Мошенничество в цифровом обществе в условиях социальных изменений

УДК 316.422.44 DOI 10.26425/2658-347X-2023-6-1-59-71

Получено 27.02.2023 Доработано после рецензирования 21.03.2023 Принято 29.03.2023

Сергеев Артем Юрьевич

Канд. техн. наук, магистрант

ORCID: 0000-0003-3251-4770
E-mail: 6feeling5element@mail.ru

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, г. Москва, Российская Федерация

Широкова Олеся Вадимовна

Канд. социол. наук, доц. каф. организационного проектирования систем управления

ORCID: 0000-0001-6984-6627
E-mail: ov.shirokova@igsu.ru

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, г. Москва, Российская Федерация

АННОТАЦИЯ

В статье проанализированы проблемы мошенничества в современном цифровом обществе в условиях социальных изменений, вызванных как пандемией COVID-19, так и сложившейся геополитической ситуацией. Подробно изучены виды финансового мошенничества в данной области. Особое внимание уделено видам цифрового мошенничества: телефонному мошенничеству и IP-телефонии, СМС-мошенничеству, фишингу (от англ. fishing – «рыбная ловля, выуживание»), снифферингу (от англ. to sniff – «нюхать» – перехват сообщений), скиммингу (от англ. to skim – «бегло прочитывать», «скользить» – кража данных карты), которые связаны с появлением криптовалют. В работе приведены данные авторского социологического исследования, проведенного методом анкетного интернет-опроса (n = 765). Исследование показало, что только 44 % респондентов информированы о видах мошенничества в достаточной степени, чтобы защититься от современных интернет-злоумышленников. Анализ данных по некоторым видам цифрового мошенничества показал, что 20 % респондентов теряли деньги из-за телефонного или интернет-мошенничества, 16 % респондентов лично сталкивались с IP-телефонией, а 40 % – не имеют представления о таком виде мошенничества, как снифферинг и существующих антивирусных способах защиты от него. Исследование показало также уязвимость, в первую очередь, мужской половины населения старше 40 лет в области интернет-мошенничества. Поэтому органам государственной власти совместно со средствами массовой информации, бизнесом и другими акторами российского социума необходимо усилить проводимую политику в области повышения уровня финансовой и цифровой грамотности населения.

Ключевые слова

Интернет-мошенничество, цифровое мошенничество, киберпреступность, социальные изменения, цифровое общество, цифровой риск, телефонное мошенничество, СМС-мошенничество, фишинг, снифферинг, скимминг, защита информации, финансовая грамотность, цифровая грамотность

Для цитирования

Сергеев А.Ю., Широкова О.В. Мошенничество в цифровом обществе в условиях социальных изменений // Цифровая социология. 2023. Т. 6, № 1. С. 59–71.

Fraud in a digital society in the context of social change

Received 27.02.2023 Revised 21.03.2023 Accepted 29.03.2023

Artem Yu. Sergeyev

Cand. Sci. (Engr.), Graduate Student

ORCID: 0000-0003-3251-4770

E-mail: 6feeling5element@mail.ru

Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia

Olesya V. Shirokova

Cand. Sci. (Sociol.), Assoc. Prof. at the Organizational Design of Control Systems Department

ORCID: 0000-0001-6984-6627

E-mail: ov.shirokova@igsu.ru

Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia

ABSTRACT

The article analyzes the problems of fraud in the modern digital society in the context of social changes caused by both the COVID-19 pandemic and the current geopolitical situation. The authors study in detail the types of financial fraud in this area. They pay special attention to the types of digital fraud: telephone fraud and IP-telephony, SMS fraud, phishing, sniffering (message interception), skimming (theft of card data), which are associated with the emergence of cryptocurrencies. The article presents the data of the authors' sociological research conducted by the method of an online questionnaire survey (n = 765). The study showed that only 44 % of respondents are sufficiently informed about the types of fraud to protect themselves from modern internet scammers. An analysis of data on certain types of digital fraud showed that 20 % of respondents lost money due to telephone or Internet fraud, 16 % of respondents personally encountered IP telephony, and 40 % have no idea about such a type of fraud as sniffering and existing anti-virus protection against it. The research also showed the vulnerability, first of all, of the male half of the population over 40 years of age in the field of internet fraud. Therefore, public authorities, together with the media, business and other actors of Russian society, need to strengthen the policy in the field of improving the level of financial and digital literacy of the population.

Keywords

Internet fraud, digital fraud, cybercrime, social change, digital society, digital risk, telephone fraud, sms fraud, phishing, sniffering, skimming, information protection, financial literacy, digital literacy

For citation

Sergeyev A.Yu., Shirokova O.V. (2023) Fraud in a digital society in the context of social change, *Digital Sociology*, vol. 6, no. 1, pp. 59–71. DOI: 10.26425/2658-347X-2023-6-1-59-71

ВВЕДЕНИЕ / INTRODUCTION

Распространение глобальной веб-паутины – сети «Интернет» (далее – Интернет), открыло путь к серьезным изменениям. С появлением социальных сетей общение из реальной жизни стало перетекать в онлайн, появился и был введен в научный оборот термин «цифровизация», а сам процесс прочно вошел в жизнь социума, меняя отношения, уклад жизни и влияя на развитие человека и общества с еще большей силой, чем ранее [Василенко, Мещерякова 2021]. В частности, Л. Василенко и Н. Мещерякова акцентируют внимание на двух противоположно направленных тенденциях развития цифрового общества: от суперумного общества 5.0 до высоко рискогенного, порождающего многочисленные форматы поведения, разрушающие устоявшиеся форматы социальности.

С каждым годом Интернет продуцирует новые возможности для мошенников, позволяя им совершать противозаконные действия онлайн и оставаться почти незамеченными. Мошенничество в Интернете распространяется по всем каналам взаимодействия пользователей: социальные сети, форумы, маркетплейсы и т.д.

Мошенничество и неправомерное использование компьютеров распространено во многих странах. Например, в Великобритании более 60 % случаев мошенничества происходит с помощью мобильных устройств [Manivannan, Moorthy, 2020]. В Саудовской Аравии, по оценкам, ежегодно теряется 16 млрд саудовских риалов из-за коммерческого мошенничества, значительная часть которого совершается в электронном виде. Эта страна входит в первую двадцатку стран, наиболее пострадавших от электронного мошенничества [Baz et al., 2017]. В Нигерии электронное банковское мошенничество (англ. e-fraud) при переходе к экономике безналичных расчетов стало одним из самых распространенных правонарушений [Tade, Adeniyi, 2020]. В 2019 г. убытки от глобального мошенничества составили 27 млрд долл. США [Wickramanayake et al., 2020]. Таким образом, по своей сути, человек может постоянно сталкиваться с мошенниками и стать их легкой добычей, даже не подозревая этого.

