Дата поступления рукописи в редакцию: 28.01.2026 г.
Дата принятия рукописи в печать: 25.02.2026 г.
DOI: 10.24412/2224-9133-2026-1-563-566

ПИВНЕВА Людмила Валерьевна,
аспирант кафедры уголовного права ФГБОУ ВО «Юго-Западный государственный университет», майор полиции, преподаватель кафедры оперативно-разыскной деятельности Белгородского юридического института МВД России имени И. Д. Путилина,
e-mail: iPVmila@yandex.ru.

ВИРТУАЛЬНАЯ ВИКТИМНОСТЬ: МЕТОДИКИ ПОВЫШЕНИЯ ЦИФРОВОЙ ГРАМОТНОСТИ НАСЕЛЕНИЯ КАК ИНСТРУМЕНТ ПРЕДУПРЕЖДЕНИЯ ХИЩЕНИЙ

Аннотация. *В статье рассматриваются актуальные проблемы виртуальной виктимности в контексте развития цифровых технологий и киберпреступности. Анализируются методики повышения цифровой грамотности населения как эффективного инструмента предупреждения дистанционных хищений. На основе анализа статистических данных и научных исследований доказывается, что целенаправленная работа по повышению осведомленности граждан о рисках цифровой среды способна значительно снизить уровень виктимизации. Рассматриваются направления виктимологической профилактики и предупреждения, а также выявляются основные причины повышенной уязвимости отдельных групп населения перед киберугрозами.*

Ключевые слова: *виктимность, киберпреступность, цифровая грамотность, дистанционные хищения, мошенничество, профилактика, криминология, виктимология.*

PIVNEVA Lyudmila Valerievna,
postgraduate student in the Department of Criminal Law at the Southwestern State University, police major, lecturer in the Department of Operational Investigative Activities at the Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin

VIRTUAL VICTIMITY: METHODS FOR INCREASING DIGITAL LITERACY OF THE POPULATION AS A TOOL FOR PREVENTING THEFT

Annotation. *This article examines current issues of virtual victimization in the context of digital technology and cybercrime development. It analyzes methods for improving digital literacy among the population as an effective tool for preventing remote theft. Based on an analysis of statistical data and scientific research, it is demonstrated that targeted efforts to raise public awareness of the risks of the digital environment can significantly reduce victimization rates. It examines areas of victimization prevention and warning, and identifies the main reasons for the increased vulnerability of certain population groups to cyberthreats*.

Key words: *victimization, cybercrime, digital literacy, remote theft, fraud, prevention, criminology, victimology.*

Развитие информационно-коммуникационных технологий привело к трансформации криминальной активности и появлению новых форм преступлений, совершаемых с использованием интернета и других цифровых средств, поскольку в современном постмодернистском информационном обществе, исходя из его ключевых сущностных характеристик, главным товаром выступает информация, получение и распространение которой одновременно является и основной угрозой безопасности данного общества.

Поэтому неудивительно, что в структуре современной преступности мы видим устойчивую

тенденцию к снижению так называемых контактных форм и способов совершения преступлений (убийств, разбоев, краж из жилых помещений и др.), с одновременным увеличением доли преступлений, совершаемых в информационном пространстве или с использованием методов удаленного воздействия на жертву. Такое структурное изменение преступности побудило криминологов обратить пристальное внимание на новый вид преступности — киберпреступность. При этом активно продвигаются идеи о необходимости выделения соответствующей ей отдельной частной теории криминологии, и как следствие — отдельной теории виктимологии — «кибервиктимологии» [1].

Как мы уже отметили выше, в последние годы отмечается значительный рост числа дистанционных хищений и мошеннических операций в финансовой сфере, что становится серьезной проблемой не только для Российской Федерации, но и для мирового сообщества в целом [1]. Параллельно с этим развивается и концепция виртуальной виктимности, как научного направления, изучающего закономерности становления и развития жертв в условиях цифровой среды. Основной причиной растущего уровня киберпреступлений является недостаточная цифровая грамотность значительной части населения, что делает потенциальных жертв уязвимыми перед различными видами киберугроз, поскольку низкий уровень осведомленности о методах мошенничества и способах защиты личной информации создает благоприятные условия для совершения преступлений в сфере дистанционных финансовых операций.

