

Научная статья

УДК 343.2

DOI: 10.35854/2219-6242-2025-2-243-260

Виктимологические особенности хищений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации

Игорь Николаевич Бобровничай^{1✉}, Алексей Алексеевич Тайбаков²

^{1, 2} Северный институт — филиал Всероссийского государственного университета юстиции (РПА Минюста России), Петрозаводск, Россия

¹ bobrovnichyay@mail.ru[✉]

² kafedraugolrpa@mail.ru

Аннотация. Авторами проведен криминологический анализ преступлений, совершаемых с помощью информационно-телекоммуникационных технологий и компьютерной информации. Исследованы уровень, динамика и структура указанных преступлений в течение последних лет. На основе проанализированных данных статистики МВД России и материалов специализированных сайтов (приговоров) изучены наиболее распространенные способы хищений с использованием сети Интернет и средств мобильной связи. Рассмотрены прежде всего преобладающие в этой сфере виды мошенничества с применением электронных средств платежа (ст. 159.3. Уголовного кодекса РФ) и кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 Уголовного кодекса РФ). Основное внимание в статье уделено исследованию виктимологических особенностей преступлений, поскольку поведение жертв хищений, особенно мошенничества, имеет ярко выраженный виктимный характер, то есть потерпевший будто допускает совершение в отношении него противоправных действий. Причины такого поведения представляют научный интерес и имеют важное значение в целях профилактики хищений.

Ключевые слова: хищения, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, дистанционное мошенничество, кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 Уголовного кодекса РФ), виктимология, потерпевший, жертва преступления, классификация потерпевших, типы потерпевших, виктимность, виктимная ситуация, виктимологическая профилактика, предупреждение преступлений, кибервиктимология, виктимология цифровой преступности

Для цитирования: Бобровничай И. Н., Тайбаков А. А. Виктимологические особенности хищений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации // Социология и право. 2025. Т. 17. № 2. С. 243–260. <https://doi.org/10.35854/2219-6242-2025-2-243-260>

Victimological aspects of thievery committed using information and telecommunications technologies or in the field of computer information

Igor N. Bobrovnichiy^{1✉}, Aleksey A. Taibakov²

^{1, 2} Northern Institute — a branch of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Petrozavodsk, Russia

¹ bobrovnichiyin@mail.ru✉

² kafedraugolrpa@mail.ru

Abstract. We conducted a criminological analysis of crimes committed using information and telecommunications technologies and computer information. The level, dynamics, and structure of these crimes over the past years were studied. The analyzed statistical data of the Ministry of Internal Affairs of Russia and materials from specialized websites (sentences) were used to investigate the most common methods of thievery using the Internet and mobile communications. The work primarily examines the types of fraud, that are most common in this field, using electronic payment instruments (Article 159.3 of the Criminal Code of the Russian Federation) and theft from a bank account, as well as in relation to electronic funds (Article 158, Part 3, Item “d” of the Criminal Code of the Russian Federation). The article mainly focuses on the study of victimological aspects of crimes, since the behavior of victims of thievery, especially fraud, has a pronounced victim nature, that is, the victim seems to allow illegal actions to be committed against him. The reasons for such behavior are of scientific interest and are important for the prevention of theft.

Keywords: thefts committed using information and telecommunication technologies or in the field of computer information, remote fraud, thefts from a bank account, as well as in relation to electronic funds (Article 158, Part 3, Item “d” of the Criminal Code of the Russian Federation), victimology, wronged person, victim of a crime, classification of wronged persons, types of wronged persons, victimity, victim situation, victimological prevention, crime prevention, cyber victimology, victimology of digital crime

For citation: Bobrovnichiy I.N., Taibakov A.A. Victimological aspects of thievery committed using information and telecommunications technologies or in the field of computer information. *Sociology and Law*. 2025;17(2):243-260. <https://doi.org/10.35854/2219-6242-2025-2-243-260>

Введение

Борьба с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приобретает с каждым годом все большую актуальность.

Как показывает статистика, доля этих преступлений стремительно растет. В январе — декабре 2024 г. зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1 % больше, чем в аналогичный период прошлого года. В общем количестве зарегистрированных преступлений их удельный вес увеличился, от 34,8 % в январе — декабре 2023 г. до 40,0 % [1]. В январе — декабре 2023 г. таких преступлений зарегистрировано на 29,7 % больше, чем в аналогичный период 2022 г. В общем количестве зарегистрированных преступлений их удельный вес увеличился, от 26,5 % в январе — декабре 2022 г. до 34,8 % [2].

В 2022 г. рост преступлений этой категории незначителен: на 0,8 % больше, чем в аналогичный период прошлого года. В общем количестве зарегистрирован-

ных преступлений их удельный вес увеличился, от 25,8 % в январе — декабре 2021 г. до 26,5 % [3].

Анализ динамики преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации на протяжении последних трех лет, свидетельствует об их росте. В связи с этим особое значение имеют изучение особенностей таких преступлений и выявление причин, условий их совершения.

Характеризуя преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, следует указать, что четыре преступления из пяти (84,8 %) совершают с использованием сети Интернет (649,1 тыс.; +23,2 %), почти половина (45,2 %) — с помощью средств мобильной связи (346,0 тыс.; +14,3 %) [1]. Современные исследователи пишут о том, что «по состоянию на 2024 г. в России киберпреступность приобрела черты угрозы государственного масштаба» [4, с. 17]. Общий ущерб от таких преступлений, например в Республике Карелия, только в 2023 г. превысил 641 млн рублей [5].

Количество потерпевших по данным преступлениям превышает «полмиллиона человек в год», сталкивались с деятельностью мошенников в сфере информационно-телекоммуникационных технологий «десятки миллионов жителей России» [6]. Например, главными потерпевшими по банковским операциям без согласия клиентов выступают физические лица, а проблема утечек данных «затрагивает практически все активное население страны» [4, с. 18].

Ученые все больше указывают на связь глобализации с киберпространством. В современных условиях, по их мнению, «преступники нашли новую среду для своей деятельности, которая не требует от них находиться в той же географической близости, что и их жертвы» [7, с. 88]. Бороться с такого рода преступлениями особенно сложно.

В этих условиях очень важно, на наш взгляд, изучать не только способы совершения преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, но и их причины, личность преступников, а в первую очередь — особенности жертв преступлений. Процесс изучения жертв рассматриваемой категории преступлений активно развивается в рамках относительно новых научных направлений, в частности кибервиктимологии [8], виктимологии цифровой преступности [9]. В контексте упомянутых направлений исследуют прежде всего особенности виктимизации в киберпространстве. Зная эти особенности, можно повысить эффективность работы с потенциальными жертвами, что поможет предотвратить многие преступления.

В целом проведенное нами исследование поведения жертв хищений, особенно мошенничества, в современных условиях свидетельствует о том, что оно имеет ярко выраженный виктимный характер [10; 11; 12]. Иными словами, потерпевший будто допускает совершение в отношении него противоправных действий. Причины такого поведения представляют, на наш взгляд, особый научный интерес, поскольку имеют огромное значение для профилактики преступлений.

Теория

Изучая особенности жертв хищений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за основу мы взяли классификацию потерпевших по характеру их поведения, предложенную Д. В. Ривманом [13]. Он выделил следующие типы потерпевших: агрессивный, активный, инициативный, пассивный, некритический

и нейтральный. Согласно этой классификации, жертва может не провоцировать в отношении себя преступные действия (нейтральный тип) либо своим поведением так или иначе способствовать преступлению.

Названия типов жертв точно отражают особенности виктимного поведения. Пассивные — это лица, которые не оказывают должного противодействия преступным посягательствам. Некритичное поведение жертв часто связано с непониманием опасности виктимной ситуации ввиду личностных особенностей. Инициативные — лица, которые с учетом своей деятельности, носящей положительный, то есть социально значимый характер, могут стать жертвой. Особое внимание к себе привлекают жертвы, активно или даже агрессивно провоцирующие в отношении себя преступные действия умышленно или неосторожно.

