УДК 343.9

ПРЕДУПРЕЖДЕНИЕ КИБЕРМОШЕННИЧЕСТВА: ВИКТИМОЛОГИЧЕСКИЙ АСПЕКТ

Светлана Михайловна Голятина
Волгоградская академия МВД России, Волгоград, Россия, sgoliatina@mvd.ru

Аннотация. В статье приводятся актуальные статистические данные о состоянии киберпреступности в России в 2022—2024 гг. Указывается, что на протяжении последних нескольких лет наибольший удельный вес в ее структуре имеет дистанционное (телефонное и компьютерное) мошенничество. Представлен усредненный портрет лица, пострадавшего от действий злоумышленников. Особое внимание уделяется анализу субъективных виктимогенных факторов — личностных и поведенческих качеств человека, которые позволяют ему стать жертвой преступления. В число таких входят низкий уровень цифровой грамотности, доверчивость, наивный оптимизм, жажда легкой наживы, ответственность, склонность к овершерингу. Отмечается, что последняя выступает основой мошенничества с использованием технологии Deepfake, так как дает злоумышленникам возможность генерировать реалистичные изображения из тех, что размещаются в социальных сетях в открытом доступе, и в дальнейшем использовать их в преступных целях. Делается вывод о том, что главным инструментом предупреждения киберпреступности должна стать работа с субъективными виктимогенными факторами, направленная на развитие у потенциальных жертв критического мышления, эмоционального интеллекта, формирование навыков распознавания манипуляций и противодействия им.

Ключевые слова: киберпреступность, мошенничество, жертва, виктимное поведение, субъективные виктимогенные факторы, девиктимизация.

Для цитирования: Голятина С. М. Предупреждение кибермошенничества: виктимологический аспект // Вестник Волгоградской академии МВД России. 2025. № 4 (75). С. 31—36.

CYBERFRAUD PREVENTION: VICTIMOLOGIC ASPECT

Svetlana Mikhailovna Golyatina
Volgograd Academy of the Ministry of the Interior of Russia, Volgograd, Russia, sgoliatina@mvd.ru

Abstract. This article deals with the latest statistic data related to the situation with cybercrime in Russia in 2022—2024 time period. The author of the article notes that for the recent several years remote (telephone and computer) fraud has accounted for the largest share of cybercrime. There is an average profile of a victimized person. The author pays a great attention to the analysis of subjective victimogenic factors, i. e. personal and behavioral human qualifications that let a person become a victim of the mentioned crime. These factors include low digital literacy, gullibility, naive optimism, greed for profit, responsibility and a tendency to oversharing. The author also notes that the latter is the basis for fraud applying Deepfake technology as it gives criminals an opportunity to create realistic images from those ones posted publicly on social media and then to use them for criminal purposes. The author concludes that the primary tool to prevent cybercrime should be dealing with subjective victimogenic factors aimed at developing critical thinking, emotional intelligence of potential victims as well as forming skills to recognize manipulations and counteract them.

Keywords: cybercrime, fraud, a victim, victim behavior, subjective victimization factors, devictimization

For citation: Golyatina S. M. Cyberfraud prevention: victimologic aspect. Journal of the Volgograd Academy of the Ministry of the Interior of Russia, 31—36, 2025. (In Russ.).

В последние годы в России киберпреступность стала носить характер национального бедствия. Данный тезис подтверждается количеством зарегистрированных уголовно наказуемых деяний, увеличивающимся из года в год (522 100 в 2022 г., 677 000 в 2023 г., 765 400 в 2024 г.[1]), суммой ущерба, нанесенного экономике страны (91 млрд руб. в 2022 г., 156 млрд руб. в 2023 г.[2], более 200 млрд руб. в 2024 г.[3]), а также тем, что в настоящее время киберпреступники все чаще совершают посягательства на критически важную инфраструктуру (учреждения здравоохранения, топливно-энергетический комплекс, транспортные системы и т. д.), что может повлечь за собой массовый коллапс и поставить на карту жизни и здоровье людей. Президент Российской Федерации В. В. Путин, говоря о подписании Конвенции Организации Объединенных Наций против киберпреступности, подчеркнул: «Преступления такого рода, зачастую тесно связанные с терроризмом и пропагандой экстремистской идеологии, незаконным оборотом наркотиков и оружия, представляют серьезную угрозу безопасности как отдельных граждан, так и целых государств»[4].

