Максим Юрьевич СЕМЁНОВ[1]
Полина Владимировна КАЧАНОВА[2]

УДК 343.721

МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ: ОТНОШЕНИЕ МОЛОДЕЖИ

[1] кандидат социологических наук,
доцент кафедры общей и экономической социологии,
Тюменский государственный университет
m.y.semenov@utmn.ru

[2] бакалавр социологии, Тюменский государственный университет
polinak74@mail.ru

Аннотация

В современных условиях постоянной интеграции информационных технологий в повседневную жизнь человека обостряется проблема формирования и проявления новых рисков при использовании сети Интернет. Согласно международным и всероссийским данным, отмечается значимый рост числа киберпреступлений, постоянно появляются новые формы интернет-мошенничества и увеличивается фактический ущерб от противоправных действий в виртуальном пространстве. Представители молодежи как наиболее активные пользователи глобальной сети становятся объектами деятельности мошенников в Интернете.

Цель исследования — изучить отношение представителей современной молодежи к мошенничеству в Интернете, а также различным формам его проявления. Теоретико-методологический анализ исследования осуществлен на базе теорий девиантного поведения и теории манипуляции. Для получения первичных социологических данных в работе использован метод онлайн-опроса молодежи, проживающей в г. Тюмень. Опрос проведен летом 2020 года.

По результатам исследования определено отношение представителей современной молодежи к интернет-мошенничеству. Зафиксировано, что подавляющее большинство (85%)

Цитирование: Семёнов М. Ю. Мошенничество в сети Интернет: отношение молодежи / М. Ю. Семёнов, П. В. Качанова // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2021. Том 7. № 3 (27). С. 71-85. DOI: 10.21684/2411-7897-2021-7-3-71-85

молодых людей сталкивались с различными проявлениями мошенничества в Интернете, при этом каждый четвертый (26%) респондент пострадал от данного негативного социального явления. Наиболее часто мошенничество в сети Интернет молодежью фиксируется в виртуальных социальных сетях при использовании технологий социальной инженерии. Кроме того, не все формы интернет-мошенничества хорошо известны молодежи, например, мошенничество с использованием интернет-банкинга знают чуть менее половины опрошенных. В общем по выборке, молодые люди негативно оценивают интернет-мошенничество как явление, хотя существуют некоторые различия во мнениях в зависимости от их личного жизненного опыта. В заключении статьи определены возможные перспективы дальнейших исследований в данной области.

Ключевые слова

Интернет, мошенничество, киберпреступность, социальная инженерия, цифровая грамотность, молодежь, социальные сети.

DOI: 10.21684/2411-7897-2021-7-3-71-85

Введение

Мошенничество как явление выступает одним из наиболее распространенных видов социальных девиаций негативного характера. Технологический уровень развития за несколько последних десятилетий позволил виртуализировать практики отклоняющегося поведения, в том числе определил появление интернет-мошенничества. Только в США по данным Федерального бюро расследований за период с 2015-го по 2019-й год количество зафиксированных рекламаций по поводу актов мошенничества в Интернете возросло с 288 до 467 тыс., при этом сумма финансового ущерба увеличилась с 1,1 до 3,5 млрд долларов [17]. Помимо того, мировой объем экономического ущерба от киберпреступности в целом за последние 5 лет увеличился более чем в 6 раз (с 445 млрд долларов в 2016 г. и до 3 трлн долларов в 2020 г.) [9]. Учитывая вышеперечисленные факты, можно сделать вполне обоснованный вывод о том, что данное социальное явление становится новым вызовом цивилизации в эпоху цифрового общества.

Ситуация, связанная с проявлением практик интернет-мошенничества на территории России, может быть охарактеризована как сложная и обладающая неутешительной динамикой. По данным отчета Министерства внутренних дел Российской Федерации, в период с января по июнь 2020 года было зарегистрировано 222,5 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 91,7% больше, чем за аналогичный период 2019 года. На данный момент удельный вес данного типа преступлений в стране составляет 22,3% (для сравнения — 11,6% в 2019 году) [11]. Из этого следует, что за последний год можно отметить значимое увеличение доли интернет-мошенничества в общей структуре зарегистрированных деяний неправомерного характера на территории РФ. В связи с чем возникает вполне логичный вопрос о том, чем обоснован такой всплеск количества мошенничества в интернет-пространстве в России в 2020 году.

Помимо того, важно понимать, каким образом это сказалось на восприятии и отношении различных социальных групп к данному явлению.

