АКТУАЛЬНЫЕ ПРОБЛЕМЫ ГОСУДАРСТВА И ПРАВА
2021. Т. 5. № 19 http://journals.tsutmb.ru/current-issues-of-the-state-and-law.html

AKTUAL'NYE PROBLEMY GOSUDARSTVA I PRAVA = CURRENT ISSUES OF THE STATE AND LAW
2021, vol. 5, no. 19 http://journals.tsutmb.ru/current-issues-of-the-state-and-law-eng.html
ISSN 2587-9340

Перечень ВАК, РИНЦ, CrossRef, НЭБ «eLIBRARY.RU», ЭБ «КиберЛенинка»

НАУЧНАЯ СТАТЬЯ
УДК 343.988
DOI 10.20310/2587-9340-2021-5-19-510-524
Шифр научной специальности 12.00.08

ВИКТИМОЛОГИЧЕСКОЕ ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ

Е.А. Родина[1,2]
[1]Урюпинская межрайонная прокуратура Волгоградской области
403113, Российская Федерация, Волгоградская обл., г. Урюпинск, Ульяновский пер., 2
[2]ФГБОУ ВО «Саратовская государственная юридическая академия»
410056, Российская Федерация, г. Саратов, ул. Вольская, 1
rodina-caterina2010@yandex.ru

Аннотация. Несмотря на усилия по совершенствованию уголовного законодательства, продолжается рост числа преступных посягательств, совершаемых в киберпространстве. Это предопределяет необходимость совершенствования мер предупреждения, в том числе и виктимологических. Цель работы: разработка комплекса мер виктимологической профилактики преступлений, совершаемых в киберпространстве. В числе применяемых методов диалектический метод научного познания, системный, структурный, сравнительно-правовой, контент-анализ. На основе анализа причин виктимизации пользователей в киберпространстве разработаны предложения по комплексу мер виктимологической профилактики, включая совершенствование информирования граждан о мерах безопасности, государственную поддержку разработки открытого программного обеспечения, запрет государственным учреждениям требовать от граждан представления документов в одном формате, либо использовать программное обеспечение, способное функционировать лишь под одной операционной системой, законодательное увеличение установленного срока информирования оператора платежной системы о несанкционированном переводе денежных средств до 30 суток, внесение изменений в ряд законов, направленных на ограничение доступа несовершеннолетних к информации, способной причинить вред их разви-

тию, изменение порядка доступа несовершеннолетних к информации, содержащейся в компьютерных сетях на основе белых списков, разработку национальной цифровой валюты и ряд других.

Ключевые слова: киберпространство, виктимологическое предупреждение, преступность, мошенничества, несовершеннолетние

Киберпространство, под которым мы понимаем сферу общественных отношений, реализуемую посредством различных компьютерных сетей, из научно-фантастической абстракции на наших глазах стало реальностью. Растет многообразие отношений, которые в нем реализуются. Одновременно происходит быстрое увеличение числа преступлений в этой сфере. Несмотря на предпринимаемые меры как в части трансформации уголовного законодательства, так и в части специального предупреждения, количество преступных посягательств в этой сфере растет. При этом мы считаем недостаточно проработанными проблемы виктимологической профилактики таких преступлений. Несмотря на то, что этому аспекту предупредительной деятельности уделяется внимание [1–3 и др.], значительная часть предложений ограничивается различными видами информирования граждан о способах совершения в отношении них преступных посягательств. Очевидно, что развитие технологий, сопровождающееся появлением новых способов совершения преступлений, необходимо учитывать и при разработке адекватных средств противодействия, в том числе и мер виктимологической профилактики.

В статье мы преследуем цель разработки комплекса мер виктимологической профилактики преступлений, совершаемых в киберпространстве. Для достижения этой цели автором использован ряд научных методов: диалектический метод научного познания, системный, структурный, сравнительно-правовой, контент-анализ.

Как мы уже сказали, что наиболее часто в качестве меры виктимологической профилактики в криминологических работах предлагают различные способы информирования потенциальных преступников об ответственности за совершение определенных действий, либо потенциальных жертв преступных посягательств о новых видах преступлений и способах защиты от них.

