*На правах рукописи*

**Родина Екатерина Анатольевна**

# ПРОТИВОДЕЙСТВИЕ КРИМИНАЛЬНОЙ ВИКТИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ «ИНТЕРНЕТ» В КИБЕРПРОСТРАНСТВЕ

5.1.4. Уголовно-правовые науки

**Автореферат**
диссертации на соискание ученой степени
кандидата юридических наук

Саратов – 2022

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Саратовская государственная юридическая академия».

| | |
|---|---|
| **Научный руководитель** | доктор юридических наук, профессор<br>**Варыгин Александр Николаевич** |
| **Официальные оппоненты:** | **Антонян Елена Александровна**<br>доктор юридических наук, профессор,<br>ФГБОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)», заведующий кафедрой |
| | **Шалагин Антон Евгеньевич**<br>кандидат юридических наук, доцент,<br>ФГКОУ ВО «Казанский юридический институт МВД России», начальник кафедры |
| **Ведущая организация** | Федеральное государственное казенное образовательное учреждение высшего образования **«Краснодарский университет Министерства внутренних дел Российской Федерации»** |

Защита диссертации состоится 22 декабря 2022 года в 12:00 на заседании диссертационного совета 24.2.390.03, созданного на базе федерального государственного бюджетного образовательного учреждения высшего образования «Саратовская государственная юридическая академия», по адресу: 410056, г. Саратов, ул. Чернышевского, д. 104, зал заседаний диссертационных советов.

С диссертацией можно ознакомиться в научной библиотеке и на сайте федерального государственного бюджетного образовательного учреждения высшего образования «Саратовская государственная юридическая академия» (http://test.ssla.ru/dissertation/dissert/14-10-2022-1d.pdf).

Автореферат разослан «__» октября 2022 года.

**Ученый секретарь диссертационного совета** **Кобзева Елена Васильевна**

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования**. Развитие в России коммуникационных сетей, информационных технологий и массовая компьютеризация повлекли революционные изменения в различных сферах общественно-политической жизни страны, в экономике, образовании, организации труда и досуга, в других областях.

Многие направления деятельности граждан, организаций и государства, как показали недавние карантинные ограничения в связи с коронавирусной инфекцией, были целиком или в значительной части перенесены в новую виртуальную реальность, в киберпространство. Можно спорить о недостатках этой трансформации, однако общий вектор развития представляется неизменным – дальнейшее расширение дистанционных форм взаимодействия в обществе и наделение киберпространства новыми функциями, ранее для него не характерными.

Выгоды компьютеризации или, как иногда говорят, цифровизации общества сегодня таковы, что отказаться от них без катастрофической утраты конкурентных экономических и политических преимуществ не может ни одно государство в мире.

Однако, как и любое явление, наблюдаемые процессы влекут и негативные последствия, в том числе в интересующей сфере преступности. Появляются новые способы совершения преступлений, качественно изменяются возможности преступников, увеличивается причиняемый ими вред.

Введение карантинных мероприятий в связи с распространением эпидемии COVID-19 резко интенсифицировало хозяйственную деятельность в киберпространстве, что в свою очередь сопроводилось взрывным ростом киберпреступности. В частности, за последние два года доля преступлений, совершаемых с использованием информационно-коммуникационных технологий, возросла до 25,3 % от общей массы всех зарегистрированных преступных посягательств и составила в 2021 году 517772 преступления[1].

[1] Состояние преступности в России за январь – декабрь 2021 г. М., 2022 // Портал правовой

На фоне общего снижения числа практически всех видов преступлений наблюдается стабильный рост мошенничеств, происходящий, главным образом, за счёт активизации деятельности преступников в киберпространстве. Подтверждением этому являются статистические сведения о зарегистрированной преступности: из 339606 мошенничеств в 2021 году 249249 или 73,4 % совершены с использованием информационно-коммуникационных технологий[1], причем динамика кибермошенничеств впечатляющая – например, в 2020 году она составила 75,6 %[2].

Количество потерпевших только по зарегистрированным преступлениям, совершаемым с использованием информационно-коммуникационных технологий, превышает полмиллиона человек в год. Количественные оценки уровня кибермошенничеств показывают, что в той или иной его форме с деятельностью мошенников сталкивались десятки миллионов жителей России. На фоне неэффективности предпринимаемых государством усилий это придает проблеме киберпреступности политическое значение, поскольку ставит вопрос о самой способности государства обеспечивать защиту прав своих граждан. Неудивительно, что в подобной ситуации последним бастионом в предупреждении киберпреступлений выступают меры виктимологической профилактики, в полной мере отражая текущее состояние дел крылатой латинской фразой «cura te ipsum» – помоги себе сам.

Виктимологические исследования – относительно молодое и вместе с тем активно развивающееся направление криминологической науки. Жертва и механизм виктимизации находятся в центре многих криминологических исследований, поскольку позволяют криминологам глубже проникать в особенности механизма преступной деятельности, его детерминации, предлагать новые и более эффективные способы предупреждения

---

статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/analytics (дата обращения: 07.02.2022).

[1] Там же.

[2] Состояние преступности в России за январь – декабрь 2020 г. // Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/analytics (дата обращения: 17.02.2021).

преступлений.

