.

Через дейтинговые ресурсы мошенник реализует долгосрочные обманные сценарии, жертвами чаще выступают лица, которые используют сеть Интернет в целях поиска новых знакомств, для общения, в частности близких (романтических) отношений. По словам

экспертов, аферистам легче найти жертву именно на дейтинговых платформах – такие сервисы анонимны, предполагают общение с незнакомцами, что зачастую усыпляет бдительность пользователей.

Дейтинговые платформы дают преступнику возможность действовать дистанционно, без личных встреч, посредством чего он получает возможности установить дружеские или даже романтические отношения с жертвой. Мошенник использует метод «социальной инженерии», посредством которого получает личные данные непосредственно от самого владельца, либо посредством фишинговых ресурсов (ссылки на сайты, требующие ввода персональных данных) [5].

Количество фишингового мошенничества неуклонно растёт. Если в 2018 году 28% посетителей таких ресурсов сталкивались с мошенничеством, то по данным на 2021 год уже 34%. За период с 2018 по 2021 гг. выросло и количество людей, которые получают вирусы и подозрительные ссылки на сайтах знакомств, с 28% до 38%, а каждый десятый (в 2021 году – 11%) сталкивается со случаями шантажа (в 2018 году – 8%) [2]. Преступники киберпространства становятся все более изобретательными, а их методы – все более изощренными. Они вынуждены постоянно модернизировать вредоносное программное обеспечение и способы его распространения.

Злоумышленники используют методы «социальной инженерии», тщательно планируют атаку, исходя из особенностей конкретной жертвы. При этом мошенниками создано множество способов обмануть доверчивых пользователей дейтинговых ресурсов: фишинг, распространение вирусов, вымогательство и шантаж. Популярен такой метод, как создание вымышленной личности, с помощью которой злоумышленник выясняет персональные данные банковских карт жертвы, предлагает приобрести билеты в кино или театр на фишинговом сайте.

Чаще всего мошенники создают поддельную страницу девушки или молодого человека мечты и после личного общения с жертвой предлагают скачать архив с фотографиями, содержащий вирусное программное обеспечение, перейти по ссылке на фишинговый ресурс или, получив откровенные фото, шантажируют свою жертву.

По прогнозам аналитиков, к 2023 году доля киберпреступлений может вырасти с 14% до 30%. Это связано с низкой раскрываемостью и слабыми возможностями по идентификации онлайн-злоумышленников.

На данный момент органы дознания нуждаются в новом технологическим обеспечением, которое позволит эффективно находить нарушителей Уголовного кодекса по электронно-цифровому следу. В МВД, однако, утверждают, что количество раскрытых IT-преступлений за 2018–2019 годы выросло в полтора-два раза. Однако, как показывает практика, около 80% пострадавших от киберпреступлений несут небольшой ущерб – менее 5 тыс. рублей. Такие дела не подпадают под действие Уголовного кодекса. На данный момент российское законодательство недостаточно в сфере определения и регулирования киберпреступлений. В своей работе М. М. Могунова утверждает, что законодательству РФ «требуются если не кардинальная переработка, то, во всяком случае, серьезные дополнения в соответствии с реалиями времени». В соответствии с полученными выводами автор даже предлагает собственный вариант дополнения статьи гл. 28 УК РФ ст. 272.1 «Получение путем

обмана или методов социальной инженерии электронных персональных данных для использования в корыстных целях» [5].

Интернет-мошенничество представляет собой одну из основных экономических угроз в интернет-пространстве, прогнозы аналитиков по динамике роста киберпреступлений заставляют принять во внимание динамично растущую проблему. Использование персональных данных посторонними лицами нарушает экономическую безопасность личности.

Государство заинтересовано в обеспечении экономической безопасности личности, поскольку данный процесс тесно взаимосвязан с экономической безопасностью государства. Стабильное развитие государства достигается за счёт экономической и социальной стабильности граждан. Поэтому требуется поддерживать экономическую защищённость личности, которая определяется как: «такое состояние, в котором происходит максимальное обеспечение всей совокупности необходимых условий охраны жизненных экономических интересов личности при регулярном протекании процесса реализации ее социальной защищенности и развития». Охрана жизненных экономических интересов осуществляется посредством комплекса мер, затрагивающих различные сферы: экономическую, правовую, политическую, социальную, а также пропагандистскую [7].

