ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И ПРЕДУПРЕЖДЕНИЯ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ И ЛИЦ ПОЖИЛОГО ВОЗРАСТА С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Учебное пособие

Воронеж
2025

УДК 343.9
ББК 67.99
О-75

Коллектив авторов:
И. А. Кравцов – кандидат юридических наук, доцент;
А. Н. Белоусова – кандидат юридических наук, доцент;
А. В. Польшиков – кандидат юридических наук, доцент;
В. С. Прохонов;
С. Г. Родин;
А. А. Кулешов.

Рецензенты:
М. М. Буслов – начальник отделения НЦБ Интерпола ГУ МВД России по Воронежской области, кандидат юридических наук, доцент;
Е. В. Маликовский – начальник ОСО УР УМВД России по г. Воронежу.

Особенности квалификации и предупреждения мошенничеств, совершенных в отношении несовершеннолетних и лиц пожилого возраста с использованием сети Интернет : учебное пособие / И. А. Кравцов, А. Н. Белоусова, А. В. Польшиков [и др.]. – Воронеж : Воронежский институт МВД России, 2025. – 42 с.
О-75
ISBN 978-5-00229-215-8.

Учебное пособие содержит результаты исследования особенностей квалификации и предупреждения мошенничеств, совершенных в отношении несовершеннолетних и лиц пожилого возраста с использованием сети Интернет. В работе раскрываются понятие, сущность, уголовно-правовая характеристика и особенности квалификации мошенничеств, совершенных в отношении несовершеннолетних и лиц пожилого возраста с использованием сети Интернет, и их отграничение от смежных составов преступлений, а также состояние, основные тенденции и детерминанты совершения таких преступлений. Предложены рекомендации по повышению эффективности деятельности в этой сфере с учетом полученных данных.

Пособие предназначено для сотрудников территориальных органов Министерства внутренних дел Российской Федерации, курсантов, слушателей, студентов, адъюнктов, аспирантов и преподавателей образовательных организаций юридического профиля.

О-42-47(I)-25 УДК 343.9
ББК 67.99

ISBN 978-5-00229-215-8

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире исследование проблем профилактики мошенничеств, совершаемых в отношении несовершеннолетних и пожилых людей с использованием сети Интернет, представляет собой актуальную и социально значимую проблему. Прежде всего стоит отметить, что с развитием информационно-коммуникационных технологий значительно возросло количество преступлений, совершаемых с использованием сети Интернет. Одной из наиболее уязвимых категорий населения в этом контексте становятся несовершеннолетние и пожилые люди, которые обладают рядом специфических особенностей, влияющих на степень их подверженности мошенничеству. Несовершеннолетние зачастую отличаются недостаточным уровнем критического мышления и доверчивостью, что обусловлено их психофизиологическим развитием, а также недостаточным опытом распознавания угроз в киберпространстве. С возрастанием числа пользователей Интернета среди детей и подростков их поведение становится потенциальной мишенью для злоумышленников, которые используют различные приёмы для манипулирования и обмана. Особую опасность представляют социальные сети, мессенджеры и игровые платформы, где несовершеннолетние вступают в контакт с незнакомыми людьми, что повышает вероятность их вовлечения в мошеннические схемы.

Пожилые люди также подвержены риску стать жертвами мошенничества в интернете. Это связано с тем, что многие из них не обладают достаточными навыками работы с современными цифровыми технологиями и не всегда могут адекватно оценивать риски, возникающие при использовании онлайн-сервисов. Кроме того, доверчивость, наивность и социальная изоляция, характерные для некоторых пожилых людей, делают их лёгкой мишенью для мошенников, использующих различные виды обмана: поддельные

сайты, фальшивые предложения о помощи и ложные сообщения от имени государственных служб.

С учетом вышеизложенного становится очевидной необходимость всестороннего изучения проблем профилактики интернет-мошенничества в отношении этих социально уязвимых категорий граждан. Данная задача требует разработки эффективных методов предупреждения, а также повышения уровня цифровой грамотности среди несовершеннолетних и пожилых людей. Научные исследования в этой области направлены на выявление психологических, социальных и правовых факторов, способствующих успешной профилактике интернет-мошенничества. Таким образом, исследование вопросов профилактики кибермошенничества, направленного на несовершеннолетних и пожилых граждан, является крайне актуальным и требует всестороннего анализа.

В современных условиях вышесказанное предопределяет целесообразность разработки соответствующего учебного пособия по результатам комплексного исследования, проведенного кафедрой уголовного права и криминологии Воронежского института МВД России по указанной тематике.

1. Понятие, уголовно-правовая характеристика и особенности квалификации мошенничеств, совершенных в отношении несовершеннолетних и лиц пожилого возраста с использованием сети Интернет

В условиях активного развития информационно-коммуникационных технологий и повышения уровня их проникновения в повседневную жизнь всё большее значение приобретают вопросы, связанные с защитой уязвимых групп населения от мошенничества, совершаемого с использованием сети Интернет. Особенно это касается несовершеннолетних и пожилых людей, которые в силу различных причин оказываются более восприимчивыми к киберугрозам. Исследования в области юридической и криминологической науки демонстрируют, что понятие «мошенничество» допускает различные интерпретации, и авторы предлагают различные подходы к определению данного явления в отношении уязвимых категорий граждан.

Согласно традиционному определению, мошенничество представляет собой преступление, при котором лицо путем обмана или злоупотребления доверием завладевает имуществом другого лица либо правом на него. Это определение закреплено в Уголовном кодексе Российской Федерации (ст. 159 УК РФ), где мошенничество рассматривается как преступление против собственности. Однако с ростом использования сети Интернет и появлением новых форм мошеннических схем ученые начали предлагать расширенные и дифференцированные подходы к этому понятию, выделяя различные его аспекты, особенно когда речь идет о преступлениях в отношении несовершеннолетних и пожилых граждан.

В частности, А. В. Сычева отмечает, что традиционные признаки мошенничества, такие как обман и злоупотребление доверием, приобретают новые формы, когда речь идет о мошенничестве в сети Интернет. Исследователь подчеркивает, что обман в виртуальной среде часто носит характер информационного воздействия, направленного на использование низкого

уровня цифровой грамотности жертвы[1].

В соответствии с учением о составе преступления объект мошенничества, совершаемого в отношении несовершеннолетних и лиц пожилого возраста посредством сети Интернет, обладает рядом признаков, позволяющих определить его как значимый элемент состава преступления, требующий тщательного анализа. Объект преступления представляет собой общественные отношения, охраняемые уголовным законом, на которые направлено преступное деяние, что обуславливает необходимость его классификации на несколько видов.

Первым видом объекта является общий объект, который охватывает совокупность общественных отношений, охраняемых уголовным законом. В данном случае мошенничества, направленные на несовершеннолетних и лиц пожилого возраста, затрагивают правопорядок и общественную безопасность в целом, нарушая правомерность владения и распоряжения имуществом. Общий объект включает все общественные отношения, которые нуждаются в уголовно-правовой защите от противоправных посягательств, угрожающих их стабильности.

Родовым объектом рассматриваемых видов мошенничества выступают права и свободы личности, поскольку преступное воздействие затрагивает как имущественные, так и личные интересы потерпевшего. Мошенничества, совершаемые в отношении несовершеннолетних и пожилых граждан, нарушают не только их имущественные права, но и безопасность, право на информационную защиту и доверие в цифровой среде. Этот вид объекта особенно значим, потому что данная категория граждан очень уязвима к манипулятивному воздействию и обману в интернете.

Видовой объект мошенничеств – это право собственности как основа

---

[1] Сычева А. В. Некоторые вопросы криминалистической характеристики «дистанционных» мошенничеств, совершенных в отношении пожилых людей // Вестник Волгоградской академии МВД России. 2022. № 1 (60). С. 136.

имущественных интересов, подлежащих уголовно-правовой защите. Преступные действия, направленные на незаконное завладение имуществом пожилых лиц и несовершеннолетних, посягают на их материальное благосостояние и подрывают общественные отношения, связанные с правомерным использованием собственности. Видовой объект предполагает посягательство на имущественные права личности, что требует повышенного внимания к охране и защите права собственности, особенно в отношении уязвимых категорий граждан в цифровом пространстве.

Непосредственным объектом мошенничества является конкретное имущество или имущественные права, на которые направлено преступное деяние. В цифровой среде это приводит к искажению восприятия реальной картины правомерности действий у жертвы, что позволяет преступникам достигать своих целей. Непосредственный объект включает конкретные имущественные права и ценности, которых жертва лишается вследствие мошенничества, что особенно актуально для уязвимых групп населения, испытывающих недостаток цифровой грамотности и защиты в Интернете.

