МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра уголовного права и криминологии

ДИПЛОМНАЯ РАБОТА

на тему **«ВИКТИМОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННОГО И КОМПЬЮТЕРНОГО ОБОРУДОВАНИЯ В РОССИИ»**

Выполнил
Яхин Тимур Рафаильевич
обучающийся по специальности
40.05.02 Правоохранительная деятельность
2020 года набора, 0202 учебной группы

Руководитель
доцент кафедры,
кандидат юридических наук
Пейзак Анастасия Викторовна

К защите рекомендуется
рекомендуется / не рекомендуется
Начальник кафедры _____ И.Р. Диваева
подпись
Дата защиты «___» _____ 2026 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Актуальность темы исследования. Современные цифровые технологии обеспечили достижение более комфортной среды для жизни человека. Вместе с тем, процессу цифровизации подверглось и такое негативное социальное явление как преступность. В результате произошел резкий всплеск роста преступлений, совершенных с помощью информационных и телекоммуникационных технологий. Только за пятилетний период указанная группа преступлений выросла на 76,7 % с 517722 преступлений в 2021 году до 675372 преступлений в 2025 году[1].

Одним из наиболее распространенных преступлений, совершаемых в киберпространстве, является мошенничество. Кибермошенники совершают хищения самыми разными и изощренными способами благодаря таким показателям цифровой среды как анонимность, быстродействие, минимальная информация о следовой картине преступления и т.д. Только за последний год удалось снизить количество кибермошенничеств на 34300 преступлений, однако, общий тренд роста еще сохраняется за период с 2021 по 2025 года (см. Приложение 1)[2].

В системе борьбы с кибермошенничествами важна консолидация сил и средств государства, заинтересованных организаций (банковские и кредитные организации, операторы сотовой связи, интернет-провайдеры и др.), а также физических лиц, т.е. граждан, которые становятся жертвами таких преступлений. Этот особенный механизм по становлению жертвы от кибермошенничества является базой той части системы предупреждения преступлений, которая должна быть направлена на прекращение кибервиктимизации. В этой связи, учеными-криминологами изучается виктимологическая характеристика кибермошенничеств с целью планирования

[1] Доклад МВД России о состоянии преступности за 2021-2025 года: [Электронный ресурс]: Интернет-портал МВД России. URL://http://мвд.рф (дата обращения: 11.02.2026).

[2] Там же.

и реализации мероприятий по виктимологическому предупреждению кибермошенничеств[1].

Виктимологическое предупреждение как часть общего предупреждения кибермошенничества реализуется путем воздействия на причины и условия, детерминирующие процесс виктимизации, а также учитывает элементы личности отдельных групп жертв, подверженных кибермошенничеству.

В этой связи субъектами виктимологического предупреждения реализуется общее предупреждение кибермошенничеств и вообще киберпреступлений и индивидуальную профилактику, направленную на конкретных лиц. органы внутренних дел являются субъектами реализации практически всех направлений виктимологического предупреждения кибермошенничества. В этих целях, в структуре органов внутренних дел функционирует служба, специально уполномоченная на профилактику преступлений в целом – служба участковых уполномоченных полиции. В его арсенале закреплены формы несения службы, в рамках которых может осуществлять и виктимологическая профилактика кибермошенничеств. Однако, такая деятельность участковых уполномоченных полиции требует модернизации, например, нормативного закрепления обязанности проводить виктимологическую профилактику, а также внедрение новых технологических средств предупреждения на базе национального мессенджера Макс.

В свете сказанного, необходимо исследовать общую характеристику потерпевших от преступлений, связанных с мошенничеством, совершаемым с использованием телекоммуникационного и компьютерного оборудования, и на основе результатов этого исследования спланировать мероприятия по виктимологическому предупреждению кибермошенничеств.

Цель выпускной квалификационной работы заключается в исследовании виктимологической характеристики мошенничества, совершаемого с

[1] Гришко Н. А. Защита потенциальных жертв киберпреступлений: виктимологический подход / Н. А. Гришко // Вестник Университета имени О.Е. Кутафина (МГЮА). 2025. № 5(129). С. 234-243.

использованием телекоммуникационного и компьютерного оборудования в России.

Указанная цель предполагает решение следующих задач:

– изучить структуру, динамику и виды потерпевших от мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования;

– рассмотреть причины и условия становления гражданина жертвой от мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования;

– охарактеризовать общее виктимологическое предупреждение мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования;

– проанализировать роль участковых уполномоченных полиции в индивидуальной виктимологической профилактике мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования.

Объектом выпускной квалификационной работы являются общественные отношения, которые складываются в процессе виктимологического предупреждения кибермошенничеств.

Предмет выпускной квалификационной работы составляют: комплекс научной и учебной литературы по проблемам виктимологической характеристики и виктимологического предупреждения рассматриваемых преступлений, статистические и аналитические данные Министерства внутренних дел Российской Федерации, территориальных органов внутренних дел.

Структуру выпускной квалификационной работы составляют введение, две главы, включающие в себя четыре параграфа, заключение, список использованной литературы, а также приложения.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПОТЕРПЕВШИХ ОТ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С МОШЕННИЧЕСТВОМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННОГО И КОМПЬЮТЕРНОГО ОБОРУДОВАНИЯ

§ 1. Структура, динамика и виды потерпевших от мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования

Одним из важнейших предназначений виктимологической науки является практическая значимость результатов, которые получают криминологи в рамках исследований элементов виктимологической характеристики преступности или какой-то отдельной группы преступлений. В целях планирования и практической реализации виктимологического предупреждения преступлений, связанных с мошенничествами, совершаемыми с использованием телекоммуникационного и компьютерного оборудования, необходимо изучить общую виктимологическую характеристику таких преступлений, которая состоит из следующих элементов: определение исследуемой группы преступлений, жертвами которых становятся граждане, выявление количественных и качественных показателей о потерпевших, рассмотрение комплекса причин и условий процесса виктимизации по исследуемой группе преступлений, а также определение типов жертв, с которыми следует проводить виктимную профилактику в первую очередь.

В криминологической науке под виктимологией понимают раздел, посвященный изучению психофизиологических особенностей жертв преступлений. При этом, достаточно развита общая виктимология, как наука о комплексе причин и условий детерминирующих поведение жертв преступлений и типизации личности таких жертв. Также развиваются узкие исследования поведения жертв конкретных групп преступлений или жертв в определенных

условиях, например, в условиях алкогольного или наркотического опьянения, или, например, жертв в условиях цифрового пространства.

В свете сказанного, достаточно динамично в настоящее время развивается такой раздел криминологии как кибервиктимология. Если виктимное поведение представляет собой совокупность элементов такой модели поведения, в результате которой гражданин становится жертвой противоправного деяния, то кибервиктимное поведение, соответственно, в качестве таких элементов модели поведения учитывает те из них, которые связаны с факторами цифровой среды, как источника формирования подструктур личности.

Таким образом, современные криминологи, которые занимаются проблемами виктимологии, понимают под указанным разделом криминологии область научного знания, направленного «на формирование новых средств и технологий виктимологической защиты для обеспечения виктимологической безопасности потенциальных жертв киберугроз»[1]. Вместе с тем, нами в настоящей выпускной квалификационной работе будет рассмотрен частный подраздел кибервиктимологии, связанный с мошенничествами, совершаемыми с использованием телекоммуникационного и компьютерного оборудования.

Прежде чем рассматривать структуру и динамику потерпевших от мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, необходимо ввести определение указанной группы преступлений. Часть ученых-криминологов в научной литературе под группой преступлений, связанных с мошенничеством, совершаемым с использованием телекоммуникационного и компьютерного оборудования, понимают совокупность преступлений, совершающихся при помощи информационных технологий и имеющих экономический характер[2].

---

[1] Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии:краткий статистический анализ показателей криминальной виктимности2021-2022 гг // Виктимология. 2023. Т. 10, № 1. С. 17-28.

[2] Андрианова Е. В. Социальный портрет жертв кибермошенничества // Экономическая безопасность страны, регионов, организаций различных видов деятельности : Материалы Четвертого Всероссийского форума в Тюмени по экономической безопасности, Тюмень, 19–22 апреля 2023 года. Тюмень: ТюмГУ-Press, 2023. С. 265-269.

Отдельные ученые предлагают исследуемую группу преступлений именовать кибермошенничество и оперируют следующим понятием: «кибермошенничество выступает видом ИТ-преступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации и персональных данных пользователя»[1].

По нашему мнению, кибермошенничество или цифровое мошенничество наиболее удачное название для исследуемой группы преступлений, т.к. киберпространство или цифровое пространство является одновременно местом совершения преступления (или его характеристикой) и способом совершения такого мошенничества. Таким образом, под кибермошенничеством нами предлагается понимать такой вид хищений, который направлен на получение персональных данных, имущества или финансовых средств потерпевшего в цифровом пространстве с помощью киберресурсов, а также сопряжен с обманом или злоупотреблением доверием, т.е. введением в заблуждение потерпевшего.

Действительно, пронизывание всех сфер жизни человека процессом цифровизации обусловил и цифровизацию криминальной сферы. При этом, с помощью цифровых технологий совершаются самые разные преступления. Рост их общего количества преступлений, совершенных с помощью информационно-телекоммуникационных технологий, только за последние пять лет с 2021 по 2025 год составил 76,7 %[2]. И если раньше для совершения преступлений, связанных с мошенничеством, нужен был физический контакт с другими лицами или объектами, то сегодня такие преступления совершаются с применением информационно-телекоммуникационных технологий и, в частности, сети Интернет, мобильной связи и т.д. Именно поэтому исследуемую группу преступлений также называют «цифровое мошенничество»,

---

[1] Коленова И. И. Виктимологическая профилактика кибермошенничеств // Объект преступления и уголовно правовой охраны: историко-правовой, аксиологический, методологический и формально-юридический аспекты : Материалы международной научно-практической конференции, Екатеринбург, 03 марта 2023 года. Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2023. С. 363-371.

[2] Доклад МВД России о состоянии преступности за 2021-2025 года: [Электронный ресурс]: Интернет-портал МВД России. URL://http://мвд.рф (дата обращения: 11.02.2026).

«кибермошенничество», встречается также понятие дистанционного мошенничества[1].

Законодатель предусмотрел уголовную ответственность за кибермошенничества. Так, ст. 159 Уголовного кодекса Российской Федерации[2] (далее – УК РФ) предусматривает общую ответственность за мошенничество, в т.ч. те его виды, которые могут быть совершены с помощью информационно-телекоммуникационных средств. Кроме того, законодатель обозначил отдельные виды мошенничеств в статьях 159.1, 159.2, 159.3, 159.5 и 159.6 УК РФ, некоторые из которых также предполагают возможность их совершения в киберпространстве.

С точки зрения применения результатов настоящей выпускной квалификационной работы действующими сотрудниками органов внутренних дел для планирования и реализации виктимной профилактики с гражданами территории обслуживания территориальным органом внутренних дел наиболее обоснованной считаем классификацию исследуемой группы преступлений на основании указания Генпрокуратуры России № 503/11, МВД России № 1 от 28 июля 2025 года «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности»[3] (далее – Указание Генпрокуратуры).

Так, анализ Перечня 25 Указания Генпрокуратуры позволяет выделить среди перечисленных в нем составов те виды мошенничества, совершенные с

---

[1] Павленко О. С. Кибермошенничество как дистанционное преступление: особенности совершения и перспективные меры профилактики / О. С. Павленко // Пермский период : Сборник материалов XI Международного научно-спортивного фестиваля курсантов и студентов образовательных организаций, посвященного 145-летию уголовно-исполнительной системы Российской Федерации, Пермь, 20–24 мая 2024 года. Пермь: Пермский институт Федеральной службы исполнения наказаний, 2024. С. 374-378.

[2] Уголовный кодекс Российской Федерации: Федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

[3] О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генпрокуратуры России № 503/11, МВД России № 1 от 28 июля 2025 года. [Электронный ресурс]. URL:// http://www.pravo.gov.ru (дата обращения: 08.02.2026).

использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации, на которые возможно эффективно виктимологическии воздействовать: ст. 159 (при условии наличия отметки в статистической карточке о способе совершения), ст. 159.3 и 159.6 (без условий) УК РФ.

Для понимания объема предупредительной работы, которую необходимо запланировать для борьбы с кибермошенничеством, важно оценить основные показатели такой преступности, а также сформировать понимание динамики элементов, характеризующих потерпевших от кибермошенничества.

Нами выбран период с 2021 по 2025 года для статистического исследования, чтобы можно было внимательнее рассмотреть факторы, которые повлияли на рост количества исследуемой группы преступлений – пандемия 2020 года, начало специальной военной операции, проводимой Российской Федерацией, а также реализация недавних законодательных решений, позволивших значительно снизить мошеннические кибератаки на граждан России.

Так, в Российской Федерации за период с 2021 по 2025 год количество кибермошенничеств демонстрирует тенденцию к увеличению со средним показателем прироста 26725 преступлений в год. Так, в 2021 году количество кибермошенничеств составило 238560 преступлений, в 2022 году – 249984, в 2023 году – 353201, в 2024 году – 379762, в 2025 году – 345461 (Приложение 1)[1].

Анализ диаграммы, представленной в Приложении 1, позволяет сделать вывод, что количество кибермошенничеств характеризуется ростом за исследуемый период наблюдений, вместе с тем, за последний год удалось значительно снизить количество указанных преступлений, в т.ч. посредством введения правового обеспечения различных кибератак. Однако, на фоне продолжающегося совершенствования общего предупреждения киберпреступлений, важно также развивать и меры профилактики,

[1] Доклад МВД России о состоянии преступности за 2021-2025 года: [Электронный ресурс]: Интернет-портал МВД России. URL://http://мвд.рф (дата обращения: 11.02.2026).

предлагаемые кибервиктимологией.

Указанный вид преступлений характеризуется крайне низким показателем раскрываемости, что значительным образом осложняет накопление следственного опыта и, следовательно, его унификацию и автоматизацию. Кроме того, низкий коэффициент раскрываемости свидетельствует о слабой системе общего предупреждения киберпреступлений. Так, в 2021 году коэффициент раскрываемости кибермошенничеств в России составило 9,1 %, в 2022 году – 12,2 %, в 2023 году –10,9 %, в 2024 году – 10 %, в 2025 году – 9,7 % (Приложение 2)[1].

Анализ диаграммы, представленной в Приложении 2, позволяет сделать вывод, что на фоне снижения общего количества мошенничеств, коэффициент раскрываемости продолжает снижаться за исследуемый период наблюдений. Данный факт свидетельствует о том, что помимо тех кибератак, которые удается блокировать посредством общепредупредительных мер, все еще остается та часть граждан, которая подвержена высокому риску стать жертвой кибермошенничеств, обходящих развернутые способы кибербарьеров общего предупреждения.

Рассмотрим динамику пострадавших лиц от кибермошенничества в России за период с 2021 по 2025 года. Так, в Российской Федерации за рассматриваемый период количество жертв от кибермошенничеств демонстрирует тенденцию к увеличению со средним показателем прироста 27579 жертв в год. Так, в 2021 году количество жертв от кибермошенничеств составило 239894 лиц, в 2022 году – 252798, в 2023 году – 352741, в 2024 году – 380203, в 2025 году – 350211 (Приложение 3)[2].

Положительно следует оценить и работу правоохранительных органов по выявлению кибермошенников. Так, в 2021 году количество выявленных кибермошенников в России составило 7749 лиц, в 2022 году – 11046, в 2023 году

[1] Доклад МВД России о состоянии преступности за 2021-2025 года: [Электронный ресурс]: Интернет-портал МВД России. URL://http://мвд.рф (дата обращения: 11.02.2026).

[2] Там же.

– 14568, в 2024 году – 14073, в 2025 году – 13247 (Приложение 4)[1].

Однако, как правило, среди кибермошенников выявляют исполнителей и пособников, но организаторов кибератак выявить получается редко, что только актуализирует развитие системы виктимологической профилактики, т.к. лишившись исполнителей, организатор заново собирает команду преступников, которые продолжают свою киберпреступную деятельность.

Группа преступлений, связанных с кибермошенничеством, является достаточно многогранной, в т.ч. и по способу покушения и по сфере общественных отношений, на которые они посягают. Вместе с тем, нами предпринята попытка выявить структуру кибермошенничества исходя из указанных признаков.

Необходимо отметить, что в период с 2022 года значительно активизировались заграничные источники кибермошенничества в отношении российских граждан, которые в т.ч. используют данный механизм для осуществления подрыва основ конституционного строя России в условиях специальной военной операции.

Рассмотрим структуру кибермошенничества для выявления наиболее характерных действий, которые совершают кибермошенники и которые возможно учитывать при планировании виктимной профилактики. Указанный анализ в настоящей выпускной квалификационной работе произведен на основе пятидесяти произвольно выбранных уголовных дел, связанных с кибермошенничеством, совершенным в отношении граждан Республики Башкортостан за период с 2021 по 2025 год (далее – выборка уголовных дел)[2].

Итак, исследование различных подходов к классификации видов кибермошенничества, а также выборки уголовных дел позволил выделить следующие из них (Приложение 5):

– добровольная передача жертвой своих денежных средств

---

[1] Доклад МВД России о состоянии преступности за 2021-2025 года: [Электронный ресурс]: Интернет-портал МВД России. URL://http://мвд.рф (дата обращения: 11.02.2026).

[2] Аналитическая таблица за 2021-2025 года по Форме SPS294 в сфере ИТТ Перечень 25. Архив ИЦ МВД России по Республике Башкортостан.

злоумышленнику за оказание услуг или выполнение работ, а также в счет выполнения обязательств по поставке какой-либо продукции (24 % от выборки уголовных дел);

– хищение денежных средств субъектом преступления путем введения жертвы в заблуждение, совершенное с использованием сотовой связи (30 % от выборки уголовных дел);

– хищение денежных средств у жертвы посредством получения незаконного доступа к системам удаленного банковского обслуживания (мобильный банк), в т.ч. при помощи вредоносного программного обеспечения (12 % от выборки уголовных дел);

– распространение злоумышленником заранее недостоверных данных в сети Интернет с указанием реквизитов платежа для перевода денежных средств потерпевшим и их последующего хищения (34 % от общего количества рассмотренных обвинительных заключений)[1].

Анализ представленной структуры в Приложении 5 позволяет сделать вывод, что чаще всего кибермошенничество совершается в виде хищения денежных средств субъектом преступления путем введения жертвы в заблуждение, совершенное с использованием сотовой связи, а также путем распространения злоумышленником заранее недостоверных данных в сети Интернет с указанием реквизитов платежа для перевода денежных средств потерпевшим и их последующего хищения.

То, каким образом совершается кибермошенничество, тесно связано с личностью самой жертвы. Так, нами проведен перекрестный анализ некоторых социально-экономических показателей личностей потерпевших от кибермошенничества из выборки уголовных дел. При этом, отметим, что невозможно выявить достоверную типичную личность жертвы кибермошенничества, т.к. очень вариативен ряд элементов, составляющих такую личность. Вместе с тем, нам удалось на примере выборки уголовных дел за 2021-

[1] Аналитическая таблица за 2021-2025 года по Форме SPS294 в сфере ИТТ Перечень 25. Архив ИЦ МВД России по Республике Башкортостан.

2025 года рассмотреть некоторые типичные элементы личности жертв от кибермошенничества в Республике Башкортостан[1].

Так, рассматривая характеристику возраста жертв кибермошенничества, мы выявили следующую структуру: самую большую долю жертв от кибермошенничества составили лица в возрасте старше 50 лет – 48,0 %, в возрасте 30-49 лет – 18,0 %, в возрасте 19-29 лет – 12,0 %, в возрасте до 18 лет – 22,0 %. Среди указанных жертв от кибермошенничества были лица женского пола – 29 человек или 58,0 %, лица мужского пола составили – 42,0 %[2].

Следует отметить достаточно разнообразную структуру социально-экономического статуса среди жертв кибермошенничества. Так, 40,0 % составили пенсионеры, 28,0 % – работающие лица, 22,0 % учащиеся школ, 8,0 % – студенты, 2,0 % – безработные[3].

Также некоторые жертвы кибермошенничества были ранее знакомы с лицами, которым они передали свои денежные средства. Таких жертв в выборке уголовных дел было 3 лица, т.е. 6 %[4].

Перекрестный анализ выявленных нами криминологических способов совершения (конкретных действий) кибермошенничества и элементов личности жертв кибермошенничества позволили сформировать несколько типичных жертв:

1. Пенсионер, женского пола, которая была введена в заблуждение по сотовому телефону кибермошенниками.

2. Работающие мужчина или женщина, которые оплатили товары или услуги по недостоверным реквизитам.

3. Граждане, чьими данными завладели удаленно с последующим хищением денежных средств.

4. Работающие мужчина или женщина, передавшие свои денежные средства

---

[1] Аналитическая таблица за 2021-2025 года по Форме SPS294 в сфере ИТТ Перечень 25. Архив ИЦ МВД России по Республике Башкортостан.

[2] Там же.

[3] Там же.

[4] Там же.

для инвестирования, развития бизнеса, дополнительного заработка и т.д.

5. Несовершеннолетние, которые были введены в заблуждение и передали денежные средства или персональные данные своих родителей кибермошенникам.

Так, несовершеннолетний Р. был введен в заблуждение неизвестным лицом, которое позвонило ему на сотовый телефон и представилось сотрудником полиции К. В ходе разговора неизвестное лицо убедило несовершеннолетнего Р. в необходимости «задекларировать» доход его родителей через онлайнвидеосъемку. После отправки «видеодекларации» несовершеннолетним, введенным в заблуждение, полицейский-мошенник попросил передать все деньги и ценности курьеру, подъехавшему к дому несовершеннолетнего Р., который выполнил указание неизвестного лица. О случившемся неизвестное лицо попросило не сообщать родителям[1].

Несмотря на то, что выявленные элементы не могут дать полную картину о типичной личности жертвы кибермошенничества, считаем необходимым, эти элементы учитывать при формирование системы предупреждения.

В качестве вывода отметим, что для того, чтобы достичь целей противодействия конкретной группе преступлений, необходимо понять, каковы сущностные признаки такой группы, что ее обособляет среди других видов преступлений, кроме того, следует изучить состояние такой преступности, а также исследовать виктимологические особенности исследуемой группы преступлений. Нами выявлено, что с проникновением цифрового пространства в разные сферы жизни людей появились и новые способы совершения преступлений, в т.ч. мошенничеств. Так, кибермошенничества представляют такую собой группу хищений, которые направлены на захват персональных данных, имущества или финансовых средств потерпевшего в цифровом пространстве с помощью киберресурсов, а также сопряжены с обманом или злоупотреблением доверием, т.е. введением в заблуждение жертвы. Выявлено,

[1] Материалы уголовного дела № 125018000010000** от 12.*.2025 по ч. 2 ст. 159 УК РФ, возбужденное ОМВД России по Белебеевскому району.

что за последние пять лет наблюдений с 2021 по 2025 года указанные преступления демонстрируют тенденцию к росту. В этой связи, учеными и практическими работниками правоохранительных органов, а также заинтересованными финансовыми и сотовыми организациями, разрабатываются специальные меры по противодействию указанной группе преступлений, в т.ч. в рамках виктимологической оставляющей. Для планирования мероприятий, снижающих риски кибервиктимизации населения, нами выявлены типичные действия, которые совершают кибермошенники в отношении граждан, в совокупности с отдельными социально-экономическими элементами личности жертвы от кибемошенничества на основе анализа выборки уголовных дел. Выявлено, что самыми виктимными группами населения, в отношении которых совершаются кибермошенничества являются пенсионеры и учащиеся школ. Нами также разработаны типичные портреты жертв от киберпреступлений. В следующем параграфе рассмотрим причины и условия становления жертвой от кибермошенничества.

