Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовская государственная юридическая академия»

На правах рукописи

Родина Екатерина Анатольевна

ПРОТИВОДЕЙСТВИЕ КРИМИНАЛЬНОЙ ВИКТИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ «ИНТЕРНЕТ» В КИБЕРПРОСТРАНСТВЕ

5.1.4. Уголовно-правовые науки

Диссертация
на соискание учёной степени
кандидата юридических наук

Научный руководитель –
доктор юридических наук, профессор
Варыгин Александр Николаевич

Саратов – 2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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].

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[2], причем динамика кибермошенничеств впечатляющая – например, в 2020 году она составила 75,6 %[3].

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

---

[1] Состояние преступности в России за январь – декабрь 2021 г. М., 2022 // Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/analytics (дата обращения: 07.02.2022).

[2] Там же.

[3] 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).

исследований, поскольку позволяют криминологам глубже проникать в особенности механизма преступной деятельности, его детерминации, предлагать новые и более эффективные способы предупреждения 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.

ГЛАВА 1. КИБЕРПРОСТРАНСТВО И КИБЕРПРЕСТУПНОСТЬ КАК КРИМИНОЛОГИЧЕСКИЕ КАТЕГОРИИ

§ 1. Криминологическая характеристика киберпространства и киберпреступности

Изменения, которые вносят цифровые технологии в нашу жизнь, многомерны, затрагивают самые разнообразные аспекты общественных отношений и вызывают их трансформацию. Часто они отражаются и на этической сфере, меняя границы представлений о должном и допустимом. Последнее характерно и для других изобретений. Например, распространение почтовых сообщений привело к формированию специфической письменной культуры, определённого этикета, регламентирующего обращение к адресату, формы начала и завершения письма. Всеобщая автомобилизация породила культуру вождения, неформальные нормы поведения на дороге, системы звуковых и световых сигналов. Правилом хорошего тона стало пропускать автомобили, выезжающие с второстепенной дороги в сложных условиях, даже при наличии формального преимущества, закреплённого в Правилах дорожного движения. Однако масштабы социальных последствий внедрения различных технологий несопоставимы с последствиями компьютеризации, которая оказала и продолжает оказывать могучее воздействие на общественные отношения и порождает новые правила и нормы.

Если появление первых компьютеров сопровождали сомнения относительно перспектив их распространения, то в настоящее время их количество измеряется сотнями миллионов, а если включить в их число и современные смартфоны – миллиардами. Компьютеризация приводит к изменению структуры занятости, отмиранию либо трансформации некоторых старых профессий и появлению новых. Практически нет каких-либо сфер человеческой деятельности, не охваченных этим процессом. Возникают новые этические нормы поведения в компьютерных сетях, меняются стандарты поведения и взаимоотношения людей и т.д.

Появились новые виды преступлений, охватываемые термином «компьютерная преступность», изменились способы совершения традиционных, когда злоумышленники приспосабливают возможности компьютерных технологий для своих нужд.

И, пожалуй, самое главное, сформировалась новая сфера человеческих отношений, новое пространство, обладающее специфическими характеристиками, имеющими, в том числе, и криминологическое значение.

В данной работе хотелось бы заострить внимание именно на последнем явлении в его криминологическом измерении.

В настоящее время общепринятого термина, который характеризует сферу отношений посредством компьютерной связи (компьютерных сетей), нет.

В литературе встречается термин инфосфера (компьютерная инфосфера), понимаемая как «совокупность общих и специальных программных средств создания, обработки и хранения компьютерных данных, и собственно компьютеризированные данные на любых типах носителей информации»[1].

Понятие «инфосфера» семантически является наследником таких сущностей как биосфера, ноосфера, техносфера, сама последовательность которых предполагает восхождение человечества к новым формам существования. При этом инфосфера имеет кроме собственно технологической и социально-культурную составляющую, когда «главными становятся информация, творчество и интеллектуальные технологии, а субъектом мыследеятельности является интеллектуальный работник, обладающий мастерством квалифицированно и эффективно работать со все более сложной и разнообразной информацией…»[2].

---

[1] *Бородакий Ю.В., Добродеев А.Ю., Пальчун Б.П., Болдина М.Н.* Инсайдерология – наука о нелегитимности в компьютерной инфосфере // Известия ЮФУ. Технические науки. 2008. № 8. С. 55.

[2] Подробнее см.: *Моторина И.Е.* Позитивные и негативные аспекты становления инфосферы // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2011. № 8-4 (14). С. 135.

В Российской Федерации в нормативных актах используются сходные понятия «информационная сфера», «информационная инфраструктура». Так, в Доктрине информационной безопасности Российской Федерации под «информационной сферой», в соответствии с положениями ст.1 предлагается понимать «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений»[1]. Информационная сфера, как это следует из значения составляющих этот термин слов, представляет собой область, в которой главенствуют процессы обработки информации. В свою очередь последняя, в соответствии со ст. 2 Закона РФ «Об информации, информационных технологиях и о защите информации» означает сведения (сообщения, данные) независимо от формы их представления[2].

Как видно, в указанном определении информация не привязана к способу её обработки (а нас интересует, в первую очередь, информация в её компьютерном преломлении, информация, обрабатываемая компьютерами, передаваемая по компьютерным сетям). Поэтому круг отношений, складывающихся в информационной сфере, формально выходит далеко за рамки интересующих нас компьютерных сетей. Так, в информационную сферу попадают, например, средства массовой информации, как компьютерные (сайты в сети «Интернет»), так и традиционные бумажные газеты и журналы.

---

[1] Доктрина информационной безопасности Российской Федерации (утв. указом Президента РФ от 5 декабря 2016 г. № 646) // СЗ РФ. 2016. № 50, ст. 7074.

[2] Федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. и доп. от 14 июля 2022 г., № 325-ФЗ) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I), ст. 3448; 2022. № 29 (ч. III), ст. 5292.

С точки зрения законодательной техники такой подход представляется оправданным, поскольку позволяет применять положения закона к любым возможным формам работы с информацией, абстрагируясь от технологии работы с ней.

Однако для характеристики криминогенных процессов термин «информационная сфера», на наш взгляд, не вполне удобен по следующим обстоятельствам. Во-первых, это определение является узкофункциональным, во главу угла в нем ставятся процессы обработки информации. В то время как социально значимые процессы, интересующие криминолога, порождаются, прежде всего, не обработкой информации, а возможностями удаленного взаимодействия людей посредством компьютерных сетей. Во-вторых, информационная сфера понимается не просто как всемирная компьютерная сеть, но и как информационная среда, в которой Российская Федерация осуществляет свои суверенные полномочия по обеспечению безопасности. Это следует, в частности, из характеристики внешних угроз, перечисленных в «Доктрине информационной безопасности Российской Федерации», указания на трансграничность обмена информацией для достижения целей, противоречащих интересам Российской Федерации. Трансграничность – термин, означающий пересечение границ. Трансграничность информации, таким образом, – перемещение информации через границы информационного пространства Российской Федерации. В-третьих, понятие информационной сферы не включает в себя неформальные компьютерные сети, которые не являются частью интернета (в том смысле, что не обладают общей с интернетом системой адресации ресурсов, а иногда и физически отделены от него – Tor, DarkNet (скрытая сеть), DeepWeb (глубинная сеть – сайты, которые не индексируются поисковыми системами), FidoNet (компьютерная сеть, поддерживаемая энтузиастами) и т.д.

Другим термином, обозначающим взаимодействие людей посредством компьютеров, является «киберпространство», который иногда понимается как

область взаимодействия информационных систем различного уровня, включающих следующие элементы: компьютерные системы, сети (как глобальные, так и локальные), компьютерные программы пользователей, а также данные, циркулирующие в перечисленных элементах[1].

Данный термин в отечественной правовой литературе применяется с конца XX века[2] и является, скорее всего, калькой с английского «cyberspace», т.е. «кибернетическое пространство», «виртуальное пространство», появившегося впервые в литературных произведениях жанра «киберпанк» американо-канадского писателя Уильяма Гибсона в начале 80-х годов XX века. Ещё одним возможным значением этого термина является «виртуальная реальность» – то есть реальность, обладающая отдельными атрибутами физического пространства, но не существующая в материальном мире.

Постепенно термин «киберпространство» вышел за рамки фантастических книг, и стал активно применяться социологами и юристами как удобная социально-философская абстракция, описывающая специфические взаимодействия людей посредством компьютерных сетей. При изучении литературы нам встретились упоминания киберпространства в связи с изучением морально-этических аспектов виртуальной свободы[3], отдельных аспектов боевых действий[4], трансформаций медицинских технологий[5], сложных взаимодействий людей в социальных сетях[6], преступного поведения[1]

---

[1] *Шевченко* Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … канд. юрид. наук. М., 2016. С. 37.

[2] *Федотов М.А.* Киберпространство как сфера обитания права // Бюллетень ЮНЕСКО по авторскому праву. 1998. №2 (т. XXXII). С. 21.

[3] *Кот Я.И.* Нравственные аспекты свободы в киберпространстве // Гуманитарный вестник. 2018. № 11. С. 1.

[4] *Гриняев С.Н., Правиков Д.И.* Основы общей теории киберпространства. теория боя в киберпространстве. М.: АНО ЦСОиП, 2018. С. 40.

[5] *Хмель П.С.* Правовое регулирование медицинского киберпространства // Актуальные вопросы современной медицины: матер. II Дальневосточного медицинского молодежного форума / под ред. Е.Н. Сазоновой. 2018. Владивосток, 2018. С. 148.

[6] *Егоров Н.С., Туркина В.Г.* Человек в социальных сетях киберпространства // Современные научные исследования и разработки. 2018. Т. 1. № 4 (21). С. 196.

и т.д.

Какие свойства киберпространства характеризуют его как действительно некое самостоятельное явление, представляющее криминологический интерес? На наш взгляд, к их числу можно отнести следующие:

- киберпространство в некоторой степени сходно с обычным физическим пространством: в нем есть аналоги перемещения (например, при переходе по гиперссылкам от одного сайта к другому). Оно, с точки зрения обычного пользователя компьютерной сети, является бесконечным (количество сайтов только в сети WWW (общедоступная часть сети «Интернет», так называемая World Wide Web, всемирная сеть) превышает 1,7 млрд[2] и продолжает расти). Пространство сети раскрывается постепенно с возрастанием опыта пользователя, открывая ему все новые и новые ресурсы. Увлечённые пользователи могут найти здесь почти любую интересующую их информацию, в том числе, недоступную другим, имеют возможности для неограниченного профессионального роста в части понимания устройства сети, программирования и т.п. Неудивительно, что завсегдатаи киберпространства обретают чувство превосходства над обычными пользователями и пытаются проверить свои возрастающие навыки, в том числе, и преступным путём (например, взломом сайтов и получением несанкционированного доступа к хранящейся на них информации);
- киберпространство, как и обычное пространство, имеет зоны общего доступа, так и части, недоступные не только для непосвящённых, но и для контроля со стороны государства. Здесь концентрируется киберпреступность – торговля наркотиками, порнографией, оружием, контрафактной продукцией, незаконные денежные переводы и т.д.;

---

[1] *Бутусова Л.И.* К вопросу о киберпреступности в международном праве // Вестник экономической безопасности. 2016. № 2. С. 48.

[2] Как росло количество веб-сайтов в мире. URL: https://www.kommersant.ru/doc/4147760 (дата обращения 20.07.2020).

- в киберпространстве, как и в физическом пространстве, информация имеет привязку к определённому месту (например, она хранится на винчестере конкретного компьютера или в сети компьютеров). Таким образом, возникает аналогия между «своей» и «чужой» информацией, проникновением на чужую территорию. Полагаем, что это обуславливает и сходство психических механизмов, лежащих в основе мотивации преступников, совершающих традиционные общеуголовные преступления, и злоумышленников, действующих в киберпространстве. Проводится разделение киберпространства и на межгосударственном уровне. Например, Российская Федерация в обязательном порядке требует от владельцев социальных сетей размещения учётных данных пользователей на серверах, которые физически расположены на территории нашей страны. Распространение государственного суверенитета на информационные ресурсы предопределяет и возникновение враждебной деятельности иностранных государств и отдельных лиц по поводу этих ресурсов. Впрочем, здесь есть и существенные отличия, о которых будет сказано далее;
- как и в физическом пространстве, деятельность преступников в его кибернетическом аналоге оставляет следы, по которым их можно обнаружить. Компьютерные преступники, как и обычные, обладают целым арсеналом средств, затрудняющих обнаружение следов своей деятельности, идентификацию и обнаружение.

Хотелось бы остановиться и на отличительных признаках киберпространства, которые позволяют некоторым авторам говорить о новой реальности[1] и обуславливают криминологический интерес к этому явлению.

Одним из важных факторов, провоцирующих людей на несвойственное им поведение, является анонимность пользователей в киберпространстве.

---

[1] *Иконникова С.Н., Большаков В.П.* История культурологических теорий. СПб.: Издательский дом «Питер», 2005. С. 51 и след.

В реальном мире они опасаются совершать некоторые действия из-за контроля со стороны родственников, супругов, знакомых, из страха причинения ущерба репутации и т.п. Полагая, что в киберпространстве они останутся незамеченными, такие «путешественники» могут стать лёгкой добычей при посещении различных «злачных мест» – сайтов, на которых размещается запрещённый контент, предлагаются незаконные услуги и т.д.

Подобное поведение в физическом пространстве демонстрируют мигранты, выпавшие из привычной социальной среды и сопутствующих ограничений и демонстрирующие в новой стране нетипичное для своей обычной жизни поведение.

Ещё одним важным последствием анонимности в киберпространстве является возможность для граждан находить партнёров для реализации самых экзотических фантазий, которые в реальном мире, скорее всего, остались бы нереализованными в силу упомянутых выше причин. В киберпространстве такие антикриминогенные факторы отсутствуют. В результате в нем формируются группы, практикующие немыслимые в обычной жизни способы реализации самых изощрённых фантазий. Речь может идти и о совместных самоубийствах, о причинении себе увечий (порезов, прижиганий кожи), об убийствах и даже каннибализме по совместной договорённости с жертвой[1]. Именно в киберпространстве стало возможным такое явление как игры, в которые вовлекают несовершеннолетних с целью склонения их к самоубийству.

Таким образом, в киберпространстве поведение людей свободно от ограничений, накладываемых обычно на них обществом, культурой, религией и т.д.

Безграничность киберпространства позволяет людям находить единомышленников, тогда как, в физическом мире они так и оставались бы

[1] Речь идет об Арвине Майвесе, убившего, а затем съевшем немецкого программиста Юргена Брандеса с его добровольного согласия. См.: Interview mit dem Kannibalen von Rotenburghttps. URL: www.welt.de/fernsehen/article1269371/Interview-mit-dem-Kannibalen-von-Rotenburg.html (дата обращения 21.07.2020).

неуслышанными одиночками. Сообщества, образующиеся в киберпространстве, формируют специфическое мировоззрение, систему ценностей, вырабатывают собственные регламенты поведения. Здесь стоит упомянуть о таком, немыслимом ранее, явлении как «Wikileaks», публикующем секретную информацию, попадающую в руки участникам сообщества в результате утечек, от сочувствующих идеям цифровой свободы служащих государственных организаций и т.п. Несмотря на арест основателя этой организации, Джулиана Ассанжа, прекратить деятельность «Wikileaks» в киберпространстве до настоящего времени США, главному «потерпевшему» от деятельности этой организации, не удалось[1]. Таким образом, налицо одна отличительная особенность киберпространства – в нем одиночки или небольшие группы могут какое-то время противостоять мощи государственных спецслужб, как это было с Джулианом Ассанжем или Эдвардом Сноуденом, опубликовавшим информацию о преступлениях американской армии в Ираке и бежавшим от преследования в Россию. В этом же ряду стоит упомянуть эпопею с безуспешными в течение многих месяцев попытками блокировать интернет-мессенджер «Telegramm» в Российской Федерации.

Ещё одна особенность киберпространства связана с временными характеристиками совершаемых в нем деяний. Во многих случаях таких, к примеру, как размещение незаконного контента, опубликование экстремистских высказываний на каком-либо сайте, может длиться неопределённо долгое время. Если в обычном мире экстремистское высказывание ограничено коротким промежутком времени, то будучи размещённым в сети, оно останется там навсегда. Даже если деятель пожелает убрать его со страницы, оно может разойтись во множестве копий по другим сайтам, попасть в архив интернета и т.д. То же самое касается вредоносных программ: попав в сеть, они копируются и продолжают свою деятельность

[1] На момент написания работы сайт «Wikileaks» был доступен по адресу: https://wikileaks.org/

неопределённое количество времени. С уголовно-правовой точки зрения можно вести речь об аналоге длящихся преступлений, с тем только отличием, что продолжительность их осуществления в киберпространстве может не зависеть от воли злоумышленника.

Хотелось бы также обратить внимание на следующее обстоятельство. В киберпространстве, как ни в какой другой области человеческой деятельности, огромна разница между специалистом (программистом, системным администратором, хакером-взломщиком, специалистом по кибербезопасности) и обычным пользователем компьютера. Киберпространство, несмотря на видимую простоту использования, в основе своей – высокотехнологичная система. Знание особенностей её функционирования неинтересно и непонятно рядовым пользователям, что не оставляет последним ни единого шанса защитить свои права в столкновении с киберпреступником-профессионалом.

Выше говорилось об аналогии между границами информации и границами в реальном мире. Однако и здесь у киберпространства есть существенное отличие. В последнее время в связи с повышением активности государств (не только России), пытающихся усилить контроль над национальными информационными ресурсами, появились и новые средства противодействия государственной активности. В частности, мощным оружием против государственного надзора является децентрализация информации – когда определённый контент, переписка и т.д. не хранится в одном месте, а разбивается на мелкие фрагменты, которые шифруются и размещаются на множестве сайтов. Таким образом, для киберпреступников, как замечают Е.А. Антонян и Е.В. Бархатова, не существует границ и юрисдикций[1].

Впрочем, если в начале 2000-х годов общим местом публикаций о компьютерных сетях было указание на их неподконтрольность власти, то в

[1] *Антонян Е.А., Бархатова Е.В.*.Противодействие киберпреступности // Евразийский союз ученых. 2019. № 7-4. С. 55.

настоящее время в подобных оценках следует проявлять большую осторожность. Пример Китая показывает, что государство при наличии политической воли и технологического потенциала может в значительной степени контролировать информационные потоки в национальном сегменте киберпространства, принуждать иностранные компании подчиняться своему законодательству, ограничивать выдаваемую гражданам страны информацию и т.п.[1]

Также появлялась информация о том, что в Иране во время беспорядков, инициированных и поддерживаемых из-за рубежа, резко снизился исходящий из страны трафик, т.е. государство фактически закрыло доступ граждан к информационным ресурсам других стран[2].

Завершая обзор особенностей киберпространства, представляющих криминологический интерес, хотелось бы обратить внимание на то, какое большое значение имеет «произнесённое» в нем слово. Самые популярные блоггеры, видеоблоггеры, авторы страниц в популярных сетях имеют аудиторию, сравнимую, а иногда и превосходящую аудиторию традиционных средств массовой информации (телевидения, печати, радио). Эта ситуация вызывает естественное беспокойство у государств, утрачивающих монополию на формирование мировоззрения своих граждан.

Видимо, в силу этого в действующем УК РФ предусматривается ответственность за размещение некоторых видов высказываний: оправдание терроризма (ст. 205^2), реабилитация нацизма (ст. 354^1) и др. И здесь очевидно явное злоупотребление законодателя мерами уголовной репрессии. Общественная опасность тех или иных деяний определяется и масштабом их воздействия на общественные отношения. В киберпространстве эти масштабы

---

[1] В Китае вступает в силу резонансный закон о кибербезопасности. URL: https://ria.ru/20170601/1495523455.html (дата обращения 21.07.2020).

[2] *Френкель Д., Бородихин А.* «Мы дали отпор врагу». Иранские власти отключили страну от интернета. URL: https://yandex.ru/turbo/s/zona.media/article/2019/11/20/iran-404 (дата обращения 21.07.2020).

определяются популярностью автора соответствующих текстов. Очевидно, что влияние на умы авторов, имеющих миллионы просмотров, несравнимо с подавляющим большинством обычных пользователей сети (по большей части уголовные дела возбуждаются в отношении пользователей сети «ВКонтакте»), чьи аудитории исчисляются, в лучшем случае, десятками или сотнями человек, причём, в случае экстремистских высказываний их адресатами выступают, как правило, друзья или единомышленники. Поэтому и общественное значение соответствующих высказываний ничтожно. Зачастую общество узнает о них лишь после возбуждения уголовных дел по соответствующим статьям УК РФ.

Полагаем, что складывающаяся практика, формально соответствуя букве уголовного закона, противоречит его духу, идее заложенной законодателем. Предупредительный эффект таких мер ничтожен и, наоборот, даже имеет негативную окраску – внимание граждан привлекается к той информации, от которой их государство хотело бы оградить.

Чтобы избежать подобного нежелательного эффекта, предлагается учитывать количество просмотров соответствующих текстов и популярность в киберпространстве их авторов в качестве криминоообразующих или квалифицирующих признаков по статьям УК РФ, предусматривающих уголовную ответственность за экстремизм, терроризм, реабилитацию нацизма и т. п.[1]

В целом, подводя итог рассуждениям, хотелось бы отметить, что термин «киберпространство», на наш взгляд, является исключительно удачным для описания реальности, возникшей с приходом в нашу жизнь компьютерных сетей. Он свободен от нормативной нагрузки, которой отягощено сходное понятие «информационная сфера». За годы массовой компьютеризации представления о киберпространстве развились в массовом сознании, наполнились глубокими смыслами, аналогиями, делающими этот термин

[1] *Родина Е.А.* Киберпространство как криминологическая категория // Вестник Казанского юридического института МВД России. 2021. № 1. С. 70.

понятным даже далёким от техники людям. Поэтому считаем использование этого термина предпочтительным для анализа криминогенных и виктимогенных детерминант, действующих в компьютерных сетях.

Само же определение киберпространства, полагаем, должно выглядеть следующим образом: *киберпространство – 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.*

Определив, таким образом, сущность понятия «киберпространство», в рамках криминологического исследования неминуемо возникает вопрос о том, какие посягательства порождают потерпевших пользователей киберпространства.

В литературе в последнее время наряду с термином «киберпространство» стало активно использоваться понятие «киберпреступность», призванное подчеркнуть отличие совершаемых в киберпространстве преступлений от посягательств, предусмотренных главой 28 «Преступления в сфере компьютерной информации» УК РФ, иначе именуемых компьютерными преступлениями. Отмечается, что «киберпреступность» – наиболее оптимальный термин, охватывающий всю совокупность преступлений в сфере информационно-телекоммуникационных сетей[1].

Действительно, терминологический анализ показывает, что киберпреступность по своему содержанию шире, чем преступления в сфере компьютерной информации. Соотношение между этими понятиями, на наш взгляд, носит характер отношения части и целого. Если для констатации факта совершения преступления в сфере компьютерной информации достаточно совершения отдельных действий в отношении любого компьютера, даже не

[1] *Шатилов А.В.* Особенности криминологической характеристики и предупреждения мошенничества, совершаемого организованными преступными формированиями: дис. … канд. юрид. наук. Саратов, 2019. С. 52, 53 и др.

подключенного к какой-либо сети, то киберпреступность подразумевает обязательно воздействие, которое осуществляется через сети на удаленные устройства. Другим отличием, на наш взгляд, является то, что перечень преступлений в сфере компьютерной информации является исчерпывающим, в то время как киберпреступления и киберпреступность не связаны с каким-то отдельным видом преступлений. Теоретически к киберпреступлениям могут быть отнесены любые преступления, предусмотренные уголовным законодательством.

Изучение теоретической литературы позволило выявить различные подходы к определению киберпреступности. Как отмечает В.С. Овчинский, из числа 200 актов национального законодательства, менее чем в 5 % этот термин присутствовал в названии или содержании правовых норм[1].

В некоторых случаях она отождествляется с преступлениями в сфере компьютерной информации, предусмотренных главой 28 УК РФ[2].

Встречается подход, при котором киберпреступность связывается с определенными технологиями. Так, Е.П. Ищенко приводит определение киберпреступности, содержащееся в отдельных документах ООН, в соответствии с которыми под киберпреступностью понимаются преступления в сфере высоких информационных технологий, совершаемые злоумышленниками, использующими эти технологии в противоправных целях»[3].

Нам такая дефиниция представляется неудачной, поскольку она базируется на использовании достаточно расплывчатого термина «высокие

---

[1] *Овчинский В.С.* Криминология цифрового мира: учебник для магистратуры. М.: НОРМА: ИНФРА-М, 2018. С. 68.

[2] *Козлова О.Е., Самойлова А.В., Твердохлебова Э.В.* Перспективы применения положительного опыта зарубежных стран в борьбе с киберпреступностью в Российской Федерации // Актуальные научные исследования в современном мире. 2020. № 8-5 (64). С. 44.

[3] *Ищенко Е.П.* О криминалистическом обеспечении раскрытия и расследования киберпреступлений // Деятельность правоохранительных органов в современных условиях: сб. матер. 20-й междунар. науч.-практ. конф. (28-29 мая 2015 г.). В 2 т. Т. 1. Иркутск: Изд-во Вост.-Сиб. ин-та МВД России, 2015. С. 336.

информационные технологии», который при желании можно толковать как угодно. В узком смысле – это могут быть преступления, использующие самые последние достижения в сфере цифровых технологий. В широком – любые посягательства, основанные на достаточно архаичных методах, например, посредством проводной телефонной связи. Вызывает несогласие и используемое словосочетание «сфера высоких технологий». Технология, в соответствии со словарным определением, – это «…совокупность методов и процессов определенного производства, а также научное описание способов производства»[1]. Толкование термина «сфера высоких технологий», в строгом соответствии с приведенным определением, приводит нас к выводу, что киберпреступления – это преступления, связанные с методами и процессами производства высокотехнологичной компьютерной техники, устройств связи и проч. Очевидно, что такое понимание чрезмерно сужает анализируемое понятие и лишает его практического смысла. В то же время, как и говорилось, отступление от формального определения размывает содержание киберпреступности.

Часто киберпреступность определяется через базовое понятие – «киберпространство» (киберпреступность – это преступления, совершаемые в киберпространстве)[2], однако и здесь имеет место большое разнообразие, связанное с отдельными смысловыми нюансами, имеющими большое значение для правоприменения.

В отдельных международных документах и работах отечественных криминологов, опирающихся на них, встречается определение киберпреступности как совокупности преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем,

[1] *Ожегов С.И., Шведова Н.Ю.* Толковый словарь русского языка. М., 2006. С. 797.

[2] См., напр.: *Вепрев С.Б., Нестерович С.А.* 2018. Киберпреступность как новая форма преступности // Расследование преступлений: проблемы и пути их решения. 2018. № 3. С. 79.

компьютерных сетей и компьютерных данных[1].

С нашей точки зрения, приведенное определение имеет то достоинство, что в качестве существенного, неотъемлемого признака киберпреступности называет киберпространство. Вместе с тем с формальной, уголовно-правовой точки зрения нельзя говорить о киберпространстве как о таком факультативном признаке совершения преступления, как место совершения преступления, поскольку физически деяние совершается все же в реальном, физическом пространстве. Преступник, находясь в точно определенном месте, совершает посредством компьютерной техники манипуляции, а отдаваемые им управляющие сигналы передаются через сети к удаленным устройствам. Таким образом, позиция «киберпреступность – это преступность в киберпространстве» не вполне корректно, поскольку трактует киберпространство как место совершения преступления.

Однако в этом определении есть верное, на наш взгляд, указание на то, что киберпространство является и средством совершения преступления, поскольку термин «киберпространство» в данном контексте содержит указание на то, что удаленное воздействие осуществляется посредством использования технических средств и сетей.

Как отмечают авторы учебника «Цифровая криминология», Конвенция о преступности в сфере компьютерной информации 2001 года предусматривает 4 группы киберпреступлений: против конфиденциальности, целостности и доступности компьютерных данных и систем; связанные с компьютерами; с контентом; с правами собственности[2].

---

[1] См., напр.: Всестороннее исследование проблемы киберпреступности. URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 13.11.2021); *Тропина Т.Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. … канд. юрид. наук. Владивосток, 2005. С. 9; *Номоконов В.А.*, *Тропина Т.Л.* Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1. С. 45 и др.

[2] *Антонян Е.А.* Международное сотрудничество в сфере противодействия кибертерроризма // Правовой альманах, 2022. № 2. С. 11; *Ищук Я.Г., Пинкевич Т.В.,*

В качестве недостатка подобных определений можно отметить, что в качестве объекта воздействия называются компьютерные системы, сети и компьютерные данные. С точки зрения действующего уголовного права такое понимание объекта неприемлемо, поскольку традиционно для нас в качестве объекта воздействия рассматривается какое-либо общественное отношение, благо, интерес[1].

Впрочем, в настоящее время представлены и иные воззрения на объект. И.П. Семченков, например, указывает, что объектом посягательства всегда будет человек[2]. Хотя принципиально такое понимание объекта посягательства не влияет на высказанное нами ранее соображение – компьютерные системы и данные в любом случае не могут признаваться объектом посягательства.

Наконец, еще одна позиция, выявленная нами, состоит в том, что киберпреступность не связывается с определенными объектами посягательства. В отчете Управления ООН по наркотикам и преступности «Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств – членов международного сообщества и частного сектора» отмечается, что содержание термина «киберпреступность» зависит от контекста. В его общепринятом определении нет нужды, поскольку в электронных носителях и в сетях может быть информация, имеющая отношение к любым преступлениям, как совершаемых в киберпространстве, так и в обычном физическом пространстве[3].

Сходную позицию высказал в своем диссертационном исследовании М.А. Простосердов, охарактеризовавший киберпреступление как

Смольянинов Е.С. Цифровая криминология: учебное пособие. М.: Академия управления МВД России, 2021. С. 98.

[1] *Верина Г.В.* Об истоках современных концепций объекта преступления // Уголовное право. 2016. № 1. С. 4.

[2] *Семченков И.П.* Объект преступления: социально-философские и методологические аспекты проблемы: автореф. дис. … канд. юрид. наук. М., 2003. С. 7.

[3] UNODC. Comprehensive Study on Cybercrime. February 2013. P. xvii. URL: https://www.studymode.com/essays/Comprehensive-Study-On-Cybercrime-51826748.html (дата обращения: 13.11.2021).

посягательство «на разнородные общественные отношения, совершаемое дистанционно, путем использования средств компьютерной техники и информационно-телекоммуникационных сетей и образованного ими киберпространства»[1].

В определении М.А. Простосердова правильно, на наш взгляд, определено киберпространство как средство совершения преступления (оно образовано средствами компьютерной техники и компьютерных сетей), справедливо отмечается возможность причинения вреда самым различным общественным отношениям.

Иногда вместо термина «киберпространство» используют синонимичные словосочетания, не меняющие основной сути киберпреступности. Так, С.В. Воронцова определяет ее как преступность в виртуальном пространстве, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в локальных и глобальных сетях[2].

Здесь, как видно, используется термин «виртуальное пространство», которое содержит определенные сведения, т.е., по сути, сочетает в себе компьютеры с находящимися на них данными и компьютерные сети.

В определении С.В. Воронцовой импонирует отсутствие указания на определенный объект посягательства, поскольку нами разделяется точка зрения, что киберпреступления способны причинять вред любым объектам уголовно-правовой охраны. А поскольку объект посягательства может быть любым, то и указание на него в определении лишено смысла. Однако термин «виртуальное пространство» неудачен: он не является общепринятым, а следовательно не наделен общепринятым содержанием.

Учитывая изложенное, попытаемся сформулировать собственное

---

[1] *Простосердов М.А.* Экономические преступления, совершаемые в киберпространстве, и меры противодействия им. Диссертация … кандидата юридических наук. М., 2016. С. 43.

[2] *Воронцова С.В.* Киберпреступность: проблемы квалификации преступных деяний // Российская юстиция. 2011. № 2. С. 14.

определение киберпреступности на основе данного ранее понятия «киберпространство» с учетом достоинств и недостатков представленных в литературе определений, а также общепринятого в отечественной криминологии определения преступности.

Под киберпреступностью предлагается понимать совокупность преступлений, совершаемых за определенный период времени посредством возможностей, предоставляемым киберпространством.

Анализ показывает, что киберпреступления могут посягать на самые различные объекты. Еще 20 лет назад на многообъектность таких посягательств обращал внимание С.Ю.Бытко[1].

В 2012 году В.А. Номоконов и Т.Л.Тропина в зависимости от объекта и предмета посягательства в самостоятельные группы выделяли экономические компьютерные преступления, компьютерные преступления против личных прав и неприкосновенности личной жизни, компьютерные преступления против общественных и государственных интересов[2].

И, наконец, в 2017 году это обстоятельство признано официально. Свидетельством этому является появление в статистических сборниках МВД РФ, начиная с этого года, нового раздела «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации».

В литературе отмечается, что осуществление полноценного криминологического анализа киберпреступности, так как это можно было бы сделать с общеуголовными преступлениями, вряд ли возможно.

В.А. Номоконов и Т.Л.Тропина в числе обстоятельств, существенно затрудняющих исследование, указывают трансграничность киберпреступности.

---

[1] *Бытко* С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис. … канд. юрид. наук. Саратов, 2002. С. 8-9.

[2] *Номоконов В.А., Тропина Т.Л.* Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1. С. 48.

Официальная статистика, как указывают эти авторы, не способна дать представление об истинных масштабах явления[1].

Отмечается также, что в настоящее время отсутствует не только релевантная статистика киберпреступности, но и надежные методы сбора соответствующих данных[2].

Соглашаясь с приведенными мнениями, отметим, что в Российской Федерации постепенно возрастает объем статистической информации по киберпреступлениям, однако более-менее подробные данные публикуются лишь, начиная с 2019 года, что ограничивает глубину анализа.

При таких условиях вполне естественно, что киберпреступность характеризуется высокой латентностью, достигающей в России более 90 %, в США – 80 %, в Великобритании – до 85 %, в ФРГ – 75 %[3].

В качестве факторов латентности называются непрерывно возрастающий объем информации о киберпреступности, нахождение необходимой информации на серверах, не принадлежащих Российской Федерации, сложность установления лиц, совершающих конкретные киберпреступления, нежелание компаний заявлять о фактах совершенных в отношении них киберпреступлениях[4].

Действительно, официальная статистика подтверждает беспрецедентный рост киберпреступлений, количество которых в 2020 году возросло по сравнению с 2017 годом (когда впервые в статистических данных появилась соответствующая информация) более чем в 5 раз (таблица № 1) и преступлений в сфере компьютерной информации (таблица № 2).

Поэтому вал сообщений, захлестывающий правоохранительные органы,

---

[1] *Номоконов В.А., Тропина Т.Л.* Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1. С. 46.

[2] *Gercke, M.* Understanding Cybercrime: A Guide for Developing Countries. ITU, 2009. P. 19; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[3] Kabay M. Studies and Surveys of Computer Crime. Northfield, 2001. P. 2.

[4] *Бойко О.А., Унукович А.С.* Детерминанты латентных преступлений, совершаемых с использованием информационно-коммуникационных технологий // Юридический вестник Самарского университета. 2020. № 3. С. 55.

полагаем, способствует дальнейшему росту уровня латентности таких посягательств.

Таблица № 1. Общее количество зарегистрированных преступлений с использованием информационно-телекоммуникационных технологий

	2017	**2018**	**2019**	**2020**	**2021**
Количество преступлений	90587	174674	294409	510396	517722

Таблица № 2. Сведения о зарегистрированных преступлениях в сфере компьютерной информации за 2016-2020 гг.

	2016	**2017**	**2018**	**2019**	**2020**	**2021**
Количество преступлений	1748	1883	2500	2883	4498	6869

Еще одним фактором, затрудняющим их выявление и раскрытие, как отмечают С.Б. Вепрев и С.А. Нестерович, является возрастающая связь киберпреступности и организованной преступной деятельности[1].

Данное обстоятельство подтверждается и результатами других исследований. В частности, в диссертационном исследовании А.В. Шатилова приводится ряд характерных примеров мошенничеств, совершаемых организованными группами, в том числе, в киберпространстве, когда до задержания преступники совершали десятки и сотни преступлений[2].

Из числа всех киберпреступлений наиболее быстро растет число посягательств, совершаемых с применением платежных карт (прирост в 2020 году составил +453,1 % по сравнению с 2019 годом), с использованием средств мобильной связи (+88,3 %), сети «Интернет» (+91,3%), (таблица № 3). При этом нужно понимать, что в последних двух случаях речь идет, скорее всего, об одних и тех же преступлениях, поскольку использование мобильной связи, в

[1] *Вепрев С.Б., Нестерович С.А.* 2018. Киберпреступность как новая форма преступности // Расследование преступлений: проблемы и пути их решения. 2018. № 3. С. 80.