На протяжении нескольких лет наибольший удельный вес в структуре киберпреступности имеет дистанционное мошенничество — хищение путем обмана или злоупотребления доверием, совершаемое удаленно с использованием телефонных или компьютерных сетей. Так, в 2022 г. в России было зарегистрировано 257 606 кибермошенничеств, в 2023 г. — 356 079, в 2024 г. — 380 344[5]. Несмотря на оповещения в средствах массовой информации об используемых злоумышленниками схемах, невзирая на распространение банками и полицией памяток, предупреждающих о недопустимости перевода денежных средств незнакомым лицам, практически ежедневно сотрудники правоохранительных органов регистрируют заявления граждан о совершении в отношении них дистанционных мошенничеств. С учетом того что раскрытие данных преступлений составляет порядка 23 %[6], а их расследование сопровождается рядом трудностей, большое значение приобретает «деятельность государства и общества, направленная против возможного, но еще не задуманного, задуманного или готовящегося, а также происходящего, но еще не оконченного преступления» [1, с. 60], т. е. предупреждение. Выразим согласие с точкой зрения И. М. Антонова, Н. В. Бойко о том, что оно «может быть обеспечено и за счет активизации самого потерпевшего, повышения его защитительных возможностей, укрепления воли к самозащите» [2, с. 86], поскольку особенность мошенничества состоит в том, что жертва сама является активным участником преступления: общественно опасные последствия не наступят, если она добровольно не переведет деньги, не сообщит код и т. д. В связи со сказанным обратим внимание на личность жертвы кибермошенничества, составим ее портрет и обозначим некоторые направления девиктимизации.

На расширенном заседании коллегии МВД России 5 марта 2025 г. В. В. Путин отметил, что в минувшем году четверть обманутых аферистами

---

[1] См.: Состояние преступности в России за январь — декабрь 2022 г. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Состояние%20преступности%20в%20Росс.pdf (дата обращения: 28.09.2025); Состояние преступности в России за январь — декабрь 2023 г. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Состояние%20преступности%20в%20Росс1.pdf (дата обращения: 28.09.2025); Состояние преступности в России за январь — декабрь 2024 г. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Sbornik_UOS_2024.pdf (дата обращения: 28.09.2025).

[2] См.: МВД раскрыло сумму ущерба от IT-преступлений за три года. URL: https://news.ru/russia/mvd-raskrylo-summu-usherba-ot-it-prestuplenij-za-tri-goda?ysclid=-mhqeeugccz159821250 (дата обращения: 28.09.2025).

[3] См.: Расширенное заседание коллегии МВД России. URL: http://www.kremlin.ru/events/president/news/76408 (дата обращения: 28.09.2025).

[4] Россия открыта к сотрудничеству в борьбе с IT-преступностью, заявил Путин. URL: https://ria.ru/20251025/putin-2050547638.html?ysclid=mhqggk662234211662 (дата обращения: 26.10.2025).

[5] См.: Состояние преступности в России за январь — декабрь 2022 г. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Состояние%20преступности%20в%20Росс.pdf (дата обращения: 28.09.2025); Состояние преступности в России за январь — декабрь 2023 г. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Состояние%20преступности%20в%20Росс1.pdf (дата обращения: 28.09.2025); Состояние преступности в России за январь — декабрь 2024 г. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Sbornik_UOS_2024.pdf (дата обращения: 28.09.2025).

[6] См.: Расширенное заседание коллегии МВД России. URL: http://www.kremlin.ru/events/president/news/76408 (дата обращения: 28.09.2025).

граждан пришлась на пенсионеров[1]. По информации Банка России, наибольший интерес для мошенников представляли экономически активные люди 25—65 лет, часто пользовавшиеся банковскими сервисами. При этом доля женщин, пострадавших от мошенничества в 2024 г., составила 52,6 %, мужчин — 47,4 %. 74,4 % потерпевших — городские жители. Таким образом, портрет жертвы кибераферистов выглядит следующим образом: женщина 25—44 лет со средним уровнем дохода и средним образованием, проживающая в городе и имеющая постоянную занятость[2]. Естественно, от действий телефонных и интернет-злоумышленников не застрахован никто. Мужчины и женщины, дети и взрослые, работающие и нет, с высшим образованием и без такового, информационно грамотные и не очень, жители мегаполисов и небольших населенных пунктов — жертвой может стать любой.

