УДК 343.988(045)

С.А. Стяжкина

ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА КИБЕРМОШЕННИЧЕСТВА

Проблема противодействия киберпреступности на сегодняшний день выходит на одно из лидирующих позиций во всем мире. Особенность данной проблемы в ее многогранности и многоаспектности. Для эффективной борьбы с этим относительно новым видом преступности требуется объединение усилий представителей различных сфер деятельности (юридической, технической, психологической, социальной и др.). Общество перешло на новый этап развития, совершенно иной, требующий комплексного подхода в регулировании складывающихся общественных отношений. Информатизация и кибернетизация всех процессов жизнедеятельности человека и общества предполагает и адекватную реакцию со стороны государства в части защиты и обеспечения безопасности индивидов в новом цифровом пространстве.

В статье раскрываются актуальные вопросы противодействия киберхищениям. Анализируется понятие кибержертвы, раскрываются его признаки. Предлагается авторская классификация жертв мошенничества в сфере компьютерной информации. С учетом данной классификации раскрываются социально-психологические особенности разных типов жертв киберхищений. Предлагаются меры виктимологической профилактики киберпреступности. В статье приводятся примеры деятельности органов государственной власти и общественных объединений в сфере противодействия киберпреступности.

Ключевые слова: кибервиктимология, кибержертва, мошенничество в сфере компьютерной информации, виктимология, виктимологическая профилактика, информационные технологии, преступность.

DOI: 10.35634/2412-9593-2022-32-3-546-552

Проблема противодействия киберпреступности на сегодняшний день выходит на одно из лидирующих позиций во всем мире. Особенность данной проблемы в ее многогранности и многоаспектности. Для эффективной борьбы с этим относительно новым видом преступности требуется объединение усилий представителей различных сфер деятельности (юридической, технической, психологической, социальной и др.). Общество перешло на новый этап развития, совершенно иной, требующий комплексного подхода в регулировании складывающихся общественных отношений. Информатизация и кибернетизация всех процессов жизнедеятельности человека и общества предполагает и адекватную реакцию со стороны государства в части защиты и обеспечения безопасности индивидов в новом цифровом пространстве.

По данным Росстата, на 2020 г. в России сеть Интернет используют 88,6 % населения (в городах 91 %). Самая активная возрастная группа пользователей - это лица от 15 до 24 лет (97 % данной возрастной группой пользуются сетью Интернет), далее идут группы 25–34 года (96,3 %) и 35–44 года (93,8 %). Меньше всех используют Интернет лица в возрасте от 65 лет - всего 39,5 % от всех лиц данной возрастной группы. Данные показатели очень точно отражают целевую аудиторию цифрового пространства и основных его потребителей. Естественно, что на сегодняшний день в основном молодежь является активным пользователем информационных ресурсов, она же будет и основным объектом виктимологической профилактики.

Наиболее распространенными целями использования Интернета являются: общение в социальных сетях (76,7 % от всех пользователей сети), звонки и видеосвязь (71 %), чаты и мессенджеры (60,1 %), поиск информации о товарах и услугах (56,5 %), банковские операции (51,6 %), просмотр фильмов, клипов, скачивание музыки (47,6 %), электронная почта (43,1 %).

Средства защиты информации используют всего 78 % от всех пользователей (в 2015 г. этот показатель был равен 85,8 %). Наблюдается тенденция к снижению использования средств защиты на фоне увеличения количества пользователей сети Интернет.

Большинство пользователей сетей ни разу не сталкивались с угрозами информационной безопасности (70,5 %). Только 7,5 % были жертвами вирусов, 1,5 % подверглись несанкционированному доступу к их информации, 0,3 % стали жертвами хищений.

Конечно, данные цифры не в полной мере отражают реальную картину информационного развития общества. Многие правонарушения остаются за рамками официальной статистики. Информационные преступления одни из самых высоколатентных. Одной из причин данного обстоятельства выступает виктимологическая составляющая, в силу которой потерпевшие, во-первых, не всегда

знают и понимают, что они стали жертвами преступлений. А во-вторых, они очень редко обращаются в правоохранительные органы за защитой своих прав в силу незначительности нарушений и не уверенности в восстановлении их прав. Особенно это касается таких преступлений, как нарушение неприкосновенности частной жизни лица (ст. 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

На сегодняшний день быстрыми темпами развивается новое направление криминологии – кибервиктимология, под которой, по мнению Д.В. Жмурова, следует понимать «учение о жертве преступления, совершенного при помощи компьютерных технологий»[1]. Но есть и другое определение кибервиктимологии. По мнению О.Б. Бовть, под кибервиктимологией следует понимать «отрасль социально-психологической виктимологии, изучающая причины и социально-психологические механизмы становления людей кибержертвами»[2].