В процессе исследования нами установлено, что активные и агрессивные типы жертв больше характерны для преступлений против личности [14]. Изучение преступлений против собственности указывает на преобладание жертв с некритичным или нейтральным поведением [15].

По данным за 2024 г., почти две трети рассматриваемых преступлений (63,5 %) совершено путем кражи или мошенничества [1]. Исследуемые кражи с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации совершены с банковского счета, равно как и в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 Уголовного кодекса (УК) РФ) [16].

Результаты и обсуждение

Анализ краж, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, показывает, что жертвы чаще характеризуются нейтральным типом поведения, по сути, не провоцируя преступные действия. Элементы некритичности могут быть связаны лишь с вопросами обеспечения сохранности денег и имущества.

Как показал анализ, жертвы чаще всего создают виктимную ситуацию, не обеспечивая сохранность собственных банковских счетов (карт, компьютеров, телефонов). В рассматриваемых преступлениях потерпевшие нередко бывают знакомы с похитителями. Например, в Самарской области за помощью в полицию обратился 55-летний слесарь, который сообщил, что ранее судимый односельчанин, находясь у него в доме, через сотовый телефон похитил крупную сумму денег с банковского счета. Допрошенный в качестве подозреваемого в совершении преступления, предусмотренного ч. 3 ст. 158 «Кража» УК РФ, сторож одной из организаций раскаялся и признал вину.

По версии следствия, подозреваемый пришел в дом к потерпевшему и попросил показать, как работает банковское приложение. Хозяин дома, не догадываясь о подвохе, ввел пароль, передал телефон гостю для изучения и вышел поставить чайник. Местный житель воспользовался ситуацией, оформил кредит на владельца расчетного счета и, получив одобрение, перевел кредитные средства односельчанина на свою банковскую карту. Общий ущерб, причиненный заявителю, составил 730 тыс. рублей [17].

В другом случае подсудимый Ф. совершил кражу, то есть тайно похитил с банковского счета чужое имущество, причинив тем самым значительный ущерб гражданину (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ). Это произошло при следующих обстоятельствах. По дороге в санаторий, в поезде, он познакомился с гражданином К. В пути К. потерял свои документы, банковские карты и деньги. Для получения доступа к деньгам в приложении К. воспользовался телефоном Ф., ввел свои паспортные данные и код. В итоге Ф.

получил доступ к банковскому счету К. и без его разрешения снял деньги на общую сумму 20 тыс. рублей [18]. Потерпевший после операций с деньгами просил Ф. удалить с телефона его данные.

Из приведенного примера следует, что жертвам исследуемых преступлений присущи такие качества личности, как неосторожность, доверчивость и легкомыслие. В рассматриваемом примере у потерпевшего К. виктимогенные качества личности проявляются уже в пути, когда он ехал в санаторий и потерял документы, деньги и банковские карты.

Анализ преступлений показывает, что банковскую карту часто похищают именно вследствие неосторожности и невнимательности потерпевшего. Показателен следующий пример. В дежурную часть линейного отдела полиции ЛУ МВД России на транспорте с заявлением обратилась жительница г. Краснодара. Она сообщила о том, что на автовокзале утерьяла банковскую карту, факт ее отсутствия обнаружила уже дома, увидев оповещения о списании денежных средств с ее счета. В ходе оперативно-розыскных мероприятий полицейские установили злоумышленника. Им оказалась 52-летняя жительница г. Краснодара, ранее судимая за кражу. Она пояснила полицейским, что, находясь вблизи входа в автовокзал, обнаружила на земле банковскую карту и произвела ряд незаконных списаний денежных средств с нее на общую сумму более 15 тыс. руб. В отношении подозреваемой возбуждено уголовное дело по признакам преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ [19].

В другой ситуации сын потерпевшей в магазине оставил при расчете за покупку банковскую карту матери [20]. Мать, пообщавшись с продавцами, смогла найти и вернуть ее. В данном случае потерпевшая по факту жертвой не стала, поскольку поведение ее виктимным не было, в отличие от неосторожного и беспечного (пассивного) поведения ее сына.

Сложно назвать виктимным и поведение близких родственников, которые становятся жертвами рассматриваемых преступлений. Так, подсудимая К., используя банковскую карту, которая принадлежала ее матери, осуществила вход и регистрацию в личном кабинете, получила доступ к счетам матери и тайно похитила денежные средства в размере 112 500 рублей [21]. В рассмотренном случае потерпевшей стала мать, поэтому завладеть злоумышленнице банковской картой было несложно. Становится понятным, что обстоятельства, связанные с родственными отношениями, способствуют совершению краж, и аналогичные преступления не редкость. Например, 29-летняя жительница г. Новокузнецка, имея долги в микрофинансовых организациях, а также другие долговые обязательства, решила погасить их, похитив деньги со счета матери. Дочь пришла к матери на работу и, воспользовавшись тем, что мать оставила без присмотра свой телефон, с помощью смартфона получила доступ к ее банковским картам. Затем в течение нескольких дней злоумышленница девять раз переводила на свой счет денежные суммы от 50 до 200 тыс. руб. После того, как потерпевшая заметила списание, она обратилась в полицию, и было возбуждено уголовное дело по ч. 3 ст. 158 «Кража» УК РФ [22]. Мать сразу начала подозревать в совершении преступления дочь, которая ранее совершала у нее мелкие хищения.

Тем не менее чаще всего жертвы анализируемых преступлений имеют некриминальный характер поведения. Они демонстрируют неосмотрительность и неумение оценить ситуацию.

Нередко причиной виктимного поведения потерпевших служит состояние алкогольного опьянения. Злоумышленники целенаправленно используют его, создавая себе благоприятные условия для хищения. Так, в г. Новосибирске перед судом предстанут трое мужчин, обвиняемые в серии краж и мошенничествах,

предусмотренных ч. 4 ст. 158, ч. 4 ст. 159, ч. 3 ст. 30, п. «а» ч. 4 ст. 158 УК РФ. В ходе предварительного следствия установлено, что с декабря 2022 г. по январь 2024 г. подозреваемые под видом оказания услуг такси совершили кражи имущества и хищения денежных средств с банковских счетов граждан. Как установили сотрудники полиции, руководитель группы распределил между участниками обязанности. Один из них высматривал в развлекательных заведениях посетителя в состоянии опьянения, а затем предлагал ему услуги такси. Далее, в пути, один из злоумышленников похищал имущество и передавал другому подозреваемому похищенную банковскую карту для обналичивания денежных средств. Кроме того, получив доступ к личным банковским счетам пострадавших, злоумышленники оформляли на них онлайн-кредиты. В ходе личного досмотра полицейские изъяли у задержанных четыре сим-карты, пять сотовых телефонов и банковскую карту. В результате противоправной деятельности шести гражданам и двум финансовым организациям причинен ущерб на общую сумму более 1 млн 300 тыс. рублей [23].

Опьянение жертвы позволило получить доступ к ее денежным средствам в следующем случае. Потерпевшая Т. попросила незнакомца А., чтобы он сначала зачислил деньги через банкомат на свою карту, а затем с этой карты перечислил деньги на указанный ею номер телефона. Она вложила в слот банкомата купюры, А. приложил свою карту. После того, как банкомат принял купюры, А. взял свою карту и ушел, несмотря на требования Т. вернуть деньги. После ухода А. потерпевшая позвонила в полицию. В ходе допроса, на стадии предварительного расследования, потерпевшая Т. сообщила, что в момент исследуемых событий находилась в состоянии опьянения [24]. В рассмотренном примере проявляется беспечное и некритичное поведение жертвы, обусловленное, очевидно, состоянием опьянения. Это поведение — главная причина преступлений.

Таким образом, жертвами рассматриваемых краж чаще становятся по причине легкомысленного и неосторожного поведения, обусловленного нередко родственными, дружественными отношениями или состоянием опьянения.