Предмет мошенничества, совершаемого в отношении несовершеннолетних и лиц пожилого возраста посредством сети Интернет, представляет собой имущество или права на имущество, которые приобретают особое значение в цифровую эпоху. Мошенничество в интернете направлено на завладение материальными или нематериальными ценностями, при этом цифровые активы и учетные записи играют все более важную роль в структуре предмета преступления. Развитие цифровых технологий и распространение онлайн-сервисов привели к тому, что под предметом преступления стали пониматься не только традиционные формы имущества (например, денежные средства), но и такие специфические объекты, как цифровые активы и аккаунты, которые имеют существенную имущественную значимость.

Имущество как предмет преступления в данном контексте включает цифровые валюты, электронные средства на банковских счетах,

виртуальные товары, а также денежные средства, к которым преступники получают доступ обманным путем. Пожилые лица особенно подвержены кибермошенничествам, связанным с поддельными банковскими услугами, фальшивыми инвестиционными предложениями и ложными заявлениями о необходимости финансовой помощи. Дети и подростки, в свою очередь, нередко подвергаются обману в игровых сервисах или социальных сетях, где их могут побудить к покупке ненастоящих виртуальных товаров или подписок. При этом особое место в структуре предмета мошенничества занимают цифровые активы – это нематериальные блага, существующие исключительно в цифровой форме и обладающие значительной стоимостью. К цифровым активам относятся, например, виртуальные валюты (криптовалюты), внутриигровая валюта и предметы, приобретаемые на игровых платформах, а также различные электронные сертификаты и баллы лояльности, которые могут использоваться как товар с денежной стоимостью. Виртуальные активы особенно привлекательны для несовершеннолетних, которые активно участвуют в онлайн-играх и нередко вкладывают значительные суммы в свои игровые учетные записи.

Мошенничество, совершаемое в отношении несовершеннолетних и лиц пожилого возраста посредством сети Интернет, имеет специфическую объективную сторону, характеризующуюся рядом признаков, определяющих общественную опасность и механизм преступного воздействия.

Общественно опасное деяние при мошенничестве в отношении несовершеннолетних и пожилых граждан в интернете заключается в совершении действий, направленных на неправомерное завладение имуществом или имущественными правами жертвы путем обмана или злоупотребления доверием. Деяние приобретает форму активного поведения, выражающегося в использовании различных методов манипуляции информацией, которые воздействуют на сознание и поведение жертвы. Особенность общественно опасного деяния в данном случае заключается в том, что оно

осуществляется посредством цифровых каналов связи, таких как социальные сети, мессенджеры, электронная почта и фальшивые интернет-страницы, что позволяет преступникам влиять на жертву на значительном удалении. Для несовершеннолетних характерно воздействие через игровые платформы и соцсети, где преступники имитируют дружеские или коммерческие взаимодействия, чтобы завладеть ресурсами или информацией. Пожилые люди становятся жертвами через поддельные банковские уведомления, ложные консультации и фальшивые предложения помощи – мошенники используют их доверчивость.

Общественно опасные последствия включают имущественный ущерб, нанесенный потерпевшим, а также психологические травмы, которые могут нанести значительный вред жертве. Несовершеннолетние и пожилые лица нередко сталкиваются с материальными потерями в форме прямого лишения денежных средств, доступа к цифровым активам и учетным записям, которые имеют для них реальную или символическую ценность. Помимо имущественного ущерба, значительными последствиями становятся снижение доверия к цифровым технологиям и платформам, а также травмирующее воздействие на психику, особенно у несовершеннолетних, для которых потеря цифровых активов или аккаунтов может стать причиной психологического стресса. Для пожилых людей последствия могут быть выражены в виде повышенной тревожности и нарушения безопасности личного пространства в интернете, что осложняет их дальнейшее взаимодействие с цифровыми сервисами.

Способ совершения преступления в данной категории мошенничества определяется особенностями цифровой среды и представлен традиционными для мошенничества видами – обманом и злоупотреблением доверием. Обман как способ совершения мошенничества представляет собой преднамеренное введение потерпевшего в заблуждение относительно истинных намерений преступника, условий взаимодействия или правомерности

действий. В цифровой среде обман может принимать разнообразные формы: от поддельных интернет-сайтов и фальшивых аккаунтов до мошеннических сообщений, имитирующих официальные уведомления от банков или социальных служб. Для несовершеннолетних обманом являются предложения покупки виртуальных товаров, бонусы в играх или скидки, которые якобы предоставляются, чтобы получить преимущество в виртуальной среде. Пожилые граждане становятся жертвами обмана через фальшивые уведомления о финансовой помощи или инвестициях, а также через сообщения, имитирующие запросы от знакомых или государственных органов, побуждающие раскрыть личные данные или перевести денежные средства. Цифровая анонимность позволяет преступникам использовать сложные схемы обмана, часто с использованием социальной инженерии, благодаря чему жертвы, не подозревая о преступных намерениях, выполняют действия, ведущие к утрате имущества.

Злоупотребление доверием в мошенничестве основывается на преднамеренном использовании доверительных отношений с целью завладения имуществом жертвы. В цифровом пространстве это может выражаться в манипулятивных приемах, создающих иллюзию безопасности и правомерности действий преступника. Несовершеннолетние нередко становятся жертвами такого вида злоупотребления в социальных сетях или мессенджерах, где преступники, выступая под видом друзей или представителей популярных брендов, убеждают их совершить перевод денежных средств или предоставить доступ к аккаунтам. Пожилые люди, ввиду возрастных особенностей и повышенной доверчивости, могут поддаваться воздействию мнимых «советников» или «помощников», представляющихся сотрудниками банков, социальных служб или родственниками, что заставляет их раскрывать конфиденциальную информацию или передавать средства преступникам. Использование доверия позволяет преступникам обходить защитные механизмы и получать доступ к имуществу жертвы без необходимости

непосредственного контакта.

Субъектом рассматриваемого преступления является физическое, вменяемое лицо, достигшее возраста уголовной ответственности.

Для привлечения к уголовной ответственности за мошенничество, согласно ст. 20 УК РФ, субъект должен достигнуть возраста 16 лет. Это возраст, с которого лицо признается способным осознавать противоправный характер своих действий, связанных с обманом или злоупотреблением доверием, направленных на завладение чужим имуществом или правами на него. Кроме того, в соответствии с общими требованиями уголовного права, субъект мошенничества должен быть вменяемым, то есть способным осознавать общественную опасность и противоправный характер своих действий и руководить ими. Вменяемость предполагает, что лицо обладает достаточной способностью к пониманию последствий своих действий и их значения в социальном и правовом контексте. Наличие психического расстройства, исключающего вменяемость, делает лицо не подлежащим уголовной ответственности.

Субъективная сторона мошенничества характеризуется признаками, отражающими внутреннее отношение субъекта к совершенному деянию. Так, мошенничество может быть совершено только с прямым умыслом. Это означает, что субъект осознает общественно опасный и противоправный характер своих действий, направленных на завладение чужим имуществом или правом на него путем обмана или злоупотребления доверием, и желает наступления таких последствий. Прямой умысел проявляется в том, что преступник сознательно использует обман или манипулирует доверием жертвы для достижения своей корыстной цели. Данный умысел исключает возможность неосторожной или косвенной вины в данном преступлении, так как преступник целенаправленно и планомерно воздействует на жертву, чтобы получить материальную выгоду.

Субъективная сторона мошенничества обязательно включает цель –

незаконное завладение чужим имуществом или правом на него. Цель указывает на то, что субъект изначально направляет свои действия на достижение результата, который обеспечит ему имущественную выгоду. Эта цель также определяет специфику действий преступника: он обманывает или злоупотребляет доверием с намерением получения конкретного имущественного объекта, будь то деньги, ценности, имущество, услуги или иные материальные выгоды.

Разграничение мошенничеств, совершаемых в отношении несовершеннолетних и лиц пожилого возраста посредством сети Интернет, от смежных составов преступлений является актуальной задачей для правоприменительной практики. Данные преступления направлены на уязвимые группы населения и связаны с использованием цифровых технологий, что добавляет специфики их квалификации и требует особого внимания к методам воздействия, намерению преступника и особенностям преступного результата.

Разграничение мошенничества и кражи (ст. 158 УК РФ) определяется способом получения имущества. При кибермошенничестве преступник, как правило, воздействует на восприятие потерпевшего, вводя его в заблуждение или злоупотребляя доверием, благодаря чему жертва добровольно передает имущество. Кража же предполагает тайное изъятие имущества без согласия потерпевшего и без его участия, что исключает использование обмана. Например, в случае мошенничества, направленного на пожилых людей, преступник может создать фальшивый веб-сайт или поддельный профиль в социальных сетях и под видом помощи попросить перевести денежные средства якобы для обеспечения безопасности. Пожилой человек, введенный в заблуждение, добровольно передает деньги, полагая, что действует в своих интересах, что соответствует признакам мошенничества по ст. 159 УК РФ. В отличие от этого кража не требует обмана: например, если преступник получает доступ к устройству жертвы и переводит средства без

ее ведома, то данное деяние квалифицируется как кража.

