Научная статья
УДК 343.988
https://doi.org/10.36511/2078-5356-2022-4-135-142

Общая виктимологическая профилактика киберпреступности

Жмуров Дмитрий Витальевич
Байкальский государственный университет, Иркутск, Россия, zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X

Аннотация. Статья посвящена анализу общих мер виктимологической профилактики киберпреступности. В работе предложено определение указанных мероприятий, перечисляются их основные признаки и целевые параметры. Исходя из проведенного анализа научной литературы и законодательных источников автором выделены следующие уровни виктимологической превенции: 1) легальный (формирование виктимологического законодательства); 2) академический (активизация виктимологических исследований); 3) институциональный (администрирование и организация процессов виктимологической превенции в цифровой среде), последний, в свою очередь, предполагает несколько базисных основ: организационную, информационную, дидактическую, координационную, процедурную; 4) технический (внедрение перспективных разработок, направленных на девиктимизацию субъектов информационно-технологического мира); 5) идеологический (выработка системы идей и взглядов, в которых осознаются отношения людей, как субъектов виртуальной жизни, способных пострадать от правонарушений). Каждый из указанных уровней является базовой функциональной частью общей виктимологической превенции в информационно-телекоммуникационном пространстве.

***Ключевые слова*:** кибервиктимизация, жертвы в интернете, кибервиктимность, кибервиктимология, интернет-потерпевший

Для цитирования: Жмуров Д. В. Общая виктимологическая профилактика киберпреступности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 135—142. https://doi.org/10.36511/2078-5356-2022-4-135-142.

Original article

Measures of general victimological prevention of cybercrime

Dmitry V. Zhmurov
Baikal State University, Irkutsk, Russian Federation, zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X

Abstract. The article is devoted to the analysis of general measures of victimological prevention of cybercrime. The paper proposes a definition of these measures, lists their main features and target parameters. Based on the analysis of scientific literature and legislative sources, the author identifies the following levels of victimological prevention: 1) legal (formation of victimological legislation); 2) academic (activation of victimological research); 3) institutional (administration and organization of victimological prevention processes in the digital environment), the latter, in turn, understands several basic foundations: organizational, informational, didactic, coordination, procedural; 4) technical (introduction of advanced developments aimed at the devictimization of the subjects of the information and technological world); 5) ideological (development of a system of ideas and views in which the relations of people as subjects of virtual life, capable of suffering from offenses, are realized). Each of these levels is a basic functional part of the general victim prevention in the information and telecommunications space.

***Keywords*:** cybervictimization, victims on the Internet, cybervictimity, cybervictimolet victimogy, Intern

For citation: Zhmurov D. V. Measures of general victimological prevention of cybercrime. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2022, no. 4 (60), pp. 135—142. (In Russ.). https://doi.org/10.36511/2078-5356-2022-4-135-142.

Виктимологическая профилактика кибержертв — весьма сложная задача. И сейчас, к сожалению, она не в приоритете. В последние годы государство предприняло немалое число инициатив, направленных на профилактику IT-преступности, при этом не всегда учитывая виктимологический аспект проблемы. Так, проделана значительная работа по подготовке и введению в действие комплекса законов о защите критической информационной инфраструктуры, внедрению Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, создания Центра мониторинга и реагирования на компьютерные атаки («ФнЦЕРТ»), а также Национального координационного центра по компьютерным инцидентам (НКЦКИ), как части сил, направляемых на предупреждение и ликвидацию последствий компьютерных инцидентов [1]. Очевидно, что основные ресурсы отнимает насущная «борьба» с киберпреступностью, в то время как работа с ее жертвами представляется чем-то второстепенным и малозначимым. В условиях дефицита средств, времени и квалифицированных кадров — это выглядит вполне логично. Действительно, нужно ли заниматься киберпотерпевшими, когда еще с интернет-преступниками имеется множество проблем?

Несмотря на эти, казалось бы, убедительные аргументы, недооценивать виктимологический компонент профилактики не совсем правильно. Парадигма виктимологии зиждется на идее о том, что потерпевшего можно сделать союзником правоохранительных органов, принимающим участие в деле предупреждения преступности. Иными словами, нужно дать ему в руки инструменты профилактики и мотивировать ими пользоваться, минимизируя при этом контрольно-карательную роль государства. Это обоснованно с точки зрения снижения затрат, уменьшения числа профилактических усилий и криминальных рисков, а в конечном итоге, служит целям экономии уголовной репрессии. Ведь лучше предупреждать преступления, чем карать за них (Ч. Беккария).