[2] *Шатилов А.В.* Особенности криминологической характеристики и предупреждения мошенничества, совершаемого организованными преступными формированиями: дис. … канд. юрид. наук. Саратов, 2019. С. 52, 53 и др.

подавляющем большинстве случаев, предполагает и использование сети «Интернет».

При этом наблюдается возрастание доли общеуголовных преступлений, совершаемых в общей массе соответствующих посягательств. Так, из 774 159 краж, совершенных в 2019 году, 98 798 краж, или 12,8 %, было совершено с применением информационно-телекоммуникационных технологий (как правило, это снятие денег с чужих пластиковых карт). Количество таких краж по сравнению с 2018 годом возросло на 200,2 %. А в 2020 году таких краж было почти в 2 раза больше – 173 416, доля таких преступлений в общей массе краж в 2020 году составила уже 23,1 %. В 2021 году удельный вес подобных краж несколько снизился в пределах статистической погрешности и составил 20,3 % в общей их массе.

Таблица № 3. Характеристика средств и способов совершения преступлений с использованием информационно-телекоммуникационных технологий

	с применением пластиковых карт	**с применением комп. техники**	**с применением программного обеспечения**	**фиктивные электронные платежи**	**с использованием сети «Интернет»**	**с использованием средств мобильной связи**
2019	34383	18261	6283	984	157036	116154
2020	190167	28653	10050	1374	300337	218739

Если говорить о мошенничествах, то удельный вес кибермошенничеств составил в 2019 году 54,7 % в общей массе мошенничеств, а в 2020 году – уже 72,3 %. (таблица № 4).

Таким образом, статистические данные свидетельствуют о тенденции переноса преступной деятельности по общеуголовным корыстным преступлениям в киберпространство. Это объясняется, во-первых, меньшими рисками привлечения к уголовной ответственности, во-вторых, большими преступными доходами и, в-третьих, что связано с предыдущим соображением, с возможностью охвата большего числа потерпевших.

Таблица № 4. Количество отдельных видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий,

в общей массе таких преступлений

Годы/ст.УК	158	159	159.3	159.6	272	273	274, 274.1
2019	98798	119903	16119	687	2420	455	8
2020	173416	210493	25820	761	4105	371	22
2021	156792	238560	10258	431	6392	317	160

Содержащиеся в данных официальной статистики показатели не отражают реального числа совершаемых киберпреступлений. С учетом высокой степени их латентности, число подобных посягательств может значительно превышать официальную цифру 517722 преступлений (таблица № 1).

По данным заместителя председателя Сбербанка С.К. Кузнецова, мошенники в 2020 году совершили около 15 млн звонков обычным гражданам с целью обмана[1].

В сообщениях служб безопасности называется еще большее число. Так, средний мошеннический кол-центр осуществляет от 3 до 7 тысяч звонков в сутки. В половине случаев операторы не дозваниваются. Успешными для мошенников оказываются 1 % дозвонов[2] (или 30-70 оконченных мошенничеств).

В другом сообщении специалистов Сбербанка указывается общее количество мошеннических звонков из преступных кол-центров в 100 тысяч в сутки[3]. При этом 80 % звонков идут с подменных телефонных номеров. Количество жалоб на мошеннические действия выросло в 2020 году по сравнению с 2017 годом в 30 раз, а по сравнению с 2019 годом – более чем в 2

[1] «Сбер» оценил количество мошеннических звонков в России в 15 миллионов с начала 2020 года. URL: https://vc.ru/finance/186662-sber-ocenil-kolichestvo-moshennicheskih-zvonkov-v-rossii-v-15-millionov-s-nachala-2020-goda (дата обращения: 28.12.2020).

[2] Сбербанк подсчитал, сколько мошенники крадут со счетов россиян в месяц. URL: https://ria.ru/20210609/moshenniki-1736229634.html (дата обращения: 17.07.2021).

[3] Сбербанк назвал телефонное мошенничество национальным бедствием. URL: https://ria.ru/20210707/moshennichestvo-1740256569.html (дата обращения: 17.07.2021).

раза[1].

Если исходить из приведенной цифры в 100 тысяч звонков в день, то за год их количество составит 35,6 млн. С учётом числа зарегистрированных мошенничеств, равного 335 631, можно вывести уровень латентности, превышающий 99 %.

Таким образом, 99 % звонков представляют собой уголовно-наказуемые покушения на мошенничество. С учётом того, что в подавляющем большинстве потерпевшие обращаются в правоохранительные органы лишь при оконченных преступлениях, можно было бы оценить уровень латентности кибермошенничеств в 99 %. Однако, думаем, фактический уровень латентности ещё выше. В пользу этого свидетельствуют результаты проведённого нами анкетирования, в ходе которого было установлено, что из числа тех, кто становился жертвой мошенничества, в правоохранительные органы обращалось лишь 13,3 % потерпевших. Остальные сочли размер похищенного несущественным и не стали обращаться за помощью государства. Проанкетированные нами граждане, обращавшиеся с заявлениями о совершённых в отношении них преступлений, также отметили низкую результативность работы правоохранительных органов. О раскрытии преступлений не заявил никто из проанкетированных, а уголовные дела возбуждались лишь по 30,8 % заявлений.

Общее количество потерпевших от зарегистрированных преступлений в стране оценивается по данным Росстата цифрой порядка 1 млн 335 тысяч человек. С учетом того, что по многим киберпреступлениям может быть более одного потерпевшего, а общее количество киберпреступлений (т. е. в терминологии официальной статистики – преступлений, совершаемых с использованием информационно-коммуникационных технологий) превышает полмиллиона, то реальное число потерпевших от оконченных

[1] Банки и операторы запустят сервисы против подмены номеров мошенниками. URL: https://www.rbc.ru/society/12/12/2020/5fd446c49a7947746aba6e19 (дата обращения: 28.12.2020).

киберпреступлений в стране значительно превышает 500 тысяч человек. С учетом неоконченных посягательств, количество граждан, вступающих в контакт с киберпреступниками, как было показано ранее, исчисляется несколькими миллионами человек в год. И это обстоятельство переводит киберпреступность в разряд не только социальных, но и политических проблем, так как граждане, по большей части, противостоят преступным посягательствам в одиночку, не видят ощутимых результатов правоохранительной деятельности в этой сфере и формируют на основе этого претензии к бездействию государства.

В данной работе не рассматривается ряд преступлений, совершаемых в сети «Интернет», такие как незаконные организация и проведение азартных игр (ст. 171^2 УК РФ), незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (ст. 228^1 УК РФ), публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ) и некоторых других, постольку, поскольку в них отсутствует как таковая фигура потерпевшего. Исключение составляют посягательства, связанные с вовлечением несовершеннолетних в противоправную деятельность, когда сам факт вовлечения причиняет вред интересам нормального развития и воспитания последних. Такие случаи рассматриваются в работе. Кроме того, здесь не освещены проблемы краж, совершаемых с использованием платежных карт, поскольку виктимизация потерпевших в большинстве подобных случаев осуществляется за пределами киберпространства.

Статистическая информация о преступлениях, совершаемых с использованием информационно-коммуникационных сетей, свидетельствует, как уже говорилось, об их взрывном росте, хронологически совпадающем с эпидемией коронавирусной инфекции (COVID-19). Как отмечается

в специальных исследованиях, криминальный мир пытается извлечь из этого явления максимальную прибыль и адаптирует к условиям пандемии новые виды кибератак[1]. Другое объяснение связывает это явление с резкими изменениями хозяйственного уклада, вызванными массовыми карантинными ограничениями, появлением новых форм мошенничества, возрастанием числа покупок в интернет-магазинах и т.д. и т.п.[2]

Действительно, рост киберпреступности имеет временную привязку к карантинным ограничениям и с высокой степенью вероятности порожден ими. В соответствии с принципом «post hoc, ergo propter hoc» («после» не значит «вследствие») пока нельзя это утверждать определенно, однако множество наблюдаемых фактов свидетельствует о наличии причинной связи между предпринимаемыми карантинными мерами и ростом киберпреступности.

Если исходить из того, что такая зависимость существует, то, основываясь на дальнейших планах Правительства РФ о развитии комплекса карантинных мероприятий, прежде всего, связанных с повсеместным введением QR-кодов для граждан, получивших прививку от коронавируса и ограничением прав остальных[3] (здесь не будут обсуждаться проблемы соответствия подобных мер Конституции РФ), можно с уверенностью утверждать, что рост киберпреступности только ускорится. Причины этого будут связаны с тем, что в условиях ограничений на посещение отдельных учреждений, граждане будут активнее использовать возможности онлайн-торговли, пытаться обойти ограничения попыткой приобретения поддельных

---

[1] *Жданов Ю.Н., Кузнецов С.К., Овчинский В.С.* COVID-19: преступность, кибербезопасность, общество, полиция. М.: Международные отношения, 2020. С. 211-213.

[2] См., напр.: Coronavirus: The impact on crime and criminal networks. URL: https://globalinitiative.net/analysis/crime-contagion-impact-covid-crime/ (дата обращения: 14.11.2021); *Warrell Helen, Fildes Nic.* Cyber criminals exploit coronavirus disruption. Financial Times. 2020. March 16; *Уразалиев М.* Вопросы криминализации общества в условиях пандемии – новые угрозы и вызовы // Review of Law Sciences. 2020. С. 192-197. *Петров И.* Затишье перед бурей: как COVID-2019 повлияет на преступность // Известия. 2020. 26 мар. и др.

[3] В ГД внесены законопроекты об использовании QR-кодов в общественных местах и на транспорте. URL: http://duma.gov.ru/news/52707/ (дата обращения: 14.11.2021).

QR-кодов, осуществлять подкуп должностных лиц, прибегать к услугам хакеров и т.п. В частности, по состоянию на ноябрь 2021 года на сайте бесплатных объявлений «Avito.ru» уже появилось множество объявлений, в которых граждане, имеющие QR-коды, предлагают за плату приобретать продукты питания, товары народного потребления и даже одежду (указывают свои размеры, по которым будут примерять обувь, одежду).

В средствах массовой информации появляется информация о подделке сертификатов о вакцинации от коронавируса[1].

Нет никакого сомнения, что попытки усиления ограничительных мер в отношении непривитых выступят мощнейшим криминогенным фактором, и нас уже в самом скором будущем ожидает еще более значительный рост киберпреступности. Скорее всего, он будет связан с появлением новых видов мошенничеств, однако можно ожидать и массового переноса в киберпространство и других общеуголовных преступлений, таких, например, как подделка документов, подкуп должностных лиц и т.п.

Таким образом, проведенный анализ позволяет сделать следующие выводы.

1. Киберпространство – 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.

2. Киберпреступность – совокупность преступлений, совершаемых за определенный период времени посредством возможностей, предоставляемым киберпространством.

3. Масштабы и скорость распространения киберпреступности, большое количество потерпевших от нее, переводят ее из разряда социальных проблем в

[1] На Кубани с середины года выявили 17 случаев подделки сертификатов о вакцинации. URL: https://tass.ru/obschestvo/12906209?utm_source=yxnews&utm_medium=desktop&nw=1636888000000 (дата обращения: 14.11.2021).

политические, когда неспособность государства быстро обуздать ее рост может трансформироваться в недовольство государством в целом.

4. Причины взрывного роста киберпреступности в последние два года связаны с карантинными ограничениями. Развитие таких ограничений неминуемо ускорит рост киберпреступности и появление ее новых разновидностей.

§ 2. Проблемы криминальной виктимизации пользователей сети «Интернет» в киберпространстве

Основным понятием виктимологии является «жертва» или «потерпевший». Иногда эти понятия предлагается использовать как синонимы, имея в виду, что оба относятся к преступлению. Поэтому в криминологических исследованиях более точно было бы говорить о «жертве преступления» или «потерпевшем от преступления». Содержание этих понятий и их соотношение между собой определяются по-разному.

Термин жертва является переводом с латинского «viktima». В русском языке этот термин означает «приносимый в дар божеству предмет или убиваемое живое существо, кого-либо страдающего от насилия, несчастья, неудачи»[1]. Мифологический и религиозный подтекст данного понятия объясняется тем, что отдельные типы жертв, выделяемые в теории виктимологии, имеют прообразы в мифологических или религиозных сюжетах (например, Эдипова жертва, синдром Авеля и т.п.)[2].

Этимология термина «потерпевший» в этимологических словарях не рассматривается, видимо, в силу ее очевидности. Толковый словарь В. Даля содержит определение слова «потерпеть» – претерпеть, понести на себе,

---

[1] Этимологический словарь современного русского языка / сост. А. К. Шапашников: в 2 т. Т. 1. М.: Флинта: Наука, 210. С. 269.

[2] *Смирнов А.М.* Виктимология сексуальных инверсий. М.: Юрлитинформ, 2012. С. 9-10.

испытать, вынести тягость, бедствие; подвергнуться, подпасть беде[1].

В истории уголовного законодательства России «потерпевший» появляется в Уложении о наказаниях уголовных и исправительных 1845 года, при этом данное слово всегда сопровождалось уточнением, от чего или что лицо потерпело. Например, в ст. 1712 предписывается «потерпевшему от того убыток предоставляется искать на виновном удовлетворения установленным порядком»[2]. В ст. 177 Устава о наказаниях, налагаемых мировыми судьями 1864 года, наказание для виновного в присвоении или растрате чужого имущества смягчается, если «растрата была совершена по легкомыслию и виновные добровольно обязываются вознаградить потерпевшему убыток»[3].

В уголовных законах советского периода термин «потерпевший» упоминается, как и в действующем УК РФ, без дополнительных уточнений. В настоящее время это понятие можно рассматривать в качестве правового. Оно часто встречается в статьях Общей и Особенной части УК РФ. Соответствующие дефиниции имеются в УПК РФ и КоАП РФ.

В соответствии с положениями ст. 42 УПК РФ потерпевшими могут быть физические лица, которым преступлением был причинен физический, имущественный, моральный вред, а также юридические лица, если преступление причиняет вред их имуществу или деловой репутации.

В ч. 1 ст. 25 КоАП РФ указано, что потерпевшими от административных правонарушений могут быть как физические, так и юридические лица, которым административным правонарушением причинен физический, имущественный или моральный вред.

Как видим, имеется небольшое формальное отличие в определении потерпевших по делам об административных правонарушениях и о

---

[1] Даль В.И. Словарь живого великорусского языка в 4 т. Т. 3. М: РИПОЛ классик, 2006. С. 350-351.

[2] *Бытко Ю.И., Бытко С.Ю.* Сборник нормативных актов по уголовному праву России X-XX веков. Саратов, 2006. С. 364.

[3] Там же. С. 464.

преступлениях: в КоАП РФ ими могут быть юридические лица, которым может быть причинен физический вред, а в УПК РФ для них предусматривается только имущественный или репутационный ущерб.

Анализируемый термин применяется и в гражданском законодательстве. Например, в ст. 1101 ГК РФ размер компенсации устанавливается в зависимости от характера причиненных потерпевшему физических и нравственных страданий.

В теоретической литературе было высказано мнение о том, что в криминальной виктимологии оправдано использование как равнозначных понятий терминов «потерпевший» и «жертва преступления», однако, при обозначении жертв-носителей криминально обусловленной и, тем более, реализованной виктимности, предпочтительным является термин «потерпевший»[1]. Основатель отечественной виктимологии Л.В. Франк допускал использование синонимов слова «потерпевший», в особенности, термина «жертва», для более точного описания отдельных смысловых нюансов фигуры потерпевшего от преступления[2]. Однако в праве последнее понятие не является однозначно определённым.

В УК РФ в большинстве случаев термин «потерпевший» применяется по отношению к физическим лицам, причём во многих случаях – исключительно к этой категории. В частности, в ряду смягчающих обстоятельств предусмотрены: противоправность или аморальность поведения потерпевшего, явившегося поводом для преступления (п. «з» ч. 1 ст. 61) и оказание медицинской и иной помощи потерпевшему непосредственно после совершения преступления, добровольное возмещение имущественного ущерба и морального вреда, причинённых в результате преступления, иные действия, направленные на заглаживание вреда, причинённого потерпевшему (п. «к» ч. 1 ст. 61). Среди отягчающих обстоятельств предусмотрено совершение

[1] *Ривман Д.В.* Криминальная виктимология. СПб.: Питер, 2002. С. 34.

[2] *Франк Л.В.* Потерпевшие от преступления и проблемы советской виктимологии. Душанбе: Ирфон, 1977. С. 9.

преступления с особой жестокостью, садизмом, издевательством, а также мучениями для потерпевшего (п. «и» ч. 1 ст. 63). Ряд норм Особенной части УК РФ предусматривает в качестве квалифицирующих признаков наступление последствий, характерных только для физических лиц: убийство в состоянии аффекта (ст. 107), доведение до самоубийства (ст. 110), умышленное причинение тяжкого вреда здоровью, повлекшее по неосторожности смерть потерпевшего (ч. 4 ст. 111) и т.д.

В ряде случаев в качестве потерпевших упоминаются наравне с физическими лицами организации, общество и государство (например, при злоупотреблении должностными полномочиями в ст. 285 УК РФ).

Название главы 20 «Преступления против семьи и несовершеннолетних» УК РФ свидетельствует о том, что в качестве потерпевших от преступлений могут выступать и семьи.

Таким образом, в УК РФ имеет место указание на то, что вред от преступления может причиняться широкому кругу субъектов. При этом следует учитывать, что в конструкции уголовно-правовых норм законодатель решает, прежде всего, не терминологические проблемы виктимологии, а специфические задачи. Указание на последствия как обязательный признак объективной стороны материальных составов преступлений является способом конкретизировать объект посягательства и степень его опасности. Как указывает А.В. Наумов, законодатель избирает способ конструирования объективной стороны с учётом и в зависимости от характера и специфических особенностей общественной опасности соответствующего преступления[1].

Несмотря на то, что собственного определения потерпевшего в УК РФ не содержится, теоретиками уголовного права отмечается, что содержание этого понятия не совпадает с таковым в уголовно-процессуальном праве и является

[1] *Наумов А.В.* Российское уголовное право: курс лекций: в 2 т. Т. 1. Общая часть. 3-е изд., перераб. и доп. М.: Юрид. лит., 2004. С. 192.

первичным по отношению к последнему[1]. В уголовном праве фигура потерпевшего возникает с момента наступления предусмотренных объективной стороной состава последствий, а в формальных составах – с момента совершения деяний, указанных в диспозиции статьи. В уголовно-процессуальном праве потерпевший появляется значительно позже – лишь с момента возбуждения уголовного дела и оформления соответствующего постановления, либо с момента получения данных о лице, которым преступлением был причинен вред (ч. 1 ст. 42 УПК РФ).

Однако даже в УПК РФ, в ряде случаев, это понятие используется в уголовно-правовом смысле. Например, в ч. 3 ст. 20 УПК РФ указывается, что уголовные дела частно-публичного обвинения возбуждаются только по заявлению потерпевшего. При этом, как отмечает Д.В. Шаров, до возбуждения уголовного дела лицо не может быть признано потерпевшим в порядке ст. 42 УПК РФ. Следовательно, здесь речь может идти о понимании потерпевшего только в уголовно-правовом смысле[2].

Следует иметь в виду, что в ряде случаев при совершении преступления уголовные дела не возбуждаются. Ст. 24 УПК РФ содержит перечень соответствующих оснований, включающий такие, как истечение сроков давности уголовного преследования; смерть подозреваемого, обвиняемого; отсутствие заявления потерпевшего, в случаях, когда это является необходимым условием возбуждения уголовного дела и т.д.

В подобных случаях в уголовно-процессуальном смысле фигура потерпевшего не появляется, в то время как фактически (в уголовно-правовом смысле) она есть.

Исходя из изложенного, следует признать верным утверждение, что

---

[1] См., напр.: *Красиков А.Н.* Сущность и значение согласия потерпевшего в советском уголовном праве. Саратов: изд-во Сарат. ун-та, 1976. С. 45-46.

[2] *Шаров Д.В.* Соотношение уголовно-процессуального и уголовно-правового понятий потерпевшего: проблемы и пути их решения // Вестник Московского университета МВД России. 2013. № 7. С. 81.

виктимологическое понятие «потерпевший» не может быть связано с аналогичным понятием в уголовном процессе. Одновременно ошибочным представляется утверждение о том, что впервые жертва, а точнее, потерпевший как субъект правоотношений возникает в уголовном процессе[1], поскольку она возникает еще до момента возникновения уголовно-процессуальных отношений.

С виктимологической точки зрения важно разграничить понятие потерпевшего в административном и уголовно-процессуальном законодательстве. Несмотря на то, что криминальная виктимология обращается, преимущественно, к изучению жертв преступлений, реалии современного права таковы, что необходимо выходить за границы преступного поведения. В теории уголовного права активной и обоснованной критике подвергается институт административной преюдиции[2]. Однако законодатель в последнее время последовательно расширяет её использование в качестве криминообразующего признака отдельных составов преступлений. Например, условием уголовной ответственности по ст. 158[1] УК РФ является совершение мелкого хищения лицом, подвергнутым административному наказанию за мелкое хищение, предусмотренное ч. 2 ст. 7.27 КоАП РФ. Исходя из содержания диспозиции ст. 158[1] УК РФ, одни и те же граждане в некоторых случаях могут быть потерпевшими от административного правонарушения, а если имеет место административная преюдиция, то одновременно и от преступления. Таким образом, виктимологическая информация о жертве преступления и о процессах ее виктимизации актуальна и для жертв правонарушений.

Следует также иметь в виду, что в отличие от УПК РФ, в КоАП РФ не предусмотрено специальной процедуры для признания лица потерпевшим.

---

[1] *Бойко О.А., Хоменко А.Н., Пестерева Ю.С., Бражников В.В.* Актуальные проблемы виктимологии: учебное пособие. Омск: Омская юридическая академия, 2017. С. 19.

[2] *Лопашенко Н.А.* Административной преюдиции в уголовном праве – нет! // Вестник Академии Генеральной прокуратуры Российской Федерации. 2011. № 3. С. 64.

Соответствующая информация указывается в протоколе об административном правонарушении в соответствии с ч. 2 ст. 28.2 КоАП РФ, либо в постановлении прокурора о возбуждении дела об административном правонарушении в соответствии со ст. 28.4 КоАП РФ. В теории административного права имеется мнение, что появление фигуры потерпевшего не связано с процессуальными действиями, а обусловлено реальным причинением вреда совершением административного правонарушения[1].

Если же рассматривать гражданское законодательство, то здесь понятие «потерпевший» может быть связано с фактом причинения вреда административным правонарушением, преступлением либо с действиями, не являющимися правонарушением.

Указанные ранее обстоятельства свидетельствуют о том, что не только уголовно-процессуальное, но и административно-правовое или гражданско-правовое понятие потерпевшего не может являться базовым для соответствующего виктимологического термина.

Ввиду изложенного полагаем, что, определяя объем понятия о жертве преступления в виктимологическом смысле, необходимо исходить из положений не процессуального, а материального права, которое является первичным и определяет наиболее существенные признаки жертвы, состоящие, прежде всего, в причинении вреда её разнообразным правам и интересам путём совершения противоправных деяний. Хотя и при таком подходе виктимологическое определение потерпевшего будет шире правового. Если рассматривать неоконченные преступления или преступления с формальными составами, то вред потерпевшим может фактически и не причиняться. В п. 2 постановления Пленума Верховного Суда РФ «О практике применения судами

---

[1] См., напр.: *Бахрах Д.Н., Герман Е.С.* Вопросы административно-процессуального статуса потерпевшего в производстве по делам об административных правонарушениях // Современное право. 2010. № 5. С. 115; *Новиков В.П.* Физические и юридические лица как потерпевшие по делам об административных правонарушениях: автореф. дис. ... канд. юрид. наук. М., 2004. 24 с.

норм, регламентирующих участие потерпевшего в уголовном судопроизводстве» при разрешении вопроса о признании лиц потерпевшими в подобных случаях судам предписывается выяснять, в чем конкретно выразился вред[1]. С учётом позиции Верховного Суда РФ в тех случаях, когда вред не причиняется, фигура потерпевшего в уголовном деле не возникает. Однако криминологов такое решение не удовлетворяет, поскольку все факторы, интересующие нас при изучении жертв преступления, имеют место и при неоконченных преступлениях, и при совершении посягательств, в составы которых законодатель по тем или иным соображениям не включил наступление общественно опасных последствий (например, при посягательстве на жизнь сотрудника правоохранительных органов, предусмотренном ст. 317 УК РФ).

В теории виктимологии нет однозначного подхода относительно того, кого следует признавать жертвой преступления. Часть криминологов полагают, что таковой могут признаваться только физические лица. Другие относят к ним не только отдельных людей, но и их общности. Третьи расширяют круг жертв за счёт таких институтов, как все общество, государство и даже международный порядок[2].

Определение круга потерпевших осуществляется криминологами на основе анализа положений ст. 42 УПК РФ, потерпевших по статьям, предусмотренных Особенной частью УК РФ, названия глав и статей Особенной части УК РФ[3]. Однако такой подход нам представляется формальным. Как отмечалось ранее, указывая на лица, организации, которым причиняется вред (здесь, прежде всего, имеются в виду положения УК РФ), законодатель

---

[1] Постановление Пленума Верховного Суда РФ от 29 июня 2010 г. № 17 (с изм. и доп. от 16 мая 2017 г., № 17) «О практике применения судами норм, регламентирующих участие потерпевшего в уголовном судопроизводстве» // Бюллетень Верховного Суда РФ. 2010. № 9.

[2] Подробный анализ подходов к определению круга жертв см., напр.: *Ривман Д.В.* Криминальная виктимология. СПб.: Питер, 2002. С, 35; *Кабанов П.А., Маргизов Р.Р.* Криминологическая виктимология: учебное пособие. Казань: Изд-во Казан. ун-та, 2018. С. 6-10;

[3] См., напр.: *Сабитов Р.А.* Соотношение понятий «потерпевший от преступления», «пострадавший от преступления» и «жертва преступления» // Виктимология. 2014. № 1. С. 17.

преследует цели уточнения специфических характеристик преступления. Полагаем, что виктимология, преследуя собственные интересы, не должна ограничиваться пределами, установленными законодателем.

Не вызывает сомнения общепринятое представление о том, что к числу жертв преступлений следует относить физических лиц, подкреплённое ссылкой на солидный международный источник – Декларацию основных принципов правосудия для жертв преступления и злоупотребления властью, п. 1 которой определяет жертв как лиц, которым индивидуально или коллективно действием или бездействием, нарушающим национальный уголовный закон, был причинён ущерб[1].

В п. 2 этой же Декларации указывается, что понятие жертвы может быть расширено за счёт близких родственников или иждивенцев непосредственной жертвы, а также лиц, которым был причинён ущерб при попытке оказать помощь жертвам, находящимся в бедственном положении, или предотвратить виктимизацию[2]. Аналогичное положение содержится и в УПК РФ, п. 8 ст. 42 которого указывает, что по уголовным делам о преступлениях, последствием которых явилась смерть лица, права потерпевшего, предусмотренные настоящей статьей, переходят к одному из его близких родственников и (или) близких лиц, а при их отсутствии или невозможности их участия в уголовном судопроизводстве – к одному из родственников.

Здесь следует заметить, что с точки зрения охраны прав и свобод граждан, отнесение к числу потерпевших близких лиц является, несомненно, необходимой мерой. Однако указание в УПК РФ на то, что такие лица не становятся потерпевшими, а лишь получают права таковых, свидетельствует о том, что с виктимологической точки зрения такая правовая манипуляция имеет

---

[1] Декларация основных принципов правосудия для жертв преступления и злоупотребления властью: принята резолюцией 40/34 Генеральной Ассамблеи ООН от 29 ноября 1985 г. // Международные акты о правах человека: сб. док. М.: НОРМА-ИНФРА, 1998. С. 165.

[2] Там же.

весьма ограниченное практическое значение лишь в части возмещения причинённого преступлением ущерба[1]. Между тем, наделяя близких лиц правами потерпевших законодатель, прежде всего, преследует цель обеспечения непрерывности уголовного процесса. Потерпевшие получают ряд прав (например, на защиту) и обязанностей (давать показания). Однако поведение таких лиц в период, предшествующий совершению преступления нас, как правило, не интересует, поскольку оно, строго говоря, не является виктимным, не оно спровоцировало преступление, не оно привлекло преступников, а изучение таких лиц вряд ли может пролить дополнительный свет на причины и условия совершаемых преступлений и меры по их предупреждению.

Если же говорить о коллективах лиц как о жертвах, то в виктимологической литературе приводятся примеры виктимности отдельных социально-демографических групп (женщин, престарелых, инвалидов, молодёжи и детей, мигрантов и т.п.)[2]. Однако, на наш взгляд, групповая виктимность не тождественна жертвам в виде коллективов лиц, упоминаемых в п. 1 Декларации основных принципов правосудия для жертв преступления и злоупотребления властью. В последнем случае речь идёт, по нашему мнению, именно о коллективах, т.е. связанных общими интересами, правами и обязанностями группах физических лиц, например пациентах больницы, членов трудовых коллективов, отдельных семьях и т.п.

В теории представлено мнение, что в круг виктимологического изучения необходимо включить и жертв - юридических лиц. Обосновывая его, П.А. Кабанов и Р.Р. Маргизов ссылаются на ст. 42 УПК РФ[3]. Это предложение вызывает ряд вопросов, требующих теоретического осмысления.

---

[1] О предмете и задачах виктимологии подробнее см.: *Полубинский В.И.* Фундаментальные и прикладные начала криминальной виктимологии. М.: ВНИИ МВД России, 2010. С. 70-75.

[2] См., напр.: *Варчук Т.В., Вишневецкий К.В.* Виктимология. М.: ЮНИТИ-ДАНА, 2017. С. 73-92.

[3] *Кабанов П.А., Маргизов Р.Р.* Указ. соч. С. 9.

В.И. Полубинский, говоря о задачах виктимологии, видит их, в частности, в том, чтобы проявить закономерности упречного, отрицательного поведения пострадавшего, механизм его взаимоотношений с правонарушителем[1]. Однако в какой мере можно говорить об упречном поведении юридического лица? А.О. Харитонов и Н.М. Александрина, исследовавшие виктимизацию юридических лиц (в терминологии авторов – корпоративную виктимизацию), характеризуют ее как процесс превращения юридического лица в жертву преступления, протекающий в форме виктимного поведения как отдельных представителей, так и группы лиц корпорации в условиях криминогенно-виктимогенного взаимодействия преступника и его жертвы и завершающийся причинением юридическому лицу вреда преступлением[2]. Механизм процесса, приведённый в определении понятен. Говоря о деятельности юридических лиц, необходимо подразумевать исполнение ими договорных обязательств, осуществление деятельности в соответствии с уставом организации и прочее. Однако в криминологическом смысле имеют значения лишь действия сотрудников юридического лица, которые выполняют, не выполняют, либо выполняют не в полном объёме предписанные трудовыми соглашениями действия, создающие условия для совершения преступлений против интересов юридического лица. Однако в анализируемом определении имеется терминологическая неточность, состоящая в том, что виктимным поведением обладает, с точки зрения его авторов, не только само юридическое лицо (в терминологии авторов – корпорация), но и отдельные её представители. Поскольку виктимное поведение – это поведение жертвы, то из приведённого определения следует, что жертвами в подобных случаях выступают не только юридические лица, но и работники. Однако это противоречит исходной посылке авторов.

---

[1] *Полубинский В. И.* Указ. соч. С. 70-71.

[2] *Харитонов А.О., Александрина Н.М.* Системный подход к исследованию корпоративной виктимизации // Современная экономика: актуальные вопросы, достижения и инновации: сб. ст. IX междунар. науч.-практ. конф. Пенза, 2017. С. 229.

Полагаем, что А.О. Харитонов и Н.М. Александрина имели в виду такое упречное поведение сотрудников, при котором юридическое лицо становится уязвимым для преступных посягательств.

Однако затем эти авторы в качестве факторов виктимности корпораций приводят ряд обстоятельств, которые могут привести к противоположенным выводам. Как они пишут, корпорации становятся привлекательными в качестве жертв, если они обладают такими признаками, как наличие неконсолидированного пакета акций (что характерно для акционерных обществ); успешность бизнеса; наличие привлекательных активов; жёсткая конкуренция на рынке; наличие конфликтов между участниками и акционерами; неконтролируемая кредиторская задолженность[1]. Обращает на себя внимание то, что успешность бизнеса несовместима с упречным поведением сотрудников корпорации. Скорее наоборот – качественное выполнение обязанностей всеми сотрудниками является предпосылкой успешности бизнеса. Здесь налицо парадокс – как плохое, так и образцовое исполнение обязанностей сотрудниками корпорации одинаково могут сделать её уязвимой для преступного воздействия. В какой-то мере сказанное распространяется и на такой фактор виктимности, как наличие привлекательных активов, поскольку формирование последних может быть связано с успешностью бизнеса.

Имеется ещё один аспект виктимности юридических лиц, остающийся вне поля зрения исследователей. Жертвами большей части посягательств на интересы юридических лиц, являются компании, осуществляющие предпринимательскую деятельность, основной целью которой является извлечение прибыли. Поэтому в большинстве случаев причинения вреда страдают не только сами юридические лица, их имущественные права, но и стоящие за ними владельцы, акционеры и т.д. Например, члены преступного сообщества Матюшев, Жданов и Кулабухов путем использования ошибок в

[1] Там же. С. 230.

программном обеспечении незаконно получили доступ к реквизитам банковских карт множества граждан. Используя эти данные, они приобретали железнодорожные билеты, которые затем возвращали по украденным паспортам, обналичивая таким образом украденные со счетов граждан деньги[1]. В данном случае потерпевшими будут банки, чья компьютерная информация о реквизитах банковских карт стала известна злоумышленникам, и граждане, являющиеся владельцами этих карт. С точки зрения уголовного права здесь имеет место совокупность преступлений, предусмотренных ст. 272 и 159[6] УК РФ, однако с позиций криминологии имеет место сложная преступная схема, в которой эти преступления являются неотъемлемыми звеньями единого замысла. Поэтому в данном случае можно говорить о смешанной виктимности, когда потерпевшими одновременно будут выступать и граждане и юридические лица. Думаем, что в большинстве случаев посягательств на интересы коммерческих организаций имеет место смешанная виктимность.

Наконец, следует остановиться на точке зрения, согласно которой в качестве потерпевшего может выступать государство. Действующий УК РФ, равно как и предшествующие ему уголовные законы, предусматривает ответственность за посягательства против государства. К таковым, например, относятся преступления, включённые в раздел X «Преступления против государственной власти», ряд экономических преступлений (например, налоговых) и т. д. Однако с криминологической точки зрения полагать государство жертвой считаем нецелесообразным. Полагаем, что не дело криминологов вмешиваться в политические процессы, порождающие такие преступления. Кроме того, во многих случаях соответствующие посягательства порождаются непреклонной и последовательной государственной политикой, как это происходит, к примеру с преступлениями террористического характера. Поэтому в таких случаях формулирование предложений по изменению

[1] *Петров И.* Крах «билетной мафии»: киберворам дали рекордные сроки. URL: https://iz.ru/958391/ivan-petrov/krakh-biletnoi-mafii-kibervoram-dali-rekordnye-sroki (дата обращения 27.12.2019).

государственной политики в интересах профилактики отдельных видов преступлений явно выходит за рамки предмета криминологии. Обратим внимание на то, что такие посягательства всегда связаны с причинением вреда организациям или физическим лицам, поэтому здесь, с точки зрения виктимологии, следует говорить о смешанной виктимности, а виктимологическая профилактика будет осуществляться в традиционных формах – устранением различных нарушений в организации деятельности предприятий и учреждений, их должностных лиц и т.п.

С учетом изложенного полагаем, что *под жертвой следует понимать физическое или юридическое лицо, которым в результате совершения общественно опасного деяния причиняется или создается угроза причинения ущерба*.

Отсутствие указания в данном определении на преступность деяния связано с тем, что, как уже говорилось, в деянии могут отсутствовать некоторые признаки состава преступления.

Применительно к жертвам киберпреступлений указанное определение следует модифицировать следующим образом: *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 криминологической теории проблема детерминации преступности является одной из самых сложных. Несмотря на то, что теории причинности развиваются уже длительное время, до настоящего времени здесь есть ряд неясных вопросов. Ещё более слабо развита теория виктимологической детерминации, которая начала развиваться значительно позже, и в которой до настоящего времени, как указывает К.В. Вишневецкий, вопрос о механизме виктимного поступка и системе его детерминации до настоящего времени остаётся открытым, поскольку преступник и жертва – индивидуально и

типологически разные люди[1].

Не стоит говорить о том, что проблематика виктимологической детерминации преступлений, совершаемых в сети «Интернет», и виктимологического предупреждения таких преступлений, разработаны в ещё меньшей степени.