Сложность возникает и при разграничении мошенничества и вымогательства (ст. 163 УК РФ), которое включает угрозы применения насилия, уничтожения имущества или разглашения позорящих сведений с целью принудить потерпевшего к передаче имущества. Мошенничество, напротив, не включает явных угроз, а предполагает воздействие на потерпевшего с помощью обмана или злоупотребления доверием. При интернет-мошенничестве преступники могут использовать завуалированные угрозы, например, угрожая заблокировать аккаунт жертвы или распространить ложные сведения. Однако если потерпевший поддается на обман и передает имущество добровольно, это квалифицируется как мошенничество. В отличие от этого при вымогательстве лицо передает имущество, испытывая страх перед угрозой. Таким образом, ключевым признаком вымогательства является характер воздействия: если потерпевший действует под воздействием страха, то деяние следует квалифицировать по ст. 163 УК РФ. Вместе с тем разграничение мошенничества и присвоения или растраты (ст. 160 УК РФ) также имеет принципиальное значение для правоприменительной практики. Присвоение и растрата касаются случаев, когда преступник изначально получает доступ к имуществу на законных основаниях, но затем обращает его в свою пользу вопреки воле собственника. В мошенничестве же имущество или права на него изначально передаются преступнику под влиянием обмана или злоупотребления доверием, то есть незаконно. Например, если пожилой человек добровольно передает деньги под предлогом финансовой помощи, которую предложил якобы представитель банка, то это является мошенничеством. В противоположность этому, если преступник получает имущество на законных основаниях, а затем использует его вопреки воле владельца, то действия квалифицируются по ст. 160 УК РФ как присвоение или растрата.

Кроме того, отграничение мошенничества, совершенного в

отношении уязвимых категорий граждан посредством сети Интернет, необходимо проводить и от преступлений в сфере компьютерной информации, предусмотренных ст.ст. 272–274 УК РФ. Несанкционированный доступ к компьютерной информации, если он осуществляется с целью хищения, квалифицируется по совокупности преступлений, включая ст. 159 УК РФ. Например, если преступник взламывает аккаунт пожилого человека и переводит его средства на свой счет, то это деяние квалифицируется как несанкционированный доступ в совокупности с мошенничеством.

Таким образом, в условиях активного развития интернет-технологий защита уязвимых групп населения, таких как несовершеннолетние и пожилые люди, от кибермошенничества становится приоритетной задачей. Исследование показывает, что противодействие современным мошенникам требует расширенного понимания состава преступления, предусмотренного ст. 159 УК РФ, особенно в связи с появлением цифровых активов и виртуальных ценностей, которые все чаще становятся предметом преступлений. В цифровой среде традиционные способы мошенничества, такие как обман и злоупотребление доверием, приобретают новые формы, например, использование фальшивых аккаунтов и фальсифицированных уведомлений, что требует особого подхода при квалификации преступлений. Отграничение мошенничеств от смежных составов является сложной, но выполнимой задачей для сотрудников правоохранительных органов и основано на учете особенностей взаимодействия преступников с жертвами.

2. Состояние и тенденции совершения в России мошенничеств в отношении несовершеннолетних и лиц пожилого возраста с использованием сети Интернет

Мошеннические действия ежегодно наносят огромный ущерб гражданам, обществу и государству. Так, согласно данным, приведенным заместителем начальника следственного департамента МВД России Данилом Филипповым в рамках Восточного экономического форума, в период с 2022 года по август 2024 года мошенниками было похищено и выведено за границу более 350 миллиардов рублей, и за это время было совершено более 1,5 миллиона киберпреступлений[1].

Обратимся более подробно к статистике совершения мошенничеств в Российской Федерации. В данном исследовании в качестве источников статистической информации нами были использованы материалы Министерства внутренних дел Российской Федерации о состоянии преступности в 2023[2], 2022[3], 2021[4], 2020[5] и 2019[6] годах.

Так, в 2023 году совершено 443 708 мошенничеств. В структуре преступности мошенничества составляют 22,3 % от общего количества преступлений в России, уступая только кражам (30 %) (Рис. 1). Важно отметить,

---

[1] Кибермошенники вывели за границу более 350 млрд рублей за три года // Информационное агентство ТАСС [Электронный ресурс]. URL: https://tass.ru/proisshestviya/21789361 (дата обращения: 21.10.2024).

[2] Состояние преступности в Российской Федерации за январь-декабрь 2023 года // официальный сайт МВД России [Электронный ресурс]. URL: https://media.mvd.ru/files/application/5095078 (дата обращения: 21.10.2024).

[3] Состояние преступности в Российской Федерации за январь-декабрь 2022 года // официальный сайт МВД России [Электронный ресурс]. URL: https://media.mvd.ru/files/application/5130663 (дата обращения: 21.10.2024).

[4] Состояние преступности в Российской Федерации за январь-декабрь 2021 года // официальный сайт МВД России [Электронный ресурс]. URL: https://media.mvd.ru/files/application/2315310 (дата обращения: 21.10.2024).

[5] Состояние преступности в Российской Федерации за январь-декабрь 2020 года // официальный сайт МВД России [Электронный ресурс]. URL: https://media.mvd.ru/files/application/2041459 (дата обращения: 21.10.2024).

[6] Состояние преступности в Российской Федерации за январь-декабрь 2019 года // официальный сайт МВД России [Электронный ресурс]. URL: https://media.mvd.ru/files/application/1748898 (дата обращения: 21.10.2024).

что высокая доля мошенничеств среди всех преступлений подтверждает значимость проблемы и подчеркивает необходимость приоритетного подхода к борьбе с этим видом преступлений.

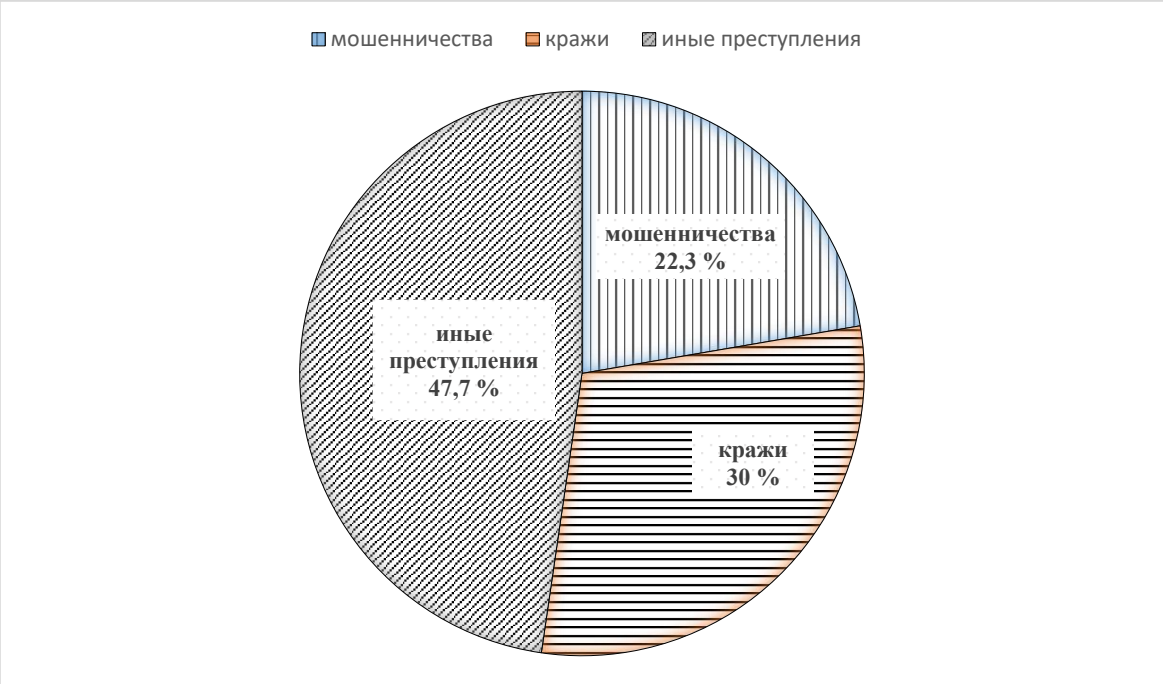

Рис. 1. Структура преступности в России в 2023 году

Анализ данных о динамике мошенничеств в России показал значительное увеличение числа таких преступлений за период с 2019 по 2023 год. Если в 2019 году было зарегистрировано 257 187 случаев, то в 2023 году этот показатель возрос до 443 708 (Рис. 2). Рост на протяжении всего периода позволяет сделать вывод об устойчивой тенденции к увеличению количества случаев мошенничества и может свидетельствовать об усилении активности преступников в цифровом пространстве, а также о расширении методов и сфер распространения мошеннических действий. Данные в очередной раз свидетельствуют о том, что проблема кибермошенничества приобретает всё более серьезные масштабы и требует незамедлительных мер по профилактике и защите уязвимых групп населения.