В процессе анализа приведенной выше официальной статистики важно понимать, что она имеет специфическое ограничение, так как отражает лишь зафиксированные факты интернет-мошенничества. Это определено рядом причин. Во-первых, люди пострадавшие от киберпреступности, по мнению экспертов, зачастую не обращаются в полицию, так как принимают вину на себя [5]. Во-вторых, учитывая медианный ущерб от удаленного типа мошенничества, который, по данным за 2018 год, составил 5 тыс. рублей [6, с. 4], пострадавшие могут не считать потерянные средства достаточно значительными для контакта с полицией. В-третьих, недостаточный уровень доверия населения к деятельности правоохранительных органов. В конечном счете это негативно сказывается на формировании установок ко взаимодействию с полицией при наступлении случая удаленного мошенничества. Таким образом, прорисовывается потребность как со стороны общества, так и со стороны социальных институтов, отвечающих за общественную безопасность, в наличии дополнительных способов выявления возникающих практик интернет-мошенничества. При этом крайне важно, чтобы они носили не констатирующий (отмечающий постфактум), а превентивный характер распознавания рисков киберпреступности, ее постоянно трансформирующихся форм.

Существует множество известных способов мошенничества в Интернете. Наиболее распространенными являются такие мошеннические практики, как фишинг (хищение личных данных), онлайн-продажи товаров и услуг, мошенничество в сфере интернет-банкинга. Фишинг как наиболее часто встречающаяся форма мошенничества в Интернете представляет собой способ хищения персональных данных при помощи фальсификации различных сайтов. Однако, по мнению экспертов Group-IB [16], такая форма мошенничества в Интернете в последнее время трансформируется в более сложный способ (кроличья нора), в котором исправлены слабые места классического фишинга. Среди актуальных практик мошенничества в Интернете можно отметить и букмекерские сайты, онлайн-казино, которые также работают по фишинговой схеме. Такие схемы достаточно серьезно распространены на различных тематических сайтах, что привлекает внимание их посетителей.

Разновидности мошеннических схем в Интернете находятся в процессе постоянной трансформации. Особенно это становится заметным в периоды общественных кризисов или сложных социально-экономических периодов, таких как, например, пандемия новой коронавирусной инфекции. Так, в период мировой пандемии, как отмечает Ю. Н. Руф [10], появились такие новые формы мошенничества, как ложные рассылки о необходимости оплаты штрафа за несоблюдение самоизоляции, комиссии за получение государственных выплат, фиктивные предложения о различных товарах («чудо-таблетках» от Covid-19, фильтры, очистители воздуха) и многое другое. Иными словами, мошенничество в Интернете приобретает уникальные черты для каждого пользователя, превращая обезличенный продукт мошеннических действий в персонифицированный,

что усложняет его идентификацию и впоследствии может привести к увеличению негативных рисков использования виртуального пространства в повседневности индивидов.

Ни для кого не секрет, что наиболее вовлеченными в использование Интернета и практики интернет-коммуникаций являются представители молодого поколения. В связи с этим именно они могут одними из первых сталкиваться с новыми формами мошенничества в Интернете, быть подвержены его негативным последствиям, самостоятельно вырабатывать способы защиты и минимизации рисков при попытках стать жертвой действий неправомерного характера в онлайне. Таким образом, целью данной статьи является анализ отношения представителей современной молодежи к мошенничеству в Интернете, а также различным формам его проявления.

Методология исследования

Исследование практик интернет-мошенничества обладает не только практической значимостью, с целью минимизации рисков, возникающих при использовании глобальной сети, но и теоретической актуальностью, так как объект исследования находится на стыке ряда научных дисциплин. В первую очередь, мошеннические действия в Интернете как объект исследования можно встретить в работах юридического профиля. Представители права зачастую разбирают типы интернет-мошенничества, его криминологические аспекты, методику и проблемы расследования. Помимо того, данная тема привлекает специалистов из области информационных технологий, которые обращают внимание на технологическую специфику реализации мошеннических действий в Интернете, а также технические возможности их предупреждения и информационной безопасности. Вместе с тем мошенничество в Интернете хоть и находит отражение в работах социологов, однако имеет низкую степень как теоретико-методологической, так и практико-эмпирической разработанности.

Интернет-мошенничество с позиции социологического подхода возможно рассматривать как форму девиантного (асоциального) поведения индивида, обладающую противоправным характером и имеющий глобальный географический охват. Однако саму природу мошеннических действий в теоретическом плане с точки зрения социологии считаем возможным изучать сквозь призму ряда научных концепций. В первую очередь, можно использовать теорию аномии (Э. Дюркгейм [3], Р. Мертон [8]), которая подразумевает взаимосвязь количества фактов отклоняющегося поведения в обществе и наличия затяжных кризисов социального, политического и экономического характера, приводящих к конфликту социальных норм. Вместе с тем может быть использована концепция подражания (Ж. Г. Тард), согласно которой субъекты (акторы) мошенничества стали таковыми в связи со спецификой их окружения в наиболее активные периоды социализации.