Поэтому, прежде чем строить научно-обоснованную систему виктимологического предупреждения преступлений в сети «Интернет» необходимо прояснить авторское отношение к некоторым неразрешённым общим вопросам причинности.

Необходимость исследования этого вопроса, на наш взгляд, обусловлена тем, что предупреждение преступности, как и любая целенаправленная деятельность, нуждается в точном определении желаемых результатов воздействия. В связи с этим необходимо разграничить виктимологическую профилактику от специально-криминологической – с тем чтобы определить объекты воздействия в обоих случаях. И, если они не совпадают, ставить вопрос о нормативном определении виктимологической профилактики. Для этого нужно уяснить, какое место в детерминации преступлений занимают обстоятельства, относящиеся к его жертве, являются ли они лишь условиями, или могут выступать и в качестве причин совершаемого преступления.

В отдельных работах по криминологии встречаются пессимистические взгляды относительно возможностей корректно определить причины преступлений. Так, Е.Г. Самовичев, характеризуя современную концепцию причин преступности, отметил, что она не выдерживает никакой критики, поскольку никаких причин в строгом смысле слова установить не удаётся[2].

---

[1] *Вишневецкий К.В.* Механизм виктимологической детерминации // Теория и практика общественного развития. 2014. № 10. С. 154.

[2] Здесь приводится выдержка из стенограммы научно-практического межвузовского семинара «Какая криминология сегодня нужна стране? (Проблемы преподавания и практического применения)», прошедшего 19 апреля 2011 г. Цит. по: *Фадеев В.Н.* Причинность в криминологии и детерминация преступности // Криминология: вчера, сегодня, завтра. 2017. № 3 (46). С. 23.

В.Н. Фадеев, в ходе глубокого анализа современной концепции причинности, приходит даже к более радикальному выводу о необходимости в объяснении причин преступности отказаться от материализма и сформулировать новую концепцию[1].

В качестве основной проблемы он указывает на то, что разработанный в криминологической теории комплекс представлений о причинах, условиях, факторах и детерминации преступности с точки зрения диалектической логики функционален лишь на уровне частного, но не общего[2].

Разделяем мнение, что в объяснении причин преступности всё «хорошо работает» на уровне единичных преступлений, однако попытка перенести эти объяснения на уровень всей преступности упирается в необходимость возвращать к жизни отвергнутые ранее положения позитивистской школы, и поэтому криминологи, как отметил Е.Г. Самовичев, уводят проблематику «в сферу системности, сложности», уклоняясь от предметного объяснения.

Проиллюстрируем сказанное на примере. Если говорить о сущности причинной связи, то в соответствии с определением, она состоит в производстве причиной следствия. Причина – это внутренняя связь между тем, что уже есть и тем, что им порождается, им только становится[3].

В приложении к преступному поведению это означает, что причина – это то, что со всей необходимостью, закономерно побуждает лицо совершить общественно опасное деяние. Здесь уместно вспомнить, что фундаментальной предпосылкой юридической ответственности является свобода воли индивида. Таким образом, в юриспруденции и, наиболее детально, в уголовном праве в настоящее время определено, что уголовная ответственность устанавливается лишь в отношении вменяемых лиц, т.е. лиц, осознающих фактический характер своих действий и способных руководить ими или, иными словами,

---

[1] *Фадеев В.Н.* Причинность в криминологии и детерминация преступности // Криминология: вчера, сегодня, завтра. 2017. № 3 (46). С. 24.

[2] Там же. С. 23.

[3] Философский энциклопедический словарь. М.: Сов. энциклопедия, 1983. С. 532.

обладающими свободой воли. Неспособность хоть в малейшей степени осознавать фактический характер своих действий или руководить ими является, в соответствии со ст. 21 УК РФ, признаком невменяемости, исключающей уголовную ответственность.

Сказанное означает, что причина любого преступления лежит не в сфере общественной жизни, как указывается во многих учебниках криминологии[1], не в особенностях экономических отношений, имущественном неравенстве, несправедливости и т.п., а в личности преступника. Как писал Н.А. Стручков, непосредственные причины преступления находятся в сфере сознания, поскольку все побудительные силы, вызывающие действия человека, должны обязательно пройти через его голову и превратиться в побуждения его воли[2].

По поводу того, как формируются эти побуждения воли, есть несколько объяснений. А.И. Долгова указывала, что традиционно-диалектический подход предусматривает односторонне влияние объективных факторов преступности на субъективные: «материальные условия жизни людей определяют общественное сознание, а уже оно – преступность. Отсюда оценка общественной психологии (ранее упоминалось в связи с этим об «отставании сознания от бытия») как непосредственной, ближайшей причины преступности[3].

Э.А. Поздняков в своей работе «Философия преступления» красной нитью проводит мысль, что причина совершения преступлений состоит, прежде всего, в том, что человек от природы склонен к отклоняющемуся поведению. Такое поведение – не патология, а норма[4].

Этому мнению вторит В.Н. Фадеев, по мнению которого «корни

---

[1] Как, к примеру, писал М.Д. Шаргородский, причины конкретного преступления – это … те активные силы, которые вызывают у субъектов интересы и мотивы для его совершения». См.: *Шаргородский М.Д.* Преступность, её причины и условия в социалистическом обществе // Преступность и ее предупреждение. Л., 1966. С. 30.

[2] *Стручков Н.А.* Преступность как социальное явление: лекции. Л., 1979. 120 с.

[3] *Долгова А.И.* С. Криминология: учебник для вузов / под общ. ред. А.И. Долговой. 3-е изд., перераб. и доп. М.: Норма, 2005. С. 258-259.

[4] *Поздняков Э.А.* Философия преступления. М., 2001.

преступности кроются в самой дуально-диалектической природе человека, как социально-биологического существа, а плохие условия жизни людей являются лишь катализатором, ускоряющим проявление правонарушающего, «криминального начала» в сознании и жизни индивидуума»[1].

Таким образом, имеются две точки зрения на непосредственную причину преступности, плохо совместимые между собой для того, чтобы уместить их в единой теории. Нетрудно заметить, что абсолютизация каждой из них возвратит нас на те же теоретические позиции, которые сложились в криминологии больше ста лет назад (мы имеем в виду социологическое и антропологическое направление в криминологии). При этом обе эти позиции слабо совместимы и с представлениями о свободе воли, лежащей в основе уголовной ответственности. Однако у этих взглядов есть и нечто общее – причинами единичного преступления можно называть некоторые особенности личности, делающие для соответствующего индивида позволительным совершение преступления для реализации своих потребностей (иногда в таких случаях говорят о деформациях личности). В криминологии эта часть причинного комплекса сконцентрирована в представлениях о формировании личности преступника и обычно «выносится за скобки» в рассуждениях о причинах конкретного преступления, ограничивая их изучение относительно небольшим интервалом времени, связанным с негативными изменениями в личности отдельного человека.

Зафиксировав это, перейдём к следующему проблемному вопросу теории детерминации. Оставив за кадром рассуждения о том, как формируются побудительные мотивы, обратимся к тому, как в теории происходит переход от рассмотрения причин единичного преступления к причинам всей преступности.

Приняв за отправную точку то, что в обществе есть определённая группа лиц, склонных в силу имеющихся деформаций к совершению преступлений,

---

[1] *Фадеев В.Н.* Причинность в криминологии и детерминация преступности // Криминология: вчера, сегодня, завтра. 2017. № 3 (46). С. 24.

можно ожидать, что при возникновении неблагоприятных внешних условий или в случае возникновения удобной ситуации они будут интенсивно этим заниматься.

Однако здесь возникает следующая сложность: имея возможность заранее определить количество совершаемых преступлений, нельзя точно предположить, кто именно их совершит. Так, изучая статистические данные МВД, Генеральной прокуратуры, Судебного департамента при Верховном Суде РФ за ряд лет, можно прогнозировать, что в 2021 году будет зарегистрировано около 7 тысяч убийств и покушений на убийство. Уверенность нашим ожиданиям придаёт то, что в течение ряда лет количество таких преступлений постоянно снижалось и, несмотря на то, что в стране в связи с неблагополучной эпидемиологической обстановкой наблюдаются и негативные процессы в экономике, каких-либо катастрофических сценариев изменения преступности не наблюдается.

Также можно очертить и примерный круг лиц, совершивших такие преступления: как правило, это граждане, не имеющие постоянного места работы, недавно освободившиеся из мест лишения свободы и злоупотребляющие алкоголем[1].

Казалось бы: вот точно очерченный объект для специально-криминологического воздействия, и нужно всего лишь подвергнуть профилактическому воздействию силами правоохранительных органов 3,6 млн безработных (по данным Росстата), чтобы радикально снизить не только количество убийств, но и целый ряд других посягательств против личности и собственности. Однако, по всей видимости, даже такое количество потенциальных подозреваемых составляет чрезмерную нагрузку на нашу

[1] По данным С.Ю. Бытко, более 70 % убийств совершается в состоянии алкогольного опьянения, и доля таких лиц постоянно растёт, более 70 % убийц не имели места работы, примерно треть из них – имеют неснятую или непогашенную судимость. См.: *Бытко С.Ю.* Эффективность предупредительного воздействия уголовного наказания на преступность: теоретический и прикладной аспекты: дис. … д-ра юрид. наук. Саратов, 2018. С. 56, 65 и др.

правоохранительную систему. Сузить же их круг, вычленив из этой массы всего 5-6 тысяч наиболее вероятных убийц, к нашему огромному разочарованию, нельзя. И здесь возникает один из самых сложных вопросов – как сочетать представления о причинности как проявлении закономерных процессов, хорошо работающих на уровне конкретного преступления, с вероятностными результатами, возникающими при рассмотрении массовых проявлений преступности и попытках прогноза индивидуального поведения? Проблема в том, что включение в процесс детерминации стохастического элемента полностью обесценивает все предшествующие рассуждения о механизме детерминации, поскольку, согласно теории вероятности, вероятность совершения преступления будет определяться уже не строго детерминированными закономерностями в поведении человека, а именно той, не поддающейся полноценному исследованию, случайностью. Так, для рассмотренных ранее убийств, вероятность успешного поиска возможного убийцы на основе приведённых данных о его личности во всей массе безработных составляет, по нашим оценкам, 0,15 %. Для организации целенаправленной государственной деятельности такой прогноз бесполезен и равносилен отсутствию всякого прогноза.

Возможно, именно такой низкой результативностью прогнозов и обусловлена потеря государством интереса к результатам криминологических исследований. Интересно, что сходная ситуация сложилась с исследованиями склонности к преступному поведению на основе анализа дерматоглифической картины рук. Так, изучение дерматоглифики серийных маньяков показало, что все они обладают редким типом асимметрии в распределении узоров. Для А. Чикатило, как указывают авторы работы, была характерна локализация узора более высокой сложности на большом пальце левой руки – самый редкий

тип левшества, составляющий всего 2,5 % в популяции[1]. Заметим, что 2,5 % носителей такого типа ассимметрии во всей массе населения Российской Федерации составляет 3,6 млн человек. Так что «угадать» серийного убийцу только по дерматоглифическим признакам не удастся.

В.Е. Эминов, задаваясь вопросами о том, возможен ли переход от объяснения единичного преступления к общему (всей преступности), подчиняется ли движение преступности тем же причинным законам, что и поведение отдельного лица, или речь должна идти о совершенно иных типах детерминации, пришёл к выводу, что причинные связи, применительно к преступности, вообще несколько иные, чем в каждом индивидуальном акте преступного поведения, поскольку массовые явления имеют специфические свойства (например, количественную устойчивость), которых у индивидуального события нет[2].

При этом этот автор указывает, что механистическое понимание причинности как «жёсткой», однозначной связи между явлениями, приводит к выводу о неприменимости этого понятия для объяснения массовых вероятностных процессов[3].

Здесь не совсем понятен термин «механистическое понимание причинности». Полагаем, что причинная связь, если она есть, предполагает именно такую, «жёсткую», как характеризует её В.Е. Эминов, связь между явлениями и процессами. Другое дело, что, исследуя поведение человека, не представляется возможным в полной мере уяснить всю сложность психических процессов, нюансов его реакции на изменения в окружающей обстановке, природных факторов и т.п.

Отсюда возникает и та неточность наших прогнозов преступного

---

[1] *Богданов Н.Н.* Дерматоглифика пишущих левой // Вопросы психологии. 1997. № 2. С. 76–87; *Богданов Н.Н., Самищенко С.С., Хвыля-Олинтер А.И.* Дерматоглифика серийных убийц // Вопросы психологии. 1998. № 4. С. 64.

[2] *Эминов В.Е.* Причины преступности в России: криминологический и социально-психологический анализ. М.: Норма: ИНФРА-М, 2011. С. 11, 12.

[3] Там же.

поведения, о которой писалось ранее. Сделанные нами предположения основываются лишь на мизерном количестве факторов преступности, доступных для количественной и качественной оценки, поэтому несоответствие наших теоретических оценок реальным показателям преступности воспринимается как отсутствие жёсткой связи.

Однако, на наш взгляд, это никак не свидетельствует о принципиально иной природе детерминации всей преступности. Скорее речь идёт о степени неполноты наших знаний о поведении человека. Возвращаясь к примеру с убийствами, сказанное можно сформулировать так: наши знания о поведении обеспечивают нам точность прогноза индивидуального преступного поведения на уровне 0,15 %. Несомненно, наращивая объем данных о преступниках, уже в настоящее время можно резко повысить точность прогноза. Например, включая в анализ пол, возраст, образование, состояние здоровья, круг общения, продолжительность пребывания в статусе безработного, наличие семьи, детей, родственников и т.п., можно довести его точность до приемлемых для практического применения показателей.

Подводя итог нашим рассуждениям, можно сделать некоторые промежуточные выводы:

- непосредственные причины преступления кроются в личности;

- наиболее общие причины всей преступности, влияющие на деформацию системы нравственных ценностей личности, её потребности и прочее, относятся к сфере личности преступника и поэтому, являясь, по сути, элементами причинного комплекса, в качестве таковых не рассматриваются;

- причины конкретного преступления и причины всей преступности сходны и относятся между собой как часть и целое (где часть – причины конкретных преступлений, целое – причины всей преступности);

- внешние по отношению к личности факторы, именуемые в криминологии причинами преступлений, таковыми фактически не являются. Имеет место своеобразная терминологическая маскировка, при которой

наиболее важные и близкие по времени к преступлению условия именуются причинами;

- изучение причин конкретных преступлений необходимо переводить на современные рельсы, накапливая максимальное количество информации о личности преступника, обстоятельствах совершения преступления для дальнейшей её автоматизированной обработки (речь идет о таком направлении исследования огромных массивов данных, которые вручную обработать невозможно, и именуемом «Big Data», большие данные)[1].

В той части, которая характеризуется причинами индивидуального поведения, наши рассуждения применимы и к причинам виктимизации. 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[2].

В ряде случаев вообще нельзя говорить о включении виктимности в механизм детерминации.

Например, П., имея в силу служебных полномочий доступ к служебным базам данных оператора сотовой связи «Вымпел-Коммуникации», намереваясь использовать доступ в интернет для преступных целей и в целях маскировки своей деятельности, получил доступ к управлению абонентским номером и сопряжёнными с ним мобильными приложениями клиента компании, телефонный номер которого он выбрал произвольно, что привело к блокированию доступа к компьютерной информации для потерпевшего[3].

---

[1]См., напр.: *Вишневецкий К.В., Кашкаров А.А.*Влияние инновационных технологий на сферу предупреждения преступности // Гуманитарные, социально-экономические и общественные науки. 2021. № 3. С. 139.

[2]К.В. Вишневецкий в этой связи указывает, что наличие виктимных признаков зависит от определенных психофизиологических особенностей личности, а их реализация – от социально-демографических, морально-правовых признаков. См.: *Вишневецкий К.В., Доев В.А.* Виктимологическая характеристика личности жертвы доведения до самоубийства // Гуманитарные, социально-экономические и общественные науки. 2020. № 6. С. 112.

[3] Уголовное дело № 12007180001000009.

В других случаях характерным свойством отдельных видов преступлений в сети «Интернет» является то, что вред может причиняться неопределённому числу лиц. Например, мошенники организовывают колл-центр и обзванивают граждан, обращаясь к ним под видом сотрудников социальных служб и обещая компенсацию.

В таких ситуациях личные качества потерпевшего выступают необходимым условием совершения в отношении него преступления.

Но, если говорить об общем, например, об отдельном виде преступлений, то ситуация несколько иная. Мошенники, организуя некоторый вид обмана, учитывают потенциальный круг потерпевших с тем, чтобы оценить прибыль от совершения преступлений. Например, получая доступ к базе данных лиц, ранее пострадавших от каких-либо незаконных действий, они рассчитывают, что значительная часть из них может быть обманута ими. Если эта часть меньше определённого значения, то потенциальная прибыль не возместит расходов на организацию преступления. В таких ситуациях распространенность виктимогенных качеств личности потенциальных жертв может выступать в качестве причины вида преступлений. В нашем случае таковой является значительное число лиц пожилого возраста, имеющих сходные проблемы и обладающих слабыми знаниями о функционировании сети «Интернет», особенностях государственного социального обеспечения, позволявших бы им узнать мошенника и т.п. В этой связи особый интерес представляет позиция К.В. Вишневецкого, который рассматривает в качестве предмета виктимологии процессы виктимизации не только отдельных личностей, но и социальных групп.[1]

Сходная ситуация складывается и с лицами, подыскивающими малолетних для совершения в отношении них посягательств против их половой неприкосновенности и полового развития. Сама преступная деятельность

[1] *Вишневецкий К.В.* Социальный аспект криминальной виктимологии // Гуманитарные, социально-экономические и общественные науки. 2021. № 3. С. 138.

строится на эксплуатации таких качеств потерпевших, как доверчивость, отсутствие опыта взаимоотношений с противоположенным полом, неуверенность, вызванная малолетним возрастом (или, наоборот, излишняя самоуверенность из-за отсутствия негативного опыта), относительная автономность от родителей в киберпространстве и т.п. Подробнее об этом будет сказано далее.

Наличие потерпевших с такими качествами – не просто предположение преступника, а объективный факт, который положен им в основу своей преступной деятельности.

Таким образом, в механизме преступного поведения наличие у достаточно большого числа граждан набора повторяющихся качеств, обусловливающих их виктимность, может выступать не только условием, но и причиной возникновения отдельных видов общественно опасных посягательств либо, как в случае с киберпреступностью, появлением киберразновидностей общеуголовных преступлений.

Изучение материалов уголовных дел и сообщений в средствах массовой информации о киберпреступлениях позволяет сделать вывод, что причины виктимизации пользователей можно разделить на объективные, не зависящие от их воли и сознания, и субъективные. По источнику возникновения можно выделить факторы, обусловленные техническими особенностями функционирования киберпространства: техническими ошибками, сложностью программного обеспечения и т.д., причины, обусловленные особенностями реализации прав субъектов в киберпространстве. По характеру последствий можно выделить причины виктимизации жертв корыстных посягательств и, прежде всего, мошенничеств и преступлений против личности (в том числе, посягательств против жизни и здоровья и против половой неприкосновенности личности).

Рассмотрим основные причины и условия виктимизации в киберпространстве более подробно.

К числу ее объективных предпосылок, прежде всего, нужно отнести сложность современного программного обеспечения. Несмотря на то, что производители прикладывают значительные усилия к тому, чтобы пользовательские интерфейсы стали более дружелюбными, понятными для людей, объективная сложность решаемых задач, большое количество требуемых от пользователей действий приводят к тому, что не всегда последние точно представляют последствия тех или иных своих действий.

Эта проблема усугубляется тем, что производители периодически кардинально перерабатывают интерфейсы программ, как это было с одним из наиболее распространенных программных пакетов Microsoft Office при переходе с традиционного на так называемый ленточный интерфейс. Сходным образом недавно были переработаны структура и внешний облик личных кабинетов пользователей Сбербанк-онлайн.

Подразумеваемое производителем программного обеспечения повышение удобства для пользователей на практике не всегда достигается. Кроме того, отсутствует единый стандарт размещения управляющих элементов интерфейса на экране, что затрудняет их использование.

Следует учитывать и то, что пользователями компьютеров выступают люди различных возрастных категорий. Для отдельных представителей старших поколений, сформировавшихся в докомпьютерную эпоху, пользование компьютером до сих пор представляет определённую сложность. Неслучайно значительная часть потерпевших от мошеннических преступлений в киберпространстве представлена во многом именно этой возрастной группой.

Современные программы насчитывают огромное количество строк программного кода, исчисляемое десятками миллионов[1], а количество известных ошибок – десятками тысяч. Их сложность настолько высока, что подавляющее большинство программистов просто не могут себе полностью

[1] *Грег Кенн*. Насколько сложный программный код у Windows? URL: https://www.zeluslugi.ru/info-czentr/stati/programmnyy-kod-windows (дата обращения: 20.08.2021).

представить характер взаимосвязи между отдельными компонентами операционных систем.

Неудивительно, что иногда в них встречаются программные ошибки. Причины этих ошибок могут быть самыми разными – невнимательность программиста или проектировщика программ, дополнение имеющегося программного кода новыми функциями, которые вступают в конфликт с уже имеющимися, обновление отдельных компонентов компьютеров (памяти, видеоускорителя, модулей беспроводной связи, вызывающее конфликт с устаревшим программным обеспечением, нарушение логики взаимоотношений между отдельными программными подсистемами при внесении обновлений и т.д. В ряде случаев имеют место умышленные действия. Как правило, речь идёт о программистах, которые в ответ на несправедливые действия работодателей закладывают в код специфические функции, которые вызывают разрушительные последствия для компьютерной информации при возникновении некоторых условий.

В некоторых случаях, имеют место умышленные действия производителей или спецслужб по модификации программного обеспечения с тем, чтобы обеспечить возможность незаметного подключения к компьютерам, приобретаемым другой страной, удаленного считывания с них информации, отключения и т.п.

В 1996 г. на начальной стадии полёта французской космической ракеты Arian-5 ошибка в программном обеспечении привела к выдаче сигнала на самоподрыв ракеты. Причина ошибки состояла в том, что вычислительный модуль, перенёсенный с предыдущей модели ракеты Arian-4, не учитывал в своей работе изменений параметров скорости и траектории полёта новой модификации. В результате ошибки сорвалась серия коммерческих запусков ракеты, что привело к недополученной прибыли в размере 60 млрд долларов.

В 1985-1987 гг. несколько человек погибли в результате ошибки в программном обеспечении канадского медицинского ускорителя Therac-25 во

время сеансов радиационной терапии. Неисправность привела к тому, что пациенты были облучены дозами, многократно превышающими предельно допустимые[1].

Чуть позже из-за аналогичной ошибки программного обеспечения аппарата Sagitar-35 в Испании значительные дозы облучения получили не менее 25 пациентов, некоторые из которых погибли[2].

Если о перечисленных ошибках можно сказать, что они не имеют прямого отношения к криминологическим проблемам, то этого нельзя отрицать в случае так называемого блэкаута (полного обесточивания линий электропередач) из-за программной ошибки в оборудовании американской компании General Electric Energy в 2003 г., приведшему к тому, что на Восточном побережье США без электричества оказалось 55 млн человек, обесточенными оказались объекты жизнеобеспечения, больницы, тюрьмы, линии связи[3].

Очень часто встречаются ошибки в массовом программном обеспечении, которые приводят к возможности для злоумышленника получать доступ к персональным данным пользователя, перехватывать управление компьютерами, завладевать паролями от платёжных систем, почты, мессенджеров и аккаунтов в социальных сетях[4].

К счастью, в большинстве случаев программные ошибки не влекут тяжких последствий и, как правило, проявляются лишь при стечении некоторых факторов, таких как нажатие редких комбинаций клавиш, выбор одновременно нескольких элементов управления, ввод специфического текста,

---

[1] *Leveson N.G., Turner C.S.* An investigation of the Therac-25 accidents // Computer. 1993. V. 26. Iss. 7. P. 18–41.

[2] Trevor Cradduck LINAC deaths at Zaragoza // The RISKS Digest Vol. 11 Iss. 18. URL: http://catless.ncl.ac.uk/Risks/11.18.html#subj6.1 (дата обращения: 20.08.2021).

[3] Катастрофические последствия программных ошибок. URL: https://habr.com/ru/company/mailru/blog/370153/ (дата обращения: 20.08.2021).

[4] Можно ли справиться с уязвимостями в программном обеспечении? URL: https://www.kaspersky.ru/blog/mozhno-li-spravitsya-s-uyazvimostyami-v-programmnom-obespechenii/14939/ (дата обращения: 20.08.2021).

считывание некоторых комбинаций символов и т.п. Однако иногда они приводят к возможности перехвата управления компьютером сторонними пользователями.

Как правило, при выявлении таких уязвимостей производители программного обеспечения принимают меры к их устранению путём выпуска обновлений. Но иногда исправление ошибок может затягиваться, а некоторые вовсе не устраняются, поскольку производитель классифицирует их как некритичные.

Существует черный рынок, на котором предметом сделки являются подобные уязвимости, позволяющие перехватить управление компьютером, еще не ставшие известными компаниям-производителям, а также основанные на эксплуатации этих ошибок программы (эксплойты) позволяющие реализовывать на компьютерах пользователей вредоносный функционал[1].

Общая практика борьбы с уязвимостями состоит в переписывании программного кода и его распространении конечным пользователям. Поэтому компьютерная грамотность предполагает осведомлённость последних о необходимости отслеживать и устанавливать обновления программного обеспечения. Однако многие пользователи даже не подозревают о необходимости таких действий[2].

Во многих случаях ослабление безопасности является не следствием ошибок, а результатом целенаправленной деятельности самих производителей программ или поставщиков информации.

В настоящее время многие банки, операторы сотовой связи в поисках новых источников дохода предлагают пользователям новые услуги, причём зачастую это идёт в разрез с требованиями обеспечения безопасности.

---

[1]Почем сегодня продают уязвимости в программном обеспечении? URL: http://www.aethra.ru/pochem-segodnya-prodayut-uyazvimosti-v-programmnom-obespechenii/ (дата обращения: 20.08.2021).

[2]*Jason Morris, Ingolf Becker, Simon Parkin* In Control with no Control: Perceptions and Realityof Windows 10 Home Edition Update Features. URL: https://www.ndss-symposium.org/wp-content/uploads/2019/02/usec2019_02-5_Morris_paper.pdf (дата обращения: 20.08.2021).

Например, банки разрабатывают программное обеспечение для смартфонов, позволяющее их владельцам управлять своими банковскими счетами. Однако при этом они полностью снимают с себя ответственность за безопасность средств пользователя. Если при традиционном обращении в офис банка пользователь предъявляет документы, по которым его личность может быть идентифицирована, то единственным средством идентификации при пользовании онлайн-банком является пароль. Если злоумышленники получат к нему доступ, то они смогут распоряжаться всеми средствами на счетах.

Получившие широкое распространение переводы денег с помощью смс-сообщений, с одной стороны, привносят значительное удобство для пользователей. С другой – существенно ослабляют уровень защиты средств граждан. Утрата гражданином своего телефона может повлечь и утрату средств со счетов, привязанных к его номеру.

Впрочем, в настоящее время поступает информация о том, что злоумышленникам для совершения хищения не нужно даже похищать телефоны – достаточно по поддельным документам получить в офисе мобильного оператора дубликат сим-карты[1].

Появляются сообщения о том, что преступники при звонке на мобильные номера потенциальных жертв, получили техническую возможность осуществлять подмену телефонного номера. Таким образом, при получении входящего звонка на телефоне потерпевшего высвечивается не реальный номер звонящего, а какой-то другой. Мошенники могут использовать для подстановки номера телефонов из адресной книги потерпевшего, широко известные номера мобильных сервисов, например номер 900, принадлежащий сбербанку. Кроме того, мошенники используют технологию deepfake, позволяющую сымитировать голос любого человека. Таким образом, потерпевший пребывает в полной уверенности, что звонок совершается из службы безопасности

[1] *Нефедова М.* Задержаны мошенники, похищавшие деньги у VIP-клиентов банков с помощью клонов SIM-карт. URL: https://xakep.ru/2020/07/16/sin-swap-arrest/ (дата обращения: 23.12.2020).

Сбербанка или от его знакомых[1].

Масштабы действий мошенников позволяют им гарантированно находить жертв. Даже если большая часть граждан будет проявлять бдительность, всегда найдутся те, которые по тем или иным причинам доверятся преступникам.

В обществе до настоящего времени нет осознания важности хранения в тайне персональных данных, граждане, как отмечает в этой связи Е.А. Антонян проявляют беззаботность по отношению к обеспечению их сохранности.[2] Это объясняется тем, что проблема сохранности конфиденциальной информации до недавнего времени не была столь актуальной. Однако повсеместное распространение электронных коммуникаций приводит к тому, что ранее безобидные утечки конфиденциальных данных могут стать причиной крупных материальных потерь. Имея доступ к персональной информации о гражданах, мошенники могут её использовать в различных мошеннических схемах, например, выдавая себя за других людей. Одна из крупнейших утечек конфиденциальной информации произошла в конце 2020 г., когда в открытом доступе оказались персональные данные 300 тыс. человек, переболевших COVID-19. В числе утраченных данных были фамилии, имена и отчества больных, адреса проживания и регистрации, номера телефонов и паспортов, вся информация о течении болезни и заборах анализов.[3]

В настоящее время процедуры осуществления перечисления денежных средств регламентируются федеральным законом «О национальной платёжной системе»[4]. В соответствии с ч. 11 ст. 9 этого закона при утрате электронного

---

[1] *Некезова К.* В России распространился новый вид мошенничества по телефону. URL: https://www.vzsar.ru/news/2020/12/25/v-rossii-rasprostranilsya-novyy-vid-moshennichestva-po-telefony.html (дата обращения: 28.12.2020).

[2] *Антонян Е.А., Клещина Е.Н.* Кибервиктимность // Вестник Пермского института ФСИН России. 2019. № 3 (34). С. 7.

[3] Разгорающийся скандал: большой московский слив. URL: https://zavtra.ru/events/razgorayushijsya_skandal_bol_shoj_moskovskij_sliv (дата обращения: 28.12.2020).

[4] Федеральный закон от 27 июня 2011 г. № 161-ФЗ (с изм. и доп. от 14 июля 2022 г., № 331-ФЗ) «О национальной платежной системе» // СЗ РФ. 2011. № 27, ст. 3872; 2022. № 29 (ч. III), ст. 5298.

средства платежа и (или) его использования без согласия клиента, последний обязан в течение 24 часов уведомить оператора по переводу денежных средств в предусмотренной форме незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента. По истечении этого срока вернуть деньги отменить транзакцию и вернуть деньги практически невозможно.

Обращает на себя формулировка ч. 11 ст. 9, согласно которой клиент, во-первых, ограничен 24-часовым сроком для уведомления оператора и, во-вторых, он обязуется сообщать банку о несанкционированной транзакции. Толкование этого положения приводит к тому, что если клиент по каким-либо причинам не проверил состояние средств на своих счетах в личном кабинете соответствующего приложения, то он считается не выполнившим своих обязанностей. Однако даже в тех случаях, когда клиент вовремя направляет уведомление, вернуть деньги не всегда представляется возможным, поскольку банки стараются максимально затянуть процедуру возврата денег или уклониться от неё. Показательным примером является дело, рассмотренное девятым арбитражным апелляционным судом г. Москвы. Истец обратился в суд с требованием вернуть денежные средства в сумме 1 млн 963 тыс. рублей, которые без его согласия были перечислены с его счета в АО «АЛЬФА-БАНК» на счета ООО «Ласточка». Как было установлено в судебном заседании, в офис АО «АЛЬФА-БАНК» пришёл неизвестный с поддельной доверенностью от заявителя на замену электронной подписи от личного кабинета пользователя. Получив электронную подпись, преступник зашёл в личный кабинет законного пользователя и перечислил имевшиеся на счету средства на счета ООО «Ласточка». Несмотря на то, что клиент обратился в АО «АЛЬФА-БАНК» с заявлением об отмене перевода в срок, меньший установленного законом, суд первой инстанции отказал в удовлетворении его исковых требований. И лишь в апелляционной инстанции права потерпевшего были восстановлены спустя

почти два года.[1]

В другом случае клиенты банка ВТБ столкнулись ситуацией, когда из-за сбоя в программном обеспечении банка их личные кабинеты оказались заблокированными. Многим клиентам стали поступать СМС-сообщения о списаниях денежных средств.

Несмотря на то, что эти сообщения оказались ошибочными, фактический доступ к своим счетам пользователи утратили на несколько часов. В этот период в банке не отвечали телефоны службы поддержки клиентов. При таких условиях, выполнить свои обязанности по информированию оператора клиенты физически не могли[2].

На основе проведенного анализа можно выделить следующие характерные черты ситуации, складывающейся в сфере обеспечения безопасности платёжных переводов:

1. Безопасность платёжных переводов должны обеспечивать операторы по переводу денежных средств (банки). Они обязаны разрабатывать программное обеспечение, системы идентификации пользователей в платёжных системах, исключающие возможность доступа к денежным средствам пользователей посторонних лиц. Они могут эмитировать электронные подписи и т.п.
2. Ответственности за поддержание высокого уровня безопасности платёжных переводов операторы фактически не несут.
3. Пользователи не имеют возможности каким-то образом повышать уровень безопасности переводов, поскольку это находится в компетенции банков.

---

[1]Постановление Девятого арбитражного апелляционного суда г. Москва от 29 июня 2016 г. № 09АП-4829/2016г по делу № А40-120498/1. URL: https://kad.arbitr.ru/Document/Pdf/aefaed33-b367-4655-ab56-43934ee99872/6fae96aa-309b-41ae-80d6-2cf8f5b1dabc/A40-120498-2015_20160629_Postanovlenie_apelljacionnoj_instancii.pdf?isAddStamp=True (дата обращения: 28.12.2020).

[2]Телефоны молчат, деньги клиентов утекают: У ВТБ рухнуло все… URL: https://smart-lab.ru/blog/631461.php (дата обращения: 28.12.2020).

4. В случае несанкционированного перевода денежных средств на пользователя фактически возлагается бремя доказывания того, что перевод был незаконным.
5. Банки в большинстве случаев не несут потерь, связанных с незаконными переводами.

Таким образом, имеет место асимметрия в уровне правовой защищённости прав пользователей и операторов. Причём первые фактически беззащитны. В случаях хищения денежных средств со счетов в банках, вероятность получить возмещение ущерба будет только в том случае, если эти средства будут обнаружены у злоумышленников. Однако такие исходы практически не встречаются. Банки же не несут существенных потерь от несанкционированных операций. В подобной ситуации у них отсутствуют стимулы для совершенствования собственных систем безопасности и заинтересованность в изобличении и поимке мошенников.

Как отмечают специалисты, механизм блокировки несанкционированных переводов работает только лишь в отношении операций, совершенных без согласия клиента после получения соответствующего уведомления банком. Если же операции произведены до обращения в банк для блокирования счета, то суды отказывают в удовлетворении требований по этому основанию[1].

Совершенно иная ситуация складывается в США, где в соответствии с The Fair Credit Billing Act (FCBA) клиенты защищены в гораздо большей степени. Достаточно сказать, что срок уведомления операторов о незаконной транзакции составляет 60 дней, при этом клиент, чтобы получить деньги обратно обязан лишь заявить, что не осуществлял денежного перевода и предъявить кредитную карту (что является доказательством того, что он не

[1] *Вершинин И.* Операции без согласия клиента банка: практика по предотвращению. URL: https://bosfera.ru/bo/operacii-bez-soglasiya-klienta-banka-praktika-po-predotvrashcheniyu (дата обращения: 28.12.2020).

передавал её третьим лицам)[1].

Изменение баланса интересов в защите прав клиентов и операторов платёжных систем в пользу клиентов приводит к тому, что в США банки напрямую заинтересованы в розыске и изобличении мошенников, совершенствовании программного обеспечения и систем безопасности.

В настоящее время в нашей стране банки активно навязывают пользователям финансовые услуги, разнообразные кредитные карты. При этом финансовое положение пользователя зачастую не учитывается, т.е. банки сознательно создают ситуацию, при которой пользователи кредитных услуг могут превысить лимиты по кредитным картам, не успеть вовремя заплатить проценты и, таким образом, попадут в кабальную долговую зависимость. Ещё более циничной является ситуация, когда подобные услуги навязываются несовершеннолетним. По закону кредитные карты им предоставляться не могут, но в ряде случаев школьникам выдают дебетовые карты с возможностью овердрафта (т.е. возможности списывать со счета больше денег, чем находится на счёте, фактически – предоставляя кредит).

Так, в Санкт-Петербурге ряд родителей обратились в Роспотребнадзор с жалобами на Связной Банк, который заключил с их несовершеннолетними детьми договоры об открытии карт. Семьи узнали об этом только спустя много месяцев, когда начали получать письма о задолженности.