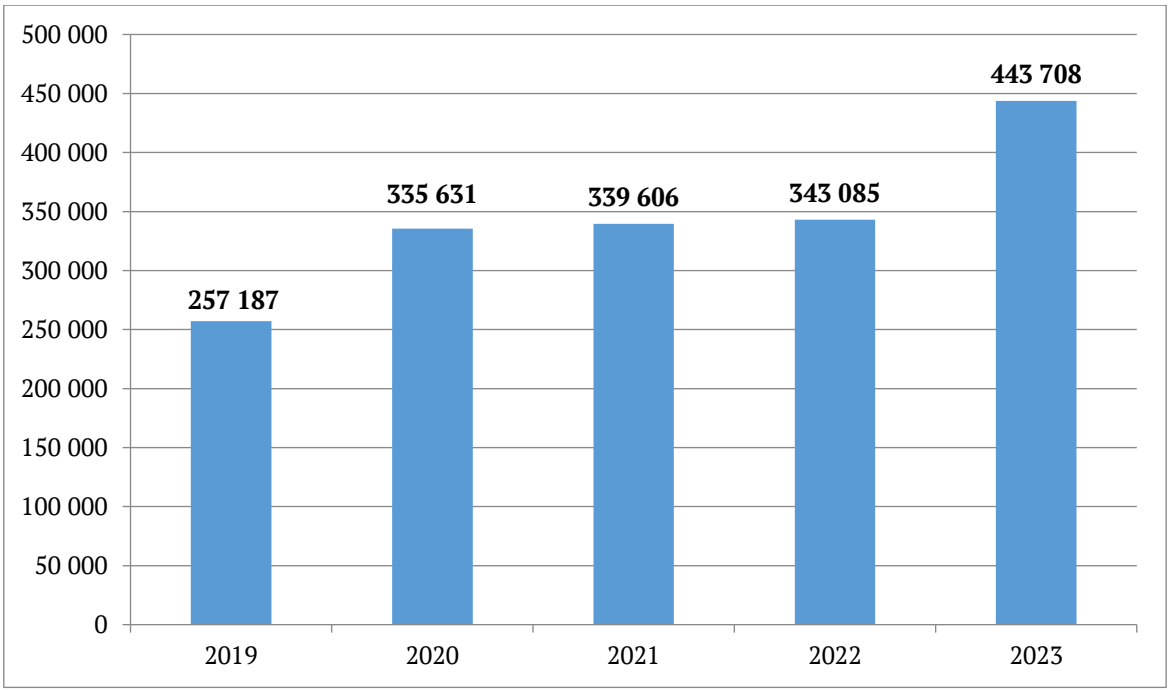

Рис. 2. Динамика количества мошенничеств в России

Вместе с тем активное проникновение информационных технологий в повседневную жизнь людей и рост числа пользователей интернета приводят к ожидаемому росту количества противоправных деяний в сфере ИТТ. В период с 2019 по 2023 год количество таких преступлений увеличилось с 294 409 до 676 951 (Рис. 3). Данная тенденция может быть следствием увеличения числа уязвимых пользователей, особенно среди несовершеннолетних и пожилых граждан, которые зачастую недостаточно осведомлены о рисках кибермошенничества. Предполагается, что с дальнейшим развитием цифровых технологий и услуг количество преступлений в сфере ИТТ, к сожалению, будет продолжать расти.

Аналогичный рост отдельно демонстрируют и мошенничества, совершаемые с использованием информационно-телекоммуникационных технологий. В 2019 году таких преступных деяний было 136 709, а к 2023 году их количество увеличилось до 356 079 (Рис. 4). Примечательно, что наибольший рост числа преступлений наблюдается в последние годы, что, вероятно, связано с увеличением активности преступников в условиях цифровизации

и внедрения новых технологий. Можно предположить, что в дальнейшем кибермошенничество будет только расширять свое присутствие в общей структуре преступности.

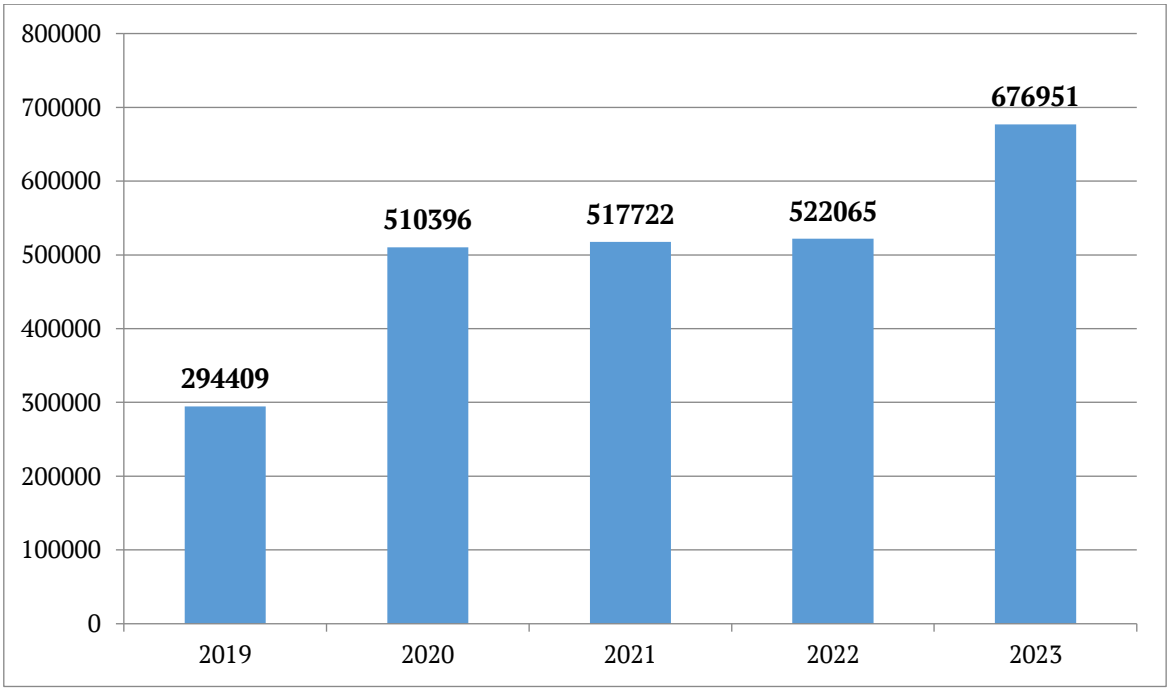

Рис. 3. Динамика количества преступлений, совершаемых в сфере ИТТ

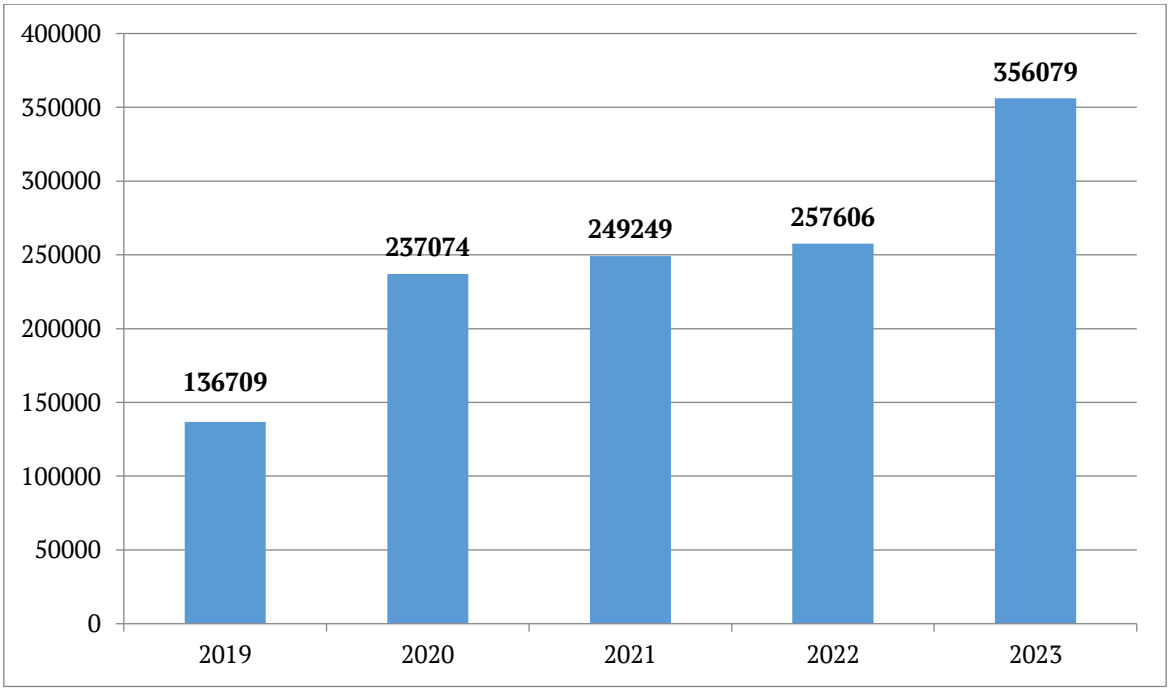

Рис. 4. Динамика количества мошенничеств, совершаемых с использованием ИТТ

Анализ данных, показывающих тенденцию к увеличению количества раскрытых мошенничеств с использованием информационно-телекоммуникационных технологий (ИТТ) из числа преступлений прошлых лет (Рис. 5), позволяет предположить, что правоохранительные органы прилагают значительные усилия для повышения раскрываемости таких преступлений. Динамика роста этого показателя может объясняться несколькими факторами, связанными с усилением технической оснащенности, развитием специализированных навыков у сотрудников правоохранительных органов и внедрением новых подходов к расследованию киберпреступлений, а также с ежегодным последовательным ростом количества совершенных деяний рассматриваемого вида.