Нас как исследователей интересует такой малоизученный аспект этих правонарушений, как цифровое мошенничество, его типологизация, виды, формы, анализ и направления, по которым наблюдается наибольшее количество пострадавших. Более того, в условиях актуальных социальных изменений, связанных со сложившейся геополитической ситуацией, признаками которой являются милитаризация киберпространства, сворачивание международного сотрудничества, усиливающийся кризис доверия и информационные войны, проблема мошенничества с использованием «больших данных» стала еще более актуальной.

ПОСТАНОВКА ПРОБЛЕМЫ / PROBLEM STATEMENT

Предпосылкой возникновения такого явления, как цифровое мошенничество, является, с одной стороны, всеобщая цифровизация в условиях нового гендерного порядка и транзитивной экономики, а с другой стороны – низкий уровень компьютерной и финансовой грамотности. Финансовая грамотность без понимания сути развития цифрового общества не дает возможности эффективно ставить и решать многие задачи.

На сегодняшний день сложилась уникальная ситуация, когда цифровизация стремительно распространяется. Это связано с тем, что в начале 2020 г. общество столкнулось с новым вызовом, которым стала пандемия коронавируса COVID-19. По прошествии последних двух лет можно утверждать, что люди сегодня гораздо больше погружены в Интернет, чем когда-либо. Последствия пандемии отразилась не только на обычных пользователях, но и на бизнесе. Сегодня бизнес перестраивается под онлайн-формат, появляется все больше маркетплейсов и экосистем, которые позволяют удовлетворять потребности потребителя при помощи двух кликов на телефоне. Тем не менее наряду с положительными сторонами развития бизнеса: оптимизацией, удобством и доступностью, открылись новые пути и возможности для преступности.

С другой стороны, текущие геополитические волнения не только способствуют увеличению известных киберугроз, затрагивающих бизнес-сферу, но и влекут другие непредсказуемые риски, которые могут привести к достаточно серьезным последствиям. Экономические проблемы, обусловленные ростом цен, инфляцией, санкциями и другими причинами, в дальнейшем могут привести к росту уровня бедности среди населения и, соответственно, уровня преступности (в том числе киберпреступности). В данной статье будут рассмотрены такие последствия пандемии, которые на фоне снижения реальных доходов населения, стремительного увеличения разрыва между доходами и расходами, обеспечили рост преступлений (мошенничества) в финансовом секторе страны.

Всеобщая цифровизация заключается в росте финансовых операций; множестве цифровых

инструментов обработки финансовой информации, в том числе и в удаленном формате. Такие процессы введут к низкому уровню финансовой грамотности среди населения. И этот вопрос тесно связан с первичной и вторичной социализацией, которые в силу столкновения двух противоположных тенденций порождают неопределенность [Василенко, 2018]: одна тенденция обусловлена феноменом спонтанной социализации Ф. Фукуямы – стихийным неуправляемым нарушением правил и норм социума, а вторая вызвана стремлением стабилизировать порядок, закрепленный в стремительно стареющих социальных институтах, уже не адекватных цифровому обществу. Процессу эволюционного развития препятствует, по мнению Ф. Фукуямы, традиционная социализированность [Fukuyama 1995]. А социальные изменения нарастают существенно. Так, например, преступники могут получать информацию о финансах через ребенка, которому многие родители доверяют самостоятельно пользоваться смартфоном или планшетом с предельно раннего возраста.

В период массированной цифровизации возникает потребность в изменении механизмов саморегуляции и форм социального контроля. Согласно М. Фуко, в прошлые эволюционные периоды развития мы наблюдали «общество наказания» с характерными для него формами социального контроля, то есть преступления карались публично и жестоко [Фуко 1999]. Современное общество, смещает акцент с жестокого наказания на вторичную социализацию, на воспитание, осознание своих ошибок [Фуко 1999, с. 15], «охватывая не только тело, но чувства, мысли и поступки человека» [Фуко 1999, с. 63]. В цифровом обществе начинают сбываться тенденции, предсказанные в конце XX в. французским ученым Ж. Делезом о приближении к «обществу контроля» и «мгновенной коммуникации» [Делез, 2004, с. 222–223].

Цифровая социализация предполагает формирование компьютерной грамотности индивидов и населения, освоение ими «цифровой среды». Это стало значимым вызовом для социализации подрастающих поколений, определяющих конкурентные преимущества как отдельных индивидов и организаций, так и целых стран, их перспективы в современных условиях.

Но новые формы контроля, адекватные цифровому обществу, пока не сложились из-за отсутствия цифровых социальных институтов [Василенко, Мещерякова 2021]. Разумеется, цифровая социализация предполагает не только привитие компьютерной грамотности, но и формирование «цифровой среды» с компьютерными технологиями и форматами цифрового контроля. Последние начинают формироваться постепенно. Так, в рамках мероприятий по реализации государственной программы «Информационное общество» выделяются весьма большие финансовые средства и другие ресурсы[1]. В феврале 2020 г. Министерство внутренних дел Российской Федерации сообщило, что в структуре ведомства появились подразделения по борьбе с киберпреступлениями[2]. Ранее такие подразделения создали в Следственном комитете Российской Федерации. Но несмотря на это, уровень мошенничества по-прежнему остается высоким. Злоумышленники пока опережают действия органов власти. Это явление требует более тщательного анализа.

ЦЕЛЬ И МЕТОДЫ ИССЛЕДОВАНИЯ / PURPOSE AND METHODS

В ходе исследования была поставлена задача провести социально- демографический срез, выявить, по отношению к каким категориям населения чаще всего применяется цифровое мошенничество, какова половозрастная структура пострадавших, иными словами, кто чаще становится жертвами цифрового и интернет-мошенничества: женщины или мужчины; к какой категории они относятся, каков их возраст и уровень образования; есть ли зависимость распространения цифрового мошенничества от норм нового гендерного порядка в условиях цифровизации, и по каким вопросам гендерные различия стираются, а по каким сохраняются и почему.

Настоящая тема чрезвычайно мало исследована на теоретическом уровне. Мировое и национальные законодательство о киберпреступности и ИТ-мошенничестве все еще находится в зачаточном состоянии и требует надежной основы. Тем не менее рост негативных последствий интернет-мошенничества по всему миру стимулировал научные исследования по этому вопросу.