Однако нюансы, связанные с особенностями функционирования киберпространства и реализации общественных отношений в этой среде, не до конца осмыслены и раскрыты в криминологической теории. В частности, требуют уточнения содержание и соотношение базовых понятий виктимологии – «жертва» и «потерпевший», поскольку это предопределяет объем научных исследований и практических мер по предупреждению преступности. Нуждаются в развитии представления о механизме виктимологической детерминации, впрочем, как и о детерминации преступлений вообще, об объёме и содержании других понятий и терминов, характеризующих процессы виктимизации в виртуальной реальности.

С практической точки зрения назрела необходимость в осмыслении накопленного за период активного развития компьютерных сетей, опыта предупреждения киберпреступлений как в России, так и в других государствах, оценке эффективности предпринимаемых усилий и их корректировки с учётом возможностей, предоставляемых виктимологией, новых, более эффективных мер защиты граждан от киберпреступлений.

Сказанное подчеркивает актуальность избранной темы исследования.

**Степень научной разработанности проблемы**. Изучение процессов виктимизации в киберпространстве на уровне самостоятельного монографического научного исследования в отечественной криминологии за последние пять лет не осуществлялось.

Теоретические представления о виктимологической профилактике, особенностях реализации мер защиты от отдельных видов преступных посягательств, развивались в работах Н.М. Александриной, О.А. Бойко, А.А. Бочкова, В.В. Бражникова, Н.А. Вакуленко, Т.В. Варчук, К.В. Вишневецкого, Л.В. Жихаревой, П.А. Кабанова, Е.С. Качуровой, Е.Н. Клещиной, А.А. Комарова, Н.А. Коротковой, Л.В. Майорова, Р.Р. Маргизова, А.А. Нестеровой, В.И. Полубинского, Ю.С. Пестеревой, Д.В. Ривмана, Р.А. Сабитова, Е.В. Савиных, Э.Л. Сидоренко, А.М. Смирнова,

Л.В. Франка, А.О. Харитонова, А.Н. Хоменко, А.Е. Шалагина, В.П. Шейнова.

Отдельные аспекты виктимологической профилактики преступлений, совершаемых в киберпространстве, исследовали Е.А. Антонян, В.А. Бессонов, Н.В. Докучаев, А.П. Комаров, М.Н. Кочеткова, Т.М. Лопатина, Д.В. Никулин, В.С. Овчинский, А.Ю. Пальцева, О.С. Ронжина, Ф.С. Сафуанов, А.А. Скурихина, Э.В. Сысоев и др.

Однако до настоящего времени не было работ, в которых сочеталось бы комплексное изучение киберпространства, киберпреступности, особенностей криминогенной виктимизации пользователей киберпространства в сети «Интернет». В связи с этим тему диссертации можно охарактеризовать как недостаточно исследованную.

**Объектом исследования** выступают общественные отношения, возникающие в связи с совершением в киберпространстве преступных посягательств на охраняемые законом права и интересы личности, общества и государства, а также деятельность по предупреждению указанных преступлений.

**Предметом исследования** выступают связанные с объектом исследования нормы Конституции РФ, Уголовного кодекса РФ, других правовых актов; статистические сведения о состоянии преступности и её отдельных показателях; материалы следственной и судебной практики; результаты проведенного анкетирования граждан и сотрудников правоохранительных органов; результаты криминологических и социологических исследований, содержащихся в трудах отечественных и зарубежных исследователей.

**Целью диссертационного исследования** выступает разработка концептуальных основ системы виктимологической профилактики преступлений, совершаемых в киберпространстве.

Для достижения цели исследования поставлены следующие **исследовательские задачи**:

- разработать терминологический аппарат криминальной виктимизации

пользователей сети «Интернет» в киберпространстве;

- выявить причины и условия криминальной виктимизации пользователей сети «Интернет» в киберпространстве;
- определить особенности личности потерпевшего от посягательств, совершаемых в киберпространстве, имеющие значение для виктимологической профилактики;
- разработать рекомендации по совершенствованию законодательства в части повышения уровня защищенности отдельных категорий лиц в киберпространстве;
- обобщить зарубежный опыт профилактики криминальной виктимизации пользователей сети «Интернет» в киберпространстве;
- разработать комплекс мер виктимилогической профилактики киберпреступности.

**Методология и методы исследования.** Основу научного исследования образует всеобщий диалектический метод познания, предполагающий исследование процессов виктимизации в киберпространстве во всей полноте взаимосвязей общественных отношений, регулируемых нормами различных отраслей права, а также общие и специальные методы познания. К числу используемых общенаучных методов относятся анализ и синтез, индукция и дедукция, абстрагирование, системно-структурный подход и др. Частнонаучными методами послужили формально-юридический, логический, статистический и другие специально-криминологические: анкетирование граждан и сотрудников правоохранительных органов, интервьюирование, изучение следственной и судебной практики, контент-анализ средств массовой информации.

**Теоретической основой исследования** послужили труды в области теории государства и права, уголовного права и криминологии, а также работы в области философии, психологии, кибернетики и других отраслей научного знания, касающиеся рассматриваемых в диссертации вопросов.