Особую тревогу в настоящее время вызывают дистанционные мошенничества или мошенничества, совершаемые с использованием информационно-телекоммуникационных технологий. Это подтверждается статистическими данными, которые приведены нами ранее. К таким видам мошенничества относятся мошенничество с использованием электронных средств платежей (ст. 159.3 УК РФ) [16], мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Указанные составы преступления в подразделениях органов дознания МВД РФ и следственных отделов МВД РФ часто именуют собирательным понятием «бесконтактные мошенничества» [25].

Как выявлено в процессе исследования, большинство жертв (потерпевших) мошенничества, на наш взгляд, можно отнести к некритичному, но активному типу, с ярко выраженной корыстной мотивацией (жадностью). Вероятно, что именно на этих качествах «играют» мошенники, обманывая жертв. Например, в отдел полиции Управления МВД России по г. Петрозаводску поступило заявление от 59-летней жительницы столицы Республики Карелия, которая сообщила, что ее ввели в заблуждение в результате мошеннических действий. На одном из сайтов она нашла информацию о заработке на инвестициях. Проводить обучение в этой сфере якобы должны были представители известного российского банка. Петрозаводчанка заинтересовалась, нажала виртуальную кнопку «звонить». Вскоре с ней связался незнакомец и предложил поработать с ведущим специалистом в области инвестиций А. Он был готов взять гражданку в команду. Требовалось лишь установить приложение для видеозвонков и онлайн-кошелек. После того, как петроза-

водчанка это сделала, А. позвонил ей, рассказал многое об инвестициях, биржах и вкладах, пообещал вести дальнейшее активное сотрудничество. Пенсионерку убедили перечислить «кассиру из инвестиционной команды» 10 500 руб., а затем ей пояснили, что теперь на ее счете появились первые 100 долларов. Для большего заработка были нужны более крупные вложения. Однако вкладывать сбережения и далее гражданка не захотела, перестала отвечать на навязчивые звонки инвестора. Позднее она поняла, что стала жертвой мошенников [26].

Похожим способом решила «разбогатеть» 67-летняя жительница города, которая в одном из онлайн-приложений увидела всплывающую рекламу от известной компании о дополнительном заработке на бирже. Кликнув на «окошечко», женщина заполнила специальную форму и указала свой номер телефона. После того, как она ввела нужные цифры, на экране возникло сообщение о том, что с ней свяжется специалист. Чуть позднее ей позвонил П., представившись финансовым аналитиком, сопровождающим инвесторов в онлайн-сделках. Мужчина уточнил, что все сделки проводятся в валюте, поэтому нужно обменять рубли на доллары. Он рассказал, как это делать при помощи «обменника». После объяснений заявительница оказалась в специальном чате в мессенджере. Следуя инструкциям П., она указывала в сообщении суммы, которые планировала перевести в валюту, а в ответ получала реквизиты счетов. На эти счета петрозаводчанка перечислила личные сбережения в надежде на то, что вложения вскоре окупятся. К тому же она оформила два кредита на общую сумму свыше 400 тыс. руб. и заняла часть средств у знакомых, не пояснив, для каких целей они ей понадобились. Эти деньги также женщина отправила на сторонние счета. Впоследствии лжеинвесторы перестали выходить на связь с горожанкой [27]. Попытки заработать на инвестициях привели жертву к потере денежных средств. Интернет-мошенники ввели ее в заблуждение. Ущерб составил 1 392 000 руб. Возбуждено уголовное дело по ч. 4 ст. 159 «Мошенничество, совершенное в особо крупном размере» УК РФ.

В течение дня сразу пять жителей Республики Карелия пострадали от действий мошенников. Их обманули разными способами, но все схемы обмана оказались стандартными [28]. В частности, в полицию поступило сообщение от 49-летней гражданки, которая перевела неизвестным более 1 250 000 руб. Женщина рассказала, что ей поступил звонок якобы от менеджера московской финансовой биржи, который предложил зарабатывать на продаже акций. Гражданка установила на телефон специальное приложение, затем под руководством собеседника стала переводить деньги. После того, как они закончились, оформила в банке кредит и заняла около 600 тыс. руб. у коллеги. Вывести прибыль не удалось, поскольку лжеинвесторы перестали выходить на связь.

В схожей ситуации оказалась и 49-летняя жительница Кондопоги, которой предложили дополнительный заработок при онлайн-вложениях. Она установила на телефон приложение и открыла брокерский счет. Чтобы пополнить его средствами, женщина уговорила супруга и его приятеля оформить кредиты в банках, а затем перевела более 2 500 000 на сторонние счета.

Житель Сегежи попался на аналогичную преступную уловку во второй раз. Мошенники под предлогом инвестирования похитили у него более 1 300 000 руб., и после этого мужчина обратился в полицию. Однако спустя время аферисты вышли на него вновь и пообещали помощь в выводе заработанных ранее денежных средств. В итоге они похитили у него еще 600 тыс. руб., которые были взяты в кредит.

В полицию Сортавалы поступило заявление от 30-летней горожанки, у которой путем обмана было похищено 400 тыс. руб. Она откликнулась на предложение

о дополнительном заработке, при этом требовалось ставить «лайки» продавцам на известной торговой площадке. Следуя инструкциям, женщина выкупала и некоторые товары. Она была уверена, что все расходы будут компенсированы. Однако в дальнейшем ей сообщили, что ее счет заблокирован, и, чтобы его разблокировать, требуется заплатить. В итоге женщина поняла, что стала жертвой обмана, и прекратила дальнейшие финансовые операции.

Итак, корыстные мотивы у жертв могут появляться по разнообразным поводам. Мошенники, используя дистанционные технологии, эксплуатируют различные потребности не критичных, но активных жертв. Складываются порой криминальные ситуации, в которых жертва мошенничества, будучи личностью с корыстной направленностью, одновременно совершает и корыстные противоправные действия. Например, в Смоленской области местную жительницу 1988 года рождения подозревают в хищении денег, которые она впоследствии перевела мошенникам. Она пояснила, что ранее, получив предложение о дополнительном доходе на биржевой платформе, переводила деньги на специальный счет, но ее обманули мошенники, похитив около 3 млн руб. В ходе опроса заявительницы установлено, что она, желая участвовать в биржевых сделках, похитила деньги у коллеги. Сначала женщина попросила у коллеги телефон, чтобы позвонить. Коллега передала ей в руки свой смартфон, а заявительница перешла в мобильное приложение банка, оформила на коллегу кредит и перевела 860 тыс. руб. на свою карту, а затем вложила в биржевую сделку.

Спустя время снова потребовались деньги, и женщина попросила у этой же коллеги телефон для звонка. На этот раз она после того, как вошла в приложение банка, увеличила лимит кредитной карты, принадлежащей коллеге, и перевела с нее около 360 тыс. руб. на свой счет, а затем снова вложилась в биржевую платформу. Когда заявительница поняла, что ее обманули мошенники, она призналась коллеге в хищении денег. Коллега ни о чем не подозревала и обратилась с заявлением в полицию. Возбуждены уголовные дела по признакам преступления, предусмотренного ч. 3 ст. 159 «Мошенничество» и ч. 3 ст. 158 «Кража» УК РФ [29]. Становится понятным, что корыстная направленность личности одновременно может стать причиной и виктимного поведения, и преступного.

Помимо распространенного корыстного мотива поведения жертвы, для обмана и незаконного обогащения мошенники нередко используют потребности в общении, признании и любви. Так, 68-летняя женщина из Барнаула познакомилась в социальных сетях с мужчиной и под воздействием обмана перевела ему на банковские счета более 600 тыс. рублей [30]. Интернет-знакомый убедительно писал ей о своих проблемах, и сердобольная женщина даже брала для него кредиты.

В этих мошенничествах, на наш взгляд, ярко выражены виктимные особенности потерпевших. С учетом специфики поведения жертвы данным преступлениям обычно свойственен латентный характер. Ввиду их особенностей раскрывать такого рода мошенничества сложно. Поэтому пострадавших в результате подобного обмана жертв может быть много.