Государству следует принять во внимание реальную угрозу фишингового мошенничества и принять эффективные меры для её предотвращения. Безусловно, меры будут наиболее эффективны при объединении их в целостную программу при комплексной реализации всех мер. Однако обеспечение защиты личности от интернет-мошенничества достигается по большей части за счёт реализации правовых мер.

Соответственно, необходимо разрабатывать новые и действенные механизмы экономической безопасности, развивать цифровую и финансовую грамотность молодых людей. Для информирования граждан следует активно распространять информацию о фактах интернет-мошенничества посредством правоохранительных органов, СМИ и интернет-порталов.

На наш взгляд, снижения количества киберпреступлений возможно достичь, реализуя меры государственной политики по двум направлениям.

Во-первых, необходим более жёсткий контроль правоохранительных органов за действиями лиц в сети Интернет. Следует уделить особое внимание действиям участников дейтинговых платформ, а также законодательно установить наказание, следующие за фишинговое мошенничество. Так государство сможет определить мошенников и преостановить правонарушительные действия, обеспечить экономическую безопасность граждан. Наращивание технологических мощностей правоохранительных органов будет повышать качество контроля за сетевыми правонарушениями.

При этом совершенствование уголовного законодательства в сфере интернет-мошенничества следует проводить совместно с правоведами и специалистами в области кибербезопасности [5]. Посредством объединения специалистов из разных сфер удастся комплексно изучить проблему и усовершенствовать законодательную базу. определить справедливое наказание. за совершённое правонарушение и предупредить совершение новых преступлений.

Во-вторых, требуется, чтобы граждане умели обеспечить себя безопасностью самостоятельно. Этого реализуемо за счёт повышения цифровой грамотности населения, в частности за счёт повышения цифровой компетентности.

Для обеспечения экономической безопасности граждан на дейтинговых платформах, требуется развить следующие навыки:

– не переходить по подозрительным ссылкам от малознакомых собеседников;
– не распространять персональную информацию в профиле и переписках;
– не разглашать банковские данные посторонним людям (вводить банковские реквизиты исключительно для оплаты на официальных сайтах);
– устанавливать исключительно официальные приложения из достоверных источников;
– не поддаваться на провокации малознакомых людей в сети (к примеру, крайне щедрые предложения или подозрительным просьбы).

Владение вышеперечисленными компетенциями позволит гражданину самостоятельно обеспечить свою экономическую безопасность в интернет-пространстве. Также не попасться на уловку мошенников гражданам поможет умение отличать фишинговые сайты. В случае предоставления интернет-знакомым ссылки на сайт следует обратить внимание на адресную строку, оно будет отличаться от оригинала, иметь лишние знаки. В таком случае можно ввести «любой вымышленный адрес электронной почты и случайный набор символов в качестве пароля» Если сайт ненастоящий, то он примет введенные данные как правдивые и произведёт переадресацию на настоящий сайт [6].

Список литературы

1. Не пойман – не разговор // Коммерсантъ. URL: https://www.kommersant.ru/doc/4627498 (дата обращения: 22.04.2021)
2. Небезопасные связи: на сайтах знакомств стало больше мошенников // Известия. URL: https://iz.ru/975882/anastasiia-gavriliuk/nebezopasnye-sviazi-na-saitakh-znakomstv-stalo-bolshe-moshennikov (дата обращения: 22.04.2022).
3. Число дел о мошенничестве рекордно выросло на фоне пандемии // РБК. URL: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d (дата обращения: 22.04.2021)
4. Википедия [Электронный ресурс] – https://ru.wikipedia.org.
5. Могунова, М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) / М. М. Могунова // Вестник Саратовской государственной юридической академии. – 2020. – № 4(135). – С. 135-141. – DOI 10.24411/2227-7315-2020-10110. – EDN HFBJRG.
6. Бачиева, А. В. Фишинг как один из способов мошенничества в сфере компьютерной информации / А. В. Бачиева, Т. О. Бозиев // Актуальные проблемы юридической науки и практики, Гатчина, 31 марта 2017 года. – Гатчина: Государственный институт экономики, финансов, права и технологий, 2017. – С. 232-235. – EDN ZHTGZH.

7. Моштакова, М. А. Экономическая безопасность личности / М. А. Моштакова, В. Ю. Щеглов, А. О. Скворцов // Вестник Пензенского государственного университета. – 2020. – № 4(32). – С. 45-49. – EDN SWDDAN.