В частности, в 1953 г. Д.Р. Кресси опубликовал концепцию «треугольника мошенничества» (англ. Fraud triangle theory) [Cressey, 1954]. В на основании данной теории Л. Коэном и М. Фелсоном

[1] *Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации*. Приказ от 29.04.2016 № 183 (ред. от 14.06.2016) «О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных». Режим доступа: https://digital.gov.ru/ru/documents/5015/?utm_referrer=https %3a %2f %2fyandex.ru %2f (дата обращения: 18.02.2023).

[2] *РИА Новости* (Пятница 7 февраля 2020). В МВД создали подразделения по борьбе с киберпреступлениями. Режим доступа: https://ria.ru/20200207/1564386506.html (дата обращения: 18.02.2023).

в 1979 г. была выдвинута теория рутинных действий, согласно которой для совершения мошеннических преступлений, в том числе с использованием сети «Интернет», в одном и том же месте и в одно и то же время должны быть: 1) «подходящие цели» (наивные и доверчивые клиенты банков, банки, интернет-банкинг, электронные деньги, банковские чеки и дебетовые карты); 2) «мотивированные» правонарушители (низкооплачиваемый банковский персонал, жадные банковские сотрудники и клиенты, безработные выпускники и т.д.); 3) отсутствие эффективных мер защиты (слабая кибербезопасность, слабый внутренний контроль доступа и санкции, то есть отсутствие физических и электронных мер безопасности) [Cohen, Felson, 1979].

Американский исследователь Д.Б. Паркер, родоначальник научных теорий в сфере «киберзлоупотреблений» и автор первого «Справочника по уголовному правосудию» для правоохранительных органов США, понимал под объектом компьютерного преступления отношения, которые обусловливают защищенность / незащищенность компьютерных сетей финансовых организаций [Parker, 1976]. Д.С. Уолл дополняет объект компьютерной информацией, которая функционирует в сетях [Wall, 2007]. Причиной онлайн-преступлений выступает сложность их выявления, так как информация зачастую скрывается пострадавшими [Smith, 2007].

В. Кандпал определяет и представляет достаточно подробную классификацию киберпреступлений: кибер-преследование, преступления против интеллектуальной собственности; бот-сети, передача вируса, взлом сети; кражи интернет-времени, фишинг, голосовой фишинг, кардинг, подмена электронной почты/СМС, межсайтовый скриптинг, кибersквоттинг/сквоттинг, кибервандализм, киберторговля и другие [Kandpal, Singh, 2013].

На этом фоне выделяется публикация В. Шиловой и М. Печалиной, в которой на основании анализа ресурсов интернет-пространства обоснована типология интернет-мошенничества по нескольким основаниям: по методике исполнения, по каналам коммуникации и по сферам воздействия [Шилова, Печалина, 2014].

Приведем эмпирическую базу настоящей работы.

1. Статистические данные. Обращаясь к открытой статистической базе данных Министерства внутренних дел Российской Федерации, отметим, что каждое четвертое преступление совершается с использованием ИТ-технологий. С января по сентябрь 2022 г. зарегистрировано 378,5 тыс. преступлений в сфере компьютерной преступности, при этом 71,2 % совершается путем кражи или мошенничества. В перечень таких деяний входят мошенничества через телефонные звонки, кардинг, фишинг и другие виды киберпреступлений[3].

2. Данные авторского социологического исследования. Метод: анкетный интернет-опрос; объем выборки – 474 человека. Средний возраст респондентов составляет 38 лет и выше, гендерный срез характеризуется равным соотношением мужчин и женщин, 90 % имеют высшее образование.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ / RESULTS

Проанализировав полученные данные, можно сказать, что большинство респондентов сталкивались с цифровым мошенничеством напрямую или с неудачной попыткой украсть у них денежные средства подобным образом. Об этом заявили 86 % респондентов, причем мужчины преобладают в гендерном срезе над женщинами, их доля составляет 62 %.

Согласно полученным результатам, 74 % опрошенных имеют две и более банковских карты, однако они либо не установили защиты по лимитам на снятие средств с карт, либо не владеют последними программами по защите своих средств на картах, что делает их более уязвимыми перед мошенниками. 16 % респондентов «затруднились ответить», что характеризует их осторожность и повышенный уровень недоверия и нежелания делиться своими персональными данными даже в ходе электронного опроса. Из них большинство оказались женщины старше 50 лет – 67 %. Также многие респонденты предпочитают снимать денежные средства в одном месте или в одном и том же отделении банка. Об этом заявило 38 % женщин и 36 % опрошенных мужчин соответственно. 22 % респондентов не задумываются об этом и снимают деньги, где им удобно. Также у 34 % процентов респондентов не установлен лимит на снятие денежных средств с банковской карты, и только у половины опрошенных он имеется, что показывает халатное отношение к своим сбережениям.

Рассмотрим основные виды цифрового мошенничества, а также опишем на основе анализа полученных ответов респондентов сложившуюся ситуацию, попробуем выявить гендерные различия в ответах респондентов по отношению к данной проблематике.

[3] *Министерство внутренних дел Российской Федерации*. Состояние преступности в Российской Федерации за январь – сентябрь 2022 года. Режим доступа: https://мвд.рф/reports/item/33388812/ (дата обращения: 15.02.2023).

Основными видами мошенничества, которые будут более подробно рассмотрены в данной статье, являются:

1) телефонное мошенничество и IP-телефония (от англ. Internet Protocol – «межсетевой протокол»);

2) СМС-мошенничество;

3) фишинг (от англ. fishing – «рыбная ловля, выуживание»);

4) снифферинг (от англ. to sniff – «нюхать» – перехват сообщений);

5) скимминг (от англ. to skim – «бегло прочитывать», «скользить» – кража данных карты).

Перейдем к рассмотрению каждого из вышеперечисленных видов мошенничества и проанализируем степень вовлеченности, процентное соотношение респондентов, столкнувшихся с тем или иным видом цифрового мошенничества, проанализируем пострадавших от того или иного вида мошенничества в гендерном ракурсе.