Однако эффективность такой меры невысока. Например, в средствах массовой информации в разделах криминальной хроники самыми, наверное, распространенными являются новости о новых видах мошенничеств. Однако ситуация не только не меняется, но и продолжает

ухудшаться, причем граждане раз за разом попадают в уже известные ловушки преступников.

Н.В. Никулин, исследовавший виктимологические аспекты профилактики мошенничеств, обращает внимание на то, что при всех предпринимаемых усилиях по информированию только 2 из 25 опрошенных им граждан слышали о памятках, выпущенных МВД для предотвращения мошенничеств. Этот же ученый предлагает вместо памяток распространять предостерегающую информацию на телевидении [4].

Полагаем, что в настоящее время телевидение не является самым эффективным средством доставки информации, кроме того, предлагая меры по информированию о возможных преступлениях, необходимо учитывать то, что граждане не всегда готовы или желают воспринимать такую информацию. Потоки информации, которые ежедневно обрушиваются на современного человека, формируют отторжение, невосприимчивость к нежелательной информации, донесение которой воспринимается как своего рода психологическое насилие.

Полагаем, что информирование осуществлять необходимо именно в те моменты, когда люди готовы воспринимать соответствующие предостережения, и именно в таких формах, которые смогут быть в этот момент восприняты. Хорошим примером является электронная форма оплаты железнодорожных билетов на официальном сайте ОАО «РЖД»: возможность перейти к форме оплаты выбранных билетов с помощью банковской карты появляется лишь после того, как пользователь ознакомиться с информацией об особенностях такой оплаты.

Такой подход должен быть распространен и на другие дистанционные способы оплаты и перечисления денежных средств с помощью банковских карт. Например, после указания реквизитов получателя платежа в системах с двухфакторной идентификацией пользователю приходит СМС-сообщение с одноразовым паролем. В таких СМС кроме самого пароля могут содержаться и другие сведения: например, бесплатный телефон службы безопасности банка, уведомления о недопустимости указания кому бы то ни было реквизитов банковских карт по телефону, вне банковской организации и т. д.

Такие же уведомления могут появляться и в личном кабинете пользователя при совершении отдельных операций.

Большая часть мошенничеств связана с перечислением средств со счетов потерпевших на другие счета. Для повышения защищенности граждан нам представляется необходимым изменить установленный законом срок в один день, в течение которого клиент может уведомить

оператора о совершении электронных переводов без его участия. За ориентир мы предлагаем принять сроки, установленные для уведомления операторов платежных систем в США – 30 суток. Таким образом, в статье 11 ФЗ «О национальной платежной системе» необходимо слова «не позднее дня, следующего за днем…» заменить словами «не позднее тридцати суток, следующих за днем…». При этом на оператора платежной системы должна возлагаться обязанность в безусловном порядке вернуть деньги клиенту в день обращения.

Такая мера будет сдерживать операторов платежных систем в их стремлении всемерно расширить использование электронных платежных систем в ущерб безопасности платежей и стимулировать их к совершенствованию систем безопасности.

Одной из причин виктимизации выступают ошибки в программном обеспечении, приводящие к техническим авариям, нарушению прав граждан в отдельных областях.

Выявление таких ошибок является весьма трудоемкой задачей ввиду необходимости изучения значительных объемов исходных текстов программ. Многие коммерческие продукты являются закрытыми (проприетарными). Пользователи таких программ получают их уже в виде скомпилированных машинных кодов, а исходные тексты им не предоставляются. Такая практика сложилась в связи с охраной производителями своих разработок.

В тех случаях, когда программные продукты используются при обработке сведений, содержащих государственную тайну, по сложившейся практике производители предоставляют государственным органам исходные тексты своих программ, в свою очередь, последние обязуются сохранять эти сведения в тайне[1].

Как отмечается специалистами, анализ исходного кода операционной системы Windows повысит безопасность информационных систем, работающих на этой платформе[2].

Однако для рядовых граждан и организаций такой подход не практикуется, что создает риски причинения вреда в случае наличия в программном коде ошибок или программных закладок, реализующих передачу конфиденциальной информации пользователей третьим лицам.