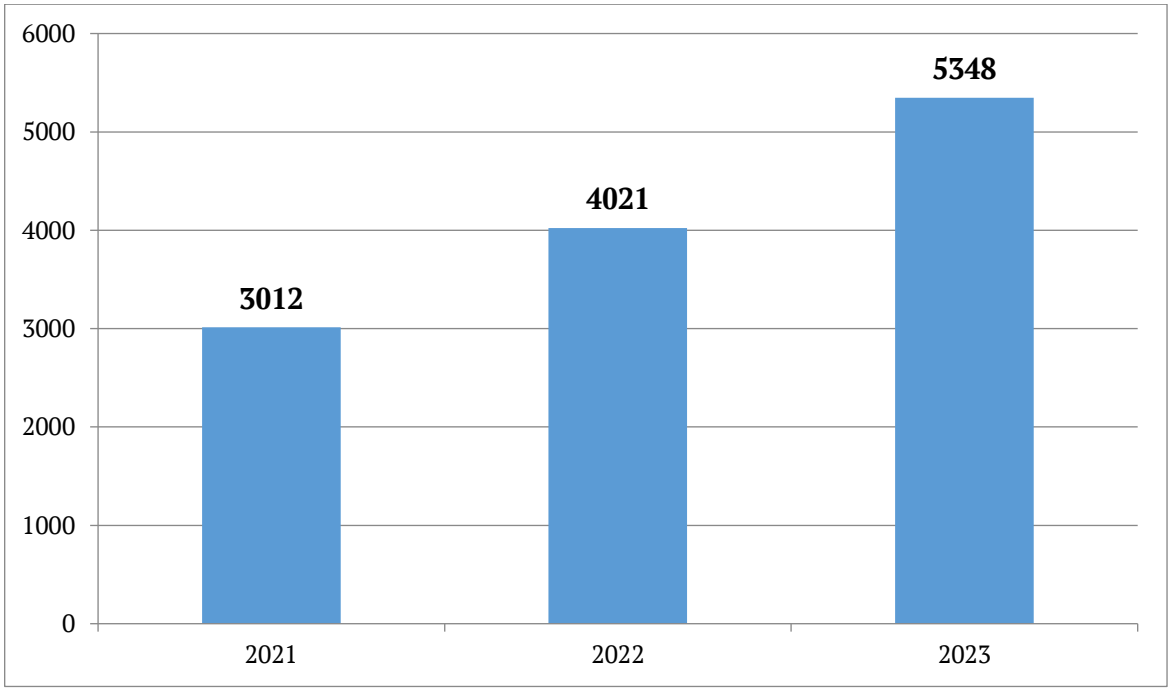

Рис. 5. Раскрыто мошенничеств с использованием ИТТ из числа преступлений прошлых лет

Анализ представленных данных позволяет сделать вывод о нарастающей тенденции к увеличению числа мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий (ИТТ). Ежегодное увеличение зарегистрированных случаев подтверждает, что

кибермошенничество становится всё более распространённой и значимой проблемой в структуре преступности.

Таким образом, можно сделать принципиальный вывод о том, что существенный рост числа таких преступлений в последние годы свидетельствует об усилении активности преступников в цифровом пространстве и указывает на привлекательность этой сферы для осуществления противоправных действий. Наблюдается также повышение доли кибермошенничеств в общей структуре преступности, что требует приоритетного подхода к их профилактике. Вероятно, данная тенденция сохранится, особенно с учётом дальнейшего расширения цифровизации и увеличения числа пользователей, что обуславливает необходимость усиленных мер по защите уязвимых категорий населения, таких как несовершеннолетние и пожилые граждане.

3. Факторы, способствующие совершению мошенничеств в отношении несовершеннолетних и лиц пожилого возраста с использованием сети Интернет

Снижение уровня экономической киберпреступности возможно лишь при уменьшении степени влияния на нее совокупности детерминирующих факторов, которые условно можно разделить на общие и специальные причины и условия.

Первая группа связана с наличием государственного экономического кризиса, увеличением социальной и политической напряженности в стране, низким уровнем правовых знаний населения. Общие детерминанты характерны для всей преступности в целом, однако исследование экономической киберпреступности требует обращения внимания на специальные детерминирующие факторы.

Так, по результатам опроса сотрудников территориальных органов МВД России относительно причин совершения экономических киберпреступлений в наибольшей степени детерминирующее воздействие на экономическую киберпреступность оказывают:

1) анонимность пользователей киберпространства;

2) возможность получения при минимальных затратах высокой прибыли в киберпространстве;

3) несовершенство законодательства;

4) недостаточная регламентация правил поведения в сети;

5) техническое несовершенство киберпространства;

6) низкие показатели раскрываемости экономических киберпреступлений и безнаказанность лиц, совершающих соответствующие преступления;

7) виктимное поведение жертв киберпреступлений[1].

---

[1] Польшиков А. В., Кулешов А. А., Павленко О. С. Детерминанты и перспективные направления профилактики экономической киберпреступности в России // Современное общество и право. 2024. № 3 (70). С. 103.

Анонимность пользователей киберпространства предполагает использование различных способов сокрытия своей личности в сети:

– использование псевдонимов, чужих имен и фотографий;

– сокрытие технических данных (IP-адрес, идентификационный номер персонального компьютера и т. д.) посредством использования компьютерных программ и специальных устройств;

– действие в рамках анонимных информационно-телекоммуникационных сетей («TOP», «Darknet», «Freenet» и др.)

Возможность получения при минимальных затратах высокой прибыли в киберпространстве, по результатам опроса сотрудников ОВД, является второй по значимости причиной совершения экономических преступлений, поскольку привлекательность высокого заработка, скрытого от органов налогового и правового контроля, на фоне сокращения трудовых мест в материальном мире побуждает к совершению неправомерных поступков в сфере киберпространства. Представляется, что это соответствует и реальному положению дел.

Несовершенство законодательства представляет собой весомую объективную причину существования киберпреступности: пробелы в праве создают препятствия для осуществления правоприменительной деятельности, привлечения к ответственности виновных лиц и назначения им справедливого наказания, соответствующего характеру и степени общественной опасности совершенного деяния. Так, до сих пор недостаточной является регламентация сделок и иных манипуляций, осуществляемых с криптовалютой: она не признана ни в качестве электронного средства платежа, ни в качестве предмета уголовно наказуемого хищения, несмотря на высокую распространенность ее использования[1].

[1] О национальной платежной системе : Федеральный закон от 27.06.2011 № 161-ФЗ // Собрание законодательства Российской Федерации. 2011. № 27. Ст. 3872.

Представляется, что планомерное совершенствование отечественного законодательства позволит обеспечить надлежащую реализацию целей уголовного и уголовно-процессуального закона, а также укрепление правопорядка и стабильность общественных отношений.

Недостаточная регламентация правил поведения в сети проявляется в отсутствии минимального уровня цифровой грамотности населения, позволяющего адекватно оценивать уровень киберугроз на различных информационных площадках и выбирать способы своей технической и социальной защищенности, что повышает их риск стать жертвой киберпреступления. В связи с этим нельзя не отметить важность идеологических мер профилактики киберпреступности, состоящих в организации правового и технического просвещения населения, информировании их о типичных схемах совершения противоправных действий в сети и методах противодействия им.

Техническое несовершенство киберпространства играет значительную роль среди обозначенных выше детерминирующих факторов, поскольку наличие технических лазеек, уязвимостей программного и физического характера в системе защиты и функционирования компьютерных и информационных систем сводит на нет всю предупредительную работу.