Несомненно, что проблемы исследования вопросов виктимизации жертв киберпреступлений на сегодняшний день приобретают особую актуальность. Преступность, как и остальные сферы общественного развития, все больше и больше смещается в виртуальную сферу.

По данным официальной статистики, уже более четверти от всех преступлений составляют киберпреступления (26,6 %). Из числа киберпреступлений 212,8 тыс. совершены с использованием Интернета, 126,7 тыс. – мобильной связи, 103,7 тыс. – банковских карт, 21,8 тыс. – компьютерной техники, 6,6 тыс. – программных средств, 922 – фиктивных электронных платежей, сообщает комитет Госдумы по информполитике. В сумме это даёт 0,47 миллиона[3]. В 2021 г. общий ущерб от преступлений с использованием компьютерных технологий в России превысил 150 млрд руб., через год он может достичь 165 млрд руб., подсчитали аналитики RTM Group[4].

Ранее Генпрокуратура сообщала, что почти в 40 тыс. случаев жертвами киберпреступлений стали пенсионеры, еще в 3,3 тыс. – несовершеннолетние, в 1,4 тыс. случаев – инвалиды I и II групп[5].

Чаще всего злоумышленники атаковали госучреждения, промышленные компании и организации в сфере науки и образования. Основным мотивом в атаках как на организации, так и на частных лиц остается получение данных. Главными целями злоумышленников являются персональные и учетные данные, а при атаках на организации к ним добавляется еще и коммерческая тайна.

Следует согласиться с мнением Д.В. Жмурова, что «тотальное распространение интернета, его симбиоз с системами жизнеобеспечения общества добавят к списку кибержертв даже тех, кто не является пользователями виртуальных сетей»[6]. Таким образом, проблема обеспечения кибербезопасности сегодня выходит на первый план.

Для начала следует определиться с понятием жертвы киберпреступлений. Традиционно под жертвой преступления понимается лицо, которому причинен вред, ущерб в результате совершения преступления. Жертва – это всегда лицо, пострадавшее от преступления. Вред может быть физический, психологический, моральный, экономический и т.д. Но в любом случае жертва – это субъект, подвергшийся противоправному влиянию и пострадавший в результате преступных действий.

О.Б. Бовть отмечает, что кибержертва – это «лица или группы людей, подвергшиеся кибервиктимизации, то есть пострадавшие от информационно-психологического кибервоздействия»[7]. Д.В. Жмуров под кибержертвой предлагает рассматривать организацию, группу или человека, пострадавших от уголовно-наказуемых актов, реализованных преимущественно в цифровой среде[8].

---

[1] Жмуров Д.В. Кибервиктимология как новая реальность технотронного общества (гендерное исследование) // Электронный научный журнал Байкальского государственного университета. 2020. Т. 11, № 1.

[2] Бовть О.Б. Кибервиктимология: мультидисциплинарность и перспективы развития. Грантовая научно-исследовательская и научно-образовательная деятельность: цели, технологии, результаты. Ростов-на-Дону, 2017.

[3] URL: https://d-russia.ru/komitet-gosdumy-privjol-dannye-statistiki-o-kiberprestuplenijah.html

[4] URL: https://www.forbes.ru/biznes/457481-restoratory-rasskazali-o-vynuzdennom-otkaze-ot-importnyh-produktov

[5] URL: https://d-russia.ru/komitet-gosdumy-privjol-dannye-statistiki-o-kiberprestuplenijah.html

[6] Жмуров Д.Б. Кибервиктимология. Грядущая неизбежность. Академический юридический журнал. 2021. Т. 22, № 1. С. 26.

[7] Бовть О.Б. Кибервиктимология: мультидисциплинарность и перспективы развития. Грантовая научно-исследовательская и научно-образовательная деятельность: цели, технологии, результаты. Ростов/н Д., 2017.

[8] Жмуров Д.В. Кибержертва: решение проблемы терминологической неопределенности // Вестник Восточно-Сибирского института МВД России. 2(97) 2021.