**Правовую базу исследования** образуют Конституция РФ, международно-

правовые акты, Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ, Кодекс РФ об административных правонарушениях, федеральный закон «Об информации, информационных технологиях и о защите информации», федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», иные федеральные законы и нормативные акты, регламентирующие отдельные аспекты функционирования киберпространства, Доктрина информационной безопасности РФ, правовые позиции Конституционного Суда РФ и Верховного Суда РФ по отдельным вопросам, связанным с объектом исследования.

**Эмпирическая база исследования** включает:

- статистические сведения Генеральной прокуратуры РФ о состоянии преступности за 2016–2021 гг.;

- результаты изучения и обобщения опубликованных и архивных материалов 176 уголовных дел о преступлениях, совершенных в киберпространстве;

- 63 судебных решения о внесении доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащих информацию, распространение которой в Российской Федерации запрещено;

- результаты анкетирования 204 граждан по проблемам, связанным с осведомленностью об опасности совершения в отношении них посягательств в киберпространстве и мерах защиты от них;

- результаты анкетирования 148 сотрудников правоохранительных органов по проблемам виктимизации в киберпространстве;

- личные страницы 87 несовершеннолетних участников групп антиобщественной направленности и 50 несовершеннолетних девушек, находящиеся в открытом доступе в социальных сетях;

- сведения о преступлениях, совершенных в киберпространстве, содержащиеся в публикациях средств массовой информации.

**Научная новизна исследования** состоит в том, что впервые

на диссертационном уровне разработан терминологический аппарат, получены данные об особенностях виктимологической детерминации и личности жертв киберпреступлений, на основе чего разработана концепция противодействия криминальной виктимизации пользователей сети «Интернет» в киберпространстве.

**Основные положения, выносимые на защиту**

**1.** Киберпространство – это совокупность проводных и беспроводных сетей связи, аппаратных средств и программного обеспечения, обеспечивающих возможность произвольной коммуникации между любыми пользователями, а равно доступ каждого пользователя к произвольному устройству в таких сетях и содержащимся в нем данным.

Киберпространство является благоприятной средой для совершения различных преступлений, количество которых, их постоянный рост, особенности совершения позволяют вести речь о киберпреступности – совокупности преступлений, совершаемых за определенный период времени посредством возможностей, предоставляемых киберпространством (киберпреступлений).

Масштабы и динамика распространения киберпреступности, неспособность государства остановить ее рост, трансграничность, увеличение количества потерпевших переводят киберпреступность из разряда криминологических проблем в проблему политическую.

**2.** Под жертвой киберпреступления следует понимать физическое или юридическое лицо, которому в результате совершения общественно опасного деяния в киберпространстве причиняется или создается угроза причинения ущерба.

При характеристике личности жертвы преступлений, совершаемых в киберпространстве, следует учитывать повторяющиеся наборы признаков, способствующих их виктимизации. К их числу следует относить молодой или, наоборот, пожилой возраст, рассеянность внимания, стремление к легкому обогащению, излишнюю доверчивость, низкий уровень компьютерной

грамотности, повышенный уровень тревожности.

В последнее время размывается возрастное деление жертв мошенничеств, поскольку представители различных возрастных групп оказываются жертвами разных видов таких преступлений.

Для несовершеннолетних жертв киберпреступлений характерны такие признаки, как педагогическая запущенность, фактическая безнадзорность при действиях в киберпространстве, отсутствие близких доверительных отношений с родителями (отсутствие одного из родителей).

**3.** Общественная опасность противоправных деяний, связанных с размещением информации, содержащей призывы к террористической деятельности, экстремизму, реабилитации нацизма в киберпространстве, определяется не только содержанием самих высказываний, но и размером аудитории, которая фактически может с ними ознакомиться. Последний фактор должен учитываться в качестве криминоообразующего или квалифицирующего признака в статьях УК РФ, предусматривающих уголовную ответственность за терроризм, экстремизм, реабилитацию нацизма.

**4.** Криминальная виктимизация пользователей сети «Интернет» в киберпространстве обусловлена следующими причинами и условиями:

- сложность программного обеспечения, которая, с одной стороны, затрудняет его изучение и использование пользователями, а с другой – проявляется в большом количестве программных ошибок, позволяющих злоумышленникам получать доступ к компьютерам жертв; намеренное ослабление производителями систем безопасности в угоду удобству использования программ;

- недостаточность предпринимаемых мер для сохранения конфиденциальной информации о гражданах, а также непонимание самими гражданами важности обеспечения конфиденциальности информации о себе;

- асимметрия в уровне правовой защищённости прав пользователей и операторов платежных систем, при которой операторы извлекают доход от эксплуатации таких систем, а все издержки, связанные с несовершенством

систем безопасности, возлагаются на пользователей;

- незнание или игнорирование гражданами базовых требований безопасности в киберпространстве: о своевременном обновлении программного обеспечения своих компьютеров, недопустимости использования простых паролей и одинаковых паролей для разных сервисов, отсутствие навыков сокрытия персональной информации;

- отсутствие культуры общения в социальных сетях, асоциальное поведение в киберпространстве;

- отсутствие возрастных ограничений для регистрации в социальных сетях.