В числе психологических качеств личности, определяющих ее виктимность, чаще всего указываются доверчивость, порядочность, готовность прийти на помощь другим, наивный оптимизм, вера в доброту и справедливость. Мошенники выбирают «тех, кто привык быть вежливым, ответственным, соблюдать правила. Тех, кто скорее поверит в чужую беду, чем усомнится в чьей-то лжи»[3]. При определенных обстоятельствах названные качества превращаются в уязвимости и делают человека беззащитным перед лицом злоумышленников. Кроме того, не стоит забывать, что схемы мошенничества постоянно совершенствуются, манипуляции становятся все изощреннее и жертвы просто не успевают выработать психологический иммунитет к ним.

По мнению А. Н. Хоменко, «доминантой причин виктимизации… является невежество в использовании средств информационно-телекоммуникационных технологий и нерациональная доверительность, основанная на… самоуверенности и самонадеянности» [3, с. 146]. В свою очередь Д. Р. Белодед выделяет следующие особенности жертв кибермошенничества:

— отсутствие осведомленности о различных видах киберугроз и методах мошенничества в онлайн-среде;

— эмоционально уязвимое состояние, такое как стресс, тревога или финансовые трудности;

— доверчивость, временами даже наивность, толкающая людей без должной осторожности верить незнакомцам;

— жажда легкого заработка, выгодных сделок или удовлетворения иных потребностей [4, с. 320].

Приведенный перечень мы дополним еще одним пунктом — склонностью к овершерингу — поведению, при котором человек делится подробностями своей жизни (проблемами со здоровьем, неудачами в отношениях, финансовыми трудностями и т. д.) с окружающими. Сегодня довольно часто такое поведение можно наблюдать в социальных сетях. Особую тревогу вызывает тот факт, что некоторые пользователи указывают в Интернете адрес своего места жительства или выкладывают фотографии с одним и тем же геотегом. Это может поставить под угрозу не только сохранность персональных данных, но и безопасность самого автора публикации и членов его семьи. Заместитель председателя правления «Сбера» С. Кузнецов отмечает: «…мы фиксируем случаи, когда злоумышленники даже не утруждают себя и не формируют легенду, а с самого начала угрожают физической расправой жертве и ее близким, называя персональную информацию, которую можно найти в открытом доступе в Интернете, например, адрес места жительства»[4]. Кроме того, овершеринг выступает своеобразным фундаментом мошенничества с использованием технологии Deepfake: публикуемые в социальных сетях в открытом доступе фото- и видеоматериалы позволяют злоумышленникам создавать реалистичные изображения, которые затем используются в преступных целях.

Практически во всех мошеннических схемах еще до совершения преступления злоумышленники уже владеют некоторыми данными о потенциальной жертве, что позволяет установить с ней контакт и поддержать легенду: если человека называют по имени и отчеству, сообщают адрес его места жительства или паспортные данные,

[1] См.: Расширенное заседание коллегии МВД России. URL: http://www.kremlin.ru/events/president/news/76408 (дата обращения: 28.09.2025).

[2] См.: ЦБ составил портрет жертвы кибермошенников. URL: https://www.rbc.ru/finances/17/02/2025/67b30f299a7947b73cc000f6?ysclid=mhs3s1xj39240445959 (дата обращения: 28.09.2025).

[3] Хабарова Т. Ю. Когда доброта становится уязвимостью или Психологический портрет жертвы мошенничества. URL: https://www.b17.ru/article/671097/?ysclid=mgp5t578ib310569441 (дата обращения: 09.09.2025).

[4] Станислав Кузнецов: мошенники всегда воздействуют на эмоции человека. URL: https://ria.ru/20240904/kuznetsov-1970240962.html?ysclid=mhrqsd8eem855203175 (дата обращения: 29.09.2025).