Можно предложить и такое определение «кибержертвы» - это лицо, которому причинен вред в результате преступных действий с использованием цифровых технологий. В данном случае акцент сделан именно на способе причинения вреда. Речь идет об использовании преступником различного рода информационных технологий (это может быть как киберпространство, так и различного рода цифровые устройства).

Одним из признаков жертвы выступает тот факт, что лицу всегда причиняется вред. Иначе рассматривать в качестве жертвы мы его не можем. Но рядом ученых отмечается тот факт, что «кибержертва не всегда «страдающая» или «претерпевающая». В ряде случаев наносимый вред минимален, нераспознаваем, неочевиден даже для самого потерпевшего[9]. Здесь, наверное, стоит не согласиться с данным мнением. Если вред минимален и нераспознаваем для лица, то на каком основании он будет являться жертвой? Отсутствие вреда свидетельствует и об отсутствии преступления. В данном случае будет отсутствовать такой признак преступления, как его общественная опасность. Если лицо извлекает какую-либо выгоду, используя цифровые технологии, не причиняя при этом вреда, то данные действия не целесообразно рассматривать в качестве преступлений (речь идет о, так называемом, майнинге). Представляется, что жертва киберпреступлений – это лицо, которому всегда причиняется вред в результате совершения преступления с использованием информационных технологий.

Следует отметить, что большинство киберпреступлений по своему содержанию и направленности вреда мало чем отличаются от ранее совершаемых преступлений. Клевета, нарушение неприкосновенности частной жизни лица, посягательства на коммерческую, налоговую и банковскую тайны, хищения - все эти преступления существовали и раньше, но сейчас они в основном совершаются с использованием информационно-телекоммуникационных сетей. Основное отличие на сегодняшний день заключается в способе воздействия на охраняемые объекты, в качестве которых преступники выбирают цифровые технологии. В связи с чем большинство жертв преступлений по своим психологическим характеристикам мало чем отличаются от жертв иных преступлений.

Основной особенностью кибержертв выступает активное использование ими информационных технологий и зачастую пренебрежительное отношение к средствам и способам защиты информации.

Традиционно большая часть киберпреступлений носит корыстную направленность и в основном выражается в хищении денежных средств. В частности, количество заявлений о мошенничестве выросло на 5,1 %, превысив 249 тыс. Однако количество заявлений о возбуждении уголовных дел в связи с компьютерными преступлениями со взломом сократилось на 10,6 %, до 157 тыс.

По данным официальной статистики, в России из-за пандемии в 1,5 раза выросло число ИТ-преступлений. По словам В.А.Колокольцева, министра внутренних дел основную часть таких правонарушений составляет мошенничество. За шесть месяцев 2021 года зарегистрировано свыше 84 тыс. ИТ-краж (+11,1 % по сравнению с аналогичным периодом прошлого года) и свыше 117 тыс. ИТ-мошенничеств (+12,8 %) - сообщил замминистра внутренних дел РФ, начальник Следственного департамента МВД РФ, генерал-лейтенант юстиции Сергей Лебедев.

С массовым распространением информационно-телекоммуникационных систем, активным внедрением цифровых технологий естественным образом видоизменяются и способы совершения преступлений. На сегодняшний день денежный оборот в основном осуществляется в безналичной форме. Согласно данным Центробанка, на исходе 9 мес. 2021 г. на руках у населения было 325,1 млн платёжных карт. На каждого гражданина страны приходится больше двух штук, и эта цифра постоянно растёт. Помимо этого, существуют еще локальные платежные системы, электронные деньги и т. д. Таким образом, преступники вынуждены перепрофилировать свои способы изъятия денежных средств, исходя из особенностей их электронной формы.

В связи с этим особый интерес представляют именно жертвы хищений, совершенных с применением IT-технологий.

На сегодняшний день преступники активно используют как относительно новые технические способы хищения, связанные с неправомерным доступом к компьютерной информации (взломы, подбор паролей, использование вредоносных программ и т.д.), так и традиционные способы, связанные с обманом жертвы, введением ее в заблуждение, в результате чего жертва сама переводит денежные средства мошенникам или сообщает им свои данные, с помощью которых уже идет незаконное списание денежных средств с их счетов.

[9] Жмуров Д.В. Кибервиктимология как новая категория виктимологии постмодерна. Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. № 2. С. 118.