§ 2. Причины и условия становления гражданина жертвой от мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования

Для понимания общего состояния элементов виктимологической характеристики кибермошенничеств необходимо выявить те детерминанты, которые определяют возможность совершения указанных преступлений, что также необходимо для формирования системы их предупреждения.

В научной литературе под детерминантами, как элементом криминологической характеристики, понимают совокупность причин и условий отдельной группы преступлений или преступности в целом[1]. Такие причины и

[1] Никульченкова Е. В. Кибераддикции как детерминанты виктимности жертв кибермошенничества // Психопедагогика в правоохранительных органах. 2025. Т. 30, № 3(102). С. 306-310.

условия в зависимости от групп преступлений имеют свои особенности, присущие конкретной группе преступлений с криминологического аспекта. Вместе с тем, в такой системе детерминантов есть и такие, которые характерны для виктимологического аспекта совершения преступлений.

Рассмотрим понятие факторов, обуславливающих виктимизацию, которое сформировалось в криминологической науке. Следует выделить три подхода, в соответствии с которыми рассматривается обозначенный термин.

Так, в соответствии с первым подходом под факторами виктимизации необходимо понимать различные обстоятельства, которые обеспечивают превращение субъекта в жертву. Особенностью обозначенного подхода является то, что, как правило, субъект превращается в жертву из-за воздействия внешней среды. Второй подход понимания факторов виктимизации обеспечивается их пониманием в качестве определенных особенностей личности, которые могут спровоцировать преступное деяние. К примеру, речь может идти об агрессивности, доверчивости и т.д. Третий подход понимания факторов, способствующих виктимизации, характеризуется объединением свойств первого и второго подходов. Так, последователи указанного подхода обозначают, что имеющиеся у субъекта личностные особенности не могут спровоцировать совершение преступления при отсутствии необходимых условий. Получается, что совершению против конкретного лица преступления могут поспособствовать как его личные особенности в совокупности с внешними обстоятельствами, так и исключительно внешние обстоятельства, но факт посягательства на личность, который связан только с ее личностными особенностями, мы исключаем, так как если на лицо некому будет совершать посягательство, то его личностные особенности не играют никакой роли. Таким образом, под факторами обуславливающими виктимизацию необходимо считать систему причин, обусловивших виктимное поведение субъекта, последствием чего стала возможность совершения в отношении него преступного деяния[1].

[1] Веряскин И. А. Факторы криминальной виктимизации несовершеннолетних // Общественная безопасность, законность и правопорядок в III тысячелетии. 2022. № 8-1. С. 23-28.

Отдельными авторами исследуются конкретные элементы личности, которые могут стать определяющими в процессе виктимизации – пол, возраст, социальный и имущественный статус, психофизиологические особенности и т.д.[1]. сочетание нескольких показателей или характеристик личности потенциальной жертвы может обусловить совершение кибермошенничества в отношении нее. Например, учеными-криминологами чаще всего в структуре жертв от кибермошенничества выделяется группа пожилых людей или пенсионеров. В научных публикациях можно встретить достаточное количество исследований, посвященных виктимизации конкретной группы населения в кибермошенничество – пенсионеры, несовершеннолетние, одинокие граждане, граждане с наличием сберегательных счетов, женщины, лица, занятые в отдельных видах профессиональной деятельности (госслужащие, работники сферы предпринимательства) и т.д.

В свете сказанного, нами предлагается рассматривать всю совокупность причин и условий кибервиктимизации в виде двух групп:

1) общие факторы, детерминирующие становление гражданина жертвой от кибермошенничества;

2) специальные факторы, связанные с кибервиктимизацией конкретных групп населения.

В качестве общих причин, оказывающих влияние на виктимизацию всех групп населения, необходимо выделять экономические, политико-правовые и социальные-психологические факторы.

1. Важное место среди экономических факторов, влияющих на виктимизацию населения, необходимо выделить низкий уровень жизни населения, расслоение общества, а также безработицу. Необходимо отметить, что обозначенные факторы являются также и детерминантами преступности, что еще раз подчеркивает тесную взаимосвязь виктимизации и криминализации населения. Низкий уровень жизни может способствовать формированию в

[1] Семеняченко А. А. Кибермошенничество и кибербезопасность: как защитить пенсионеров и уязвимые слои общества // Юный ученый. 2025. № 11(96). С. 60-63.

обществе различных негативных социальных явлений, к примеру, развитию алкоголизма, наркомании, проституции и т.д., что само по себе может детерминировать виктимизацию. Расслоение общества также обеспечивает возможность формирования условий виктимизации населений. К примеру, появления категории граждан с высоким доходом может обеспечивать условия совершения в отношении них преступлений, а также формирования у них виктимного поведения. Фактор безработицы также может способствовать виктимизации населения, что выражается в появлении категории граждан, которые социально не защищены, что может способствовать совершению в отношении них различных преступлений.

2. Важность имеют и политико-правовые факторы, оказывающие влияние на виктимизацию населения. В частности, в криминологических исследования имеет место термин «принудительная виктимизация», означающий процесс осуществления принятия определенных решений, либо бездействия органов государственного управления, что непосредственным образом может влиять на виктимизацию населения. Так, П.Н. Фещенко связывает процесс принудительной виктимизации населения с множеством аспектов, которые находятся в зоне ответственности различных органов государственного управления, к примеру, низкая эффективность пенитенциарной системы, что выражается в количестве преступлений, совершаемых лицами повторно, отсутствием необходимых инструментов снижения виктимизации населения, к примеру, механизма криминологической экспертизы нормативных правовых актов, отсутствием разработанных нормативных актов в области осуществления снижения уровня виктимизации населения, в том числе, по линии отдельных органов власти и т.д.[1].

3. В качестве социально-правовых факторов общего роста виктимизации населения необходимо рассматривать различные критерии. В частности, большое влияние на виктимизацию населения оказывает отсутствие должного

[1] Жмуров Д. В. Кибервиктимизация: понятие и характерные свойства // Международный научный вестник. 2025. № 3. С. 44-48.

воспитания в семьях, когда виктимное поведение начинает формироваться еще с детства. Так, привитие детям агрессивности, аморального поведения, иных негативных черт, может в дальнейшем спровоцировать виктимное поведение. Важно понимать, что субъект сам может и не осознавать, что является субъектом процесса виктимизации, а полное осознание этого может наступить лишь после реального совершения в отношении него преступления. Негативное влияние на виктимизацию населения оказывают идеологические и культурные факторы, среди которых отказ от ценностей и стереотипов советского общества без замены их на альтернативные ценности, отсутствие официальных молодежных движений, составляющих «конкуренцию» неформальным подростковым группам, десоциализирующее влияние массовой культуры на личность, политико-идеологический плюрализм, не подкрепленный историческими и культурными предпосылками и др.

Рассмотрим комплекс специальных факторов, которые детерминируют виктимизацию совершения кибермошенничеств в отношении отдельных групп населения.

Так, одним из таких факторов является компьютеризация и развитие информационных и телекоммуникационных технологий. Указанные процессы значительным образом влияют на виктимизацию группы лиц по возрастному признаку. В частности, субъекты пенсионного возраста часто становятся жертвами преступлений в силу отсутствия у них необходимых знаний и навыков использования таких технологий. Этим объясняется рост группы преступлений, совершенных с помощью информационных технологий, где значительной частью потерпевших выступают лица пенсионного возраста[1]. С другой стороны, компьютеризация и внедрение новых информационных и телекоммуникационных технологий может провоцировать виктимизацию несовершеннолетних. В частности, это происходит посредством развития социальных сетей, иных площадок общения, где активно участвуют

[1] Палий Е. С. Виктимологическая характеристика лиц пенсионного возраста: постановка проблемы // Судебная экспертиза и исследования. 2025. № 1. С. 115-123.

несовершеннолетние граждане[1].

Для лиц пенсионного возраста могут иметь определяющее значение факторы попадания в среду виктимности, связанные со снижением жизненной активности, умственных способностей, развитием различных болезней, в том числе психических и т.д.

Необходимо учитывать, что обозначенные факторы могут способствовать совершению в отношении пожилых граждан различных преступлений. В частности, низкий уровень умственных способностей может легко провоцировать мошеннические действия. Наличие физиологических недостатков, заболеваний может способствовать совершению кибермошенничества. В силу определенных обстоятельств, многие пожилые граждане проявляют доверчивость к определенному типу субъектов, в частности сотрудникам полиции, работникам специальных и социальных служб, чем активно пользуются преступники.

Для жертв кибермошенничества женского пола является характерным их специфические личностные качества – забота об окружающих, гиперответственность, проявления беспокойства и тревожности за близких и родных, что также является удобным для кибермошенников, которые выбирают такой способ совершения преступления, когда вводят жертву в заблуждение относительно оказания помощи другим людям, в частности, родным, близким и т.д. Несомненно, указанная предрасположенность

В научной литературе в качестве факторов кибервиктимизации также называют следующие комплексы триггеров[2]:

1) поведенческие. Эти триггеры связаны с видимым в цифровом пространстве для кибермошенников образом потенциальной жертвы при ее точечном выборе. Кроме того, кибермошенники, предполагая встретить

---

[1] Макаримова Н. Т. Изучение проблемы виктимизации в юношеском возрасте и её последствий для личности // Лучшая исследовательская работа 2022. Сборник статей IV Международного научно-исследовательского конкурса. Петрозаводск, 2022. С. 249-261.

[2] Жмуров Д. В. Кибервиктимология / Д. В. Жмуров. М.: Издательство «Юрлитинформ», 2023. С. 98.

подобных потенциальных жертв, могут осуществлять сплошную кибератаку на неограниченный круг лиц, например, настраивать автодозвоны на более чем тысячу номеров операторов сотовой связи. Итак, среди поведенческих триггеров следует выделять:

– активное участие в социальных сетях, высокая онлайн активность, избыточная увлеченность интернетом; участие в онлайн играх;

– чрезмерная репрезентация личности в сетевом пространстве;

– просмотр порнографических, экстремистских и иных запрещенных или антисоциальных материалов;

– использование неоднозначных средств виртуальной коммуникации, например, порнографических онлайн-чатов;

– скачивание пиратских программ, видео- и аудио контента;

– установка программ и приложений с низким рейтингом или отрицательными отзывами;

– совершение покупок в интернете, импульсивное финансовое и «эмоциональное» потребительское поведение;

– стремление к быстрому и высокому заработку;

– пренебрежение программами антивирусной защиты: отказ от их установки либо обслуживания;

– неосмотрительное и некритичное поведение при использовании электронных устройств, например, использование общественного Wi-Fi;

– демонстрация вербальной агрессии;

– виктимная инертность, т. е. неспособность или нежелание реагировать на действия киберпреступников адекватным образом;

2) психологические. Обозначенный вид триггеров связан с совокупностью сознательных и подсознательных подструктур личности кибержертвы. Несмотря на то, что невозможно универсализировать миллиарды вариаций человеческой психики, учеными предпринята попытка выявить отдельные психологические симптомы, которые могут быть присущи кибержертвам:

– симптомокомплекс виртуальной жертвы (беспокойство, неуверенность в

себе, подверженность настроению, неусидчивость, неустойчивость настроения, гневливость);

– высокие баллы по шкале нейротизма, открытость, антисоциальное поведение, застенчивость, отстраненность, психопатологические расстройства;

– установка на рискованное социальное поведение, конформность, тревожность, интроверсия, склонность к зависимому и беспомощному поведению, высокая чувствительность, потребность в поддержке и сочувствии;

– посттравматические и стрессовые реакции;

– внушаемость, доверчивость, неосмотрительность, отсутствие критического мышления, беспечность;

– отдельная группа качеств, связанных с функционированием индивида в условиях виртуальной реальности и погружением в нее (виртуализация сознания, кибер-аутизация, виктимная амбивалентность, психологические особенности киберсерфинга, т.е. мнимой безопасности);

3) социальные. Среди таких триггеров следует указать те, которые меняют архитектуру социальных связей в новом цифровом обществе и при этом оказывают воздействие на кибервиктимизацию:

– всеобщая компьютеризация и цифровизация;

– увеличение потока персональных данных частных лиц и организаций в различные информационные системы;

– недостаточное вмешательство в регулирование складывающихся отношений в киберпространстве;

– формирование в обществе культурных взглядов, связанных с поощрением самопрезентации собственного «Я»;

– невысокий уровень компьютерной грамотности;

– социальные проблемы в микросреде кибержертв, например, необустроенность быта, сложные отношения в семье обуславливают включение индивида в цифровое пространство, уход от реальности, в которой социально некомфортно;

4) технические. В научной среде под указанным комплексом триггеров

понимают такое явление как «виктимность компьютера»[1]:

– несовершенство и уязвимости компьютерных систем,

– технические риски, связанные с работой оборудования,

– ориентация на техноценоз;

– техническая дезадаптация.

