ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СРЕДЕ

Муллахметова Н.Е.,
доцент кафедры организации судебной и прокурорской деятельности ФГБОУ ВО «Смоленский государственный университет», кандидат юридических наук, доцент

Компьютеризация и цифровизация всех сфер жизни современного общества несет не только несомненные преимущества в плане упрощения рутинных процессов, удобства передачи, хранения и обработки больших массивов данных, но и угрозы имущественной, информационной безопасности граждан и организаций, что требует консолидированных усилий правоохранительных органов и государства в целом. С каждым годом становится все больше новых способов совершения киберпреступлений, атак на информационные ресурсы, преступность перемещается в виртуальную среду. Вред, причиняемый такими посягательствами, огромен, он исчисляется миллиардами рублей. Так, по данным МВД РФ в 2025 году зарегистрировано более 675 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, хотя это на 11,8% меньше, чем в 2024 году. Более половины таких преступлений относятся к категории тяжких и особо тяжких, почти две трети (63,5%) совершены путем кражи или мошенничества, а почти каждое шестое – с целью незаконного производства, сбыта или пересылки наркотических средств [1].

Большую тревогу вызывает также проблема защиты персональных данных граждан, которые очень востребованы в криминальном мире, поскольку они облегчают совершение преступлений, прежде всего, кибермошенничества.

При совершении таких преступных посягательств широко используются методы социальной инженерии, т.е. преступникам уже не надо выходить на улицы, подкарауливать своих жертв в темном переулке, а нужно просто подобрать «ключик» к психике конкретного человека, убедив его выполнить определенную последовательность действий, приводящих к получению доступа злоумышленников к персональным данным для дальнейшего списания денежных средств. Преступники выигрывают на человеческих слабостях, воздействуют на эмоциональную сферу людей, создают ощущение срочности выполнения их указаний, убеждая жертв, что промедление может привести к потере денежных средств или к тяжким последствиям для их близких. Информация, которая интересует таких «социальных инженеров», – это личные идентификационные данные (номер паспорта, СНИЛС), пароли для входа на портал Госуслуг и все, что позволит в дальнейшем получить доступ к финансовым ресурсам. К числу факторов, влияющих на значительный рост числа

киберпреступлений, можно отнести также цифровое неравенство – ситуацию, при которой часть населения владеет современными технологиями в цифровой сфере на высоком уровне, а у других отсутствует даже элементарная компьютерная грамотность [2, с. 542]. К группе риска при совершении преступлений в цифровой среде относятся несовершеннолетние, пожилые граждане, а также те, кто не имеет даже элементарных навыков использования современных компьютерных технологий и легко поддаются влиянию злоумышленников. Большую опасность сегодня представляют дипфейки – использование образа человека, его голоса для введения в заблуждение собеседника и получения доступа к персональным данным.

Противодействие киберпреступности не будет эффективным без реализации комплекса мер виктимологической профилактики, под которой понимается «включенная в систему предупреждения преступлений подсистема общесоциальных и специально-криминологических мер, направленных на снижение индивидуальной и массовой виктимности посредством устранения негативных предрасположений, активизации возможностей потенциальных жертв преступлений и обеспечения их безопасности» [3, с. 241]. Преступления в сфере информационно-телекоммуникационных технологий легче предотвратить, чем раскрыть и довести до суда с достаточной доказательственной базой. Виктимологическая профилактика входит в общую систему профилактики преступлений, воздействуя преимущественно на потенциальную жертву, снижая уровень ее уязвимости, способствуя повышению предусмотрительности, критичности. Сегодня на страницах юридических изданий появляются публикации, в которых говорится о возникновении нового направления в рамках отечественной виктимологии – кибервиктимологии, которая изучает социально-демографические характеристики жертв преступлений в информационно-телекоммуникационной сфере, разрабатывает в отношении них меры превентивного характера [4, с. 27].

Жмуров Д.В. рассматривает уровни общей виктимологической профиактики, которые относит также к преступлениям в информационно-телекоммуникационной сфере: 1) легальный (разработка виктимологического законодательства); 2) академический (проведение виктимологических исследований); 3) институциональный (государственное управление в сфере виктимологической профилактики, проведение обучающих тренингов, виктимологический мониторинг); 4) технический (создание и внедрение перспективных разработок по защите персональных данных, блокированию нежелательных звонков); 5) идеологический (повышение уровня правовой культуры потенциальных жертв, реализация мер, направленных на осознание важности роли жертвы в контроле над преступностью) [5, с. 136–140].

Проведение широкомасштабной информационной работы с населением, включающей правовую пропаганду, разъяснение правил безопасности при атаках телефонных мошенников, относится к мерам девиктимизации, но эти меры, к сожалению, не устраняют криминальные угрозы полностью, поскольку злоумышленники постоянно совершенствуют способы обмана.