Природа программных технических уязвимостей носит, как правило, неосторожную основу, однако в некоторых случаях они могут быть созданы умышленно. В частности, имеют место т. н. «backdoor» (от англ. «закрытая дверь») – программный код, искусственно внедряемый разработчиками в целях быстрого и удобного обращения с приложением в обход системы защиты на стадии его создания, которые становятся доступными злоумышленниками.

В свою очередь, ярким примером технической проблемой физического характера является сложившая система безопасности аккаунтов (персональных страниц) в социальных сетях, мессенджерах, приложениях, электронных платежных системах, а также на отдельных сайтах. Дело в том, что

большинство из них в качестве одного из условий регистрации или восстановления доступа к персональной странице предусматривают «привязку» электронной почты и номера мобильного телефона.

Представляется, что это сильно облегчает совершение мошенничеств. Так, имея доступ к мобильному устройству или электронной почте человека, киберпреступник получает возможность совершать манипуляции и с иными принадлежащими ему ресурсами, в том числе электронным денежным средствам.

Виктимное поведение жертв также играет высокую роль в процессе детерминации интернет-мошенничеств, особенно когда речь заходит о таких уязвимых категориях населения, как несовершеннолетние и лица пожилого возраста. Оценка показателя возраста жертв мошенничеств, совершаемых в киберпространстве, неоднозначна. В соответствии с результатами исследования Л. Е. Солянкиной, социально-психологический портрет жертвы интернет-мошенничества представлен следующими группами граждан: лица в возрасте от 19 до 30 лет – 10 %; лица в возрасте от 30 до 39 лет – 43 %; лица в возрасте от 40 до 59 лет – 10 %; лица старше 60 лет – 37 %[1].

По мнению автора, наиболее уязвимой группой является экономически активная категория граждан ввиду того, что они чаще остальных используют возможности информационных технологий и систем при совершении операций по оплате товаров.

В то же время, согласно данным Центрального Банка России, основной удар мошеннических действий в сети приходится на пожилое население – 27 %, при этом по мере уменьшения возраста граждан снижается и степень их подверженности данной категории преступлений. Так, 20 % названных

[1] Солянкина Л. Е. Социально-психологический портрет жертв финансового мошенничества с использованием информационно-телекоммуникационных технологий // Психолого-педагогический поиск. 2023. № 1 (65). С. 129.

киберпреступлений пришлось на лиц в возрасте 50-59 лет; 19 % – 40-49 лет; 17 % – 30-39 лет; 17 % – 29 лет и младше[1].

Синтез статистических данных МВД России, а также результатов научных исследований в области психологии[2] и права[3] показал, что в 65 % случаев жертвой информационных финансовых атак становятся женщины.

Кроме того, ключевыми триггерами, используемыми для выработки метода психологического воздействия на женщин, являются стремление выделиться среди подруг, избавиться от лишнего веса и сохранить красоту; желание оказать помощь больному или лицу, оказавшемуся в трудной жизненной ситуации; склонность к конформизму и подражанию; одиночество, стремление обрести семью и др.

Аналогичными рычагами воздействия на мужчин выступают: стремление быть нужным; желание быстро заработать; неловкость при обращении за помощью в решении финансовых проблем к родственникам; страх отказать и выглядеть бесчувственным и др.

Интересным является то, высокий уровень образования и устойчивое финансовое положение лица не является ни криминогенным, ни антикриминогенным фактором. Так, согласно наблюдениям Л. Е. Солянкиной, среди лиц, имеющих высшее образованием, в том числе ученую степень, занимающих преподавательские, служебные должности, 42 % граждан чаще остальных подвергались обману со стороны кибермошенников[4]. Следовательно, наличие высшего образования, в отличие от развитого уровня цифровой грамотности, не ограждает лицо от возможности стать жертвой экономического преступления в киберпространстве.

---

[1]«Изобразили жертву…» // МИЦ «Известия». URL: https://iz.ru/1140892/anna-kaledina/izobrazili-zhertvu-v-47-sluchaev-kibermoshenniki-obmanyvaiut-liudei-starshe-50-let (дата обращения: 25.09.2024).

[2] Солянкина Л. Е. Указ соч. С. 130.

[3] Хоменко А. Н. К вопросу о виктимизации жертв киберпреступлений // Виктимология. 2021. Т. 8. № 2. С. 145.

[4] Солянкина Л. Е. Указ соч. С. 131.

Оценка личностных свойств жертв позволяет выделить следующие качества: чрезмерную доверчивость, уступчивость, неспособность к отказу; низкий уровень эмоционального контроля, импульсивность; внушаемость, слабую развитость коммуникативных качеств, в том числе «коммуникативный голод», возникающий при одиночестве и нарушении социализации; низкую самооценку, внешний локус контроля; возрастные когнитивные изменения и заболевания (деменция, болезнь Альцгеймера).

Обобщая и анализируя вышеизложенное, можно выделить следующие основные причины совершения мошенничеств в отношении пожилых людей.

1. Чрезмерно доверчивый характер: пожилые люди в силу своего возраста становятся более доверчивыми, тем более мошенники могут выбирать себе авторитетные роли, которые располагают к себе, например, представляясь работниками органов социальной защиты населения.

2. Уязвимость: пенсионеры часто являются более уязвимыми из-за физических или когнитивных ограничений, а также из-за их потенциального отсутствия цифровой грамотности, они становятся наиболее виктимными. Мошенники, и особенно дети и подростки, могут использовать эмоциональные приемы, чтобы легче обмануть пожилых людей, например, утверждая, что им нужна помощь или поддержка.

3. Недостаток информации: пожилые люди имеют ограниченный доступ к информации или знаниям о том, как определить мошеннические схемы, используемые подростками, а также не имеют доступа к подробной информации, которая носит ранний профилактический характер.

4. Финансовые ресурсы: пенсионеры часто имеют накопления или пенсии, что делает их привлекательной целью для мошенников, которые стремятся получить доступ к их деньгам.

5. Изоляция: некоторые пожилые люди могут испытывать определенную социальную изоляцию, недостаток общения, что делает их более

уязвимыми, поэтому для подростков-мошенников они могут стать наиболее доступным источником «общения».

Еще одной виктимной категорией населения являются несовершеннолетние. Ввиду активного использования детьми и подростками цифровых устройств и социальных сетей, а также низкого уровня цифровой грамотности, несовершеннолетние становятся легкой целью для преступников, использующих информационные технологии для совершения мошенничеств.

Основные формы виктимного поведения несовершеннолетних в сети Интернет включают демонстрацию личных данных, участие в сомнительных активностях, доверчивое отношение к неизвестным пользователям и стремление к публичной демонстрации своей социальной жизни. Исследования показывают, что дети и подростки склонны делиться информацией о себе, публиковать личные фотографии и участвовать в открытых обсуждениях на форумах и социальных платформах, что облегчает преступникам доступ к данным и формирует основу для манипулятивных воздействий.

Одной из причин виктимного поведения несовершеннолетних является их недостаточно критичное отношение к информации, получаемой в интернете. Согласно теории когнитивного развития, несовершеннолетние менее склонны подвергать сомнению намерения других людей и часто принимают за достоверные сведения, полученные от внешне авторитетных источников, что делает их уязвимыми для манипуляций. Например, мошенники могут легко создать поддельные аккаунты, представляясь знакомыми или представителями известных брендов, и завоевать доверие подростков. Вследствие этого подростки способны доверить не только личные данные, но и свои цифровые активы, что делает их жертвами мошенничества.

Кроме того, значимым аспектом виктимного поведения несовершеннолетних является их психологическая потребность в социальной принадлежности и признании. Интернет и социальные сети предоставляют платформу, на которой подростки могут взаимодействовать с друзьями и

выражать свою индивидуальность. Однако эта потребность в социальной связи делает их подверженными влиянию со стороны преступников, которые могут использовать эмоциональные и психологические приемы для завоевания доверия. Например, подростки могут стать жертвами мошенничества, связанного с покупкой виртуальных товаров или подпиской на «эксклюзивный» контент, который якобы поможет им занять более высокое положение среди сверстников.

Исследователи также отмечают, что виктимное поведение несовершеннолетних связано с недостатком навыков безопасного поведения в интернете, что обусловлено, в том числе, и пробелами в семейном воспитании и отсутствии систематического обучения цифровой безопасности в школе. Например, подростки могут не знать о том, как защитить свои аккаунты, не осознавать риски, связанные с передачей данных третьим лицам, или недостаточно понимать последствия необдуманных действий в виртуальном пространстве. Этот пробел в знаниях о безопасности особенно ярко проявляется при взаимодействии с незнакомыми людьми в интернете, когда подросток, полагаясь на интуицию или дружелюбный подход, открывает доступ к личным данным.