**5.** Снижению виктимизации пользователей сети Интернет могут служить следующие меры общесоциального характера:

- формирование полноценного цифрового суверенитета Российской Федерации, то есть способности государства реализовывать и контролировать весь спектр технологий и программного обеспечения, лежащих в основе функционирования киберпространства, для чего необходимо построение современной национальной полупроводниковой индустрии и переход на национальное программное обеспечение, начиная с государственных учреждений, и переноса деятельности всех цифровых компаний отечественного происхождения в отечественную юрисдикцию;

- разработка отечественной цифровой валюты;

- поддержка государственным финансированием наиболее успешных информационных проектов патриотической, образовательной, энциклопедической и культурной направленности, формирующих общее культурное пространство страны, повышающих уровень грамотности населения и снижающих тем самым риски виктимизации пользователей с условием бесплатного доступа для всех желающих либо радикального снижения расценок на такой доступ;

- министерствам просвещения, образования и науки, министерствам образования субъектов РФ необходимо стимулировать перенос обучающих

видеоматериалов, которые готовятся преподавателями учебных заведений, на российские аналоги западных видеосервисов;

- органы государственной власти должны обязать подчиненные им подразделения переносить проведение дистанционных мероприятий на российские программные платформы, запретить использование иностранных мессенджеров и обеспечить переход на российские программные продукты аналогичной функциональности.

**6.** Виктимологическая профилактика преступлений в киберпространстве требует реализации следующих мер:

- изменение вектора развития компьютерной грамотности при подготовке пользователей, при которой необходимо делать акцент на изучении технических особенностей функционирования компьютерных сетей, базовых аспектах безопасного поведения в киберпространстве;

- немедленный и безоговорочный отказ от очернения любых эпизодов отечественной истории и пересмотр политики финансирования Министерством культуры РФ художественных фильмов и театральных постановок. Государство может и обязано подвергать государственной цензуре художественные произведения (фильмы, театральные постановки, скульптурные изображения, картины и т.п.), созданные на деньги государства, на предмет их соответствия исторической правде, отсутствия элементов порнографии, неоправданного изображения сцен насилия, секса, нецензурной лексики;

- для мобильных устройств, используемых несовершеннолетними, необходимо предусмотреть использование операторами сотовой связи специальных детских тарифов, предусматривающих фильтрацию сети «Интернет» с использованием белых списков. Возможность включения такой фильтрации необходимо предусмотреть и для остальных пользователей, компьютеры которых используются совместно с детьми.

## Предложения по совершенствованию законодательства и практики противодействия преступности

**1.** Для повышения защищённости прав граждан предлагается установить уголовно-правовой запрет на преследование со стороны должностных лиц за обоснованную критику, дополнив УК РФ статьёй $136^1$ следующего содержания:

«**Статья $136^1$. Преследование граждан за критику**

Умышленное ущемление должностным лицом прав и законных интересов граждан, связанное с преследованием за обоснованную критику, содержащуюся в публичном выступлении, публикации в средствах массовой информации, сети «Интернет», –

наказывается штрафом в размере до ста тысяч рублей или в размере заработной платы или иного дохода осуждённого за период до одного года, либо лишением права занимать определённые должности или заниматься определённой деятельностью на срок до двух лет, либо обязательными работами на срок до двухсот часов, либо исправительными работами на срок до шести месяцев.»

**2.** Для повышения защищённости пользователей платёжных систем от мошеннических посягательств необходимо изменить установленные законом сроки, в течение которых клиент может уведомить оператора о совершении электронных переводов без его участия. Для этого в статье 11 федерального закона от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» слова «не позднее дня, следующего за днем…» следует заменить словами «не позднее тридцати суток, следующих за днем…». При этом на оператора платёжной системы должна возлагаться обязанность в безусловном порядке вернуть деньги клиенту в день обращения.

**3.** 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, утверждённых постановлением Правительства РФ от 16.11.2015 № 1236, необходимо дополнить пунктом «и» следующего содержания: «*и) программное обеспечение может быть без дополнительной модификации использовано в операционных системах, включённых в Единый реестр российских программ для электронных вычислительных машин и баз данных*».

**4.** Часть вторую статьи 10 федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», регламентирующей обязанности владельцев сайтов сети «Интернет», после слов «которые достаточны для идентификации такого лица» необходимо дополнить словами «, а также возрастные ограничения для размещённой на сайте информации в соответствии с федеральным законом «О защите детей от информации, причиняющей вред их здоровью и развитию».

**5.** Статью $10^3$ федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» необходимо дополнить частью девятой следующего содержания: «9. 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».

**Теоретическая значимость исследования** определяется комплексным решением ряда теоретических проблем виктимологической профилактики киберпреступлений, разработкой соответствующего терминологического аппарата, выявлением качеств личности, имеющих виктимогенное значение в киберпространстве, анализом причин и условий криминальной виктимизации пользователей. Указанные сведения могут быть использованы в дальнейших доктринальных исследованиях киберпреступности.

**Практическая значимость исследования** состоит в том, что разработанный автором комплекс мер предупреждения виктимизации пользователей киберпространства направлен на снижение, в первую очередь,

преступлений, развивающихся наиболее быстрыми темпами, способен значительно снизить риски вовлечения несовершеннолетних в противоправную деятельность, защитить их от нежелательной информации. Предложенные в исследовании меры по совершенствованию законодательства направлены на повышение защищенности различных категорий граждан при осуществлении ими деятельности в киберпространстве и могут быть использованы для совершенствования законодательства и разработки мер противодействия киберпреступности.

