Факторы и условия, влияющие на тенденцию виктимологии киберперхищений

Factors and conditions affecting the victimology trend of cybertheft

DOI: 10.12737/2500-333X-2026-11-2-157-165

Фрасов А.Д.
Аспирант 2-го курса по направлению 5.1.4. Уголовно-правовые науки, кафедра Уголовного права, ФГБОУ ВО «Ульяновский государственный университет», г. Ульяновск
e-mail: ebrezneva@list.ru

Frasov A.D.
2nd year postgraduate student in the field of 5.1.4. Criminal Law Sciences, Department of Criminal Law, Ulyanovsk state university, Ulyanovsk
e-mail: ebrezneva@list.ru

Аннотация
Введение. В настоящее время общественным отношениям характерны мощные перемены, которые проявляются в активном внедрении и развитии информационных технологий, что создает условия взаимодействия в формате виртуальной реальности. Статистические сведения указывают на то, что численность пользователей Интернетом прогрессирует, совершенствуются и масштабируются ИКТ. Подобного рода достижения человечества создают условия и для преступной активности в киберпространстве, которая демонстрируют экспоненциальный рост. В соответствии с данной причинно-следственной связью прорывных технологий в области цифровизации в сравнении с тенденций правонарушений в виртуальном пространстве, следует отметить необходимость разработки более эффективных уголовно-правовых и криминологических мер борьбы с киберхищениями. *Материалы и методы*. Данное исследование проведено с применением логического, системно-структурного, социологического, статистического методов, теоретического анализа научной литературы, направленных на выявление условий и факторов, влияющих на виктимологию киберхищений. *Результаты исследования и их обсуждения.* На основе проведенного обзора терминологии киберпреступности в условиях цифровой трансформации, проявляющихся в выстраивании цифровых ресурсов и сквозных цифровых процессов установлена истинная сущность и особенность киберхищений как преступлений, совершаемых в цифровой среде дистанционно с использованием информационно-коммуникационных технологий и социальной инженерии по отношению к большей численности потенциальных жертв и управлению их поведением, что способствует ускорению транзита передачи информации, бесшовному функционированию множества сервисов, способствующих проведению безналичных платежей на условии подчинения воли жертв корыстным интересам киберпреступников. *Заключение* В целях противодействия киберхищений предложены важные подходы: во-первых, важна индивидуальная виктимологическая профилактика уязвимых субъектов; во-вторых, необходима актуализация национального законодательства, на предмет ответственности за совершение киберпрхищений; в-третьих, необходим комплексный подход в борьбе с киберхищениями.
Ключевые слова: киберхищения, киберпреступления, социальная инженерия, информационно-коммуникационные технологии, киберпреступники, кибержертвы, виктимология.

Abstract
Currently, social relations are characterized by powerful changes, which manifest themselves in the active introduction and development of information technologies, which creates conditions for interaction in the format of virtual reality. Statistical data indicates that the number of Internet users is progressing, and ICTs are being improved and scaled. Such achievements of humanity also create conditions for criminal activity in cyberspace, which is growing exponentially. In accordance with this causal relationship of breakthrough technologies in the field of digitalization in comparison with the trends of offenses in the virtual space, it should be noted that it is necessary to develop more effective criminal law and criminological measures to combat cyber-thefts. *Materials and methods.* This study was conducted using logical, system-structural, sociological, and statistical methods, as well as theoretical analysis of scientific literature, aimed at identifying the conditions and factors that influence the victimology of cyberthefts. *Research results and their discussion.* Based on the review of the terminology of cybercrime in the context of digital transformation, which manifests itself in the creation of digital resources and end-to-end digital processes, the true essence and characteristics of cybertheft as a crime committed in the digital environment remotely using information and communication technologies and social engineering in relation to a large number of potential victims and the management of their behavior have been established. This contributes to the acceleration of information transfer, the seamless functioning of multiple services that facilitate the transfer of non-cash payments, and the subjugation of victims' will to the malicious interests of cybercriminals. *Conclusion* In order to counter cyber-theft, important approaches have been proposed: first, individual victimological prevention of vulnerable subjects is important; second, the national legislation should be updated to provide for liability for cyber-theft; third, a comprehensive approach to combating cyber-theft is necessary.
Keywords: cyber-theft, cyber-crime, social engineering, information and communication technologies, cyber-criminals, cyber-victims, victimology.