Ряд зарубежных исследователей так же обращают внимание на тот факт, что значительная часть угроз кибербезопасности пользователей исходит от самих пользователей. Они обращают внимание на ненадлежащее поведение в области кибербезопасности, отмечая, что гражданам не хватает знаний в области кибербезопасности при использовании интернета и цифровых устройств, и в целом существует несоответствие между возможностями интернета и поведением людей. Предлагается использовать теорию мотивации защиты (PMT) для поощрения надлежащего поведения в области кибербезопасност. Она предполагает, что оценка угрозы и оценка преодоления — это два основополагающих механизма, лежащих в основе поведенческих действий, когда люди сталкиваются с угрожающими событиями. Таким образом, они предлагают практику модели кибербезопасности, ориентированной на граждан [8] .

То есть пользователи постоянно становятся мишенями злоумышленников, и им требуется обладать достаточными знаниями, чтобы выявлять такие атаки и избегать их. В связи с этим, как мы видим, часть зарубежных криминологических исследований посвящена снижению виктимности у населения путем их обучения, повышения осведомленности в области кибербезопасности [8].

В связи с чем, данная проблема требует комплексного подхода к разработке и внедрению методик по повышению цифровой грамотности граждан, которые могли бы служить эффективным инструментом предупреждения криминальной виктимизации, поэтому актуальность исследования в данной сфере определяется необходимостью выработки эффективных стратегий предупреждения виктимизации населения в цифровой среде и развития научно обоснованных методов повышения цифровой грамотности граждан.

Виктимология цифровой преступности представляет собой относительно новое направление в системе криминологических наук, ориентированное на изучение характеристик, поведения и условий жизнедеятельности жертв киберпреступлений [6]. Вот почему в контексте развития информационного общества виктимология приобретает все большую значимость и позволяет выявить закономерности и факторы, способствующие виктимизации отдельных лиц и социальных групп. Необходимо отметить, что жертвы киберкраж и дистанционных хищений занимают особое место в системе объектов криминологического анализа и требуют специального внимания и комплексной защиты [4].

Анализ статистических показателей криминальной виктимности за 2021–2022 годы и данных последних лет свидетельствует о неуклонном росте числа лиц, ставших жертвами киберпреступлений [4]. Из него становится очевидным, что особенно уязвимыми перед киберугрозами оказываются граждане пожилого возраста, люди с низким уровнем технологической подготовки, а также лица, не обладающие достаточными знаниями о методах мошенничества и способах защиты в цифровой среде, что в условиях расширения спектра предоставляемых электронных услуг и роста объемов онлайн-транзакций, является потенциальной угрозой и как следствие виктимизация касается все более широких слоев населения.

Дистанционные хищения включают в себя различные формы неправомерного завладения чужим имуществом с использованием информационно-коммуникационных технологий [1]. К наиболее распространенным видам относятся фишинг, социальная инженерия, использование вредоносного программного обеспечения, кража учетных данных и несанкционированный доступ к банковским счетам. При этом, мошенничества в банковской сфере занимают отдельное место в системе дистанционных хищений и характеризуются специфическими чертами, связанными с особенностями функционирования финансовых учреждений [5]. Виктимологический анализ таких

преступлений показывает, что в значительном большинстве случаев именно поведение потенциальной жертвы, обусловленное недостатком знаний и навыков безопасной работы с цифровыми инструментами, становится основным фактором, позволяющим преступнику реализовать свой преступный замысел.

Повышение криминальной виктимности юридических лиц в Российской Федерации представляет собой отдельную проблему, требующую специального внимания [7]. Организации, в том числе банки, страховые компании и торговые сети, все чаще становятся жертвами киберпреступлений, что приводит к значительным финансовым потерям и репутационному ущербу, что свидетельствует о том, что недостаточная цифровая грамотность как отдельных граждан, так и сотрудников организаций является серьезным фактором риска в условиях современной цифровой экономики. В связи с чем, направления виктимологической профилактики и предупреждения дистанционных хищений должны быть основаны на комплексном подходе, включающем информационно-просветительскую работу, развитие навыков критического мышления в цифровой среде, повышение уровня технического образования граждан [3]. Актуальные направления виктимологической профилактики включают в себя разработку специализированных образовательных программ, проведение общественных кампаний по информированию о киберугрозах, совершенствование системы консультирования жертв киберпреступлений, а также установление партнерских связей между правоохранительными органами, учреждениями образования и коммерческими организациями, деятельность которых связана с защитой персональных данных граждан.