В качестве вывода отметим, что кибервиктимизация представляет собой процесс становления гражданина жертвой от киберпреступлений, в т.ч. от кибермошенничеств. Указанный процесс детерминируется различными причинами и условиями. Анализ научной литературы и выборки уголовных дел позволил выявить две группы детерминант виктимности от кибермошенничества: общая группа факторов и группа специальных факторов, связанных с кибервиктимизацией конкретных групп населения. Кроме того, нами проанализирован комплекс триггеров, разработанный отечественными учеными по кибервиктимизации граждан. Таким образом, нами выявлено, что необходимо на основе указанных детерминант разрабатывать как меры общего предупреждения, так и индивидуальной профилактики. Особенностью такого предупреждения должна быть работа с выявленными нами отдельными группами граждан, подверженными кибервиктимизации – пожилые и несовершеннолетние граждане.

[1] Жмуров Д. В. Техногенные предпосылки кибервиктимизации // Виктимология. 2023. Т. 10, № 2. С. 138-146.

ГЛАВА 2. ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННОГО И КОМПЬЮТЕРНОГО ОБОРУДОВАНИЯ

§ 1. Общее виктимологическое предупреждение мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования

Рассмотрение в первой главе исследования элементов, составляющих криминологическую характеристику мошенничеств, совершаемых с использованием телекоммуникационного и компьютерного оборудования, позволило выявить необходимость совершенствования основ их общего и индивидуального предупреждения применительно к жертвам обозначенных деяний. Как и при осуществлении профилактического воздействия в сфере иных групп преступлений, целесообразно рассматривать два взаимодействующих элемента обозначенной деятельности, среди которых общее виктимологическое предупреждение, а также индивидуальная виктимологическая профилактика[1].

Как уже было указано в первом параграфе выпускной квалификационной работы, рассматриваемая группа преступлений имеет существенные особенности, что неминуемо отражается на необходимости применения особых механизмов такой профилактики. В настоящем параграфе исследования необходимо рассмотреть проблематику реализации общего виктимологического предупреждения в рассматриваемой сфере.

Важным представляется то, что обеспечение должного предупредительного эффекта в рассматриваемой сфере общественных отношений должно реализовываться именно через виктимологическое предупреждение. При осуществлении обозначенного направления следует

[1] Голятина С. М. Предупреждение кибермошенничества: виктимологический аспект // Вестник Волгоградской академии МВД России. 2025. № 4 (75). С. 31-36.

минимизировать возможности мошеннического воздействия на потенциальных жертв подобных преступлений. Таким образом, целью общего виктимологического предупреждения рассматриваемой группы преступлений должно стать эффективное воздействие на комплекс процессов, которые оказывают влияние на формирование субъекта как жертвы обозначенных преступных деяний. В конечном итоге, обозначенное воздействие должно сформировать такие условия жизнедеятельности общества, в которых минимизированы возможности осуществления механизмов, связанных с совершением рассматриваемых преступлений, в том числе и тех, которые непосредственным образом связаны с поведенческой составляющей граждан.

Обеспечение общего виктимологического предупреждения рассматриваемых преступлений реализуется посредством деятельности значительного количества различных субъектов, включая государственные органы власти, коммерческие организации, в том числе финансовой сферы и сферы информационных технологий, общественные организации, отдельные исследователи обозначенной проблематики и т.д. При осуществлении указанной деятельности обеспечивается решение комплекса задач, среди которых комплексная деятельность, связанная с выявлением причинного комплекса совершения обозначенных противоправных деяний, выработка системы специальных мер, реализация которых сможет обеспечить нейтрализацию выявленных причин и условий совершения названных преступлений, обеспечение эффективного нормативного сопровождения, создание специальных организаций и государственных органов или подразделений государственных органов, обеспечивающих реализацию общего предупреждения названных преступлений, а также обеспечение процесса вовлечения в предупредительную работу всех заинтересованных субъектов, включая финансовые и телекоммуникационные учреждения[1].

Решение обозначенных задач должно обеспечиваться специальными

[1] Сорокун Н. С., Рудов М. В. Современное мошенничество и его предупреждение: учебное пособие. Ростов-на-Дону, 2024. С. 14.

группами мер, реализация которых позволит снизить количество рассматриваемых преступлений. Так, среди них необходимо рассматривать четыре основные группы: правовые, экономические, социально-психологические и организационные меры[1]. Важным представляется то, что в Российской Федерации обеспечивается реализация всех вышеобозначенных мер на уровне общего предупреждения названных преступлений, что позволило за последний год значительно снизить количественные показатели совершения мошенничеств с использованием телекоммуникационного и компьютерного оборудования, однако методика совершения обозначенных преступлений постоянно совершенствуется, что требует и модернизации специальных мер общего предупреждения.

Итак, одним из элементов реализации общего предупреждения рассматриваемых преступлений, являются правовые меры. В настоящее время в Российской Федерации идет процесс формирования специальной правовой базы, обеспечивающей рассматриваемые отношения. Необходимо указать, что обозначенный процесс происходит в большинстве правовых отраслей, что обеспечивает комплексность подхода. Вместе с тем, появляются новые угрозы, связанные с совершением рассматриваемых правонарушений, что требует от государственных органов, ответственных за правовое обеспечение рассматриваемых общественных отношений, оперативного реагирования посредством принятия новых нормативных правовых актов, а также изменения и дополнения уже действующих.

Так, в структуре реализации правовых мер предупреждения рассматриваемых преступлений были внедрены механизмы, связанные с возможностью установления запрета на получение кредитных продуктов финансовых учреждений, введен специальный период охлаждения по уже выданным гражданам кредитам, создана специальная государственная информационная система противодействия рассматриваемым

[1] Шашкин В. К. Виды и меры предупреждения киберпреступности // Вестник науки. 2025. Т. 3. № 5 (86). С. 725-731.

правонарушениям, обеспечено формирование специальных норм в законодательстве о связи, в том числе, по вопросам регистрации новых абонентов, предоставления услуг, а также обеспечения маркировки входящих звонков и т.д.

Кроме того, в структуре рассматриваемых мер обеспечивалось и планомерное обеспечение уголовно-правовой, а также административно-правовой охраны отношений в области противодействия мошенническим действиям с использованием телекоммуникационного и компьютерного оборудования. Так, появились нормы об ответственности в том числе для финансовых и телекоммуникационных организаций.

Безусловно, модернизация правовых мер, обеспечивающих предупреждение рассматриваемых преступлений должна продолжаться. По нашему мнению, среди приоритетных шагов законодателя в рассматриваемой области следует рассматривать необходимость правового обеспечения отношений в сфере использования специальных цифровых интеллектуальных систем противодействия кибермошенничеству на основе искусственного интеллекта. Необходимо отметить, что без действенного правового регулирования обозначенных отношений будет достаточно проблематично внедрять в деятельность заинтересованных субъектов обозначенные системы. На сегодняшний день, среди ведущих организаций финансового и телекоммуникационного сектора уже ведутся такие разработки, целью которых является предупреждение совершения подобных преступлений[1]. Так, ПАО «Сбербанк» разрабатывает и внедряет комплексную интерактивную систему безопасности, основанную на применении искусственного интеллекта, основанную на выявлении нетипичного поведения клиентов, выявления подозрительных банковских операций, обеспечения мониторинга иной активности, позволяющей констатировать возможные мошеннические действия.

[1] Лащёнов М. С., Лащёнов П. М. Роль информационных технологий в борьбе с кибермошенничеством // Информатизация и информационная безопасность правоохранительных органов. Сборник трудов Международной научно-практической конференции. Москва, 2025. С. 214-219.

Уже тестируются определенные механизмы блокировки финансовых операций. Вместе с тем, для полноценного применения обозначенных механизмов необходима соответствующая база, так как отдельные методы ее реализации могут быть связаны с серьезными ограничениями в области финансовых прав граждан. В структуре телекоммуникационных отношений также имеют место новаторские разработки, касающиеся отслеживания и блокирования подозрительных звонков, а также противодействия использованию технического оборудования, позволяющего обеспечить мобильную связь по национальным мобильным идентификаторам, находясь за пределами территории Российской Федерации.

По нашему мнению, в структуре правовых мер предупреждения рассматриваемых правонарушений следует рассматривать и необходимость регламентирования специальных механизмов работы с населением, включая обязанности финансовых и телекоммуникационных организаций по осуществлению должного обучения и информирования граждан в области финансовой и телекоммуникационной грамотности. Отметим, что на сегодняшний день подобные нормы в действующем законодательстве отсутствуют.

Не менее важной группой мер, обеспечивающих должное предупреждение мошенничеств, совершенных с использованием телекоммуникационного и компьютерного оборудования, являются экономические меры. Необходимо отметить, что экономические меры всегда являлись действенным инструментом предупреждения любых групп преступлений. Исследование личности жертв обозначенных преступлений показывает, что значительная их масса нуждается в дополнительных мерах защиты экономического характера. К примеру, группа граждан пенсионного возраста, в большей степени подвержена рассматриваемым мошенническим воздействиям. Это происходит, в том числе и потому, что названная социальная группа имеет низкий доход, а большинство таких граждан обеспечены лишь пенсионными выплатами. Необходимость дополнительного поиска дохода может существенным образом провоцировать

причины совершения в отношении них мошеннических действий.

В связи с этим, среди общих экономических мер необходимо рассматривать необходимость повышения уровня жизни населения, включая отдельных групп населения. Здесь же следует рассматривать и необходимость обеспечения возможности занятости, в том числе, гражданам пенсионного возраста. Обозначенные факторы сформируют здоровый социально-экономический фон, что обеспечит не только общее повышение уровня жизни населения, но и обеспечит повышение финансовой грамотности населения. Это подтверждается и отдельными научными исследованиями, где оговаривается связь экономических показателей с количественными характеристиками совершения преступлений, в том числе мошенничеств[1].

По нашему мнению, в структуре обозначенных предупредительных мер необходима деятельность финансовых организаций банковской сферы. В частности, анализ конкретных примеров совершения мошеннических действий показал, что достаточное количество жертв не хранили свои денежные средства в банках, в большинстве случаев, это касается лиц пенсионного возраста. Вместе с тем, среди таких жертв имели место и субъекты иных возрастных групп. Кроме того, значительное количество случаев мошеннических действий было связано с использованием несовершеннолетних, которые отдавали хранящиеся в жилом помещении денежные средства курьерам. В связи с этим, считаем целесообразным активизировать работу финансовых учреждений по популяризации хранения накоплений в банковских учреждениях, в связи с чем необходимо разрабатывать и внедрять льготные программы для отдельных групп населения, обеспечивать продвижение дополнительных стимулирующих продуктов. Кроме того, следует активнее внедрять и цифровой рубль, что позволит обеспечить значительную эффективность противодействия рассматриваемым преступлениям.

---

[1] Акжигитова А. Р., Егорова А. Н. Мошенничество как угроза экономической безопасности // Молодежь и наука: шаг к успеху. Сборник научных статей 7-й Всероссийской научной конференции перспективных разработок молодых ученых. Курск, 2024. С. 10-13.