Введение

Динамика киберпреступлений, представленная на рисунке 1 отражает экспоненциальный рост, а именно темп роста киберпреступлений за последние 10 лет с 11000 в 2013 г. до 764 400 киберпреступлений в 2024 г., который составил почти 70 раз, а за последние 5 лет рост киберпреступлений составил 4,5 раза.

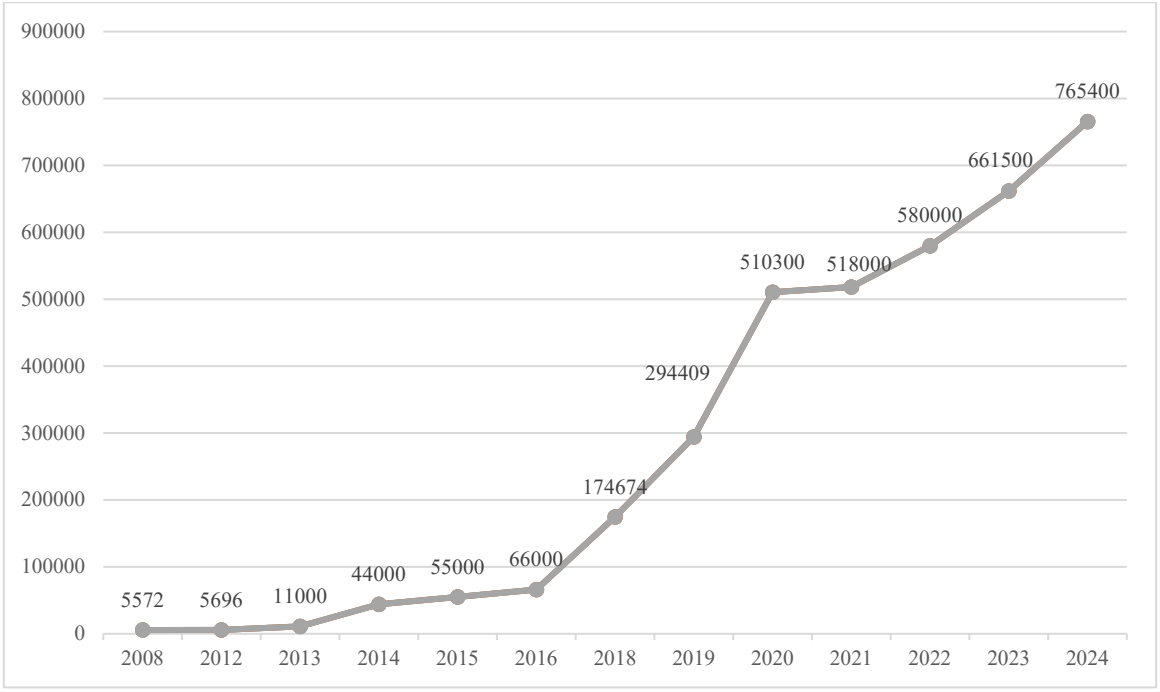

Рис. 1. Динамика зарегистрированных киберпреступлений за период 2008 по 2024 г. [7]

Резкий рост киберпреступлений произошел в период 2019-2020 гг., в пандемийный период, с 174 674 преступлений в 2018 г. до 510 300 преступлений в 2020 г. Данная тенденция развивалась на фоне таких сопутствующих факторов, как: снижение социализации в обществе и одновременным ростом инновационной активности в сфере информационных технологий как со стороны производителей технического оснащения, так и с его практическим применением со стороны пользователей.

В настоящее время киберпреступления в общем объеме преступлений занимают весомое место, примерно 70%, при этом доля киберхищений в составе киберпреступлений весомая, около 30%. Заметим, что в период с 2023 по 2025 г. более интенсивный рост относится к киберхищениям, которые совершаются с использованием методов социальной инженерии и психологического давления, доля которых составляет около 56%, а в 40% случаев в кибермошенничестве было задействовано использование вредоносного программного обеспечения, которое внедрялось в компьютеры и смартфоны потерпевших путем перехода пользователей Интернет, потенциальных жертв, по опасной ссылке. Стоит отметить, что в 31% случаев указанными программами являлись «трояны» для удаленного управления или программы удаленного доступа.