Отдельно для анализа мошеннических действий в виртуальном пространстве можно использовать теорию манипуляции (Г. Шиллер [13], С. Г. Кара-Мурза [4], Е. Л. Доценко [2]), раскрывающую специфические манипулятивные технологии,

которые применяют мошенники при взаимодействии с потенциальной жертвой в виртуальном пространстве. Согласно теориям манипуляции, все мошенничество основано на действиях манипулятивного характера с целью присвоения чужого имущества. Помимо того, в процессе теоретико-методологического рассмотрения интернет-мошенничества приемлемо использовать целый пул социологических теорий, связанных с описанием феномена жертвы. Виктимиологический подход необходим для определения социальных групп, наиболее подверженных негативным рискам интернет-мошенничества.

Вместе с использованием разработанных и перечисленных теоретических концепций для исследования интернет-мошенничества следует обратиться к имеющейся эмпирической практике. Все имеющееся данные можно разделить на две основные группы.

В первую группу входят аналитические отчеты, статистические сборники, сайты, относящиеся к специализированным ведомствам, министерствам, службам и организациям, которые аккумулируют информацию о мошенничестве в Интернете. Подобные данные можно найти в открытом доступе по различным странам мира. К примеру, достаточно интересным представляется Австралийский опыт, где на государственном уровне комиссией по конкуренции и защите прав потребителей создан специализированный портал Scamwatch, цель которого помочь распознать, избежать и сообщить о мошенничестве в Интернете [19]. В США можно выделить ежегодные отчеты спецслужб по тематике мошенничества в Интернете. В Российской Федерации подобная информация имеется в открытых данных, публикуемых Министерством внутренних дел РФ или прокуратурой России. Благодаря таким ресурсам можно проанализировать как локальную, так и международную динамику зафиксированных фактов интернет-мошенничества. Помимо того, представленные данные демонстрируют соотношение различных практик виртуального мошенничества, превалирующего в той или иной стране.

Вторая группа практических данных включает в себя прикладные исследования, которые так или иначе затрагивают тему интернет-мошенничества. Зачастую в прикладных исследованиях виртуального пространства используют индикатор цифровой грамотности, что напрямую связано с рисками мошенничества в виртуальной сети. Именно наличие цифровой грамотности обеспечивает безопасное использование различных интернет-площадок и ресурсов.

Методология исследования цифровой грамотности населения, основанная на индексном анализе ее структурных компонентов, одним из которых выступает цифровая безопасность, обозначенная в рамках реализации программы обучения граждан цифровым навыкам Европейской Комиссией [14]. По данной методологии проводятся исследования и на территории России. Так, в начале 2020 года аналитический центр НАФИ провел всероссийский опрос населения, в результате чего выявлены определенные различия в цифровой грамотности относительно таких показателей респондентов, как возрастная группа, вид занятости, пол и тип населенного пункта [12]. Так, высочайший уровень цифровой

грамотности был зафиксирован среди работающих студентов, а самый низкий — среди неработающих пенсионеров.

Наличие высокого уровня цифровой грамотности может быть прообразом для формирования новой и немаловажной в современных условиях компетенции — цифровой безопасности. Так, Н. Д. Берман отмечает, что цифровая безопасность пользователя сети Интернет заключается в «способности обеспечить защиту и конфиденциальность персональных данных; в уровне культуры общения в социальных сетях, соблюдении этических и правовых правил при размещении контента; а также в способности защитить себя от уловок интернет-мошенников» [1, с. 37]. Таким образом, в настоящее время становится все более актуальным социальный запрос на обладание знаниями и навыками безопасности в виртуальном пространстве.

Анализ интернет-мошенничества может стать составляющей частью больших социологических опросов, связанных с изучением преступности в целом, как это показано в исследовании Института проблем правоприменения «Преступность и виктимизация в России» [6]. Помимо того, существуют и отдельные социологические исследования, посвященные изучению проблем мошенничества в социальных сетях [7]. Несмотря на все это, как отмечают австралийские ученые (С. М. Гейнсбери, М. Браун, М. Роклофф), занимающиеся исследованием рисков использования Интернета (онлайн-виктимизацией), одним из недостатков подобного типа опросов является использование данных самоотчета, которые ограничивают точность [15]. В конечном итоге это негативно влияет на объективность результатов.

В нашем исследовании предметом выступает отношение представителей молодого поколения к мошенничеству в Интернете, а также различным формам его проявления. Для получения первичных эмпирических социологических данных по данному предмету исследования в период с мая по июнь 2020 года авторами статьи был проведен анкетный онлайн-опрос среди представителей молодого поколения, проживающих на территории г. Тюмень. Сервис Google forms был использован в качестве платформы для проведения онлайн-опроса. Полученные данные проанализированы при помощи лицензионной версии программы IBM SPSS Statistics.

