Ибатуллина Диана Марсовна
адъюнкт
ФГКОУ ВО «Казанский юридический
институт МВД РФ»
г. Казань, Республика Татарстан

DOI 10.31483/r-150458

ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА КОРЫСТНЫХ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация*: в статье рассматриваются две основные проблемы, получившие распространение, в связи с цифровизацией общества: отсутствие цифровой гигиены и идеализация виртуального пространства, которые ведут к серьезным угрозам, в том числе и к угрозам материального (имущественного) ущерба. Автор статьи отмечает, что самозащита – базовый инструмент, предоставленный каждому человеку, который позволяет обеспечивать безопасность в виртуальном пространстве.*

Ключевые слова*: виктимология, цифровизация, корыстные преступления, собственность, самозащиты, цифровая гигиена.*

В 2024 году на форуме «Кибербезопасность в финансах» представители МВД России сообщили, что ущерб от киберпреступлений в России в 2024 году составил 200 миллиардов рублей, это на 36% больше, чем годом ранее.

Данные ГИАЦ МВД России за аналогичный период свидетельствуют о крайне высоком уровне корыстных преступлений против собственности, совершенных с использованием информационных технологий. Всего зарегистрировано 486281 корыстных преступлений против собственности, совершенных с использованием информационных технологий, в их числе: кражи – 105937 фактов; мошенничество (ст. ст. 159, 159.3, 159.6 УК РФ) – 380344 фактов [1].

По данным Банка России в 2024 году каждый 3-й из 10 респондентов сталкивался с разными видами финансового кибермошенничества, при этом 9% пострадавших лишились денег [2].

При этом, шесть регионов Российской Федерации (Республика Марий Эл (977,53), Республика Карелия (952,17), Томская область (923,53), Новгородская область (907,69), Республика Удмуртия (888,43) и Кировская область (870,4)) образуют группу с наиболее высоким уровнем киберпреступности [4].

В условиях массовой цифровизации общества значительное количество государственных ресурсов направлено именно на борьбу с преступностью и укрепление информационной сферы. Виктимологическая профилактика, заключающаяся в работе с потенциальными и реальными жертвами корыстных преступлений против собственности, совершенных с использованием информационных технологий, не является ключевой задачей. Однако данное направление профилактики преступности требует особого внимания и разработки более эффективных механизмов по защите населения от корыстных посягательств на собственность. Д.М. Жмуров отмечает, что «в последние годы государство предприняло немалое число инициатив, направленных на профилактику преступности, при этом не всегда учитывая виктимологический аспект проблемы» [7, с. 136].

В рамках анализа преступлений, совершаемых с использованием информационных технологий, виктимологическая профилактика рассматривается как имманентный элемент противодействия преступности. Роль виктимологической профилактики заключается в снижении риска стать жертвой корыстного преступления против собственности, активизировать и совершенствовать алгоритмы по самозащите от последующих преступных посягательств, совершаемых с использованием информационных технологий.

В данном исследовании мы хотим обратить внимание на алгоритмы, позволяющие самостоятельно реализовывать комплекс мер, входящих в виктимологичекую профилактику корыстных преступлений против собственности, совершаемых с использованием информационных технологий, поскольку каждый человек является потенциальной жертвой преступления.

На наш взгляд, в эффективной практической реализации виктимологической профилактики обнаруживается две серьезные проблемы.

1. Отсутствие цифровой гигиены у пользователей.

Распространение информационных технологий безусловно способствует подверженности дополнительным угрозам населения, в связи с чем обнаруживается необходимость соблюдать правила цифровой гигиены.

Под цифровой гигиеной следует понимать комплекс мер, направленных на снижение рисков пользователей цифровым пространством и повышения уровня безопасности.

Пользователи, не применяющие базовые правила по обеспечению своей безопасности в цифровом пространстве, значительнее подвержены угрозе причинения материального ущерба.

2. Идиализация виртуального пространства.

Е.А. Колесников указывает, что 62,1% всех пользователей социальных сетей – лица, не достигшие 24 лет [8, с. 151]. Именно подростки и обладают совокупностью признаков «цифровой жертвы». Во-первых, одной из потребностей поколения является ежедневное использование цифровых платформ, необходимость длительного времяпрепровождения в социальных сетях. Во-вторых, несформированность психики предполагает повышенный уровень доверия, предрасположенность к освоению нового, в том числе и новым знакомствам, отсутствие критического анализа, склонность к риску, необходимость подтверждения собственной значимости и т. д.

Очевидно, что замена окружающей среды цифровым пространством ведет к чрезмерному уровню доверия к виртуальным площадкам, что влечет за собой бесконтрольное оставление цифрового следа в сети, распространения личной информации, которую затем используют преступники в корыстных целях.

Рассмотрим практический пример. В период времени с 02.05.2019 г. по 06.05.2019 г. неустановленное в ходе предварительного следствия лицо, используя информационно-телекоммуникационные сети посредством сообщений в мессенджерах «WhatsApp», «Telegram» передало гражданину С. и гражданину К.