Конечной целью указанных мер является достижение относительно приемлемого уровня виктимологической безопасности в виртуальном пространстве.

Последняя понимается как состояние защищенности лиц (наиболее уязвимых категорий) от всевозможных угроз в веб-континууме, в том числе криминального характера. Достижение этой цели обеспечивается государством, его многочисленными субъектами посредством снижения виктимности участников виртуальной коммуникации, а также ослабления негативного влияния виктимогенных факторов, путем внедрения и применения мер, выработанных киберВиктимологией. О целесообразности виктимологической профилактики киберпреступности в своих работах неоднократно высказывались А. И. Бастрыкин [2], Е. А. Родина [3], С. М. Миронова, С. С. Симонова [4], С. А. Стяжкина [5], А. П. Суходолов, Л. А. Колпакова, Б. А. Спасенников [6].

Под виктимологической профилактикой на общесоциальном уровне понимается деятельность, направленная на устранение и нейтрализацию факторов, способствующих виктимизации общества, сокращению показателей массовой виктимности граждан [7; 8]. Профилактика при этом затрагивает различные общественные сферы: информационную, правовую, политическую, нравственную, экономическую и проч. А ее объектом является «абстрактный» индивид, независимо от степени индивидуальной виктимности, то есть все граждане государства как совокупность возможных жертв.

Таким образом, следует указать на несколько отличительных признаков общей виктимологической профилактики в контексте представленной темы:

— направлена на неограниченный и неперсонифицированный круг лиц, являющихся потенциальными жертвами киберпреступлений;

— носит перманентный и устойчивый характер, не являясь сиюминутной и единоразовой формой деятельности;

— оказывает глобальное воздействие на всю социальную сферу.

Исходя из вышесказанного, перечислим основные уровни общей виктимологической профилактики.

1. ***Легальный*** (формирование виктимологического законодательства). Это связано с необходимостью корректировки национальной правовой базы для повышения эффективности работы с жертвами киберпреступлений.

Необходимо артикулировать важность проблемы киберпотерпевших на уровне Стратегии национальной безопасности Российской Федерации (в разделе «Информационная безопасность») [9], доктрине информационной безопасности Российской Федерации [10] или «Концепции плана действий и инструментария в вопросах противодействия кибервызовам и угрозам» [11].

Назрела потребность в разработке национальной стратегии борьбы с киберпреступностью.

О необходимости подобной программы, основанной на прогнозировании ситуации, учете потенциальных рисков для общества и государства, высказался Президент Российской Федерации В. Путин [12]. Содержание указанной стратегии окажется неполным без виктимологического раздела «Об основах виртуальной безопасности личности и жертвах киберпреступлений». Там следует отразить ключевые аспекты многоуровневой системы виктимологической профилактики, заложить ее терминологическую базу (например, предусмотреть дефиниции кибержертвы, киберинцидента, киберугрозы и прочих), обозначить особенности правового статуса интернет-потерпевших, а также цели и направления государственной политики по отношению к данной категории лиц; предоставляемые им гарантии.

Немаловажной представляется работа по совершенствованию и своевременной актуализации уголовного и административного законодательства в соответствии с реалиями цифрового мира.

Законодатель не всегда успевает отражать в нормативной базе весь спектр современных компьютерных нарушений, таких, например, как скрытый майнинг, DDoS-атаки, воровство игрового инвентаря (имеющего реальную стоимость), кибербуллинг и проч. Решение указанных задач позволило бы повысить эффективность защиты прав лиц, пострадавших от киберпреступлений. Кроме того, некоторые специалисты высказывают мнение о необходимости усиления уголовной ответственности за ряд компьютерных преступлений. Так, по статье 272 УК РФ «Неправомерный доступ к компьютерной информации» максимальный срок наказания составляет до семи, а по совокупности приговоров — до десяти лет, тогда как в практике США по Закону «О мошенничестве и злоупотреблении с использованием компьютеров» (*Computer Fraud and Abuse Act*) за повторное киберпреступление может быть назначено тюремное заключение сроком до 20 лет, а за проникновение в компьютеры государственной инфраструктуры — до 30 лет лишения свободы без права досрочного освобождения [13]. Следовательно, потенциал квалификации компьютерных преступлений не должен исключать вероятности признания их тяжкими или особо тяжкими. Настоятельно требуют решения вопросы ответственности поставщиков услуг хостинга, поисковых машин, введения солидарной ответственности ресурсов за размещаемые на них гиперссылки.

