КРАТКИЕ СООБЩЕНИЯ И ПЕРВЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ОПЫТ

BRIEF MESSAGES AND FIRST RESEARCH EXPERIENCE

Научная статья / Research Article
УДК: 316.61
DOI: 10.14258/SSI(2024)4-10

Социальный портрет жертвы мошенничества, совершенного с использованием информационно-коммуникационных технологий, в современной России

Екатерина Евгеньевна Самойличенко[1]

Мария Олеговна Дятлева[2]

Елизавета Алексеевна Цыкина[3]

[1]Северо-Западный институт (филиал) Университета имени О. Е. Кутафина (МГЮА), Вологда, Россия, samoilich@mail.ru, https://orcid.org/0009-0008-7464-3427

[2]Северо-Западный институт (филиал) Университета имени О. Е. Кутафина (МГЮА), Вологда, Россия, dyatleva_maria@mail.ru, https://orcid.org/0009-0000-9907-6440

[3]Северо-Западный институт (филиал) Университета имени О. Е. Кутафина (МГЮА), г Вологда, Россия, tsykina.e.a_bo14_1@mail.ru, https://orcid.org/0009-0007-5332-207X

Аннотация. С развитием цифровых технологий увеличилось количество фактов финансовых мошенничеств, совершенных с использованием информационно-коммуникационных технологий или в сфере компьютерной информации, жертвами которых становятся преимущественно физические лица. Механизмы совершения таких преступлений постоянно развиваются и совершенствуются. Поэтому даже в условиях постоянного информирования граждан о видах финансового мошенничества и способах их предотвра-

щения количество самих преступлений и жертв кибермошенников, а также финансовые потери пострадавших увеличиваются из года в год.

С целью выявления социального портрета типичной жертвы кибермошенников авторы данной статьи обобщили и сравнили результаты исследований ряда государственных и коммерческих организаций, осуществленных на протяжении последнего десятилетия. Рассматриваемые социальные критерии (возраст, пол, образование, тип местности проживания и уровень дохода) позволили составить наиболее типичный социальный портрет жертвы киберпреступника: это работающая женщина в возрасте от 25 до 44 лет, имеющая среднее образование и средний доход, а также проживающая в городе. Кроме того, авторами был проведен социологический опрос среди студентов Северо-Западного института (филиала) Университета имени О. Е. Кутафина (МГЮА), подтвердивший наличие высокого уровня риска попадания студентов под влияние кибермошенников. Так, более 75% опрошенных студентов в текущем календарном году (январь — апрель 2024 г.) подвергались мошенническим действиям. Из них более 25% признались в том, что они сами или их знакомые и родственники попадались на уловки мошенников и теряли определенные суммы денежных средств.

Представленный в научной статье материал не только расширяет наше знание о механизмах мошенничества, но и может служить основой для разработки широкого спектра профилактических мер и образовательных программ, направленных на защиту населения от действий финансовых преступников, формирование навыков распознавания потенциальных угроз и принятие соответствующих мер предосторожности.

Ключевые слова: финансовое мошенничество, телефонное мошенничество, кибермошенники, социологический опрос, статистика, типичный портрет жертвы, сеть Интернет

Для цитирования: Самойличенко Е. Е., Дятлева М. О., Цыкина Е. А. Социальный портрет жертвы мошенничества, совершенного с использованием информационно-коммуникационных технологий, в современной России // Society and Security Insights. 2024. Т. 7, № 4. С. 157–171. doi: 10.14258/ssi(2024)4-10.

Social Portrait of a Victim of Fraud Committed Using Information and Communication Technologies in Modern Russia

Ekaterina E. Samoilichenko[1]

Maria O. Dyatleva[2]

Elizaveta A. Tsykina[3]

[1]the North-West Institute (branch) of Kutafin Moscow State Law University (MSLA), Vologda, Russia, samoilich@mail.ru

[2]the North-West Institute (branch) of Kutafin Moscow State Law University (MSLA), Vologda, Russia, dyatleva_maria@mail.ru

[3]the North-West Institute (branch) of Kutafin Moscow State Law University (MSLA), Vologda, Russia, tsykina.e.a_bo14_1@mail.ru

Abstract. With the development of digital technologies, the number of facts of financial fraud committed using information and communication technologies or in the field of computer information has increased, the victims of which are mainly individuals. The mechanisms for committing such crimes are constantly being developed and improved. Therefore, even in conditions of constant informing citizens about the types of financial fraud and ways to prevent them, the number of crimes themselves and victims of cyber fraudsters, as well as the financial losses of victims, increase from year to year.