он, конечно, может поверить в то, что с ним говорит представитель госорганов или финансово-кредитных организаций. В дальнейшем с помощью психологических манипуляций (как правило, чрезмерно высокого темпа речи, чтобы у визави не было времени осознать смысл сказанного; назидательного, не терпящего возражений тона; запугивания и т. д.) аферисты окончательно вводят жертву в заблуждение и заставляют действовать по заранее составленному сценарию. Большинство мошеннических схем основывается на том, что злоумышленники выдают себя за сотрудников полиции, Федеральной службы безопасности Российской Федерации, Следственного комитета Российской Федерации, компаний сотовой связи, портала «Госуслуги» и т. д. и играют на эмоциях собеседника, чаще всего на страхе, который называют «одним из самых мощных инструментов мошенников»[1]. При этом жертва, находясь в стрессе, становится рассеянной и невнимательной и в результате совершает необдуманные поступки. Так, 54-летней жительнице города Чебоксары позвонил мужчина, представившийся сотрудником органов соцзащиты, и предложил обратиться в пенсионный фонд для перерасчета будущей пенсии. Для записи на личный прием он попросил назвать коды, поступившие в сообщениях. Далее потерпевшей позвонила девушка (якобы сотрудник Роскомнадзора) и сообщила, что в личном кабинете на портале «Госуслуги» от имени чебоксарки была оформлена доверенность на гражданина Украины, который собирается взять кредит. Затем женщине позвонил «следователь». Поверив во все услышанное, жертва оформила кредиты в двух банках и перечислила злоумышленникам более 800 тыс. руб. При этом денежные средства были переведены через банкомат, установленный в одном из торговых центров города, рядом с которым находилась ростовая фигура полицейского с памяткой, предупреждающей о том, что сотрудники правоохранительных органов никогда не звонят через мессенджеры, понятия «безопасный счет» не существует и перечислять деньги незнакомцам нельзя[2]. Приведенный пример наглядно демонстрирует, как, поддавшись эмоциям, человек отключил критическое мышление и логику, впал в состояние арефлексивности и в результате стал жертвой преступления.

Однако не только страх заставляет людей поступать нерационально. Мошенники активно эксплуатируют такие личностные качества потенциальных жертв, как жадность, что отчетливо проявляется, например, в схемах, где аферисты обещают легкий заработок, выигрыш в лотерею и т. п.; ответственность, которая «срабатывает» в сценарии Fake Boss, когда работнику звонит якобы работодатель и просит перевести деньги на «безопасный счет» или сообщить конфиденциальные данные; милосердие, на каком играют фейковые благотворители; любопытство, заставляющее пользователей переходить по фишинговым ссылкам на мошеннические сайты; иные.

Личностные и поведенческие качества представляют собой субъективные виктимогенные факторы, на которые необходимо обращать особое внимание при предупреждении киберпреступлений. Работа с ними должна включать в себя не только информационно-разъяснительный аспект — оповещение о способах совершения мошенничества и недопустимости перевода денежных средств неизвестным лицам, но и психологический — формирование психологической устойчивости к манипуляциям (обучение приемам распознавания манипуляций, повышение уровня цифровой грамотности, работа с эмоциональным интеллектом и др.). Каким же образом достичь этих целей? Обратимся к такому инструменту, как социальная (виктимологическая) реклама. Сегодня ее можно увидеть и услышать в местах массового пребывания людей (на вокзалах, в общественном транспорте, торговых центрах и т. д.). Многие отметят, что подобной рекламы хватает, а удельный вес кибермошенничества только увеличивается. Однако проблема состоит в том, что при ее транслировании нередко выбираются не те каналы для общения с целевой аудиторией. Так, в вагоне метро или троллейбусе звучит устное предупреждение о недопустимости перевода денежных средств незнакомым людям, но его никто не воспринимает, поскольку пассажиры заняты просмотром новостей, лент социальных сетей и т. д. или попросту не слышат из-за шума, музыки в наушниках и др. Следовательно, оно не работает. То же можно сказать и о визуальной рекламе (плакатах, листовках). Она должна быть яркой и доступной, содержать четкие инструкции (какие действия предпринять в той или иной ситуации,

[1] Омельчук Э. Мошенники и их тактика воздействия на жертву. URL: https://www.b17.ru/article/662256/?ysclid=mhvu2zzu51638987736 (дата обращения: 29.09.2025).

[2] См.: Жительница Чебоксар перечислила аферистам более 800 тысяч рублей, стоя около фигуры полицейского, предупреждающего о мошенничестве. URL: https://21.мвд.рф/news/item/57454059 (дата обращения: 30.09.2025).

хотя бы в складывающихся наиболее часто) и размещаться там, где ее наверняка увидят. Социальные ролики необходимо регулярно транслировать и по телевидению (по охватным и таргетированным каналам), желательно в прайм-тайм и не в блоке рекламы, а в самой телепередаче (пусть и в виде бегущей строки). Особенно это касается новостных программ, к которым с максимальным доверием относятся люди пенсионного возраста (здесь о мошенниках может предупреждать и ведущий информационного выпуска). Сообщение типа «Осторожно, мошенники!» с кратким пояснением действий аферистов должно появляться в виде всплывающего окна при запуске онлайн-банкинга, чтобы пользователь видел его каждый раз, когда пытается зайти в личный кабинет.