В онлайн-анкетировании приняло участие 387 человек из г. Тюмень. Возраст респондентов от 18 до 30 лет. Имеющуюся выборочную совокупность можно поделить на три возрастные подгруппы: младшая — 18-22 (41%), средняя — 23-26 (31%) и старшая — 27-30 (28%). Таким образом, первая возрастная группа молодежи представляет собой учащуюся молодежь, вторая — выпускников учебных заведений, находящейся в стадии активной профессиональной адаптации в социально-профессиональной структуре, третья группа — работающая молодежь, которая в массе своей уже определилась со своей профессиональной траекторией развития. Такая дифференциация респондентов была проведена с целью определения возможных различий в ответах среди представителей различных возрастных групп молодежи.

Результаты

С целью понимания интегрированности респондентов исследования в процесс использования Интернета в своей повседневности, им было предложено ответить на ряд вопросов. В первую очередь оценивалась величина времени, проводимого в сети Интернет. Предложенными вариантами ответа были: «менее 2 часов», «от 2 до 4 часов», «от 4 до 6 часов» и «более 6 часов». Большинство респондентов ответили, что проводят в сети Интернет «от 4 до 6 часов» в день. Дифференцируя ответы по возрастам, можно отметить, что младшая и средняя возрастные группы молодежи в основном проводят в Интернете от 4 до 6 часов в день, при этом в старшей возрастной группе молодежи были зафиксированы максимальные показатели по наименьшему времяпрепровождению в Интернете (15%), и в то же время по наибольшему (36%).

Для понимания того, на каких онлайн-площадках представители современной молодежи могут встретиться с практиками проявления или рекламы мошенничества им было предложено перечислить те интернет-ресурсы, которые они посещают наиболее часто. В лидерах данного перечня оказались социальные сети (85%). Данные онлайн-сервисы являются современным и крайне распространенным средством опосредованной коммуникации, которое может быть использовано как для дружеского, так и профессионального общения. После них респонденты отмечали поисковые системы (69%), сайты банков (интернет-банкинг) (43%), электронную почту (42%), новостные ленты (41%) и видео-хостинги (38%).

При половой дифференциации ответов опрошенной молодежи о наиболее часто посещаемых сервисах в сети Интернет было отмечено, что женщины чаще, чем мужчины, используют виртуальные социальные сети, при этом мужчины, в отличие от женщин, чаще предпочитают пользоваться сайтами знакомств. Помимо того, представители молодежи женского пола чаще, чем их сверстники-мужчины, участвуют в электронной коммерции (совершают онлайн-покупки), при этом обращение к поисковым системам не зависит от пола респондента, что может быть определено равнозначностью в потребности поиска информации.

Важным показателем информационной безопасности индивида является его компетентность при использовании Интернета. В связи с этим респондентам был задан вопрос о том, насколько компетентными интернет-пользователями они являются. В связи со спецификой выборочной совокупности респондентам было доступно три варианта ответа на выбор: «уверенный пользователь (смотрю новости, пользуюсь социальными сетями)», «продвинутый пользователь (знаю принципы создания и раскрутки веб-страниц)», «эксперт (знаю языки программирования и принципы взлома веб-страниц)». По результатам опроса 71% респондентов оценили себя как уверенного пользователя, 23% охарактеризовали себя как продвинутого пользователя и 6% — как эксперта. При этом количество респондентов, которые оценили себя как эксперта, в старшей возрастной группе равняется 11%, в то время как в младшей и средней — 5 и 6%. Таким образом, можно сделать вывод о том, что представители старшей возрастной группы среди молодежи должны быть менее подвержены негативным последствиям от мошеннических действий в сети Интернет.

Перед оценкой отношения представителей молодого поколения необходимо было определить их уровень информированности о различных практиках интернет-мошенничества. Согласно результатам опроса, 92% респондентов отметило, что они замечали проявления мошенничества в Интернете. Наиболее часто мошеннические действия были отмечены в социальных сетях (73%), на электронной почте (40%) и в мессенджерах (39%). Можно предположить, что частое столкновение с мошенническими действиями в социальных сетях и сервисах электронной переписки связано с использованием мошенниками технологий социальной инженерии, которая основана на психоэмоциональном воздействии на объект мошеннического действия. Меньше всего мошенничество было замечено на площадках электронной торговли, в интернет-магазинах (26%) и иных виртуальных ресурсах.

Основываясь на отчетах и публикациях экспертов из Group-IB для нашего исследования, был сформирован перечень наиболее часто встречаемых видов интернет-мошенничества. Респондентам было предложено отметить наиболее знакомые виды мошенничества из данного списка (см. рис. 1).