In order to identify the social portrait of a typical victim of cyberbullying, the authors of this scientific article summarized and compared the results of research conducted by a number of government and commercial organizations over the past decade. The considered social criteria (age, gender, education, type of place of residence and income level) made it possible to create the most typical social portrait of a cybercriminal victim — a working woman aged 25 to 44 years old, with secondary education and average income, as well as living in a city. In addition, the authors conducted a sociological survey among students of the Northwestern Institute (branch) Kutafin University (MGUA), which confirmed the presence of a high level of risk of students falling under the influence of cyberbullies. Thus, more than 75% of the surveyed students were subjected to fraudulent activities in the current calendar year (January-April). Of these, more than 25% admitted that they themselves or their friends and relatives fell for the tricks of scammers and lost certain amounts of money.

The material presented in the scientific article not only expands our knowledge of the mechanisms of fraud, but can also serve as a basis for the development of a wide range of preventive measures and educational programs aimed at protecting the population from the actions of financial criminals, developing skills to recognize potential threats and taking appropriate precautions.

Keywords: financial fraud, telephone fraud, cybercriminals, sociological survey, statistics, typical portrait of the victim, the Internet

For citation: Samoilichenko, E. E., Dyatleva, M. O., Tsykina, E. A. Social Portrait of a Victim of Fraud Committed Using Information and Communication Technologies in Modern Russia // *Society and Security Insights, 7*(4), 157–171. (In Russ.). doi: 10.14258/ssi(2024)4-10.

Эволюция человеческого общества на современном этапе преимущественно обусловлена развитием информационно-коммуникационных и цифровых технологий, охватывающих все сферы жизнедеятельности человека, и в первую очередь экономическую, т.е. деятельность, связанную с извлечением дохода и его сбережением. Цифровые технологии существенно облегчают жизнь человека, но вместе с тем несут в себе определенные риски, в том числе финансовые, обусловленные как ошибками самого пользователя этих технологий, так и действиями различного рода мошенников. В соответствии с аналитической справкой Министерства внутренних дел Российской Федерации за январь — декабрь 2023 г. было зарегистрировано 677,0 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 29,7% больше, чем за аналогичный период прошлого года[1].

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года. URL: https://мвд.рф/reports/item/47055751/.

При этом в 2023 г. финансовые потери клиентов банков в России от действий кибермошенников составили в общей сложности 15,8 млрд руб., что на 11,5% больше, чем в 2022 г. (14,2 млрд руб.) и на 17,1% больше, чем в 2021 г. (13,5 млрд руб.)[2]. Аналогичная картина наблюдается и в ряде других стран. Так, за 2023 г. интернет-мошенники украли у казахстанцев 11,3 млрд тенге[3], при этом среди наиболее распространенных видов мошенничества выделяют получение предоплаты за товар или услугу по объявлениям; оформление онлайн-займов на сайтах микрокредитных организаций; хищения денежных средств с банковских счетов после получения персональных данных граждан[4]. По данным Министерства внутренних дел Республики Беларусь в республике также наблюдается устойчивый рост количества регистрируемых киберпреступлений: в 2015 г. — 2 440 преступлений, а в 2020 г. уже 25 561[5].

В настоящее время в научной литературе и публицистике можно встретить достаточное количество материалов, посвященных понятию кибермошенничества, характеристике его видов, описанию наиболее распространенных мошеннических схем, советам, как не стать жертвой телефонных мошенников (Квятковский, 2022; Мырзахмет, *2019;* Романовская, 2017; Батюкова, 2020; Еськова, Рябчиков, 2020*).*

В соответствии со ст. 159 УК РФ мошенничество — это неправомерное завладение чужими деньгами или имуществом с целью обращения его в свою пользу или в пользу третьих лиц, совершаемое с помощью обмана или злоупотребления доверием. Финансовое мошенничество представляет собой совершение противоправных действий в сфере денежного обращения, подпадающих под действие ст. 159.3 УК РФ — мошенничество с использованием средств платежа, и предполагает совершение преступлений с использованием поддельных или принадлежащих другому лицу кредитных, расчетных и иных платежных карт. Потерпевшим от такого мошенничества является владелец счета, с которого списываются денежные средства.

Следует различать два внешне схожих понятия: преступления в сфере компьютерной информации, под которыми в целом следует понимать общественно опасные деяния, предусмотренные гл. 28 УК РФ, посягающие на компьютерную информацию, и киберпреступления — преступления, совершаемые с использованием компьютерных технологий. Порой в научной литературе выделяют и термин «компьютерные преступления», либо отождествляя его с преступлениями в сфере компьютерной информации, либо определяя их намного шире, включая деяния, где компьютерная информация является не только предметом,

---

[2] Потери банков от киберпреступности. URL: https://www.tadviser.ru/index.php/.

[3] Интернет-мошенники украли у казахстанцев 11,3 млрд тенге. Способы обмана раскрыли в МВД. URL: https://kz.kursiv.media/2023-10-20/tksh-internet-moshenniki/.