---

[1] *Пичахчи М.* Microsoft открывает России исходные коды Windows. URL: https://club.cnews.ru/blogs/entry/microsoft_otkryvaet_rossii__06554 (дата обращения: 02.05.2021).

[2] ФАПСИ: получение исходного кода Windows повысит безопасность Рунета. URL: https://edu.rin.ru/cgi-bin/news.pl?idn=885 (дата обращения: 02.05.2021).

Вместе с тем в сфере программирования есть и другой подход, при котором все тексты программ передаются в общественное достояние и доступны для анализа. В настоящее время практически для всех проприетарных программ имеются открытые аналоги. Поэтому в интересах обеспечения безопасности пользователей в киберпространстве государство должно оказывать поддержку и отдавать приоритет тем разработчикам, которые при прочих равных условиях предоставляют доступ к исходным текстам своих программ.

Такая практика, на наш взгляд, позволит существенно снизить риски ситуаций, подобных той, что возникла в Великобритании, когда ошибка, присутствовавшая в программном обеспечении, использовавшемся британской почтовой компанией более 20 лет, приводила к систематической выдаче сообщений о недостачах, в результате чего к уголовной ответственности было незаконно привлечено 740 человек, некоторые закончили жизнь самоубийством[3].

Из этих же соображений государство должно активно развивать и поддерживать разработку отечественных операционных систем для компьютеров и мобильных устройств, поскольку только такой подход позволит своевременно изучать исходные тексты программного обеспечения на предмет наличия ошибок, гарантировать отсутствие программных закладок, отправляющих обрабатываемую информацию третьим лицам, и т. д.

Здесь следует сказать, что, несмотря на декларируемые благие намерения в этой сфере и создание реестра отечественного программного обеспечения, развитие национальных операционных систем тормозится ввиду того, что многие ведомства до настоящего времени требуют использования программного обеспечения для зарубежных систем (как правило, Windows). Так, заполнение формы налоговой декларации для государственных служащих предполагает установку специального программного обеспечения «Справки БК», размещенного для свободного скачивания на сайте Президента РФ. Представленная версия программы функционирует только под операционной системой Windows.

Таким образом, пользователи отечественных операционных систем (например, Альтлинукс, Астра и т. п.) не смогут запустить эту программу на своих компьютерах.

[3] Почтальонов 20 лет по ошибке сажали в тюрьму из-за «кривого» ПО. URL: https://www.cnews.ru/news/top/2021-04-26_krivoj_soft_krupnoj_pochtovoj (дата обращения: 03.05.2021).

Полагаем, что подобная ситуация должна быть исправлена. Для этого необходимо разработчикам программного обеспечения, используемого для государственных нужд, установить в качестве обязательного требования разработку версий для различных операционных систем. В этом смысле хороший пример представляет отечественная разработка для проведения видеоконференций TrueConf, отечественные пакеты офисных программ «Р7-Офис», «Мой офис» и т. д.

На уровне всех государственных учреждений необходим отказ от обязательного требования документов только в формате, используемом для офисного пакета Microsoft Office. Гражданам должна в обязательном порядке предоставляться возможность выбора формата документов, поддерживаемых свободным программным обеспечением.

Для того чтобы зафиксировать обязательность поддержки программного обеспечения, работоспособного на отечественных операционных системах, необходимо дополнить статью 5 «Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов евразийского экономического союза, за исключением Российской Федерации»[4] пунктом «и» следующего содержания:

«программное обеспечение может быть без дополнительной модификации использовано в операционных системах, включенных в Единый реестр российских программ для электронных вычислительных машин и баз данных».

Н.А. Короткова в числе важнейших элементов виктимологической профилактики посягательств в отношении несовершеннолетних пользователей сети Интернет называет их защиту от посторонних и от доступа к запретного рода информации [5]. В этой связи необходимо высказать несколько критических замечаний по поводу политики в сфере защиты детей от информации, способной причинить вред их нормальному развитию и воспитанию, нормативной базе, которую составляют

[4] Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов евразийского экономического союза, за исключением Российской Федерации (Утверждены постановлением Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд») // Собрание законодательства РФ. 2015. № 47. Ст. 6600.