На основании проведенного анализа можно сделать следующие выводы. Во-первых, основными факторами, детерминирующими совершение мошенничеств в отношении несовершеннолетних и лиц пожилого возраста посредством сети Интернет, являются как общие социальные и экономические причины (например, экономический кризис и низкий уровень правовых знаний населения), так и специальные детерминанты, непосредственно связанные с особенностями киберпространства. К числу последних относятся анонимность пользователей, высокая прибыльность преступлений, несовершенство законодательства и технические уязвимости, а также низкие показатели раскрываемости таких преступлений, что создает чувство безнаказанности у преступников.

Во-вторых, значимую роль играют и личные качества жертв, обуславливающие их виктимное поведение. В частности, уязвимость лиц пожилого возраста и несовершеннолетних, обусловленная низким уровнем цифровой грамотности, доверчивостью и стремлением к социальной принадлежности, делает их особенно восприимчивыми к кибермошенничеству. Пожилые люди, как правило, более подвержены манипуляциям, связанным с фальшивыми банковскими уведомлениями и поддельными инвестиционными предложениями. Дети и подростки, стремясь к признанию в социальных сетях, часто игнорируют меры безопасности и открывают доступ к личным данным, что делает их легкой целью для мошенников.

4. Меры предупреждения мошенничеств, совершаемых в отношении несовершеннолетних и лиц пожилого возраста с использованием сети Интернет

Основу правового регулирования профилактики кибермошенничества, направленного на несовершеннолетних и лиц пожилого возраста, составляет комплекс нормативных правовых актов, предусматривающих меры предупреждения преступности и повышение безопасности в сети Интернет. Эти акты создают рамки для работы государственных органов, учебных заведений и других организаций, ответственных за разработку и реализацию мер профилактики киберпреступлений.

Одним из ключевых документов, регулирующих меры предупреждения преступности, является Федеральный закон от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»[1], который устанавливает общие принципы профилактики и определяет круг субъектов, обязанных участвовать в предупреждении правонарушений. Этот закон регулирует деятельность по профилактике преступлений, включая кибермошенничество, и предусматривает участие в этой деятельности различных государственных структур, таких как МВД России, Министерство образования и науки и Минтруд, а также местные органы власти и общественные организации. Основная цель закона – создать систему профилактики, направленную на снижение уровня преступности, в том числе кибермошенничества, через взаимодействие всех заинтересованных сторон.

Значимым нормативным правовым актом, направленным на защиту детей в интернете, является Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и

[1] Об основах системы профилактики правонарушений в Российской Федерации : Федеральный закон от 23 июня 2016 г. № 182-ФЗ // Собрание законодательства Российской Федерации. 2016. № 26 (часть I). – Ст. 3851.

развитию»[1]. Этот закон не только ограничивает доступ несовершеннолетних к опасному контенту, но и регулирует меры, которые должны предпринимать интернет-ресурсы и организации для обеспечения безопасного использования информационных технологий детьми. Закон обязывает владельцев сайтов маркировать контент, вводить возрастные ограничения и внедрять средства защиты, что снижает риск их контакта с мошенническими схемами и вредоносными материалами.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[2] также выполняет важную профилактическую роль, защищая персональные данные пользователей от неправомерного использования. Пожилые и несовершеннолетние пользователи часто становятся жертвами мошенничества из-за утечки или неправомерного использования их данных. Данный закон предусматривает обязательства для операторов персональных данных по обеспечению их безопасности, что косвенно предотвращает риски мошенничеств, связанных с использованием персональной информации.

Кроме того Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»[3] определяет нормативную основу для проведения профилактических образовательных программ по цифровой грамотности и информационной безопасности. В рамках данного закона образовательные учреждения обязаны обеспечивать безопасную образовательную среду, включая обучение детей и подростков основам безопасного поведения в интернете. Включение программ по цифровой грамотности и

---

[1] О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон от 29 декабря 2010 г. № 436-ФЗ // Собрание законодательства Российской Федерации. 2011. № 1. Ст. 48.

[2] О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31 (часть I). Ст. 3451.

[3] Об образовании в Российской Федерации : Федеральный закон от 29 декабря 2012 г. № 273-ФЗ // Собрание законодательства Российской Федерации. 2012. № 53 (часть I). Ст. 7598.

профилактике кибермошенничества в школьные и образовательные курсы направлено на формирование навыков противодействия мошенникам и осознание потенциальных угроз.

Важную роль играют и подзаконные акты, направленные на регулирование профилактической деятельности. Например, постановление Правительства РФ, касающееся реализации национальной программы «Цифровая экономика»[1], включает меры по повышению цифровой грамотности населения, созданию образовательных материалов и разработке профилактических проектов в области информационной безопасности. Национальная программа «Цифровая экономика» способствует внедрению цифровой грамотности в образовательные стандарты, что позволяет снижать уязвимость пользователей к киберпреступлениям.

Профилактика мошенничеств, совершаемых в отношении несовершеннолетних и лиц пожилого возраста, включает в себя различные виды мер, направленных на снижение уровня преступности и повышение защиты граждан в цифровом пространстве. Общесоциальные меры профилактики охватывают правовое регулирование, повышение уровня цифровой грамотности населения, улучшение информационной безопасности и проведение массовых информационных кампаний для повышения осведомленности о киберугрозах. Важнейшее значение в рамках борьбы с кибермошенничествами имеет виктимологическая профилактика, представляющая собой работу с потенциальными жертвами преступлений.

Меры виктимологической профилактики мошенничеств, совершаемых в отношении несовершеннолетних и лиц пожилого возраста посредством сети Интернет, представляют собой систему действий, направленных на снижение виктимного поведения и повышение осведомленности о

[1] О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» : постановление Правительства РФ от 2 марта 2019 г. № 234 // Официальный интернет-портал правовой информации. URL: https://publication.pravo.gov.ru/Document/View/0001201903070015 (дата обращения: 25.09.2024).

потенциальных угрозах в цифровой среде. Особенности поведения и восприятия уязвимых категорий, таких как несовершеннолетние и пожилые люди, обуславливают необходимость разработки специфических мер, ориентированных на минимизацию рисков стать жертвой киберпреступлений.

Одной из ключевых мер виктимологической профилактики является формирование критического восприятия информации у уязвимых групп. Несовершеннолетние, как нами было отмечено ранее, отличаются доверчивостью и недостатком опыта в распознавании манипулятивных сообщений, что делает их легкой целью для мошенников, использующих техники социальной инженерии. В данном случае необходимо внедрение образовательных курсов, нацеленных на формирование у подростков навыков критического мышления и понимания основ цифровой безопасности. Обучение должно включать примеры типичных схем обмана в интернете, объяснение методов защиты личных данных, а также формирование привычки проверять источники информации. Подобные программы могут проводиться в школах в рамках предметов по информационной безопасности, а также в форме практических семинаров и тренингов, что позволит детям и подросткам не только усвоить теоретические основы, но и научиться применять их на практике.

В отношении пожилых граждан особое внимание следует уделить обучению цифровой грамотности и навыкам безопасного поведения в интернете. Виктимное поведение пожилых людей часто проявляется в чрезмерной доверчивости к незнакомым людям и недостатке знаний о современных технологиях, что делает их уязвимыми для различных форм интернет-мошенничества, включая фальшивые сообщения от банков и других организаций. Поэтому профилактические мероприятия должны включать образовательные программы по основам работы с электронными сервисами, которые помогут пожилым людям различать подлинные сайты и фальшивые, избегать фишинговых ссылок и защищать свои учетные записи. Такие

занятия могут проводиться в центрах социального обслуживания, библиотеках и других учреждениях, ориентированных на поддержку пенсионеров, и должны быть адаптированы к уровню знаний данной группы граждан.

Психологическая поддержка играет важную роль в снижении виктимного поведения у обеих категорий. Пожилые люди часто испытывают одиночество и стремление к общению, что может побуждать их вступать в контакт с незнакомыми людьми в интернете, не осознавая возможных рисков. Поэтому социальные работники и психологи могут работать с пожилыми людьми, разъясняя им риски доверчивого поведения и формируя навыки отказа от общения с подозрительными источниками. Важно разъяснять пожилым людям, что личные данные и доступ к финансовой информации не должны передаваться третьим лицам ни под каким предлогом. В случае с несовершеннолетними психологи и педагоги могут обучать подростков методам безопасного общения в интернете и укреплять у них уверенность в том, что подозрительные запросы и предложения необходимо обсуждать с родителями или педагогами.

Виктимологическая профилактика также требует применения технических средств защиты. Использование технологий родительского контроля для несовершеннолетних и ограниченного доступа к сайтам и приложениям с высоким риском мошенничества снижает вероятность контакта с мошенниками. Кроме того, важно устанавливать на устройства пожилых пользователей программное обеспечение для фильтрации подозрительных ссылок и защиту от фишинга. Виктимологическая профилактика в данном случае тесно связана с техническими аспектами, поскольку позволяет создать барьеры для мошенников и уберечь пожилых и несовершеннолетних пользователей от несанкционированного доступа к их устройствам и личной информации.