[4] Самые популярные виды мошенничества в Казахстане назвали в МВД. URL: https://www.nur.kz/incident/crime/1955979-samye-populyarnye-vidy-moshennichestva-v-kazahstane-nazvali-v-mvd/

[5] Основные аспекты профилактики киберпреступности в Республике Беларусь. URL: https://minsk.gov.by/ ru/actual/view/209/2021/inf_material_2021_05.shtml.

но и средством преступления. Во всяком случае, киберпреступления остаются самым широким понятием из представленных, охватывая не только преступления, связанные с использованием компьютерных технологий и сетей, но и деяния, осуществляемые другими средствами доступа к киберпространству (Квятковский, 2022). В рамках рассматриваемого вопроса следует говорить именно о последних.

Сегодня мошенничество с использованием цифровых технологий представляет собой широкий спектр незаконных методов и практик, направленных на обман с целью получения финансовой выгоды, а также любые махинации, целью которых является лишение другого имущества или денег путем уловок, обмана или других нечестных действий. Так, в уголовном праве Китая используются различные вариации характеристик мошеннических деяний и определены соответствующие меры ответственности. В частности, согласно ст. 266 УК КНР, завладение путем мошенничества государственным или частным имуществом в сравнительно крупном размере наказывается лишением свободы на срок до трех лет, арестом или надзором, а также штрафом (Романовская, 2017). В Казахстане в числе наиболее распространенных видов мошенничества выделяют получение предоплаты за товар или услугу по объявлению; оформление онлайн-займов на сайтах микрокредитных организаций; хищения денежных средств с банковских счетов после получения персональных данных граждан[6], а также финансовые мошенничества, осуществляемые посредством сети Интернет: виртуальные кошельки; предложения о стабильном заработке в интернете при определенных условиях; продажа бизнес-пакетов, которые навязываются пользователю, на сайтах-однодневках с утверждением, что «это сделает вас богатым» (Мырзахмет, 2019). В Беларуси распространенными видами мошенничества считаются вишинг (преступники звонят гражданам, представляясь сотрудниками правоохранительных органов, банковских учреждений, сотовых операторов); схема «Алло, мама!» (звонки от имени родственников, которые сообщают о некой беде, для предотвращения которой необходимо передать курьеру или перечислить на какой-то счет крупную денежную сумму); создание фейковых интернет-магазинов[7].

В период коронавирусной пандемии получили распространение новые формы мошенничества, среди них — заведомо ложное привлечение к ответственности за нарушение режима ограничительных мер, а также заведомо ложные предложения о продаже фиктивных товаров и услуг, необходимых гражданам в период ограничительных мер и профилактики заболеваемости; об оказании услуг социального характера (Батюкова, Еськова, Рябчиков, 2020).

В зависимости от того, какую роль играет в совершаемом преступлении сам потерпевший (активную или пассивную), все виды мошенничества можно подразделять на «техногенные мошенничества» — от жертвы преступления ничего

[6] Самые популярные виды мошенничества в Казахстане назвали в МВД. URL: https://www.nur.kz/incident/crime/1955979-samye-populyarnye-vidy-moshennichestva-v-kazahstane-nazvali-v-mvd/.

[7] В Следственном комитете рассказали о самых распространенных видах мошенничества. URL: https://sk.gov.by/ru/news-ru/view/v-sledstvennom-komitete-rasskazali-o-samyx-rasprostranennyx-vidax-moshennichestva-v-belarusi-14073/.

не зависит; и «человекогенные мошенничества» — если человек сам предпринимает ошибочные действия, приводящие к потере его денег (Братусин, Власенко, 2019).

В зависимости от того, каким образом осуществляется обман граждан, выделяют следующие виды мошенничеств:

1. Фишинг — мошенничество, направленное на получение таких персональных данных, как логин, пароль, данные банковских карт и паспортов, коды верификации посредством электронных писем, сообщений в социальных сетях, поддельных сайтов. В данном случае цель мошенника — получить не само имущество (в большинстве случаев это денежные средства), а данные, обеспечивающие доступ к нему. Так, отправляя поддельные электронные письма владельцам учетных записей, они просят их срочно проверить, подтвердить или обновить информацию об их учетных записях, нажав на ссылку в электронной почте. Ссылка переходит на фейковый веб-сайт, почти полностью идентичный официальному веб-сайту банковской организации. Вследствие чего введенная на подобном сайте информация перехватывается мошенником, который с ее помощью «законным» способом получает желаемое имущество[8].

2. Инвестиционное мошенничество заключается в том, что псевдоброкеры, а также организаторы финансовых пирамид, функционирующих в сети Интернет, призывают потенциальную жертву мошенничества вкладывать деньги в акции, криптовалюты, проекты, связанные с альтернативными источниками энергии, и иные активы, умело играя на желании легко и быстро заработать денежные средства[9].