Например, в Санкт-Петербурге в суд по преступлению такого рода направлено уголовное дело в отношении 44-летнего брачного афериста. Противоправную деятельность он вел около десяти лет, до момента задержания в марте 2023 г. За это время он успел обмануть 24 женщины, проживающие во Владимирской, в Московской, Ярославской, Тверской, Ленинградской, Волгоградской областях, Санкт-Петербурге, Нижнем Новгороде, Казани, Москве и Воронеже. Одна из его жертв проживала на территории сопредельного государства.

Под вымышленными именами злоумышленник регистрировался на сайтах знакомств и общался с жительницами регионов РФ. Войдя в доверие, назначал

избраннице встречу, ради которой готов был приехать даже из другого города. После пары свиданий мужчина обычно «искренне» влюблялся, предлагая даме сердца создать семью. Владея навыками психологических манипуляций, он находил индивидуальные подходы к компаньонкам, и многие женщины соглашались. Для подготовки к будущей совместной жизни злоумышленник просил избранниц помочь ему большими или маленькими суммами. Обнадеженные женщины отдавали ему личные сбережения, брали кредиты на свое имя или продавали недвижимость, иное имущество. После получения существенной суммы избранник обычно пропадал и больше на связь с потенциальной будущей супругой не выходил. Женщины пытались найти скрывшегося с их деньгами мужчину, но безуспешно, поскольку человека с такими данными не существовало, а его карты и счета были оформлены на третьих лиц. Суммарно все потерпевшие лишились более 34 000 000 рублей [31].

Жертвами такого рода мошенничеств, основанных на потребности в «любви», становятся и мужчины. Используя возможности интернета, обманывают их под видом женщин к тому же представители мужской половины. Например, в Петрозаводске мужчина в социальных сетях познакомился с девушкой, которая представилась жительницей Санкт-Петербурга. Встретиться с ней ему не удалось, но в качестве помощи он ей за четыре месяца перевел 330 тыс. руб. После этого страничка собеседницы в социальной сети оказалась заблокированной. Мужчина обратился в полицию. По данному факту возбуждено уголовное дело по признакам преступления, предусмотренного ст. 159 УК РФ. В результате оперативно-розыскных мероприятий полицейские установили, что в роли обаятельной незнакомки выступал 32-летний житель Петрозаводска. Подозреваемого задержали. В ходе обыска в его квартире были изъяты компьютерная техника, банковские карты и сим-карты, телефоны, другие предметы, имеющие доказательственное значение [32].

Как следует из рассмотренного примера, обману жертв способствовало виктимное поведение потерпевших, основанное на потребности в общении, признании и любви. К тому же существенное значение для связи с жертвой имеет использование преступниками возможностей интернета и социальных сетей.

С учетом изложенного становится очевидным, что мошенники чаще всего используют естественное желание людей удовлетворить свои потребности, что-то выгодно приобрести, получить компенсацию, стать богаче и счастливее. Это позволяет им, применяя информационно-телекоммуникационные технологии, легче найти жертву и обмануть ее.

Некорыстные типы тоже оказываются жертвами мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий. Распространенный предлог мошенников — «на вас оформлен кредит». Аферисты представляются сотрудниками портала «Госуслуги», ФСБ, Центробанка. Злоумышленники при помощи разных уловок прежде всего заставляют жертву паниковать и на эмоциях совершать различные финансовые операции. Они убеждают граждан в том, что злоумышленники воспользовались их данными и стали оформлять кредиты. После введения жертвы в заблуждение мошенники рассказывают, что для «спасения» сбережения нужно перечислить на некий безопасный счет. Так, 61-летний пенсионер, обманутый по этой схеме, обратился в отдел МВД России по Пудожскому району. Он рассказал, что лишился 456 тыс. руб. из личных накоплений, поверив, что некто оформил займ от его имени. Возбуждено уголовное дело по ч. 3 ст. 159 «Мошенничество, совершенное в крупном размере» УК РФ.

Аналогичным способом обманут 73-летний житель Сортавалы. В отделе полиции он рассказал, что обналичил 103 тыс. руб. по просьбе якобы сотрудника

службы безопасности банка и перевел их стороннему лицу [33]. В рассмотренных случаях, на наш взгляд, жертвы чаще имеют некритичный и даже пассивно-некритичный тип личности. Эти люди, как правило, легковнушаемы, пассивны, легковверны, с замедленными реакциями. В отличие от предыдущей категории потерпевших, они чаще некорыстны. Мошенники используют прежде всего такую сильную эмоцию, как «страх». У жертв искусственно, путем обмана, формируется вполне естественный страх потерять сбережения.

Иногда потерпевшие демонстрируют бдительность и пытаются критически мыслить, но злоумышленники проявляют упорство и настойчивость. Так, в полицию обратился 67-летний горожанин и сообщил, что у него похитили 123 тыс. руб. Полицейские установили обстоятельства произошедшего: для обмана использована стандартная схема, но с небольшими коррективами. В данном случае аферисты связались с пенсионером по телефону и представились сотрудниками полиции. Они сообщили, что в связи с участвовавшими случаями мошенничества ему следует срочно сменить номер телефона. Он отказался и не стал продолжать разговор. Жителю Петрозаводска снова сообщили, что его сбережения находятся под угрозой. Ему требовалось срочно пополнить свой счет на 340 000 руб., а спустя время их обналичить. Пенсионер не стал участвовать и в этом.

Но позднее аферистам все-таки удалось обмануть его, при этом банальным образом. Они предложили ему наиболее простой способ «спасти сбережения»: назвать номер банковской карты и код из сообщения. После того, как мужчина их назвал, деньги списали с его счета [34].

Лишь в некоторых ситуациях, по случайному (благоприятному) стечению обстоятельств, некритичным людям удастся не стать жертвой при покушении мошенников. Так, 42-летняя жительница села Алтайского края чуть не лишилась более полумиллиона рублей. Она дошла до последнего шага, то есть внесения денег, но банк заблокировал карту и вход в приложение [35].

В Архангельской области участковый уполномоченный полиции остановил мужчину от перевода денежных средств мошенникам. Ему позвонил руководитель строительного объекта и сообщил, что одного из его подчиненных, видимо, пытаются обмануть мошенники. Мужчина в течение нескольких часов непрерывно говорит по телефону, при этом речь идет о «безопасном счете». Один из коллег пытался объяснить ему, что, скорее всего, он общается с аферистами, но доверчивый гражданин отказался его слушать и продолжил разговор с мошенниками. Участковый уполномоченный прибыл на объект, зашел в помещение, но рабочий, не прерывая телефонного разговора, потребовал, чтобы полицейский вышел. Прислушавшись к разговору, участковый понял, что с 60-летним мужчиной действительно общаются телефонные аферисты. В итоге сотрудник полиции убедил его прервать разговор [36].

В Красноярске дистанционный обман пенсионерки пресекла артистка Музыкального театра. Она позвонила в полицию и сообщила, что встретила в торговом центре незнакомую пожилую женщину, которую, судя по ее поведению и разговорам, пытаются обмануть телефонные мошенники. Аферисты уговаривают бабушку пройти к другому банкомату, чтобы перевести крупную сумму денег. При этом бабушка игнорирует советы о том, чтобы не совершать такой финансовой операции, и направляется в отделение банка. По указанному адресу незамедлительно выехал наряд полиции. По прибытии полицейские поняли, что 72-летняя женщина общается с мошенниками, и отговорили ее от дальнейшего общения. В процессе разбирательства обнаружено, что потерпевшая успела снять со своего счета и перевести злоумышленникам 350 тыс. руб. Она готова была и дальше следовать указаниям незнакомцев, переводить им оставшиеся накопления [37].