При более детальном исследовании общего количества киберпреступлений, около 80-85% приходится на кибермошенничество от 47% в 2019 г. до 59% в 2024 г. (ст. 159, 159.3, УК РФ), на долю киберхищений приходится от 38% в 2019 г. до 25% в 2024 г. (ст.158 УК РФ). При этом уровень раскрываемости киберпреступлений остается одним из низких, за текущий период данный показатель не превысил 20-23%. Причиной данного положения является виртуальность применения цифровых решений в ходе совершения преступный действий, что ускоряет процесс совершения киберпреступления и позволяет скрывать вещественные улики, к тому же, инновационные решения области ИКТ, которые злоумышленники используют в преступных целях, более мобильны в сравнении с преследованиями, регламентированными в УК РФ. Резюмируя данное описание, очевидно, что необходима разработка более эффективных уголовно-правовых и криминологических мер борьбы с киберпреступлениями.

Методология и методы

Методологическую основу исследования составляет комплекс общенаучных и специальных методов познания: диалектический, раскрывающий тенденцию инновационного развития информационно-коммуникационных технологий в единстве противоречий, отражающихся в росте киберпреступлений; системно-структурный, описывающий причинно-следственные связи. В исследовании применялся комплексный подход знаний: юриспруденции, социологии, психологи и экономики. Цель - выявление причинно-следственной связи между поведением человека и процессами киберпреступности.

Результаты исследования и их обсуждение

Основными способами совершения киберхищений являются: информационно-коммуникационные технологии, которые позволяют получить данные чужой банковской карты посредством: подключения к POS–терминалам техники в торговых точках или использование переносных устройств в ресторанах; организация фиктивных пунктов выдачи наличных (ПВН); установка накладок на приемные устройства и клавиатуру банкоматов, перехватывающей спецтехники внутри них (также «скимминг» – копирование данных магнитной полосы карты) [2].

На ряду применения информационно-коммуникационных технологий для совершения киберхищения злоумышленники используют способ социальной инженерии, - наиболее распространенный способ совершения хищения в настоящее время, который базируется на специфике «человеческого фактора» посредством телефонного разговора или переписки путем претекстинга, посредством аудио контакта, используя дипфейк для получения искомой информации или подчинения жертвы, а также спуфинга, путем подделки контакта: адреса

электронной почты, сайта, номера телефона направленных на психологическое манипулирование жертвы с целью получения денежных средств обманным способом. По мнению Стяжкиной С.А., методы социальной инженерии, информационно-телекоммуникационные технологии обеспечивают адаптацию киберпреступников к потребностям криминальной деятельности, особенностям общественно-политической обстановки в стране и разработке новых способов обмана жертвы; возможность поиска и выбора потенциальных жертв обеспечивает адресность криминальной деятельности с учетом их индивидуального или группового преступного посягательства [3] Структура способов совершения киберхищений представлена на рис. 2.

Рис. 2. Структура способов совершения киберхищений

Использование современных и постоянно развивающихся информационно-телекоммуникационных технологий в комплексе с подходами социальной инженерии дает возможность мошенникам осуществлять преступные действия, нанося ущерб большому числу граждан.

При этом киберпреступники, используя инструменты социальной инженерии прибегают к моделированию коннекта с жертвой в соответствии с моделью пирамиды человеческих потребностей, только в перевернутом виде.

Очевидно, что и отражает пирамида Маслоу, главной целью человека является стремление к раскрытию его потенциала, признание обществом, но для этого формируется личность в результате воспитания, обучения, получения профессиональных навыков, которые в последствии и применяются на практике (рис. 3).