Условно можно выделить два типа жертв в зависимости от способа изъятия денежных средств: жертвы технического воздействия и жертвы информационного воздействия.

Для первого типа жертв характерно активное использование электронных систем платежей, внедрение новых информационных технологий в сфере оплаты товаров, услуг, как правило, приобретаемых через маркетплейсы, интернет-ресурсы с активным использованием сервисов заказов и т. д. Это молодые, активные люди, пользующиеся современными достижениями информационного пространства, владеющие навыками работы с информационными ресурсами и техническими средствами. Им удобно использовать новейшие достижения, не выходя из дома заказывать продукты, товары, оплачивать счета, переводить деньги, пользоваться бонусами и скидками. Но для данного типа жертв основным виктимологическим фактором выступает достаточно легкомысленное поведение в сфере обеспечения компьютерной безопасности и безопасности своих электронных денежных средств. Их уверенность в собственных знаниях, нежелание совершать дополнительные действия по проверкам электронных ресурсов, стереотипы поведения в информационной среде, активное использование различных ресурсов, где они оставляют о себе информацию, делают их уязвимыми для мошенников.

Второй тип жертвы практически ничем не отличается от жертв обычных мошенничеств. Следует отметить, что в данном случае речь идет не о каких-то специфических особенностях кибержертв, а об особенностях личности потерпевшего от мошеннических действий. Для второго типа жертв мошенничества, независимо от сферы его совершения, характерна чрезмерная доверчивость, небрежность и легкомысленность. Достаточно частым аспектом в поведении жертвы выступает корыстная направленность (приобрести товар дешевле, обойти системы дополнительных платежей, избавиться от затрат и т.д.). Они легко поддаются влиянию, внушаемы, для них характерно стремление получить максимальную выгоду с минимальными затратами.

Согласно статистике, именно второй тип жертв преобладает в общей структуре киберхищений. Это обусловлено прежде всего тем, что для мошенников работать с такими жертвами гораздо проще и удобнее, не требуется особых навыков программирования, технических характеристик оборудования. При данном виде мошенничества для преступников ничего не меняется, кроме того, что нет прямого контакта с жертвой, а связь осуществляется через технические устройства (телефоны, планшеты, смартфоны и т.д.).

«Социальная инженерия» - термин, получающий широкое распространение в контексте информационной безопасности. Речи идет о психологическом манипулировании людьми с целью получения конфиденциальной информации с последующим ее использованием при совершении хищений. Намного проще получить пароли, логины путем обмана, нежели взламывать системы безопасности. Существуют различные способы и техники обмана. Самыми распространенными являются фишинг, несуществующие ссылки, претекстинг и др.

Немаловажную роль для выбора жертвы играют такие характеристики личности потерпевших от киберпреступлений, как демонстративность, открытость, тщеславие. Потенциальные жертвы сами выкладывают всю информацию о себе в открытый доступ, привлекая внимание не только подписчиков, но и мошенников.

По мнению Сафуанова Ф.С., жертвы противоправных посягательств в Интернете имеют специфический симптомокомплекс индивидуально-психологических особенностей, включающий беспокойство, неуверенность в себе, подверженность настроению, неусидчивость, неустойчивость настроения, гневливость и определенные способы совладания и психологической защиты в психотравмирующих ситуациях: поиск эмоциональной социальной поддержки, фокусировку на эмоциях, самоограничение и проекцию[10].

Для кибермошенничеств в меньшей мере характерна личная взаимосвязь с жертвой. Нет прямого контакта, что делает процесс мошенничества более безопасным для преступника. Действия преступника зачастую носят более агрессивный характер. Жертвы таких преступлений легко внушаемые, поддающиеся влиянию. Интернет-пространство создает широкое поле деятельности для мошенников, упрощая им работу в поиске информации о жертве. По информации, содержащейся в социальных сетях, группах, форумах и т.д. можно изучить личность потенциальных потерпевших, их социально-

[10] Портал психологических изданий PsyJournals.ru. URL: https://psyjournals.ru/psyandlaw/2015/n4/Safuanov_Dokuchaeva_full.shtml [Особенности личности жертв противоправных посягательств в Интернете -–Психология и право. 2015. Т. 5, № 4.]