Закон «О защите детей от информации, причиняющей вред их здоровью и развитию»[5], Закон «Об информации, информационных технологиях и о защите информации»[6] (Далее – Закон об информации), Закон «О средствах массовой информации»[7] (далее – Закон о СМИ).

Статьей 5 Закона о защите детей предусмотрены виды информации, причиняющей вред здоровью и развитию детей, а в статье 11 устанавливается положение, согласно которому оборот такой информации запрещается в местах, доступных для детей, и возможен лишь при наличии административных и организационных мер, технических и программно-аппаратных средств защиты детей от указанной информации.

В соответствии со статьей 15.1 Закона об информации в Российской Федерации создается реестр, в который заносятся доменные имена, указатели страниц сайтов в сети Интернет и сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено. При обнаружении соответствующей информации она в соответствии с установленной процедурой заносится в Реестр, а доступ к ней блокируется.

Однако это не значит, что несовершеннолетние не смогут получить доступ к запрещенной информации. Во-первых, существуют технические способы обхода блокировок с использованием VPN-сервисов, которые позволяют скрывать информацию о посещаемых пользователем сайтах, о самом пользователе и его действиях в киберпространстве. Информация о таких сервисах широко распространена в молодежной среде, в том числе и среди несовершеннолетних. Во-вторых, информация с заблокированных сайтов легко копируется (в течение минут) на другие страницы, которые еще не выявлены правоохранительными органами, но становящиеся мгновенно известными несовершеннолетним. Таким образом, при существующей системе блокирования нежелательной для несовершеннолетних информации всегда имеются временной зазор, когда любая информация остается доступной (иногда речь идет о неделях или даже месяцах), и возможности обхода блоки-

[5] О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2012 № 436-ФЗ (ред. от 5.04.2021) // Собрание законодательства РФ. 2011. № 1. Ст. 48.

[6] Об информации, информационных технологиях и о защите информации: федеральный закон от 27.06.2006 № 149-ФЗ (ред. от 3.04.2020) // Собрание законодательства РФ. 2006. № 31 (ч. I). Ст. 3448.

[7] О средствах массовой информации: Федеральный закон от 27.12.1991 № 32 (ред. от 30.12.2020) // Ведомости СНД и ВС РФ. 1992. № 7. Ст. 300.

ровок. Таким образом, в настоящее время можно говорить не о полноценной реализации этой политики, а лишь об ее имитации.

В некоторых случаях складывается парадоксальная ситуация: прокуратурой подаются исковые заявления о блокировке сайтов, содержащих запрещенную информацию, однако суды по различным причинам отклоняют их, и процедура блокировки фактически приостанавливается. При этом сайты годами продолжают работу в обычном режиме.

Именно подобным образом проходила процедура блокировки порносайта Yourporn.com. В соответствии с решением Первореченского районного суда г. Владивостока этот сайт был внесен в реестр запрещенных сайтов. Однако это решение было впоследствии отменено, поскольку к заявлению прокурора не были приложены результаты соответствующей экспертизы[8].

Таким образом, несмотря на фактический запрет распространения порнографии, устанавливаемый статьей 4 Закона о СМИ, статьями 10.4, 10.5, пунктом «а» части 5 статьи 15.1 Закона о средствах массовой информации, статьей 5 Закона о защите детей, статьей 242 УК РФ, на территории Российской Федерации безнаказанно в течение многих лет функционируют сайты, распространяющие исключительно информацию, запрещенную для демонстрации. Органы же, которые в соответствии со статьей 20 Закона о защите детей должны осуществлять государственный надзор за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, демонстрируют бездействие по этому вопросу.

Изучение судебной практики Первореченского районного суда г. Владивостока показало, что решение, в соответствии с которым был заблокирован сайт Yourporn, является типовым для этого суда. Аналогичные решения выносились 13 июля 2016 г., 23 июня 2016 г. по делу № 2-2409/16г., 23 июня 2016 г. по делу № 2-2414/16г. и т. д. Причем, как следует из названия блокируемых сайтов, большинство из них имеют российское происхождение (по этическим соображениям мы здесь их приводить не будем). Информации об обжаловании блокировок таких сайтов у нас не имеется. И лишь для двух крупнейших иностранных порносайтов российское правосудие сделало исключение и фактически легализовало их деятельность вопреки положениям российского же законодательства.