Полученные данные свидетельствуют о том, что наиболее распространенным и известным среди представителей молодежи видом интернет-мошенничества были отмечены фейковые просьбы о помощи, направленные на сбор средств. Важно понимать, что указанный вид мошенничества является ярким примером использования технологий социальной инженерии. В данном случае мошеннические действия направлены на убеждение жертвы через использование чувства сопереживания событию, беде другого человека или группы лиц с целью получения денежных средств для помощи.

Помимо того, из результатов исследования следует, что более половины респондентов не знают о таких видах мошенничества, как онлайн-опросы за вознаграждение, поддельные Интернет-магазины, мошенничество с использованием Интернет-банкинга. Данный факт может свидетельствовать о необходимости увеличения информированности представителей современной молодежи о перечисленных видах мошеннических действия, так как их финансовые угрозы могут быть достаточно значимыми, особенно в сфере интернет-банкинга.

Оценивая реальный опыт участия в мошеннических действиях в Интернете в качестве жертвы, выяснилось, что доля пострадавших среди опрошенных равняется 26%, еще 59% ответили, что сталкивались с мошенничеством, но вовремя осознали, что находятся под угрозой и смогли ее избежать. Только 15% респондентов никогда не встречались лично с интернет-мошенничеством. Таким образом, 85% представителей современной городской молодежи так или иначе попадались под воздействие мошенников в сети Интернет, что еще раз подтверждает актуальность изучаемого тематического поля.

В ходе проведенного опроса респондентам было предложено указать степень согласия с рядом суждений, определяющим их отношение к мошенничеству в сети Интернет. Отметим, что в среднем по выборке с суждением «мошеннические действия противозаконны и должны строго наказываться правоохранительными

органами» согласны 89% опрошенных. Таким образом, можно определить негативное отношение среди подавляющего большинства представителей молодежи к интернет-мошенничеству как явлению. При этом в группе тех, кто попадался на обман мошенников в Интернете, а также тех, кто успел вовремя осознать ситуацию, данный показатель несколько выше (90%), чем среди тех, кто никогда не сталкивался с мошенничеством в виртуальном пространстве (82%). Предполагаем, что данное различие связано с наличием реального опыта, который формирует конкретное отношение личности к происходящему. Подобная ситуация прослеживается и при оценке иных высказываний.

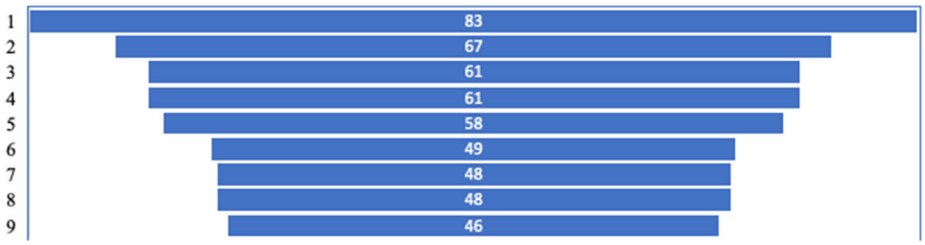

Рис. 1. Распределение ответов респондентов на вопрос «Какие из перечисленных типов интернет-мошенничества Вам знакомы?» (в % от числа опрошенных, n = 387)

На данном рисунке: 1 — Фейковые просьбы о помощи в сборе средств на лечение/материальную поддержку в экстренных ситуациях (пожары, наводнения); 2 — Фишинг (незаконное получение персональных данных путем фальсификации сайтов банков, сервисов курьерской доставки, социальных сетей); 3 — Кликбейт (яркие заголовки, например, «Я похудела...», «Только три знака выживут — это...»); 4 — Фишинговые сообщения в мессенджерах / по e-mail / SMS со ссылками на Троянские программы (например, «Вся правдивая информация о коронавирусе тут: http:456fshfu...»); 5 — Казино/ставки/ онлайн-брокинг; 6 — Мошенничество с использованием интернет-банкинга; 7 — Финансовые пирамиды; 8 — Поддельные интернет-магазины; 9 — Онлайн-опросы за вознаграждение.

Fig. 1. Distribution of respondents' answers to the question "Which of the listed types of Internet fraud are you familiar with?" (in % of the respondents' number, n = 387)

In this figure: 1 — Fake requests for help in fundraising for treatment/material support in emergency situations (fires, floods); 2 — Fishing (illegal acquisition of personal data by falsifying bank websites, courier delivery services, social networks); 3 — Clickbait (bright headlines, for example, "I lost weight…", "Only three signs will survive — this is…"); 4 — Fishing messages in messengers/by e-mail/SMS with links to Trojans (for example, "All truthful information about the coronavirus is here: http: 456fshfu…"); 5 — Casino/betting/ online brokerage; 6 — Internet banking fraud; 7 — Financial pyramids; 8 — Fake online stores; 9 — Online Surveys for Reward.