3. Мошенничество с помощью поддельных интернет-магазинов. Распространение получили два основных вида обманных схем, по которым работают мошенники: доставка некачественного или поддельного товара и воровство данных банковских карт — «фишинг». Используя известные бренды и низкие цены, они стремятся привлечь как можно больше покупателей. После того как потребители совершают покупку и передают свои личные данные или средства, магазин исчезает, оставив покупателей без товара и денег.

Признаками «фейкового» магазина могут быть более низкие цены по сравнению с другими платформами, особенно если это популярная продукция; отсутствие сведений о продавце или его контактной информации; отсутствие описания товаров или их существенное отличие от аналогичных на сайтах конкурентов; требование осуществить предоплату через малоизвестные платежные системы или банковские переводы на личные счета; отсутствие информации относительно гарантий и условий возврата товара[10].

Также важно обращать внимание на дизайн самого сайта и наличие отзывов. Если ресурс выглядит неаккуратно, изображения имеют низкое качество, а текст полон орфографических ошибок, то это может свидетельствовать о ненадежно-

---

[8] Что такое фишинг и чем он опасен? URL: https://www.cism-ms.ru/poleznye-materialy/chto-takoe-fishing-i-chem-on-opasen/.

[9] Мошенничество в сфере инвестиций, или инвестиционное мошенничество. URL: https://www.cism-ms.ru/poleznye-materialy/chto-takoe-fishing-i-chem-on-opasen/.

[10] Как работают фальшивые интернет-магазины? URL: https://www.cism-ms.ru/poleznye-materialy/chto-takoe-fishing-i-chem-on-opasen/

сти продавца. Кажется подозрительным отсутствие в интернете информации о магазине либо когда все отзывы выглядят положительными и неестественными.

4. Телефонное мошенничество — самый популярный и простой, но от этого не менее эффективный способ. Для осуществления звонков мошенники используют технологию подмены номера, используют номера, похожие на официальные телефоны банков или государственных учреждений либо ставшие им известными благодаря незаконному получению персональных данных абонентов. Могут звонить и с незнакомого номера, представляясь родственником, знакомым, сотрудником банка, государственным служащим или мобильным оператором, и сообщают неблагоприятную информацию, которая деморализует слушателя: взломали банковский счет, аккаунт на портале «Госуслуги», близкий родственник попал в ДТП, стал участником преступления или же на самого потерпевшего завели уголовное дело, сообщают об ошибочном переводе денег на счет мобильного телефона и просят вернуть их владельцу. Зачастую голосовые сообщения заменяются SMS-сообщениями, содержание которых идентично вышеуказанному.

В последнее время стали получать распространение сообщения, касающиеся возможности получения услуг с сайта портала Госуслуг, учреждений здравоохранения и социального обеспечения.

Таким образом, в настоящее время существуют различные схемы мошеннических действий, совершаемых с использованием информационно-коммуникационных технологий, ориентированные на различные категории граждан.

Пытаясь отыскать ответы на вопрос, почему мошенникам удается обманывать людей в условиях максимального контроля и постоянных предостережений, различные авторы и организации (государственные, публично-правовые и коммерческие) стали формировать социально-психологический портрет человека, который чаще всего находится в зоне риска подвергнуться мошенничеству. Анализ психологических особенностей жертвы мошенников в трудах российских ученых представлен достаточно широко: А. Р. Братусин, Е. Е. Власенко (2019), Н. В. Мешкова, В. Т. Кудрявцев, С. Н. Ениколопов (2022), А. Л. Репецкая, Л. А. Петрякова (2022). Среди исследователей социально-демографической составляющей жертвы следует назвать А. С. Камко (2017). Аналогичные исследования проводили специалисты ЦБ РФ, ВТБ, ВЦИОМ, МВД РФ и его отдельных управлений, аналитики финансового маркетплейса «Выберу.ру»[11].

Обобщение и систематизация информации о социально-демографической составляющей жертв преступлений позволяет не только ее структурировать, но и закрепить в сознании, что, в свою очередь, может служить предостережению людей от уловок мошенников.

Цель настоящего исследования: на основе обобщения и анализа результатов исследований сформировать представление о социальных чертах (типичном портрете) потенциальной жертвы мошеннических действий, совершенных с ис-

---

[11] Более 40% россиян столкнулись с мошенническими звонками из «прокуратуры». URL: https://iz.ru/1639926/2024-01-26/bolee-40-rossiian-stolknulis-s-moshennicheskimi-zvonkami-iz-prokuratury.

пользованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Материалы и методы исследования

Исследование базировалось на синтезе ряда методов: документальный анализ (изучение и обобщение информации научных статей, аналитических обзоров, статистических отчетов), статистико-математические методы, социологический опрос (анкетирование), аналитический.

Эмпирическую базу исследования составили данные статистической отчетности Судебного департамента при Верховном суде РФ за 2023 г., Министерства внутренних дел России за 2022–2023 гг.; Обзор операций, совершенных без согласия клиентов финансовых организаций, Банка России за 2022–2023 гг., данные Федеральной службы государственной статистики (Росстата) за 2023 г., результаты собственного исследования, проведенного путем письменного опроса студентов Северо-Западного института (филиала) Университета имени О.Е. Кутафина (г. Вологда, 2024).