[8] *Овечкин О.* Роскомнадзор разблокировал порносайт YouPorn по решению суда. URL: https://rb.ru/news/pobeda-dobra/ (дата обращения: 16.04.2021).

Полагаем, что отсутствие экспертного заключения, ставшее отменой для судебного решения, вызвано не халатностью прокурорских работников, а финансовыми ограничениями. Стоимость искусствоведческой экспертизы исчисляется суммами порядка десяти тысяч рублей и более. Однако сайтов, требующих блокировки, огромное количество, что влечет резкое увеличение расходов на блокировку сайтов. Поэтому с учетом масштабов задачи блокировки представляется правильным создавать при отдельных прокуратурах специальные должности экспертов, которые обладают лицензиями на проведение наиболее востребованных экспертиз (например, искусствоведческой, лингвистической), и возложить на них обязанности по подготовке экспертных заключений. Информацию же о сайтах, по которым требуется соответствующая экспертиза, необходимо централизованно направлять в такие прокуратуры от всех правоохранительных органов, их выявивших. Полагаем, что такой порядок значительно упростит и ускорит процесс блокировки сайтов, содержащих запрещенную информацию.

В настоящее время ее блокировка осуществляется по модели «черных списков» – ограничиваются источники информации, внесенные в специальный реестр. Иными словами, реализуется принцип: разрешено все то, что не запрещено. При таком подходе всегда остается возможность донести до подростка нежелательную информацию либо путем обхода блокировок, либо путем быстрого создания новых сайтов, еще не внесенных в черный список.

Принципиально другой подход состоит в том, чтобы доступ в киберпространство для подростков осуществлять по белым спискам, то есть только к тем ресурсам, которые заранее одобрены как допустимые.

В соответствии со статьей 6 Закона об информации, классификация информации осуществляется ее производителями и распространителями. Полагаем, что аналогичным образом должны маркироваться сайты или отдельные страницы в сети Интернет. Обязанность соответствующей маркировки, ответственность за достоверность такой маркировки должна возлагаться на владельцев сайтов. Сайты, не маркированные соответствующим образом, не должны попадать в поисковую выдачу для несовершеннолетних.

В связи с изложенными соображениями считаем необходимым дополнить часть 2 статьи 10 Закона об информации, регламентирующей обязанности владельцев сайтов сети Интернет, после слов «которые достаточны для идентификации такого лица» словами «, а также возрастные ограничения для размещенной на сайте информации в соот-

ветствии с Федеральным законом «О защите детей от информации, причиняющей вред их здоровью и развитию».

Обязанность выдачи информации в соответствии с возрастной маркировкой и возрастом пользователя должна возлагаться на поисковые системы, например, «Яндекс», «Google». Поэтому соответствующие требования необходимо внести в статью 10.3 Закона об Информации, дополнив ее пунктом 9 следующего содержания: «Оператор поисковой системы предоставляет информацию по запросу пользователя в соответствии с возрастными ограничениями на основе данных, предоставляемых владельцами информационных ресурсов, и сведениями о возрасте пользователя».

Для мобильных устройств, используемых несовершеннолетними, предусмотреть использование специальных детских тарифов, предусматривающих фильтрацию Интернета с использованием белых списков. Возможность включения такой фильтрации необходимо предусмотреть и для остальных пользователей, компьютеры которых используются совместно с детьми.

Для таких тарифов необходимо сформировать белые списки адресов Интернета, которые содержат ссылки на контент, разрешенный в соответствии со статьями 7–10 Закона о защите детей, для различных возрастных групп (до шести лет, достигших шести лет, достигших двенадцати лет и достигших возраста шестнадцать лет). При передаче данных в сети Интернет оператор связи должен предоставлять по запросу поисковых систем сведения о возрасте потребителя и блокировать передачу информации, которая не соответствует заявленному возрасту или не промаркирована соответствующим образом. В любом случае на мобильные устройства, принадлежащие несовершеннолетним, не должна попадать информация, позволяющая им подключаться к сервисам анонимизации, таким как VPN-сервисы, сети TOR и т. п.