Поэтому наиболее эффективным средством противодействия киберпреступлениям является разработка правовых механизмов, направленных на блокирование поступающих от мошенников звонков, а также затрудняющих их быстрый доступ к финансовым средствам в случае получения персональных данных человека, на применение дополнительных мер безопасности со стороны банковских организаций при выдаче кредитов, переводе больших сумм со счетов клиентов. Это требует создания соответствующей нормативной базы.

Так, действенной мерой предупреждения кибермошенничества можно считать принятие Федерального закона от 26.02.2024 № 31-ФЗ «О внесении изменений в Федеральный закон «О кредитных историях» и Федеральный закон «О потребительском кредите (займе)», в соответствии с которым гражданин вправе бесплатно любое количество раз подать заявления во все квалифицированные бюро кредитных историй через МФЦ или с использованием Единого портала Госуслуг о внесении в свою кредитную историю сведений о запрете (либо снятии запрета) на заключение с ним договоров потребительского займа (кредита) (за исключением отдельных видов кредитов). Миллионы россиян уже воспользовались этим механизмом.

Еще одним значимым шагом в совершенствовании мер предупреждения мошенничества стало принятие Федерального закона от 13 февраля 2025 г. № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», в соответствии с которым предусмотрено введение так называемого «периода охлаждения», т.е. ограничения по времени выдачи кредитов на сумму более 50 тысяч рублей (за некоторыми исключениями). Это позволит предотвратить необдуманные и поспешные решения и действия потенциальных жертв мошенников. Кроме того, повышается и ответственность банков: в случае нарушения ими норм, направленных на недопущение мошеннических операций, кредиторы не смогут требовать исполнения заемщиком обязательств или уступать право требования долга.

Кроме того, в прошлом году был принят Федеральный закон от 1 апреля 2025 года № 41 «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» [6], который предусматривает следующие меры:

1) возможность онлайн-обмена информацией между государственными органами, цифровыми платформами и банковскими организациями, что позволит оперативно выявлять подозрительную активность, блокировать потенциально опасные действия и уведомлять правоохранительные органы о возможных посягательствах;

2) введение обязательной проверки идентификационных данных пользователей услугами связи, а также маркировки звонков;

3) запрет на передачу SIM-карт третьим лицам;

4) установление запрета для государственных служащих, сотрудников государственных органов, банковских работников, операторов

связи и некоторых иных категорий лиц использовать мессенджеры для общения с гражданами;

5) процедуры выявления случаев и попыток выдачи наличных денежных средств из банкоматов без добровольного согласия клиента и др.

На борьбу с мошенничеством в информационно-телекоммуникационной среде направлено также принятие Федерального закона от 24 июня 2025 года № 176 о внесении изменений в ст. 187 УК РФ об ответственности за действия лиц, которые под влиянием злоумышленников или за денежное вознаграждение оформляют или передают свои банковские карты, электронные кошельки мошенникам для использования их в преступных схемах.

В условиях нехватки сотрудников в органах внутренних дел своевременно раскрывать и расследовать огромное количество преступлений, совершаемых в виртуальном пространстве, просто невозможно. Поэтому меры виктимологической профилактики, включающие постоянную информационно-просветительскую деятельность правоохранительных органов, разъяснение населению новых криминальных схем в интернет-пространстве, разработка правовых механизмов, направленных на предотвращение контактов преступников и потенциальных жертв, в том числе блокировка звонков с номеров из «черного списка», введение самозапрета на оформление кредитов без непосредственного участия клиента, а также повышение цифровой грамотности населения должны помочь в борьбе с посягательствами. Но такие меры могут быть эффективными только при добросовестности кредитных организаций и соблюдении ими всех мер по недопущению мошеннических действий. Основой для реализации названных мер предупреждения преступлений должен стать виктимологический мониторинг, предполагающий постоянное наблюдение за процессами виктимизации, в том числе связанной с киберпреступностью, оценку всех значимых показателей виктимности в данной сфере, уровень правовой и социальной защиты жертв посягательств.

Список использованных источников:

1. Состояние преступности в России за январь-декабрь 2025 года // Официальный сайт Министерства внутренних дел РФ. – URL: file:///C:/Users/Nati/Downloads/Sbornik_dlya_UOS%20(8). pdf (дата обращения: 28.03.2026)

2. Пинкевич, Т.В. Цифровое неравенство как фактор преступности / Т.В.Пинкевич // Виктимология. – 2024. – Т. 11. – № 4. – С. 538-545.

3. Ривман, Д.В. Криминальная виктимология / Д.В. Ривман. – СПб.: Питер, 2002. – 304 с.

4. Кабанов, П.А. Жертвы киберкраж как объект современной российской кибервиктимологии: криминологический анализ статистических показателей криминальной виктимности 2021–2022 гг. / П.А. Кабанов // Виктимология. – 2024. – Т. 11. – № 1. – С. 25-42.

5. Жмуров, Д.В. Общая виктимологическая профилактика киберпреступности / Д.В.Жмуров // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2022. – № 4 (60). – С. 135-142.

6. Российская газета. – 2025. – 4 апреля.