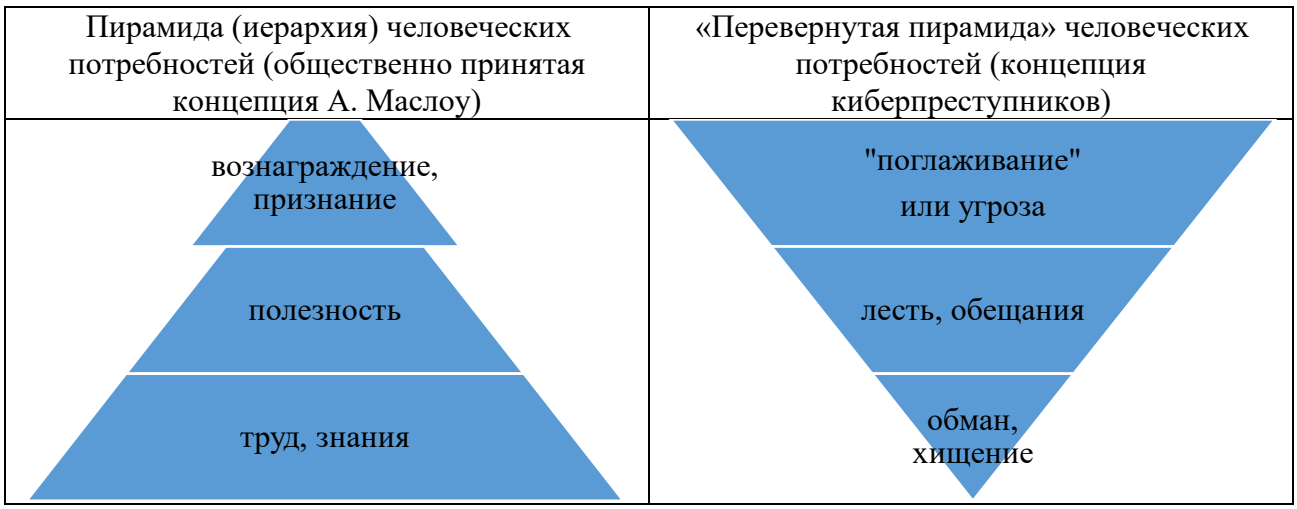

Рис. 3. Сравнение сценариев поведения человека по общественно принятой концепции и сценарию киберпреступников

Злоумышленники создают условия «перевернутой пирамиды», в которой последовательность достижения цели нарушена умышленно для того, чтобы воспользоваться ожиданиями жертвы в получении быстрого обогащения с минимальными затратами и, по сути, «навязывания» действий по сценарию жертве с целью обогащения за ее счет. При этом, жертва соглашается на совершение действий по сценарию, нераспространенному в практике, в том числе по пренебрежению общепринятыми правилами и законном для того, чтобы уладить, в данном случае, - мнимые проблемы, зачастую свои и (или) близких. В данном ключе согласны с выражением Фоминых Е.В. «….как индивид соотносит средства и цели, насколько он готов к использованию незаконных методов, стремился ли к быстрой и легкой наживе, а также учитывает ли интересы других людей в своих действиях» [4]. Важно проанализировать. Получается, что предложение о «выгодном», «быстром», «большем», «лучшем» и других заманчивых условий обладает спецификой риска и без упорядоченного в соответствии с общественно принятыми нормами и законами, может быть обманом, что неминуемо оборачивается соответствующими потерями.

В призме рассуждения все логично и понятно, но, тогда как и почему происходят киберхищения так массово и масштабно? Рассмотрим специфику поведения жертв киберпреступников, их свойства натуры, черты поведения и социальный статус.

Прежде всего, киберпреступник создает условия, так называемое обстоятельство, для того, чтобы иметь возможность манипулировать действиями жертвы. По сути, если жертва принимает условия взаимодействия, то она соглашается на те обстоятельства, которые будут удобны в сценарии киберпреступника (рис. 4).

Рис. 4. Условия коннекта жертвы и преступника

В свою очередь, киберпреступник подбирает сценарий манипулирования поведением жертвы, соответствующий ее психотипу, социально-демографическому критерию, интересам и потребностям. Рассмотрим более подробно инструментарий манипулирования, который избирает киберпреступник для совершения киберхищения.

1. Прежде всего, в данном ключе рассмотрим такой базисный аспект, как свойство натуры жертвы, ее нравственно-психологическое состояние. В данной группе следует уделить внимание таким аспектам, как: темперамент и психотип потенциальной жертвы. В целом, в призме совершения киберпреступлений (виктимизации) проведем рассуждение по трем психотипам жертвы:

- активный психотип, характерен по типу темперамента для сангвиников, в данном случае, жертва активна, склонна к импульсивным действиям и риску. В данном случае агрессор действует мощно, напористо, быстро, по сути, не дает возможности жертве для обдумывания, подчиняя ее напором под себя. При этом вспыльчивость, раздражительность и агрессивное поведение жертвы путем оскорблений и клеветы, интонацией голоса зачастую провоцирует преступное действие;
- пассивный психотип поведения потенциальной жертвы, характерен по типу темперамента для холерика и флегматика, которые зачастую не конфликтны и в силу тревожности и (или) застенчивости не способны оказывать сопротивление и давать отпор киберпреступнику. При этом они зачастую проявляют активность и вступают в контакт с киберпреступником путем обращения или просьбы в содействии и помощи. Данному психотипу характерны устойчивость и расчетливость, в силу специфики натуры, они могут в любой момент изменить линию поведения. Для киберпреступников это одни из непредсказуемых и неудобных психотипов;
- некритичный тип, характерен в большей степени для меланхоликов, - скромных, застенчивых, беззащитных, зависимых от расположения партнера. Их пассивное поведение и неспособность здраво оценивать реалистичность происходящего, - легкая и быстрая добыча для киберпреступника.

2. Следующим этапом описания признака личности «мишени» киберпреступника, рассмотрим физиологические признаки, характеризующие черту поведения человека, потенциальной жертвы.

В черте поведения человека, в данном аспекте потенциальных жертв, одними из главных условий выступают факторы, которые зачастую вызваны объективными обстоятельствами:

– во-первых, отсутствие осведомленности о киберугрозах, способах, инструментах воздействия на потенциальную жертву, доступность каналов взаимодействия с киберпреступниками для выполнения их требований на фоне недостаточных знаний и компетенций для распознания манипуляций со стороны злоумышленников, самоуверенность и легкомыслие поведения жертв;

– во-вторых, в силу социального положения, а также с возрастом потенциальных жертв киберхищений эмоциональная уязвимость повышается, иногда переходя в эмоциональные расстройства. Также в силу ухудшения состояния здоровья, имущественного положения личного или близких, равновесие может нарушаться и личность, несмотря на молодой возраст и активную социализацию, может испытывать эмоциональную уязвимость или расстройства. В таком состоянии, как следствие, возникают и увеличиваются потребности в помощи и поддержке, что отражается на усилении доверчивости, наивности, неспособности адекватно оценить истинные мотивы окружающих, тем более виртуальных.

Третьим признаком этапом для оценки личности жертвы киберпреступника является ее социально-демографическое положение: пол, возраст, род занятий, уровень образования, семейное положение, место жительства, социальное положение. Как правило, данные сведения киберпреступникам становятся доступными в результате взлома баз данных клиентов банков, страховых компаний, официальных сайтов организаций, - мест работы потенциальных жертв или их клиентов. Свод показателей по жертвам киберхищений представлен в табл. 1 и на рис. 5.

Таблица 1

Показатели социально-демографического положения жертв киберхищенииий, (%)

Место жительства		Пол		Возраст				Образование			Доход		
гор	дер	муж	жен	14-24	25-44	45-64	более 65	средн	ср. проф	выс шее	низ кий	сред ний	высо кий
74	26	47	53	19	36	27	18	32	43	25	27	46	27

Для понимания причин воздействия киберпреступников именно на данную категорию лиц, проведем аналитический обзор экономических условий, которые развиваются в условиях современных реалий.

За 2025 год по данным Минэкономразвития РФ инфляция составила 11,46% [8], при этом прирост уровня цен и тарифов составил 10,21% [9]. В сравнении с 2016 г. – 5,48%; 2017 г. – 2,51%; 2018 г. – 4,51%; 2019 г. 2,89%.

По данным аналитического обзора макроэкономических показателей очевидно, что с в период 2020-2022 гг. с дальнейшей пролонгацией до сегодняшних дней произошел резкий, 3-х кратный рост: инфляции, уровня цен на повседневные товары и услуги, а также ключевой ставки ЦБ России, что указывает на повышение барьеров как для экономического развития, так и социального положения населения.