Еще одним источником информации, представляющей опасность для несовершеннолетних, являются социальные сети. Несмотря на то, что правила регистрации, как правило, предусматривают достижение определенного возраста, документальной проверки введенной информации не осуществляется. Таким образом, возможна регистрация с любого возраста и неограниченный доступ ко всем ресурсам.

Если будет реализована предложенная нами выше возрастная маркировка информации, то дополнительных изменений для возникновения у владельцев социальных сетей обязанностей по ограничению доступа для несовершеннолетних не возникнет. Закон об информации в

пункте 1 части 4 статьи 16 устанавливает обязанность для обладателей информации, операторов информационной системы в случаях, установленных законодательством Российской Федерации, обеспечить предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней.

Другой больной темой современного общества является мошенничество, особенно его высокотехнологичные разновидности. Множество предлагаемых по борьбе с этим явлением решений не устраняют главной проблемы – обезличенности денег, порождающей широкие возможности сокрытия их происхождения. Сущность кредитно-финансовой системы до настоящего времени остается практически неизменной, даже если учет осуществляется с помощью электронных средств связи: каждому счету соответствует определенная сумма. Перечисление денежных средств от одного субъекта к другому для банка означает всего лишь уменьшение суммы на одном счете и соответственное увеличение на другом. Денежные средства из разных источников сливаются на одних счетах, перемещаются на другие и, в конечном итоге, отследить и доказать их преступное происхождение становится очень проблематичным.

До недавнего времени решение проблемы обезличенности денег представлялось невозможным. Однако бурное развитие Интернета и быстрое увеличение производительности домашних компьютеров привели к практической реализации технологии информации, при которой все ее перемещения фиксируются без возможности каких-либо сторонних манипуляций. Мы здесь имеем в виду технологию, именуемую блокчейн, и созданные на ее основе криптографические валютные системы bitcoin, ethereum и др. Надежность этих криптовалют основана на том, что на каждом компьютере пользователя этих систем хранится в зашифрованном виде полная история всех переводов денежных средств за все время существования этих систем. Теоретически, чтобы сокрыть перевод, необходимо подделать эту информацию не менее чем на 50 % компьютеров пользователей соответствующей криптовалюты, что даже теоретически не представляется возможным [6].

Однако возможны и другие варианты, когда цифровая валюта эмитируется центральным банком государства, что, при сохранении всех достоинств, исключает и недостатки криптовалют. В настоящее время пионером в этой сфере является Китай, который приступил к тестиро-

ванию своей цифровой валюты DCEP (Digital Currency Electronic Payment), или «цифровой юань»[9].

Цифровой юань по своим характеристикам отличается от криптовалют тем, что операции с ним осуществляются централизованно, а, значит, вся информация о переводах доступна государству, и любое использование денежных средств в преступных целях будет моментально установлено и пресечено. Отличие от обычной кредитно-финансовой системы состоит в высоком уровне защищенности, поскольку вся информация о перемещении средств шифруется, и подделать ее невозможно.

Поэтому государство в любой момент времени будет располагать полной и точной информацией о движении средств, о доходах и расходах граждан и т. п. Повсеместное распространение государственной цифровой валюты сделает бессмысленным совершение мошенничеств с использованием кредитных карт, наиболее распространенного вида хищений в настоящее время.

Представляется, что разработка и внедрение собственной цифровой валюты Российской Федерацией даст не только огромные экономические преимущества, такие, как высочайшая скорость финансовых транзакций, снижение их стоимости за счет того, что станут не нужны посредники в виде традиционных банков, надежность и т. п. С криминологической точки зрения цифровая валюта станет мощнейшим антикриминогенным фактором, способным радикально изменить криминогенный ландшафт, исключить анонимность финансовых транзакций и, следовательно, снизить виктимизацию граждан.