В результате анализа мер профилактики кибермошенничеств, направленных на несовершеннолетних и лиц пожилого возраста, можно

заключить, что эффективная защита этих уязвимых групп требует комплексного подхода. Правовая основа, представленная в ряде нормативных правовых актов, устанавливает ключевые принципы предупреждения преступлений и создает базу для взаимодействия различных структур в вопросах профилактики. Эти акты не только формируют правовые рамки для работы государственных органов, образовательных учреждений и социальных служб, но и закрепляют обязанности интернет-ресурсов по защите данных и ограничению доступа к потенциально опасным ресурсам.

Важно отметить значение виктимологической профилактики, которая ориентирована на работу с потенциальными жертвами, учитывая их поведенческие особенности и психологическую уязвимость. Среди подобных мер следует выделить формирование критического восприятия информации, обучение основам цифровой безопасности, психологическую поддержку и консультирование, использование технологий родительского контроля и фильтров безопасности, повышение осведомленности о типичных мошеннических схемах и способах защиты и т. п.

ЗАКЛЮЧЕНИЕ

В условиях активного развития интернет-технологий защита уязвимых групп населения, таких как несовершеннолетние и пожилые люди, от кибермошенничества становится приоритетной задачей. Исследование показывает, что противодействие современным мошенникам требует расширенного понимания состава преступления, предусмотренного ст. 159 УК РФ, особенно в связи с появлением цифровых активов и виртуальных ценностей, которые все чаще становятся предметом преступлений.

В цифровой среде традиционные способы мошенничества, такие как обман и злоупотребление доверием, приобретают новые формы, например, использование фальшивых аккаунтов и фальсифицированных уведомлений, что требует особого подхода при квалификации преступлений. Отграничение мошенничеств от смежных составов является сложной, но выполнимой задачей для сотрудников правоохранительных органов, и основано на учете особенностей взаимодействия преступников с жертвами.

Анализ представленных данных позволяет сделать вывод о нарастающей тенденции к увеличению числа мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий (ИТТ). Ежегодное увеличение зарегистрированных случаев подтверждает, что кибермошенничество становится всё более распространённой и значимой проблемой в структуре преступности. Существенный рост числа таких преступлений в последние годы свидетельствует об усилении активности преступников в цифровом пространстве и указывает на привлекательность этой сферы для осуществления противоправных действий. Наблюдается также повышение доли кибермошенничеств в общей структуре преступности, что требует приоритетного подхода к их профилактике. Вероятно, данная тенденция сохранится, особенно с учётом дальнейшего расширения цифровизации и увеличения числа пользователей, что обуславливает необходимость усиленных

мер по защите уязвимых категорий населения, таких как несовершеннолетние и пожилые граждане.

Основными факторами, детерминирующими совершение мошенничеств в отношении несовершеннолетних и лиц пожилого возраста посредством сети Интернет, являются как общие социальные и экономические причины (например, экономический кризис и низкий уровень правовых знаний населения), так и специальные детерминанты, непосредственно связанные с особенностями киберпространства. К числу последних относятся анонимность пользователей, высокая прибыльность преступлений, несовершенство законодательства и технические уязвимости, а также низкие показатели раскрываемости таких преступлений, что создает чувство безнаказанности у преступников.

Кроме того, значимую роль играют и личные качества жертв, обуславливающие их виктимное поведение. В частности, уязвимость лиц пожилого возраста и несовершеннолетних, обусловленная низким уровнем цифровой грамотности, доверчивостью и стремлением к социальной принадлежности, делает их особенно восприимчивыми к кибермошенничеству. Пожилые люди, как правило, более подвержены манипуляциям, связанным с фальшивыми банковскими уведомлениями и поддельными инвестиционными предложениями. Дети и подростки, стремясь к признанию в социальных сетях, часто игнорируют меры безопасности и открывают доступ к личным данным, что делает их легкой целью для мошенников.

Эффективная защита этих уязвимых групп требует комплексного подхода. Правовая основа, представленная в ряде нормативных правовых актов, устанавливает ключевые принципы предупреждения преступлений и создает базу для взаимодействия различных структур в вопросах профилактики. Эти акты не только формируют правовые рамки для работы государственных органов, образовательных учреждений и социальных служб, но и закрепляют обязанности интернет-ресурсов по защите данных и

ограничению доступа к потенциально опасным ресурсам.

Важно отметить значение виктимологической профилактики, которая ориентирована на работу с потенциальными жертвами, учитывая их поведенческие особенности и психологическую уязвимость. Среди подобных мер следует выделить формирование критического восприятия информации, обучение основам цифровой безопасности, психологическую поддержку и консультирование, использование технологий родительского контроля и фильтров безопасности, повышение осведомленности о типичных мошеннических схемах и способах защиты и т. п.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон от 29 декабря 2010 г. № 436-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 1. – Ст. 48.

2. О национальной платежной системе : Федеральный закон от 27 июня 2011г. № 161-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 27. – Ст. 3872.

3. Об основах системы профилактики правонарушений в Российской Федерации : Федеральный закон от 23 июня 2016 г. № 182-ФЗ // Собрание законодательства Российской Федерации. – 2016. – № 26 (часть I). – Ст. 3851.

4. О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31 (часть I). – Ст. 3451.

5. Об образовании в Российской Федерации : Федеральный закон от 29 декабря 2012 г. № 273-ФЗ // Собрание законодательства Российской Федерации. – 2012. – № 53 (часть I). – Ст. 7598.

6. О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» : постановление Правительства РФ от 2 марта 2019 г. № 234 // Официальный интернет-портал правовой информации. – URL: https://publication.pravo.gov.ru/Document/View/0001201903070015 (дата обращения: 25.02.2025).

Учебники, научные статьи, монографии

7. Польшиков, А. В. Детерминанты и перспективные направления профилактики экономической киберпреступности в России / А. В. Польшиков, А. А. Кулешов, О. С. Павленко // Современное общество и право. – 2024. – № 3 (70). – С. 102–108.

8. Солянкина, Л. Е. Социально-психологический портрет жертв финансового мошенничества с использованием информационно-телекоммуникационных технологий / Л. Е. Солянкина // Психолого-педагогический поиск. – 2023. – № 1 (65). – С. 128–135.

9. Сычева, А. В. Некоторые вопросы криминалистической характеристики «дистанционных» мошенничеств, совершенных в отношении пожилых людей / А. В. Сычева // Вестник Волгоградской академии МВД России. – 2022. – № 1 (60). – С. 135–140.

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

Статистические данные и электронные ресурсы

11. «Изобразили жертву…» // МИЦ «Известия» [Электронный ресурс]. – URL: https://iz.ru/1140892/anna-kaledina/izobrazili-zhertvu-v-47-sluchaev-kibermoshenniki-obmanyvaiut-liudei-starshe-50-let (дата обращения: 25.02.2025).

12. Кибермошенники вывели за границу более 350 млрд рублей за три года // Информационное агентство ТАСС. – URL: https://tass.ru/proisshestviya/21789361 (дата обращения: 21.10.2024).

13. Состояние преступности в Российской Федерации за январь-декабрь 2019 года // официальный сайт МВД России. – URL: https://media.mvd.ru/files/application/1748898 (дата обращения: 25.02.2025).

14. Состояние преступности в Российской Федерации за январь-декабрь 2020 года // официальный сайт МВД России. – URL: https://media.mvd.ru/files/application/2041459 (дата обращения: 25.02.2025).

15. Состояние преступности в Российской Федерации за январь-декабрь 2021 года // официальный сайт МВД России. – URL: https://media.mvd.ru/files/application/2315310 (дата обращения: 25.02.2025).

16. Состояние преступности в Российской Федерации за январь-

декабрь 2022 года // официальный сайт МВД России. – URL: https://media.mvd.ru/files/application/5130663 (дата обращения: 25.02.2025).

17. Состояние преступности в Российской Федерации за январь-декабрь 2023 года // официальный сайт МВД России. – URL: https://media.mvd.ru/files/application/5095078 (дата обращения: 25.02.2025).

Учебное издание

Иван Александрович Кравцов
Анна Николаевна Белоусова
Александр Васильевич Польшиков
Василий Степанович Прохонов
Станислав Геннадьевич Родин
Антон Александрович Кулешов

ОСОБЕННОСТИ КВАЛИФИКАЦИИ
И ПРЕДУПРЕЖДЕНИЯ МОШЕННИЧЕСТВ,
СОВЕРШЕННЫХ В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ
И ЛИЦ ПОЖИЛОГО ВОЗРАСТА
С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Учебное пособие

Редактор С. М. Русинова
Компьютерная верстка А. А. Кулешова

Подписано в печать 25.06.2025
Формат 60x84 1/16
Усл.-печ. л. 2,5
Тираж 50 экз. Заказ № 120

Воронежский институт МВД России
394065 Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065 Воронеж, просп. Патриотов, 53