Телефонное мошенничество и IP-телефония

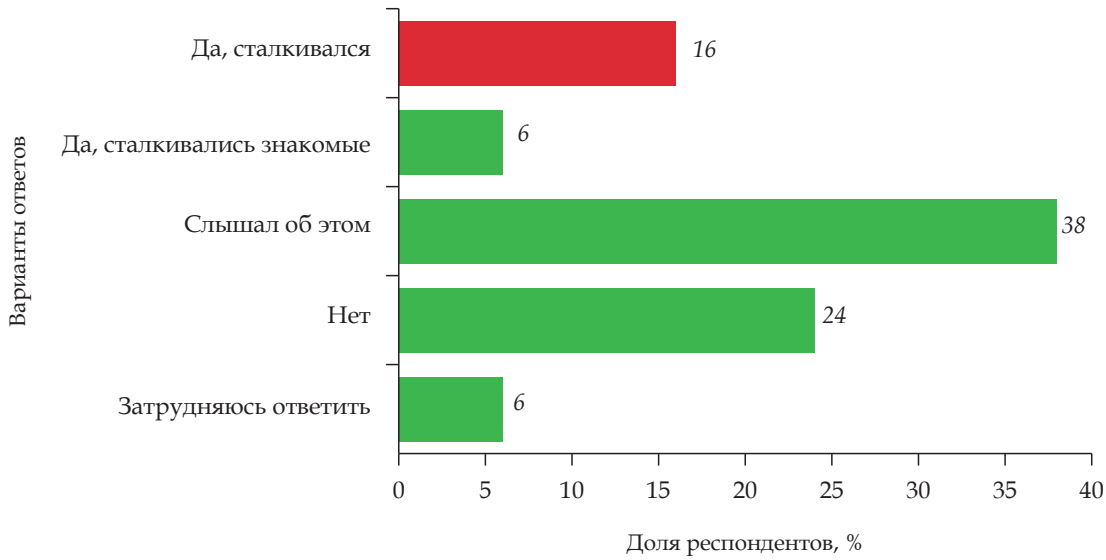
Одним из наиболее часто встречающихся видов цифрового мошенничества является акт по использованию или хищению чужого имущества или приобретению права на чужое имущество путем преступного внедрения в информационную систему или передачи данных через компьютерные сети. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видео-общение по сети «Интернет» или любым другим IP-сетям. Это мошенничество основано на возможности подменять номер абонента, используя IP-телефонию. Если вдаваться в технические подробности, в сотовых сетях номер не запрашивается, а передается коммутатором вызывающего абонента. Когда звонок идет через VoIP-шлюз, можно подставить любой номер.

Исходя из проведенного опроса, было выявлено, что 16 % респондентов лично сталкивались с подобным видом мошенничества. 6 % процентов пользователей слышали об этом от знакомых. Однако 24 % абсолютно не знакомы с данным видом социальной деструкции (рис. 1).

Рассмотрение полученных данных в гендерном ракурсе показывает нам следующую картину: с таким видом мошенничества из 16 % респондентов, ответивших «да», сталкивалось 68 % мужчин. Это позволяет сделать вывод о том, что женщины, независимо от возраста, в данном вопросе более осторожны и благоразумны.

Более того, пользователи заявляют, что получают звонки от мошенников периодически или несколько раз. Об этом свидетельствует представленная ниже диаграмма (рис. 2).

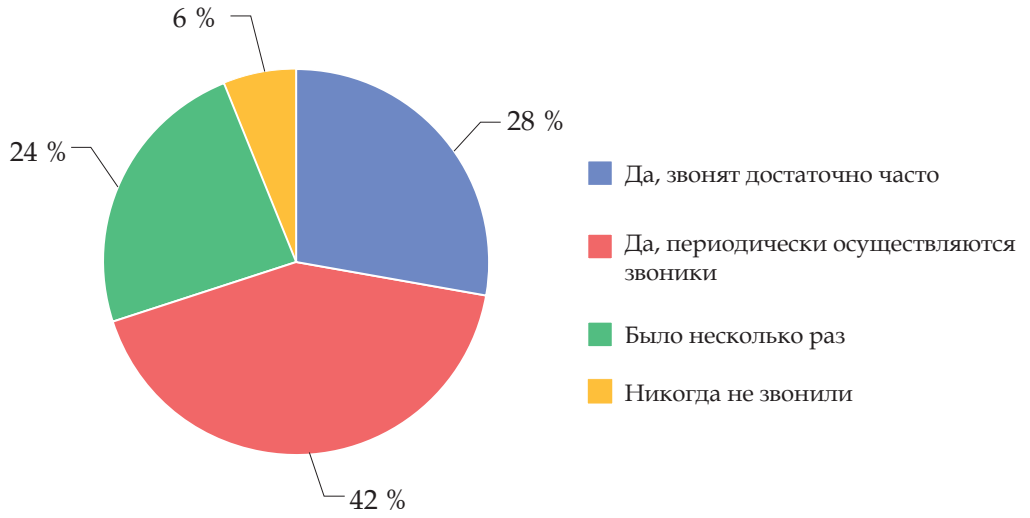
Необходимо отметить, что 20 % респондентов теряли деньги от такого вида мошенничества, а большинство сталкивалось с неудачной попыткой украсть деньги – 60 % (рис. 3). В ответах респондентов было также выявлено преобладание мужчин – 64 % и 59 % женщин соответственно. Это позволяет сделать вывод о том, что женщины более рациональны и осторожны.



Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

***Рис. 1.* Распределение ответов по вопросу несанкционированного использования услуг связи путем перепрограммирования**

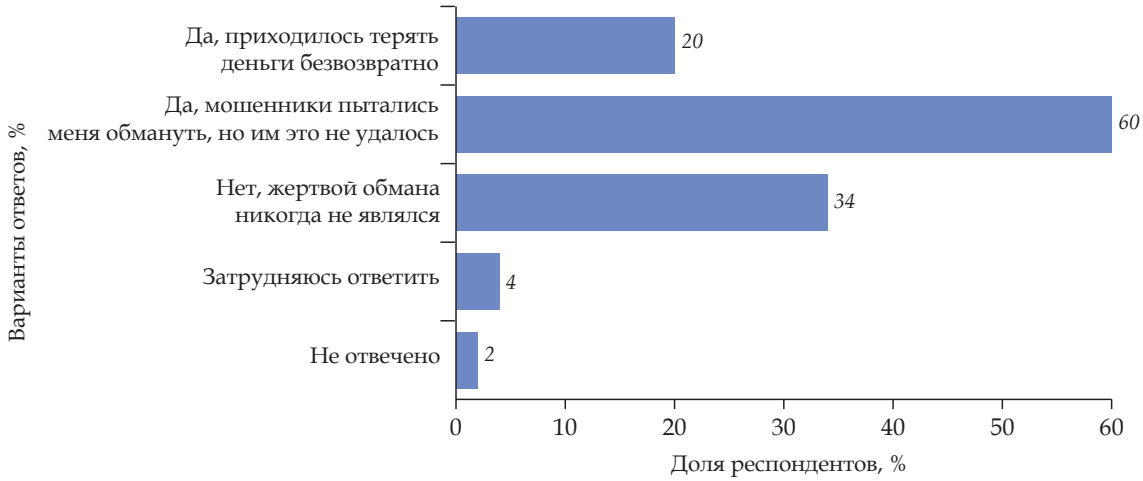
Fig. 1. Answers distribution on the unauthorized use of communication services by reprogramming issue



Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

***Рис. 2.* Распределение ответов на вопрос: «Вам звонили мошенники, представляясь сотрудниками банков, кредитных и страховых компаний, медицинскими работниками и даже вашими знакомыми?»**

Fig. 2. Distribution of answers to the question: "Did fraudsters call you, posing as employees of banks, credit and insurance companies, medical professionals and even your acquaintances?"



Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

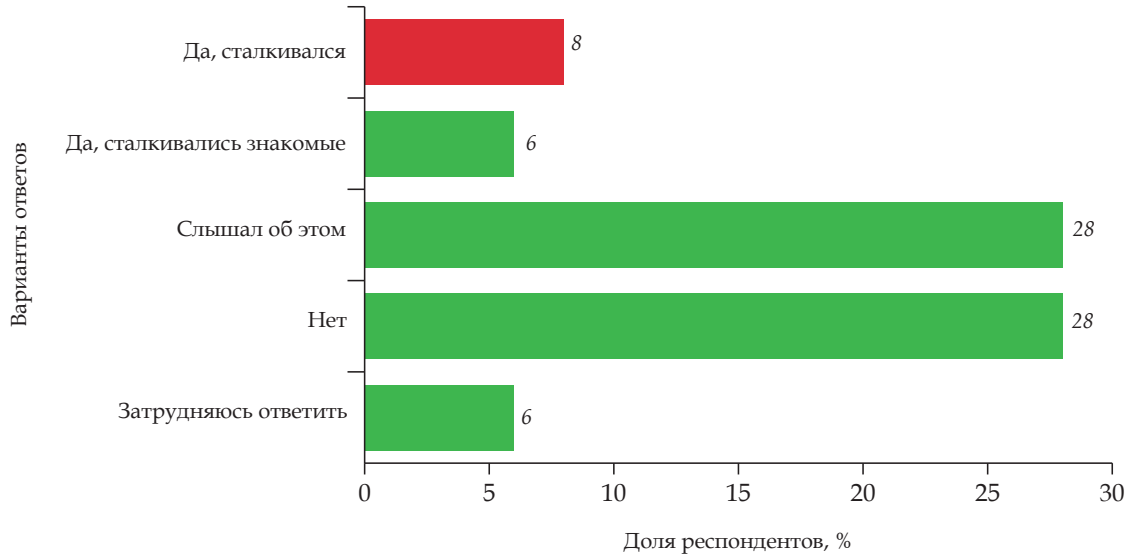
***Рис. 3.* Распределение ответов на вопрос: «Были ли вы жертвой телефонного или интернет-мошенничества?»**

Fig. 3. Answers distribution to the question: "Have you been a victim of telephone or internet fraud?"

СМС-мошенничество

Далее поговорим о второй разновидности цифрового мошенничества – СМС-мошенничестве, которое схоже с мошенничеством с использованием IP-телефонии. Данная разновидность представляет собой сбор данных через предложение владельцу денежных средств перечислить какую-то сумму с помощью СМС-сообщения. При этом преступники заранее не владеют информацией, обладает ли этот абонент какими-либо средствами. Для выявления необходимых данных человеку отправляется сообщение, что его карта заблокирована или что ее работа приостановлена, и предлагается по телефону совершить какие-то действия в банкомате, нажать названные кнопки, что приводит к перечислению денег на счета мошенников.

Описывая полученные данные (рис. 4), мы видим, что респонденты имели меньше личного опыта с таким видом мошенничества, чем с предыдущим – 8 % опрошенных. Однако по-прежнему большой остается совокупность респондентов, которая слышала об этом – 28 %. Из 8 % респондентов, которые ответили «Да, сталкивался» – 60 % женщин. И здесь мы видим совершенно другой гендерный ракурс. При этом виде мошенничества большинством пострадавших стали женщины.

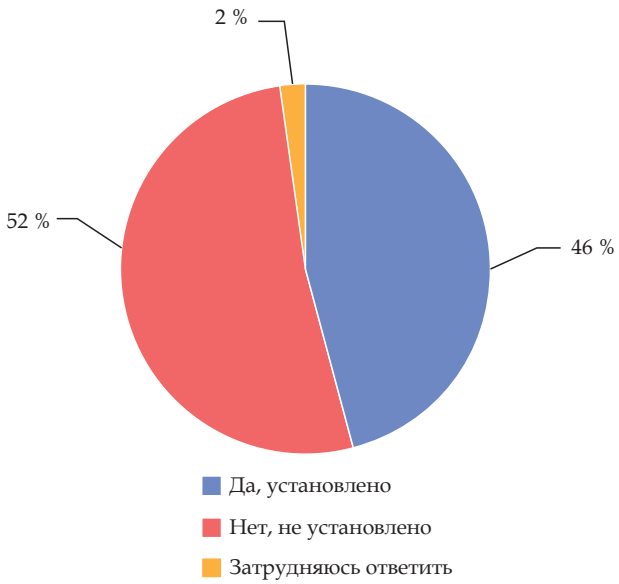


Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

***Рис. 4.* Распределение ответов на вопрос об изъятии средств с помощью СМС-мошенничества**

Fig. 4. Distribution of answers to the question about the withdrawal of funds using SMS fraud

В ходе исследования выяснилось, что половина респондентов – 52 % – не защищают свои мобильные телефоны при помощи блокировщиков подозрительных номеров, тем самым подвергают себя большим финансовым рискам (рис. 5). Кроме того, 18 % не знали о том, что мошенники могут воспользоваться стандартным номером банка или же номерами близких им знакомых.



Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

***Рис. 5.* Распределение ответов на вопрос: «Установлено ли у вас на телефоне приложение, блокирующее подозрительные номера?»**

Fig. 5. Answers distribution to the question: "Do you have an application that blocks suspicious numbers on your phone?"