Нельзя не отметить важность изменений процессуального законодательства, регулирующего вопросы собирания и фиксации цифровых доказательства (информационных источников). Уже сегодня высказываются мнения о том, что назрела необходимость введения «цифровой информации» в качестве нового вида источников доказательств [14].

На основе регулярной новеллизации нормативных источников выглядит разумным дополнение методических рекомендаций по выявлению и расследованию киберпреступлений (в методических материалах Следственного комитета), рекомендаций по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (для сотрудников прокуратуры) [15].

2. ***Академический*** (активизация виктимологических исследований). Предполагает диверсификацию изыскательской деятельности научно-исследовательских институтов (ВНИИ МВД, НИИ университета прокуратуры Российской Федерации, института государства права РАН, философии и права РАН и др.), независимых ученых в рамках грантовой поддержки. Виктимологические риски киберпреступности требуют оценки на должном научно-аналитическом уровне, учитывая вероятность их реализации и формат возможных последствий. Перед научным сообществом выдвигается ряд серьезных задач:

— формирование теоретической модели цифровой виктимности и кибервиктимологии как междисциплинарной области ее исследующей;

— описание и классификация угроз информационного пространства;

— разработка методик их обнаружения, идентификации и предотвращения;

— выявление причин и условий кибервиктимизации (на общесоциальном и индивидуальном уровнях);

— изучение личности кибержертвы и потенциала воздействия на нее;

— исследование и оценка поствиктимного поведения потерпевших;

— проведение комплексного анализа проблем безопасности (с виктимологической точки зрения) как существующих, так и будущих цифровых сервисов;

— разработка основ цифровой психовиктимологической экспертизы, направленной на установление связей между виктимным поведением человека и причиняемым ему вредом;

— создание прогнозных моделей, направленных на оценку масштабов кибервиктимизации и опасности влекомых ею последствий.

Указанные инициативы, в конечном счете, позволят актуализировать средства и методы обеспечения кибербезопасности на концептуальном (теоретическом) уровне. Понимание процессов детерминации виктимности в интернете позволит обратить внимание на конкретные факторы и попытаться их корректировать, исследование личности потерпевшего позволит создать средства индивидуальной виктимологической профилактики, основанные на использовании искусственного интеллекта.

3. ***Институциональный*** (администрирование и организация процессов виктимологической превенции в цифровой среде). Предполагает создание и обеспечение работоспособности систем, направленных на выявление (предупреждение) виктимогенных ситуаций в киберпространстве. Важна ориентировка на реализацию мероприятий, благодаря которым обеспечиваются:

— *организационные основы виктимологической безопасности*. Их реализация предполагает создание органов, межведомственных (межправительственных) структур, обеспечивающих учет и реагирование по фактам виктимизации в цифровом пространстве. Например, на базе Национального координационного центра по компьютерным инцидентам (НКЦКИ) может функционировать Единый центр кибервиктимизации и защиты жертв киберпреступлений (ЕЦК). Его основными задачами видятся: фиксация численности кибержертв; оценка вредоносного воздействия на них; обеспечение взаимодействия с правоохранительными органами (выработка скриптов обращения в правоохранительные органы, а также других юридически значимых действий, направленных на защиту цифровых прав); поддержка межведомственного взаимодействия при расследовании транснациональных и межрегиональных киберпреступлений; методическое обеспечение виктимологической профилактики компьютерных преступлений; проведение удаленных судебно-виктимологических экспертиз; оказание правовой и консультационной помощи кибержертвам.

В рамках организационного обеспечения виктимологической безопасности нельзя обойти вниманием кадровую политику организаций. К примеру, кажется важным, чтобы государственные или частные компании, занятые в критически важных отраслях, принимали на аутсорсинг или вводили в штатное расписание должность главного сотрудника по информационной безопасности (*CISO*) или группу реагирования на компьютерные инциденты (*CERT*), отвечающих за инициативы в области кибербезопасности. Это положение должно стать неотъемлемой частью стандартов кадрового менеджмента.