Важной составляющей обеспечения должного общего виктимологического предупреждения рассматриваемой группы мошеннических действий, следует считать группу мер социально-психологического характера. В структуре реализации обозначенных мер задействованы различные субъекты, в том числе, различные государственные органы, средства массовой информации, финансовые, телекоммуникационные организации, общественные организации и иные. С помощью названной группы мер удается устранить значительное количество криминогенных факторов, способствующих совершению рассматриваемых преступлений[1]. Так, посредством названных мер формируется идеологическая и воспитательная составляющая, финансовая грамотность населения, умения использовать современные технические средства информационного и телекоммуникационного свойства. Важными методами, используемыми в структуре реализации названных мер, следует признать социальный видеоконтент, специализированные обучающие программы, а также информационные материалы печатного характера.

Вместе с тем, считаем, что обозначенное направление общего предупреждения рассматриваемых преступлений должно основываться и на комплексе научных исследований. К примеру, существует значительное количество исследований, посвященных проблематике выявления психологических факторов, особенностей личности потерпевших, а также иных составляющих, которые прямо или косвенно могут обеспечивать становление гражданина как жертвы возможных мошеннических действий. В связи с этим, существует необходимость обеспечения использования результатов таких исследований при формировании информационных и обучающих материалов, способствующих формированию у населения иммунитета к восприятию возможных механизмов, с помощью которых осуществляется преступное воздействие.

---

[1] Курумбаева А. Б. Общесоциальные меры предупреждения мошенничества, совершаемого с использованием информационных систем // Уголовно-правовое обеспечение информационной безопасности человечества. Материалы международной научно-практической конференции. Москва, 2025. С. 48-57.

Важным представляется то, что формирование обозначенного иммунитета должно иметь место во всей структуре цифровой среды, а именно в средствах массовой информации (телевидении, печатных изданиях, сети Интернет)[1]. Кроме того, необходимо обеспечить разработку и внедрение в цифровое поле специальных обучающих программных комплексов, с помощью которых будет обеспечено обучение отдельных групп населения способам исключения на них воздействия со стороны преступного элемента.

Также, важной составляющей общего предупреждения мошеннических действий с использованием телекоммуникационного и компьютерного оборудования, необходимо признать комплекс организационных мер предупреждения, направленных на потенциальных жертв обозначенных преступлений. В структуре обозначенных мер используются достижения научно-технического прогресса, связанные с предупреждением преступлений. Отметим, что на сегодняшний день активно разрабатываются и внедряются различные программные комплексы, необходимые для выполнения задач, связанных с предупреждением преступлений. В структуре предупреждения рассматриваемых видов мошенничества это является особо актуальным.

По нашему мнению, следует стимулировать деятельность специализированных организаций, обеспечивающих разработку подобных программных решений. Кроме того, существует необходимость разработки и внедрения специализированных комплексов, обеспечивающих качественное предупреждение рассматриваемых преступлений с использованием искусственного интеллекта.

Важной составляющей реализации организационных мер необходимо считать и соответствующую деятельность субъектов профилактики правонарушений. Так, в Российской Федерации сформирована система законодательных норм, посвященных проблематике деятельности различных

---

[1] Сырьев Б. О., Бурханова С. Д. Предупреждение кибермошенничества в социальных сетях // Юность и Знания - Гарантия Успеха - 2024. сборник научных статей 11-й Международной молодежной научной конференции : в 3 т.. Курск, 2024. С. 171-173.

субъектов в области профилактики правонарушений, однако, отсутствуют специальные алгоритмы осуществления общего предупреждения определенных групп преступлений. Внедрение таких алгоритмов может обеспечить должное применение всех законных методов профилактического воздействия, в том числе, в структуре виктимологического предупреждения, обеспечить должное взаимодействие всех заинтересованных субъектов[1].

Таким образом, в Российской Федерации предпринимаются значительные шаги по реализации системы правовых, экономических, социально-психологических, а также организационных мер общего предупреждения мошеннических преступлений, совершенных с использованием телекоммуникационного и компьютерного оборудования. Вместе с тем, реализация всех обозначенных в параграфе мер должна осуществляться комплексно, с привлечением всех заинтересованных субъектов. Необходимо указать, что важной составляющей такой реализации следует считать деятельность органов внутренних дел. Указанные субъекты обеспечивают широкий спектр задач в области предупреждения различных групп преступлений. Важной составляющей их деятельности является индивидуальная профилактика, в том числе, в отношении потенциальных потерпевших от мошеннических действий рассматриваемого вида, что реализуется посредством ежедневного несения службы.

В качестве вывода по параграфу выпускной квалификационной работы отметим, что обеспечение минимизации совершения мошенничеств с использованием телекоммуникационного и компьютерного оборудования может иметь значительный эффект в случае организации эффективного виктимологического предупреждения. Его реализация осуществляется как на общем уровне, так и на индивидуальном.

Так, общее виктимологическое предупреждение обозначенных преступлений обеспечивается четырьмя группами мер, среди которых правовые,

---

[1] Ильин И. С., Рязанова Е. Н. Виктимологическое предупреждение краж и мошенничеств, совершаемых бесконтактным способом // Закон и право. 2024. № 12. С. 208-214.

экономические, социально-психологические, а также организационные. В их реализации задействованы различные субъекты, среди которых государственные органы, коммерческие организации, общественные учреждения и иные. Применение всех обозначенных мер должно строится на эффективной правовой основе.

В структуре правовых мер следует продолжать работу по формированию законодательных механизмов, обеспечивающих минимизацию обозначенных деяний. В обозначенной работе должны принимать участие государственные органы, а также заинтересованные субъекты финансовых и телекоммуникационных организаций. Со стороны законодателя необходима проработка и закрепление механизма возможности использования специальных программных средств, в том числе, основанных на искусственном интеллекте, которые помогут обеспечить предупреждение рассматриваемых преступлений, а в отдельных случаях полностью исключат их совершение, в том числе путем определенных ограничений финансового и иного характера. В структуре реализации экономических мер предупреждения следует обеспечить продолжение комплексного решения общих социально-экономических проблем, связанных с уровнем жизни населения, формированием качественной трудовой инфраструктуры, в том числе для отдельных категорий граждан. Кроме того, считаем целесообразным обеспечить более оперативное внедрение в оборот цифрового рубля. Обеспечение социально-психологических мер предупреждения должно строиться на необходимости полномасштабного использования всей цифровой среды для обучения граждан, их информирования, повышения их финансовой грамотности, включая средства массовой информации, печатные издания, сеть Интернет. Нельзя забывать и про организационную составляющую, где основной упор необходимо делать на разработку специальных информационно-телекоммуникационных технических решений, а также на достижение системности и комплексности использования сил и средств всех субъектов предупреждения правонарушений, достижения их должного взаимодействия.

§ 2. Роль участковых уполномоченных полиции в индивидуальной виктимологической профилактике мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования

Не менее важной составляющей достижения минимизации совершения мошенничеств, совершаемых с использованием телекоммуникационного и компьютерного оборудования, следует признать деятельность, обеспечивающую индивидуальное виктимологическое воздействие. Обозначенная деятельность реализуется различными субъектами, однако, важный вклад в уровень ее эффективности вносится органами внутренних дел. В их структуре созданы и функционируют специальные подразделения участковых уполномоченных полиции, чья деятельность направлена, в большей степени, на обеспечение профилактического воздействия.

Деятельность обозначенных подразделений полиции регламентирована специальной системой нормативных правовых актов, где основным является ведомственная Инструкция[1], в положениях которой обеспечивается регламентирование специальных форм несения службы, а также методов профилактического воздействия, которые используются в целях индивидуальной профилактики рассматриваемых противоправных деяний. Вместе с тем, положения обозначенной Инструкции не содержат в себе положений, характеризующих понятие индивидуального профилактического воздействия. Кроме того, в названной Инструкции отсутствуют и положения, обеспечивающие процесс виктимологической индивидуальной профилактики.

В связи с этим, необходимо рассмотреть положения иных нормативных правовых актов, где имеют место нормы, закрепляющие подходы к пониманию обозначенной деятельности. Так, в структуре норм федерального закона «Об

[1] О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности: приказ МВД России от 29 марта 2019 № 205 // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 11.02.2026).

основах системы профилактики правонарушений в Российской Федерации»[1] содержится как общее понятие профилактической деятельности, так и оговаривается подход к пониманию содержательных особенностей индивидуальной профилактики правонарушений.

В ст. 2 названного федерального закона закреплено, что профилактика правонарушений представляет собой совокупность различных мер, среди которых меры социального, правового, организационного, информационного и иного характера, реализация которых направлена на обеспечение выявления и устранения причинного комплекса, способствующего совершению правонарушений, а также обеспечение должного воспитательного воздействия лиц в целях предотвращения ими правонарушений и антиобщественного поведения. Укажем, что законодатель обозначил достаточно широкий круг признаков, которые характеризуют обозначенную деятельность.

Понятие индивидуальной профилактики определяется в структуре положений ст. 15 названного федерального закона, в соответствии с которой под индивидуальной профилактикой следует понимать обеспечение воспитательного воздействия определенных субъектов, в целях исключения факторов, способствующих их противоправному поведению. Законодатель также указал, что индивидуальная профилактика может быть реализована с помощью специальных механизмов – мер профилактического воздействия[2].

Таким образом, законодатель подразумевает под индивидуальной профилактикой правонарушений именно воздействие на лиц, которые в силу определенных обстоятельств могут допускать противоправное поведение, в связи с чем предусматривает комплекс специальных мер воздействия, среди которых административный надзор, профилактический учет и иные. Вместе с

---

[1] Об основах системы профилактики правонарушений в Российской Федерации: Федер. закон Рос. Федерации от 23 июня 2016 г. № 182-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 10 июня 2016 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 15 июня 2016 г. // Собр. законодательства Рос. Федерации. – 2016. – № 26 (ч. 1), ст. 3851.

[2] Редькина Е. А. Профилактика преступлений: учебное пособие. Казань, 2024. С. 13.

тем, законодатель не регламентирует проблематику необходимости обеспечения должного виктимологического воздействия. Как уже отмечалось, в структуре рассматриваемых в работе проблем, виктимологическая профилактика имеет более весомое значение в достижении результата снижения рассматриваемых видов преступлений.

Вместе с тем, законодательство, регламентирующее деятельность участковых уполномоченных полиции, а также общее предупреждение правонарушений, закрепляет и иные формы профилактического воздействия, которые должны использоваться участковыми уполномоченными полиции в структуре индивидуальной виктимологической профилактики мошенничеств с использованием телекоммуникационного и компьютерного оборудования. Так, среди них особое значение имеют профилактические беседы, правовое информирование и просвещение, а также помощь лицам, пострадавшим от правонарушений или подверженным риску стать таковыми.

В первой главе выпускной квалификационной работы были выявлены категории граждан, которые в особенности подвержены риску совершения в отношении них рассматриваемых преступлений. Так, к обозначенным категориям следует относить граждан, пенсионного возраста, несовершеннолетних, а также иные категории. Именно в отношении указанных категорий должна организовываться индивидуальная виктимологическая профилактика на закреплённом административном участке посредством вышеуказанных форм воздействия.

Как уже было отмечено, реализация такой профилактической работы должна строиться на применении механизмов профилактического воздействия, среди которых профилактические беседы, правовое информирование и просвещение, а также помощь лицам, пострадавшим от правонарушений или подверженным риску стать таковыми. Необходимо рассмотреть указанные механизмы более детально и определить возможные направления их модернизации, что позволит обеспечить общее снижение количественных показателей совершения мошенничеств с использованием

телекоммуникационного и компьютерного оборудования [1].