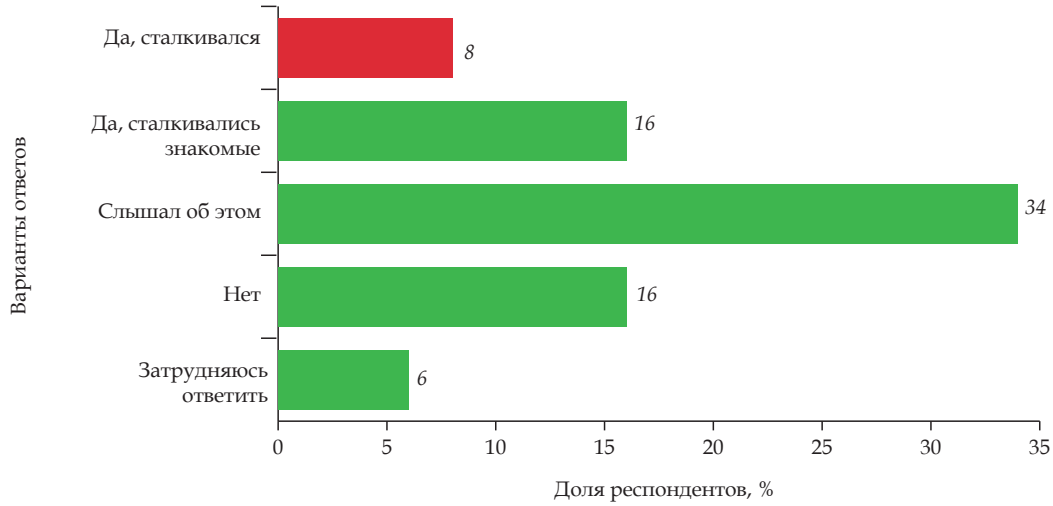
Фишинг

Фишинг представляет собой совокупность методов доступа к личным финансовым данным (логин и пароль от личного кабинета на сайте банка). Осуществляется это с помощью вирусных или DDoS-атак (от англ. Distributed Denial of Service – «распределенный отказ в обслуживании»). А необходимые данные выуживаются с помощью контакта с человеком, отличающимся наивностью и слабым знанием компьютерных технологий, который, например, отправляет свою парольную информацию в ответ на подставное письмо якобы от известной фирмы.

Данная методика мошенничества наиболее актуальна сегодня. Многие работодатели, перенося офлайн процессы на удаленную форму взаимодействия, выбирают основным источником коммуникации электронную почту, где пользователи могут столкнуться с мошенниками. В по данным «Лаборатории Касперского», в 2021 г. от фишинговых атак пострадали 8,2 % пользователей. «Атаки на клиентов платежных систем составили треть от всех случаев финансового фишинга. Еще 26,6 % финансовых фишинговых схем пришлись на долю банковских сервисов, с которыми связаны 11,1 % от общего числа фишинговых инцидентов»[4].

Однако данные авторского исследования показывают, что в действительности только малый процент опрошенных столкнулся с фишингом лично – 8 %, а процент людей, которые имеют печальный опыт своих знакомых, намного выше

[4] *Securelist.* Финансовые киберугрозы в 2021 году. Отчет «Лаборатории Касперского». Режим доступа: https://securelist.ru/financial-cyberthreats-in-2021/104553/ (дата обращения: 18.02.2023).



Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

Рис. 6. Распределение ответов на вопрос, сталкивались ли респонденты с фишингом

Fig. 6. Answers distribution to the question whether respondents have experienced phishing

в случае сравнения с другими методами цифрового мошенничества – порядка 16 %. Также мы продолжаем наблюдать уже сложившуюся тенденцию, показывающую, что большинство респондентов (34 %) также, как в указанных выше примерах, знакомы с данным видом мошенничества.

Снифферинг

Еще одним распространенным методом, которым часто пользуются мошенники, является снифферинг. Под этим понятием понимают перехват данных при помощи специального программного обеспечения (сниффера). Оно анализирует входящий и исходящий трафик компьютера и собирает данные, причем многие ошибочно полагают, что стать участником такого мошенничества можно лишь при подключении к Интернету через незащищенные точки доступа, например в кафе или других общественных местах, в то время как пользователь любого интернет-магазина или банковской системы может пострадать от этого вида мошенничества. Хакеры с помощью специальной программы могут запросто узнавать данные банковских карт или данные входа в сервисы платежных систем или онлайн-банкинга. По информации специалистов «Лаборатории Касперского», ситуация развивается достаточно динамично. Так в списке «Топ-10 стран и регионов» Япония в 2020 г. заняла первое место, хотя в предыдущем году она «не входила даже в первую десятку»[5].

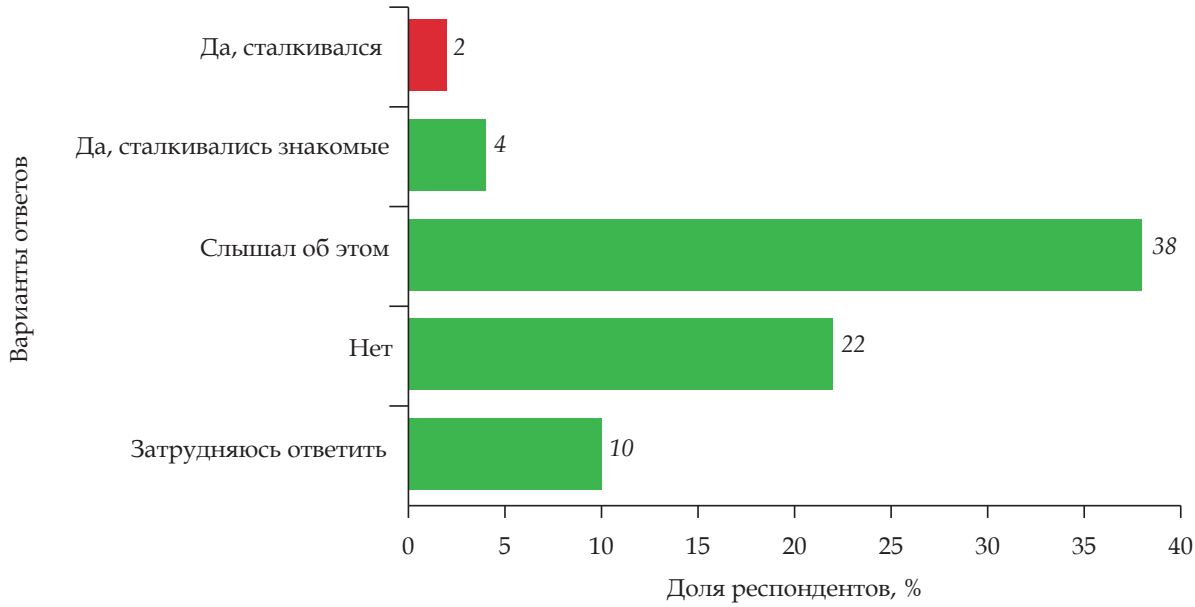
Стать жертвой снифферинга достаточно просто. Однако из опроса мы видим, что большинство респондентов не сталкивались с данным видом мошенничества лично – 2 %. Большинство из них слышали об этом (38 %), а 22 % опрошенных не сталкивались с ним вовсе, что указывает на низкую осведомленность в этой области цифрового мошенничества, а также на отсутствие достаточно полной информации об этом явлении; люди могут даже и не предполагать о том, что мошенники воспользовались их данными (рис. 7).