**Степень достоверности результатов диссертационного исследования** определяется комплексным подходом, применением общих и специальных методов научного познания, выбор которых обусловлен целью и задачами исследования, сравнением имеющихся теоретических положений и сведений, полученных в ходе эмпирических исследований, обобщением правоприменительной практики, сопоставлением результатов настоящего исследования с положениями других научных исследований, научно-теоретическим аргументированием.

**Апробация результатов диссертационного исследования**. Диссертация обсуждена и рекомендована к защите кафедрой прокурорского надзора и криминологии ФГБОУ ВО «Саратовская государственная юридическая академия».

Основные научные результаты исследования отражены в 7 научных статьях общим объемом 3,1 а.л., 4 из которых – в рецензируемых научных журналах из перечня, рекомендованного ВАК при Минобрнауки России, а также доводились диссертантом до сведения научных и практических работников в ходе международных и всероссийских научных мероприятий, состоявшихся в Саратове (Саратовская государственная юридическая академия) и Москве (Университет прокуратуры РФ, Московский финансово-юридический университет (МФЮА)).

Полученные результаты исследования используются в практической деятельности следственного отдела УФСБ России по Волгоградской области, в

учебном процессе ФГБОУ ВО «Саратовская государственная юридическая академия» при проведении лекционных и практических занятий по дисциплине «Криминология», «Теория профилактики», «Использование криминологических знаний в деятельности органов прокуратуры».

**Структура диссертации** определяется целью, задачами и логикой исследования. Она включает введение, две главы, объединяющие шесть параграфов, заключение, библиографический список и приложения.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** автор обосновывает актуальность темы диссертационного исследования и освещает степень ее научной разработанности, определяет цель, задачи, объект и предмет исследования, приводит данные о научной новизне, раскрывает методологию и методы исследования, теоретическую, нормативную и эмпирическую базу диссертации, формулирует научные положения, выносимые на защиту и предложения по совершенствованию законодательства, обосновывает теоретическую и практическую значимость, характеризуется степень достоверности полученных результатов, приводятся сведения об апробации результатов и структуре диссертации.

**Глава 1 «Киберпространство и киберпреступность как криминологические категории»** состоит из трех параграфов. Параграф 1 **«Криминологическая характеристика киберпространства и киберпреступности»** автор начинает с упорядочивания терминологического аппарата. В настоящее время общепринятого термина, который характеризует сферу отношений посредством компьютерной связи (компьютерных сетей), нет. В нормативных актах и специальной литературе сейчас используются понятия «сеть «Интернет», «информационная сфера», «информационное пространство», «киберпространство». Проведенным анализом определены достоинства и недостатки указанных дефиниций и предложено в качестве универсального понятия *«киберпространство»*, то есть *совокупность проводных и беспроводных сетей связи, аппаратных средств и программного обеспечения,*

*обеспечивающих возможность произвольной коммуникации между любыми пользователями, а равно доступ каждого пользователя к произвольному устройству в таких сетях и содержащихся в нем данных*.

Киберпространство имеет сходства и отличия с обычным физическим пространством, налагающие отпечаток и на криминологические и, в особенности, виктимологические характеристики совершаемых в нем преступлений. В нем есть аналоги физического перемещения, зоны общего и ограниченного доступа. Информация в нем имеет привязку к определенному месту (физическому устройству, локализованному в физическом пространстве), что позволяет говорить о «своей» и «чужой» информации, о государственном суверенитете, распространяющемся на информационные ресурсы в киберпространстве. Деятельность преступников так же, как и в физическом пространстве, оставляет следы.

К числу криминологически значимых отличий следует отнести анонимность, исключающую какой-либо контроль над действиями пользователя в киберпространстве, возможность находить единомышленников для любых антиобщественных начинаний, возможность противостоять действиям государства, неограниченно долгое сохранение размещенных в киберпространстве высказываний, информации, зловредных программ. В киберпространстве, как ни в какой другой сфере человеческой деятельности, велика разница между специалистом в сфере ИТ-технологий и обычным пользователем, не оставляющая последним шансов защитить свои права в столкновении с киберпреступником-профессионалом.

Существенным отличием информации, размещенной в киберпространстве, является аудитория соответствующего пользователя. Это обстоятельство в значительной степени влияет на общественную опасность преступлений, связанных с размещением отдельных видов информации.

Преступления, совершаемые в киберпространстве, не тождественны преступлениям в сфере компьютерной информации, предусмотренным главой 28 УК РФ. В работе обосновывается понятие киберпреступности как

совокупности преступлений, совершаемых за определенный период времени посредством возможностей, предоставляемым киберпространством.

Исследование статистических данных показывает беспрецедентный ее рост в 2020 г., что, скорее всего, связано с карантинными ограничениями и возросшим использованием гражданами возможностей дистанционной торговли и общения. Наибольший рост, в соответствии со статистической отчетностью, демонстрируют посягательства, совершенные с использованием платежных карт, использованием средств мобильной связи и сети «Интернет». Наблюдается рост числа общеуголовных преступлений, совершенных с использованием информационно-коммуникационных технологий и, в первую очередь, мошенничеств. По результатам проведенной в работе оценки, их латентность, с учетом неоконченных посягательств, превышает 99 %.