Правовое информирование, как форма профилактического воздействия регламентирована ст. 18 федерального закона «Об основах системы профилактики правонарушений в Российской Федерации». В соответствии с ее положениями правовое информирование представляет собой процесс доведения до субъектов профилактики правовой информации с целью обеспечения предупреждения противоправных деяний. Обозначенная форма имеет значительную важность, так как большинство субъектов требующих индивидуального виктимологического профилактического воздействия, не обладают комплексом специальных правовых знаний, позволяющих обеспечить свою безопасность и не стать жертвой мошеннических действий. Так, в практике правоприменения существует достаточное количество случаев совершения противоправных деяний в отношении пожилых граждан, а также несовершеннолетних, которые в силу незнания положений правовых актов становились объектами мошеннических воздействий[2]. В этой связи, необходима и работа участкового уполномоченного полиции с семьями, где воспитываются несовершеннолетние. Отметим, что такая работа должна осуществляться во взаимодействии с подразделениями по делам несовершеннолетних.

Безусловно, в части лиц, требующих виктимологической профилактики, правовое информирование должно осуществляться в зависимости от категории таких лиц. К примеру, обеспечение правового просвещения и информирования лиц пенсионного возраста должно осуществляться с учетом их низкого уровня пользования информационно-телекоммуникационными устройствами, а также средствами электронных платежей.

---

[1] Габова О. С., Лукичев Ю. В. О роли участкового уполномоченного полиции в проведении общей профилактики преступлений и административных правонарушений // Административно-правовое регулирование охраны общественного порядка и обеспечения общественной безопасности: проблемы и пути их решения. Материалы ежегодной межвузовской научно-практической конференции . Санкт-Петербург, 2024. С. 52-56.

[2] Пономарева О. М. Правовое информирование как форма профилактического воздействия // Сборник материалов научно-представительских мероприятий Барнаульского юридического института МВД России. Сборник статей конференций. Барнаул, 2025. С. 141-144.

Правовое информирование как форма профилактического воздействия реализуется в структуре профилактической беседы, которая представляет собой важнейший инструмент достижения необходимого профилактического эффекта. В ст. 19 федерального закона «Об основах системы профилактики правонарушений в Российской Федерации» указывается, что профилактическая беседа состоит в разъяснении лицу, в отношении которого применяются меры индивидуальной профилактики правонарушений, существующих правил поведения, которые исключат возможность применения в отношении него мошеннических действий. В структуре названной нормы, имеет место и положение, в соответствии с которым порядок осуществления таких бесед должен определяться органами, уполномоченными осуществлять индивидуальное профилактическое воздействие. Необходимо отметить, что в структуре руководящей Инструкции, обеспечивающей деятельность участковых уполномоченных полиции отсутствуют обозначенные положения, а указывается лишь на обозначенные в вышеупомянутом федеральном законе положения. Считаем необходимым разработку специальных алгоритмов профилактических бесед с категориями граждан, подверженных совершению в отношении них мошеннических действий и последующего их внедрения в практику деятельности участковых уполномоченных полиции[1].

Кроме того, в ходе обеспечения деятельности, связанной с проведением индивидуальной виктимологической профилактической работы, участковому уполномоченному полиции следует разрабатывать специальные планы осуществления профилактических бесед в зависимости от категории граждан. Помимо категории граждан, в таких планах должны учитываться и иные факторы, среди которых особенности обслуживаемой территории, особенности, связанные с возрастными характеристиками лиц, особенности складывающейся на административном участке оперативной обстановки и т.д.

---

[1] Изингер А. В. Реализация отдельных форм профилактического воздействия в деятельности органов внутренних дел Российской Федерации // Вестник Тюменского института повышения квалификации сотрудников МВД России. 2024. № 1 (22). С. 11-17.

Профилактическую беседу следует рассматривать как самостоятельную форму индивидуальной профилактики с лицами, состоящими на профилактическом учете, в деятельности участкового уполномоченного полиции. В процессе несения службы участковым уполномоченным полиции, ее использование приносит весомый эффект, в том числе во взаимодействии с другими формами профилактического воздействия, а также методами общей профилактики, которые реализуются участковым уполномоченным в отношении всего населения административного участка[1]. Обозначенная форма должна реализовываться применительно ко всем субъектам, подверженным рискам совершения в отношении них мошеннических действий.

В процессе профилактических бесед целесообразно обеспечивать доведение до категорий, подверженных возможности совершения в отношении них мошеннических действий, объема информации, позволяющей обеспечить невозможность взаимодействия таких категорий граждан с мошенниками, обеспечивать их специальными памятками с разъяснениями положений норм различного законодательства, обеспечивающего снижение рассматриваемых преступлений. Важным является и то, что профилактическая беседа, как универсальный способ профилактического воздействия обеспечивает значительную эффективность, однако в процессе выявления факторов не позволяющих довести до гражданина необходимой информации, следует применять иные механизмы, среди которых профилактическая работа с родственниками таких граждан.

В положениях ст. 27 «Об основах системы профилактики правонарушений в Российской Федерации» закрепляется еще одна форма профилактического воздействия, а именно помощь лицам, пострадавшим от правонарушений или подверженным риску стать таковыми. В соответствии с названной нормой, указанная форма обеспечивает оказание правовой, социальной,

[1] Ковалев С. М. Особенности проведения профилактических мероприятий участковым уполномоченным полиции на административном участке // Международный журнал гуманитарных и естественных наук. 2025. № 1-1 (100). С. 230-233.

психологической, медицинской и иной поддержки таким лицам, осуществляемой в соответствии с законодательством Российской Федерации с их согласия в целях минимизации последствий правонарушений либо снижения риска стать пострадавшими от правонарушений. Однако, ведомственное законодательство МВД РФ не предусматривает реализацию обозначенной формы профилактического воздействия и не регламентирует порядок ее осуществления[1].

Таким образом, деятельность участкового уполномоченного полиции по осуществлению индивидуальной виктимологической профилактики преступлений, связанных с мошенническими действиями, строится на классических формах воздействия, среди которых правовое информирование и просвещение, а также профилактическая беседа. По нашему мнению, в целях повышения ее эффективности названная деятельность требует значительной модернизации.

Так, первым необходимым шагом обозначенной модернизации должно стать обеспечение должного правового механизма наличия в деятельности участковых уполномоченных полиции индивидуальной виктимологической профилактики преступлений. Для этого в структуре ведомственной Инструкции следует предусмотреть специальный раздел, посвященных обозначенным вопросам, который будет в себя включать обязательные категории субъектов, в отношении которых необходима такая профилактика, а также формы профилактического воздействия. Это позволит исключить формальный подход отдельных должностных лиц полиции к обеспечению задачи виктимологической профилактики правонарушений в процессе несения службы на административном участке, что осуществляется путем профилактических обходов, индивидуальной профилактики, работы с обращениями граждан, приемом граждан, а также отчетов перед населением. Отметим, что именно

[1] Терещенко А. И. К вопросу о методах и субъектах виктимологического предупреждения преступности // Социально-экономические процессы современного общества. Материалы II Всероссийской научно-практической конференции. Чебоксары, 2024. С. 147-150.

участковые уполномоченные полиции в силу особой приближенности к населению смогут эффективно реализовывать обозначенную деятельность.

Во-вторых, существует необходимость обеспечения внедрения в деятельность участковых уполномоченных полиции специальных современных механизмов индивидуальной виктимологической профилактики преступлений. Так, по нашему мнению, перспективны разработка и внедрение специальных инструментов на базе социальных сетей, в том числе национального мессенджера «Макс», позволяющих обеспечивать удаленное виктимологическое профилактическое воздействие на отдельные категории граждан, в том числе, пенсионного возраста. Реализация обозначенных задач может осуществляться и через портал оказания Государственных услуг, где следует внедрить специальные разделы работы участкового уполномоченного с населением, предусматривающие удаленный прием граждан, рассмотрение их обращений, а также отчетов перед населением. Внедрение обозначенных механизмов позволит охватить больший круг субъектов, к которым необходимо применять профилактическое воздействие, а также обеспечить реализацию отдельных форм профилактического воздействия посредством использования возможностей искусственного интеллекта.

В качестве вывода по параграфу выпускной квалификационной работы отметим, что важным субъектом обеспечения эффективной индивидуальной виктимологической профилактики совершения мошенничеств с использованием телекоммуникационного и компьютерного оборудования, следует считать участковых уполномоченных полиции. В силу того, что названные подразделения осуществляют несение службы в непосредственном контакте с населением, реализация механизмов такой профилактики может быть особо эффективной. На сегодняшний день указанная работа осуществляется в соответствии с ведомственными указаниями посредством классических форм профилактического воздействия, среди которых правовое информирование и просвещение, а также профилактическая беседа. При обеспечении такой работы, как правило, не берутся в расчет криминологические исследования, где

выявлены особо подверженные риску совершения в отношении них мошеннических действий категории граждан, среди которых граждане пенсионного возраста, несовершеннолетние и иные категории. Кроме того, было выявлено, что в структуре законодательства, определяющего задачи профилактики правонарушений в Российской Федерации, а также в ведомственных нормативных правовых актах, регламентирующих непосредственную деятельность участковых уполномоченных полиции, отсутствуют положения, касающиеся форм и методов осуществления виктимологической профилактики правонарушений. Решением обозначенной недоработки могло бы стать предусмотрение в обозначенной системе законодательства такого направления предупреждения преступлений, а также перечня субъектов, в чьи полномочия оно входит. Кроме того, в части деятельности участковых уполномоченных полиции необходима разработка специальных алгоритмов осуществления виктимологической профилактики преступлений, реализация которых должна осуществляться в зависимости от количественных показателей совершения определенных групп преступлений. Также, в целях повышения эффективности виктимологической деятельности участковых уполномоченных на административном участке, считаем целесообразным внедрять специальные цифровые механизмы взаимодействия с гражданами, которые позволят обеспечивать удаленное профилактическое воздействие, в том числе на потенциальных жертв мошеннических действий. Реализацию таких механизмов необходимо обеспечить на площадках портала оказания Государственных услуг, а также национального мессенджера «Макс».

ЗАКЛЮЧЕНИЕ

В заключении исследования еще раз отметим результаты, полученные в ходе написания выпускной квалификационной работы.

Чтобы достичь целей противодействия конкретной группе преступлений, необходимо понять, каковы сущностные признаки такой группы, что ее обособляет среди других видов преступлений, кроме того, следует изучить состояние такой преступности, а также исследовать виктимологические особенности исследуемой группы преступлений. Нами выявлено, что с проникновением цифрового пространства в разные сферы жизни людей появились и новые способы совершения преступлений, в т.ч. мошенничеств. Так, кибермошенничества представляют такую собой группу хищений, которые направлены на захват персональных данных, имущества или финансовых средств потерпевшего в цифровом пространстве с помощью киберресурсов, а также сопряжены с обманом или злоупотреблением доверием, т.е. введением в заблуждение жертвы. Выявлено, что за последние пять лет наблюдений с 2021 по 2025 года указанные преступления демонстрируют тенденцию к росту. В этой связи, учеными и практическими работниками правоохранительных органов, а также заинтересованными финансовыми и сотовыми организациями, разрабатываются специальные меры по противодействию указанной группе преступлений, в т.ч. в рамках виктимологической оставляющей. Для планирования мероприятий, снижающих риски кибервиктимизации населения, нами выявлены типичные действия, которые совершают кибермошенники в отношении граждан, в совокупности с отдельными социально-экономическими элементами личности жертвы от кибемошенничества на основе анализа выборки уголовных дел. Выявлено, что самыми виктимными группами населения, в отношении которых совершаются кибермошенничества являются пенсионеры и учащиеся школ. Нами также разработаны типичные портреты жертв от киберпреступлений.

Кибервиктимизации представляет собой процесс становления гражданина

жертвой от киберпреступлений, в т.ч. от кибермошенничеств. Указанный процесс детерминируется различными причинами и условиями. Анализ научной литературы и выборки уголовных дел позволил выявить две группы детерминант виктимности от кибермошенничества: общая группа факторов и группа специальных факторов, связанных с кибервиктимизацией конкретных групп населения. Кроме того, нами проанализирован комплекс триггеров, разработанный отечественными учеными по кибервиктимизации граждан. Таким образом, нами выявлено, что необходимо на основе указанных детерминант разрабатывать как меры общего предупреждения, так и индивидуальной профилактики. Особенностью такого предупреждения должна быть работа с выявленными нами отдельными группами граждан, подверженными кибервиктимизации – пожилые и несовершеннолетние граждане.