Респонденты, оценивая степень согласия с высказыванием «из-за мошенничества теряется доверие к другим пользователям», в среднем по выборке в большей степени выразили согласие с данной формулировкой. Так, полностью согласных и согласных — 57%; с одной стороны согласных, с другой — нет — 21%; несогласных и совершенно не согласных — 22%. Вместе с тем в группе пострадавших от мошенников в Интернете согласие выразили 66%; среди тех, кто не пострадал, но столкнулся с этим — 55%; доля согласных у не сталкивающихся с интернет-мошенничеством составила 49%. Помимо того, респонденты, которые никак не сталкивались с таким видом мошенничества, в большей степени склонны считать, что на интернет-мошенничество попадаются лишь неопытные пользователи, с этим согласны 40%, в то время как в иных группах доля таких людей не превышает 25%. Таким образом, можно предположить, что именно пережитый опыт встречи с мошенничеством в сети Интернет серьезно влияет на отношение к данному явлению.

Выводы

Результаты проведенного исследования свидетельствуют о заметной эскалации практик мошенничества в сети Интернет. При анализе отчетов международных организаций и специализированных социальных институтов, функционирующих с целью поддержания общественного порядка и пресечения противозаконной деятельности, прослеживается постоянное увеличение не только случаев киберпреступности, но и нанесенного ее ущерба, исчисляемого в триллионах долларов США. Подобная проблема является актуальной и для России.

Современное российское общество плотно интегрировано в мировое интернет-пространство, занимая 6 место по количеству интернет-пользователей (109 млн человек) по данным Всемирного банка [18]. Таким образом, для сохранения общественной безопасности в России особое внимание должно уделяться как научному изучению, так и практической работе в области исследования и пресечения практик интернет-мошенничества.

По результатам эмпирической части исследования отмечено, что среди представителей современной молодежи плотно интегрирована практика использования Интернета в своей повседневности. Это автоматически делает их потенциальными объектами мошеннических действий в сети Интернет. Вместе с тем основным онлайн-ресурсом, на котором проводит время молодежь, являются социальные сети, где ими и фиксируются проявления интернет-мошенничества в наибольшей степени. Скорее всего это может быть связано с тем, что в ходе противозаконных действий мошенники прибегают к практикам социальной инженерии, для реализации которой очень важно иметь возможность прямой коммуникации с объектом мошеннического действия.

Далеко не все имеющиеся практики мошенничества в сети Интернет хорошо знакомы современной молодежи. В особенности можно отметить, что менее половины представителей молодого поколения знают о возможных противозаконных действиях со стороны третьих лиц в области интернет-банкинга. Все это

свидетельствует о необходимости развития социальных проектов в области просветительских курсов по цифровой и финансовой грамотности для молодого поколения. Конечно, в данном направлении уже многое делается. Это и обучение со стороны образовательных учреждений, и со стороны банковских организаций, однако до сих пор каждый четвертый молодой человек, активный пользователь Интернета, «попадается в лапы» интернет-мошенников.

Позитивным выводом в процессе исследования отношения молодежи к мошенничеству в сети Интернет может стать общее согласие подавляющего большинства респондентов с тем, что данные действия являются противозаконными и должны строго наказываться и пресекаться специализированными органами. Несмотря на некоторые существующие различия во мнениях респондентов в зависимости от их опыта взаимодействия с интернет-мошенничеством, в общем можно говорить о наличии отрицательной установки молодежи по отношению к изучаемому явлению.

Среди перспектив для исследования мошенничества в сети Интернет с позиции социологического подхода можно выделить следующие направления. Во-первых, в связи с повсеместной интеграцией Интернета в повседневную жизнедеятельность людей, проведение сравнительного анализа по различным возрастным группам населения, выходящим за пределы молодого поколения. Во-вторых, определение и систематизация факторов виктимизации пользователей сети Интернет в процессе постоянного распространения практик интернет-мошенничества. В-третьих, важным с точки зрения практического применения результатов станет углубленное изучение существующих и потенциальных возможностей превентивных методов общественного мониторинга появления новых форм мошенничества в виртуальном пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. Берман Н. Д. К вопросу о цифровой грамотности / Н. Д. Берман // Современные исследования социальных проблем (электронный научный журнал). 2017. Т. 8. № 6-2. С. 35-38.
2. Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита / Е. Л. Доценко. М.: ЧеРо, Издательство МГУ, 1997. 344 с.
3. Дюркгейм Э. Норма и патология / Э. Дюркгейм // Социология преступности. Современные буржуазные теории: Сборник статей: Перевод с английского. М.: Прогресс, 1966. С. 39-44.
4. Кара-Мурза С. Г. Манипуляция сознанием / С. Г. Кара-Мурза. М.: Изд-во: Эксмо, 2005. 832 с.
5. Киберпреступность в домашних тапочках // Ведомости. URL: https://www.vedomosti.ru/opinion/articles/2018/10/17/783976-kiberprestupnost (дата обращения: 25.03.2021)
6. Кнорре А. Преступность и виктимизация в россии. Результаты всероссийского виктимизационного опроса / А. Кнорре, К. Титаев // Аналитический обзор.