Указанные качества — не критичность, пассивность, легковёрность — не всегда связаны с возрастом жертвы. Например, бдительная пенсионерка 84 лет не поверила мошеннику, представившемуся врачом [38]. Сообщив женщине по телефону о том, что «Ваш родственник попал в ДТП», то есть воспользовавшись распространенной мошеннической схемой, у нее пытались похитить более миллиона рублей. Но пенсионерка прекратила разговор и позвонила дочери, которая объяснила, что с ней все хорошо, аварии не было. Женщина поняла, что общалась с мошенниками, и незамедлительно сообщила об этом в полицию. В данном случае возбуждено уголовное дело по ч. 3 ст. 30, ч. 4 ст. 159 «Покушение на мошенничество в особо крупном размере» УК РФ. В этом примере отражена роль критичного мышления, помогающего не стать жертвами, прежде всего лицам нейтрального типа поведения.

Вместе с тем, как показывает исследование, некритичные, то есть неосмотрительные и неосторожные люди, в аналогичных ситуациях чаще всего становятся жертвами преступлений. Для их предупреждения необходимо информировать людей о возможных виктимных ситуациях обмана в сфере информационных технологий и развивать критичное мышление. Но, как указано ранее, в настоящее время способов мошеннических действий в сфере информационных технологий и компьютерной информации очень много, и они часто видоизменяются.

Мошенники все чаще используют социальную инженерию, и жертвы предоставляют необходимую информацию. Злоумышленники могут применять шпионские программы, которые передают все вводимые на устройстве данные, чтобы украсть пароли от интернет-банка. Они могут быть установлены на компьютер или телефон, если жертва перейдет по неизвестной ссылке, которая может быть отправлена, например, на электронную почту или в мессенджере [39].

Так, в Челябинской области задержали подозреваемого в неправомерном доступе к охраняемой законом компьютерной информации в виде логина и пароля доступа к персональной странице «Госуслуги». В результате доступ к странице законного пользователя был заблокирован. Потерпевшая не сразу осознала, что неизвестные, получив доступ к ее учетной записи, смогли воспользоваться ей по своему усмотрению. Сначала потерпевшая не смогла войти в свой аккаунт на портале «Госуслуги», а после восстановления учетной записи в МФЦ и проверки данных обнаружила, что посредством использования данных на ее имя оформлены кредит и заказы в рассрочку в интернет-магазинах. Возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 272 УК РФ [40].

Для совершения рассматриваемых преступлений злоумышленники используют разнообразные способы в сфере информационно-телекоммуникационных технологий и компьютерной информации. Так, 21-летний житель одного из сел Новосибирской области путем неправомерного доступа к охраняемой законом компьютерной информации, мошенническим способом, совершил хищения денежных средств с чужих банковских счетов и произвел ряд оформлений на граждан финансовых займов. Он приобретал сим-карты операторов сотовой связи, вычислял, какие из этих абонентских номеров их прошлые владельцы использовали в интернет-банкинге и не прекратили дистанционное обслуживание. Далее обвиняемый неправомерно получал доступ в личные кабинеты граждан через авторизацию в различных приложениях по СМС-сообщениям и, воспользовавшись чужими расчетными счетами, похищал имеющиеся на них деньги либо оформлял займы в микрофинансовых организациях. Для получения денежных средств, добытых преступным путем, гражданин указывал подконтрольные счета, получая денежные средства в личное пользование [41].

В приведенном примере прослеживаются элементы виктимного поведения жертв преступлений в сфере информационно-телекоммуникационных технологий и компьютерной информации. Прошлые владельцы использовали в интернет-банкинге сим-карты и не прекратили их дистанционное обслуживание. Этим и воспользовался обвиняемый.

Выводы

Таким образом, анализ рассмотренных преступлений свидетельствует о том, что виктимогенные факторы все больше связаны с развитием информационных технологий. Данные технологии формируют киберпространство, условия которого могут быть использованы в преступных целях. Эти факторы усложняют борьбу с преступностью такого рода. В таких условиях виктимное поведение зависит часто от того, как потерпевший ориентируется в компьютерной информации и информационно-телекоммуникационных технологиях.

Иными словами, человек может стать жертвой преступления в сфере информационных технологий ввиду недостаточной компетенции. Более того, в некоторых рассмотренных нами ситуациях потерпевший объективно не мог предвидеть и противодействовать преступным посягательствам.

Анализ краж с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации показывает, что жертвы этих преступлений чаще характеризуются нейтральным типом поведения, по сути, не провоцируя преступные действия. Элементы некритичности могут быть связаны лишь с вопросами обеспечения сохранности денег и имущества. Большинство жертв (потерпевших) мошенничества, на наш взгляд, можно отнести к некритичному, но активному типу, с ярко выраженной корыстной мотивацией (жадностью). Вероятно, что именно на этих качествах «играют» мошенники, обманывая жертв.

Корыстные мотивы у жертв могут появляться по разнообразным поводам. Мошенники, используя информационные технологии, эксплуатируют различные потребности некритичных, но активных жертв. Вместе с тем и некорыстные типы становятся жертвами мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий.

Помимо распространенного корыстного мотива поведения жертвы для обмана и незаконного обогащения, мошенники нередко используют даже потребности в общении, признании и любви. Существенное значение для связи с жертвой имеет использование преступниками возможностей интернета и социальных сетей.

В целом исследование подтверждает вывод о том, что мошенники используют вполне естественное желание людей удовлетворить свои потребности, что-то выгодно приобрести, получить компенсацию, стать богаче и счастливее. Это позволяет аферистам, применяя информационно-телекоммуникационные технологии, легче найти жертву и обмануть ее.

В приведенных случаях, на наш взгляд, жертвы чаще имеют некритичный и даже пассивно-некритичный тип личности. Эти люди, как правило, легковнушаемы, пассивны, легковверны, с замедленными реакциями. Мошенники нередко используют прежде всего такую сильную эмоцию, как страх. У жертв искусственно, путем обмана, формируется вполне естественный страх потерять сбережения. Иногда потерпевшие демонстрируют бдительность и пытаются критически мыслить, но злоумышленники проявляют упорство и настойчивость.

Рассмотренные качества — некритичность, пассивность, легковверность — не всегда связаны с возрастом жертвы. В этих случаях велика роль критичного мышления. Данный вид мышления помогает не стать жертвами, прежде всего

лицам нейтрального типа поведения. Вместе с тем, как показывает исследование, не критичные люди, то есть неосмотрительные и неосторожные, в аналогичных ситуациях чаще всего становятся жертвами преступлений. Для их предупреждения целесообразно информировать людей о возможных виктимных ситуациях обмана в сфере информационных технологий и развивать критическое мышление.

Итак, профилактика рассматриваемых преступлений с учетом их специфики требует разработки адекватных и постоянных мер правового и технического обеспечения безопасности в сфере информационно-телекоммуникационных технологий и компьютерной информации. Кроме виктимологической профилактики, следует повышать эффективность работы по выявлению и привлечению к уголовной ответственности лиц, совершающих преступления с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Список источников

1. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года // МВД России: офиц. сайт. URL: <https://xn--b1aew.xn--p1ai/reports/item/60248328/?ysclid=mb93hh6roj987292506> (дата обращения: 22.02.2025).
2. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2023 года // МВД России: офиц. сайт. URL: <https://xn--b1aew.xn--p1ai/reports/item/47055751/?ysclid=mb93l0pzx1440130902> (дата обращения: 22.02.2025).
3. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2022 года // МВД России: офиц. сайт. URL: <https://xn--b1aew.xn--p1ai/reports/item/35396677/?ysclid=mb93lmktxj890008102> (дата обращения: 22.02.2025).
4. Швыряев П. С. Киберпреступность как социальная проблема: стратегии противодействия: автореф. дис. ... канд. социол. наук. М., 2024. 30 с.
5. Отчет о деятельности МВД по Республике Карелия за 2023 год // МВД по Республике Карелия: офиц. сайт. URL: <https://10.xn--b1aew.xn--p1ai/activity/direction> (дата обращения: 10.10.2024).
6. Родина Е. А. Противодействие криминальной виктимизации пользователей сети Интернет в киберпространстве: автореф. дис. ... канд. юрид. наук. Саратов, 2022. 27 с.
7. Dolliver D. S., Love K. L. Criminogenic asymmetries in cyberspace: A comparative analysis of two Tor marketplaces // *Journal of Globalization Studies*. 2015. Vol. 5. No. 2. 2015. С. 75–96. URL: https://www.sociostudies.org/journal/files/jogs/2015_2/075-096.pdf (дата обращения: 10.10.2024).
8. Жмуров Д. В. Кибервиктимология. Грядущая неизбежность // Академический юридический журнал. 2021. Т. 22. № 1. С. 26–32. DOI: 10.17150/1819-0928.2021.22(1). 26-32
9. Майоров А. В. Виктимология цифровой преступности: концепция научного направления // Виктимология. 2024. Т. 11. № 1. С. 7–12. DOI: 10.47475/2411-0590-2024-11-1-7-12
10. Бобровнический И. Н., Голенок С. Г. Мошенничество как угроза криминологической безопасности личности // Правовая безопасность: сб. науч. ст. по материалам Междунар. науч. конф., посвященной 110-й годовщине со дня рождения Ю. В. Андропова и 70-летию со дня образования КГБ при Совете Министров СССР. Петрозаводск: Северный институт (филиал) Всероссийского государственного университета юстиции, 2024. С. 51–72.
11. Говоров Е. А., Бобровнический И. Н. Некоторые особенности противодействия современному мошенничеству в Алтайском крае // Общество. Экономика. Культура: актуальные проблемы, практика решения: сб. науч. ст. XIII Междунар. науч.-практ. конф. (Барнаул, 19–20 апреля 2023 г.) / под общ. ред. Г. М. Гриценко. Барнаул: Алтайский государственный технический университет имени И. И. Ползунова, 2023. С. 124–134.
12. Аникаева О. В., Бобровнический И. Н. Особенности преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в современных условиях // Социология и право. 2023. Т. 15. № 4. С. 565–577. DOI: 10.35854/2219-6242-2023-4-565-577

13. Ривман Д. В. Виктимологические факторы и профилактика преступлений: учеб. пособие. Л.: Изд-во ВПУ МВД СССР, 1975. 153 с.
14. Бобровнический И. Н. Виктимологические аспекты преступлений против личности: социологический анализ // Социология и право. 2022. Т. 14. № 2. С. 130–139. DOI: 10.35854/2219-6242-2022-2-130-139
15. Бобровнический И. Н. Виктимологические особенности преступлений против собственности в современных условиях // Социология и право. 2023. Т. 15. № 3. С. 383–398. DOI: 10.35854/2219-6242-2023-3-383-398
16. Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. № 63-ФЗ (в ред. от 03.04.2023) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.
17. В Самарской области полицейскими задержан подозреваемый в краже денег с банковской карты // МВД России: офиц. сайт. 2025. 18 марта. URL: <https://xn--b1aew.xn--p1ai/news/item/62808997?ysclid=mb96u7016w265132856> (дата обращения: 22.04.2025).
18. Приговор Эжвинского районного суда г. Сыктывкара (Республика Коми) от 29 июля 2024 г. по делу № 1-69/2024 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/ba5MgcY7tgWC/?ysclid=mbjgxe9n5b799548687> (дата обращения: 22.03.2025).
19. Сотрудники транспортной полиции раскрыли кражу денежных средств с банковской карты // МВД России: офиц. сайт. 2025. 22 марта. URL: <https://xn--b1aew.xn--p1ai/news/item/62887448?ysclid=mb96vd3drj700203583> (дата обращения: 10.04.2025).
20. Приговор Октябрьского районного суда г. Барнаула Алтайского края от 29 ноября 2021 г. по делу № 1-850/2021 // Государственная автоматизированная система РФ «Правосудие». URL: <https://bsr.sudrf.ru/big5/portal.html> (дата обращения: 25.12.2023).
21. Приговор Октябрьского районного суда г. Барнаула Алтайского края от 19 марта 2021 г. по делу № 1-225/2021 // Государственная автоматизированная система РФ «Правосудие». URL: <https://bsr.sudrf.ru/big5/portal.html> (дата обращения: 15.04.2023).
22. В Кемеровской области перед судом предстанет местная жительница, которая похитила со счета своей матери крупную сумму денег // МВД России: офиц. сайт. 2025. 6 февраля. URL: <https://xn--b1aew.xn--p1ai/news/item/61011844/?ysclid=mb96wfv2bo514331281> (дата обращения: 10.02.2025).
23. В Новосибирске перед судом предстанут трое мужчин, обвиняемые в серии краж и мошенничествах // МВД России: офиц. сайт. 2025. 30 января. URL: <https://xn--b1aew.xn--p1ai/news/item/60717046?ysclid=mb96xtsifg971411092> (дата обращения: 10.03.2025).
24. Приговор Бийского городского суда г. Барнаула Алтайского края от 9 декабря 2022 г. по делу № 1-867/2022 // Государственная автоматизированная система РФ «Правосудие». URL: <https://bsr.sudrf.ru/big5/portal.html> (дата обращения: 25.04.2022).
25. Журихина А. В. Проблема раскрытия преступлений, связанных с дистанционным хищением денежных средств с банковских счетов // Молодой ученый. 2023. № 16. С. 182–184.
26. Мошенники под видом сотрудников банка вовлекли петрозаводчанку в «инвесторскую деятельность» // МВД России по Республике Карелия: офиц. сайт. 2024. 24 октября. URL: <https://10.xn--b1aew.xn--p1ai/news/item/56349452/> (дата обращения: 27.02.2025).
27. Жительница Петрозаводска лишилась более 1 300 000 рублей, желая получить дополнительный заработок // МВД России по Республике Карелия: офиц. сайт. 2024. 29 октября. URL: <https://10.xn--b1aew.xn--p1ai/news/item/56585013/> (дата обращения: 27.02.2025).
28. Более семи миллионов рублей перевели мошенникам жители Карелии за один день // МВД России по Республике Карелия: офиц. сайт. 2024. 24 октября. URL: <https://10.xn--b1aew.xn--p1ai/news/item/56381242/?year=2024&month=12&day=8> (дата обращения: 24.02.2025).
29. В Смоленской области местная жительница подозревается в хищении денег, которые она впоследствии перевела мошенникам // МВД России: офиц. сайт. 2025. 30 января. URL: <https://67.xn--b1aew.xn--p1ai/news/item/60703545/> (дата обращения: 24.03.2025).
30. Барнаульская пенсионерка, познакомившись с «французом» в Интернете, лишилась более 600 000 рублей // Главное управление МВД России по Алтайскому краю:

- офиц. сайт. 2023. 9 февраля. URL: <https://22.xn--b1aew.xn--p1ai/news/item/35606873> (дата обращения: 24.03.2025).
31. В Санкт-Петербурге направлено в суд уголовное дело в отношении брачного афериста // МВД России: офиц. сайт. 2025. 14 февраля. URL: <https://78.xn--b1aew.xn--p1ai/news/item/61354946> (дата обращения: 24.03.2025).
32. В Петрозаводске полицейские задержали местного жителя, который под видом девушки обманывал интернет-пользователей // МВД России: офиц. сайт. 2022. 11 марта. URL: <https://xn--b1aew.xn--p1ai/news/item/28949555?ysclid=mb96b9v4jc662812941> (дата обращения: 22.03.2025).
33. Мошенники активно обманывают жителей районов Карелии // МВД России по Республике Карелия: офиц. сайт. 2024. 12 сентября. URL: <https://10.xn--b1aew.xn--p1ai/news/item/54922450/> (дата обращения: 24.02.2025).
34. Мошенники долго искали способ, как обмануть жителя Петрозаводска // Главное управление МВД России по Алтайскому краю: офиц. сайт. 2024. 7 октября. URL: <https://10.xn--b1aew.xn--p1ai/news/item/55920638/> (дата обращения: 24.02.2025).
35. Жительница Бийского района чуть не лишилась более полутора миллиона рублей // Главное управление МВД России по Алтайскому краю: офиц. сайт. 2023. 12 марта. URL: <https://22.xn--b1aew.xn--p1ai/news/item/36368003/> (дата обращения: 15.02.2025).
36. В Архангельской области участковый уполномоченный полиции остановил мужчину от перевода денежных средств мошенникам // МВД России: офиц. сайт. 2025. 21 марта. URL: <https://xn--b1aew.xn--p1ai/news/item/63005350/?ysclid=mb96i8h0we607033779> (дата обращения: 15.04.2025).
37. Полицейские Красноярска поблагодарили артистку Музыкального театра, которая пресекла дистанционный обман пенсионерки // МВД России: офиц. сайт. 2025. 21 марта. URL: <https://24.xn--b1aew.xn--p1ai/news/item/62983223/> (дата обращения: 15.04.2025).
38. Бдительная пенсионерка не поверила мошеннику, представившемуся врачом // Главное управление МВД России по Алтайскому краю: офиц. сайт. 2023. 9 марта. URL: <https://22.xn--b1aew.xn--p1ai/news/item/36243660/> (дата обращения: 15.02.2025).
39. Юрист рассказал о способах кражи мошенниками денег с банковских счетов // Известия. 2023. 27 октября. URL: <https://iz.ru/1595892/2023-10-27/iurist-rasskazal-o-sposobakh-krazhi-moshennikami-deneg-s-bankovskikh-schetov> (дата обращения: 15.02.2025).
40. Оперативники задержали в Челябинской области подозреваемого в неправомерном доступе к компьютерной информации // МВД России: офиц. сайт. 2025. 6 февраля. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/%D1%83%D0%B1%D0%BA/Publikacii_i_vistuplenija/item/61030991/?ysclid=mb96oarc7h73457164 (дата обращения: 24.03.2025).
41. В Новосибирске расследовано уголовное дело в отношении мужчины, обвиняемого в совершении серии преступлений в информационно-телекоммуникационной сфере // МВД России: офиц. сайт. 2025. 5 февраля. URL: <https://xn--b1aew.xn--p1ai/news/item/60953044/?ysclid=mb96q9x0ad432916503> (дата обращения: 24.03.2025).

References

1. Brief description of the state of crime in the Russian Federation for January-December 2024. Ministry of Internal Affairs of Russia official website. URL: <https://xn--b1aew.xn--p1ai/reports/item/60248328?ysclid=mb93hh6roj987292506> (accessed on 22.02.2025). (In Russ.).
2. Brief description of the state of crime in the Russian Federation for January-December 2023. Ministry of Internal Affairs of Russia official website. URL: <https://xn--b1aew.xn--p1ai/reports/item/47055751?ysclid=mb93l0pzx1440130902> (accessed on 22.02.2025). (In Russ.).
3. Brief description of the state of crime in the Russian Federation for January-December 2022. Ministry of Internal Affairs of Russia official website. URL: <https://xn--b1aew.xn--p1ai/reports/item/35396677?ysclid=mb93lmktxj890008102> (accessed on 22.02.2025). (In Russ.).
4. Shvyryaev P.S. Cybercrime as a social problem: Countermeasure strategies. Cand. sociol. sci. diss. Synopsis. Moscow, 20254. 30 p. (In Russ.).

5. Report on the activities of the Ministry of Internal Affairs in the Republic of Karelia for 2023. Ministry of Internal Affairs in the Republic of Karelia official website. URL: <https://10.xn--blaew.xn--p1ai/activity/direction> (accessed on 10.10.2024). (In Russ.).
6. Rodina E.A. Combating criminal victimization of Internet users in cyberspace. Cand. legal sci. diss. Synopsis. Saratov, 2022. 27 p. (In Russ.).
7. Dolliver D.S., Love K.L. Criminogenic asymmetries in cyberspace: A comparative analysis of two Tor marketplaces. *Journal of Globalization Studies*. 2015;5(2):75-96. URL: https://www.sociostudies.org/journal/files/jogs/2015_2/075-096.pdf (accessed on 10.10.2024).
8. Zhmurov D.V. Cyber victimology: The impending inevitability. *Akademicheskii yuridicheskii zhurnal = Academic Law Journal*. 2021;22(1):26-32. (In Russ.). DOI: 10.17150/1819-0928.2021.22(1).26-32
9. Mayorov A.V. Victimology of digital crime: Research direction concept. *Viktimologiya = Victimology*. 2024;11(1):7-12. (In Russ.). DOI: 10.47475/2411-0590-2024-11-1-7-12
10. Bobrovnichiy I.N., Golenok S.G. Fraud as a threat to criminological security of the individual. In: Legal security. Proc. Int. sci. conf. dedicated to the 110th anniversary of the birth of Yu.V. Andropov and the 70th anniversary of the formation of the KGB under the Council of Ministers of the USSR. Petrozavodsk: Northern Institute (branch) All-Russian State University of Justice; 2024:51-72. (In Russ.).
11. Govorov E.A., Bobrovnichiy I.N. Some features of combating modern fraud in the Altai Territory. In: Gritsenko G.M., ed. Society. Economy. Culture: Current issues, solution practices. Proc. 13th Int. sci.-pract. conf. (Barnaul, April 19-20, 2023). Barnaul: Polzunov Altai State Technical University; 2023:124-134. (In Russ.).
12. Anikayeva O.V., Bobrovnichiy I.N. Characteristics of crimes committed with the use of information and telecommunication technologies or in the sphere of computer information in modern conditions. *Sotsiologiya i pravo = Sociology and Law*. 2023;15(4):565-577. (In Russ.). DOI: 10.35854/2219-6242-2023-4-565-577
13. Rivman D.V. Victimological factors and crime prevention. Leningrad: Higher Political School of the USSR Ministry of Internal Affairs; 1975. 153 p. (In Russ.).
14. Bobrovnichiy I.N. Victimological aspects of crimes against the person: Sociological analysis. *Sotsiologiya i pravo = Sociology and Law*. 2022;14(2):130-139. (In Russ.). DOI: 10.35854/2219-6242-2022-2-130-139
15. Bobrovnichiy I.N. Victimological features of property crimes against property in current conditions. *Sotsiologiya i pravo = Sociology and Law*. 2023;15(3):383-398. (In Russ.). DOI: 10.35854/2219-6242-2023-3-383-398
16. Criminal Code of the Russian Federation. Federal Law of June 13, 1996 No. 63-FZ (as amended on April 3, 2023). Konsul'tantPlyus. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (In Russ.).
17. In the Samara region, police detained a suspect in the theft of money from a bank card. Ministry of Internal Affairs of Russia official website. Mar. 18, 2025. URL: <https://xn--blaew.xn--p1ai/news/item/62808997?ysclid=mb96u7016w265132856> (accessed on 22.04.2025). (In Russ.).
18. Sentence of the Ezhvinsky District Court of Syktyvkar (Komi Republic) dated July 29, 2024 in case No. 1-69/2024. Judicial and Regulatory Acts of the Russian Federation. URL: <https://sudact.ru/regular/doc/ba5MgcY7tgWC/?ysclid=mbjgxe5b799548687> (accessed on 22.03.2025). (In Russ.).
19. Transport police officers solved the theft of funds from a bank card. Ministry of Internal Affairs of Russia official website. Mar. 22, 2025. URL: <https://xn--blaew.xn--p1ai/news/item/62887448?ysclid=mb96vd3drj700203583> (accessed on 10.04.2025). (In Russ.).
20. Verdict of the Oktyabrsky District Court of Barnaul, Altai Krai, dated November 29, 2021, in case No. 1-850/2021. Pravosudie. URL: <https://bsr.sudrf.ru/big5/portal.html> (accessed on 25.12.2023). (In Russ.).
21. Verdict of the Oktyabrsky District Court of Barnaul, Altai Krai, dated March 19, 2021 in case No. 1-225/2021. Pravosudie. URL: <https://bsr.sudrf.ru/big5/portal.html> (accessed on 15.04.2023). (In Russ.).
22. In the Kemerovo region, a local resident will appear in court for stealing a large sum of money from her mother's account. Ministry of Internal Affairs of Russia official