Обеспечение минимизации совершения мошенничеств с использованием телекоммуникационного и компьютерного оборудования может иметь значительный эффект в случае организации эффективного виктимологического предупреждения. Его реализации осуществляется как на общем уровне, так и на индивидуальном. Так, общее виктимологическое предупреждения обозначенных преступлений обеспечивается четырьмя группами мер, среди которых правовые, экономические, социально-психологические, а также организационные. В их реализации задействованы различные субъекты, среди которых государственные органы, коммерческие организации, общественные учреждения и иные. Применение всех обозначенных мер должно строится на эффективной правовой основе. Так, в структуре правовых мер следует продолжать работу по формированию законодательных механизмов, обеспечивающих минимизацию обозначенных деяний. В обозначенной работе должны принимать участие государственные органы, а также заинтересованные субъекты финансовых и телекоммуникационных организаций. Со стороны законодателя необходима проработка и закрепление механизма возможности использования специальных программных средств, в том числе, основанных на искусственном интеллекте,

которые помогут обеспечить предупреждение рассматриваемых преступлений, а в отдельных случаях полностью исключат их совершение, в том числе путем определенных ограничений финансового и иного характера. В структуре реализации экономических мер предупреждения следует обеспечить продолжение комплексного решения общих социально-экономических проблем, связанных с уровнем жизни населения, формированием качественной трудовой инфраструктуры, в том числе для отдельных категорий граждан. Кроме того, считаем целесообразным обеспечить более оперативное внедрение в оборот цифрового рубля. Обеспечение социально-психологических мер предупреждения должно строиться на необходимости полномасштабного использования всей цифровой среды для обучения граждан, их информирования, повышения их финансовой грамотности, включая средства массовой информации, печатные издания, сеть Интернет. Нельзя забывать и про организационную составляющую, где основной упор необходимо делать на разработку специальных информационно-телекоммуникационных технических решений, а также на достижение системности и комплексности использования сил и средств всех субъектов предупреждения правонарушений, достижения их должного взаимодействия.

Важным субъектом обеспечения эффективной индивидуальной виктимологической профилактики совершения мошенничеств с использованием телекоммуникационного и компьютерного оборудования, следует считать участковых уполномоченных полиции. В силу того, что названные подразделения осуществляют несение службы в непосредственном контакте с население, реализация механизмов такой профилактики может быть особо эффективной. На сегодняшний день указанная работа осуществляется в соответствии с ведомственными указаниями посредством классических форм профилактического воздействия, среди которых правовое информирование и просвещение, а также профилактическая беседа. При обеспечении такой работы, как правило, не берутся в расчет криминологические исследования, где выявлены особо подверженные риску совершения в отношении них

мошеннических действий категории граждан, среди которых граждане пенсионного возраста, несовершеннолетние и иные категории. Кроме того, было выявлено, что в структуре законодательства, определяющего задачи профилактики правонарушений в Российской Федерации, а также в ведомственных нормативных правовых актов, регламентирующих непосредственную деятельность участковых уполномоченных полиции, отсутствуют положения, касающиеся форм и методов осуществления виктимологической профилактики правонарушений. Решением обозначенной недоработки могло бы стать предусмотренные в обозначенной системе законодательства обозначенного направления предупреждения преступлений, а также перечня субъектов, в чьи полномочия оно входит. Кроме того, в части деятельности участковых уполномоченных полиции, необходимо предусмотренные специальных алгоритмов осуществления виктимологической профилактики преступлений, реализация которых должна осуществляться в зависимости от количественных показателей совершения определенных групп преступлений. Также, в целях повышения эффективности виктимологической деятельности участковых уполномоченных на административном участке, считаем целесообразным внедрять специальные цифровые механизмы взаимодействия с гражданами, которые позволят обеспечивать удаленное профилактическое воздействие, в том числе на потенциальных жертв мошеннических действий. Реализацию таких механизмов необходимо обеспечить на площадках портала оказания Государственных услуг, а также национального мессенджера «Макс».

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL:// http://www.pravo.gov.ru (дата обращения: 11.02.2026).

2. Уголовный кодекс Российской Федерации: Федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

3. Об основах системы профилактики правонарушений в Российской Федерации: Федер. закон Рос. Федерации от 23 июня 2016 г. № 182-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 10 июня 2016 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 15 июня 2016 г. // Собр. законодательства Рос. Федерации. – 2016. – № 26 (ч. 1), ст. 3851.

4. О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генпрокуратуры России № 503/11, МВД России № 1 от 28 июля 2025 года. [Электронный ресурс]. URL:// http://www.pravo.gov.ru (дата обращения: 11.02.2026).

5. О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности: приказ МВД России от 29 марта 2019 № 205 // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 11.02.2026).

II. Учебная, научная литература и иные материалы

1. Акжигитова А. Р., Егорова А. Н. Мошенничество как угроза экономической безопасности // Молодежь и наука: шаг к успеху. Сборник научных статей 7-й Всероссийской научной конференции перспективных

разработок молодых ученых. Курск, 2024. С. 10-13.

2. Андрианова Е.В. Социальный портрет жертв кибермошенничества // Экономическая безопасность страны, регионов, организаций различных видов деятельности : Материалы Четвертого Всероссийского форума в Тюмени по экономической безопасности, Тюмень, 19–22 апреля 2023 года. Тюмень: ТюмГУ-Press, 2023. С. 265-269.

3. Веряскин И. А. Факторы криминальной виктимизации несовершеннолетних // Общественная безопасность, законность и правопорядок в III тысячелетии. 2022. № 8-1. С. 23-28.

4. Габова О. С., Лукичев Ю. В. О роли участкового уполномоченного полиции в проведении общей профилактики преступлений и административных правонарушений // Административно-правовое регулирование охраны общественного порядка и обеспечения общественной безопасности: проблемы и пути их решения. Материалы ежегодной межвузовской научно-практической конференции . Санкт-Петербург, 2024. С. 52-56.

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

6. Гришко Н. А. Защита потенциальных жертв киберпреступлений: виктимологический подход / Н. А. Гришко // Вестник Университета имени О.Е. Кутафина (МГЮА). 2025. № 5(129). С. 234-243.

7. Жмуров Д. В. Кибервиктимизация: понятие и характерные свойства // Международный научный вестник. 2025. № 3. С. 44-48.

8. Жмуров Д. В. Кибервиктимология / Д. В. Жмуров. Москва : Издательство «Юрлитинформ», 2023. 296 с.

9. Жмуров Д. В. Техногенные предпосылки кибервиктимизации // Виктимология. 2023. Т. 10, № 2. С. 138-146.

10. Изингер А. В. Реализация отдельных форм профилактического воздействия в деятельности органов внутренних дел Российской Федерации // Вестник Тюменского института повышения квалификации сотрудников МВД

России. 2024. № 1 (22). С. 11-17.

11. Ильин И. С., Рязанова Е. Н. Виктимологическое предупреждение краж и мошенничеств, совершаемых бесконтактным способом // Закон и право. 2024. № 12. С. 208-214.

12. Кабанов П.А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии:краткий статистический анализ показателей криминальной виктимности2021-2022 гг // Виктимология. 2023. Т. 10, № 1. С. 17-28.

13. Ковалев С. М. Особенности проведения профилактических мероприятий участковым уполномоченным полиции на административном участке // Международный журнал гуманитарных и естественных наук. 2025. № 1-1 (100). С. 230-233.

14. Коленова И. И. Виктимологическая профилактика кибермошенничеств // Объект преступления и уголовно правовой охраны: историко-правовой, аксиологический, методологический и формально-юридический аспекты : Материалы международной научно-практической конференции, Екатеринбург, 03 марта 2023 года. Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2023. С. 363-371.

15. Курумбаева А. Б. Общесоциальные меры предупреждения мошенничества, совершаемого с использованием информационных систем // Уголовно-правовое обеспечение информационной безопасности человечества. Материалы международной научно-практической конференции. Москва, 2025. С. 48-57.

16. Лащёнов М. С., Лащёнов П. М. Роль информационных технологий в борьбе с кибермошенничеством // Информатизация и информационная безопасность правоохранительных органов. Сборник трудов Международной научно-практической конференции. Москва, 2025. С. 214-219.

17. Макаримова Н.Т. Изучение проблемы виктимизации в юношеском возрасте и её последствий для личности // Лучшая исследовательская работа 2022. Сборник статей IV Международного научно-исследовательского конкурса.

Петрозаводск, 2022. С. 249-261.

18. Никульченкова Е. В. Кибераддикции как детерминанты виктимности жертв кибермошенничества // Психопедагогика в правоохранительных органах. 2025. Т. 30, № 3(102). С. 306-310.

19. Павленко О. С. Кибермошенничество как дистанционное преступление: особенности совершения и перспективные меры профилактики / О. С. Павленко // Пермский период : Сборник материалов XI Международного научно-спортивного фестиваля курсантов и студентов образовательных организаций, посвященного 145-летию уголовно-исполнительной системы Российской Федерации, Пермь, 20–24 мая 2024 года. Пермь: Пермский институт Федеральной службы исполнения наказаний, 2024. С. 374-378.

20. Палий Е. С. Виктимологическая характеристика лиц пенсионного возраста: постановка проблемы // Судебная экспертиза и исследования. 2025. № 1. С. 115-123.

21. Пономарева О. М. Правовое информирование как форма профилактического воздействия // Сборник материалов научно-представительских мероприятий Барнаульского юридического института МВД России. Сборник статей конференций. Барнаул, 2025. С. 141-144.

22. Редькина Е. А. Профилактика преступлений: учебное пособие. Казань, 2024. С. 13.

23. Семеняченко А. А. Кибермошенничество и кибербезопасность: как защитить пенсионеров и уязвимые слои общества // Юный ученый. 2025. № 11(96). С. 60-63.

24. Сорокун Н. С., Рудов М. В. Современное мошенничество и его предупреждение: учебное пособие. Ростов-на-Дону, 2024. С. 14.

25. Сырьев Б. О., Бурханова С. Д. Предупреждение кибермошенничества в социальных сетях // Юность и Знания - Гарантия Успеха - 2024. сборник научных статей 11-й Международной молодежной научной конференции : в 3 т.. Курск, 2024. С. 171-173.

26. Терещенко А. И. К вопросу о методах и субъектах виктимологического

предупреждения преступности // Социально-экономические процессы современного общества. Материалы II Всероссийской научно-практической конференции. Чебоксары, 2024. С. 147-150.

27. Шашкин В. К. Виды и меры предупреждения киберпреступности // Вестник науки. 2025. Т. 3. № 5 (86). С. 725-731.

III. Эмпирические материалы

1. Аналитическая таблица за 2021-2025 года по Форме SPS294 в сфере ИТТ Перечень 25. Архив ИЦ МВД России по Республике Башкортостан.

2. Доклад МВД России о состоянии преступности за 2021-2025 года: [Электронный ресурс]: Интернет-портал МВД России. URL://http://мвд.рф (дата обращения: 11.02.2026).

3. Материалы уголовного дела № 125018000010000** от 12.*.2025 по ч. 2 ст. 159 УК РФ, возбужденное ОМВД России по Белебеевскому району.