По выдаваемым картам допускался овердрафт свыше 300 тыс. рублей, что в сумме с набежавшими процентами привело к образованию крупных долгов вместе с начисленными процентами за просрочку платежей. Очевидно и то, что банки в подобных ситуациях осуществляют свою деятельность недобропорядочно, заведомо поставляя законопослушных граждан (родителей)

[1]Lost or Stolen Credit, ATM, and Debit Cards. URL: https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards (дата обращения: 28.12.2020).

в крайне тяжёлое положение[1].

В числе объективных факторов виктимизации называлось наличие ошибок в программном обеспечении. В этой связи стоит отметить, что многие пользователи стараются сразу же обновлять установленные на компьютерах программы при появлении новых версий. Такое поведение следует классифицировать как виктимное, поскольку новые версии программ, хотя и устраняют часть уязвимостей, однако вносят и много новых, которые ещё не стали известными. Поэтому безопасное поведение состоит в том, чтобы не пользоваться сразу новейшими версиями популярных программ, а делать это лишь спустя некоторое время, когда критически важные для безопасности уязвимости будут выявлены и устранены.

В настоящее время пользователи в киберпространстве имеют возможность делать покупки, передавать сообщения посредством электронной почты, мессенджеров, общаться в социальных сетях, видеоконференциях, скачивать фильмы, музыку и т.п.

Для многих подобных операций необходима точная идентификация пользователя, с тем, чтобы избежать доступа к личным данным или финансам посторонних лиц. Для идентификации в киберпространстве обычно используются пары логин-пароль, иногда осуществляется многофакторная аутентификация пользователей – когда при вводе логина и пароля пользователю отправляется дополнительный одноразовый пароль в смс-сообщении или электронным письмом. При этом логин пользователя является общедоступной информацией, а пароль должен храниться в тайне.

Ответственность за сохранение идентификационных данных в тайне целиком возлагается на пользователей, что не в полной мере осознаётся ими в силу непонимания значимости таких сведений как пароли и логины, отсутствия соответствующих навыков, небрежности. Иногда пароли и логины

---

[1] *Токарева А., Биянова Н.* Детские долги. URL: https://www.banki.ru/news/daytheme/?id=3959932 (дата обращения: 31.12.2020).

записываются на бумаге и хранятся в доступных для посторонних местах.

Зачастую пользователи не понимают, что пароли должны быть сложными. Пароли от различных ресурсов не должны совпадать. Однако на практике пользователи используют одни и те же пароли и для почты и для доступа к различным ресурсам, а иногда и в качестве пин-кодов кредитных карт. При этом в качестве паролей обычно выбираются годы рождения (свои, супругов, детей), памятные даты (например, год свадьбы) и т.п. При этом пользователи не понимают, что подбор таких паролей не составляет особого труда для злоумышленника, который, получив биографические данные пользователя, может без труда сконструировать вероятные пароли.

Иногда, как правило в связи со служебной необходимостью, пользователи вынуждены работать на чужих компьютерах и указывать свои персональные реквизиты для аутентификации. При этом они не учитывают, что некоторые программы, такие как браузеры, могут сохранять для посещаемых страниц пароли и логины пользователей. Обычно это делается для большего удобства пользователей, но может привести и к утрате секретных сведений.

Одним из источников утраты конфиденциальной информации является работа на личных ноубтуках или планшетах в общественных местах. Здесь усматриваются два фактора виктимизации. Во-первых, информация, которую пользователи выводят на экраны своих устройств, может быть легко считана и зафиксирована современными техническими средствами. При нынешнем уровне развития фототехники для этого может быть достаточно обычного смартфона с высококачественной камерой. Кроме того, возможна и визуальная фиксация клавиш, которые нажимает пользователь при вводе паролей или другой информации.

Другая угроза связана с передачей данных по общественным сетям. В нашей стране многие учреждения предоставляют гражданами бесплатный доступ к Интернету посредством организации общедоступных wifi сетей. Это становится стандартным сервисом и конкурентным преимуществом для многих

кафе, ресторанов, иных общественных мест. Однако здесь существуют следующие угрозы. Данные, передаваемые по таким сетям легко доступны для перехвата. Несмотря на то, что сведения передаются в таких сетях, как правило, в зашифрованном виде, существуют программы (снифферы), позволяющие такую информацию перехватывать и расшифровывать. Зачастую для этого не требуется какого-либо специального оборудования – достаточно разместить в зоне доступа сети wifi обычный ноутбук с программой-сниффером.

В ряде случаев владельцы wifi сетей вообще не закрывают доступ к своим сетям и передаваемые по ним данные вообще никак не защищаются.

В настоящее время на фоне распространения информации об усилении контроля со стороны государства над распространением информации в киберпространстве, все шире распространяется отказ от какой-либо защиты личных данных, начиная от личной переписки и заканчивая интимными подробностями личной жизни. Показное бесстыдство, на наш взгляд, является своеобразной формой защиты от возможного шантажа, связанного с обнародованием личных данных.

Слабая техническая грамотность пользователей может проявляться в том, что они не уделяют достаточного внимания техническим аспектам сохранения в тайне конфиденциальных сведений. Это может проявляться в различных формах: иногда пользователи не закрывают паролем доступ в частные wifi сети. В ряде случаев используют устаревшие и недостаточно защищённые протоколы шифрования. Однако даже в тех случаях, когда используются считающиеся надёжными криптографические алгоритмы, пользователи уклоняются от периодического обновления паролей доступа к сетям. То же самое справедливо и по отношению к паролям от других ресурсов киберпространства (электронной почты, аккаунтов в социальных сетях, форумах и т.п.).

В настоящее время подавляющее большинство пользователей использует для работы и игр компьютеры с установленной системой Windows, меньшая часть – с операционной системой фирмы Apple. Однако и та, и другая система

разработаны в США, их исходные коды недоступны для анализа и в компьютерной прессе периодически появляется информация о том, что при подключении к Интернету компьютеры передают большие объёмы информации без ведома пользователя на самые разные сайты в сети. Как правило, речь идёт об отладочной информации, о состоянии системы, работе прикладных программ. Но точно гарантировать, что компьютер не передаёт заодно и пользовательские данные не может никто. Сообщения об отправке некоей информации поступали и от владельцев смартфонов с различными операционными системами.

В настоящее время в социальных сетях формируются группы, включающие представителей различных социальных слоев, обладающих различным культурным уровнем, опытом общения в сетях, специфическим сленгом и т.п. Типичным примером являются группы родителей учеников одного класса, создаваемые в Viber или Whatsapp. Общение в таких группах ведётся преимущественно путём переписки. Поэтому иногда возникают ситуации, при которых те или иные фразы слабо знакомых между собой людей могут неадекватно восприниматься другими участниками чата. Так, возникшая по незначительному поводу перепалка в родительском чате привела к тому, что женщина, посчитавшая себя оскорблённой собеседником, обратилась к брату с просьбой «разобраться с обидчиком». При личной встрече брат этой женщины нанес потерпевшему несколько сильных ударов по голове, от которых последний скончался[1].

Несмотря на то, что преступление было совершено за пределами киберпространства, процесс виктимизации был запущен именно там. Причина, на наш взгляд, кроется в отсутствии культуры общения в подобных социальных сетях. Вполне вероятно, что потерпевший не имел намерения кого-либо унижать и выражался в обычной для себя манере, которая была неверно

[1]Обвиняемому в убийстве из-за конфликта в школьном чате Арсену Мелконяну продлили арест. URL: https://v1.ru/text/criminal/2020/12/21/69646916/ (дата обращения: 23.12.2020).

интерпретирована как оскорбление.

Другим примером виктимного поведения являются знакомства в сети «Интернет». Особенности киберпространства позволяют злоумышленникам легко входить в доверие к потерпевшим, фальсифицировать данные о себе, вызывая расположение и желание встретиться в реальном мире.

Так, гражданка П., подала объявление о знакомстве на одном из сайтов в сети «Интернет», на которое откликнулся ранее ей незнакомый Саблин, ранее судимый за убийство и изнасилование. В ходе беседы П. пригласила Саблина к себе домой. Во время встречи Саблин применил к потерпевшей насилие и потребовал передать ему деньги и ценности, находящиеся в квартире[1].

В другом случае, Р. обратилась в полицию с заявлением об изнасиловании, которое якобы совершил Н., с которым она познакомилась на сайте знакомств. Как пояснила Р., желание написать заявление об изнасиловании возникло у нее, так как Н. после их встречи не дал ей денег на такси[2].

Из приведённых примеров видно, что у жертв преступлений ещё не сформировалось представления о свойствах киберпространства. Заводя виртуальные знакомства, потерпевшие не учитывают того, что могут столкнуться с преступником, полагаясь на свой опыт и интуицию.

В отдельных случаях пользователи сами совершают в киберпространстве неодобряемые с точки зрения морали действия. Так, житель г. Саратова нашёл в Интернете сайт, на котором рекламировались услуги проституток. Ответившая на его звонок девушка заявила о необходимости внести предоплату. Однако после перевода денег никто к нему не приехал[3].

---

[1]Уголовное дело № 1/97-2012 // Архив Октябрьского районного суда г. Иркутска за 2012 г.

[2]Уголовное дело № 1-368/2018 // Архив Калининского районного суд г. Тюмени за 2018 г.

[3]Саратовец нарвался на мошенников при заказе проститутки в интернете. URL: https://www.vzsar.ru/news/2020/11/15/saratovec-narvalsya-na-moshennikov-pri-zakaze-prostitytki-v-internete.html (дата обращения: 28.12.2020).

Говоря о виктимных действиях пользователей необходимо упомянуть и такое явление как отсутствие у граждан навыков сокрытия персональной информации. Киберпространство вошло в нашу жизнь недавно и в обществе ещё не сформировались нормы поведения в сети, не появились представления об опасности раскрытия личных персональных данных, которые могут быть использованы преступниками. Это касается и взрослых и, особенно, детей. Распространённым явлением стала регистрация в социальных сетях малолетних, хотя официальные правила социальных сетей устанавливают возрастные ограничения на регистрацию.

Например, социальные сети Instagram и Facebook[1], мессенджер Viber устанавливают возраст регистрации с 13 лет[2]. Сеть «ВКонтакте» снимает с себя ответственность за регистрацию малолетних, указывая в пользовательском соглашении о том, что пользователем может быть физическое лицо, достигшее возраста, допустимого в соответствии с законодательством Российской Федерации[3]. В социальной сети «Одноклассники» возрастные ограничения не предусмотрены.

На нормативном уровне возрастные ограничения для регистрации в социальных сетях, мессенджерах и т.п. не устанавливаются. Между тем, дети могут столкнуться в киберпространстве с информацией, которая для них

---

[1]Деятельность Meta Platforms Inc. по реализации продуктов - социальных сетей Facebook и Instagram на территории РФ запрещена по основаниям осуществления экстремистской деятельности. Согласно данным Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, размещенных в открытом доступе на сайте http://blocklist.rkn.gov.ru, ресурс https://www.instagram.com, а также программное приложение «Instagram» заблокированы по требованию Генеральной прокуратуры РФ от 11.03.2022 № 27-31-2022/Треб292-22. URL: https://rkn.gov.ru/news/rsoc/news74180.htm?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 20.04.2022).

[2]Условия использования сервиса Instagram. URL: https://help.instagram.com/478745558852511 (дата обращения: 17.01.2021); Пользовательское соглашение сети Facebook. URL: https://www.facebook.com/terms.php?locale=ru_RU (дата обращения: 17.01.2021); Условия использования Viber. URL: https://www.viber.com/ru/terms/viber-terms-use/ (дата обращения: 17.01.2021).

[3]Пользовательское соглашение социальной сети «ВКонтакте». URL: https://vk.com/terms (дата обращения: 17.01.2021).

нежелательна или вредна, в социальных сетях они становятся лёгкой жертвой педофилов, поскольку не имеют достаточного жизненного опыта и зачастую действуют самостоятельно, без контроля со стороны взрослых. Вероятность виктимизации в таких случаях значительно повышается, если подростки выкладывают персональную информацию о себе – место учёбы, жительства, личные фотографии и т.п.

В литературе было обращено внимание на то, что увеличение числа преступлений против половой неприкосновенности малолетних в нашей стране хронологически совпал с ростом популярности социальной сети «Вконтакте»[1].

М. Фалеев указывает на то, что педофилы осуществляют активный поиск в социальных сетях и, выявляя детей, начинают активно обрабатывать их. Методики развращения отрабатываются до мелочей на специализированных форумах[2].

Примером может стать уголовное дело по ч. 2 ст. 135 УК РФ, возбуждённое в отношении К., который вступив в переписку с 13-летней А., познакомился с ней, а впоследствии совершил в отношении потерпевшей развратные действия[3].

В другом случае К. познакомился в сети «ВКонтакте» с тремя девочками 12-14 лет и путём психологического давления и угроз взлома страниц в соцсети заставил потерпевших присылать ему фотографии интимного характера, которые затем размещал в социальных сетях и рассылал знакомым[4].

В материалах гражданского иска о защите чести и достоинства, поданного впоследствии осуждённым К., указывается, что одна из потерпевших

---

[1]*Бытко С.Ю.* Оценка эффективности уголовного наказания за педофилию // Юридическая наука и правоохранительная практика. 2016. № 2. С. 56.

[2]*Фалалеев М.* Запретный секс. Педофилов ловят в сети на «веселые картинки» // Рос. газета. 2011. 23 нояб. URL: http://www.rg.ru/2011/11/23/pedofilia-site.html(дата обращения: 01.05.2015).

[3]Уголовное дело № 1-400/2016 // Архив Тосненского городского суда Ленинградской области.

[4]В Астрахани мужчина признан виновным в развращении детей. URL: https://astra-novosti.ru/v-astraxani-muzhchina-priznan-vinovnym-v-razvrashhenii-detej/ (дата обращения: 17.01.2021).

заявила, что, по её мнению, число потерпевших от его действий может достигать нескольких сотен[1].

В настоящее время ситуация осложняется тем, что в связи с карантинными ограничениями многие школьники, даже в начальных классах, вынуждены заниматься дома и пользоваться социальными сетями для учёбы. Следовательно, опасность виктимизации этой категории значительно усиливается.

Здесь же хотелось отметить, что виктимизация несовершеннолетних, на наш взгляд, может состоять не только в совершении в отношении них преступлений, но и в вовлечении их в какие-то преступные действия. Например, наличие в сети «Интернет» доступной информации о наркотиках, их «безвредности», методах их изготовления, местах сбыта и т.п. способно сформировать у несовершеннолетнего мотив приобщиться к их потреблению. Подобный процесс, на наш взгляд, также следует рассматривать как виктимизацию, в которой интересам развития несовершеннолетнего, его здоровью причиняется существенный ущерб.

По мнению А.Е.Шалагина, информация, получаемая подростком в сети «Интернет», способна оказать негативное воздействие на мотивационную направленность несовершеннолетнего, деформировать его взгляды, убеждения, потребности.[2]

То же самое можно сказать и о некоторых других процессах. Например, в г. Саратове в 2020 г. было выявлено 388 подростков, которые являлись подписчиками интернет-ресурсов, содержащих деструктивный контент, в т.ч.

---

[1]Решение Кировского районный суда г. Астрахани от 28 декабря 2017 г. по делу № 2-4076/2017. URL: https://sudact.ru/regular/doc/2rZp67WDk05x/(дата обращения: 17.01.2021).

[2]*Шалагин А.Е., Идиятуллов А.Д., Шалагин И.А.* Детерминирующие факторы противоправного поведения подростков и молодежи // Евразийское Научное Объединение. 2021. № 7-2. С. 155.

ценности сообщества АУЕ (арестантский уклад един)[1].

Массовое вовлечение в подобные сообщества возможно по нескольким причинам. Во-первых – это безнадзорность подростков и бесконтрольность пользования компьютерными сетями. Во-вторых, следует отметить недостаточность имеющихся средств фильтрации информации, попадающей к детям, причем это имеет место даже на школьных компьютерах.

В настоящее время в киберпространстве сформировалось такое явление как «информационные пузыри» – т.е. ситуация, при которой граждане, имея потенциально доступ к неограниченному количеству ресурсов, ограничиваются лишь теми, которые предоставляют информацию, с которой они согласны, либо сходную с той, которую они предпочитают получать при поиске. Причины этого лежат как в субъективной, так и в объективной плоскостях, поэтому данный фактор виктимизации следует отнести к объективно-субъективным.

В формирование «информационных пузырей огромный негативный вклад вносят современные поисковые системы (Яндекс, Google и т.п.). Поскольку эти поисковики, в первую очередь, созданы для реализации коммерческих интересов, они пытаются при выдаче ответов на поисковые запросы пользователя предугадать, какую информацию пользователь хотел бы получить. При этом поисковые системы опираются на предыдущие запросы пользователя, на профиль его интересов, который формируется из истории посещённых им страниц, скачанных файлов, контактов в социальных сетях и т.д. При таком подходе нежелательная, по мнению поисковика, информация пользователю не предоставляется. Таким образом у пользователя формируется искажённое восприятие действительности, основанное на его предпочтениях, а нежелательная, неприятная информация в киберпространстве для него перестаёт существовать. Проблема информационных пузырей весьма

[1]Сотни саратовских подростков изучали АУЕ в соцсетях. URL: https://www.vzsar.ru/news/2020/08/11/sotni-saratovskih-podrostkov-izychali-aye-v-socsetyah.html (дата обращения: 12.03.2021).

многогранна, и ей посвящена обширная литература[1].

Для целей нашего исследования важно то, что формирование информационного пузыря лишает пользователя объективной информации о предмете его интересов, делает его уязвимым для различного рода манипуляций, в том числе, и совершаемых с преступными целями.

Другая часть проблематики «информационных пузырей» состоит в сознательном уклонении граждан от столкновения с неприятной информацией, одностороннем рассмотрении отдельных аспектов действительности. Причины этого могут лежать в незнании особенностей функционирования поисковых сетей и способов персонализации результатов поиска, в ограниченности кругозора, неспособности или нежелании вести дискуссию с противниками иных точек зрения и т.д.[2]

Практическое значение «информационных пузырей» состоит в том, что они, с одной стороны, делают пользователя более уязвимым перед возможными злоумышленниками. С другой – снижают эффективность мер предупреждения преступности, осуществляемых путём информирования граждан о нежелательных действиях, влекущих риск совершения в отношении них преступлений. Типичная ситуация складывается с наркопотребителями: имеется огромное количество ресурсов, в которых пропагандируются различные наркотики, описывается их безвредность, отсутствие привыкания и т.п. Поэтому молодые люди, которые по тем или иным причинам оказались вовлечены в приём наркотических средств, скорее всего, окажутся в

---

[1] *Зайцев И.Н.* Тотальность медийного пузыря // Научная сессия ГУАП: Сборник докладов научной сессии, посвященной Всемирному дню авиации и космонавтики. В 3 ч. / Под общей редакцией Ю.А. Антохиной. СПб., 2019. С. 99; *Шкорубская Е.Г.* Коммуникативное пространство сети Интернет: бунт против анонимного избытка информации // Учёные записки Крымского федерального университета имени В.И. Вернадского. Философия. Политология. Культурология. 2018. Т. 4 (70). № 4. С. 86.

[2] В технической литературе описывается ситуация, когда одному пользователю на запрос «British Petroleum» поисковик от Google выдаёт только инвестиционные новости, а другому – только сведения о взрыве нефтяной платформы Deepwater Horizon. См.: Что такое «пузырь фильтров» и как из него выбраться. URL: https://habr.com/ru/company/riddut/blog/295714/ (дата обращения: 31.12.2020).

«информационном пузыре», блокирующем предупредительную информацию.

Подводя итоги изложенному, можно сделать следующие выводы:

1. Понятия «жертва», «потерпевший» в виктимологии являются более широкими, чем в уголовно-процессуальном праве и близки к понятию «потерпевшего» в уголовном праве.

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.

3. Признание государства жертвой преступления выходит за пределы предмета виктимологии и представляется нецелесообразным.

4. В механизме преступного поведения виктимность жертвы может выступать не только условием, но и причиной возникновения новых разновидностей общеуголовных преступлений, совершаемых в киберпространстве, либо таких, где процесс виктимизации происходит в киберпространстве.

5. В общем случае нельзя говорить о существовании каких-либо специфических признаков, которые имеются только у жертв преступлений и отсутствуют у прочих граждан. Полагаем, что речь может идти лишь о степени выраженности определённых признаков, комбинациях отдельных качеств личности. При этом нас в большей степени интересуют не какие-то неповторимые индивидуальные особенности, а устойчиво повторяющиеся наборы признаков, которые, с одной стороны, позволяют злоумышленникам осуществлять систематическую преступную деятельность и совершенствовать профессиональные навыки, а с другой – делают возможным изучение личности жертвы научными методами, например путём применения статистического анализа.

В киберпространстве виктимизация практически всегда носит активный характер – жертва активно реагирует на специфическую информацию. Именно

этот момент, по нашему мнению, и является моментом возникновения личности жертвы.

6. Находящиеся на слуху мошенничества с кредитными картами, судя по всему, составляют лишь верхушку айсберга, небольшую часть всех мошенничеств. Большая же часть – это хищения небольших сумм, никак не отражаемые в уголовной статистике.

7. Латентность мошенничеств, судя по результатам проведенного нами анкетирования и с учётом предыдущих оценок, превышает 99 %. При этом хищения небольших сумм практически не отражаются в уголовной статистике. Полагаем, что фактическое количество совершаемых в стране мошенничеств превышает 20 млн преступлений в год. Таким образом, мошенничество из уголовно-правового явления на наших глазах трансформируется в значимый социально-политический фактор, объединяющий граждан на почве недовольства государством, неспособным их защитить.

8. В подавляющем большинстве случаев мошенничество связано с методами социальной инженерии. Преступления, основанные на использовании специальных компьютерных познаний (взломы аккаунтов, личных кабинетов и проч.), составляют крайне незначительное число. Это обстоятельство необходимо учитывать при разработке мер предупреждения кибермошенничеств.

9. К причинам и условиям криминальной виктимизации пользователей сети «Интернет» в киберпространстве следует относить:

- 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 удобства использования программ;

- недостаточность предпринимаемых мер для сохранения

конфиденциальной информации о гражданах, а также непонимание самими гражданами важности сохранения в тайне конфиденциальной 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, 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.

§ 3. Характеристика личности жертвы киберпреступлений

В криминологической теории необходимость научного изучения личности преступника подвергалась сомнению. Связано это было с двумя обстоятельствами. Во-первых, с тем, что в определенные периоды в науках об обществе господствовали представления о ведущей роли социального бытия в индивидуальном поведении человека (бытие определяет сознание)[1]. Одновременно по идеологическим соображениям криминологи не могли отказаться от тезиса, выдвинутого В.И. Лениным, согласно которому в Советском Союзе искоренена частная собственность на средства производства и порождаемые ею эксплуатация, угнетение и нужда трудящихся, т.е. коренные

[1]См., напр.: *Ной И.С.* Методологические проблемы советской криминологии. Саратов: Изд-во Саратовского ун-та, 1975. С. 53-56.

причины преступности отсутствуют[1], а остающиеся преступления объяснялись действием пережитков прошлого строя[2].

При таком подходе, действительно, практическая значимость изучения личности преступника представлялась неочевидной. К настоящему времени криминология более свободна от идеологических догм и указанное возражение против необходимости изучать личность преступника может считаться снятым, причём не потому, что Советский Союз прекратил своё существование, а потому, что преступность за весь период его существования искоренить так и не удалось. Поэтому совершенно ясно, что общественные причины для сохранения и воспроизводства преступности существовали всегда.

Во-вторых, рядом криминологов высказывались сомнения относительно существования каких-либо принципиальных отличий личности преступника от личности законопослушного гражданина. Иными словами вопрос ставился так – а есть ли вообще личность преступника?

Действительно, если сравнивать качества личности преступников и законопослушных граждан, то коренных отличий, однозначно характеризующих преступников, встретить не получится. Исключение могут составить лишь отдельные патологические явления, например, маньяки, серийные убийцы на сексуальной почве. Как отмечает Я.И. Гилинский, никто и никогда еще не называл качество личности, которое имелось бы у преступников, а у прочих людей отсутствовало[3]. Ю.Д. Блувштейн отмечал, что понятие «личность преступника» должно распространяться лишь на профессиональных преступников[4].

С другой стороны, большинство криминологов говорит о личности

---

[1] *Ленин В.И.* Государство и революция: Полн. собр. соч. Т. 33. С. 91.

[2] *Курицына Е.В.* Преступность в советском обществе в 1953–1964 гг. (социально–криминологический аспект) // Известия Пензенского государственного педагогического университета им. В.Г.Белинского. 2007. № 3. С. 118.

[3] *Гилинский Я.И.* Криминология: теория, история, эмпирическая база и социальный контроль. 3-е изд. переаб. и доп. СПб.: Алефпресс, 2014. С. 210.

[4] *Блувштейн Ю.Д.* Понятие личности преступника // Советское государство и право. 1979. № 8. С. 97-102.

преступника, как о реально существующем явлении, как о совокупности психологически социально значимых негативных свойств психики[1], таких качеств, которые либо способствуют зарождению и формированию преступного умысла, либо облегчают борьбу мотивов в сознании лица в пользу преобладания отрицательных ситуаций[2].

Впрочем, последняя, наиболее распространённая точка зрения, также имеет некоторые противоречия. Они видятся, например, в том, что некоторые криминологи, как указано ранее, апеллируют к осознанным мотивам. В то время как другие, например Ю.М. Антонян, огромное значение отводят бессознательному[3].

В таком случае становится не совсем ясным – следует ли относить бессознательные процессы к свойствам личности преступника. Как отмечалось ранее, в личности преступника криминологов привлекают негативные качества. Но вопрос – можно ли давать позитивную или негативную оценку бессознательным процессам для нас не решён, поскольку в уголовном праве и криминологии позитивные и негативные оценки распространяются лишь на сферу сознательного.

Многие негативные качества свойственны не только преступникам, но и обычным людям. Например, характерная для многих преступников корысть, как движущая сила большинства преступлений, в полной мере свойственна и обычным гражданам, а во многих случаях эта характеристика личности потерпевших успешно эксплуатируется мошенниками. Весьма в этом плане красноречивую иллюстрацию жадности как важнейшего виктимогенного фактора дает уголовное дело, возбуждённое по ст. 159 УК РФ в отношении П., который, познакомившись в сети «ВКонтакте» с потерпевшим, занимал у него

---

[1]См., напр.: *Кудрявцев В.Н., Эминов В.Е.* Криминология. М.: Норма, 2009. С. 151, 152.

[2]*Яковлев А.М.* Об изучении личности преступника // Советское государство и право. 1962. № 11. С. 109-110.

[3]См., напр.: *Антонян Ю.М.* Бессознательное в корыстном преступном поведении // Общество и право. 2015. № 2. С. 120.

небольшие суммы денег под обещание возвратить долг в двойном размере. Всего в уголовном деле фигурирует 28 случаев перевода денежных средств на общую сумму 72500 руб.[1]

Такая типичная черта, характерная для преступников, как отсутствие уважения к закону (правовой нигилизм), характерна и для обычных граждан. Об этом можно судить хотя бы потому, что количество совершаемых в стране нарушений правил дорожного движения и лиц, их совершивших, значительно превышает число лиц, совершивших преступления.

У одного и того же человека свойства личности в различных ситуациях могут проявляться с разной интенсивностью, что ещё более затрудняет разграничение. Поэтому главным отличительным признаком в личности преступника, на наш взгляд, является степень выраженности негативных качеств, обусловленная внешними факторами, оказывавшими воздействие на её формирование.

При таком понимании становится ясно, что основная цель, которую должны преследовать криминологи при изучении личности преступника, состоит в том, чтобы глубже постичь механизм детерминации индивидуального преступного поведения и на этой основе предложить эффективные меры их предупреждения[2].

Теоретические проблемы, возникающие при изучении личности преступника, повторяются и при исследовании их жертв. В частности, требуют разрешения вопросы о том, существует ли, собственно, личность жертвы как объективное явление? В какой момент можно говорить о ее возникновении? Для чего требуется её изучение? и т.д.

Как и в случае с личностью преступника, в общем случае нельзя говорить

---

[1]Уголовное дело № 1-407/2019 1-51/2020 // Архив Центрального районного суда г. Воронежа за 2020 г.

[2]Подробнее об этом см., напр.: *Абельцев С.Н.* О личности преступника и практической значимости её изучения // Вестник Тамбовского государственного университета. 2000. № 2. С. 84.

о существовании каких-либо специфических признаков, которые имеются только у жертв преступлений и отсутствуют у прочих граждан. Полагаем, что речь может идти лишь о степени выраженности определённых признаков, комбинациях отдельных качеств личности.

Другой вопрос связан с моментом возникновения такого явления как «личность жертвы». Ранее, в ходе анализа понятия «потерпевший» и «жертва», был сделан вывод, что с криминологической точки зрения, жертва возникает не только в том случае, когда действиями преступника ей причинён ущерб, но и тогда, когда последствия для неё не наступили. То есть в тех ситуациях, когда процессуальный статус потерпевшего не возникает. Но с криминологической точки зрения жертва «сделала все», чтобы этот статус возник. Таким образом, момент возникновения личности жертвы связан с началом реализации преступных действий, причиняющих или создающих угрозу причинения вреда её законным правам и интересам. Чаще всего речь идёт о моменте начала совершения действий, образующих объективную сторону состава преступления.

В других случаях, причинение вреда не связано с совершением конкретного преступления. Наиболее ярким примером этого является криминализация подростков путём вовлечения их в группы различной криминальной направленности в социальных сетях.

В отечественной криминологической литературе таких подростков, на наш взгляд, справедливо относят к потерпевшим, поскольку вовлечение их в такие объединения неминуемо причиняет вред их нормальному развитию и воспитанию, формированию системы ценности и нравственности[1].

Некоторое время назад наиболее известной группой подобного рода была АУЕ. На момент написания работы движение АУЕ признано решением

[1] См.: *Демидова-Петрова Е.С.* Преступность несовершеннолетних в современной россии: теоретико-методологические и прикладные проблемы ее познания и предупреждения: дис. … д-ра юрид. наук. Казань, 2019. С. 163-164.

Верховного Суда РФ экстремистским[1]. Поэтому вовлечение несовершеннолетних в его деятельность, совершенное после того, как состоялось решение Верховного Суда, образует состав преступления, предусмотренного ст. 282[2] «Организация деятельности экстремистской организации» УК РФ. До этого момента вовлечение несовершеннолетних не образовывало состава преступления.

В настоящее время в социальных сетях имеется множество других групп, которые практически дословно воспроизводят идеологию АУЕ. Например, на момент написания работы в сети «ВКонтакте» действовало несколько групп под названием «Душа бандита», наиболее многочисленная из которых насчитывала 11 тысяч подписчиков. Изучение личных страниц их участников показало, что многие из них воспроизводят лозунги АУЕ. Однако уголовной ответственности за создание таких сообществ не предусматривается, поскольку они, фактически являясь экстремистскими, юридически таковыми не признаны.

Как указывалось ранее при анализе криминологических свойств киберпространства, информация в нем существует неопределённо долгое время. Поэтому весьма сложно понять, с какого момента у нас появляется личность жертвы. Аналогичная ситуация складывается с размещением мошеннических объявлений, например, на сайте объявлений avito.ru. Особенность виктимизации в киберпространстве, таким образом, состоит в том, что она, по аналогии с длящимися преступлениями, осуществляется непрерывно с момента размещения информации для публичного доступа. Однако это не означает автоматически появления жертвы. Необходимы и определённые действия с ее стороны. Например, когда ею будет прочитан соответствующий текст и предприняты определенные действия: написано письмо, осуществлён телефонный звонок и проч.

---

[1]По иску Генерального прокурора Российской Федерации Игоря Краснова Верховный Суд Российской Федерации запретил деятельность международного общественного движения «Арестантское уголовное единство». URL: http://genproc.gov.ru/smi/news/genproc/news-1886554/ (дата обращения: 08.07.2021).

Таким образом, виктимизация осуществляется не только односторонними действиями преступников, но и ответными действиями жертвы. И это, на наш взгляд, является отличительным специфическим признаком процесса виктимизации в киберпространстве. Если при совершении обычных преступлений от жертвы зачастую не требуется определённых действий, то в киберпространстве виктимизация практически всегда носит активный характер – жертва активно реагирует на специфическую информацию. Именно этот момент, по нашему мнению, и является моментом появления её личности.

Что касается обоснования необходимости изучения жертвы преступлений в киберпространстве, то, как и в случае с личностью преступника, таковым является необходимость более полного исследования причин и условий соответствующих видов преступлений с целью их эффективного предупреждения[1].

Как говорилось ранее, особенность изучаемого процесса виктимизации в нашем случае связана с активными действиями жертвы. Поэтому те мотивы, которые приводят к этой активности, особенности их формирования, выступают неотъемлемым звеном в цепочке условий, облегчающих совершение посягательств.

Единственное исключение, которое нами было выявлено при изучении уголовных дел о преступлениях, совершаемых в киберпространстве, это преступления, при которых особенности личности жертвы не имеют значения. При изучении уголовных дел нами была выявлена единственная разновидность таких преступлений, при которых злоумышленники ограничивают право владельцев телефонных номеров или аккаунтов на сервисах интернет-телефонии skype на доступ к компьютерной информации, когда телефонный номер выбирается преступниками случайным образом из большого числа возможных вариантов.

---

[1]См.: *Клещина Е.Н.* Понятие, значение и структура личности жертвы преступления // Вестник Московского университета МВД России. 2010. № 4. С. 129.

В рамках анализа уголовных дел, возбуждённых по факту совершения преступлений в киберпространстве, установлено, что наиболее часто пользователи сети «Интернет» становятся жертвами таких преступлений, как мошенничество (более 90 % изученных материалов). Следующими по распространённости стали жертвы посягательств на половую неприкосновенность несовершеннолетних, предусмотренные ст. 134 и 135 УК РФ (5 %). Значительно реже пользователи становятся жертвами иных видов преступлений, когда процесс виктимизации начинался в киберпространстве, а завершался причинением вреда при личном контакте виновного и жертвы:

- хищения (разбойные нападения, грабежи) и вымогательства. Жертва (обычно женщина), как правило, знакомится с преступником на сайте знакомств и легкомысленно соглашается на встречу[1];
- заведомо ложное сообщение о совершении преступления. Здесь имеет место обратная ситуация – женщина после знакомства в Интернете и реальной встрече заявляет о совершении в отношении нее изнасилования[2];
- склонение к суициду[3];
- убийство. Нам встретилось сообщение о единственном убийстве после ссоры, начавшейся при переписке в социальной сети.

В 2020 г., непосредственно перед принятием Верховным Судом РФ решения о признании движения АУЕ экстремистским, в Саратовской области насчитывалось порядка 570 участников сообществ соответствующей тематики,

---

[1]Уголовное дело № 1-97/2012 // Архив Октябрьского районного суда г. Иркутска; уголовное дело № 1-191/2017 // Архив Октябрьского районного суда г. Рязани; уголовное дело № 1-25/2016 // Архив Ингодинского районного суда г. Читы.

[2]Уголовное дело № 1-368/2018 // Архив Калининского районного суда г. Тюмени; уголовое дело № 1-281/2017 // Архив Калужского районного суда.

[3]А.Е.Шалагин и А.Д. Идиятуллов приводят целый перечень групп в социальных сетях, пропагандирующих суициды среди подростков. См.: *Шалагин А.Е., Идиятуллов А.Д.* Криминологическая характеристика и предупреждение преступлений, связанных с побуждением к суициду, совершаемых с использованием информационно-коммуникационной сети «Интернет» // Ученые записки Казанского юридического института МВД России. 2018. Т. 3. С. 83.

из них 388 или 67 % являлись несовершеннолетними[1]. Подростки, причисляющие себя к АУЕ, наблюдались практически во всех регионах. В 2019 г. по заявлению Генерального прокурора РФ действовало около 30 тысяч групп в социальной сети «ВКонтакте» и множество каналов на видеохостинге YouTube[2].

Количество подростков, вовлеченных в деятельность этого движения оценить проблематично. Но, имея в виду, что по типичная региональная группа насчитывает несколько десятков человек (минимальная оценка), общее число подростков, в той или иной форме вовлеченных в деятельность АУЕ исчисляется десятками тысяч человек. Нам встречались как более масштабные оценки их численности – 200 тысяч человек[3], так и более осторожные – до 34 тыс. человек в 40 регионах России[4].

После запрета АУЕ в соцсетях остаётся множество групп, эксплуатирующих тематику криминальной романтики и пропагандирующих антиобщественные установки. Так, на протяжении ряда месяцев в том числе, по состоянию на июль 2021 г., в сети «ВКонтакте» действовала группа «Душа бандита», насчитывающая более 11 тысяч участников.