- website. Feb. 06, 2025. URL: <https://xn--b1aew.xn--p1ai/news/item/61011844/?ysclid=mb96wfv2bo514331281> (accessed on 10.02.2025). (In Russ.).
23. Three men accused of a series of thefts and frauds will appear in court in Novosibirsk. Ministry of Internal Affairs of Russia official website. Jan. 30, 2025. URL: <https://xn--b1aew.xn--p1ai/news/item/60717046?ysclid=mb96xtsifg971411092> (accessed on 10.03.2025). (In Russ.).
 24. Verdict of the Biysk City Court of Barnaul, Altai Krai, dated December 9, 2022 in case No. 1-867/2022. Pravosudie. URL: <https://bsr.sudrf.ru/bigs/portal.html> (accessed on 25.04.2022). (In Russ.).
 25. Zhurikhina A.V. The problem of solving crimes related to remote theft of funds from bank accounts. *Molodoi uchenyi = Young Scientist*. 2003;(16):182-184. (In Russ.).
 26. Fraudsters posing as bank employees involved a resident of Petrozavodsk in “investment activities”. Ministry of Internal Affairs of Russia for the Republic of Karelia official website. Oct. 24, 2024. URL: <https://10.xn--b1aew.xn--p1ai/news/item/56349452/> (accessed on 27.02.2025). (In Russ.).
 27. A resident of Petrozavodsk lost more than 1,300,000 rubles, wanting to earn additional income. Ministry of Internal Affairs of Russia for the Republic of Karelia official website. Oct. 29, 2024. URL: <https://10.xn--b1aew.xn--p1ai/news/item/56585013/> (accessed on 27.02.2025). (In Russ.).
 28. Residents of Karelia transferred more than seven million rubles to scammers in one day. Ministry of Internal Affairs of Russia for the Republic of Karelia official website. Oct. 24, 2024. URL: <https://10.xn--b1aew.xn--p1ai/news/item/56381242/?year=2024&month=12&day=8> (accessed on 24.02.2025). (In Russ.).
 29. In the Smolensk region, a local resident is suspected of stealing money, which she subsequently transferred to fraudsters. Ministry of Internal Affairs of Russia official website. Jan. 30, 2025. URL: <https://67.xn--b1aew.xn--p1ai/news/item/60703545/> (accessed on 24.03.2025). (In Russ.).
 30. A pensioner from Barnaul, having met a “Frenchman” on the Internet, lost more than 600,000 rubles. Main Directorate of the Ministry of Internal Affairs of Russia for the Altai Territory official website. Feb. 09, 2023. URL: <https://22.xn--b1aew.xn--p1ai/news/item/35606873> (accessed on 24.03.2025). (In Russ.).
 31. In St. Petersburg, a criminal case against a marriage swindler has been sent to court. Ministry of Internal Affairs of Russia official website. Feb. 14, 2025. URL: <https://78.xn--b1aew.xn--p1ai/news/item/61354946> (accessed on 24.03.2025). (In Russ.).
 32. In Petrozavodsk, police detained a local resident who, posing as a girl, deceived Internet users. Ministry of Internal Affairs of Russia official website. Mar. 11, 2022. URL: <https://xn--b1aew.xn--p1ai/news/item/28949555?ysclid=mb96b9v4jc662812941> (accessed on 22.03.2025). (In Russ.).
 33. Fraudsters are actively deceiving residents of Karelia districts. Ministry of Internal Affairs of Russia for the Republic of Karelia official website. Sep. 12, 2024. URL: <https://10.xn--b1aew.xn--p1ai/news/item/54922450/> (accessed on 24.02.2025). (In Russ.).
 34. Fraudsters have long sought a way to deceive a resident of Petrozavodsk. Main Directorate of the Ministry of Internal Affairs of Russia for the Altai Territory official website. Oct. 07, 2024. URL: <https://10.xn--b1aew.xn--p1ai/news/item/55920638/> (accessed on 24.02.2025). (In Russ.).
 35. A resident of the Biysk region almost lost more than half a million rubles. Main Directorate of the Ministry of Internal Affairs of Russia for the Altai Territory official website. Mar. 12, 2023. URL: <https://22.xn--b1aew.xn--p1ai/news/item/36368003/> (accessed on 15.02.2025). (In Russ.).
 36. In the Arkhangelsk region, a district police officer stopped a man from transferring money to fraudsters. Ministry of Internal Affairs of Russia official website. Mar. 21, 2025. URL: <https://xn--b1aew.xn--p1ai/news/item/63005350/?ysclid=mb96i8h0we607033779> (accessed on 15.04.2025). (In Russ.).
 37. Krasnoyarsk police thanked the artist of the Musical Theater who stopped a pensioner from being deceived remotely. Ministry of Internal Affairs of Russia official website. Mar. 21, 2025. URL: <https://24.xn--b1aew.xn--p1ai/news/item/62983223/> (accessed on 15.04.2025). (In Russ.).

38. A vigilant pensioner did not believe a fraudster who introduced himself as a doctor. Main Directorate of the Ministry of Internal Affairs of Russia for the Altai Territory official website. Mar. 09, 2023. URL: <https://22.xn--b1aew.xn--p1ai/news/item/36243660/> (accessed on 15.02.2025). (In Russ.).
39. Lawyer talks about how fraudsters steal money from bank accounts. Izvestiya. Oct. 27, 2023. URL: <https://iz.ru/1595892/2023-10-27/iurist-rasskazal-o-sposobakh-krazhi-moshennikami-deneg-s-bankovskikh-schetov> (accessed on 15.02.2025). (In Russ.).
40. Operatives detained a suspect in the Chelyabinsk region for illegal access to computer information. Ministry of Internal Affairs of Russia official website. Feb. 06, 2025. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/%D1%83%D0%B1%D0%BA/Publikacii_i_vistuplenija/item/61030991/?ysclid=mb96oarc7h73457164 (accessed on 24.03.2025). (In Russ.).
41. In Novosibirsk, a criminal case has been investigated against a man accused of committing a series of crimes in the information and telecommunications sector. Ministry of Internal Affairs of Russia official website. Feb. 05, 2025. URL: <https://xn--b1aew.xn--p1ai/news/item/60953044/?ysclid=mb96q9x0ad432916503> (accessed on 24.03.2025). (In Russ.).

Информация об авторах

И. Н. Бобровничай — кандидат педагогических наук, доцент, заведующий кафедрой социально-экономических, гуманитарных и специальных дисциплин; 185005, Республика Карелия, Петрозаводск, Онежской флотилии ул., д. 51;

А. А. Тайбаков — доктор юридических наук, доцент, заведующий кафедрой уголовного права и процесса, заслуженный юрист Российской Федерации, заслуженный юрист Республики Карелия; 185005, Республика Карелия, Петрозаводск, Онежской флотилии ул., д. 51.

Information about the authors

I. N. Bobrovnichiy — PhD in Pedagogy, Associate Professor, Head of the Department of Socio-Economic, Humanitarian and Special Disciplines; 51 Onega flotilla st., Petrozavodsk, Republic of Karelia, 185005, Russia;

A. A. Taibakov — Doctor of Law, Associate Professor, Head of the Department of Criminal Law and Procedure, Honored Lawyer of the Russian Federation, Honored Lawyer of the Republic of Kazakhstan; 51 Onega flotilla st., Petrozavodsk, Republic of Karelia, 185005, Russia.

Конфликт интересов: авторы декларируют отсутствие конфликта интересов, связанных с публикацией данной статьи.

Conflict of interest: the authors declare no conflict of interest related to the publication of this article.

Статья поступила в редакцию 23.04.2025; одобрена после рецензирования 12.05.2025; принята к публикации 20.06.2025.

The article was submitted 23.04.2025; approved after reviewing 12.05.2025; accepted for publication 20.06.2025.