Методики повышения цифровой грамотности должны быть адаптированы к различным возрастным группам и уровням начальной подготовки граждан [2]. Для пожилых людей было бы целесообразно разработать специальные программы, ориентированные на формирование базовых навыков безопасного использования интернета и мобильных приложений для финансовых операций. Напротив молодежь и люди среднего возраста нуждаются в информации о более сложных формах кибератак и способах защиты от них, поэтому система образования должна включить в школьные и университетские программы обязательные курсы по цифровой безопасности и критическому анализу информации в интернете.

То есть, становится очевидным, что виктимологическая защита жертв дистанционных хищений требует создания многоуровневой системы, включающей оказание психологической помощи, правовое консультирование, содействие в восстановлении справедливости и защиту от повторной виктимизации [2]. Важным элементом такой защиты является информирование граждан об их правах и возможностях обращения в правоохранительные органы и другие компетентные учреждения при совершении против них преступлений в цифровой среде. Кроме того, необходимо развивать сферы воздействия виктимологической профилактики, расширяя количество субъектов, участвующих в предупреждении виктимизации [1].

Предупреждение виктимизации дистанционных хищений должно охватывать не только индивидуальный уровень (работа с конкретными гражданами), но и групповой и общественный уровни. Если на групповом уровне целесообразно разработать специализированные программы для отдельных социальных групп, находящихся в зоне повышенного риска, то на общественном уровне необходимо развивать культуру безопасности в цифровой среде через средства массовой информации, социальные сети и другие каналы коммуникации. При этом государственные органы должны активно участвовать в этом процессе, разрабатывая и внедряя нормативно-правовые акты, которые способствовали бы совершенствованию системы защиты граждан в цифровой среде и повышению уровня их цифровой грамотности.

Таким образом, проведенный анализ позволяет заключить, что виртуальная виктимность является объективной реальностью современного общества, требующей серьезного научного и практического внимания, поскольку рост числа жертв киберпреступлений, в особенности дистанционных хищений, непосредственно связан с недостаточным уровнем цифровой грамотности и осведомленности граждан о киберугрозах. В тоже время методики повышения цифровой грамотности населения показали свою эффективность как инструмент предупреждения криминальной виктимизации и должны развиваться и совершенствоваться на всех уровнях общественной системы. Необходимо разработать комплексную стратегию повышения цифровой грамотности, которая включала бы образовательные программы для различных возрастных групп, информационно-просветительскую деятельность, развитие навыков критического мышления в цифровой среде и систему поддержки жертв киберпреступлений. Ключевую роль в реализации этой стратегии должны играть государственные органы, учреждения образования, правоохранительные органы и коммерческие организации, деятельность которых связана с обеспечением информационной безопасности.

Дальнейшее развитие виктимологии цифровой преступности требует проведения дополнительных научных исследований, направленных на выявление новых форм киберпреступлений и

закономерностей виктимизации населения в условиях постоянно изменяющейся цифровой среды, поскольку совершенствование системы профилактики и предупреждения дистанционных хищений через повышение уровня цифровой грамотности граждан остается одной из наиболее перспективных и актуальных задач криминологии и виктимологии на современном этапе.

Список литературы:

[1] Евтушенко И. И. Предупреждение виктимизации дистанционных хищений и сферы его воздействия // Виктимология. 2024. №1. URL: https://cyberleninka.ru/article/n/preduprezhdenie-viktimizatsii-distantsionnyh-hischeniy-i-sfery-ego-vozdeystviya (дата обращения: 27.01.2026).

[2] Евтушенко И. И. Виктимологическая защита жертв дистанционных хищений // Виктимология. 2023. №1. URL: https://cyberleninka.ru/article/n/viktimologicheskaya-zaschita-zhertv-distantsionnyh-hischeniy (дата обращения: 27.01.2026).

[3] Евтушенко И. И. Актуальные направления виктимологической профилактики дистанционных хищений // Виктимология. 2022. №1. URL: https://cyberleninka.ru/article/n/aktualnye-napravleniya-viktimologicheskoy-profilaktiki-distantsionnyh-hischeniy (дата обращения: 27.01.2026).

[4] Кабанов П. А. Жертвы киберкраж как объект современной российской кибервиктимологии: криминологический анализ статистических показателей криминальной виктимности 2021–2022 гг. // Виктимология. 2024. №1. URL: https://cyberleninka.ru/article/n/zhertvy-kiberkrazh-kak-obekt-sovremennoy-rossiyskoy-kiberviktimologii-kriminologicheskiy-analiz-statistich-eskih-pokazateley (дата обращения: 27.01.2026).