Институт проблем правоприменения при Европейском Университет в Санкт-Петербурге. Санкт-Петербург, 2018. Сер. Аналитические обзоры по проблемам правоприменения.

7. Кухто А. И. Социологический анализ проблемы мошенничества на сайтах социальных сетей / А. И. Кухто, А. В. Мальцева // Siberian Socium. 2018. Том 2. № 4. С. 42-58. DOI: 10.21684/2587-8484-2018-2-4-42-58
8. Мертон Р. Социальная теория и социальная структура / Р. Мертон. М.: АСТ, Хранитель, 2006. 880 с.
9. МИД РФ: ущерб мировой экономике от киберпреступности в 2019 году может достичь $2 трлн // ТАСС. URL: https://tass.ru/politika/5551244 (дата обращения: 24.03.2021)
10. Руф Ю. Н. Мошенничество в интернете в период пандемии: схемы и их избежание / Ю. Н. Руф, Е. В. Шадрина // Цифровая экономика: перспективы аудита и безопасности бизнеса. Сборник статей по материалам Всероссийской научно-практической конференции. Ответственный редактор Д. Л. Скипин. 2020. С. 182-187.
11. Состояние преступности в России за январь-июнь 2020 года // Министерство внутренних дел Российской Федерации. ФКУ «Главный информационно-аналитический центр». Москва, 2020. С. 4. URL: https://мвд.рф/reports/item/20597695/ (дата обращения: 25.03.2021)
12. Цифровая грамотность россиян: исследование 2020. URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ (дата обращения: 26.07.2020)
13. Шиллер Г. Манипуляторы сознанием / Г. Шиллер. Пер. с англ.; науч. ред. Я. Н. Засурский. М.: Мысль, 1980.
14. EU Science Hub. DigComp. URL: https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework (дата обращения: 26.07.2020)
15. Gainsbury S. M. Defining risky Internet Use: Linking negative internet experiences to specific online behavior / S. Ginsbury, M. Brown, M. Rockloff // New Media and Society. 2019. No. 21 (6). Pp. 1232-1252. DOI: 10.1177/1461444818815442
16. Group-IB. URL: https://www.group-ib.ru (дата обращения: 25.03.2021)
17. Internet crime report // Federal bureau of investigation. 2019. URL: https://pdf.ic3.gov/2019_IC3Report.pdf (дата обращения: 24.03.2021)
18. Number of internet users by country. URL: https://ourworldindata.org/grapher/number-of-internet-users-by-country?tab=chart&time=2017&country=USA~IND~CHN~BRA~JPN~RUS~MEX~DEU~IDN~GBR (дата обращение: 10.04.2021)
19. Scamwatch. URL: https://www.scamwatch.gov.au/scam-statistics?scamid=all&date=2020 (дата обращения: 26.03.2021)

Maxim Yu. SEMENOV[1]
Polina V. KACHANOVA[2]

UDC 343.721

INTERNET FRAUD: THE ATTITUDE OF YOUNG PEOPLE

[1] Cand. Sci. (Soc.), Associate Professor,
Department of General and Economic Sociology,
University of Tyumen
m.y.semenov@utmn.ru

[2] Bachelor of Sociology, University of Tyumen
polinak74@mail.ru

Abstract

In modern conditions of information technologies constant integration into a person's everyday life, the problem of the formation and manifestation of new risks while using the Internet is aggravated. According to international and all-Russian data, there is a significant increase in the number of cybercrimes, new forms of Internet fraud are constantly appearing and the actual damage from illegal actions in the virtual space is increasing. Young people, as the most active users of the global network, become targets of Internet fraudsters.

The purpose of the study is to study the representatives attitude of modern youth to fraud on the Internet, as well as to various forms of its manifestation. The theoretical and methodological analysis of the study was carried out on the basis of the deviant behavior theories and the theory of manipulation. To obtain primary sociological data, the work used the method of young people online survey living in Tyumen. The survey was conducted in the summer of 2020.