психологические характеристики, уровень материального благосостояния, увлечения, интересы и т.д. Мошенники, изучив личность потенциальной жертвы, ее увлечения, интересы, взгляды легко могут манипулировать этим и использовать для совершения своих противоправных действий. Наверное, социальным сетям и различного рода интернет-площадкам необходимо предупреждать своих пользователей о возможном использовании информации в преступных целях и рекомендовать лицам либо ограничивать круг лиц, имеющих доступ к данным, содержащимся в их профиле, либо предусматривать технические возможности для блокирования доступа.

Особую озабоченность вызывают проблемы информационного влияния на подрастающее поколение. К сожалению, следует констатировать, что большую часть своего свободного времени подростки проводят в сети Интернет и используют различного рода технические средства. Необходимо вести разъяснительную работу прежде всего с подрастающим поколением, формировать у них навыки безопасного пользования Интернетом. Уроки информатики должны обучать не только основам программирования и основам информационно-телекоммуникационных сетей, но и безопасному их использованию. Причем речь идет не только о технической защите своих ресурсов, но и о правовой, психологической, моральной, экономической безопасности ребенка.

Также немаловажным фактором выступает компьютерная грамотность жертвы. Чем выше компьютерная грамотность населения, тем меньше должно быть преступлений в этой сфере. Но это в большей степени касается мошенничества в сфере компьютерной информации, где определяющим фактором является профессионализм мошенника и недостаточная система защиты владельцев денежных средств либо банков.

Безусловно, что основной акцент профилактических мероприятий должен быть сделан прежде всего на технической безопасности ресурсов. Вообще, если говорить о киберпреступности, то основная проблема борьбы с ней заключается в техническом противодействии. Чем выше уровень защиты информации, тем меньше возможностей у преступников.

Здесь следует работать в двух направлениях. Во-первых, это активно разрабатывать и внедрять новейшие средства и способы защиты информации, ориентированные на создание условий, при которых невозможно взломать системы защиты и осуществить неправомерный доступ к охраняемой компьютерной информации. Естественно, что данное направление может быть реализовано только высококвалифицированными специалистами, обладающими навыками программирования.

Второе направление ориентировано на информирование граждан о существующих технических способах защиты своей информации и обеспечении им возможности установить эти средства защиты на свои носители. Это возможно путем активного внедрения в образовательные процессы дисциплин, ориентированных на освоение навыков безопасного пользования компьютерной информацией. Необходимо повышать уровень цифровой грамотности населения и начинать это нужно со школьного образования. Кроме того, следует создать интернет-площадку, где лица могли бы получать информацию о новых средствах и способах защиты от преступных посягательств с возможностью бесплатного установления программного обеспечения на свои компьютеры.

Самыми незащищенными группами по-прежнему остаются пенсионеры и пожилые люди. Современные реалии заставляют их использовать информационные ресурсы, но, к сожалению, у большинства пожилых людей отсутствуют даже самые элементарные навыки работы с компьютерами и информационными системами. Хотелось бы отметить, что в Удмуртской Республике регулярно проводятся бесплатные обучающие курсы для пенсионеров, инвалидов и лиц предпенсионного возраста. Для пенсионеров, желающих не отставать от современной жизни, Региональное отделение Общероссийской общественной организации «Союз пенсионеров России» в Удмуртской Республике, Отделение Пенсионного Фонда РФ по УР и Университет «третьего возраста» проводят обучение по программе «Основы компьютерной грамотности». Учебный план программы рассчитан на 1 месяц и предусматривает изучение основ работы на компьютере и практическое использование интернет-ресурсов. Средства на обучение были выделены Общероссийской общественной организацией «Союз пенсионеров России».

В настоящий момент времени необходимо использовать различные информационные ресурсы для оповещения граждан о новых способах мошенничества и краж. Данная деятельность должна носить массовый характер и исходить как от правоохранительных органов, так и от финансовых организаций (банков, страховых компаний). Следует отметить, что правоохранительные органы регулярно оповещают граждан о новых способах мошеннических действий в сети Интернет, также имеются

и различного рода печатные материалы, содержащие информацию о мерах виктимологической профилактики, проводимой ОВД. Достаточно активно используются мессенджеры и социальные сети для информирования граждан о новых угрозах. Также немаловажный вклад в борьбу с кибермошенничеством вносят общественные организации, отельные граждане. Примером может служить сайт «Антимошенник», содержащий обширную базу мошенников, которая постоянно обновляется. Данный ресурс может помочь выявить нечестных продавцов и покупателей на просторах интернета и защитить отдельных граждан от преступников. Стоит лишь предварительно проверить своего контрагента по имеющимся базам данных.