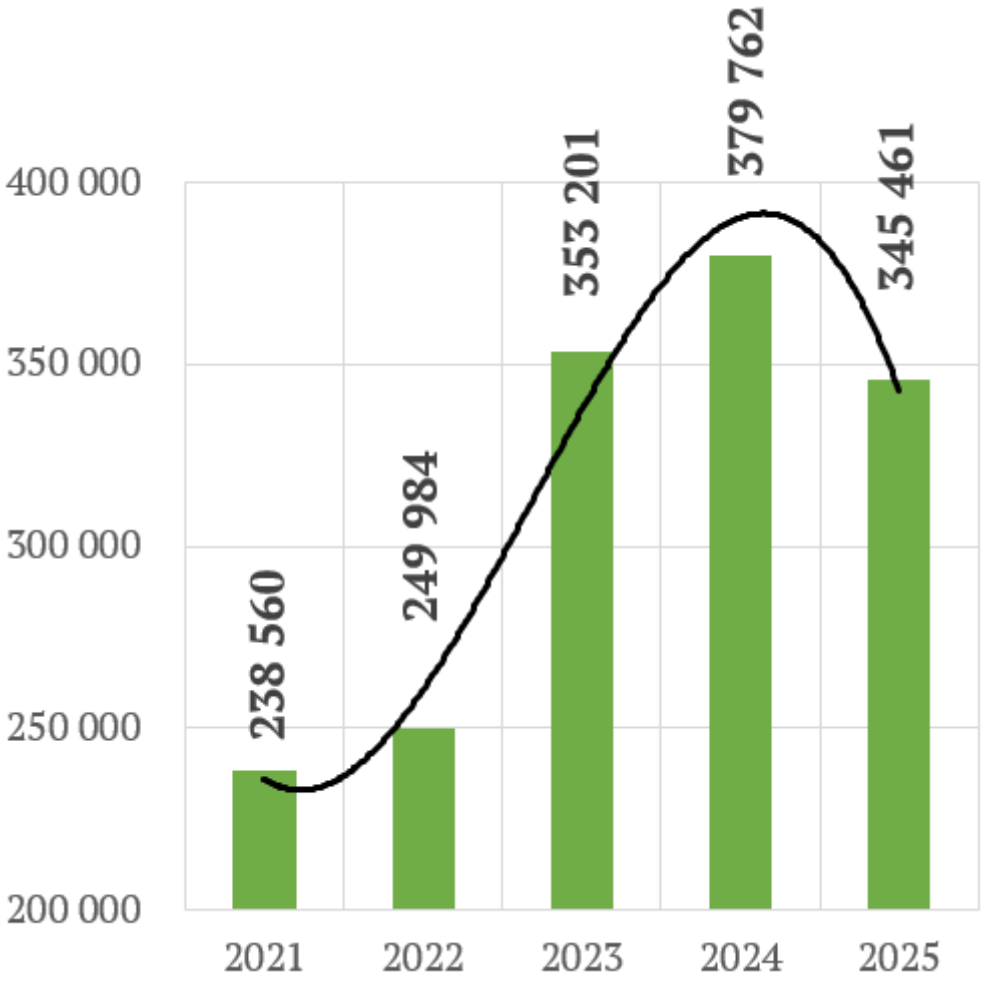
Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну.

Т.Р. Яхин

ПРИЛОЖЕНИЕ 1

Общее количество кибермошенничеств, совершенных

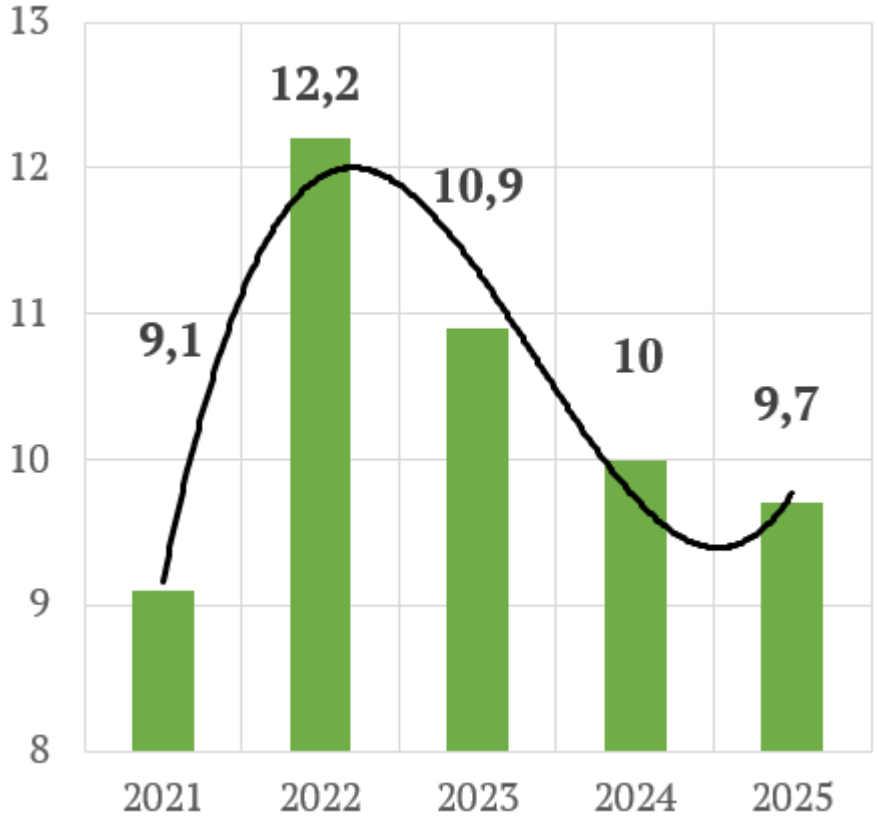
в России за период с 2021 по 2025 года



ПРИЛОЖЕНИЕ 2

Коэффициент расследования кибермошенничеств

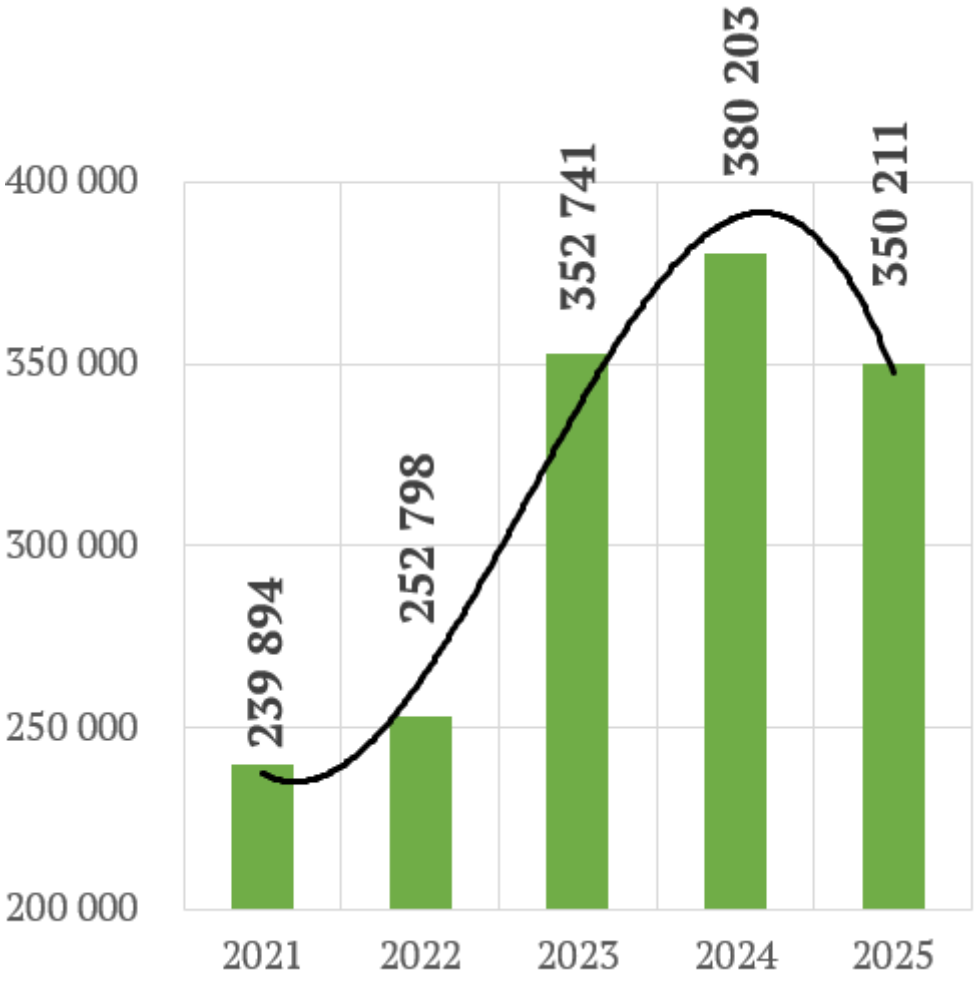
в России с 2021 по 2025 год, %



ПРИЛОЖЕНИЕ 3

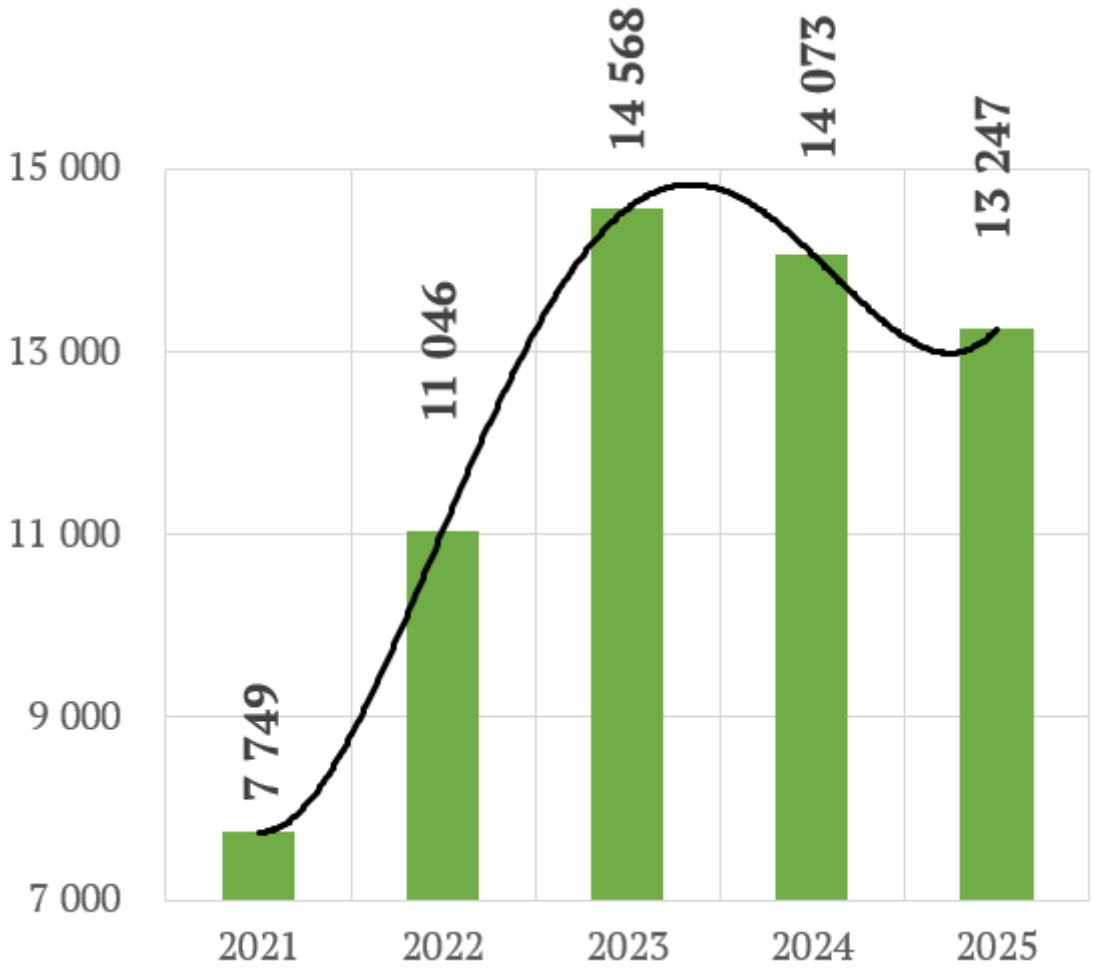
Количество жертв от кибермошенничества

в России за период с 2021 по 2025 год



ПРИЛОЖЕНИЕ 4

Количество выявленных кибермошенников
в Российской Федерации за период с 2021 по 2025 год



ПРИЛОЖЕНИЕ 5

Структура способов совершения кибермошенничества
в Российской Федерации за период с 2021 по 2025 год

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну Яхин Т.Р.