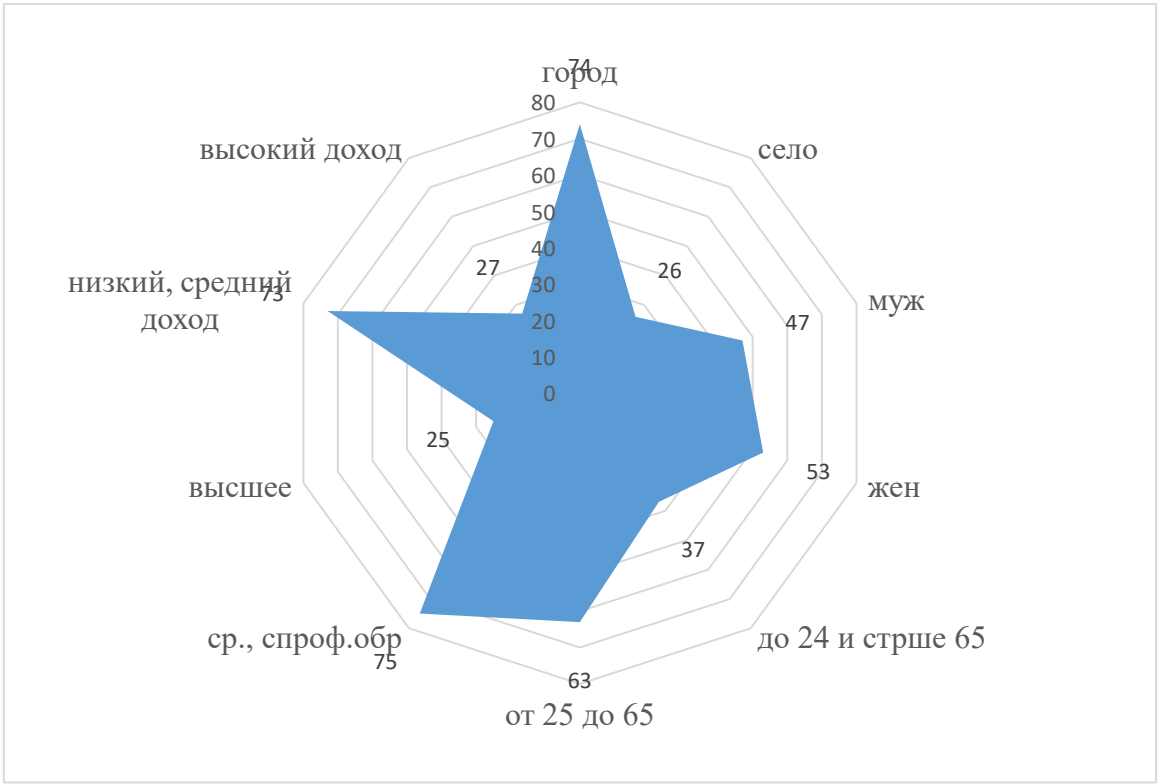

Рис. 5. Показатели социально-демографического положения жертв киберхищений, (%) [10] (составлено автором самостоятельно на основе статистического обзора Банка России)

На рис. 5 наглядно видны уровни ключевых критериев оценки жертв киберхищений и потенциально-уязвимых категорий, которые могут быть мишенью для киберпреступников (данные показатели превышают значения 50%), а более конкретно, это: городское население, в основном женщины, со средним и средним профессиональным образованием, с низким и средним доходом, дополнительно исходя из наблюдений предварительного следствия,

в условиях неполной семьи или фрагментарным контактом с ближайшим родственником или супругом.

Если учесть, что средний уровень заработной платы (на примере Ульяновской области) в 2025 г., в месяц, составил 66 426 руб., в среднем кредит (ипотечный и (или) потребительский) составляет от 15 до 25 тыс. руб., а также с учетом 1 -2 ребенка в семье (с прожиточным минимумом 18 371руб. по данным 2025 г.), при этом, на фоне роста цен и тарифов, реальный уровень дохода увеличивается в меньшей степени, то очевидно, что ввести в заблуждение граждан со стороны кибермошенников в получении дополнительного дохода, в том числе и от инвестиционной деятельности или запугать, как правило, через призму потери скопленной суммы депозита, а также деталей осуществления профессиональной деятельности, - находит свое отражение в реалии (особенно, если в семье один родитель).

Статистические данные предварительного следствия подтверждают, что более 50% пострадавших от киберпреступлений это: женщины в возрасте от 30 до 50 лет со средним профессиональным образованием с уровнем заработной платы до 50 тыс. руб., воспитывающие несовершеннолетних детей. При этом следует заметить, что в критерии оценки «состав семьи» зачастую не входит, однако в определенных случаях, как например, для женщин, не попадающих в группу «одиночек» и не претендующих на получение социальной поддержки, приходится данный вопрос решать самостоятельно, что является решающим аспектом затруднений в жизненной ситуации.