[5] Репецкая Анна Леонидовна, Петрякова Людмила Александровна. Виктимологическая характеристика мошенничеств в банковской сфере (по материалам Сибирского федерального округа) // Всероссийский криминологический журнал. 2022. №4. URL: https://cyberleninka.ru/article/n/viktimologicheskaya-harakteristika-moshennichestv-v-bankovskoy-sfere-po-materialam-sibirskogo-federalnogo-okruga (дата обращения: 27.01.2026).

[6] Майоров А. В. Виктимология цифровой преступности: концепция научного направления // Виктимология. 2024. №1. URL: https://cyberleninka.ru/article/n/viktimologiya-tsifrovoy-prestupnosti-kontseptsiya-nauchnogo-napravleniya (дата обращения: 27.01.2026).

[7] Александрина Н. М. Уровень криминальной виктимизации юридических лиц в Российской Федерации // Виктимология. 2023. №4. URL: https://cyberleninka.ru/article/n/uroven-kriminalnoy-viktimizatsii-yuridicheskih-lits-v-rossiyskoy-federatsii (дата обращения: 27.01.2026).

[8] Mahlangu G ., Chipfumbu Kangara C ., Masunda F . (2023) . Citizen-centric cybersecurity model for promoting good cybersecurity behavior // Journal of Cyber Security Technology . 2023 . Vol . 7, no . 3 . P . 154–180 . DOI: https://doi .org/10 .1080/23742917 .2023 .2217535.

References:

[1] Evtushenko I. I. Prevention of victimization of distance theft and the scope of its impact//Victimology. 2024. №1. URL: https://cyberleninka.ru/article/n/preduprezhdenie-viktimizatsii-distantsionnyh-hischeniy-i-sfery-ego-vozdeystviya (дата обращения: 27.01.2026).

[2] Evtushenko I. I. Victimological protection of victims of remote theft//Victimology. 2023. №1. URL: https://cyberleninka.ru/article/n/viktimologicheskaya-zaschita-zhertv-distantsionnyh-hischeniy (дата обращения: 27.01.2026).

[3] Evtushenko I. I. Current directions of victimological prevention of distance theft//Victimology. 2022. №1. URL: https://cyberleninka.ru/article/n/aktualnye-napravleniya-viktimologicheskoy-profilaktiki-distantsionnyh-hischeniy (дата обращения: 27.01.2026).

[4] Kabanov P. A. Victims of cybercrazh as an object of modern Russian cybervictimology: criminological analysis of statistical indicators of criminal victimization 2021-2022//Victimology. 2024. №1. URL: https://cyberleninka.ru/article/n/zhertvy-kiberkrazh-kak-obekt-sovremennoy-rossiyskoy-kibervik-timologii-kriminologicheskiy-analiz-statistich-eskih-pokazateley (дата обращения: 27.01.2026).

[5] Repetskaya Anna Leonidovna, Petryakova Lyudmila Alexandrovna. Victimological characteristics of fraud in the banking sector (based on materials from the Siberian Federal District)//All-Russian Criminological Journal. 2022. №4. URL: https://cyberleninka.ru/article/n/viktimologicheskaya-harakteristika-moshennichestv-v-bank-ovskoy-sfere-po-materialam-sibirskogo-federalno-go-okruga (дата обращения: 27.01.2026).

[6] Mayorov A.V. The victimology of digital crime: the concept of a scientific direction//Victimology. 2024. №1. URL: https://cyberleninka.ru/article/n/viktimologiya-tsifrovoy-prestupnosti-kontsept-siya-nauchnogo-napravleniya (дата обращения: 27.01.2026).

[7] Alexandrina N. M. Level of criminal victimization of legal entities in the Russian Federation//Victimology. 2023. №4. URL: https://cyberleninka.ru/article/n/uroven-kriminalnoy-viktimizatsii-yuridiches-kih-lits-v-rossiyskoy-federatsii (дата обращения: 27.01.2026).

[8] Mahlangu G ., Chipfumbu Kangara C ., Masunda F . (2023) . Citizen-centric cybersecurity model for promoting good cybersecurity behavior // Journal of Cyber Security Technology . 2023 . Vol . 7, no . 3 . P . 154–180 . DOI: https://doi .org/10 .1080/23742917 .2023 .2217535.