Из приведенной на рисунке 8 диаграммы следует, что 52 % респондентов, отвечая на вопрос об информированности о средствах антивирусной защиты от мошенников, имеют представления о том, как работает такая защита. 18 % не имеют понятия, как она работает, а 22 % и вовсе не знают об этом. Таким образом, 40 % респондентов не имеют представления о том, что это за явление, как работают мошенники и какие существуют способы защиты от снифферинга.

Скимминг

Скимминг – это считывание данных с магнитной полосы банковской карты и ПИН-кода. Затем изготавливается поддельная банковская карта и крадутся деньги, а их списание осуществляется с настоящего счета клиента банка. Чтобы избежать скимминга, во-первых, желательно осуществлять снятие наличных средств непосредственно в офисах банков, а если это невозможно, надо хорошо осмотреть банкомат до начала использования. Во-вторых, пользоваться бесконтактной или специально предназначенной картой, на которую будет предварительно переведена только разово необходимая сумма. При вводе ПИН-кода желательно прикрывать клавиши рукой.

[5] Там же.



Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

***Рис. 7.* Распределение ответов по вопросу снифферинга – перехвата данных специальной компьютерной программой**

Fig. 7. Answers distribution on the sniffering issue – interception of data by a special computer program

Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

***Рис. 8.* Распределение ответов на вопрос: «Знаете ли Вы о средствах антивирусной защиты от мошенничества?»**

Fig. 8. Distribution of answers to the question: "Do you know about anti-virus protection against fraud?"

ОБСУЖДЕНИЕ / DISCUSSION

Рассмотрев основные виды мошенничества и статистику распределения ответов, можно сделать вывод, что участники опроса сталкивались с различными видами правонарушений в цифровой среде достаточно часто, многие имеют личный опыт потери денежных средств из-за цифровых мошенников.

Результаты исследования показали, что на сегодняшний день цифровое мошенничество процветает. От него становится все сложнее защититься, так как развиваются его новые виды и формы. В ходе исследования также выяснилось, что мужчины в большей степени сталкиваются с мошенниками и страдают от их действий. Также мужчины более доверчивы и раскрывают свои данные в Интернете, например, о количестве своих дебетовых карт в опросе.

Более того, важнейшим фактором сохранения денежных средств является цифровая и финансовая грамотность, которая, согласно проведенному опросу, до сих находится на достаточно низком уровне. Например, многие респонденты по сей день не задумаются об установлении лимитов снятия

денежных средств со своих карт, еще одна значительная часть опрошенных пользуется большим количеством банковских карт, что повышает риски попадания данных к мошенникам. Около половины опрошенных не понимают, как их защищают антивирусные программы. Следовательно, они не осмысливали вопросы собственной цифровой безопасности, предоставляя цифровому мошеннику важные личные данные. Кроме того, как уже освещалось выше, многие родители невольно передают доступ к своим данным через своих несовершеннолетних детей, которые используют гаджеты взрослых для игр и учебы.

Анализ распределения ответов по гендерному признаку позволил выявить, по отношению к каким категориям населения чаще всего применяется цифровое мошенничество, каков возраст пострадавших, кто чаще становился жертвами различных видов Интернет-мошенничества. Исследование показало уязвимость в первую очередь мужской половины населения старше 40 лет. Мужчины более доверчивы и охотно делятся своими данными в Интернете, например, о количестве своих дебетовых карт в опросе. Это отчасти объясняется тем, что взрослое население Российской Федерации выросло и прошло свое становление в условиях СССР, который гарантировал своим гражданам защиту своих личных финансов, уверенность в сохранности своих накоплений и являлся гарантом финансовой безопасности, а также брал на себя все риски. Этим и объясняется некая инфантильность, наивность взрослого поколения, которой и пользуются мошенники. Люди же более взрослого поколения, как правило, после 75 лет, гораздо реже используют мобильные приложения для оплаты со своих электронных карт, предпочитая либо использование наличных денег для оплаты, либо использование одного и тот же банка для осуществления своих операций со счетами в формате офлайн без использования телефонов.

Очевидным является то, что в современных условиях развития интернет-мошенничества, людей необходимо постоянно информировать о способах защиты от него. Особенную актуальность это приобретает в сегодняшних реалиях, когда большинство людей отправлено на дистанционную работу и учебу. Исследование показало, что только 44 % респондентов информированы о видах мошенничества в достаточной степени, чтобы защититься от современных интернет-мошенников. В качестве первоочередных мер необходимо повышать уровень финансовый и цифровой грамотности населения. Для этого органы государственной власти совместно со средствами массовой информации должны активно распространять информацию о видах мошенничества и способах защиты от них.

ЗАКЛЮЧЕНИЕ / CONCLUSION

Таким образом, чтобы защитить граждан от современных мошенников, необходимо повышать их уровень финансовой и цифровой грамотности. Особое внимание необходимо обратить на то, что соблюдение нескольких основных простых правил может повысить степень собственной защиты от любого вида мошенничества. Эти правила следующие:

– не отвечать на звонки с незнакомых номеров;
– не предавать никому свои личные данные;
– следить за своими банковскими картами, особенно при их использовании;
– стараться не использовать общедоступные точки доступа в сеть «Интернет»;
– быть бдительным и понимать, что век технологий и век возможностей несет не только положительные аспекты, но и отрицательные.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Василенко Л.А. (2018). «Нормальная аномия»: трансформация институтов в сложном обществе // Научный результат. Социология и управление. Т. 4. № 3. С. 45–56. https://doi.org/10.18413/2408-9338-2018-4-3-0-4

Василенко Л.А., Кашина М.А. (2015). Будущее гендерной политики в глобализирующемся обществе: российский кейс // Управленческое консультирование. № 9 (81). С. 112–119.

Василенко Л.А., Мещерякова Н.Н. (2021). Социология цифрового общества: монография. Томск: Изд-во ТПУ.

Делез Ж. (2004). Переговоры, 1972 – 1990: [собрание писем и статей]. Пер. с фр. Быстров В.Ю. СПб.: Наука. 232 с.

Кривоухов А.А. (2020). Личная ответственность как основа информационной безопасности личности в цифровом обществе // Цифровое общество – новый формат социальной реальности: структуры, процессы и тенденции развития: материалы Всероссийской научной конференции XIV Ковалевские чтения, Санкт-Петербург, 12–14 ноября 2020 г.; отв. ред. Скворцов Н.Г., Асочаков Ю.В. СПб.: Скифия-принт. 603 с.