Масштабы и скорость распространения киберпреступности, большое количество потерпевших от нее, переводят ее из разряда социальных проблем в политические, когда неспособность государства быстро обуздать ее рост может трансформироваться в недовольство государством в целом.

Во втором параграфе **«Проблемы криминальной виктимизации пользователей сети «Интернет» в киберпространстве»** исследуются основные понятия виктимологической теории. В отечественном праве для определения лиц, которым преступлением причиняется ущерб, используется термин «потерпевший». В виктимологической литературе его иногда называют также «жертвой». В ходе проведенного анализа нормативных актов установлено, что эти понятия не тождественны. «Жертва» по своему содержанию шире, чем «потерпевший», и возникает в тех случаях, когда потерпевший не возникает, например, при неоконченных преступлениях, при отказе в возбуждении уголовного дела по основаниям, предусмотренным ст. 24 УПК РФ и т. д. Поэтому обосновывается вывод о предпочтительности в виктимологических исследованиях использования слова «жертва» и дается определение жертвы киберпреступления: *под жертвой киберпреступления следует понимать физическое или юридическое лицо, которому в результате*

*совершения общественно опасного деяния в киберпространстве причиняется или создается угроза причинения ущерба.*

В работе исследуется механизм виктимологической детерминации. Личность жертвы как совокупность специфических особенностей психики, мировоззрения, физиологических качеств формируется под влиянием общественных отношений, особенности которых, по всей видимости, и следует рассматривать в качестве общей причины виктимизации. В то же время детерминация виктимного поведения имеет и свои особенности. В ряде случаев мы вообще не можем говорить о включении виктимности в механизм детерминации. Примеры подобного рода связаны с получением доступа к абонентским номерам мобильной связи, когда преступники произвольно выбирают телефонные номера, которые собираются присвоить. В большинстве случаев наличие у потерпевшего определенных качеств (или их совокупности) выступают необходимым условием совершения преступления. Кроме того, распространенность таких качеств может учитываться преступниками при принятии решения о начале преступной деятельности. Тогда мы говорим о том, что распространенность определенных виктимных качеств выступает в качестве причины совершения отдельных видов киберпреступлений. В киберпространстве виктимизация практически всегда носит активный характер, при котором жертва активно реагирует на специфическую информацию.

Причины и условия виктимизации бывают объективными и субъективными. К объективным следует относить: сложность программного обеспечения, наличие программных ошибок, сознательное ослабление систем безопасности в пользу удобства пользователей, асимметрия в защите прав и свобод пользователей и операторов платежных систем. Здесь же следует отметить, что персонализация поиска в современных поисковых системах формирует у пользователей искаженное представление о действительности.

Субъективными предпосылками виктимизации в киберпространстве являются отсутствие навыков работы с конфиденциальными данными, использование личных устройств в общественных местах и общедоступных

сетях, низкая культура общения в социальных сетях, отсутствие представлений о криминологически значимых особенностях киберпространства. Особенности виктимизации несовершеннолетних в киберпространстве связаны с отсутствием нормативно определенных возрастных ограничений на регистрацию в социальных сетях.

В третьем параграфе **«Характеристика личности жертвы киберпреступлений»** исследуются особенности личности жертв отдельных видов, совершаемых в киберпространстве. По материалам изученных уголовных дел 90 % жертв приходилось на мошенничества в киберпространстве. Следующими по распространённости стали жертвы посягательств на половую неприкосновенность несовершеннолетних, предусмотренных ст. 134 и 135 УК РФ (5 %). В единичных случаях процесс виктимизации начинался в киберпространстве, а завершался причинением вреда при личном контакте виновного и жертвы: хищения (разбойные нападения, грабежи) и вымогательства; заведомо ложное сообщение о совершении преступления; склонение к суициду; убийство.

Во многих случаях подростки вовлекаются в деятельность антиобщественных организаций (АУЕ и др.) и, таким образом, являются жертвами в том смысле, что вред причиняется интересам их нормального развития и воспитания, хотя уголовные дела по подобным фактам в ходе исследования не встретились.

Для многих несовершеннолетних жертв киберпреступлений характерна педагогическая запущенность, их фактическая безнадзорность в киберпространстве, отсутствие доверительных отношений с родителями, травля со стороны сверстников.

При изучении жертв кибермошенничеств установлено, что наибольшее число преступлений связано с покупками в сети «Интернет» – 46,4 %, с фишингом (42,9 %), с присвоением сумм, направляемых на благотворительные цели (10,7 %), с проведением лотерей (7,1 %), со сделками с недвижимостью (7,1 %). Количество мужчин и женщин в массе потерпевших примерно равно.