Кроме того, при обзоре потенциальных жертв в расчет берется также уровень образования и социальный статус жертвы. Стоит обратить внимание на то, что основная доля жертв киберхищений это женщины, занимающие не руководящие должности, подчиняющиеся руководящему звену, чем и пользуются киберпреступники при выходе на связь. В данном случае избирают тактику подчинения жертвы запугиванием или избирают иной сценарий манипулирования, так называемым «поглаживанием», используя лесть, обещания или лицемерное признание достоинств жертвы, в силу того, что жертва не получает в реальной жизни подобных «реверансов», которые приятно получать в моменте, то она легко поддается на подобный вид вовлечения в процесс киберпреступления. Данный аспект подтверждает выражение Р. Титуса, который выдвинул гипотезу о том, что потенциальная жертва может способствовать реализации мошеннических схем [5].

Заключение

В условиях, когда поведение потенциальной жертвы характеризуется высокой степенью виктимности, обусловленной игнорированием или недостаточным пониманием принципов обеспечения имущественной и информационной безопасности, злоумышленники могут эффективно эксплуатировать уязвимости [1].

Резюмируя данное описание, очевидно, что необходима разработка более эффективных уголовно-правовых и криминологических мер борьбы с киберпреступлениями.

В целях противодействия киберхищений предлагаем выделить три важных аспекта:

– во-первых, важна индивидуальная виктимологическая профилактика уязвимых субъектов в зависимости от характеристик потенциальной жертвы (по данным проведенного обзора, табл. 1 и рис. 5) в виде консультирований и бесед с психологами, юристами и специалистами по информационной безопасности; необходимы программы по обучению граждан с применением практических кейсов (разбор конкретных случаев киберпреступлений, имитация фишинговых атак); оказание психологической поддержки и конкретной помощи жертвам киберхищений;

– во-вторых, для противодействия таким общественно опасным преступлениям, как киберхищения, необходимо установление уголовной ответственности за совершаемые с помощью информационных технологий и социальной инженерии преступные деяния [6];

– в-третьих, необходима разработка совместных действий как со стороны правоохранительных органов, так и со стороны субъектов критической информационной

инфраструктуры: банковской, налоговой, страховой систем, операторов связи для комплексного противодействия киберхищениям.

Литература

1. Графова Ю.М. Виктимологический феномен мошенничества с использованием цифровых технологий социального инжиниринга // Виктимология. 2025. Т. 12, Nob 4. С. 601–610. DOI:10.47475/2411-0590-2025-12-4-601-610 (Дата обращения: 10.01.2026).
2. Лукьянов С.О. Мошенничество с использованием банковских карт в России: современное состояние и виды защиты // Вестник ТГЭУ. 2012. № 2. С. 201
3. Стяжкина С.А. Виктимологическая профилактика кибермошенничества// ВЕСТНИК Удмуртского университета 2022. Т. 32, вып. 3 Экономика и право С. 546-551.
4. Фоминых Е.С. Психологические механизмы виктимности // Научно-методический электронный журнал «Концепт». 2014. Nob 5. С.116–120.
5. Titus R., Gover A. Personal Fraud: The Victims and the Scams. In G.Farrell and K.Pease (eds.), Repeat Victimization, Crime Prevention Studies, 2001. Vol. 12 Monsey, N.Y.: Criminal Justice Press. URL: http://www.springerlink.com/content/q3582003t7p476j6/ (Дата обращения: 02.12.2025).
6. Об исполнении поручения Президента по уточнению такого состава преступления, как мошенничество // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/acts/assignments/execution/16923 (дата обращения: 17.12.2025).
7. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // Официальный сайт Министерства внутренних дел Российской Федерации.URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 30.12.2025).
8. https://ulpravda.ru/rubrics/economics/a-tseny-rastut-kak-skladyvaetsia-ekonomicheskaia-situatsiia-v-ulianovskoi-oblasti
9. https://73.rosstat.gov.ru/storage/mediabank/Шаблон%20текстового%20документа%20Ульяновскстат%20ИПЦ_ИНДЕКСЫ%20ПОТРЕБИТЕЛЬСКИХ%20ЦЕН%20%20(ТАРИФОВ)%20НА%20ТОВАРЫ%20И%20УСЛУГИ%20ПО%20УЛЬЯНОВСКОЙ%20ОБЛАСТИ.pdf
10. https://www.forbes.ru/finansy/530998-bank-rossii-sostavil-portret-zertvy-kibermosennikov