Фуко М. (1999). Надзирать и наказывать. Рождение Тюрьмы. Пер. с фр. Наумов В. М.: Ad Marginem. 479 с.

Шилова В.А., Печалина М.К. (2014). Интернет-мошенничество как значимая характеристика «экранного мира» сети // Наука телевидения. № 11. С. 324–342.

Baz R., Shamsiah Samsudin R., Che-Ahmad A. (2017). The role of internal control and information sharing in preventing fraud in the Saudi banks // Journal of Accounting and Financial Management. V. 3, no. 1. Pp. 7–13.

Cohen L.E., Felson M. (1979). Social change and crime rate trends: A routine activity approach // August American Sociological Review. V. 44, no. 8. http://dx.doi.org/10.2307/2094589

Cressey D.R. (1954). The differential association theory and compulsive crimes // Journal of Criminal Law and Criminology. V. 45, no. 1. Pp. 29–40.

Fukuyama F. (1995). Trust: The social virtues and the creation of prosperity. New York: Free Press. 457 p.

Kandpal V., Singh R.K. (2013). Latest face of cybercrime and its prevention in India // International Journal of Basic and Applied Sciences. V. 2, no. 4, pp. 150–156.

Manivannan A., Moorthy D. (2020). Cyber attacks in the banking industry. Fern Barrow: Faculty of Science and Technology Bournemouth. http://dx.doi.org/10.13140/RG.2.2.16664.01282

Parker D.B. (1976). Computer abuse perpetrators and vulnerabilities of computer systems // AFIPS ‘76 (1899).

Smith R.G. (2007). Crime control in the digital age: An exploration of human rights implications // International Journal of Cyber Criminology. V. 1, no. 2. Pp. 167–179.

Tade O., Adeniyi O. (2020). Dimensions of electronic fraud and governance of trust in Nigeria’s cashless ecosystem // International Journal of Offender Therapy and Comparative Criminology. V. 64. Art. num. 0306624X2092802. http://dx.doi.org/10.1177/0306624X20928028

Wickramanayake B., Geeganage D. K., Ouyang C., Xu Y. (2020). A survey of online card payment fraud detection using data mining-based methods // ArXiv. V. arXiv:2011.14024. https://doi.org/10.48550/arXiv.2011.14024

REFERENCES

Baz R., Shamsiah Samsudin R., Che-Ahmad A. (2017), “The role of internal control and information sharing in preventing fraud in the Saudi banks”, *Journal of Accounting and Financial Management*, vol. 3, no. 1, pp. 7–13.

Cohen L.E., Felson M. (1979), “Social change and crime rate trends: A routine activity approach”, *American Sociological Review*, vol. 44, no. 8, http://dx.doi.org/10.2307/2094589

Cressey D.R. (1954), “The differential association theory and compulsive crimes”, *Journal of Criminal Law and Criminology*, vol. 45, no. 1, pp. 29–40.

Deleuze G. (2004), *Conversations, 1972–1990: [collection of letters and articles] [Peregovory, 1972–1990: [sobranie pisem i statej]*, Trans. from French Bystrov V.Yu., Nauka, St. Petersburg, Russia (in Russian).

Foucault M. (1999), *Surveiller et punir. Naissance de la prison [Nadzirat’ i nakazyvat’. Rozhdenie tyur’my]*, Trans. from Franch Naumov V., Ad Marginem, Moscow, Russia (in Russian).

Fukuyama F. (1995), *Trust: The social virtues and the creation of prosperity*, Free Press, New York, US.

Kandpal V., Singh R.K. (2013), “Latest face of cybercrime and its prevention in India”, *International Journal of Basic and Applied Sciences*, vol. 2. no.4, pp. 150–156.

Krivoukhov A.A. (2020), “Personal responsibility as the basis of personal information security in a digital society” [“Lichnaya otvetstvennost’ kak osnova informacionnoj bezopasnosti lichnosti v cifrovom obshchestve”], In: Skvorcov N.G., Asochakov Yu.V. (eds.) *Digital society – a new format of social reality: structures, processes and development trends: Proceedings of the All-Russian Scientific Conference XIV Kovalev Readings[Cifrovoe obshchestvo – novyj format social’noj real’nosti: struktury, processy i tendencii razvitiya: materialy Vserossijskoj nauchnoj konferencii XIV Kovalevskie chteniya], St. Petersburg, November 12–14, 2020*, Skifiya-print, St. Petersburg, Russia (in Russian).

Manivannan A., Moorthy D. (2020), *Cyber attacks in the banking industry*, Faculty of Science and Technology Bournemouth, Fern Barrow, UK, http://dx.doi.org/10.13140/RG.2.2.16664.01282

Parker D.B. (1976), “Computer abuse perpetrators and vulnerabilities of computer systems”, *AFIPS ‘76* (1899).

Smith R.G. (2007), “Crime control in the digital age: An exploration of human rights implications”, *International Journal of Cyber Criminology*, vol. 1, no. 2, pp. 167–179.

Shilova V.A., Pechalina M.K. (2014), “Internet fraud as a significant characteristic of the ‘screen world’ of the network” [Internet-moshennichestvo kak znachimaya harakteristika «ekrannogo mira» seti], *Nauka televideniya*, no. 11, pp. 324–342 (in Russian).

Tade O., Adeniyi O. (2020), “Dimensions of electronic fraud and governance of trust in Nigeria’s cashless ecosystem”, *International Journal of Offender Therapy and Comparative Criminology*, vol. 64, art. num. 0306624X2092802, http://dx.doi.org/10.1177/0306624X20928028

Vasilenko L.A. (2018), "'Normal anomie': transformation of institutions in a complex society", *Research result. Sociology and management*, vol. 4, no. 3, pp. 45–56, https://doi.org/10.18413/2408-9338-2018-4-3-0-4 (in Russian).

Vasilenko L.A., Kashina M.A. (2015), " The future of gender policies in the globalized world: Russian case", *Administrative Consulting*, no. 9(81), pp. 112–119 (in Russian).

Vasilenko L.A., Meshcheryakova N.N. (2021), *Sociology of digital society [Sociologiya cifrovogo obshchestva]: monograph*, National Research Tomsk Polytechnic University Publ. House, Tomsk, Russia (in Russian).

Wickramanayake B., Geeganage D. K., Ouyang C., Xu Y. (2020), "A survey of online card payment fraud detection using data mining-based methods", *ArXiv*, vol. arXiv:2011.14024, https://doi.org/10.48550/arXiv.2011.14024