Своевременными выглядят предложения о закреплении единых стандартов сотрудничества субъектов информационного общества — личности, организаций и государства — в области обеспечения кибербезопасности [16]. Ее обеспечение требует развития централизованного электронного правительства с безопасной системой аутентификации, сводящего воедино все социальные сервисы и бюрократические институты. Последнее гарантирует высокий уровень защиты информации, ее сохранность, единое окно доступа к государственным услугам и позволит избежать преступных злоупотреблений. Звучат мнения о разумности создания наднациональных органов, регулирующих цифровую жизнь человечества. Например, международной организации с региональными представительствами по образу ООН в киберпространстве — КиберООН, включающую несколько структур в числе которых мог быть учрежден фонд (комиссия) по защите прав киберпотерпевших [16];

— *процедурные основы виктимологической безопасности* предполагают разработку и внедрение системы сценариев реагирования на виктимизацию граждан в интернете. Это связано с обязательствами по регистрации заявлений кибержертвы, инициацией уголовного преследования, созданием механизма обратной связи с потерпевшими (например, посредством виктимологической экспертизы системы уголовного правосудия, где оценивались бы критерии удовлетворенности потерпевших после обращения за помощью). Имеет значение модификация особенностей статистического учета киберпреступлений с отражением в нем позиций, относящихся к потерпевшим. В контексте преступлений, совершаемых в виртуальной среде, это представляется важным, поскольку позволит получить сведения о дополнительных рисках, возникающих при использовании интернета, и учитывать их в дальнейшем, например, при страховании интернет виктимизации.

В системе управления организаций коммерческого и государственного сектора необходимо внедрение риск-ориентированных подходов к безопасности. Ключевыми здесь могут стать методы управления цифровыми рисками [17]. К примеру, при появлении новых форм

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2022, no. 4 (60)

киберпреступлений необходимо создание планов антикризисного регулирования, которые можно задействовать в сжатые сроки. Аналогичные руководства должны быть проработаны на случай непредвиденных последствий компьютерных атак, глобальных вмешательств в национальный сегмент интернета. Это так называемые планы восстановления после сбоев и механизмы защиты ключевых информационных инфраструктур [18].

Процедурные аспекты являются действенными не только на государственном уровне. Механизмы защиты кибержертвы могут исполняться в действиях по развитию страхового рынка в интернете (страхование персональной информации, бизнес-процессов, активов, виртуальной личности); введении регламентов провайдерских услуг, предусматривающих обязательный набор защитных механизмов для клиента; выполнении социальными сетями принятых на себя обязательств по пресечению киберинцидентов и т. п.;

— *информационные основы виктимологической безопасности* подразумевают выработку проактивных механизмов защиты потенциальной кибержертвы. Они выражаются в требовании к разработке единых стандартов политики информационной безопасности; организации мониторинга виктимологической ситуации в стране; проведении прикладных социологических исследований по материалам уголовных дел и в рамках изучения общественного мнения; создании информационного банка данных об интернет-потерпевших [19], формировании государственного реестра кибернетических рисков и прочего;

— *дидактические основы виктимологической безопасности* направлены на контрвиктимное обучение населения. Это одна из форм развития человеческих ресурсов через использование образовательных и учебных программ. Главная ее цель — получение навыков избегания виктимогенных ситуаций.

Деятельность подобного рода оценивается как одна из стратегий информационной безопасности, снижающая риски киберпреступности [20]. Указанный контекст не должен исчерпываться традиционными виктимологическими практиками, включающими: составление всевозможных памяток потенциальным жертвам, извещение граждан через средства массовой информации о совершенных фактах преступлений и т. п. [21]. Необходимо длительное обучение и приобретение устойчивых навыков безопасного поведения, начиная со среднего образования. Одной из таких мер может быть введение в школьную программу курса «Основы кибербезопасности» (5—11 класс) [22], а в учебный план ВУЗов дисциплин «Цифровая криминология» и «Кибервиктимология». Помимо этого, первостепенное значение имеет подготовка кадров в области кибербезопасности и защиты прав кибержертв. Обращает на себя внимание потребность во введении нового профессионального стандарта юриста с акцентом на цифровые компетенции. К сожалению, по состоянию на июнь 2022 года профессиональный стандарт юрисконсульта Министерством труда Российской Федерации утвержден не был [16]. Таким образом, главным назначением предложенных мер является формирование в обществе культуры безопасного киберповедения.