для использования полученные им пары «логин-пароль» клиентов ООО «Х». Гражданин С. и гражданин К., согласно отведенным им ролям, посредством сети «Интернет» с целью хищения электронных денежных средств, продолжая свой преступный корыстный умысел, осуществили ввод компьютерной информации в виде логинов и паролей, вошли в личные кабинеты клиентов мультифункциональной бонусной платёжной карты системы дистанционного обслуживания ООО «Х» и, совершили ряд операции по хищению электронных денежных средств с банковских карт ООО «Х», путем умолчания уполномоченному работнику торговой организации о незаконном владении ими платежной картой. Гражданином С. и гражданином К. были похищены денежные средства на общую сумму 2 889 980 рублей, что является особо крупным размером.

Гражданине С. и К. были признаны виновными в совершении преступления, предусмотренного ч. 4 ст. 159.3 УК РФ с назначением наказания в виде 3 лет лишения свободы [3].

Множество исследователей, среди которых В.А. Гусев [6, с. 105], И.В. Батурина, Т.Ю. Горшкова [5, с. 338], З.З. Шадманов [9, с. 192] занимающихся анализом и популяризацией цифровой гигиены сходятся во мнении в отношении методики, которая позволит обеспечить цифровую самозащиту: создание сложных паролей, ограничение контента для детей, многоступенчатая аутентификация и иное.

Предложенный нами алгоритм, дополняющий методики вышеуказанных авторов, позволит в современных условиях безопасно пользоваться цифровым пространством и значительно снизить количество корыстных преступлений против собственности, совершаемых с использованием информационных технологий, соблюдая следующие правила.

1. Создавать сложные неповторяющиеся пароли.

Пароли должны состоять из различных символов, букв, цифр, не являющихся персональными данными или данными близких.

2. Применять двухфазную систему аутентификации.

На наш взгляд, использованию любого государственного сервиса, онлайн-банка, должна предшествовать именно двухступенчатая аутентификация (одной из ступней в обязательной порядка должен выступать анализ биометрии пользователя).

3. Ограничивать публикацию и передачу персональных данных и иной личной информации через цифровое пространство.

Зачастую знакомые или близкие просят перевести денежные средства или сообщить какую-либо информацию в социальных сетях и мессенджерах, в таком случае лучше убедиться в достоверности просьбы при личной встрече или по телефонному звонку.

В случае, если незнакомые лица запрашивают какую-либо информацию (пароли, коды, персональные данные), просят перейти по ссылкам, отправить денежные средства, то необходимо немедленно прервать общение и не совершать требуемых действий.

4. Установить самозапрет на кредиты.

Сегодня портал «Госуслуги» позволяет самостоятельно установить самозапрет на получение кредита. Информация о самозапрете вносится в кредитную историю, на следующий день после внесения записи банк или микрофинансовая организация при попытке оформления кредита получит отказ.

5. При причинении материального ущерба, в результате совершения корыстного преступления против собственности, совершенного с использованием информационных технологий, незамедлительно необходимо обратиться в правоохранительные органы.

Таким образом, в условиях феноменального распространения корыстных преступления против собственности, совершаемых с использованием информационных технологий, особая роль должна быть отведена виктимологической профилактике. Особенности повышения ее эффективности заключаются в ее популяризации среди населения. Предложенный алгоритм, состоящий из пяти простых пунктов, позволит значительно повысить уровень цифровой безопасности населения, снизить число корыстных преступлений против собственности, совершаемых с использованием информационных технологий.

Список литературы

1. Главный информационно-аналитический центр МВД России (архивные данные за 2024 год) [Электронный ресурс]. – Режим доступа: https://мвд.рф/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen?ysclid=mfwrlavjjw408594289 (дата обращения: 15.09.2025).

2. Банк России. Официальный сайт [Электронный ресурс]. – Режим доступа: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 15.09.2025).

3. Приговор Куйбышевского районного суда г. Омска №1–48/2020 от 27.12.2019 г. [Электронный ресурс]. – Режим доступа: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/software/Дело%201–482020%20(Статья%20159.6%20УК%20РФ)%20(Бон.pdf (дата обращения: 16.09.2025).

4. Афанасьева О.Р. Киберпреступность в регионах России: современное тенденции и меры предупреждения / О.Р. Афанасьева, В.И. Шиян // Вестник Университета имени О.Е. Кутафина. – 2025. – №5(129). – С. 42.

5. Батурина И.В. Проблемы цифровой гигиены детей и подростков / И.В. Батурина, Т.Ю. Грошкова // Царскосельские чтения. – 2024. – №1. – С. 338. EDN FFDNDH

6. Гусев В.А. Цифровая гигиена vs. киберпреступность / В.А. Гусев // Психопедагогика в правоохранительных органах. – 2022. – №1(88). – С.105.

7. Жмуров Д.В. Общая виктимологическая профилактика киберпреступности / Д.В. Жмуров // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2022. – №4(60). – С.136.

8. Колесников Е.А. Исследование психологических характеристик подростков, склонных к виктимному поведению в виртуальном пространстве / Е.А. Колесников // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». – 2019. – №2. – С. 151. DOI 10.35634/2412-9550-2019-29-2-148-159. EDN RMMYZH

9. Шадманов З.З. Цифровая гигиена: важность и лучшие практики / З.З. Шадманов // Raqamli iqtisodiyot (Цифровая экономика). – 2025. – №10. – С. 192.