Представленные в данной статье меры по виктимологическому предупреждению преступлений в киберпространстве отличаются элементами научной новизны и включают в себя меры организационного, технического и правового характера. Их реализация, по нашему мнению, будет способствовать снижению уровня виктимности рядовых пользователей компьютерных сетей. Мы отдаем себе отчет в том, что некоторые из представленных предложений труднореализуемы на практике, например, введение российской цифровой валюты. Вместе с тем наша задача состоит и в том, чтобы найти новые аргументы для сторонников реализации таких сложных технических решений.

[9] Будущее за DCEP: что нужно знать о новой китайской криптовалюте. URL: http://ekd.me/2020/04/budushhee-za-dcep-chto-nuzhno-znat-o-novoj-kitajskoj-kriptovalyute/ (дата обращения: 09.05.2021).

Список литературы
1. *Бочков А.А.* Виктимологическая культура: теория и практика // Право. Экономика. Психология. 2016. № 2. С. 3-9.
2. *Белицкий В.Ю.* Предупреждение совершения мошенничеств участковым уполномоченным полиции // Вестник Барнаульского юридического института МВД России. 2017. № 2. С. 132-133.
3. *Шалагин А.Е.* О приоритетных направлениях деятельности органов внутренних дел по предупреждению преступлений и административных правонарушений // Вестник экономики, права и социологии. 2014. № 2. С. 153-157.
4. *Никулин Д.В.* Профилактика мошенничества в сфере глобальной сети Интернет и средств массовой информации. Виктимологический аспект // Аллея науки. 2018. Т. 6. № 6 (22). С. 786-794.
5. *Короткова Н.А.* Виктимологическая профилактика преступлений против половой неприкосновенности несовершеннолетних, совершаемых с использованием сети Интернет // Научные достижения и открытия современной молодежи: сб. ст. 2 Междунар. науч.-практ. конф. Новосибирск, 2017. С. 225-228.
6. *Калиниченко В.Н., Кондратьев В.Ю.* Принцип работы блокчейн // Цифровизация экономики: направления, методы, инструменты: сб. ст. по материалам 2 Всерос. науч.-практ. конф. Краснодар, 2020. С. 219-221.

Статья поступила в редакцию 07.06.2021 г.
Одобрена после рецензирования 15.09.2021 г.
Принята к публикации 22.09.2021 г.

Информация об авторе
Родина Екатерина Анатольевна, помощник Урюпинского межрайонного прокурора Волгоградской области, юрист 3 класса, Прокуратура Волгоградской области, г. Урюпинск, Волгоградская обл., Российская Федерация; аспирант, кафедра прокурорского надзора и криминологии, Саратовская государственная юридическая академия, г. Саратов, Российская Федерация, rodina-caterina2010@yandex.ru, https://orcid.org/0000-0003-4651-179X

Для цитирования
Родина Е.А. Виктимологическое предупреждение преступлений в киберпространстве // Актуальные проблемы государства и права. 2021. Т. 5. № 19. С. 510-524. https://doi.org/10.20310/2587-9340-2021-5-19-510-524

ORIGINAL ARTICLE
DOI 10.20310/2587-9340-2021-5-19-510-524

VICTIMOLOGICAL PREVENTION OF CYBERSPACE CRIME

E.A. Rodina[1,2]
[1]Uryupinsk Interdistrict Prosecutor's Office of Volgograd Region
2 Ulyanovsk Ln., Uryupinsk 403113, Volgograd Region, Russian Federation
[2]Saratov State Law Academy
1 Volskaya St., Saratov 410056, Russian Federation
rodina-caterina2010@yandex.ru

Abstract. Despite efforts to improve criminal legislation, the number of criminal offenses committed in cyberspace continues to grow. This predetermines the need to improve preventive measures, including victimological ones. Purpose of the work: development of a set of measures for victimological prevention of crimes committed in cyberspace. Among the methods used are the dialectical method of scientific knowledge, systemic, structural, comparative legal, content analysis. Based on the analysis of the reasons for the victimization of users in cyberspace, proposals have been developed for a set of measures for victimological prevention, including improving citizens' information about security measures, government support for the development of open source software, a ban on government agencies from requiring citizens to submit documents in one format, or using software that can function under only one operating system, the legislative increase in the established period for informing the payment system operator about an unauthorized transfer of funds to 30 days, amending a number of laws aimed at limiting the access of minors to information that could harm their development, changing the procedure for minors' access to information, contained in computer networks on the basis of white lists, the development of a national digital currency and a number of others.