Результаты исследования

Для определения социального портрета «потенциальной жертвы» кибермошенников, включающего наиболее значимые социальные показатели (пол, возраст, уровень образования и достатка, социальный статус, тип местности проживания), мы взяли результаты исследований вышеуказанных организаций, сведя их в единую таблицу (табл. 1). Для сопоставления данных в таблице представлены также социально-демографические показатели Росстата, отражающие долю данных категорий в структуре населения страны по состоянию на 1 января 2024 г.

Таблица 1.

Table 1.

Варианты социального портрета потенциальной жертвы кибермошенников в актуальных исследованиях

Variants of the social portrait of a potential victim of cyber fraudsters in current research

Источник данных	Камко А.С.	ВТБ[12]	ЦБ РФ	МВД	Росстат[13]
Отчетный период, год	2012– 2015	2022	2023	2023	2023*
Критерий оценивания:					
1. Пол					
— мужской	23,9	51	50,4	40	46,5
— женский	76,1	49	49,6	60	53,5

[12] Жертвы мошенников — социальный портрет. URL: https://dzen.ru/a/ZHBbO4kF6CrpnRd4.

[13] Статистика / Официальная статистика / Население / Демография. URL: https://rosstat.gov.ru/folder/12781.

2. Преобладающий возраст, лет	25– 44	30– 55	25– 44	30– 49	25– 44
— уд. вес в общем объеме, %	63,2	69,8	37,4	35,5	48,9
3. Преобладающий уровень образования	Среднее и СПО	–	Среднее и СПО	–	Среднее и СПО
— уд. вес в общем объеме, %	42,20	–	48,0	–	42,3
4. Признак социального статуса	Семейное положение	–	Трудовая занятость	Трудовая занятость	58,7
5. Уровень достатка	–	–	Средний	–	0,75– 1,25 медианы
— уд. вес в общем объеме, %	–	–	46,5	–	41,7
6. Тип местности проживания					
— городская, %	–	–	75,0	–	74,9
— сельская, %	–	–	25,0	–	25,1

* Доля категории в структуре населения РФ, %

Анализ представленной в таблице информации позволяет сделать следующие выводы.

Наиболее полными по изученным показателям являются данные, представленные Банком России (ЦБ РФ) от 13 февраля 2024 г., включающие все шесть критериев оценивания (аналогичные данные были представлены ЦБ РФ и за 2022 г.)[14].

1. Пол. В период 2012–2015 гг. абсолютное преобладание среди пострадавших от кибермошенников принадлежало женщинам (76,1%), что можно было бы объяснить их более высоким уровнем эмоционального восприятия, а также более высоким уровнем социальной активности в сети Интернет. Эта же картина, но уже менее явно, наблюдается и в 2023 г., что в целом соответствует структуре российского общества (женщин в России почти на 7% больше, чем мужчин).

2. Возраст. Данные исследований показывают, что, как и несколько лет назад, наиболее подвержена уловкам мошенников возрастная категория 25–44 лет. Это вполне оправданно, так как именно эта категория людей не только является преобладающей в структуре российского общества (для справки — средний возраст в России в указанный период составлял 40,7 года), но и наиболее активна

[14] Обзор операций, совершенных без согласия клиентов финансовых организаций. URL: https://cbr.ru/analytics/ib/operations_survey_2022 / https://www.cbr.ru/analytics/ib/operations_survey/2023/

в социальных сетях и в целом в сети Интернет. Исследование, проведенное Банком России, показало, что жертвой мошенников можно стать практически в любом возрасте (рис. 1).

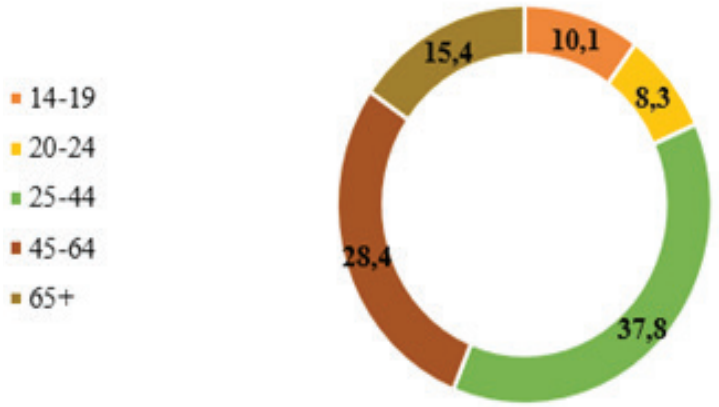

Рисунок 1 — Количество жертв мошенничества по критерию «Возраст» по данным ЦБ РФ, %, 2023 г.
Figure 1 — The number of fraud victims according to the «Age» criterion according to the Central Bank of the Russian Federation, %, 2023

3. Образование. Показатели уровня образования были оценены А. С. Камко и ЦБ РФ. В обоих исследованиях подавляющее количество потерпевших в анализируемый период имели среднее образование — более 40%. Примечательно, что по данным Росстата на долю лиц, имеющих среднее общее и среднее профессиональное образование, в России приходится примерно такое же количество граждан (42,3%). Вместе с тем достаточно высока доля пострадавших от мошенников лиц, имеющих высшее образование (28,9%). Это говорит о том, что одного только факта получения высшего образования недостаточно для того, чтобы не стать жертвой различного рода мошенников.