— *координационные основы виктимологической безопасности* исходят из обязательности международного сотрудничества при реализации указанных программ. Это требование естественно, поскольку необходимым условием является унифицированное понимание цифровых прав и свобод личности, создание единообразных механизмов их защиты, кооперация правоохранительных систем разных стран. Стандартизация подходов предполагает, что основы виктимологической профилактики киберпреступности должны быть отражены в международном законодательстве. Шагами в этом направлении являются «Глобальная программа кибербезопасности Международного союза электросвязи» или резолюция Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур». Такие меры необходимы для применения наднациональной юрисдикции; сохранения и использования компьютерной информации разных национальных сегментов веб-сети по уголовному делу, возбужденному в одной из стран; получения трансграничного доступа к данным; осуществления запросов о взаимной правовой помощи, экстрадиции преступников и многого другого.

4. ***Технический*** (внедрение перспективных разработок, направленных на девиктимизацию субъектов информационно-технологического мира). Так, предполагается, что определенный эффект может быть достигнут не только посредством работы с потенциальными потерпевшими, но и путем исправления программных ошибок, защиты информации, создания функциональных преград, затрудняющих процесс кибервиктимизации. Такая работа может быть

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2022, no. 4 (60)

выражена в обеспечении виктимологической защиты информации (криптография, распределенное хранение данных); протекции национальных сетей и правительственных ресурсов. В преференциях нуждается собственная школа прикладной математики, ведущая разработку средств криптографической защиты информации, криптологии, программируемых логических интегральных схем, квантовой криптографии и систем передачи, обработки и хранения информации [23]. Государственные органы в своей работе должны использовать продукцию преимущественно отечественной IT-отрасли.

Технический уровень виктимологической профилактики предполагает ряд важных моментов, которые нельзя оставить без внимания, а именно: идентификацию и аутентификацию субъектов доступа и объектов доступа; защиту машинных носителей информации; регистрацию событий безопасности; антивирусную защиту; обнаружение (предотвращение) вторжений; контроль (анализ) защищенности информации; целостность информационных систем и информации; доступность информации; защиту среды виртуализации; защиту технических средств; защиту информационной системы, ее средств, систем связи и передачи данных [23].

5. ***Идеологический*** (выработка системы идей и взглядов, в которых осознается важность виктимологической профилактики, места и роли жертвы в контроле над киберпреступностью). Идеологический уровень отражается в следующих тематических тезисах:

— отношение к пользователю как субъекту, наделенному цифровыми свободами и неприкосновенностью частной жизни в киберсреде;

— поддержка положений виктимологической идеологии, направленной на переориентацию общества исключительно с проблемы преступника на жертв киберпреступлений [24];

— поддержка, продвижение международных стандартов виктимологической безопасности, расширение межстранового сотрудничества в этой сфере при безусловном приоритете национальных цифровых решений (создания собственных виртуальных экосистем, антивирусного и иного программного обеспечения, контрвиктимных решений и др.);

— предпочтение активных политик информационной безопасности пассивным [25];

— укрепление нравственных основ общества и интернета, как его производной.

Таким образом, меры общей виктимологической профилактики киберпреступности направлены на переориентацию общественного сознания. Закрепляя и институционализируя представленные выше положения, мы, хотим того или нет, признаем, что виртуальная преступность стала одной из доминирующих проблем современного человечества. Указанные меры окажутся малоэффективными без коррелирующей связи с элементами индивидуальной виктимологической профилактики, которым суждено составить практическую суть превентивной политики в виртуальной среде.

Список источников

1. Кузнецов Н. В., Раков А. В. Управление в территориальных органах МВД России на районном уровне как основном звене системы МВД России // Вестник Удмуртского университета. 2021. № 5. С. 851—855.

2. Бастрыкин А. И. Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 5—12.

3. Родина Е. А. Виктимологическое предупреждение преступлений в киберпространстве // Актуальные проблемы государства и права. 2021. № 19. С. 510—524.

4. Миронова С. М., Симонова С. С. Защита прав и свобод несовершеннолетних в цифровом пространстве // Всероссийский криминологический журнал. 2020. Т. 14. № 2. С. 234—241

5. Стяжкина С. А. Виктимологическая профилактика кибермошенничества // Вестник Удмуртского университета. Серия «Экономика и право». 2002. № 3. С. 546—552.