Несмотря на то, что в начале страницы декларируется отказ от экстремизма и пропаганды насилия, фактическое её содержание свидетельствует об обратном. Чаще всего встречаются фото и видео массовых драк между фанатами различных футбольных клубов, демонстративных избиений, нападений на сотрудников правоохранительных органов с одобрительными подписями, а также фотографии полуголых девушек и

---

[1]Сотни саратовских подростков изучали АУЕ в соцсетях. URL: https://www.vzsar.ru/news/2020/08/11/sotni-saratovskih-podrostkov-izychali-aye-v-socsetyah.html (дата обращения: 09.07.2021).

[2]*Варывдин М.* «У нас должна быть обратная связь с людьми» Генпрокурор Игорь Краснов о том, как, надзирая за законностью, помогать гражданам // Коммерсантъ. 2019. № 164.

[3]*Степовой В.* Дети стали жить «по понятиям». URL: https://mirnov.ru/obshchestvo/problemy-semi-i-vospitanija/deti-stali-zhit-po-ponjatijam.html (дата обращения: 19.08.2021).

[4]Запрещённое в России движение АУЕ насчитывает до 34 тыс. приверженцев в 40 регионах. URL: https://tass.ru/obschestvo/9218777 (дата обращения: 19.08.2021).

дорогих автомобилей с надписями, формирующими у подростков неверные представления об отношениях мужчин и женщин, деформирующими систему ценностей.

Изучение личных страниц подростков, участвующих в группах, следующих идеологии АУЕ, показало, что в подавляющем большинстве это юноши в возрасте от 13 до 20 лет (большинство – до 17 лет) из неблагополучных семей (как правило, родители в разводе). Характер размещённой ими информации показывает отсутствие какого-либо педагогического и родительского надзора за ними.

Изучение профилей подростков, состоящих в подобных группах, и оставляемые ими комментарии под размещёнными материалами свидетельствуют о таких качествах их личности, как инфантилизм, примитивизм, стремление к самоутверждению, агрессивность.

Коренная причина этого кроется в педагогической запущенности и фактической безнадзорности многих из них. Как отмечают специалисты, при отсутствии у ребёнка привязанности к родителям, развиваются такие формы девиантной виктимности, как агрессия, желание нарушать нормы и правила[1].

Изучение материалов, размещённых на страницах подобных групп, вызывает двоякое чувство: с одной стороны виден явный уклон в пропаганду антиобщественных ценностей, с другой – прослеживается значительный дефицит положительных примеров в окружающей действительности приводит к тому, что подростки, которые в силу возраста всегда стремятся к каким-то идеалам (крепкой мужской дружбы, смелости, героизма, уважения к родителям, к любви), в силу деформации духовно-нравственной сферы, отсутствия положительного воздействия со стороны общества, реализуют это в крайне уродливых и антиобщественных формах. Таким образом, характерной чертой подростков, вовлекаемых в антиобщественные движения криминальной

[1] *Жихарева Л.В.* Особенности эмоциональной привязанности у подростков, склонных к девиантной виктимности // Научный результат. Педагогика и психология образования. 2018. Т. 4. № 4. С. 104.

направленности, выступает крайняя педагогическая запущенность, отсутствие в окружении авторитетных личностей, способных оказать положительное антикриминогенное воздействие.

Характерной причиной, по которой подростки отторгаются от общества и примыкают к антиобщественным группам, является пассивность государства в вопросе конструирования у подростков представления о будущем, в котором они будут жить. Формирование информационной повестки осуществляется не путем активной пропаганды ценностей общества, а негативным образом – путем запрета нежелательной информации.

Следует также отметить, что многие подростки вступают в группы антиобщественной направленности не из-за увлечения уголовной романтикой, а в силу желания избежать травли со стороны сверстников. Для таких лиц, как отмечается в специальной литературе характерен повышенный уровень тревожности, высокий уровень фрустрации. Такие дети демонстрируют снижение школьной успеваемости и активности на уроках[1].

Проинтервьюированные нами сотрудники уголовного розыска охарактеризовали участников таких сообществ, как в целом, хороших детей, не чуждых доброты, но несформировавших жизненные ориентиры.

Также ими был высказан тезис, что в настоящее время вопросы выявления и постановки на учёт таких подростков реализованы очень хорошо. Эта деятельность осуществляется на регулярной основе и находится под постоянным контролем руководства и органов прокуратуры. Однако никаких других мер в отношении таких детей государство не предпринимает. Не осуществляется внеклассная деятельность, подростки не вовлекаются в научно-техническое творчество, внеклассные программы развития. Точнее сказать – такие виды организации досуга есть, но они построены на коммерческой основе

[1] *Зинцова А.С.* Социальная профилактика кибербуллинга // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. 2014. № 3. С. 127; *Сафуанов Ф.С., Докучаева Н.В.* Особенности личности жертв противоправных посягательств в Интернете // Психология и право. 2015. Т. 5, № 4. С. 92.

и не доступны социально незащищённым семьям.

Таким образом, в предупредительной деятельности по отношению к несовершеннолетним имеется явный перекос в сторону полицейских мер контроля и надзора при практическом отсутствии планомерного и организованного педагогического воздействия.

Как отмечалось ранее, большая часть жертв преступлений по изученным нами уголовным делам, являются пострадавшими от различных видов мошенничеств, которые в отличие от большинства других преступлений демонстрируют быстрый рост. Для киберпреступлений характерно то, что мошенники не выискивают жертв по определённым признакам. Чаще они просто «расставляют ловушку», в которую жертва попадает путём своих активных действий.

Наиболее распространёнными являются мошенничества при совершении покупок. Граждане переводят на счета мошенников деньги за товары (например, по объявлениям на сайте Avito) – о таких преступлениях заявили 46,4 % потерпевших. Вторыми по распространенности стали хищения, совершаемые с использованием фишинга, т.е. сайтов, копирующих внешний вид респектабельных сетевых площадок или магазинов – 42,9% потерпевших. Граждане при таком виде преступлений совершали перевод небольших сумм (например, за услуги поиска водителя, следующего в попутном направлении, предоставляемые сервисом BlaBlaCar) на мошеннические ресурсы.

Следующими по распространенности являются мошенничества, связанные с присвоением сумм, якобы направляемых на благотворительные цели (10,7 % потерпевших), лотерейное мошенничество (7,1 % потерпевших) и мошенничество со сделками с недвижимостью (7,1 % потерпевших).

Реже всего (единичные случаи) совершаются мошенничества, связанные с инвестициями, взломом социальных сетей, аккаунтов пользователей, денежными займами.

Здесь следует заметить, что некоторые проанкетированные становились

жертвами мошенников в киберпространстве более одного раза, поэтому суммарное число потерпевших превышает 100 %.

Интересной особенностью кибермошенничеств является омоложение возраста потерпевших. Если ещё год назад типичный потерпевший являлся пенсионером (возраст от 60 лет и старше), то в настоящее время под прицелом мошенников все чаще оказываются мужчины активного трудоспособного возраста (40-50 лет). Такое наблюдение получено в рамках интервьюирования следователей, расследующих мошенничества, это же подтверждают результаты проведённого нами анкетирования граждан.

Сходная тенденция отмечается и правоохранительными органами. В частности в Калужской области отмечаемое омоложение потерпевших связывается с развитием онлайн-покупок, которые активно практикуют представители именно этой возрастной группы, при посещении сайтов, копирующих оформление известных интернет-магазинов и торговых площадок[1].

В другом сообщении отмечается, что в возрасте 20-40 лет люди чаще становятся жертвами интернет-мошенников, а старше 70 лет чаще всего становятся жертвами телефонных мошенников[2].

По результатам проведённого нами анкетирования сотрудников правоохранительных органов, распределение потерпевших по возрасту следующее:

- до 40 лет – 17,5 %
- до 50 лет – 34,7 %
- старше 50 лет – 47,8 %

В целом такое распределение, на наш взгляд, демонстрирует действие

---

[1] *Гусев А.* В Калужской области снизился возраст пострадавших от интернет-мошенничеств. URL: https://kgvinfo.ru/novosti/obshchestvo/v-kaluzhskoy-oblasti-pomolodel-vozrast-postradavshikh-ot-internet-moshennichestv/ (дата обращения: 27.07.2021).

[2] *Черноусов И.* Названы основные способы мошенничества по телефону и в Сети. URL: https://rg.ru/2020/12/01/nazvany-osnovnye-sposoby-moshennichestva-po-telefonu-i-v-seti.html (дата обращения: 27.07.2021).

одного из важнейших виктимогенных факторов – компьютерной грамотности, которая выше в младших возрастных группах. Представители старшего поколения слабо ориентируются в потоке новаций, вновь возникающих сервисов и услуг и чаще демонстрируют беспомощность.

В этом же анкетировании получены данные о наиболее распространённой причине виктимизации – отсутствии технических познаний. Эту причину указали 64,9 % проанкетированных нами сотрудников правоохранительных. Этот фактор оказался для киберпреступлений даже более значимым, чем отсутствие опыта деятельности в сети «Интернет» (16,9 %).

Половые отличия, судя по всему, не имеют определенного значения для процессов виктимизации в киберпространстве. Как отмечают в интервью следователи и подтверждает проведенное нами анкетирование, количество потерпевших мужчин и женщин примерно равно.

По образованию – наиболее распространено среднее и неполное среднее образование. Это обстоятельство подталкивает нас к выводу, что типичная жертва мошенника связывает улучшение своего материального уровня не с длительной упорной трудовой деятельностью, а с разовым успехом, чем и пользуются мошенники[1].

Проанкетированные сотрудники правоохранительных органов отмечали, что для потерпевших характерно отсутствие образования, о чем заявило 30,4 % респондентов. 12,8% отметили низкий уровень интеллекта потерпевших.

По роду деятельности в массе потерпевших чаще всего встречаются представители строителей, самозанятые, вахтовики, временно не работающие, уборщицы, пенсионеры.

Как пояснили следователи в интервью, мошенники, как правило, не

---

[1]Это качество жертв мошенников отмечают и другие авторы. См.: *Майоров А.В., Яременко Н.Е.* Виктимологический аспект мошенничества // Виктимология. 2019. № 3. С. 37; Пушмин И.И. Детерминанты виктимизации жертв мошенничеств // Научный форум: юриспруденция, история, социология, политология и философия: сб. ст. по матер. XVII междунар. науч.-практ. конф. 2018. № 4. С. 72 и др.

нацелены на специальный подбор жертв, а пытаются обработать как можно большее число граждан.

Единственное исключение составляют преступления, совершаемые банковскими служащими, которые имеют возможность подбирать жертв с учётом состояния их банковских счетов. Однако и в таком случае, преступники ориентируются не на личные качества жертвы, а на состояние счета.

Ранее отмечалось, что многие жертвы мошенников демонстрировали элементарную жадность, что и было использовано преступниками. Кроме того, изучение материалов уголовных дел показало, что потерпевшие от мошенничеств часто демонстрируют низкий уровень деловой культуры, неспособность критически воспринимать ситуацию – они не проверяют сведения о лицах, дающих объявления о продаже каких-либо вещей, переводя без всяких гарантий крупные суммы на условиях полной предоплаты. Например, по одному из уголовных дел потерпевшая увидела в сети «ВКонтакте» объявление об аренде гостиничных номеров и перевела 600 тыс. рублей за аренду 6 гостиничных номеров на 100 дней. При этом она не удосужилась навести элементарные справки о человеке, которому она перевела крупную сумму, о его репутации, отзывах о его бизнесе[1].

В аналогичном случае потерпевшая перевела деньги по объявлению о продаже предметов одежды в сети «Одноклассники» на условиях стопроцентной предоплаты. При этом она также не проверяла историю аккаунта покупателя[2].

В ходе интервьюирования следователей была выявлена одна специфическая особенность жертв телефонных мошенников. Как правило, потерпевшие в момент звонка от мошенников были заняты каким-то делом, т.е. их внимание не было сфокусировано на обеспечении безопасности.

---

[1]Уголовное дело № 1-98/2020 // Архив Лазаревского районного суда г. Сочи (Краснодарский край) за 2020 г.

[2]Уголовное дело № 1-339/2020 // Архив Усть-Илимского городского суда (Иркутская область) за 2020 г.

Впоследствии такие потерпевшие не могли внятно объяснить, почему они сообщили незнакомым лицам по телефону информацию о последних действиях с банковскими карточками.

В противоположность таким потерпевшим те лица, которым звонили в свободное время, могли сосредоточиться и прерывали разговор, прерывая тем самым преступную деятельность мошенников в отношении себя.

Аналогичная ситуация была выявлена и в ходе интервью с потерпевшей от фишингового мошенничества. Девушка пыталась после окончания летних каникул вернуться в город, в котором она учится в ВУЗе. Испытывая нехватку средств (типичную для студентов), она попыталась сэкономить, заказав поездку на сервисе “Бла бла кар”. Данный сайт предоставляет услугу подбора водителя. Лица, направляющиеся в междугородние поездки, регистрируются на таком сайте и набирают попутчиков. Цена междугородней поездки таким образом составляет 200-400 рублей, что ощутимо меньше стоимости проезда на официальном транспорте. Проинтервьюированная потерпевшая, находясь в состоянии спешки, не обратила внимание на то, что её сообщение было перенаправлено для осуществления платежа на поддельный сайт и перевела на счёт запрошенные «водителем» деньги.

О том, что деньги похищены, она поняла не сразу, поскольку, ожидая приезда водителя, пыталась с ним связаться. Преступник же уверял её, что он задерживается из-за пробок, но скоро будет. И лишь позже, в спокойном состоянии, проанализировав ситуацию с потерей денег, оплаченных за поездку, девушка увидела, как она рассказала, признаки подделки сайта.

Таким образом, важнейшая особенность виктимизации связана, в большей степени, не с личностными особенностями жертвы, а с особенностями ситуации, в которой она пребывает.

Конечно, в качестве гипотезы, можно было бы выдвинуть такое предположение, что в подобных ситуациях важнейшим качеством личности является стрессоустойчивость, возможность концентрации внимания в

условиях стресса, спешки, отвлекающих факторов.

Однако нам представляется, что такими способностями обладают лишь специально подготовленные люди. Большинство же неспособно одновременно концентрировать внимание более чем на одном объекте одновременно. Кстати, эта же особенность психики активно используется, например, карманными ворами, отвлекающими жертву различными способами: наступая ей на ногу, сильно толкая, задавая какие-то вопросы, пачкая одежду и т.п.[1]

Поэтому выделять слабую стрессоустойчивость в качестве личностной особенности жертв кибермошенников специально не следует.

В литературе есть сходное мнение относительно характеристики жертвы карманных воров. Н.А. Вакуленко указывает, что жертвой карманников может стать любой человек, но при этом вероятность виктимизации возрастает при ослаблении самоконтроля, беспечности, отвлечении внимания, попадании в места скопления людей[2].

В пользу нашего подхода говорит и такой яркий пример, как деятельность так называемых пранкеров, которые, используя методы социальной инженерии, выдают себя за каких-нибудь известных лиц и получают в ходе телефонных переговоров весьма чувствительную информацию. Известные в нашей стране пранкеры Алексей Столяров и Владимир Кузнецов (Лексус и Вован), часто совершали звонки высокопоставленным руководителям других стран, то есть преодолевали ряд административных барьеров со стороны специально подготовленных

---

[1]См., напр.: *Пацкевич А.П.* Криминалистическое исследование способа совершения карманных краж // Борьба с преступностью: теория и практика: тез. докл. IX междунар. науч.-практ. конф. Могилев, 2021. С. 262; *Скоков И.Е* Элементы оперативно-розыскной характеристики карманных краж // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований: матер. регион. науч.-практ. конф. СПб: Изд-во Санкт-Петерб. ун-та МВД России, 2020. С. 204.

[2]*Вакуленко Н.А.* Актуальность мер виктимологической профилактики карманных краж как важного компонента предупреждения преступлений // Юристъ-Правоведъ. 2020. № 4 (95). С. 68.

сотрудников служб протокола, дипломатических ведомств и т.д.[1]

В одном из недавних розыгрышей (пранков) они, представившись супругой Алексея Навального Юлией и руководителем его штаба Леонидом Волковым, позвонили министру иностранных дел Швеции Анн Линде, которая в ходе беседы сообщила им подробности внутриполитических отношений в Евросоюзе, политических сделок, которые заключают между собой различные страны, а также завила, что Швеция ведёт работу по оказанию воздействия на общественное мнение в России, финансирует российскую оппозицию[2].

Проинтервьюированные нами следователи сообщили, что каких-либо выраженных отличительных признаков, касающихся психических особенностей личности, у жертв кибермошенничества не наблюдается. Это касается как типов темперамента, так и уровня интеллектуального развития.

В ходе проведённого анкетирования нами была выявлена ещё одна психологическая особенность жертв кибермошенников. Из числа всех респондентов подавляющее большинство (98,4 %) заявили, что обладают банковской картой (одной или несколькими). При этом более половины (56,3 %) сообщили, что испытывают тревогу за сохранность своих денежных средств. Преобладающими причинами такого состояния выступают недоверие 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 %)[3].

В криминологической литературе отмечается, что тревожность является важным фактором виктимизации[4].

---

[1]«Это – гражданская разведка» – пранкер Вован о своих проделках с Лексусом. URL: https://www.5-tv.ru/news/199800/ (дата обращения: 24.07.2021).

[2]*Lapidus A* Ann Linde lurad av ryska bluffmakare. URL: https://www.expressen.se/nyheter/ann-linde-lurad-av-ryska-bluffmakare/ (дата обращения: 08.08.2021).

[3]При ответе респонденты могли указывать несколько причин, поэтому суммарное количество ответов может превышать 100 %.

[4]*Шейнов В.П.* Разработка теста «психологические факторы риска виктимизации взрослого индивида // Системная психология и социология. 2018. № 3. С. 20; *Нестерова А.А.*

При этом одной из причин тревожности является низкий уровень компьютерной грамотности. В одном из криминологических исследований приводятся данные о том, что осведомленность о способах защиты компьютера и сам факт использования защитных программ зависят от возраста пользователя. Если в группе 15-29 лет 98,5 % опрошенных заявили, что используют средства для защиты компьютера, то в группах 40-49 и 50 лет и старше таких было соответственно 66 и 40%. При этом потребность в получении информации о способах защиты компьютера, наоборот, значительно выше в старших возрастных группах[1].

Также проанкетированные сотрудники правоохранительных органов сообщили, что виктимизации способствует излишняя доверчивость (68,9 % проанкетированных).

Исходя из изложенного можно заключить, что жертвы кибермошенничеств характеризуются композицией нескольких основных особенностей: излишней доверчивостью, низким уровнем технической грамотности, тревожностью относительно сохранности денежных средств и рассеянностью внимания в момент совершения посягательства, связанного с попыткой выполнить одновременно несколько дел.

Таким образом, выявленный нами комплекс факторов виктимности жертв кибермошенников коррелирует с результатами других криминологических исследований.

При изучении материалов уголовных дел, возбуждённых по фактам совершения преступлений против половой неприкосновенности несовершеннолетних, было установлено, что во всех случаях взаимодействие жертвы и преступника происходило путем общения в социальной сети. По

Психологические особенности детей, склонных к виктимности в ситуации школьной травли // Личность в экстремальных условиях и кризисных ситуациях жизнедеятельности. 2015. № 5. С. 280.

[1] *Скурихина А.А., Ронжина О.С.* Виктимность в сфере компьютерных преступлений // Виктимология. 2014. № 2. С. 48.

изученным нами уголовным делам это была социальная сеть «ВКонтакте». Это объясняется, прежде всего, популярностью этой сети среди несовершеннолетних. Другая большая социальная сеть «Одноклассники» не столь популярна, поскольку ориентирована в большей степени на взрослую аудиторию. В специальной литературе отмечалось, что увеличение числа таких преступлений в нашей стране хронологически совпало с ростом популярности сети «ВКонтакте»[1]. Этим, думается, и объясняется виктимогенное значение этой сети.

По всем изученным уголовным делам потерпевшими были девочки.

Процесс виктимизации в отношении таких лиц разворачивается по двум типичным сценариям. В первом случае злоумышленник вступает в переписку с жертвой. Во многих случаях потерпевшие при этом не сообщают свой фактический возраст, либо сообщают его после очной встречи, закончившейся половым актом.

По второму сценарию после знакомства злоумышленник под разными предлогами пытается получить интимные фотографии девочек. В ход идут как уговоры, так и демонстрация порнографических фото- и видеоизображений. После того как потерпевшие присылают свои фотографии, их шантажом заставляют продолжать делать новые снимки снова и снова.

Обращает на себя внимание то, что в таких случаях жертвы не сразу сообщают родителям о случаях домогательства, требований со стороны педофилов и выполняют их требования – пересылают им свои интимные фотографии, вступают в переписку и проч. Объясняется это неопытностью и растерянностью жертв – они не знают что делать, не подготовлены родителями к тому, как действовать в подобных ситуациях.

Здесь налицо следующая проблема. Во-первых, многие дети, формально находясь под наблюдением родителей, в киберпространстве являются

[1] *Бытко С.Ю.* Эффективность предупредительного воздействия уголовного наказания на преступность: теоретический и прикладной аспекты: дис. … д-ра юрид. наук. Саратов, 2018. С. 242.

фактически безнадзорными. Родители по невежеству полагают, что приобретя ребенку гаджет и обеспечив доступ в сеть, они решили проблему организации его свободного времени и досуга.

Во-вторых, обращает на себя внимание отсутствие доверительных отношений между ребенком и родителями, когда потерпевшие боятся сообщить взрослым о допущенных ими аморальных действиях.

Это обстоятельство характерно для многих посягательств против половой неприкосновенности несовершеннолетних. При этом особо отмечается отсутствие доверительных отношений с матерью[1].

В-третьих, пребывание в киберпространстве сопряжено со слишком ранним ознакомлением ребенка с информацией интимного характера, с которой он ещё не может правильно распорядиться. В качестве нормы усваиваются модели поведения, демонстрируемые в роликах непристойного содержания без их критического осмысления. Т.е. происходит постепенное растление малолетних и педофил, как правило, встречает жертв, которые уже имеют представление об интимной жизни взрослых.

Слишком раннее погружение в киберпространство, происходящее в период формирования навыков коммуникации, активного усвоения моральных норм, часто приводит к деформации этого процесса,

Не обладая социальным опытом, несовершеннолетние на своих страницах в социальных сетях выкладывают много информации личного характера – о месте учёбы, жительства, личные фотографии. Девочки легко вступают с преступниками в переписку, полагая, что находятся в безопасности, а впоследствии допускают даже личные встречи, которые заканчиваются совершением в отношении них преступлений сексуального характера[2].

И, наконец, во многих случаях имеет место вопиющая компьютерная

---

[1]*Семерикова А.А.* Криминологический анализ жертвы сексуального насилия // Юридические исследования. 2018. № 7. С. 30.

[2]См., напр.: Уголовное дело № 1-400\2016 // Архив Тосненского городского суда Ленинградской области

безграмотность родителей и отсутствие представлений об опасности, с которыми могут столкнуться в киберпространстве их дети.

В отдельных случаях потерпевшие сами провоцируют противоправные действия в отношении себя. Такая ситуация сложилась после знакомства гражданина П. с несовершеннолетней в сети «ВКонтакте». Последняя в переписке заявила, что достигла возраста шестнадцать лет и согласилась на встречу, в ходе которой произошло половое сношение между ней и гражданином П. Впоследствии потерпевшая сообщила П., что она не достигла шестнадцати лет. После чего имела неоднократно половые сношения с П.[1]

Причины такого поведения кроются, на наш взгляд, в том, что подростки, испытывая объяснимый интерес к сексуальной жизни и её проявлениям, легко получают доступ к любой информации подобного рода, причём в большей части в порнографической форме, с демонстрацией различных половых извращений, что крайне разрушительно сказывается на формировании их личности. Фактически то, что происходит с детьми, имеющими неконтролируемый доступ к сети, является развращением их нравов.

Неблагополучие в семье, отсутствие доверительных отношений с родителями, конфликты с ними являются характерным признаком потерпевших и от таких преступлений, как склонение к самоубийству[2]. Так, гражданка Г., зная о конфликте несовершеннолетней потерпевшей с матерью, начала посредством переписки в сети «ВКонтакте» склонять потерпевшую к суициду, присылала ей ссылки на фото- и видеозаписи суицидов. Находясь в депрессивном состоянии, потерпевшая в результате психологического воздействия со стороны Г. предприняла попытку суицида, проглотив 10 таблеток лекарственного препарата «Феназепам» и попытавшись перерезать

---

[1]Уголовное дело № 1-24/2019 // Архив Ленинского районного суда г. Севастополь за 2019 г.

[2]*Зиновьева Н.О., Михайлова Н.Ф.* Психология и психотерапия насилия. Ребёнок в кризисной ситуации. СПб.: Речь, 2003. 248 с.

вены на руке[1].

Подводя итог нашим рассуждениям, можно сделать некоторые промежуточные выводы:

- непосредственные причины преступления кроются в личности;
- наиболее общие причины всей преступности, влияющие на деформацию системы нравственных ценностей личности, её потребности и т.п. относятся к вопросам личности преступника и, являясь элементами причинного комплекса, в качестве таковых теоретиками не рассматриваются.
- причины конкретного преступления и причины всей преступности сходны и относятся между собой как часть и целое (где часть – причины конкретных преступлений, целое – причины всей преступности).
- внешние по отношению к личности факторы, именуемые в криминологии причинами преступлений, таковыми фактически не являются. Имеет место своеобразная терминологическая маскировка при которой наиболее важные и близкие по времени к преступлению условия именуются причинами.
- изучение причин конкретных преступлений необходимо переводить на современные рельсы, накапливая максимальное количество информации о личности преступника, обстоятельствах совершения преступления для дальнейшей её автоматизированной обработки (речь идет о таком направлении исследования огромных массивов данных, которые вручную обработать невозможно, и именуемом «BigData», большие данные).

В той части, которая характеризуется причинами индивидуального поведения, наши рассуждения применимы и к причинам виктимизации. Личность жертвы как совокупность специфических особенностей психики, мировоззрения, физиологических качеств формируется под влиянием

[1]Уголовное дело № 1-25/2018 // Архив Судакского городского суда Республики Крым за 2018 г.

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. Характерным свойством отдельных видов преступлений в сети «Интернет» является то, что вред может причиняться неопределённому числу лиц. Например, мошенники организовывают call-центр и обзванивают граждан, обращаясь к ним под видом сотрудников социальных служб и обещая компенсацию.

В таких ситуациях личные качества потерпевшего выступают необходимым условием совершения в отношении него преступления.

Но если говорить об общем, например, об отдельном виде преступлений в целом, то ситуация несколько иная. Мошенники, организуя некоторый вид обмана, учитывают потенциальный круг потерпевших с тем, чтобы оценить прибыль от совершения преступлений. Например, получая доступ к базе данных лиц, ранее пострадавших от каких-либо незаконных действий, они рассчитывают, что значительная часть из них может быть обманута ими. Если круг потенциальных жертв недостаточно широк, то потенциальная прибыль не возместит расходов на организацию преступления. В таких ситуациях распространенность виктимогенных качеств личности потенциальных жертв может выступать в качестве причины вида преступлений[1].

Таким образом, можно сделать следующие выводы:

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

2. При характеристике личности жертвы преступлений, совершаемых в

[1] *Родина Е.А.* О некоторых проблемах механизма детерминации преступности и виктимного поведения // Противодействие правонарушениям, совершаемым с использованием информационных технологий: сб. ст. по матер. науч.-практ. конф. / III школы-семинара молодых ученых-юристов (11 ноября 2021 г.). М.: МФЮА, 2021. С. 172.

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 разных 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).

ГЛАВА 2. ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРЕДУПРЕЖДЕНИЯ КРИМИНОГЕННОЙ ВИКТИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ «ИНТЕРНЕТ» В КИБЕРПРОСТРАНСТВЕ

§ 1. Зарубежный опыт противодействия криминальной виктимизации пользователей сети «Интернет» в киберпространстве

Уголовно-правовые и криминологические аспекты киберпреступности в достаточной степени представлены в криминологической литературе. Чтобы не повторять других авторов, сконцентрируем внимание на мерах виктимологической профилактики таких посягательств, предпринимаемых в зарубежных странах.

В настоящее время наиболее быстро развивающимся в сфере высоких технологий государством является, наверное, Китай. Это государство отличается от западных стран наличием идеологии, ролью государства, оригинальным менталитетом и специфическими культурными традициями. Кроме того, это государство в силу внешнеполитических событий последних лет занимает место партнера России. Интенсивность двусторонних экономических, культурных и военных связей постоянно усиливается. Поэтому предпринимаемые в КНР меры представляют для нас особый интерес, поскольку они потенциально могут быть применимы и в нашей стране.

В 2014 г. было издано Постановление Госсовета КНР «О планировании строительства системы социального кредита (2014–2020)»[1].

Данный документ ориентирует народные представительства провинций, автономных регионов и муниципалитетов на создание системы, повышающей добросовестность и уровень доверия всего общества. Речь в документе идет о добросовестности не только в кредитных отношениях, но и в сфере производства промышленной, пищевой, фармацевтической и другой продукции, ужесточении наказаний за всевозможные виды обмана.

[1]Постановление Госсовета КНР «О планировании строительства системы социального кредита (2014–2020)». URL: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm (дата обращения: 10.08.2021).

В настоящее время ситуация с социальным рейтингом не совсем прозрачна. В ряде публикаций утверждается, что на основе низкого социального рейтинга граждане КНР ограничиваются в реализации отдельных прав[1]. Как отмечается в публикациях, посвящённых системе социального рейтинга (или её ещё называют системой социального кредита), каждому гражданину КНР присваивается определённое количество баллов, которое может снижаться вследствии совершения неблаговидных, неправомерных поступков, недостойного поведения, так и возрастать. В частности, указывается что в 2018 г. более 20 млн китайцев не смогли приобрести билеты на самолёты или поезда из-за низкого социального рейтинга. Кроме того, в качестве возможных негативных последствий снижения социального рейтинга отмечаются публичное порицание, снижение скорости доступа в Интернет, ограничение права на поступление в вузы, запрет на работу в государственных учреждениях и т.п.[2] Источниками информации о поведении граждан являются данные сетевых магазинов, социальных сетей, материалы административной практики, записи видеокамер наружного наблюдения, интегрированных с системой распознавания по лицу и т.п.[3]

В других публикациях дискриминационная сущность системы

---

[1]*Шалагин А.Е., Идиятуллов А.Д.* Предупреждение преступлений в эпоху цифровизации // Державинские чтения: сб. ст. XVI междунар. науч.-практ. конф. М., 2021. С. 386. *Городничев С.В., Герасимова П.Г.* Система социального рейтинга в Китае // Вестник Тульского филиала Финуниверситета. 2020. № 1. С. 134; *Графов Д.Б.* Система социального рейтинга в КНР как информационно-коммуникационная технология поощрения и наказания // Власть. 2020. № 2. С. 250.

[2]*Антропов Р.В., Лиценберг И.И.* Система социального рейтинга в Китае: прогрессивный механизм поощрения и наказания или цифровая диктатура? // Актуальные проблемы развития КНР в процессе её регионализации и глобализации: матер. XII междунар. науч.-практ. конф. Чита: Забайкальский государственный университет, 2020. С. 20; *Шведова В.О.* Цифровые идентификаторы личности как новый источник социальной дискриминации // Социальная интеграция и развитие этнокультур в евразийском пространстве. 2020. Т. 3, № 9. С. 239.

[3]*Климович А.П.* Влияние цифровых технологий на современное общество. ример системы рейтинга социального кредита в Китае // Цифровая социология. 2020. Т. 3, № 3. С. 40.

социального рейтинга и её масштабы подвергаются сомнению[1].

Однако для наших целей представляют интерес следующее: любой гражданин КНР, намереваясь приобрести какую-либо продукцию, может выяснить: является ли юридическое лицо или гражданин, у которого он желает её приобрести, добропорядочным, участвовала ли организация в мошеннических схемах или нет, имеет ли интересующий вас человек судимость или нет. Соответствующий сайт размещён по адресу https://www.creditchina.gov.cn/.

Во избежание неблагоприятных последствий из-за размещения ошибочной информации о кредитном рейтинге, в ст. 1029 гражданского кодекса КНР предусмотрено положение о праве субъектов гражданских правоотношений запрашивать сведения об оценке кредитоспособности, требовать внесения исправлений в случае размещения неверной информации, удаления соответствующих сведений или принятия иных мер по защите репутации[2].

Другой инструмент регулирования поведения граждан – создание чёрных и красных списков. В чёрные списки попадают граждане, допустившие правонарушение: курение в вагоне поезда, драку на борту авиасудна, безбилетный проезд и т.п. В подобных ситуациях фамилию правонарушителя заносят в чёрные списки сами компании-перевозчики без решения суда. Кроме того, в чёрные списки помещаются все лица, имеющие судимости за отдельные виды преступлений (убийства, мошенничества, кражи и т.п.), должники по кредитам и т.д. Доступ к таким спискам открыт для всех желающих. В частности на правительственном сайте по адресу http://www.caac.gov.cn/caaccredit/frontend/credit/personsummary/list публикуются списки лиц, которым запрещено пользование самолетами гражданской авиации,

---

[1] *Мавричев А.А., Макаров Е.А., Дьяконенко А.В., Хрипунова М.Б.* Система социального рейтинга в Китае: миф или реальность // Наука Красноярья. 2021. Т. 10, № 4-2. С. 60.

[2] Гражданский кодекс КНР / пер. П.В. Бажанова. URL: https://chinalaw.center/civil_law/china_civil_code_2020_russian/ (дата обращения: 10.08.2021).

а по адресу https://kyfw.12306.cn/otn/queryDishonest/init – списки лиц, которым запрещено пользование железнодорожным транспортом. Причём на сайте отмечается, что такой запрет вводится во исполнение требований системы социального кредита.

Еще одной особенностью использования киберпространства в КНР является то, что граждане должны регистрироваться в социальных сетях под настоящими именами, не используя псевдонимов, с указанием своих паспортных данных. Как отмечается в криминологической литературе, такая мера, была вызвана широким распространением клеветы, недобросовестной рекламы и мошенничества в киберпространстве КНР. Деанонимизация общения в сети, как указывают отечественные криминологи, фактически уничтожила свободу общения, однако уровень киберпреступности в Китае значительно снизился[1].

Впрочем, Россия также движется по пути ограничения анонимности в киберпространстве. В частности, при регистрации в социальной сети «ВКонтакте» пользователь должен указывать номер своего мобильного телефона. При этом предоставление услуг мобильной связи в связи с поправками, внесёнными в Федеральный закон «О связи», должно осуществляться лишь на основании паспортных данных пользователя[2].

Таким образом, несмотря на то, что сама сеть «ВКонтакте» достоверно знает о пользователе лишь номер его телефона, установить реального владельца аккаунта можно, воспользовавшись информацией оператора сотовой связи о владельце указанного номера.

Развитие сети «Интернет» привело к тому, что пользователям стала

---

[1] *Желудков М.А., Попов А.М., Дубровина М.М.* Особенности противодействия киберпреступности в России и зарубежных странах // Вестник Волгоградской академии МВД России. 2018. № 3 (46). С. 100; Теперь в китайских соцсетях регистрируются только по паспорту. URL: https://ovesti.ru/other/world/8844-teper-v-kitayskih-socsetyah-registriruyutsya-tolko-po-pasportu.html (дата обращения: 08.08.2021).

[2] Федеральный закон от 7 июля 2003 г. № 126-ФЗ (с изм. и доп. от 14 июля 2022 г., № 356-ФЗ) «О связи» // СЗ РФ. 2003. № 28, ст. 2895; 2022. № 29 (ч. III), ст. 5323.

доступна самая разнообразная информация, во многих случаях имеют место специальные операции по вбросу негативной информации, дискредитирующей правительства и приводящие к дестабилизации внутриполитической обстановки. В настоящее время возможности разрушительных воздействий извне не требуют специального пояснения. Россия, братское государство Беларусь столкнулось с массовыми протестами, вовлечением граждан в противоправную деятельность, инспирируемыми из-за рубежа посредством социальных сетей и интернет-мессенджеров. В КНР эти угрозы осознали значительно раньше и предприняли технические меры по предотвращению посягательств на информационную безопасность страны. Одним из самых главных достижений в этом направлении стало создание «Золотого Щита», специальной многоуровневой системы, позволяющей блокировать нежелательные сайты, деструктивный контент[1].

Кроме того, крупнейшие западные компании, работающие на китайском рынке, были принуждены к исполнению национального законодательства КНР в части фильтрации нежелательного контента. Например, компания Google самостоятельно блокирует доступ с территории Китая к сайтам, включённым в чёрные списки Правительства КНР. В то время, как другие сервисы, отказывающиеся исполнять китайское законодательство (такие, как YouTube, Facebook), остаются заблокированными[2]. Следует заметить также, что блокировки западных медийных сервисов периодически происходят и в Иране, Туркменистане, Турции, Таиланде, Бразилии, Марокко и других странах[3]. Таким образом, блокирование нежелательной информации не является чертой, присущей лишь одной стране.