4. Социальный статус. Данный критерий также оценивали А. С. Камко, ЦБ РФ и МВД России. При этом в качестве критерия А. С. Камко выбрал семейное положение респондентов, а также состав семьи. Автором было выявлено, что значительная часть пострадавших — это люди, состоявшие в браке (49,7%) и имеющие одного и более ребенка (70,6%). В качестве признака социального статуса ЦБ РФ и МВД России приняли трудовую занятость. Подавляющее большинство жертв (76,6%) работают или учатся, (для справки — коэффициент занятости российского населения по данным Росстата составлял в 2023 г. 58,7%) и 7,3% находятся на пенсии (рис. 2). Вряд ли это связано с тем, что мошенники проводят серьезную аналитическую работу и выбирают потенциальную жерт-

ву, имеющую постоянный доход и трудовую занятость. Здесь можно дать другое объяснение: именно работающие и пенсионеры являются владельцами платежных карт, на которые в настоящее время преимущественно зачисляются и заработная плата, и различного рода социальные трансферты (пенсии, пособия, компенсации и пр.).

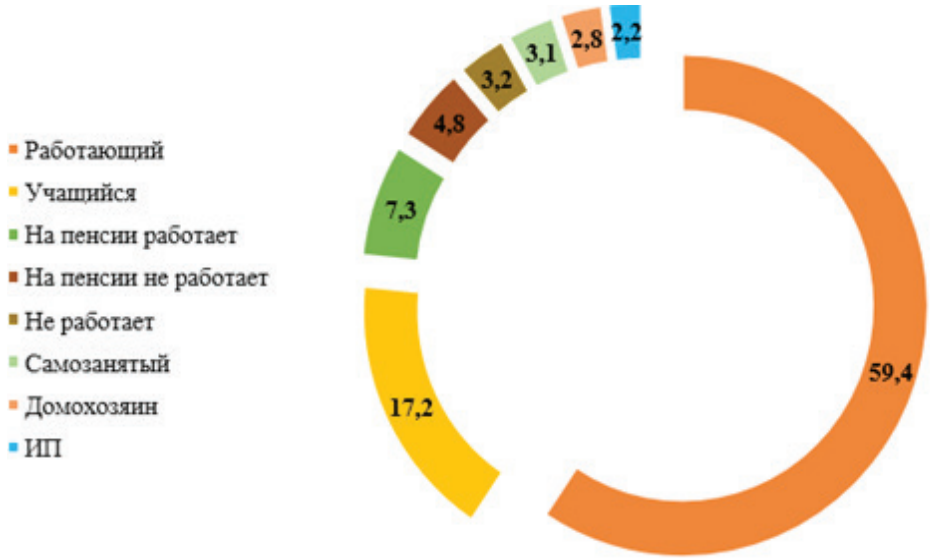

Рисунок 2 — Количество жертв мошенничества по критерию «Социальный статус» по данным ЦБ РФ, %, 2023 г.
Figure 2 — The number of victims of fraud according to the criterion of «Social status», according to the Central Bank of the Russian Federation, %, 2023

5. Тип местности проживания. Распределение пострадавших по типу места проживания вполне соответствует структуре распределения населения в стране: 75% — городское население, 25% — сельское. Но можно предположить и влияние других факторов, в частности, на территории Российской Федерации существует такая проблема, как отсутствие не только интернета, но и подключения к телефонной связи в отдельных населенных пунктах. Так, согласно данным, представленным на интернет-портале Tadviser в марте 2023 г. со ссылкой на отчет Global Digital Reports (информационно-аналитический портал и профессиональное сообщество, которые отслеживают развитие цифровой экономики в странах Евразии), в начале 2022 г. 16,04 млн чел. в России не пользовались интернетом, а это 11,0% населения страны. В связи с этим мошенники не могут воздействовать так, как это необходимо, на лиц, проживающих в сельской местности, выбирая более доступных в этом плане горожан.