6. Суходолов А. П., Колпакова Л. А., Спасенников Б. А. Проблемы противодействия преступности в сфере цифровой экономики // Всероссийский криминологический журнал. 2017. Т. 11. № 2. С. 258—267.

7. Коновалова И. А. Виктимологические аспекты предупреждения корыстных преступлений, совершаемые несовершеннолетними // Право и жизнь. 2013. № 5.

8. Савиных Е. В. Основные направления и проблемы виктимологической профилактики преступности // Виктимология. 2014. № 1 (1). С. 51—54.

9. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 2 июля 2021 года № 400 // Собрание законодательства РФ. 2021. № 27, ст. 5351.

10. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 года № 646 // Собрание законодательства РФ. 2016. № 50, ст. 7074.

11. О проекте Концепции плана действий и инструментария в вопросах противодействия кибервызовам и угрозам: постановление Парламентской Ассамблеи

Организации Договора о коллективной безопасности. М., 30 ноября 2020 года. № 13-5.4.

12. Путин призвал создать стратегию по борьбе с киберпреступностью. URL: https://ria.ru/20210224/putin-1598783523.html (дата обращения: 20.09.2022).

13. Зубова Е. Киберпреступлений становится все больше, однако их раскрываемость уменьшается. URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya (дата обращения: 20.09.2022).

14. Карташов И. И., Лесников О. А. Цифровая информация в уголовно-процессуальном доказывании: понятие и свойства // Наука. Общество. Государство. 2020. № 4 (32). С. 73—82.

15. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. URL: https://www.garant.ru/products/ipo/prime/doc/70542118/ (дата обращения: 20.09.2022).

16. Булай Ю. Г., Булай Р. И. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. № 1. С. 31—35.

17. Broadhurst R., Grabosky P., Alazab M., Chon S. Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime // International Journal of Cyber Criminology. 2014. Vol. 8. Iss. 1. Pp. 1—20.

18. Государственные стратегии кибербезопасности. URL: https://www.securitylab.ru/analytics/429498.php?R=1 (дата обращения: 20.09.2022).

19. Лелеков В. А., Щеголева А. Н. Информационно-аналитический аспект виктимологической профилактики преступности несовершеннолетних // Общество и право. 2008. № 1 (19).

20. Герке М. Понимание киберпреступности: Явление, задачи и законодательный ответ. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/CCL-R.pdf (дата обращения: 20.09.2022).

21. Будякова Т. П. Основы криминальной виктимологии: учебное пособие. Елец: Елецкий государственный университет имени И. А. Бунина, 2019. 86 с.

22. Вангородский С. Н. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы. М.: Дрофа, 2019. 238 с.

23. Луценко С. И. Политика Российской Федерации в области кибербезопасности. URL: http://digital-economy.ru/images/easyblog_articles/504/IB777.pdf (дата обращения: 20.09.22).

24. Окс Л. Е. Некоторые проблемы совершенствования правового обеспечения виктимологической профилактики преступлений // Российский следователь. 2009. № 5.

25. Казарин О. В., Тарасов А. А. Современные концепции кибербезопасности ведущих зарубежных государств // История и архивы. 2013. № 14 (115). С. 58—74.

References

1. Kuznetsov N. V., Rakov A.V. Management in the territorial bodies of the Ministry of Internal Affairs of Russia at the district level as the main link of the system of the Ministry of Internal Affairs of Russia. *Bulletin of the Udmurt University,* 2021, no. 5, pp. 851—855. (In Russ.)

2. Bastrykin A. I. Crimes against minors in the Internet space: on the issue of victimological prevention and criminal legal assessment. *All-Russian Criminological Journal*, 2017, vol. 11, no. 1, pp. 5—12. (In Russ.)

3. Rodina E. A. Victimological prevention of crimes in cyberspace. *Actual problems of state and law*, 2021, no. 19, pp. 510—524. (In Russ.)

4. Mironova S. M., Simonova S. S. Protection of the rights and freedoms of minors in the digital space. *All-Russian Criminological Journal*, 2020, vol. 14, no. 2, pp. 234—241. (In Russ.)

5. Styazhkina S. A. Victimological prevention of cyberbullying. *Bulletin of the Udmurt University. Series "Economics and Law"*, 2002, no. 3, pp. 546—552. (In Russ.)