Однако не рекламой единой можно попытаться привить цифровую грамотность и повысить уровень самозащиты личности от киберугроз. Поскольку соответствующие компетенции (а это не только знания, умения и навыки, но и личностные качества) нужно развивать с детства, считаем целесообразным предложение Г. Грефа о повсеместном введении в школьную программу учебной дисциплины «Кибербезопасность». Глава «Сбера» отметил, что традиционная информатика, которую сейчас преподают в общеобразовательных организациях, не имеет ничего общего с цифровыми навыками[1]. С приведенным тезисом трудно не согласиться. Знания об устройстве компьютера и информационных процессах, работа с текстовыми, графическими редакторами, таблицами, базами данных и т. д. не позволяют защититься от кибермошенников и их манипуляций. Несовершеннолетним нужно прививать понимание того, что посещение сомнительных сайтов, переход по непроверенным ссылкам, общение с незнакомцами в Интернете или по телефону и т. п. могут создать угрозу безопасности, а требования о регулярном обновлении паролей, установлении антивирусного программного обеспечения и двухфакторной аутентификации не прихоть, а насущная необходимость.

Не следует забывать и о том, что наряду с приведенными должны реализовываться и иные меры предупреждения киберпреступности: социально-экономические, правовые, идеологические, технические. Безусловно, государство и общество стараются сделать все возможное, чтобы снизить число граждан, пострадавших от телефонных и интернет-мошенников: совершенствуется законодательство, вводятся в эксплуатацию антифрод-системы и сервисы защиты от спам-звонков, в мобильных приложениях появляются «спецкнопки» и т. д. Однако, вероятно, до тех пор, пока в сознании россиян не укоренятся правила «не брать трубку с неизвестных номеров» и «ни при каких обстоятельствах не продолжать разговор с мошенником», пока граждане не перестанут слепо верить всем, кто позвонил и представился сотрудником госорганов, и будут оставаться внушаемыми, конформными, результаты предупредительной деятельности будут не столь высоки, как всем хотелось бы. В связи с этим еще раз подчеркнем, что главным инструментом виктимологического предупреждения киберпреступности в целом и кибермошенничества в частности должна стать работа с субъективными виктимогенными факторами, направленная на развитие эмоционального интеллекта и критического мышления, формирование уверенности в себе умений и навыков распознавания манипуляций и противодействия им.

1. Алексеева А. П. Криминология. Общая часть: учеб. пособие. Волгоград: ВА МВД России, 2020. 80 с.

2. Антонов И. М., Бойко Н. В. К вопросу о виктимологическом аспекте предупреждения преступности // Вестник Хабаровского государственного университета экономики и права. 2017. № 6 (92). С. 84—89.

[1] См.: Греф предложил новый обязательный предмет в школах. URL: https://www.rbc.ru/society/30/06/2025/68624b739a794771b69622be?ysclid=mhx8tmml2540236107 (дата обращения: 30.09.2025).

1. Alekseyeva A. P. Criminology. General part. Textbook. Volgograd: Volgograd Academy of the Ministry of the Interior of Russia; 2020: 80. (In Russ.).

2. Antonov I. M., Boiko N. V. On victimologic aspect of crime prevention. Journal of the Khabarovsk State University of Economics and Law, 84—89, 2017. (In Russ.).

3. Хоменко А. Н. К вопросу о виктимизации жертв киберпреступлений // Виктимология. 2021. Т. 8, № 2. С. 143—148.

4. Белодед Д. Р. Некоторые психологические особенности жертв преступлений, совершаемых с использованием цифровых технологий // Виктимология. 2023. Т. 10, № 3. С. 320—334.

3. Khomenko A. N. On victimization of cybercrime victims. Victimology, 143—148, 2021. (In Russ.).

4. Beloded D. R. Some psychological characteristics of victims of crimes committed by applying digital technologies. Victimology, 320—334, 2023. (In Russ.).

Голятина Светлана Михайловна,
доцент кафедры криминалистики
учебно-научного комплекса
по предварительному следствию
в органах внутренних дел
Волгоградской академии МВД России,
кандидат юридических наук;
sgoliatina@mvd.ru

Golyatina Svetlana Mikhailovna,
associate professor
at the department of forensic science
of the educational and scientific complex
for preliminary investigation
in the internal affairs bodies
of the Volgograd Academy
of the Ministry of the Interior of Russia,
candidate of juridical sciences;
sgoliatina@mvd.ru

Статья поступила в редакцию 02.10.2025; одобрена после рецензирования 11.10.2025; принята к публикации 17.11.2025.

The article was submitted 02.10.2025; approved after reviewing 11.10.2025; accepted for publication 17.11.2025.

* * *