Распределение потерпевших по возрасту следующее: до 40 лет — 17,5 %, от 40 до 50 лет — 34,7 %, старше 50 — 47,8 %. Наблюдается омоложение потерпевших в последние два года. Наиболее распространенными качествами личности мошенников являются отсутствие технических познаний и опыта деятельности в киберпространстве. Типичная жертва мошенника не имеет высшего образования и связывает улучшение своего благосостояния не с систематической трудовой деятельностью, а с разовым успехом, случаем. Для этой категории потерпевших характерна жадность, низкий уровень деловой культуры, неспособность критически воспринимать информацию. Во многих случаях жертвы мошенников в момент общения с преступником были заняты другим делом, т. е. их внимание не было сфокусировано на обеспечении собственной безопасности. Характерной чертой жертв потерпевших от мошенничеств с кредитными картами является повышенная тревожность, связанная с недоверием к банкам (50 %), негативный опыт (19,4 %), страх потери банковской карты (27,8 %), неумение правильно пользоваться банковскими терминалами, личными кабинетами в платёжных системах (11,1 %). Выявленный комплекс факторов виктимности жертв кибермошенничеств коррелирует с результатами других криминологических исследований.

Во всех случаях посягательств против половой неприкосновенности несовершеннолетних потерпевшими были девочки. Для таких лиц характерна неподготовленность к неожиданным контактам в социальной сети, отсутствие доверительных отношений с родителями, особенно – с матерью, слишком раннее ознакомление с информацией о сексуальной стороне жизни людей.

Вторая глава диссертационного исследования **«Основные направления предупреждения криминогенной виктимизации пользователей сети «Интернет»** в киберпространстве» содержит три параграфа. В первом параграфе **«Зарубежный опыт противодействия криминальной виктимизации пользователей сети «Интернет» в киберпространстве»** анализируются заслуживающие научного анализа меры противодействия

криминальной виктимизации пользователей сети «Интернет» в киберпространстве, предпринимаемые иностранными государствами.

Установлено, что наиболее высокий уровень защищённости личности может обеспечивать лишь цифровой суверенитет, т.е. способность государства реализовывать и контролировать весь спектр технологий, лежащих в основе функционирования киберпространства.

В полной мере таким суверенитетом в настоящее время обладают США, где реализована возможность производства всего комплекса аппаратных и программных средств, обеспечивающих функционирование киберпространства, сконцентрированы крупнейшие информационные ресурсы, социальные сети, имеется сообщество разработчиков любых аппаратных и программных продуктов, обладающее передовыми компетенциями. Быстрыми шагами приближается к достижению цифрового суверенитета КНР, в которой реализованы крупномасштабные меры защиты национального киберпространства. Российская Федерация цифровым суверенитетом в полном смысле этого слова пока не обладает.

На основе анализа сделан вывод, что меры защиты в киберпространстве должны носить комплексный характер, сочетая программно-технические средства и способы, а также нормативное регулирование. Запретительные меры (блокирование информации) обладают меньшей эффективностью, но их применение оправдано недостаточной технологической развитостью государства (отсутствием полноценного цифрового суверенитета).

Повышение эффективности защиты граждан связано с определёнными ограничениями в сфере свободы слова, свободы информации, тайны частной жизни. Поэтому в настоящее время наблюдается повсеместное наступление государств на эти базовые ценности.

Эффективным средством виктимологической профилактики является поддержка государством деятельности по созданию и поддержанию общедоступных массивов информации образовательного, энциклопедического и культурного характера, формирующих общее культурное пространство

страны, повышающее уровень грамотности населения и снижающее, тем самым, риски виктимизации пользователей.

Во втором параграфе **«Общесоциальная профилактика криминогенной виктимизации пользователей сети «Интернет» в киберпространстве»** автором предложен комплекс мер общесоциальной профилактики виктимизации. В него следует включать поддержку государственным финансированием наиболее успешных информационных проектов патриотической направленности и образовательных сайтов с условием бесплатного доступа для всех желающих либо радикального снижения расценок. Министерствам просвещения, образования и науки, министерствам образования субъектов РФ необходимо стимулировать перенос обучающих видеоматериалов, которые готовятся преподавателями учебных заведений на российские аналоги западных видеосервисов. Государственные органы власти должны обязать подчиненные им подразделения переносить проведение дистанционных мероприятий на российские программные платформы, запретить использование иностранных мессенджеров и обеспечить переход на российские программные продукты аналогичной функциональности.

Важнейшим направлением обеспечения безопасности в киберпространстве является достижение цифрового суверенитета. Для этого необходимо построение современной национальной полупроводниковой индустрии, переход государственных и образовательных учреждений на национальное программное обеспечение, перенос деятельности всех цифровых компаний отечественного происхождения в отечественную юрисдикцию.

В настоящее время компьютерная подготовка пользователей не соответствует целям обеспечения безопасности их деятельности в киберпространстве. Для исправления ситуации необходимо изменить вектор развития компьютерной грамотности и делать акцент на изучении технических особенностей функционирования компьютерных сетей, базовых аспектах безопасного поведения в киберпространстве.

Важнейшей задачей виктимологической профилактики, стоящей перед

государством является немедленный и безоговорочный отказ от очернения любых эпизодов отечественной истории и пересмотр политики финансирования Министерством культуры художественных фильмов и театральных постановок. Государство может и обязано подвергать государственной цензуре на предмет соответствия исторической правде, отсутствия элементов порнографии, неоправданного изображения сцен насилия, секса и проч. художественные произведения (фильмы, театральные постановки, скульптурные изображения, картины и т.п.), созданные на деньги государства.