Проблема виктимологической профилактики кибермошенничества связана прежде всего с работой с населением.

Одной из проблем виктимологической профилактики киберхищений является недоверие граждан к правоохранительным органам. К сожалению, следует отметить, что на сегодняшний день существует серьезные проблемы в части квалификации сотрудников, занимающихся расследованием преступлений в сфере компьютерной информации. Представляется, что одним из требований к таким сотрудникам должно выступать наличие у них двух образований – юридического и специалиста в области IT-технологий. Без комплексного подхода к расследованию таких преступлений нельзя эффективно бороться с киберпреступностью. Поэтому и раскрываемость компьютерных преступлений очень низкая. Большинство из подобного рода преступлений можно выявить и раскрыть достаточно быстро при условии быстрого реагирования потерпевшего и обращения его в правоохранительные органы. Преступник, совершая свои противоправные действия через систему Интернет, всегда оставляет там следы, по которым его можно найти. Денежные средства, которые списывают со счетов потерпевших, поступают на другие счета, которые можно заблокировать и остановить транзакции, тем самым предотвратить причинение ущерба собственнику.

В заключении следует отметить, что, несмотря на развитие новых технологий и активное внедрение во все сферы жизнедеятельности человека цифровых систем, принципы, содержание мошенничества остаются прежними. Меняются лишь способы обмана, активно используются новые технологии, но преступники по-прежнему используют человеческие слабости и психологические особенности личности потерпевших. А с учетом современных технических возможностей преступникам стало легче получать информацию о жертвах без особых рисков быть разоблаченными.

СПИСОК ЛИТЕРАТУРЫ

1. Бовть О.Б. Кибервиктимология: мультидисциплинарность и перспективы развития // Грантовая научно-исследовательская и научно-образовательная деятельность: цели, технологии, результаты / отв. ред. О.П. Чигишева. Ростов-н/Д., 2017. С. 5-32.
2. Жмуров Д.В. Кибервиктимология как новая категория виктимологии постмодерна // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. № 2. С. 118.
3. Жмуров Д.В. Кибервиткимология. Грядущая неизбежность // Академический юридический журнал. 2021. Т. 22, № 1. С. 26.
4. Жмуров Д.В. Кибержертва: решение проблемы терминологической неопределенности // Вестник Восточно-Сибирского института МВД России. 2021. 2(97).
5. Жмуров Д.В. Кибервиктимология как новая реальность технотронного общества (гендерное исследование) // Электронный научный журнал Байкальского государственного университета. 2020. Т. 11, № 1.

Поступила в редакцию 12.04.2022

Стяжкина Светлана Александровна, кандидат юридических наук,
доцент кафедры уголовного права и криминологии
ФГБОУ ВО «Удмуртский государственный университет»
426034, Россия, г. Ижевск, ул. Университетская, 1 (корп. 4)
E-mail: styazhkina.sv@yandex.ru

S.A. Styazhkina

VICTIMOLOGICAL PREVENTION OF CYBER-ATTACKS

DOI: 10.35634/2412-9593-2022-32-3-546-552

The problem of countering cybercrime today is one of the leading positions in the world. The peculiarity of this problem is its versatility and multi-aspect. To effectively combat this relatively new type of crime, it is necessary to combine the efforts of representatives of various fields of activity (legal, technical, psychological, social, etc.). The society has moved to a new stage of development, completely different, requiring a comprehensive approach in regulating the emerging social relations. Informatization and cybernetization of all processes of human and social life activity presupposes an adequate response from the state in terms of protecting and ensuring the safety of individuals in the new digital space. The article reveals the current issues of countering cyber-theft. The concept of cyber-victim is analyzed, its signs are revealed. The paper proposes the author's classification of fraud victims taking into account this classification, the socio-psychological features of different types of victims of cyber attacks are revealed. Measures of victimological prevention of cybercrime are proposed. The paper contains examples of the activities of state authorities and public associations in the field of countering cybercrime.

Keywords: cyber-victimology, cyber-victimization, fraud in the field of computer information, victimology, victimological prevention, information technology, crime.

Received 12.04.2022

Styazhkina S.A., Candidate of Law, Associate Professor
Udmurt State University
Universitetskaya st., 1/4, Izhevsk, Russia, 426034
E-mail: styazhkina.sv@yandex.ru