6. Уровень достатка. Данный критерий был проанализирован только Банком России. В соответствии с его исследованиями в большинстве случаев жертвами мошенничества становятся граждане со средним уровнем заработка — 46,5%, т.е. категория граждан, среднемесячный доход которых в 2023 г. составлял

32–92 тыс. руб. (для справки — средняя заработная плата в России в 2023 г. по данным Росстата составляла 73,7 тыс. руб.). Это очень привлекательная для мошенников категория, ведь такие люди сильнее всего озабочены своими финансами и поэтому наиболее подвержены обману со стороны мошенников, которые, к примеру, выдают себя за сотрудников банков.

Обобщив представленную в различных источниках информацию, можно предположить, что среднестатистический социальный портрет жертвы мошенника, применяющего в своих преступных схемах современные информационно-телекоммуникационные технологии, выглядит следующим образом: это женщина в возрасте от 25 до 44 лет, имеющая среднее образование, работающая и имеющая средний доход, а также проживающая в городе. Данный вывод относительно совпадает с выводами Банка России, сделанными по результатам статистической отчетности кредитных организаций за 2022–2023 гг., а также с социально-демографической структурой современного российского общества.

С целью выявления риска попадания студентов под действия мошенников авторами был проведен социологический опрос студентов 1–3 курсов очной формы обучения Северо-Западного института (филиала) Университета имени О. Е. Кутафина (МГЮА). Студентам было предложено ответить на вопросы: «Пол опрашиваемого»; «Звонили ли Вам мошенники хоть раз в этом году по телефону?»; «Попадались ли Вы, ваши родственники, друзья или знакомые на уловки мошенников по телефону или сети Интернет?». Ответившим положительно на последний вопрос было предложено описать социальный портрет пострадавшего по таким критериям, как пол, возраст, образование, социальный статус, местность проживания. Ответы 249 студентов, являющихся будущими юристами, показали следующее:

1) структура ответивших на анкету студентов по полу: девушки — 81,5% (203 чел.), а юноши — 18,5% (46 чел.);

2) количество студентов, которым мошенники в данном календарном году звонили по телефону, — 189 чел. (75,9%); которым не звонили — 28 чел. (11,2%); не дозвонились, не звонили, но лицо получало сообщения (почта, мессенджер) — 32 чел. (12,9%);

3) количество студентов, признавшихся в том, что они сами, их родственники, друзья и знакомые попадались на уловки мошенников, составило 28,1% (70 чел.), при этом они сообщили о 75 известных им случаях.

На основе ответов обучающихся, ответивших утвердительно на последний вопрос, был составлен следующий социально-демографический портрет пострадавших от действий финансовых мошенников в первом полугодии 2024 г. (табл. 2).

Данные, представленные в таблице, несмотря на ограниченную рамками исследования выборку, во многом совпадают с выводами Банка России и других организаций о социальном портрете жертвы мошенничества с использованием информационно-телекоммуникационных технологий и подтверждают тот факт,

что жертвой мошенников может стать практически каждый человек, относящийся к любой социальной страте.

Таблица 2

Table 2

Социально-демографический портрет жертвы кибермошенников по результатам опроса обучающихся СЗИ, 2024, %

Socio-demographic portrait of a victim of cyber fraud based on the results of a survey of NWI students, 2024, %

Показатель	**Кол-во, чел.**	**Доля в общем объеме, %**
1. Пол		
— мужской	32	42,7
— женский	43	57,3
2. Преобладающий возраст, 25–44 лет	58	77,3
3. Уровень образования		
— общее среднее	24	32,0
— СПО	12	16,0
— неоконченное высшее	18	24,0
— высшее	21	28,0
4. Социальный статус		
— студент	15	20,0
— работающий	32	42,7
— пенсионер	28	37,3
5. Тип местности проживания		
— городская	60	80,0
— сельская	15	20,0

Полученные в ходе социологического опроса данные демонстрируют, что большинство студентов имели опыт общения с мошенниками как по телефону, так и через сеть Интернет. При этом более четверти из них столкнулись с потерей денежных средств. Это подтверждает необходимость обучения молодых людей навыкам защиты от мошенничества, развитию у них навыков критического мышления и анализа информации.

Заключение

Современное общество сталкивается с возрастающей угрозой кибермошенничества, которое может затронуть любого человека, независимо от его личных характеристик и социального статуса. Потенциальной жертвой мошенничества может стать человек любого возраста, пола, уровня образования, социального статуса, уровня дохода и типа местности проживания. Важно понимать, что защита граждан от действий мошенников в области финансов с применением

информационно-телекоммуникационных технологий становится сегодня приоритетной задачей для общества. Для решения данной проблемы необходимо активное информационное просвещение граждан о возможных угрозах, обучение основам информационной безопасности и формирование культуры ответственного поведения в сети Интернет. Только совместными усилиями государства, общественных организаций и граждан можно создать надежные механизмы защиты от финансовых мошенников и обеспечить безопасность каждому члену общества.

СПИСОК ЛИТЕРАТУРЫ

Батюкова В. Е. Предупреждение кибермошенничества в период COVID-19 // Образование и право. 2020. № 11.