В третьем параграфе **«Меры специальной виктимологической профилактики»** предложен ряд мер, включающий в себя, во-первых, разработку и введение в оборот отечественной цифровой валюты, что позволит исключить анонимность финансовых транзакций и снизить, таким образом, виктимность граждан. Данная мера способна обладает предупредительным потенциалом и по отношению к широкому спектру общеуголовных преступлений, поскольку направлена на кардинальное снижение возможностей проведения анонимных платежей, легализации денежных средств, полученных преступным путем.

С учетом масштабов задач по блокировке запрещенной информации предлагается создавать при отдельных прокуратурах должности экспертов, обладающих лицензиями на проведение наиболее распространенных 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. Такой порядок значительно упростит и ускорит процесс блокировки сайтов, содержащих запрещенную информацию.

Для обеспечения безопасности несовершеннолетних в киберпространстве предлагается организация их доступа в сеть «Интернет» по «белым» спискам, в которых доступными для них будут только заранее проверенные и одобренные ресурсы. Для мобильных устройств, используемых несовершеннолетними,

необходимо предусмотреть использование специальных тарифов, предусматривающих доступ к ресурсам сети «Интернет» с использованием фильтрации передаваемой абонентам информации на основе «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, разрешённый в соответствии со статьями 7-10 федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», для различных возрастных групп. 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, сеть TOR и т. п. На владельцев информационных ресурсов необходимо дополнительно возложить обязанность по возрастным ограничениям для размещенной информации, для чего предлагается внести соответствующие изменения в ч. 2 ст. 10 федерального закона «Об информации, информационных технологиях и о защите информации». На операторов поисковых систем должна быть возложена обязанность предоставлять информацию по запросу пользователя в соответствии с возрастными ограничениями на основе данных, предоставляемых владельцами информационных ресурсов и сведениями о возрасте пользователя, для чего необходимо внести соответствующие изменения в ст. 10.3 Закона «Об информации, информационных технологиях и о защите информации».

В **заключении** сформулированы основные выводы теоретического и практического характера, а также обозначены перспективы дальнейшей разработки темы диссертационного исследования.

В **приложениях** представлены результаты анкетирования сотрудников правоохранительных органов и граждан по проблематике диссертационного исследования.

**Основные положения и выводы диссертационного исследования получили отражение в следующих опубликованных автором работах:**

*Статьи в рецензируемых научных журналах и изданиях,*

*рекомендованных ВАК при МинобрнаукиРоссии*

*для опубликования основных научных результатов диссертаций*

1. *Родина, Е.А.* Понятия «жертва» и «потерпевший» в виктимологии: содержание и соотношение [Текст] / Е.А. Родина // Правовая культура. – 2020. – № 1(40). – С. 135-149 (0,8 а.л.).

2. *Родина, Е.А.* Киберпространство как криминологическая категория [Текст] / Е.А. Родина // Вестник Казанского юридического института МВД России. – 2021. – № 1. – С. 66-71 (0,4 а.л.).

3. *Родина, Е.А*. Виктимологическое предупреждение преступлений в киберпространстве [Текст] / Е.А. Родина // Актуальные проблемы государства и права. – 2021. – Т. 5, № 19. – С. 510-524 (0,5 а.л.).

4. *Родина, Е.А.* Общесоциальная профилактика криминогенной виктимизации пользователей сети «Интернет» [Текст] / Е.А. Родина // Вестник Саратовской государственной юридической академии. – 2022. – № 3(162). – С. 197-206 (0,5 а.л.).

*Статьи в сборниках материалов*

*международных и всероссийских конференций*

5. *Родина, Е.А*. К вопросу о понятии «киберпространство»: взгляд на проблему [Текст] / Е.А. Родина // Юридическая наука и правоприменение: взгляд молодых ученых: сб. тез. докл. по матер. науч.-практ. конф. студентов, магистрантов, аспирантов и молодых ученых в рамках IV Международного фестиваля саратовской юридической науки (19-20 апреля 2019 г.). – Саратов: Изд-во ФГБОУ ВО «СГЮА», 2019. – С. 179-181 (0,2 а.л.).

6. *Родина, Е.А.* К вопросу об объеме понятия «потерпевший»

в уголовном праве и процессе [Текст] / Е.А. Родина // Сборник научных трудов по результатам V Международного фестиваля саратовской юридической науки / под общ. ред. С.А. Белоусова. – Саратов: Изд-во ФГБОУ ВО «СГЮА», 2020. – С. 64-65 (0,2 а.л.).

7. *Родина, Е.А.* О некоторых проблемах механизма детерминации преступности и виктимного поведения [Текст] / Е.А. Родина // Противодействие правонарушениям, совершаемым с использованием информационных технологий: сб. ст. по матер. науч.-практ. конф. / III школы-семинара молодых ученых-юристов (11 ноября 2020 г.) / отв. ред. В.В. Казаков; сост. К.А. Комогорцева; Университет прокуратуры РФ; Московский финансово-юридический университет (МФЮА). – М.: Изд-во МФЮА, 2021. – С. 163-172 (0,5 а.л.).

**Общий объем публикаций составляет 3,1 а.л.**