Еще одним средством предотвращения анонимности в киберпространстве

---

[1] *Чекменёва Т.Г., Ершов Б.А., Трубицын С.Д., Остапенко А.А.* Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты // Бюллетень социально-экономических и гуманитарных исследований. 2020. № 7 (9). С. 81.

[2] *Верник А.Г.* Цензура в Интернете: исторический аспект, современный опыт и перспективы // Дискуссия. 2014. № 11. С. 177.

[3] Там же.

является борьба с VPN-сервисами. VPN (от virtual private network) позволяют создавать виртуальные сети поверх обычных интернет соединений, при этом ни провайдер, ни кто-либо ещё, не могут узнать – какого рода информация передается и какие сайты посещает пользователь[1]. Использование таких сервисов существенно затрудняет блокирование нежелательной информации, поэтому в КНР VPN запрещены.

Приложения для использования vpn были удалены из магазина приложений AppStore, китайские провайдеры Интернета получили предписание о запрете подключений чрез vpn, хотя ограниченные возможности использования этой технологии ещё сохраняются[2].

Таким образом, в КНР функционирует комплексная система обеспечения кибербезопасности как государства, так и граждан, поскольку предпринятые меры существенно ограничивают возможности безнаказанного совершения мошеннических действий, вовлечения граждан (как взрослых, так и несовершеннолетних) в противоправную деятельность, совращения малолетних через соцсети, склонения к самоубийству и т.д. и т.п.

При этом обеспечение кибербезопасности не ограничивается лишь мерами по блокировки информации. Наряду с запретами, в полной мере реализованы возможности реального удовлетворения потребностей, возникающих в связи с деятельностью граждан в киберпространстве. В Китае созданы полноценные аналоги западных медиасервисов, социальных сетей, мессенджеров, интернет-магазинов, платёжных систем и т.п. Однако только этими мерами дело не ограничивается. В этой стране разрабатываются собственные процессоры, собственная операционная система для компьютеров Red Flag Linux[3], операционная система для мобильных устройств HarmonyOS[1].

---

[1] *Шабаев М.Б., Матыгов М.М.* Как работает VPN и обзор лучших VPN провайдеров // Тенденции развития науки и образования. 2020. № 68-1. С. 140.

[2] *Barbaschow A.* VPNs can still be used in China despite March 31 ban. URL: https://www.zdnet.com/article/vpns-can-still-be-used-in-china-despite-march-31-ban/ (дата обращения: 10.08.2021).

[3] Доступна по адресу https://www.chinaredflag.cn/

Кроме того, в Китае разрабатывается и производится весь спектр современной компьютерной техники: персональные компьютеры, ноутбуки и их компоненты, мобильные телефоны, роутеры, модемы, модули памяти и т.д. Эта деятельность является также очень важной для защиты прав китайских граждан, поскольку существенно ограничивает возможности воздействия извне на китайский сегмент Интернета.

Таким образом, можно говорить о реализации в КНР полноценного цифрового суверенитета и полноценной защиты прав личности в киберпространстве.

КНР является единственной страной, которая применяет столь всеобъемлющие и комплексные меры контроля за национальным киберпространством и ограничением свободы доступа к информации и свободы слова ради обеспечения кибербезопасности[2].

Для других стран такая решительность не характерна, поэтому и подходы к обеспечению безопасности пользователей отличаются.

В западных странах акцент делается на такие меры, как своевременное выявление угроз для пользователей, использование программных средств выявления потенциально опасных сообщений. В частности, для борьбы с запугиванием (кибербуллингом) детей через соцсети, активно разрабатываются программные комплексы, выявляющие угрожающие сообщения на различных языках. Принцип их действия состоит в сканировании сообщений, распространяемых в соцсетях, и поиске в них характерных для угроз слов, словосочетаний, жаргонных выражений и т.п. Подобные программы позволяют осуществлять сканирование текстов на разных языках[3].

---

[1]Официальный сайт https://www.harmonyos.com/

[2]Конечно, и в некоторых других странах осуществляется блокирование отдельных ресурсов киберпространства, но по масштабу этой деятельности, её комплексности, Китай далеко опережает другие государства.

[3]*Van Hee C, Jacobs G, Emmery C, Desmet B, Lefever E, Verhoeven B.* et al. (2018) Automatic detection of cyberbullying in social media text // PLoS ONE 13(10): e0203794. https://doi.org/10.1371/journal.pone.0203794. URL: https://doi.org/10.1371/journal.pone.0203794

Важное значение в обеспечении безопасности несовершеннолетних в киберпространстве, по мнению зарубежных учёных, отводится развитию средств родительского контроля, т.е. комплекса программных средств, позволяющих родителям контролировать поведение детей в киберпространстве: исключать возможность просмотра ими порнографии, сайтов, рекламирующих потребление наркотиков, насилие и т.п., контролировать контакты в соцсетях, переписку, время пребывания в киберпространстве и т.п. Для осуществления такого контроля разрабатываются специальные программные комплексы[1].

В целях борьбы с кибернасилием (кибербуллингом) в отношении несовершеннолетних, в странах Евросоюза развиваются национальные программы, предусматривающие комплекс организационных, технических и правовых средств предотвращения подобных преступлений[2].

Как отмечают О.Ю.Ситкова и Л.В. Шварц, проанализировавшие меры по защите детей в киберпространстве, предпринимаемые зарубежными странами, родительский контроль более эффективен в развитых странах, где и старшее и младшее поколение являются уверенными пользователями компьютеров. В тех же странах, где уровень компьютерной грамотности родителей низок, наблюдается значительное число случаев кибербуллинга[3].

Таким образом, можно сделать вывод о том, что повышение компьютерной грамотности населения рассматривается как эффективное

(дата обращения: 12.08.2021); *Hussain M.G.* An Approach to Detect Abusive Bangla // International Conference on Innovation in Engineering and Technology (ICIET). Dhaka, Bangladesh, 2018. P.1-5.

[1]*Fire M.* Online Social Networks: Threats and Solutions // IEEE Communications Surveys & Tutorials. 2014. Vol. 16. No 4. P. 2019-2036.

[2]См., напр.: Решение № 1351/2008/ЕС Европейского парламента и Совета Европейского Союза «О создании многолетней программы Сообщества о защите детей при использовании Интернета и других коммуникационных технологий» // СПС «КонсультантПлюс».

[3]*Ситкова О.Ю., Шварц Л.В.* Современное состояние зарубежных научных исследований о безопасности детей в информационно-коммуникационной среде // Правовая политика и правовая жизнь. 2020. № 2. С. 82.

средство снижения риска виктимизации пользователей в киберпространстве.

Как отмечают указанные ранее авторы, фильтрация информации на основе чёрных списков (практикуемая и в Российской Федерации) на западе практикуется, но не рассматривается в качестве эффективного средства предотвращения доступа несовершеннолетних к нежелательной информации, поскольку в принципе не способна решить такую задачу в полном объёме. Поэтому акцент делается на взаимодействии педагогов, родителей, правоохранительных органов и работе с детьми обучению детей и родителей правилам безопасного поведения в киберпространстве, основам компьютерной грамотности[1].

Особый интерес для нас представляет опыт США. Эта страна уникальна тем, что именно в США были впервые созданы персональные компьютеры[2], сеть Интернет[3], основные операционные системы для компьютеров – Microsoft Windows для персональных компьютеров, IOS и Android – для смартфонов и планшетов. В США впервые был созданы центральные процессоры для компьютеров. Крупнейшие поисковые системы и социальные сети Google и Facebook, – также появились в США. Крупнейшие медиасервисы и мессенджеры, такие, например, как Youtube, Twitter, WhatsApp – также имеют американское происхождение.

США сохраняют за собой монопольный контроль над «Корпорацией по управлению доменными именами и IP-адресами» (ICAAN) несмотря на то, что формально эта организация является независимой[4]. Это организация занимается распределением доменных имён, лежащих в основе адресации сайтов в Интернете, что позволяет США во многом определять стандарты

---

[1]Там же.

[2]*Хромой Б.П.* История развития вычислительной техники и связи // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 3. С. 82.

[3]*Василенко А.И.* История зарождения интернета и основные пути его развития // Новая наука: Опыт, традиции, инновации. 2016. № 3-2 (71). С. 165.

[4]*Роговский Е.А.* Политика США по обеспечению безопасности киберпространства // США и Канада: экономика, политика, культура. 2012. № 6. С. 15.

безопасности киберпространства, правила пользования доменными именами, воздействовать на политику других государств в данной сфере.

В силу этого правительство США и правоохранительные органы обладают уникальными технологическими возможностями по контролю за информацией.

Крупнейшие технологические компании США активно работают с американскими спецслужбами, передавая им сведения, составляющие тайну личной жизни не только американцев, но и жителей других стран. В этом числе Google, FaceBook, Amazon, Apple, которые принимают участие в операциях США, направленных на свержение законных правительств в других странах (в том числе, и в России)[1]. Однако не так широко известно, что большинство из крупнейших мировых IT-компаний создано с подачи и при участии спецслужб США, контакты между ними не прерываются[2]. Поэтому США обладают несравнимыми с другими государствами возможностями по обеспечению кибербезопасности граждан и пресечению киберпреступлений.

Значима помощь технологических компаний и в предотвращении общеуголовных преступлений. Например, компания Google обладает огромными массивами информации не только о персональных данных граждан, но и об их контактах и о местонахождении в определённые периоды времени, что активно используется для выявления преступников[3].

Компания Apple планирует в своей операционной системе iOS 15 внедрение технологий искусственного интеллекта для обнаружения на телефонах пользователей фотографий со сценами насилия над детьми и ограничения поиска запрещённого контента. В случае обнаружения

---

[1] *Ахмед Н.* Как ЦРУ создавало Google. URL: https://d-russia.ru/kak-cru-sozdavalo-google.html (дата обращения: 16.08.2021); *Никифорова Н.* «Фейсбук» – проект ЦРУ… Но разве в этом кто-нибудь сомневается? // Взгляд. 2016. 27 авг.

[2] Левин Я. Интернет как оружие. Что скрывают Google, Tor и ЦРУ / пер. Леонович М., Напреенко Е. М.: Individuum, 2019. С. 50-55.

[3] Google передает американским правоохранителям данные о пользователях, находившихся рядом с местами преступлений. URL: https://www.newsru.com/hitech/16apr2019/google_data.html (дата обращения: 14.08.2021).

подозрительных изображений, они автоматически будут перенаправляться в правоохранительные органы[1].

Крупнейшая социальная сеть на планете – Facebook с 2016 г. внедрила систему фильтрации размещаемой пользователями информации, основанную на искусственном интеллекте. Уже реализовано автоматическое выявление сцен с обнажёнными людьми, насилием в фото- и видеоматериалах[2].

Примеры подобного рода можно продолжать и далее. Однако, полагаем, их достаточно для того, чтобы сделать вывод о складывающихся тенденциях в сфере защиты личности: для США методы, применяемые в других государствах, такие как блокирование информационных ресурсов, не актуальны, поскольку это государство обладает практически исчерпывающей информацией о пользователях киберпространства и исключительными возможностями по пресечению киберпреступлений. Правоохранительные органы США смогли даже идентифицировать и арестовать владельца сайта Silk Road Росса Уильяма Ульбрихта. Данный сайт действовал в сети TOR, которая считалась до определённого времени недоступной для государственного контроля. Впоследствии задерживались и другие преступники, пытавшиеся возобновить работу этого сайта в сети TOR[3].

В 2018 г. в США была принята новая стратегия безопасности в киберпространстве. Используемые в документе формулировки носят характер скорее не правоохранительный, а военный. В документе сформулированы основные цели государства в этой сфере: укрепление национальной безопасности; создание безопасной цифровой экономики, развитие инноваций;

---

[1] *Кузнецов И.* Apple подтвердила, что будет проверять наши фото. А ещё сообщения и поисковые запросы. URL: https://appleinsider.ru/eto-interesno/apple-podtverdila-chto-budet-proveryat-nashi-foto-a-eshhyo-soobshheniya-i-poiskovye-zaprosy.html (дата обращения: 14.08.2021).

[2] *Березина Е.* Facebook будет автоматически блокировать нежелательную информацию. URL: https://rg.ru/2016/12/02/facebook-budet-avtomaticheski-blokirovat-nezhelatelnuiu-informaciiu.html (дата обращения: 14.08.2021).

[3] *Степанов В.* Великий колесный путь Власти США закрыли интернет-магазин наркотиков Silk Road. URL: https://lenta.ru/articles/2013/10/03/silkroad/ (дата обращения: 16.08.2021).

укрепление способности США и их партнёров предотвращать кибератаки и наказывать агрессоров; наращивание американского влияния за пределами страны и расширение зоны открытого и надёжного интернета[1].

В документе обращает на себя внимание то, что США занимают не оборонительную, а активную наступательную позицию, навязывая свои представления о свободе информации другим странам и размывая их способности контролировать собственное киберпространство. В качестве инструментов для этого называется развитие системы спутникового интернета, доступ к которому может осуществляться в любой точке планеты в обход национальных провайдеров.

Другим способом доминирования является навязывание собственной идеологии, видения мира путём продвижения и поддержки образовательных проектов. В доктрине называются два проекта – Википедия и «Академия Хана», финансирование которых должно осуществляться правительством США или американскими корпорациями.

Проект Википедия первоначально позиционировался как свободная энциклопедия, независимая от какого-либо идеологического влияния, не имеющая «хозяев». Информационная насыщенность ресурса сделала его одним из самых популярных в русскоязычном сегменте Интернета. Ответы из Википедии часто попадают в первые строки поисковой выдачи во всех поисковых системах (Яндекс, Google), что означает, что для подавляющего большинства наших пользователей информация, выдаваемая Википедией, и будет восприниматься как правильный ответ на заданный вопрос. И, скорее всего, ответы, размещаемые на последующих строках или страницах в поисковых выдачах, никогда не будут прочитаны.

Таким образом, этот информационный ресурс обладает огромным общественно-политическим влиянием в нашей стране.

---

[1]Явная виртуальная угроза. URL: https://www.rbc.ru/newspaper/2018/09/24/5ba4d2459a79475744112262 (дата обращения: 15.08.2021).

Между тем, фактическое состояние дел не позволяет считать этот ресурс действительно объективным. В настоящее время политика сайта такова, что из числа источников цитирования к статьям исключён ряд российских ресурсов, не пропускается информация, дискредитирующая представителей отдельных оппозиционных групп, поддерживаемых из-за рубежа, удаляется информация о позитивной деятельности органов государственной власти и отдельных политиков и т.п.[1]

Таким образом, политика США в сфере киберпространства направлена на формирование в мире и в самих США позитивного образа этого государства и негативное освещение истории и современной политики стран, не находящихся в зависимых от США отношениях.[2]

С криминологической точки зрения, навязывание одного мнения (пусть и не всегда корректного) снижает уровень скептицизма граждан по отношению к государству и препятствует развитию экстремистских проявлений, вовлечению населения в противоправную деятельность, повышает уровень лояльности политической власти.

Те же задачи решает и образовательный портал «Академия Хана»[3], который представляет на безвозмездной основе доступ к обучающим материалам по самым разным дисциплинам, охватывая как курс средней школы, так и многие дисциплины высших учебных заведений. Данный ресурс решает с точки зрения важную задачу – он, во-первых, формирует образовательный стандарт, единое представление о различных аспектах истории, исторического процесса, состояния современного общества, а, во-вторых, позволяет детям самого разного имущественного положения получать

---

[1] *Игнатов Г.* 20 лет Википедии: как российская Вики превратилась в рассадник лжи и русофобии. URL: https://jpgazeta.ru/20-let-vikipedii-kak-rossijskaya-viki-prevratilas-v-rassadnik-lzhi-i-rusofobii/ (дата обращения: 15.08.2021).

[2] *Родина Е.А.* Общесоциальная профилактика криминогенной виктимизации пользователей сети Интернет // Вестник Саратовской государственной юридической академии. 2022. № 3. С. 200.

[3] Русскоязычная версия сайта доступна по адресу https://ru.khanacademy.org/

доступ к качественным учебным материалам.

С криминологической точки зрения развитие подобных ресурсов играет важную роль в повышении культурного уровня населения, особенно – детей, формирует у них мировоззрение, представление о современном обществе и его механизмах. Отметим, что в России бесплатных образовательных сайтов такого уровня и насыщенности учебной информацией до настоящего времени не создано.

Ещё одной интересной особенностью защиты пользователей в США является высокая степень защищённости пользователей платежных карт. В этой стране действует нормативный акт The Fair Credit Billing Act (FCBA). В соответствии с положениями этого закона пользователи имеют 60 дневный срок для уведомления операторов о незаконной транзакции (например, снятии денег с карты без ведома владельца). При этом клиент, чтобы получить деньги обратно, обязан лишь заявить, что не осуществлял денежного перевода и предъявить кредитную карту (что является доказательством того, что он не передавал её третьим лицам). Максимальные потери для клиента имеют место лишь, если он сам лично передал платёжную карту третьим лицам. В таком случае он выплачивает штраф 50 долларов.[1]

В дальнейшем банки самостоятельно осуществляют розыск мошенников, располагая материальными ресурсами для привлечения частных детективов, специалистов в области интернет-технологий и т.п.

Подобная ситуация свидетельствует о том, что пользователи платежных карт, совершая покупки в интернете в значительной степени застрахованы от мошеннических действий.

Проведённый анализ позволяет нам сделать следующие выводы:

1. Высокий уровень защищённости личности обеспечивает цифровой суверенитет, т.е. способность государства реализовывать и

[1]Lost or Stolen Credit, ATM, and Debit Cards. URL: https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards (дата обращения: 28.12.2020).

контролировать весь спектр технологий, лежащих в основе функционирования киберпространства.

2. Меры защиты должны носить комплексный характер, сочетая программно-технические средства и способы и нормативное регулирование;
3. Запретительные меры (блокирование информации) обладают меньшей эффективностью, но их применение оправдано недостаточной технологической развитостью государства (отсутствием полноценного цифрового суверенитета).
4. Повышение эффективности защиты граждан связано с определёнными ограничениями в сфере свободы слова, свободы информации, тайны частной жизни. В настоящее время наблюдается повсеместное наступление государств на эти базовые ценности.
5. Важное значение имеет 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.

§ 2. Общесоциальная профилактика криминогенной виктимизации пользователей сети «Интернет» в киберпространстве

Основной целью криминологических исследований всегда выступает конструирование мер, направленных на недопущение в будущем преступности, отдельных видов преступлений на основе полученных данных об особенностях отдельных видов преступлений. В теории данное положение является общепринятым и не вызывает существенных возражений. Однако единого терминологического аппарата, отражающего деятельность по недопущению преступлений, до настоящего времени не выработано. В различных работах

используются термины «превенция», «борьба с преступностью», «контроль над преступностью», «предупреждение», «профилактика» и т.п.[1], иногда их употребляют в качестве синонимов[2], однако общепринято выделять последние два – «предупреждение» и «профилактику».

В настоящее время часть споров о соотношении этих понятий снята с принятием федерального закона РФ «Об основах системы профилактики правонарушений в Российской Федерации»[3], в п. 2 ст. 2 которого даётся следующее определение: «профилактика правонарушений – совокупность мер социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений или антиобщественного поведения».

Нам представляется логичной следующая позиция относительно соотношений этих понятий: профилактика – это часть системы предупреждения преступлений. В свою очередь предупреждение помимо профилактики включает в себя также пресечение преступлений[4]. При таком подходе не возникает ситуации со смешением понятий «виктимологическая профилактика» и «пресечение преступлений», допускаемых иногда в литературе[5].

Содержание виктимологической профилактики Д.В. Ривман определяет так: «… включённая в социальную систему предупреждения преступлений подсистема общесоциальных и специально-криминологических мер,

---

[1] *Варыгин А.Н., Громов В.Г., Шляпникова О.В.* Основы криминологии и профилактики преступлений. М.: Юрайт, 2019. С. 115-116.

[2] *Гилинский Я.И.* Криминология: теория, история, эмпирическая база и социальный контроль. СПб: Алеф-Пресс, 2014. С. 513.

[3] Федеральный закон от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // СЗ РФ. 2016. № 26 (ч. I), ст. 3851.

[4] *Аванесов Г.А.* Криминология. М., 1984. С. 333–335.

[5] *Горшенков Г.Н.* Криминология. Введение в учебный курс. Сыктывкар, 1995. С. 140.

направленных на снижение индивидуальной и массовой виктимности посредством устранения негативных виктимных предрасположений, активизации защитных возможностей потенциальных жертв преступлений и обеспечения их безопасности»[1]. Сходным образом определяют её и другие авторы[2]. В принципе, такое определение нас вполне устраивает, поскольку оно в целом отражает содержание этого термина и его соотношение с базовым понятием «предупреждение преступлений».

Определённые возражения вызывает лишь определение объекта виктимологической профилактики, под которым Д.В. Ривман понимает лиц с противоправным или аморальным поведением, а также факторы, которые обусловливают виктимность, порождаемую соответствующим поведением жертв преступлений[3].

Дело в том, что, как было показано ранее, для виктимизации в киберпространстве аморальное или противоправное поведение является необязательным признаком и характерно лишь для отдельных видов посягательств, таких, как насильственные действия, спровоцированные оскорблениями в социальных сетях, размещением своих личных данных и вступлением в контакт с неизвестными людьми в соцсетях, повлекшие посягательства на сексуальной почве и ряда других.

Если рассматривать наиболее распространенные преступления, а именно мошенничества, то, как правило, причины виктимности связаны с компьютерной неграмотностью, занятостью, повлекшей неспособность сконцентрироваться на обеспечении собственной безопасности и т.п.

Таким образом, в большинстве случаев жертвы киберпреступлений

---

[1] *Ривман Д.В.* Криминальная виктимология. СПб.: Питер, 2002. С. 241.

[2] *Алексеев А.И., Герасимов С.И., Сухарев А.Я.* Криминологическая профилактика: теория, опыт, проблемы. М.: Норма, 2001. С. 108; *Майоров Л.В.* Концептуальные основы виктимологического противодействия преступности. Челябинск: Изд. центр ЮУрГУ, 2013. С. 143; *Полубинский В.И.* Фундаментальные и прикладные начала криминальной виктимологии. М.: Изд-во ВНИИ МВД России, 2010. С. 173 и др.

[3] *Ривман Д.В.* Указ. соч. С. 241.

совершают поступки, провоцирующие совершение преступлений в отношении них, которые нельзя охарактеризовать как аморальные или противоправные.

Для того чтобы определить объекты виктимологической профилактики, необходимо определиться с её видами. В криминологии предупреждение в зависимости от охвата степени его охвата выделяют три его вида (или иногда говорят об уровнях предупреждения): общесоциальное, специальное и индивидуальное[1].

Общесоциальное предупреждение – система мер наиболее общего характера, направленных на совершенствование общественных отношений и устранение наиболее общих причин преступности. Специальное (или специально-криминологическое) предупреждение представляет собой меры, направленные на устранение причин и условий отдельных видов преступлений, а индивидуальный уровень предупреждения образуют меры, направленные на недопущение преступления со стороны отдельных лиц[2].

Полагаем, что такая же классификация допустима и для мер виктимологической профилактики. Изучение личности жертв киберпреступлений демонстрирует, что независимо от вида совершенных в отношении них посягательств имеются характерные черты, свойственные большинству из них. В то же время наблюдается и специфика жертв отдельных видов преступлений. Поэтому склонны согласиться с авторами, которые и для виктимологической профилактики выделяют три её уровня – общесоциальный, специальный и индивидуальный[3].

Исходя из такой классификации, можно определить и объекты

---

[1]Криминология: учебник для вузов / под общ. ред. А.И. Долговой. 3-е изд., перераб. и доп. М., 2007. С. 442; Криминология: учебник / под ред. Н.Ф. Кузнецовой, В.В. Лунеева. 2-е изд., перераб. и доп. М., 2004. С. 194–195; Криминология: учебник / под ред. В.Н. Кудрявцева, В.Е. Эминова. 3-е изд., перераб. и доп. М., 2005. С. 271, 280 и др.

[2]См., напр.: Криминология: учебник для ВУЗов / под ред. В.Д. Малкова. М.: ЗАО «Юстицинформ», 2006. С. 120-124.

[3]*Бойко О.А., Хоменко А.Н., Пестерева Ю.С., Бражников В.В.* Актуальные проблемы виктимологии: учебное пособие. Омск: Омская юридическая академия, 2017. С. 104; *Савиных Е.В.* Основные направления и проблемы виктимологической профилактики преступности // Виктимология. 2014. № 1. С. 51.

виктимологической профилактики. Примерный объем и содержание мер общего предупреждения очерчены в ч. 1 ст. 15 Закона РФ «Об основах системы профилактики правонарушений в РФ» и включают в себя выявление и устранение причин, порождающих правонарушения, и условий, способствующих их совершению, или облегчающих их совершение, повышение правовой грамотности граждан и развитие их правосознания.

С учётом этого можно определить содержание общей виктимологической профилактики как устранение наиболее общих причин и условий, порождающих виктимизацию граждан, повышение их правовой грамотности и развития их правосознания, информирования о направлениях повышения собственной безопасности.

Прежде всего, при конструировании комплекса мер общей виктимологической профилактики в киберпространстве нужно обратиться к вещам, которые, казалось бы, не имеют прямого отношения к теме настоящего исследования. Характеризуя меры обеспечения безопасности в киберпространстве, предпринимаемые иностранными государствами, следует отметить, что очень большое внимание (например, в США) уделяется формированию позитивного восприятия государства, целостного представления об истории, экономике и культуре путём создания и поддержки крупнейших информационных и образовательных ресурсов, таких как Википедия.

Значение таких общепризнанных источников знаний с точки зрения виктимологической профилактики весьма велико, так как они концентрируют не только энциклопедическую информацию, но и актуальные данные о политических событиях, тенденциях развития общества и государства, правовых вопросах, формируют единое культурное пространство и, тем самым, решают задачи общего предупреждения. Как отмечалось ранее, к сожалению, Википедия нацелена на продвижение американских представлений и ценностей, что способствует формированию скептического отношения граждан

России к собственному государству, деформирует правосознание и порождает недоверие к правительству, правовой нигилизм.

Следует признать, что в Российской Федерации на государственном уровне имеется понимание этой проблемы и предлагаются меры по созданию информационных ресурсов, которые смогли бы заместить в отечественном информационном пространстве Википедию и ей подобные сайты. В частности, в 2016 г. было издано распоряжение Правительства РФ о создании на основе электронной версии Большой российской энциклопедии общенационального научно-образовательного интерактивного портала[1], которое в настоящее время утратило свою силу.

Однако уже на момент опубликования этого распоряжения появились аналитические материалы, демонстрирующие, что огромные затраты (два миллиарда рублей в ценах 2016 г.[2]), которые планировалось выделить на создание такого портала, не дадут эффекта[3].

В качестве причин называлось неоправданное завышение бюджета, но, главное, – непонимание чиновниками того, как работают эффективные интернет-проекты. Если посмотреть Википедию, или популярные отечественные информационные ресурсы, то обращает на себя внимание, что они, прежде всего, создаются группами энтузиастов, которые тонко чувствуют обратную связь с обществом, его информационными потребностями, не связаны административными ограничениями. Во многих проектах (например, в Циклопедии, Руксперте, Викиреальности и т.п.) любой человек, интересующийся определенной темой, может быть автором соответствующей статьи. Таким образом создавался и проект Википедия, на начальных стадиях

[1]Распоряжение Правительства РФ от 25 августа 2016 г. № 1791-р. URL: http://publication.pravo.gov.ru/Document/View/0001201608290013?index=0&rangeSize=1 (дата обращения: 17.08.2021).

[2]Россия потратит два миллиарда рублей на аналог «Википедии». URL: https://lenta.ru/news/2019/09/26/wikipedia/ (дата обращения: 17.08.2021).

[3]Почему отечественная «Википедия» не взлетит. URL: https://cont.ws/@fritzmorgen/1463112 (дата обращения: 17.08.2021).

которого к авторству допускались все желающие, что приводило к быстрому наполнению базы данных при минимуме финансовых затрат. А затем, в процессе отбора, формировалось достаточно устойчивое сообщество специалистов во всех отраслях знаний, способное на высоком уровне наполнять и поддерживать эти ресурсы.

В нашем же случае имеет место максимально неэффективный подход, при котором чиновники полагают, что любую проблему можно решить денежными вливаниями. Однако практика показывает, что этот подход в киберпространстве не срабатывает. Бюрократический аппарат не способен быстро реагировать и пополнять базы знаний в соответствии с меняющейся политической и экономической обстановкой. Он ограничен регламентами, бюджетом и, прямо скажем, идеологически. Современное Российское государство, несмотря на отказ от официальной идеологии, тем не менее, остается весьма нетерпимым к позитивным оценкам недавнего советского прошлого, к левым идеям и т.п.[1] Эта жесткость и не позволяет создавать общепризнанные информационные ресурсы, опираться на группы энтузиастов для их создания. Такая ситуация, например, имела место с продвижением отечественной поисковой системы «Спутник», на которую также выделялось бюджетное финансирование. Идея создания национальной поисковой системы появилась после конфликта с Грузией в 2008 г., когда Российское государство столкнулось с негативной оценкой своих действий на отечественных же новостных сайтах[2].

В настоящее время этот проект закрыт, а компания ООО «Спутник»

---

[1]В этом смысле весьма показательна ситуация с отечественным кино. Финансируемые Министерством культуры РФ дорогостоящие фильмы о войне, в негативном свете демонстрирующие советское наследие, в прокате массово не окупаются. В то же время небольшие любительские проекты, привлекающие средства путем сбора пожертвований, востребованы в прокате.

[2]Национальный поисковик «Спутник» запустят до конца весны. URL: https://www.forbes.ru/news/255639-natsionalnyi-poiskovik-sputnik-zapustyat-do-kontsa-vesny (дата обращения: 17.08.2021).

признана банкротом[1].

Нам представляется, что выход из сложившегося тупика все-таки есть. Для этого необходимо наладить точечное финансирование информационных проектов патриотической направленности, образовательных сайтов, создаваемых и развиваемых энтузиастами или отдельными компаниями, с условием обеспечения бесплатного доступа всех желающих, либо радикального снижения расценок.

Важным условием успеха в развитии таких ресурсов аналитики наказывают освещение тем, которые Википедия не рассматривает по различным соображениям (например, об успехах современной отечественной промышленности, как это делается на сайте Рукспект), либо изложение материалов, которые на Википедии подаются односторонне или тенденциозно, с точки зрения обеспечения национальных интересов[2].

Кроме того, государство должно стимулировать перенос медиаинформации на отечественные ресурсы. В настоящее время отечественный аналог видеосервиса Youtube, находящийся по адресу https://rutube.ru, нацелен, в основном на развлечения, тогда как Youtube предлагает огромное количество образовательных и просветительских материалов. В период карантина, вызванного короновирусной инфекцией, множество образовательных учреждений выкладывали свои материалы по инерции на западный сервис, абсолютно игнорируя возможность использования отечественного ресурса. Этот перекос должен быть устранен. От государства даже не потребуется каких-то материальных затрат. На наш взгляд, миграции на rutube вполне могла бы способствовать воля государственных учреждений. Например, рекомендаций Министерства образования по переносу

[1]Определение арбитражного суда г. Москвы от 20 мая 2019 г. № А40-35771/18-71-46Б. URL: https://kad.arbitr.ru/Document/Pdf/296a7187-edad-4920-acf0-6fedb0a95482/f1f8baf6-4ca6-448e-a231-368566f75c06/A40-35771-2018_20190520_Opredelenie.pdf?isAddStamp=True (дата обращения: 17.08.2021).

[2]Почему отечественная «Википедия» не взлетит. URL: https://cont.ws/@fritzmorgen/1463112 (дата обращения: 17.08.2021).

учебных и образовательных программ на rutube было бы вполне достаточно. Это не вызвало бы затрат и для создателей соответствующей медиапродукции – преподавателей и учителей. Материальным стимулом для лучших создателей контента могли бы стать отчисления от рекламы, как это сделано на Youtube.

Аналогичная ситуация и с другими сервисами. Например, при наличии отечественного программного обеспечения TrueConf подавляющее большинство учебных заведений пользовались в период карантинных мероприятий западными программами Zoom, WhatsApp и т.п. Стоит добавить, что западной связью пользовались не только образовательные учреждения, но и управленческие органы, что представляется недопустимым с точки зрения обеспечения национальной безопасности. В печати появлялись сообщения, что сведения о перемещении первых лиц государства по г. Москва, передавались сотрудниками ГИБДД, обеспечивающими безопасность их проезда, посредством мессенджера WhatsApp в течение трех лет[1]. Такая ситуация представляется категорически недопустимой.

Таким образом, со стороны государства создание отечественных аналогов западных сервисов не потребует значительных затрат. Необходимо лишь рекомендовать всем государственным организациям использовать в качестве программного обеспечения отечественные аналоги западных продуктов. Естественно, такой переход не может быть гладким и будет сопровождаться определенными техническими и организационными проблемами, но этот период становления проходят все организации и необходима лишь воля государства и поддержка отечественных производителей программного обеспечения.

В развитие сказанного следует дополнить, что комплексное развитие безопасности граждан в киберпространстве невозможно в отсутствие информационного (или иногда говорят – цифрового суверенитета), т.е.

[1]Би-би-си узнала о передаче маршрутов первых лиц России через WhatsApp. URL: https://www.rbc.ru/politics/31/12/2020/5fedf4ad9a79470caa864a2f (дата обращения: 17.08.2021).

способности государства самостоятельно формировать, обеспечивать безопасное функционирование национального сегмента киберпространства[1].

Основой цифрового суверенитета выступает способность производить все компоненты вычислительной техники, формирующие техническую основу функционирования киберпространства. Сюда входит производство компьютеров и их комплектующих (процессоров, памяти, маршрутизаторов, систем хранения данных и т.п.), наличие национальных операционных систем, национального программного обеспечения, позволяющего реализовывать необходимую для пользователей функциональность, систем обеспечения безопасности в киберпространстве и т.д.

По нашим оценкам в полной мере цифровым суверенитетом обладают в полной мере две страны – США и Китай. Россия в настоящее время приближается к его достижению. У нас разрабатывается и используется ряд операционных систем на базе Linux, операционная система для мобильных устройств Аврора, несколько типов центральных процессоров для компьютеров (семейства Байкал и Эльбрус), отдельные компоненты систем хранения данных, программы для обеспечения безопасности, офисные пакеты, игры и т.д.

Однако о полноценном цифровом суверенитете говорить пока рано. В России до настоящего времени нет собственных фабрик, позволяющих выпускать компоненты персональных компьютеров по современным технологическим процессам, не производятся отдельные компоненты персональных компьютеров, в т.ч. такие важные как оперативная память и видеоускорители.

Неясна ситуация с национальной принадлежностью отдельных интернет-сервисов. Например, поисковая система «Яндекс», которая считается

[1]Подробнее о цифровом суверенитете см., напр.: *Бухарин В.В.* Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. 2016. № 6(51). С. 76.

формально отечественной, зарегистрирована в Нидерландах[1].

Поэтому важным компонентом обеспечения безопасности в киберпространстве является построение современной национальной полупроводниковой индустрии и обеспечение перехода на национальное программное обеспечение, начиная с государственных учреждений, и переноса всех цифровых компаний отечественного происхождения в отечественную юрисдикцию.

Нами ранее было установлено, что одним из факторов виктимизации в киберпространстве выступает недостаточная компьютерная грамотность пользователей. Парадоксально, но параллельно с повсеместным распространением компьютеров, планшетов и смартфонов, средний уровень компьютерной грамотности понижается[2].

На наш взгляд, это объясняется тем, что современные операционные системы позволяют осуществлять базовые функции (доступ к интернету, написание и отправка сообщений, изготовление фотографий и видеозаписей) даже начинающим. Поэтому средний пользователь современного технологичного устройства не испытывает потребности и не имеет мотивации к изучению отдельных технических аспектов функционирования компьютерных устройств и сетей.

С учётом этого полагаем изменить вектор развития компьютерной грамотности таким образом, чтобы акцент сделать не на использовании базового пакета программ (хотя и это должно входить в курс обучения), но и на технические аспекты функционирования компьютерных сетей. Пользователь, как минимум, должен понимать, что такое адрес сайта в Интернете, как он отображается в различных программах (например, в браузерах). Как выглядят

---

[1] *Русанова И.* Кому принадлежит Яндекс. URL: https://brobank.ru/komu-prinadlezhit-yandex/ (дата обращения: 17.08.2021).