According to the results of the study, the attitude of modern young people representatives to Internet fraud was determined. It was recorded that the overwhelming majority (85%) of young people faced various manifestations of fraud on the Internet, while every fourth (26%) respondent suffered from this negative social phenomenon. Most often, fraud on the Internet

Citation: Semenov M. Yu., Kachanova P. V. 2021. "Internet fraud: the attitude of young people". Tyumen State University Herald. Social, Economic, and Law Research, vol. 7, no. 3 (27), pp. 71-85.
DOI: 10.21684/2411-7897-2021-7-3-71-85

by young people is recorded in virtual social networks using social engineering technologies. In addition, not all forms of online fraud are well known to young people, for example, just under half of the respondents are aware of online banking fraud. Overall in the sample, young people negatively assess Internet fraud as a phenomenon, although there are some different opinions depending on their personal life experiences. In the conclusion of the article, possible prospects for further research in this area are identified.

Keywords

Internet, fraud, cybercrime, social engineering, digital literacy, young people, social media.

DOI: 10.21684/2411-7897-2021-7-3-71-85

REFERENCES

1. Berman N. D. 2017. “On the question of digital literacy”. Modern studies of social problems (electronic scientific journal), vol. 8, no. 6 (2), pp. 35-38. [In Russian]
2. Dotsenko E. L. 1997. Psychology of manipulation: phenomena, mechanisms and protection. Moscow: CHERO, MSU Publishing House. 344 p. [In Russian]
3. Durkheim E. 1966. “Norm and pathology”. Sociology of crime. Modern bourgeois theories: Collection of articles: Translated from English. Moscow: Progress. Pp. 39-44. [In Russian]
4. Kara-Murza S. G. 2005. Manipulation of consciousness. Moscow: Publishing house: Eksmo. 832 p. [In Russian]
5. Vedomosti. Cybercrime in slippers. Accessed on 25 March 2021. https://www.vedomosti.ru/opinion/articles/2018/10/17/783976-kiberprestupnost [In Russian]
6. Knorre A., Titaev K. 2018. “Crime and victimization in Russia. Results of the All-Russian victimization survey”. Analytical review. Institute of Law Enforcement Problems at the European University in St. Petersburg. Saint Petersburg. Series: Analytical reviews on law enforcement issues. [In Russian]
7. Kukhto A. I., Maltseva A. V. 2018. “Sociological analysis of the fraud problem on social networking sites”. Siberian Socium, vol. 2, no. 4, pp. 42-58. DOI: 10.21684/2587-8484-2018-2-4-42-58 [In Russian]
8. Merton R. 2006. Social theory and social structure. Moscow: AST, The Guardian. 880 p. [In Russian]
9. TASS. Russian Foreign Ministry: Cybercrime Damage to the World Economy Could Reach $ 2 Trillion in 2019. Accessed on 24 March 2021. https://tass.ru/politika/5551244 [In Russian]
10. Ruf Yu. N., Shadrina E. V. 2020. “Fraud on the Internet during the pandemic: schemes and their avoidance”. Digital Economy: prospects for audit and business security. Collection of articles based on the materials of the All-Russian Scientific and Practical Conference. Responsible editor D. L. Skipin. Pp. 182-187. [In Russian]
11. Ministry of Internal Affairs of the Russian Federation. FKU “Main information and analytical center”. The state of crime in Russia in January-June 2020. Moscow, 2020. P. 4. Accessed on 25 March 2021. https: //mv.d.rf/reports/item/20597695/ [In Russian]

12. Digital literacy of Russians: research 2020. Accessed on 26 July 2020. https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ [In Russian]
13. Shiller G. 1980. Consciousness manipulators. Translated from English; edited by Ya. N. Zasursky. M.: Mysl. [In Russian]
14. EU Science Hub. DigComp. Accessed on 26 July 2020. https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework
15. Gainsbury S. M., Brown M., Rockloff M. 2019. "Defining risky Internet Use: Linking negative internet experiences to specific online behavior". New Media and Society, no. 21 (6), pp. 1232-1252. DOI: 10.1177/1461444818815442
16. Group-IB. Accessed on 25 March 2021. URL: https://www.group-ib.ru
17. Federal bureau of investigation. Internet crime report. Accessed on 24 March 2021. https://pdf.ic3.gov/2019_IC3Report.pdf
18. Number of internet users by country. Accessed on 10 April 2021. https://ourworldindata.org/grapher/number-of-internet-users-by-country?tab=chart&time=2017&country=USA~IND~CHN~BRA~JPN~RUS~MEX~DEU~IDN~GBR
19. Scamwatch. Accessed on 26 March 2021. https://www.scamwatch.gov.au/scam-statistics?scamid=all&date=2020