Братусин А. Р., Власенко Е. Е. О проблемах, характерных индивидуально-типологических особенностях и поведенческих паттернах личности типичных жертв финансового мошенничества // Проблемы современного педагогического образования. 2019. № 64/4. С. 292–295.

Еськова Л. К., Рябчиков В. В. Новые преступные способы мошенничества в период пандемии коронавирусной инфекции // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2.

Камко А. С. Портрет жертвы мошенничества в сфере телекоммуникационных технологий // Власть и управление на Востоке России. 2017. № 3. С. 149–154.

Квятковский К. С. Преступления в сфере компьютерной информации, компьютерные преступления и киберпреступность: соотношение понятий // Молодой ученый. 2022. № 42. С. 108–112.

Мешкова Н. В., Кудрявцев В. Т. Ениколопов С. Н. К психологическому портрету жертв телефонного мошенничества // Вестник Московского университета. Серия 14. Психология. 2022. № 1. С. 138–157.

Мырзахмет А. А. Правовое обеспечение информационной безопасности Республики Казахстан // Молодой ученый. 2019. № 15. С. 119–122.

Репецкая А. Л., Петрякова Л. А. Виктимологическая характеристика мошенничеств в банковской сфере (по материалам Сибирского федерального округа) // Всероссийский криминологический журнал. 2022. № 4. С. 452–262.

Романовская М. Н. Мошеннические деяния по уголовному праву Китайской Народной республики // Евразийский Союз Ученых. 2017. № 4-2.

REFERENCES

Batyukova, V. E. (2020). Prevention of cyberbullying in the period of COVID-19. *Obrazovanie i pravo*, *11*. (In Russ.).

Bratusin, A. R., Vlasenko, E. E. (2019). On the problems, characteristic individual typological features and behavioral patterns of the personality of typical victims of finan-

cial fraud. *Problemy sovremennogo pedagogicheskogo obrazovaniya*, *64*(4), 292–295. (In Russ.).

Eskova, L. K., Ryabchikov, V. V. (2020). New criminal methods of fraud during the coronavirus pandemic. *Gumanitarnye, social'no-ekonomicheskie i obshchestvennye nauki*, *12*(2). (In Russ.).

Kamko, A. S. (2017). Portrait of a victim of fraud in the field of telecommunication technologies. *Vlast' i upravlenie na Vostoke Rossii*, *3*, 149–154. (In Russ.).

Kvyatkovsky, K. S. (2022). Crimes in the field of computer information, computer crimes and cybercrime: correlation of concepts. *Molodoj uchenyj*, *42*, 108–112. (In Russ.).

Meshkova, N. V., Kudryavtsev, V. T., Enikolopov, S. N. (2022). To the psychological portrait of victims of telephone fraud. *Vestnik Moskovskogo universiteta. Seriya 14. Psihologiya, 1*, 138–157. (In Russ.).

Myrzakhmet, A. A. (2019). Legal provision of information security of the Republic of Kazakhstan. *Molodoj uchenyj*, *15*, 119–122. (In Russ.).

Repetskaya, A.L., Petryakova, L.A. (2022). Victimological characteristics of fraud in the banking sector (based on the materials of the siberian federal district). *Vserossijskij kriminologicheskij zhurnal, 4*, 452–262. (In Russ.).

Romanovskaya, M. N. (2017). Fraudulent acts under the criminal law of the People's Republic of China. *Evrazijskij Soyuz Uchenyh*, 4(2). (In Russ.).

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Самойличенко Екатерина Евгеньевна — канд. экон. наук, доцент кафедры социально-гуманитарных дисциплин и правовой информатики Северо-Западного института (филиала) Университета имени О. Е. Кутафина (МГЮА), г. Вологда, Россия.

Ekaterina E. Samoilichenko — Cand. Sci (Economics), Associate Professor of the Department of Social and Humanitarian Disciplines and Legal Informatics, the North-West Institute (branch) of Kutafin Moscow State Law University (MSLA), Vologda, Russia.

Дятлева Мария Олеговна — студент Северо-Западного института (филиала) Университета имени О. Е. Кутафина (МГЮА), г. Вологда, Россия.

Maria O. Dyatleva — Student of the North-West Institute (branch) of Kutafin Moscow State Law University (MSLA), Vologda, Russia.

Цыкина Елизавета Алексеевна — студент Северо-Западного института (филиала) Университета имени О. Е. Кутафина (МГЮА), г. Вологда, Россия.

Elizaveta A. Tsykina — Student of the North-West Institute (branch) of Kutafin Moscow State Law University (MSLA), Vologda, Russia.

Статья поступила в редакцию 14.06.2024;
одобрена после рецензирования 10.12.2024;
принята к публикации 10.12.2024.
The article was submitted 14.06.2024;
approved after reviewing 10.12.2024;
accepted for publication 10.12.2024.