[2] См., напр.: *Хвостик Е.* Бедность и низкая компьютерная грамотность тормозят развитие интернета // Коммерсант. 2019. 5 ноября; Skills Matter: Further Results from the Survey of Adult Skills, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/9789264258051-en.

интернет-адреса основных ресурсов сети, которыми он пользуется, как отличить – когда в адресной строке присутствует ссылка на официальный ресурс, и как выглядят ссылки на поддельные сайты (например, при фишинге).

Кроме того, курсы компьютерной грамотности должны уделять внимание и базовым аспектам безопасного поведения в киберпространстве. Пользователей необходимо ориентировать на сохранение в тайне своей персональной информации, отказ от передачи её третьим лицам, воздержание от посещения подозрительных ресурсов в сети, от случайных знакомств в интернете и, ещё более важное, осторожности при переносе этих контактов из киберпространства в реальный мир.

Важное значение имеет развитие навыков общения в социальных сетях, мессенджерах. Пользователи должны понимать, какая форма обращения к собеседникам допустима и не вызывает отторжения, а какие выражения, слова могут быть интерпретированы как оскорбление, пренебрежение, высокомерие.

Еще одним элементом психологической подготовки пользователя является отказ от посторонних контактов, звонков, бесед с посторонними во время занятости. Современные гаджеты позволяют постоянно быть на связи, что, с одной стороны, является огромным преимуществом, но, с другой, как было показано ранее, способствует виктимизации пользователей, повышает их уязвимость к мошенническим действиям. Поэтому культура поведения в киберпространстве должна включать в себя выработку навыков отказа от контактов с третьими лицами в период высокой загруженности.

Ранее уже говорилось о проблемах российского кинематографа[1]. Очернение советской действительности, имеющее место, свидетельствует о том, что наше общество расколото идеологически. Примером такого раскола является установка в Санкт-Петербурге мемориальной доски генералу Маннергейму, который до 1918 г. служил в русской армии, однако

[1]У каждого была своя правда. Сергей Иванов открыл мемориальную доску в честь Карла Маннергейма // Рос. газета. 2016. 16 июня.

впоследствии воевал против СССР на стороне фашистской Германии[1]. Данное мероприятие представляется особенно двусмысленным в свете того, что финские войска под руководством Маннергейма в период Великой Отечественной Войны оказывали содействие немецкой армии в блокаде Ленинграда, повлёкшей гибель нескольких сот тысяч жителей города (по некоторым оценкам эта цифра доходит до 1,5 млн человек).

Сходная история имела место с попытками реабилитации в общественном сознании личности предателей Родины генерала Власова[2], Шкуро[3] воевавших на стороне фашистской Германии и т.д. и т.п.

В подобной ситуации у российского народа нет не только единой картины будущего, которое он должен формировать, но и единых представлений о прошлом. Подрастающее поколение перестает интересоваться политической и общественной жизнью в стране, поскольку в фильмах демонстрируется одна история нашей страны, а от родителей, бабушек и дедушек они слышат часто нечто диаметрально противоположенное. Неудивительно, что на почве такого двоемыслия возникает недоверие к государству и уход молодых людей в маргинальные, антиобщественные или экстремистские сообщества.

Поэтому 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. По нашему мнению, государство может и обязано подвергать государственной цензуре на предмет соответствия исторической

---

[1]О финансировании государством низкпробных фильмов см. также *Дикарев В.* Цветы, которые нам не нравятся. URL: https://craftkino.ru/sostojanie-rossiyskogo-kino/ (дата обращения: 17.08.2021).

[2]Ельцин-центр потребовал реабилитации власовцев, назвав их «диссидентами 40-х годов». URL: https://www.rline.tv/news/2016-12-15-eltsin-tsentr-potreboval-reabilitatsii-vlasovtsev-nazvav-ikh-dissidentami-40-kh-godov/ (дата обращения: 17.08.2021).

[3]*Черных Е.* Воронежский след атамана Шкуро. URL: https://infovoronezh.ru/News/Voronejskiy-sled-atamana-SHkuro-9876.html (дата обращения: 17.08.2021).

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.[1]

С учетом изложенного можно предложить следующие меры общей профилактики криминальной виктимизации пользователей сети «Интернет» в киберпространстве:

1. Поддержка государственным финансированием наиболее успешных информационных проектов патриотической направленности и образовательных сайтов с условием бесплатного доступа для всех желающих либо радикального снижения расценок.

2. Министерствам просвещения, образования и науки, министерствам образования субъектов РФ необходимо стимулировать перенос обучающих видеоматериалов, которые готовятся преподавателями учебных заведений на российские аналоги западных видеосервисов.

3. 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.

4. Важным компонентом обеспечения безопасности в киберпространстве является наличие цифрового суверенитета, т. е. способности государства самостоятельно формировать, обеспечивать безопасное функционирование национального сегмента киберпространства. Для этого необходимы: построение современной национальной полупроводниковой индустрии, переход государственных и образовательных учреждений на национальное программное обеспечение, перенос деятельности всех цифровых компаний

[1] *Родина Е.А.* Общесоциальная профилактика криминогенной виктимизации пользователей сети Интернет // Вестник Саратовской государственной юридической академии. 2022. № 3. С. 205.

отечественного происхождения в отечественную юрисдикцию.

5. При подготовке пользователей необходимо изменить вектор развития компьютерной грамотности и делать акцент на изучении технических особенностей функционирования компьютерных сетей, базовых аспектах безопасного поведения в киберпространстве.

6. 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.

§ 3. Меры специальной виктимологической профилактики

В криминологической литературе специальный уровень виктимологической профилактики связывается с осуществлением мероприятий, направленных на недопущение реализации виктимных свойств и качеств отдельных групп населения[1]. С учётом того, что жертвы отдельных видов посягательств обладают сходными признаками, можно говорить о том, что объектами специальной виктимологической профилактики должны выступать не только представители отдельных групп населения, но и группы лиц, которые по своим отличительным признакам способны стать жертвами определённых преступлений.

Проанкетированные нами специалисты в своём большинстве

[1] *Бойко О.А., Хоменко А.Н., Пестерева Ю.С., Бражников В.В.* Актуальные проблемы виктимологии: учебное пособие. Омск: Омская юридическая академия, 2017. С. 104-105.

придерживаются оптимистического взгляда, в соответствии с которым граждане могут избегать совершения в отношении них преступлений в киберпространстве при условии соблюдения мер безопасности.

Анализируя причинный комплекс виктимизации в киберпространстве, в качестве одной из причин указывалась анонимность пользователей, которая выступает не только в качестве побочного эффекта использования обезличенных средств связи посредством компьютеров, но и выполняет важные функции в киберпространстве. В частности, с виктимологической точки зрения анонимность можно рассматривать как средство обеспечения безопасности личности в киберпространстве. Однако, как и всякое другое явление, она имеет не только положительные, но и отрицательные свойства. При этом возникает противоречие, при котором анонимность и шифрование данных являются, с одной стороны, неотъемлемыми правами личности, позволяющими в цифровую эпоху свободно высказывать свое мнение[1], а с другой – злоупотребление этим правом способно повлечь ущерб правам и интересам третьих лиц.

В настоящее время распространяется точка зрения о необходимости отказа от этого права[2]. Причём, как отмечает А.В. Козлов, фактически право на анонимность уже фактически отменено поскольку владельцы сервисов, позволяющих обмениваться электронными сообщениями, обязаны передавать ключи шифрования по требованию ФСБ РФ[3].

Думаем, что изложенная позиция не вполне корректна, поскольку

---

[1]ООН признала анонимность в Интернете правом человека. URL: http://www.gazeta.ru/tech/news/2015/08/25/n_7509455.shtml (дата обращения: 07.10.16).

[2]*Козлов А.В.* Проблемы правового ограничения анонимности граждан в сети Интернет // Стратегические коммуникации в современном мире: сб. матер. по результатам науч.-практ. конф. Пятой и Шестой Международных научно-практических конференций, Четвертой и Пятой всероссийских научно-практических конференций. 2018. С. 176; *Комаров А.А.* Криминологические аспекты мошенничества в глобальной сети Интернет: автореф. дис. … канд. юрид наук. Саратов, 2011. С. 10.

[3]Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ. 2016. № 28, ст. 4558.

Конституция Российской Федерации в ст. 55, уголовно-процессуальное законодательство, закон «Об оперативно-розыскной деятельности»[1] традиционно предусматривают возможность ограничения конституционных прав и свобод граждан в случаях, предусмотренных законом, однако это обстоятельство не отменяет права на анонимность при общении в киберпространстве и фактического сохранения приватности, под которой понимается возможность пользователя сохранять в тайне свои имя и фамилию, иные личные данные при совершении определённых действий, общении с другими лицами, если при этом не нарушается действующее законодательство.

В такой трактовке, передача ключей шифрования по требованию Федеральной службы безопасности, на наш взгляд, не противоречит Конституции. Однако, на наш взгляд, необходимо обратить внимание и на то обстоятельство, что анонимность рассматривается как возможность свободно высказывать своё мнение. В Российской Федерации, к сожалению, имеют место случаи, когда граждан, высказывавших обоснованную критику действий органов власти, пытались привлекать к уголовной ответственности за клевету. Интерес в связи с этим представляет определение Конституционного Суда РФ, посвящённое оценке конституционности привлечения гражданина к уголовной ответственности за клевету в случае, если соответствующие сведения содержатся в обращениях гражданина в органы государственной власти. По сути, Конституционный Суд рассматривает один из вариантов преследования за критику[2].

Безотносительно к результатам рассмотрения уголовного дела в

---

[1]Федеральный закон от 12 августа 1995 г. № 144-ФЗ (с изм. и доп. от 28 июня 2022 г., № 202-ФЗ) «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. № 33, ст. 3349; 2022. № 27, ст. 4603.

[2]Определение Конституционного Суда РФ № 3272 от 5 декабря 2019 г. «Об отказе в принятии к рассмотрению жалобы гражданина Москалева Михаила Васильевича на нарушение его конституционных прав частью первой статьи 128.1 Уголовного кодекса Российской Федерации и статьей 318 Уголовно-процессуального кодекса Российской Федерации». URL: http://doc.ksrf.ru/decision/KSRFDecision445450.pdf (дата обращения: 24.04.2021).

отношении заявителя Москалева М.В., следует признать существование этой проблемы и предложить определенные правовые гарантии недопущения преследования за нее.

В соответствии со ст. 139[1] УК РСФСР «Преследование граждан за критику» предусматривалась уголовная ответственность за умышленное ущемление должностным лицом прав и охраняемых законом интересов гражданина, связанное с преследованием его за подачу в установленном порядке предложений, заявлений, жалоб, либо за содержащуюся в них критику, а равно за выступление с критикой в иной форме[1]. Обращает на себя внимание, что данная норма была введена в законодательство лишь в 1985 г., в период активного реформирования государства.

В научной литературе высказывалось мнение, что деятельность правоохранительных органов по борьбе с преступностью из уголовно-правового часто перетекала в уголовно-политическое русло против лиц, которые в виде лайков, репостов и комментариев высказывали свое критическое отношение к действиям отдельных политических, религиозных и общественных деятелей, в связи с чем предлагалось декриминализировать такую критику[2].

Заметим, что формально уголовной ответственности за критику в УК РФ не предусмотрено и речь идёт лишь о тех случаях, когда граждане преследовались за свои высказывания с применением положений ст. 282 УК РФ.

Судебная практика знает ряд примеров, когда граждане или должностные лица, не довольные критикой в свой адрес, обращались с гражданскими исками о защите чести и достоинства в адрес критикующих их лиц, требуя

---

[1] *Бытко Ю.И., Бытко С.Ю.* Сборник нормативных актов по уголовному праву России X-XX веков. Саратов: Научная книга, 2006. С. 670.

[2] *Давитадзе М.Д.* Современные проблемы уголовной политики // Вестник Московского университета МВД России. 2018. № 6. С. 126.

компенсации морального вреда[1].

Законом РФ «О порядке обращения граждан» в ст. 6 «Гарантии безопасности гражданина в связи с его обращением» запрещается преследование граждан за критику деятельности государственных органов, органов местного самоуправления или должностных лиц[2].

Однако, несмотря на название статьи, механизма гарантирования безопасности граждан от такого преследования до настоящего времени не выработано. С учётом всего изложенного УК РФ необходимо дополнить статьей 136^1 следующего содержания.

Статья 136^1. Преследование 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 осужденного за период до одного года, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет, либо обязательными работами на срок до двухсот часов, либо исправительными работами на срок до шести месяцев.

Полагаем, что предупредительное воздействие данной нормы будет достаточным даже при таких мягких санкциях, поскольку основным сдерживающим фактором здесь будет выступать сама возможность привлечения к уголовной ответственности и связанная с ней невозможность занимать должностное положение в органах государственной власти.

---

[1]Решение Кочевского районного суда Пермского края от 24 июня 2019 г. по делу № 2-154/2019

[2]Федеральный закон от 2 мая 2006 г. № 59-ФЗ (с изм. и доп. от 27 декабря 2018 г., № 528-ФЗ) «О порядке рассмотрения обращений граждан Российской Федерации» // СЗ РФ. 2006. № 19, ст. 2060; 2018. № 53 (ч. I), ст. 8454.

Возвращаясь к проблеме анонимности в киберпространстве, позволим себе не согласиться с приведённой точкой зрения по поводу необходимости отказа соответствующего права. На наш взгляд, необходимо разграничивать анонимность как безусловное право гражданина и право государство на получение информации о переписке или о личности пользователя киберпространства в случаях, если этого требуют интересы раскрытия преступлений, обеспечения безопасности. В последнем случае правоохранительные органы, получающие доступ к конфиденциальной информации граждан, не причастных к совершению преступлений, обязаны обеспечивать ее сохранность. Кроме того, анонимность следует рассматривать не только как способ защиты от преследования за критику, но и как дополнительный способ обеспечения прав и свобод граждан от преступных посягательств различного рода. Отказ от анонимности облегчит сбор пользовательских данных, которые могут быть использованы в различных мошеннических схемах, посягательствах на личность и т.д.

Как отмечалось при анализе причин и условий виктимизации пользователей киберпространства, в настоящее время сложилась асимметрия прав и обязанностей пользователей и операторов платежных систем, при которой последние обладают значительными преимуществами в отстаивании своих интересов. Для изменения ситуации и повышения защищенности граждан нам представляется необходимым изменить установленные законом сроки, в течение которых клиент может уведомить оператора о совершении электронных переводов без его участия. За ориентир предлагается принять аналогичные сроки, установленные для уведомления операторов платежных систем в США – 30 суток. Таким образом, в ст. 11 федерального закона «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.

Мы полагаем, что 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.

Специфика предупреждения виктимизации пользователей в киберпространстве состоит в том, что организационные меры предупреждения зачастую неотделимы от технических: те или иные мероприятия всегда сопровождаются разработкой программ, изменения режима доступа к информации, то есть, сочетают в себе признаки и организационных и технических мероприятий.

Одной из причин виктимизации выступают, как уже отмечалось, ошибки в программном обеспечении. Скрытые ошибки приводят к техническим авариям, нарушению прав граждан в отдельных областях (например, как это было продемонстрировано на примере США, к нарушению избирательных прав), а в отдельных случаях – к незаконному осуждению граждан на основании ошибочных результатов работы бухгалтерских программ.

Выявление таких ошибок является весьма трудоёмкой задачей ввиду необходимости изучения значительных объёмов исходных текстов программ (то есть, текстов, которые пишут программисты на языках программирования, до их преобразования в машинные коды). Однако это – решаемая задача, если исходные тексты доступны для анализа. 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[1].

В тех случаях, когда программные продукты используются при обработке

[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).

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.

Как отмечается специалистами, анализ исходного кода операционной системы Windows позволит качественно повысить безопасность информационных систем, работающих на этой платформе[1].

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. В пользовательских соглашениях, прилагаемых к экземплярам программного обеспечения, раздел об ответственности его производителя за вред, причиненный ошибками в программном обеспечении, не указывается, а соответствующая практика освобождает его от любой ответственности.

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, возникших в Великобритании, когда ошибка, присутствовавшая в программном обеспечении, использовавшемся британской почтовой компанией более 20 лет, приводила к систематической выдаче сообщений о недостачах, в

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

результате чего к уголовной ответственности было незаконно привлечено 740 человек, некоторые закончили жизнь самоубийством[1].

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, в том числе, сотрудников органов прокуратуры, предполагает установку специального программного обеспечения «Справки БК», размещенного для свободного скачивания на сайте Президента РФ. Представленная версия программы функционирует только на компьютерах, работающих под управлением операционной системы Windows[2].

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

Не стоит и говорить, что подобные случаи снижают мотивацию для перехода на отечественное программное обеспечение.

Полагаем, что подобная ситуация должна быть исправлена. Для этого

---

[1]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).

[2]См., напр.: СПО «Справки БК» (версия 2.4.4) от 26.06.2020. URL: http://static.kremlin.ru/media/events/files/ru/SyU6G8jjjL9oEZPU4L67QV9aLZA5Ahl4.zip (дата обращения: 03.05.2021).

необходимо для разработчиков программного обеспечения, используемого для государственных нужд, установить в качестве обязательного требования разработку версий для различных операционных систем. В этом смысле хороший пример представляет отечественная система для проведения видеоконференций TrueConf, отечественные пакеты офисных программ «Р7-Офис», «Мой офис» и т.д.

Распространенная практика предоставления документов в государственные органы состоит в требовании использования, как правило, форматов фиры Microsoft, что резко снижает конкурентные преимущества других производителей. Фактически в подобных случаях имеет место ситуация, когда государство открыто встает на путь поддержки иностранных производителей в ущерб отечественным.

Поэтому 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 представляться возможность выбора формата документов, поддерживаемых свободным программным обеспечением.

Для того, чтобы нормативно зафиксировать обязательность поддержки программного обеспечения, работоспособного на отечественных операционных системах, необходимо дополнить ст.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»[1] пунктом «и»

[1]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 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и

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

Больной темой современной России в последнее время стало мошенничество, особенно его высокотехнологичные разновидности. Распространение коронавирусной инфекции и связанные с ней ограничения, привели к тому, что огромное большинство наших граждан вынуждены были находится на карантине и всю активность перенесли в киберпространство. Здесь имеется в виду не только выполнение рабочих обязанностей, но и развлечения, общение, покупки и т.д. Есть веские основания полагать, что именно карантин вызвал резкий рост кибермошенничеств и актуализировал проблемы его профилактики, в том числе, и виктимологической.

Нам представляется, что множество предлагаемых по борьбе с кибермошенничеством мероприятий, таких, например, как информирование граждан о новых способах совершения хищений, частное предупреждение со стороны отдельных лиц и т.п., не решают одной главной проблемы – обезличенности денег, порождающей широкие возможности сокрытия их происхождения и, тем самым, выступающей фундаментальным условием совершения многих преступлений. Сущность кредитно-финансовой системы до настоящего времени остаётся практически неизменной, даже если учёт осуществляется с помощью электронных средств связи: каждому счету соответствует определённая 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

муниципальных нужд») (с изм. и доп. от 8 августа 2022 г. № 1393) // СЗ РФ. 2015. № 47, ст. 6600; 2022. № 33, ст. 5906.

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 её перемещения фиксируются без возможности каких-либо сторонних манипуляций. Здесь имеется в виду технология, именуемая блокчейном, и созданные на её основе криптографические валютные системы bitcoin, ethereum и другие. Надёжность 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[1].

По состоянию на май 2021 г. весь блокчейн (файл, содержащий историю всех операций) самой старой криптовалюты Bitkoin занимает на жёстком диске 399,7 Гигабайт. То есть, возможностей обычного персонального компьютера гарантировано хватит на будущее десятилетие[2]. Поэтому полные копии блокчейнов хранятся на огромном числе компьютеров, разбросанных по всей планете.

Особенности современных криптовалют позволяют совершать полностью анонимные сделки, что привлекает к ним преступников и снижает их ценность

---

[1]Подробнее о технологии блокчейн см., напр.: *Антонян Е.А., Аминов И.И.* Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6. С. 167; *Калиниченко В.Н., Кондратьев В.Ю.* Принцип работы блокчейн // Цифровизация экономики: направления, методы, инструменты. сб. ст. по матер. II всерос. науч.-практ. конф. Краснодар, 2020. С. 219; *Лунтовская М.А.* Технологии блокчейн: понятие и принципы работы // Ученые записки Российской Академии предпринимательства. 2020. Т. 19. № 2. С. 72; *Свищёв А.В., Хлоповская А.В.* Понятие распределенных реестров и принцип работы блокчейн // Моя профессиональная карьера. 2021. Т. 1, № 23. С. 210.

[2]Cryptocurrency statistics. URL: https://bitinfocharts.com/ (дата обращения: 09.05.2021).

для государств. Кроме обычной уголовной преступности к использованию криптовалют перешли взяточники[1] и наркодилеры[2].

В литературе достоинства и недостатки криптовалют стали предметом специального исследования. Наряду с положительными сторонами отмечается и масса возможных негативных последствий их широкого распространения[3].

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 тестированию своей цифровой валюты DCEP (Digital Currency Electronic Payment) или «цифрового юаня»[4].

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 защищённости, поскольку вся информация о перемещении средств шифруется и подделать её невозможно[5].

Поэтому государство в любой момент времени будет располагать полной

---

[1] *Акимов Н.* Вынесен приговор следователям ФСБ, бравшим взятку криптовалютой. URL: https://legal.report/vynesen-prigovor-sledovatelyam-fsb-bravshim-vzyatku-kriptovaljutoj/ (дата обращения: 09.05.2021); В Приморье экс-борца с наркотиками будут судить за взятку в биткоинах. URL: https://ria.ru/20201021/bitkoin-1580777237.html (дата обращения: 09.05.2021).

[2] *Сидоренко Э.Л.* Наркотики и криптовалюта: мировые криминологические тренды // Наркоконтроль. 2018. № 2. С. 8.

[3] *Сидоренко Э.Л.* Криптовалюта как новый юридический феномен // Общество и право. 2016. № 3. С. 193; *Пинкевич Т.В.* Легализация криптовалюты в россии: за и против // Уголовная политика и правоприменительная практика: сб. матер. V междунар. науч.-практ. конф. СПб.: Петрополис, 2018. С. 296,297.

[4] 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).

[5] Отдельные технические подробности о CDEP можно найти здесь. URL: https://dcep.ru/ (дата обращения: 09.05.2021).

и точной информации 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 распространённого вида хищений в настоящее время.

Представляется, что разработка и внедрение собственной цифровой валюты Российской Федерацией даст не только огромные экономические преимущества: высочайшую скорость финансовых транзакций, снижение их стоимости за счёт того, что станут ненужны посредники в виде традиционных банков, надёжность 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.

Целью индивидуальной профилактики, как отмечается в криминологической литературе, является предупреждение преступлений со стороны отдельных лиц[1]. По аналогии можно определить индивидуальную виктимологическую профилактику как совокупность мер, направленных на предотвращение посягательств в отношении конкретных граждан. Однако, как указывается в литературе, она может быть направлена не только на жертв преступлений, но и на их окружение, социальные связи и микросреду[2].

Прежде всего, хотелось бы остановиться на такой мере предупреждения, наиболее часто предлагаемой в криминологических работах, как информирование потенциальных жертв преступных посягательств о новых видах преступлений и способах защиты от них[3].

---

[1]См., напр.: *Курганов С.И.* Криминология. М.: Юннити, 2007. С. 81.

[2]*Качурова Е.С.* Современные возможности индивидуального виктимологического предупреждения преступности // Проблемы современного законодательства России и зарубежных стран: матер. VIII междунар. науч.-практ. конф. Иркутск: Иркутский институт (филиал) ВГУЮ (РПА Минюста России), 2019. С. 322.

[3]См., напр.: *Бочков А.А.* Виктимологическая культура:теория и практика // Право. Экономика. Психология. 2016. № 2. С. 7; *Белицкий В.Ю.* Предупреждение совершения мошенничеств участковым уполномоченным полиции // Вестник Барнаульского юридического института МВД России. 2017. № 2. С. 132; *Шалагин А.Е.* О приоритетных

Полагаем, что такая мера является полезной, однако не следует переоценивать её эффективность. Применительно к мошенничеству наблюдается такая картина: количество преступлений, особенно связанных с хищениями денежных средств, постоянно растёт. В средствах массовой информации непрерывно размещаются публикации о таких хищениях. Во многих городах практикуется информирование граждан о видах мошенничеств с помощью уличных рекламных проекторов, вставок в радиопередачах и т.п.

Однако ситуация не только не меняется, но и продолжает ухудшаться. Н.В. Никулин, исследовавший виктимологические аспекты профилактики мошенничеств, обращает внимание на то, что граждане при всех предпринимаемых усилиях, в недостаточной степени информированы о мерах, позволяющих избегать преступных посягательств на своё имущество. По данным этого автора, только 2 из 25 опрошенных им граждан слышали о памятках, выпущенных МВД для предотвращения мошенничеств. Этот же автор предлагает вместо памяток распространять предостерегающую информацию на телевидении[1].

Полагаем, что в настоящее время телевидение не является самым эффективным средством доставки информации. Согласно имеющимся рейтингам, аудитория наиболее популярного в России канала «Россия-1» составляет всего 12,5 % от всех зрителей старше 4 лет. В отдельных возрастных группах она еще ниже[2]. При этом значительная часть жителей страны отдает предпочтение платным каналам[3], на которых количество рекламных вставок меньше, а, следовательно, и меньше возможностей для правоохранительных

направлениях деятельности органов внутренних дел по предупреждению преступлений и административных правонарушений // Вестник экономики, права и социологии. 2014. № 2. С. 155 и др.

[1] *Никулин Д.В.* Профилактика мошенничества в сфере глобальной сети Интернет и средств массовой информации. виктимологический аспект // Аллея науки. 2018. Т. 6, № 6 (22). С. 790.

[2] *Ефимович Е.* «Россия 1» стала ударником пятилетки. URL: https://www.rbc.ru/newspaper/2020/12/08/5fca6f359a79470a0b53912a (дата обращения: 18.08.2021).

[3] Аналитики сообщили об ускорении роста аудитории платного ТВ в России на 25%. URL: https://www.kommersant.ru/doc/4683284 (дата обращения: 18.08.2021).

органов доносить до них предупредительную информацию таким образом.

Значительная часть граждан в качестве основного источника информации рассматривает Интернет. При этом количество посещаемых сайтов, на которых теоретически возможно размещение предупредительной информации, не поддается никаким оценкам. Кроме того, предлагая меры по информированию о возможных преступлениях, необходимо учитывать то, что граждане не всегда готовы или желают воспринимать постороннюю информацию при просмотре сайтов. Потоки разнообразных сведений, которые ежедневно обрушиваются на современного человека, формируют отторжение, невосприимчивость к нежелательной информации, донесение которой воспринимается как своего рода психологическое насилие. Поэтому повсеместной практикой среди пользователей киберпространства становится отсечение всех информационных блоков. Например, при просмотре текстов включаются специальные режимы чтения, оставляющие на просматриваемой странице только текст материала. Расширяется практика получения медиаконтента по платным подпискам, основным условием которых является отсутствие посторонних материалов. Кроме того, по публикуемым оценкам, 27 % пользователей блокирует на своих устройствах рекламу[1].

В подобных условиях массовое распространение предупредительной информации будет восприниматься как некая разновидность спама, от которой нужно привычно избавляться. Следует иметь в виду, что размещение таких сведений в рекламных блоках является платным. Поэтому возникает вопрос о росте затрат на предупредительную деятельность без внятной оценки их эффективности.

Поэтому в качестве допустимого (но не самого эффективного) средства информирования населения о возможных преступных посягательствах и способах их предотвращения рассматривается размещение соответствующих

[1] *Лакодин В.* «Непокоренные»: как и почему миллиард человек противостоит интернет-рекламе. URL: https://texterra.ru/blog/nepokorennye-kak-i-pochemu-milliard-chelovek-protivostoit-internet-reklame.html (дата обращения: 18.08.2021).

материалов на местных новостных сайтах, аудиторию которых, как правило, составляет активная часть взрослого населения региона.

Кроме того, на наш взгляд, должна быть пересмотрена сама концепция информирования. Оно должно стать точечным, направленным на конкретных адресатов и осуществляться именно в те моменты, когда потенциальные жертвы киберпреступлений готовы воспринимать соответствующие предостережения, причём именно в таких формах, которые смогут быть в этот момент восприняты.

Хорошим примером является электронная форма оплаты железнодорожных билетов на официальном сайте ОАО «РЖД»: после выбора поезда, вагона и ввода данных о пассажирах, пользователь предоставляется возможность перейти к форме оплаты выбранных билетов с помощью банковской карты. Причём соответствующая кнопка на сайте становится доступной лишь после того, как пользователь ознакомится с информацией об особенностях такой оплаты. Технически это выглядит так, что пользователь просматривает соответствующий текст и ставит внизу отметку о согласии.

Полагаем, что это является хорошим примером, который может быть распространен и на другие дистанционные способы оплаты и перечисления денежных средств с помощью банковских карт. Например, после указания реквизитов получателя платежа в системах так называемой двухфакторной идентификации, пользователю приходит СМС-сообщение с одноразовым паролем. В таких СМС могут быть кроме самого пароля содержаться и другие сведения: например бесплатный круглосуточный телефон службы безопасности банка, уведомления о недопустимости указания кому бы то ни было реквизитов банковских карт по телефону, вне банковской организации и т.д.

Однако это далеко не весь перечень возможной информации, точечно предоставляемой клиенту банка. Службами безопасности банков накапливается огромный массив данных о переводах, о номерах телефонов и счетов в платёжных системах, которые принадлежат мошенникам. Поэтому в случае

попытки перечисления денег на счета, которые могут принадлежать мошенникам, необходимо немедленное оповещение клиента банка о том, что он, с большой долей вероятности, подвергается кибермошенничеству.

Эффективность такой системы может быть многократно повышена при объединении баз данных банковских служб безопасности, содержащих реквизиты мошеннических счетов и телефонов, с которых осуществляются мошеннические звонки. Кроме того, объединённая база должна постоянно пополняться информацией, получаемой от правоохранительных органов, получающих заявления от граждан о совершении ими хищений, а также службами безопасности банков, получивших от граждан аналогичную информацию.

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[1].

Действительно, в киберпространстве можно обнаружить любые сведения, например, о способах изготовления взрывных устройств или оружия, порнографические материалы и предложения сексуальных услуг, о продаже наркотиков и т.п. Все предпринимаемые попытки закрыть доступ к ним на практике оборачиваются лишь незначительным увеличением временных затрат любопытных граждан.

В этой связи необходимо высказать несколько критических замечаний по поводу сформировавшейся политики в сфере защиты детей от информации, способной причинить вред их нормальному развитию и воспитанию, нормативную базу которой составляют Закон «О защите детей от информации,

[1] *Короткова Н.А.* Виктимологическая профилактика преступлений против половой неприкосновенности несовершеннолетних, совершаемых с использованием сети Интернет // Научные достижения и открытия современной молодёжи: сб. ст. II междунар. науч.-практ. конф. Новосибирск, 2017. С. 227.

причиняющей вред их здоровью и развитию»[1] (далее – *Закон о защите детей*), Закон «Об информации, информационных технологиях и о защите информации»[2] (Далее – *Закон об информации*), Закон «О средствах массовой информации»[3] (Далее – *Закон о СМИ*).

Статьёй 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 ст. 15.1 Закона об информации в Российской Федерации создаётся 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, как было сказано ранее, наличие нормативного запрета не означает, что несовершеннолетние не смогут получить доступ к запрещённой информации. Для того чтобы понимать сущность проблемы блокировки информации, следует понимать, что физически с этой информацией ничего не происходит. Она как была, так и остаётся на определенном сервере в киберпространстве. Однако её интернет-адрес заносится в список

---

[1]Федеральный закон от 29 декабря 2010 г. № 436-ФЗ (с изм. и доп. от 5 апреля 2021 г., № 65-ФЗ) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1, ст. 48; 2021. № 15 (ч. I), ст. 2432.

[2]Федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. и доп. от 14 июля 2022 г., № 325-ФЗ) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I), ст. 3448; 2022. № 29 (ч. III), ст. 5292.

[3]Федеральный закон от 27 декабря 1991 г. № 32 (с изм. и доп. от 14 июля 2022 г., № 255-ФЗ) «О средствах массовой информации» // Ведомости СНД и ВС РФ. 1992. № 7, ст. 300; СЗ РФ. 2022. № 29 (ч. II), ст. 5222.

заблокированных ресурсов. Этот список доступен для всех организаций (интернет-провайдеров), предоставляющих в нашей стране услуги доступа к сети Интернет. Примерами организаций-провайдеров выступают Ростелеком, Дом.ру, все операторы сотовой связи.

Пользователи, желая получить доступ к какому-либо ресурсу, либо вводят его адрес в адресной строке соответствующей программы (например, браузера), либо выбирают интересующий ресурс из списка, полученного от поисковой системы.

В тех случаях, когда пользователь намеревается посетить ресурс, доступ к которому заблокирован, провайдер просто не осуществляет подключения. Вместо этого пользователь перенаправляется на страницу с информацией, что запрашиваемый им ресурс заблокирован на территории страны.

Существующую систему блокирования можно обойти самыми различными методами. 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. VPN-сервис – это сервер в сети Интернет, как правило, размещенный на территории другой страны. Этот сервис создает защищенное соединение, при котором вся информация, курсирующая между пользователем и сервером шифруется, а сам выступает промежуточным звеном в передаче информации от пользователя к запрещенному ресурсу. В подобных случаях провайдер не может заблокировать доступ к запрещенной информации, поскольку он видит лишь, что пользователь подсоединился к какому-то адресу в сети, которого нет в списке защищенных ресурсов.

Информация о таких VPN-сервисах широко распространена в молодёжной среде, в том числе, и среди несовершеннолетних. Многие браузеры предусматривают возможности поиска и подключения к таких ресурсам.

Во-вторых, информация с заблокированных сайтов легко копируется (в

течение минут) на другие страницы, которые еще не выявлены правоохранительными органами и не заблокированы, но становящиеся мгновенно известными заинтересованным лицам (в нашем случае – несовершеннолетним). Таким образом, при существующей системе блокирования нежелательной для несовершеннолетних информации всегда имеется временной зазор, между появлением информации на каком-то сервере и до того момента, пока она остаётся доступной, не занесенной в соответствующие списки. Иногда это неконтролируемое правоохранительными органами состояние может длиться недели или даже месяцы.

Таким образом, в настоящее время можно говорить не о полноценной реализации политики защиты несовершеннолетних от информации, причиняющей вред здоровью и развитию детей, а лишь о её имитации.

В некоторых случаях складывается парадоксальная ситуация: прокуратурой подаются судебные иски о блокировании сайтов, содержащих запрещенную информацию, однако суды по различным причинам отклоняют их и процедура блокирования фактически приостанавливается. При этом сайты продолжают работу в обычном режиме.

Именно подобным образом проходила процедура блокировки порносайта yourporn.com. В соответствии с решением Первореченского районного суда г. Владивостока по иску прокуратуры этот yourporn.com был внесен в реестр запрещенных сайтов[1]. Однако это решение было впоследствии отменено, поскольку к заявлению прокурора не были приложены результаты соответствующей экспертизы[2]. Сходная ситуация сложилась с блокировкой другого порносайта Pornhub, который был сначала заблокирован, а затем разблокирован по решению суда[3].

---

[1]*Стаценко Н.* Роскомнадзор заблокировал Pornhub на всей территории России. URL: https://rb.ru/news/pornhub-down/ (дата обращения: 05.05.2021).

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

[3]Роскомнадзор разблокировал PornHub. URL: https://ria.ru/20170413/1492189250.html (дата обращения: 16.04.2021).

Таким образом, несмотря на фактический запрет на распространение порнографии, устанавливаемый ст. 4 Закона о СМИ, ст. 10.4, 10.5, п. «а» ч 5 ст. 15^1 Закона о средствах массовой информации, ст. 5 Закона о защите детей, ст. 242 УК РФ, на территории Российской Федерации безнаказанно в течение многих лет функционировали сайты, распространяющие исключительно информацию, запрещённую для демонстрации. Органы же, которые в соответствии со ст. 20 Закона о защите детей, должны осуществлять государственный надзор за соблюдением законодательства РФ о защите детей от информации, причиняющей вред их здоровью и (или) развитию – демонстрируют бездействие и бессилие в попытках их блокирования.