6. Sukhodolov A. P., Kolpakova L. A., Spasennikov B. A. Problems of countering crime in the field of digital economy. *All-Russian Criminological Journal*, 2017, vol. 11, no. 2, pp. 258—267. (In Russ.)

7. Konovalova I. A. Victimological aspects of the prevention of capital crimes committed by minors. *Law and life*, 2013, no. 5. (In Russ.)

8. Savinykh E. V. Main directions and problems of victimological crime prevention. *Victimology*, 2014, no. 1 (1), pp. 51—54. (In Russ.)

9. On the National Security Strategy of the Russian Federation: decree of the President of the Russian Federation no. 400 of July 2, 2021. *Collection of legislative acts of the RF*, 2021, no. 27, art. 5351. (In Russ.)

10. On the approval of the Information Security Doctrine of the Russian Federation: decree of the President of the Russian Federation no. 646 of December 5, 2016. *Collection of legislative acts of the RF*, 2016, no. 50, art. 7074. (In Russ.)

11. On the Draft Concept of an Action Plan and an Instrument for countering cyber calls and threats: resolution of the Parliamentary Assembly of the Collective Security Treaty Organization. Moscow, 2020, November 30, no. 13-5.4. (In Russ.)

12. Putin called for the creation of a strategy to combat cybercrime. URL: https://ria.ru/20210224/putin-1598783523.html (accessed 20.09.2022). (In Russ.)

13. Zubova E. Cybercrimes are becoming more and more, but their disclosure is decreasing. URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya (accessed 20.09.2022). (In Russ.)

14. Kartashov I. I., Lesnikov O. A. Digital information in criminal procedural proof: concept and properties. *The science. Society. State,* 2020, no. 4 (32), pp. 73—82. (In Russ.)

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2022, no. 4 (60)

15. Methodological recommendations on the implementation of prosecutorial supervision over the execution of laws in the investigation of crimes in the field of computer information. URL: https://www.garant.ru/products/ipo/prime/doc/70542118/ (accessed 20.09.2022). (In Russ.)

16. Bulai Yu. G., Bulai R. I. Prevention and counteraction of cyber crime, as well as international cyber threats. *Academic Thought*, 2017, no. 1, pp. 31—35. (In Russ.)

17. Broadhurst R., Grabosky P., Alazab M., Chon S. Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, 2014, vol. 8, issue 1, pp. 1—20. (In Russ.)

18. State cybersecurity strategies. URL: https://www.securitylab.ru/analytics/429498.php?R=1 (accessed 20.09.2022). (In Russ.)

19. Lelekov V. A., Shchegoleva A. N. Information and analytical aspect of victimological prevention of juvenile delinquency. *Society and law*, 2008, no. 1 (19). (In Russ.)

20. Gerke M. Understanding cybercrime: Phenomenon, tasks and legal response. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/CCL-R.pdf (accessed 20.09.2022). (In Russ.)

21. Budyakova T. P. Fundamentals of criminal victimology: a textbook. Elec: *Yelets State University named I. A. Bunin*, 2019. 86 p. (In Russ.)

22. Vangorodsky S. N. Fundamentals of cybersecurity: an educational and methodological guide. Grades 5—11. Moscow: Drofa Publ., 2019. 238 p. (In Russ.)

23. Lutsenko S. I. The policy of the Russian Federation in the field of cyber security. URL: http://digital-economy.ru/images/easyblog_articles/504/IB777.pdf (accessed 20.09.2022). (In Russ.)

24. Oks L. E. Some problems of improving the legal support of victimological crime prevention. *Russian Investigator,* 2009, no. 5. (In Russ.)

25. Kazarin O. V., Tarasov A. A. Modern concepts of cyber-threats of leading foreign states. *History and archives,* 2013, no. 14 (115), pp. 58—74. (In Russ.)

Информация об авторе

Д. В. Жмуров — кандидат юридических наук, доцент.

Information about the author

D. V. Zhmurov — Candidate of Sciences (Law), Associate Professor.

Статья поступила в редакцию 10.10.2022; одобрена после рецензирования 30.11.2022; принята к публикации 01.12.2022.

The article was submitted 10.10.2022; approved after reviewing 30.11.2022; accepted for publication 01.12.2022.