Keywords: cyberspace, victimological prevention, crime, fraud, minors

References

1. Bochkov A.A. Viktimologicheskaya kul'tura: teoriya i praktika [Victimological culture: theory and practice]. *Pravo. Ekonomika. Psikhologiya – Law. Economics. Psychology*, 2016, no. 2, pp. 3-9. (In Russian).
2. Belitskiy V.Y. Preduprezhdeniye sovershenniya moshennichestv uchastkovym upolnomochennym politsii [Prevention of committing fraud by the district police officer]. *Vestnik Barnaul'skogo yuridicheskogo instituta MVD Rossii – Bulletin of the Barnaul Law Institute of the Ministry of Internal Affairs of Russia*, 2017, no. 2, pp. 132-133. (In Russian).
3. Shalagin A.E. O prioritetnykh napravleniyakh deyatel'nosti organov vnutrennikh del po preduprezhdeniyu prestupleniy i administrativnykh pravonarusheniy [On the priori-

ty directions of the activities of the internal affairs bodies for the prevention of crimes and administrative offenses]. *Vestnik ekonomiki, prava i sotsiologii – the Review of Economy, the Law and Sociology*, 2014, no. 2, pp. 153-157. (In Russian).
4. Nikulin D.V. Profilaktika moshennichestva v sfere global'noy seti Internet i sredstv massovoy informatsii. Viktimologicheskiy aspekt [Fraud prevention in the global Internet and mass media. Victimological aspect]. *Alleya nauki – Alley of Science*, 2018, vol. 6, no. 6 (22), pp. 786-794. (In Russian).
5. Korotkova N.A. Viktimologicheskaya profilaktika prestupleniy protiv polovoy neprikosnovennosti nesovershennoletnikh, sovershayemykh s ispol'zovaniyem seti Internet [Victimological prevention of crimes against sexual inviolability of minors committed using the internet]. *Sbornik statey 2 Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Nauchnyye dostizheniya i otkrytiya sovremennoy molodezhi»* [Collection of Works of the 2nd of International Scientific and Practical Conference "Scientific Achievements and Discoveries of Modern Youth"]. Novosibirsk, 2017, pp. 225-228. (In Russian).
6. Kalinichenko V.N., Kondratyev V.Y. Printsip raboty blokcheyn [How blockchain works]. *Sbornik statey po materialam 2 Vserossiyskoy nauchno-prakticheskoy konferentsii «Tsifrovizatsiya ekonomiki: napravleniya, metody, instrumenty»* [Collection of works based on the materials of the 2nd All-Russian Scientific and Practical Conference "Digitalization of the Economy: Directions, Methods, Tools"]. Krasnodar, 2020, pp. 219-221. (In Russian).

The article was submitted 07.06.2021
Approved after reviewing 15.09.2021
Accepted for publication 22.09.2021

Information about the author

Ekaterina A. Rodina, Assistant to the Uryupinsky Interdistrict Prosecutor of Volgograd Region, Lawyer of the 3rd Class, Prosecutor's Office of Volgograd Region, Uryupinsk, Volgograd Region, Russian Federation; Post-Graduate Student, Prosecutor's Supervision and Criminology Department, Saratov State Law Academy, Saratov, Russian Federation, rodina-caterina2010@yandex.ru, https://orcid.org/0000-0003-4651-179X

For citation

Rodina E.A. Viktimologicheskoye preduprezhdeniye prestupleniy v kiberprostranstve [Victimological prevention of cyberspace crime]. *Aktual'nye problemy gosudarstva i prava – Current Issues of the State and Law*, 2021, vol. 5, no. 19, pp. 510-524. https://doi.org/10.20310/2587-9340-2021-5-19-510-524 (In Russian, Abstr. in Engl.)