В функционировании упомянутых порносайтов имелось небольшое отличие. Yourporn предоставлял доступ к любой информации без какой-либо идентификации пользователя, то есть даже без имитации проверки возраста посетителей сайта. Pornhub требует входа через сеть «ВКонтакте», т.е. предполагается, что контроль за возрастом пользователя возлагается на эту социальную сеть. Однако, как известно, регистрация в сети «ВКонтакте» не требует подтверждения возраста, достаточно того, что пользователь выбирает его по своему желанию. Единственное ограничение, которое формально выдвигает эта социальная сеть, состоит в том, что возраст пользователя должен быть не менее 14 лет. Однако никаких соответствующих проверок не проводится. Малолетние пользователи сети при регистрации всегда завышают свой возраст, причём к этому их подталкивает и позиция образовательных учреждений, требующих зачастую от младших школьников участия в группах этой сети для того, чтобы обмениваться внутриклассной информацией. Однако парадокс ситуации состоит в том, что фактически сложившаяся неурегулированность вопроса о запрете порнографии, приводит к легальной возможности лиц, достигших четырнадцатилетнего возраста, пользоваться порнографическими ресурсами.

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.[1] Причем, как следует из названия блокируемых сайтов, большинство из них имеет российское происхождение (по этическим соображениям их конкретные названия не приводятся). Информации об обжаловании блокировок таких сайтов у нас не имеется. И лишь для двух указанных крупнейших иностранных порносайтов российское правосудие сделало исключение и фактически легализовало их деятельность вопреки положениям российского же законодательства.

Полагаем, что основание, по которому обжалуется блокировка сайтов (в данном случае адвокат ссылался на отсутствие экспертного заключения о характере изображений, размещаемых на этих сайтах), связано не халатностью прокурорских работников, а, скорее, финансовыми ограничениями. Дело в том, что решение суда должно быть основано на заключении эксперта, которым будет подтверждено, что размещенные на сайте фото- и видеоматериалы относятся к порнографическим.

Стоимость искусствоведческой экспертизы исчисляется суммами порядка десяти тысяч рублей и более. Однако сайтов, требующих блокировки огромное количество, что влечет резкое увеличение расходов на блокировку.

Поэтому с учётом масштабов задачи блокировки представляется правильным создавать при отдельных прокуратурах специальные должности экспертов, которые обладают лицензиями на проведение наиболее часто востребованных экспертиз (например, искусствоведческой, лингвистической) и возложить на них обязанности по подготовке экспертных заключений.

---

[1]Решение Первореченского районного суда г. Владивостока (Приморский край) по делу № 2-2409/2016. URL: https://sudact.ru/regular/doc/wYbYK2yGMx1m/?regular-judge=&=1629717705515 (дата обращения: 23.08.2021); Решение Первореченского районного суда г. Владивостока (Приморский край) по делу № 2-2414/2016. URL: https://sudact.ru/regular/doc/amZLetyb8NrT/?&regular-judge=&=1629717865756 (дата обращения: 23.08.2021) и др.

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.

Впрочем, даже если процесс блокировки будет упрощен и ускорен, это не сможет, по нашему мнению, в полной мере оградить несовершеннолетних от запрещённой информации. В настоящее время её блокировка осуществляется по модели «чёрных списков» – ограничиваются источники информации, внесённые в специальный реестр. Иными словами, реализуется принцип – разрешено все то, что не запрещено. При таком подходе всегда остаётся возможность донести до подростка нежелательную информацию либо путём обхода блокировок, либо путём быстрого создания новых сайтов, ещё не внесённых в чёрный список.

Принципиально другой подход состоит в том, чтобы доступ в киберпространство для подростков осуществлять по белым спискам, то есть спискам ресурсов, которые проверены и признаны допустимыми. Все же остальные ресурсы считать по умолчанию запрещенными к просмотру несовершеннолетними. Такой подход значительно проще реализовать технически, поэтому идея фильтрации контента по белым спискам предлагалась экспертным советом Лиги безопасного интернета для реализации еще в 2012 г.[1], однако реализован не был, хотя примеры белых списков, заранее изученных экспертами, имеются.

В соответствии с государственной программой «Цифровая экономика»[2] разработанной в 2017 г., к 1 кварталу 2020 г. должна была быть введена в

---

[1]*Хазов В.* Фильтрация интернет-контента для школ. Использование «белых списков» (ACL). URL: https://vasexperts.ru/blog/filtraciya-internet-kontenta-dlya-shkol-ispolzovanie-belyx-spiskov-acl/ (дата обращения: 06.05.2021).

[2]Распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. URL: https://www.garant.ru/products/ipo/prime/doc/71634878/ (дата обращения: 06.05.2021).

эксплуатацию национальная система фильтрации интернет-трафика при использовании информационных ресурсов детьми.

Однако позже появились сообщения о том, что Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации отказалось от реализации этой идеи, посчитав её избыточной на том основании, что в школах уже имеется достаточное количество решений, реализующих эту функциональность[1].

Однако с учётом распространённости персональных компьютеров, ноутбуков, планшетов и смартфонов среди подростков и молодёжи, ограничение контент-фильтрации только школьными компьютерами не является решением проблемы безопасности несовершеннолетних в киберпространстве. Интернет, соцсети, мессенджеры, игровые платформы становятся естественной и постоянной средой их общения. Поэтому необходим комплекс мер, которые позволят обезопасить подростков не только в школьное, но и во внеурочное время.

В соответствии со ст. 6 Закона о защите детей, производители и распространители информации осуществляют её классификацию по возрасту, начиная с которого она может быть предоставлена (для лиц, не достигших шести лет, для достигших шести, двенадцати и шестнадцати лет). Полагаем, что аналогичным образом должны маркироваться сайты или отдельные страницы в сети «Интернет». Обязанность соответствующей маркировки и ответственность за ее достоверность должна возлагаться на владельцев сайтов. Сайты, не маркированные соответствующим образом, не должны попадать в поисковую выдачу для несовершеннолетних.

Для того, чтобы нормативно закрепить такое положение, необходимо дополнить ч. 2 ст. 10 Закона об информации, регламентирующей обязанности владельцев сайтов сети «Интернет», после слов «которые достаточны для

[1] *Клевошин П.* Минцифры отказалось от фильтра интернет-трафика для детей. URL: https://www.vedomosti.ru/technology/articles/2020/11/22/847846-mintsifri-otkazalos (дата обращения: 06.05.2021).

идентификации такого лица», 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”».

Обязанность выдачи информации в соответствии с возрастной маркировкой и возрастом пользователя должна возлагаться на поисковые системы, например Яндекс, Google. Поэтому соответствующие требования к необходимо внести в ст. 10^3 Закона об Информации, регламентирующую обязанности операторов поисковых систем. Предлагаем дополнить эту статью 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, необходимо предусмотреть использование специальных пользовательских 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 в сети «Интернет», которые содержат ссылки на контент, разрешённый в соответствии со статьями 7-10 Закона о защите детей, 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.

Полагаем, что предложенный комплекс мер в значительной мере улучшит ситуацию с обеспечением духовного и нравственного развития несовершеннолетних и ограничит негативное информационное влияние на эти процессы со стороны сторонних лиц в киберпространстве. При этом устанавливать дополнительную ответственность для субъектов, указанных в Законе об информации, на наш взгляд, не нужно, так как КоАП РФ уже содержит ряд статей, предусматривающих административную ответственность за нарушение указанного закона. В частности в ст. 6.17 КоАП РФ устанавливается административная ответственность за нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, в ч. 16 ст. 19.5 КоАП РФ – за невыполнение в установленный срок предписания федерального органа исполнительной власти, осуществляющего государственный надзор за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

Ещё одним источником информации, представляющей опасность для несовершеннолетних, являются социальные сети. Несмотря на то, что правила регистрации, как правило, предусматривают в качестве обязательного условия достижение определённого возраста, однако в действительности документальной проверки введённой информации не осуществляется. Таким образом, возможна регистрация с любого возраста, что обеспечивает несовершеннолетним доступ к любой информации, размещённой в сети или даже на других ресурсах.

Если будет реализована предложенная нами ранее возрастная маркировка информации, то дополнительных изменений для возникновения у владельцев социальных сетей обязанностей по ограничению доступа для несовершеннолетних не возникнет. Закон Об информации уже в действующей редакции устанавливает обязанность в п. 1 ч. 4 ст. 16 обязанность обладателей

информации, операторов информационной системы в случаях, установленных законодательством Российской Федерации, обеспечить предотвращение несанкционированного доступа к ней и (или) передачи её лицам, не имеющим права на доступ к информации.

Таким образом, введение возрастной маркировки информации в киберпространстве позволит без значительных изменений действующего законодательства повысить защищённость несовершеннолетних от потенциально вредных для них ресурсов.[1]

С учетом изложенного предлагаются следующие меры индивидуальной профилактики криминальной виктимизации пользователей сети «Интернет» в киберпространстве:

1. Разработка и введение в оборот отечественной цифровой валюты, что позволит исключить анонимность финансовых транзакций и снизить, таким образом, виктимность граждан.

2. 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.

3. Организация доступа несовершеннолетних в сеть «Интернет» по «белым» спискам, в соответствии с которым доступными для них будут только сайты, заранее внесенные в такие списки.

4. Для мобильных устройств, используемых несовершеннолетними,

---

[1] *Родина Е.А.* Виктимологическое предупреждение преступлений в киберпространстве // Актуальные проблемы государства и права. 2021. № 19. С. 518.

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 Закона о защите детей, 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.

5. Дополнить ч. 2 ст. 10 федерального закона «Об информации, информационных технологиях и о защите информации», регламентирующей обязанности владельцев сайтов сети «Интернет», после слов «которые достаточны для идентификации такого лица» 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”».

6. Дополнить статью 10^3 федерального закона «Об информации, информационных технологиях и о защите информации» 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».

ЗАКЛЮЧЕНИЕ

Новизна и актуальность избранной темы диссертационного исследования обусловлены масштабами внедрения компьютерных технологий в повседневную жизнь граждан. Уже в период завершения нашей работы произошли события, значительно ускорившие эти процессы. Имеется в виду, прежде всего, коронавирусная инфекция и связанные с нею карантинные ограничения, которые привели к изменению образа жизни многих граждан, вынужденных оставаться в течение длительного времени в изолированных условиях и перенесшими в связи с этим всю деловую и социальную активность в киберпространство. Многие виды деловой деятельности также вынуждены были адаптироваться к новой ситуации, а такие сферы, как образование, в течение долгого времени осуществлялись исключительно в дистанционном варианте.

В новых реалиях существенно возросло количество экономических операций, осуществляемых посредством киберсетей, качественно изменился охват отраслей, перешедших на дистанционное обслуживание клиентов.

Не удивительно, что киберпреступность также демонстрирует тектонические изменения, затрагивая все аспекты взаимодействия субъектов в киберпространстве и моментально адаптируясь к новым возможностям.

К эпидемиологическому присоединилось действие внешнеполитических факторов, в числе которых, в первую очередь, следует назвать укрепление суверенитета России, что привело к обострению международных отношений и к осознанию на всех уровнях государственной власти остроты проблемы киберпреступности и необходимости ограничения граждан от враждебного влияния в культурной, нравственной и духовной сферах, реализуемого иностранными государствами посредством размещения соответствующей информации в киберпространстве.

Комплексная разработка мер виктимологической профилактики потребовала от нас детального анализа виктимологической теории и уточнения

базовых виктимологических понятий. В частности, на основе анализа положений уголовного, уголовно-процессуального, административного и гражданского права было установлено, что термин потерпевший, которым традиционно оперируют виктимологи, не охватывает в полном объеме всех особенностей и аспектов, которые характерны для лиц, пострадавших от преступлений. За пределами этого понятия остаются лица, пострадавшие от посягательств, которые еще не закреплены в качестве преступлений или правонарушений, хотя фактически вред им причиняется. В ряде случаев постановление о признании лица потерпевшим не выносится. В случае вовлечения граждан в деятельность организаций противоправной направленности, например, запрещенной Верховным Судом организации АУЕ, вред нормальному развитию несовершеннолетних причиняется с момента их вовлечения, однако сама деятельность организации признается преступлением лишь после признания судом ее деятельности незаконной. Между этими событиями может лежать длительный период времени, в течение которого вовлекаемые в деятельность организации несовершеннолетние не являются потерпевшими.

Приведенные примеры можно продолжать и далее, однако из сказанного уже ясно, что термин потерпевший не отражает всего объема виктимологической характеристики лиц, пострадавших от преступлений. Поэтому в данной работе обосновывается необходимость его повсеместной замены термином «жертва».

Также неопределенным оставалось до недавнего времени содержание и криминологические свойства киберпространства. В литературе имеется множество синонимов этого термина, которые с различной полнотой отражают его криминологически значимые свойства. В работе показано, что с наибольшей полнотой отражает сущность и важнейшие черты взаимодействий, осуществляемых путем компьютерных сетей, термин «киберпространство». Именно такое понимание позволяет нам уяснить его

сущность, сравнивая совершение преступлений в обычном, физическом пространстве, познать важнейшие криминологически и виктимологически значимые его свойства, в том числе, имеющие значение для оценки характера и степени общественной опасности посягательств, которые в нем совершаются. В частности показано, что последняя характеристика для преступлений, связанных с распространением специфической информации (например, экстремистского характера), определяется не только содержанием этих сообщений, но и аудиторией, на которую их распространитель в принципе может воздействовать.

Особенности киберпространства определяют и характер виктимологической детерминации. Если для преступлений, совершаемых в физическом пространстве, она может осуществляться как путем активных действий, так и бездействием, то в киберпространстве в подавляющем большинстве случаев речь идет об активных действиях пользователя с компьютерной информацией, таких, как, открытие файла, переход по ссылке, выбор элемента управления и т. п.

При изучении причин криминальной виктимизации пользователей сети «Интернет» в киберпространстве были вычленены объективные и субъективные причины. К числу объективных, не зависящих от личности и поведения пользователя причин криминальной виктимизации, следует отнести сложность современного программного обеспечения и наличие в его используемых версиях большого числа ошибок, часть которых еще не известна его производителям. В ряде случаев безопасность программного обеспечения намерено ослабляется в пользу удобства пользователя, что характерно, в основном, для банковского сектора.

Современные технологии позволяют злоумышленникам охватывать огромную аудиторию потенциальных жертв, что в совокупности с отсутствием в широких массах населения культуры обращения с конфиденциальной информацией, образует устойчивую предпосылку для увеличения числа

мошеннических посягательств в киберпространстве.

Впервые в отечественной литературе был выявлен такой фактор виктимизации как асимметрия в уровне правовой и технической защищённости прав пользователей и операторов платежных систем, когда пользователь максимально ограничен в способах защиты информации, сроках уведомления операторов о несанкционированных действиях со счетами.

К субъективным факторам виктимизации следует отнести низкий уровень компьютерной грамотности пользователей, которые при изучении работы с компьютерами не акцентируют внимание на вопросах обеспечения безопасности. В ряде случаев в киберпространстве происходили процессы виктимизации жертв от насильственных посягательств, что связано с отсутствием культуры и навыков общения в социальных сетях.

Во многих случаях жертвы киберпреступников, ошибочно полагая, что их действия остаются анонимными, провоцируют посягательства в отношении себя путем совершения неодобряемых обществом действий (просмотр порнографии, общение с незнакомыми людьми на провокационые темы и проч.).

Проблема отсутствия культуры общения усугубляется неурегулированностью вопроса о возрасте, начиная с которого разрешается пользоваться отдельными ресурсами. В условиях пандемии учебные заведения предписывают младшим школьникам регистрироваться на различных ресурсах, поставляя их, таким образом, в положение потенциальной жертвы киберпреступников.

Также впервые в криминологической литературе было обращено внимание на такое виктимогенное явление, как «информационный пузырь», когда пользователь ограничивает свое информационное окружение небольшим количеством предпочитаемых сайтов, игнорируя все остальные. Столь однобокий подход к информации формирует предвзятое отношение к отдельным явлениям, игнорирование альтернативных точек зрения, узость

кругозора. При этом каких-то других каналов для доставления гражданам информации от государственных органов практически не остается. Это явление, с одной стороны, детерминирует виктимизацию пользователей, а с другой – существенно затрудняет осуществление профилактической и воспитательной работы в отношении таких лиц.

При изучении материалов уголовных дел о преступлениях, совершаемых в киберпространстве, сообщений средств массовой информации о таких посягательствах, результатов анкетирования граждан, были установлены признаки, характерные для жертв отдельных видов преступлений.

Из числа посягательств, механизм преступной виктимизации в которых был запущен активными действиями жертвы в киберпространстве, наиболее часто совершаются мошенничества. В отношении несовершеннолетних распространено вовлечение их в деятельность организаций антиобщественной направленности. Значительно реже встречаются разбойные нападения, грабежи, посягательства против половой неприкосновенности малолетних, доведение до самоубийства.

Российская Федерация столкнулась с проблемами виктимизации пользователей сети «Интернет» в киберпространстве позже других стран, поэтому в работе был изучен накопленный за рубежом опыт противодействия этому явлению. Установлено, что профилактическая деятельность базируется на двух принципиально отличающихся направлениях. Первое, характерное для КНР, заключается в создании развитой системы киберконтроля. Подобный подход демонстрирует высокую эффективность. Однако он требует наличия государственной идеологии, развитой технологической базы, огромных материальных затрат. Позволить себе его полноценную реализацию могут немногие страны. Второе, более экономичное, но менее эффективное направление, характерное для европейских стран, состоит в комплексе мер воспитательно-педагогического характера, привлечении к профилактическим мероприятиям родителей, учителей.

Особняком в этом процессе стоят США, которые обладают уникальным технологическим потенциалом и являются родиной для наиболее крупных технологических сервисов. Эта страна активно использует технические меры предупреждения виктимизации, но и активно формирует информационную повестку как внутри страны так и извне, экспортируя свои национальные ценности и интересы в другие страны.

На основе полученных данных о причинах и условиях криминогенной виктимизации нами были предложены меры общесоциальной профилактики этого явления. Прежде всего необходима разработка информационных ресурсов, способных заменить крупнейшие зарубежные источники и, таким образом, нейтрализовать их виктимогенное влияние, а также обеспечение полноценного информационного суверенитета, под которым понимается способность государства проектировать и производить все компоненты вычислительной техники, образующие технологическую базу киберпространства, разрабатывать национальные операционные системы и программное обеспечение, закрывающие потребности государственных органов и рядовых граждан.

В рамках общесоциальной профилактики необходимо изменить подходы к подготовке пользователей киберпространства, акцентируя внимание на способах обеспечения безопасности личных данных. Важнейшим элементом преодоления правового нигилизма пользователей, способствующего их криминальной виктимизации является отказ государства от очернения любых эпизодов отечественной истории, пересмотр политики финансирования художественных фильмов и театральных постановок.

Специальное предупреждение криминальной виктимизации предусматривает установление ответственности за преследование граждан за обоснованную критику, государственную поддержку разработки программного обеспечения с открытыми исходными кодами, создание отечественной цифровой валюты и ряд других.

Индивидуальное предупреждение криминальной виктимизации пользователей в киберпространстве включает в себя ряд мер, направленных на повышение безопасности обращения с отдельными видами информации, включающих маркировку информации, предполагающую доступ к ней только лиц, достигших определенного возраста и нормативное обеспечение для создания такой системы маркировки. Кроме того предложены меры по правовой регламентации режима использования гражданами социальных сетей, поскольку в текущем виде они не обеспечивают защиту детей от информации, угрожающей их нормальному развитию.

Несомненно, что в условиях стремительного развития компьютерных технологий, пользователи будут сталкиваться с новыми видами угроз их законным правам и интересам, однако, как нам представляется, предложенные в настоящем диссертационном исследовании комплексные меры профилактики при их реализации создадут фундамент для надежной системы обеспечения кибербезопасности.

С учетом изложенного предлагаем следующие меры индивидуальной профилактики криминальной виктимизации пользователей сети «Интернет» в киберпространстве:

1. Разработка и введение в оборот отечественной цифровой валюты, что позволит исключить анонимность финансовых транзакций и снизить, таким образом, виктимность граждан.

2. 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.

3. Организовать доступ несовершеннолетних в сеть «Интернет» по «белым» спискам, в соответствии с которым доступными для них будут только сайты, заранее внесенные в такие списки.

4. 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 Закона о защите детей, 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.

5. Дополнить ч. 2 ст. 10 федерального закона «Об информации, информационных технологиях и о защите информации», регламентирующей обязанности владельцев сайтов сети «Интернет», после слов «которые достаточны для идентификации такого лица» 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”».

6. Дополнить статью 10^3 федерального закона «Об информации,

информационных технологиях и о защите информации» 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».

Тема диссертационного исследования может быть развита по следующим направлениям:

- противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве от новых видов посягательств;

- противодействие криминальной виктимизации отдельных групп пользователей сети «Интернет» в киберпространстве;

- противодействие вовлечения пользователей сети «Интернет» в сообщества антисоциальной направленности.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

Международные правовые акты

1. Декларация основных принципов правосудия для жертв преступления и злоупотребления властью: принята резолюцией 40/34 Генеральной Ассамблеи ООН от 29.11.1985 [Текст] // Международные акты о правах человека: сб. док. – М., 1998. – С. 165.

Нормативно-правовые акты и иные официальные документы Российской Федерации

2. Конституция РФ: принята всенародным голосованием 12 декабря 1993 г. (с изм. и доп. от 14.03.2020, № 1-ФКЗ) [Текст] // Рос. газета. –1993. –25 дек.; СЗ РФ. – 2014. – № 30, ст. 4202.

3. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ (с изм. и доп. от 14 июля 2022 г., № 345-ФЗ) [Текст] // СЗ РФ. – 1996. – № 25, ст. 2954; 2022. – № 29 (ч. III), ст. 5312.

4. Уголовно-процессуальный кодекс РФ от 18 декабря 2001 г. № 174-ФЗ (с изм. и доп. от 14 июля 2022 г., № 346-ФЗ) [Текст] // СЗ РФ. – 2001. – 52 (ч. I), ст. 4921; 2022. – № 29 (ч. III), ст. 5313.

5. Кодекс РФ об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (с изм. и доп. от 14 июля 2022 г., № 291-ФЗ) [Текст] // СЗ РФ. – 2002. – № 1 (ч. I), ст. 1; 2022. – № 29 (ч. III), ст. 5258.

6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. и доп. от 14 июля 2022 г., № 325-ФЗ) «Об информации, информационных технологиях и о защите информации» [Текст] // СЗ РФ. – 2006. – № 31 (ч. II), ст. 3448; 2022. – № 29 (ч. III), ст. 5292.

7. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [Текст] // СЗ РФ. – 2016. – № 28, ст. 4558.

8. Федеральный закон от 12 августа 1995 г. № 144-ФЗ (с изм. и доп. от 28 июня 2022 г., № 202-ФЗ) «Об оперативно-розыскной деятельности» [Текст] // СЗ РФ. – 1995. – № 33, ст. 3349; 2022. – № 27, ст. 4603.

9. Федеральный закон от 2 мая 2006 г. № 59-ФЗ (с изм. и доп. от 27 декабря 2018 г., № 528-ФЗ) «О порядке рассмотрения обращений граждан Российской Федерации» [Текст] // СЗ РФ. – 2006. – № 19, ст. 2060; 2018. – № 53 (ч. I), ст. 8454.

10. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ (с изм. и доп. от 5 апреля 2021 г., № 65-ФЗ) «О защите детей от информации, причиняющей вред их здоровью и развитию» [Текст] // СЗ РФ. – 2011. – № 1, ст. 48; 2021. – № 15 (ч. I), ст. 2432.

11. Федеральный закон от 27 декабря 1991 г. № 32 (с изм. и доп. от 14 июля 2022 г., № 255-ФЗ) «О средствах массовой информации» [Текст] // Ведомости СНД и ВС РФ. – 1992. – № 7, ст. 300; СЗ РФ. – 2022. – № 29 (ч. II), ст. 5222.

12. Федеральный закон от 27 июня 2011 г. № 161-ФЗ (с изм. и доп. от 14 июля 2022 г., № 331-ФЗ) «О национальной платежной системе» [Текст] // СЗ РФ. – 2011. – № 27, ст. 3872; 2022. – № 29 (ч. III), ст. 5298.

13. Федеральный закон от 7 июля 2003 г. № 126-ФЗ (с изм. и доп. от 14 июля 2022 г., № 356-ФЗ) «О связи» [Текст] // СЗ РФ. – 2003. – № 28, ст. 2895; 2022. – № 29 (ч. III), ст. 5323.

14. Доктрина информационной безопасности Российской Федерации (утв. указом Президента РФ от 5 декабря 2016 г. № 646) [Текст] // СЗ РФ. – 2016. – № 50, ст. 7074.

15. Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Утвердить прилагаемую программу «Цифровая экономика Российской Федерации» [Электронный ресурс]. – URL: https://www.garant.ru/products/ipo/prime/doc/71634878/ (дата обращения: 06.05.2021).

16. Распоряжение Правительства РФ от 25 августа 2016 г. № 1791-р [Электронный ресурс]. – URL: http://publication.pravo.gov.ru/Document/View/0001201608290013 (дата обращения: 17.08.2021).

17. 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: утв. постановлением Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд») (с изм. и доп. от 8 августа 2022 г., № 1393) // СЗ РФ. – 2015. – № 47, ст. 6600; 2022. – № 33, ст. 5906.

18. Постановление Пленума Верховного Суда РФ от 29 июня 2010 г. № 17 (с изм. и доп. от 16 мая 2017 г., № 17) «О практике применения судами норм, регламентирующих участие потерпевшего в уголовном судопроизводстве» [Текст] // Бюллетень Верховного Суда РФ. – 2010. – № 9.

Научная литература

19. Gercke, M. Understanding Cybercrime: A Guide for Developing Countries [Text] / M. Gercke. ITU, 2009. 225 p.

20. Walden, I. Computer Crimes and Digital Investigations [Text] / I. Walden, 2006, Chapter 1.29.

21. Алексеев, А.И. Криминологическая профилактика: теория, опыт, проблемы [Текст] / А.И. Алексеев, С.И. Герасимов, А.Я. Сухарев. – М.: Норма, 2001. – 481 с.

22. Варчук, Т.В. Виктимология [Текст] / Т.В. Варчук, К.В. Вишневецкий. – М.: ЮНИТИ-ДАНА, 2017. – 191 с.

23. Гриняев, С.Н. Основы общей теории киберпространства. Теория боя в

киберпространстве [Текст] / С.Н. Гриняев, Д.И. Правиков. – М. : ЦСОиП, 2018. – 121 с.

24. Жданов, Ю.Н. COVID-19: преступность, кибербезопасность, общество, полиция [Текст] / Ю.Н. Жданов, С.К. Кузнецов, В.С. Овчинский. – М.: Международные отношения, 2020. – 448 с.

25. Зиновьева, Н.О. Психология и психотерапия насилия. Ребёнок в кризисной ситуации [Текст] / Н.О. Зиновьева, Н.Ф. Михайлова. – СПб.: Речь, 2003. – 248 с.

26. Иконникова, С.Н. История культурологических теорий [Текст] / С.Н. Иконникова, В.П. Большаков. – СПб.: Питер, 2005. – 474 с.

27. Кабанов, П.А. Криминологическая виктимология : учебное пособие [Текст] / П.А. Кабанов, Р.Р. Маргизов. – Казань: Изд-во Казан. ун-та, 2018. – 117 с.

28. Красиков, А.Н. Сущность и значение согласия потерпевшего в советском уголовном праве [Текст] / А.Н. Красиков. Саратов: Изд-во Сарат. ун-та, 1976. – 121 с.

29. Левин, Я. Интернет как оружие. Что скрывают Google, Tor и ЦРУ. Перевод Леонович М., Напреенко Е. [Текст] / Я. Левин М.: Individuum, 2019. – 360 с.

30. Ленин, В.И. Государство и революция [Текст] / В.И. Ленин : Полн. собр. соч, изд. 5. – Т. 33. – С. 1-120.

31. Майоров, Л.В. Концептуальные основы виктимологического противодействия преступности [Текст] / Л.В. Майоров. – Челябинск: Изд. центр ЮУрГУ, 2013. – 181 с.

32. Ной, И.С. Методологические проблемы советской криминологии [Текст] / И.С. Ной. – Саратов: Изд-во Саратовского ун-та, 1975. – 222 с.

33. Поздняков, Э.А. Философия преступления [Текст] / Э.А. Поздняков. – М.: Интурреклама, 2001. – 575 с.

34. Полубинский, В.И. Фундаментальные и прикладные начала

криминальной виктимологии [Текст] / В.И. Полубинский. – М.: ВНИИ МВД России, 2010. – 227 с.

35. Ривман, Д.В. Криминальная виктимология [Текст] / Д.В. Ривман. – СПб.: Питер, 2002. – 304 с.

36. Смирнов, А.М. Виктимология сексуальных инверсий [Текст] / А.М. Смирнов. – М., 2012. – 141 с.

37. Франк, Л.В. Потерпевшие от преступления и проблемы советской виктимологии [Текст] / Л.В. Франк. – Душанбе: Ирфон, 1977. – 240 с.

38. Эминов, В.Е. Причины преступности в России: криминологический и социально-психологический анализ [Текст] / В.Е. Эминов. – М.: Норма: ИНФРА-М, 2011. – 126 с.

Учебная литература

39. Аванесов, Г.А. Криминология: учебник. 2-е изд., перераб. и доп. [Текст] / Г.А. Аванесов. – М.: Изд-во Акад. МВД СССР, 1984. – 500 с.

40. Бойко, О.А. Актуальные проблемы виктимологии: учебное пособие [Текст] / О.А. Бойко, А.Н. Хоменко, Ю.С. Пестерева, В.В. Бражников. – Омск, 2017. – 240 с.

41. Варыгин, А.Н. Основы криминологии и профилактики преступлений [Текст] / А.Н. Варыгин, В.Г. Громов, О.В. Шляпникова. – М.: Юрайт, 2019. – 165 с.

42. Гилинский, Я.И. Криминология: теория, история, эмпирическая база и социальный контроль. 3-е изд. перераб. и доп. [Текст] / Я.И. Гилинский. – СПб.: Алефпресс, 2014. – 574 с.

43. Горшенков, Г.Н. Криминология. Введение в учебный курс [Текст] / Г.Н. Горшенков. – Сыктывкар: Сыктывк. гос. ун-т, 1995. – 237 с.

44. Ищук, Я.Г. Цифровая криминология: учебное пособие [Текст] / Я.Г. Ищук, Т.В. Пинкевич, Е. С. Смольянинов. – М.: Академия управления МВД России, 2021. – 244 с.

45. Криминология: учебник для вузов [Текст] / под ред. А.И. Долговой. –

3-е изд., перераб. и доп. – М.: Норма, 2005. – 912 с.

46. Криминология: учебник / под ред. Н.Ф. Кузнецовой, В.В. Лунеева. 2-е изд., перераб. и доп. [Текст]. – М.: Волтерс Клувер, 2004. – 640 с.

47. Криминология: учебник для ВУЗов / под ред. В.Д. Малкова [Текст]. – М.: ЗАО «Юстицинформ», 2006. – 528 с.

48. Кудрявцев, В.Н. Криминология [Текст] / В.Н. Кудрявцев, В.Е. Эминов. – М.: Норма, 2009. – 800 с.

49. Курганов, С.И. Криминология [Текст] / С.И. Курганов. – М.: Юннити, 2007. – 184 с.3

50. Наумов, А.В. Российское уголовное право: курс лекций в 2 т. Т. 1: Общая часть. 3-е изд перераб. и доп. [Текст] / А.В. Наумов. – М., Юрид. лит., 2004. – 832 с.

51. Овчинский, В.С. Криминология цифрового мира: учебник для магистратуры [Текст] / В.С. Овчинский. – М.: НОРМА: ИНФРА-М, 2018. – 352 с.

52. Стручков, Н.А. Преступность как социальное явление: лекции [Текст] / Н.А. Стручков. – Л.: Высшее политическое училище им. 60-летия ВЛКСМ, 1979. – 120 с.

Статьи в научных журналах и сборниках

53. Fire, M. Online Social Networks: Threats and Solutions [Текст] / M. Fire // IEEE Communications Surveys & Tutorials. – 2014. – Vol. 16. – No 4. – P. 2019-2036.

54. Leveson, N.G. An investigation of the Therac-25 accidents [Текст] / N.G. Leveson, C.S. Turner // Computer. – 1993. – Vol. 26. – № 7. – P. 18–41.

55. Hussain, M.G. An Approach to Detect Abusive Bangla [Текст] / Hussain, M.G. // International Conference on Innovation in Engineering and Technology (ICIET). – Dhaka, Bangladesh, 2018. – P.1-5.

56. Абельцев, С.Н. О личности преступника и практической значимости её изучения [Текст] / С.Н. Абельцев // Вестник Тамбовского государственного

университета. – № 2. – 2000. – С. 83-85.

57. Антонян, Ю.М. Бессознательное в корыстном преступном поведении [Текст] / Ю.М. Антонян // Общество и право. – 2015. – № 2. – С. 120-126.

58. Антонян, Е.А. Кибервиктимность [Текст] / Е.А. Антонян, Е.Н.Клещина // Вестник Пермского института ФСИН России. – 2019. – № 3. – С. 5-10.

59. Антонян, Е.А. Международное сотрудничество в сфере противодействия крибертерроризма [Текст] / Е.А. Антонян // Правовой альманах. – 2022. – № 2. – С. 9-14.

60. Антонян, Е.А. Противодействие киберпреступности [Текст] / Е.А. Антонян, Е.В. Бархатова // Евразийский союз ученых. – 2019. – № 7-4. – С. 54-57.

61. Антонян, Е.А. Блокчейн-технологии в противодействии кибертерроризму [Текст] / Е.А. Антонян, И.И. Аминов // Актуальные проблемы российского права. – 2019. – № 6. – С. 167-177

62. Антропов, Р.В. Система социального рейтинга в Китае: прогрессивный механизм поощрения и наказания или цифровая диктатура? [Текст] / Р.В. Антропов, И.И. Лиценберг //Актуальные проблемы развития КНР в процессе её регионализации и глобализации: сб. науч. тр. по матер. XII междунар. науч.-практ. конф. – Чита: Забайкальский государственный университет, 2020. – С. 20-27.

63. Бахрах, Д.Н. Вопросы административно-процессуального статуса потерпевшего в производстве по делам об административных правонарушениях [Текст] / Д.Н. Бахрах, Е.С. Герман // Современное право. – 2010. – № 5. – С. 114-119.

64. Белицкий, В.Ю. Предупреждение совершения мошенничеств участковым уполномоченным полиции [Текст] / В.Ю. Белицкий // Вестник Барнаульского юридического института МВД России. – 2017. – № 2. – С. 132-133.

65. Блувштейн, Ю.Д. Понятие личности преступника [Текст] / Ю.Д. Блувштейн // Советское государство и право. – 1979. – № 8. – С. 97-102.

66. Богданов Н.Н. Дерматоглифика пишущих левой [Текст] / Н.Н. Богданов // Вопросы психологии – 1997. – № 2. – С. 76 – 87.

67. Богданов, Н.Н. Дерматоглифика серийных убийц [Текст] / Н.Н. Богданов, С.С. Самищенко, А.И. Хвыля-Олинтер // Вопросы психологии. – 1998. – № 4. – С. 64.

68. Бойко, О.А. Детерминанты латентных преступлений, совершаемых с использованием информационно-коммуникационных технологий [Текст] / О.А. Бойко, А.С. Унукович // Юридический вестник Самарского университета. – 2020. – № 3. – С. 53-59.

69. Бородакий, Ю.В. Инсайдерология – наука о нелегитимности в компьютерной инфосфере [Текст] / Ю.В. Бородакий, А.Ю. Добродеев, Б.П. Пальчун, М.Н. Болдина // Известия ЮФУ. Технические науки. – 2008. – № 8. – С. 55-64.

70. Бочков, А.А. Виктимологическая культура: теория и практика [Текст] / А.А. Бочков // Право. Экономика. Психология. – 2016. – № 2. – С. 3-9.

71. Бутусова, Л.И. К вопросу о киберпреступности в международном праве [Текст] / Л.И. Бутусова // Вестник экономической безопасности. – 2016. – № 2. – С. 48-52.

72. Бухарин, В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности [Текст] / В.В. Бухарин // Вестник МГИМО-Университета. – 2016. – № 6. – С.76-91.

73. Бытко, С.Ю. Оценка эффективности уголовного наказания за педофилию [Текст] / С.Ю. Бытко // Юридическая наука и правоохранительная практика. – 2016. – № 2. – С. 54-58.

74. Вакуленко, Н.А. Актуальность мер виктимологической профилактики карманных краж как важного компонента предупреждения преступлений [Текст] / Н.А. Вакуленко // Юристъ-Правоведъ. – 2020. – № 4 (95). – С. 65-70.

75. Василенко, А.И. История зарождения интернета и основные пути его развития [Текст] / А.И. Василенко // Новая наука: Опыт, традиции, инновации. – 2016. – № 3-2 (71). – С. 164-166.

76. Вепрев, С.Б. Киберпреступность как новая форма преступности [Текст] / С.Б. Вепрев, С.А. Нестерович // Расследование преступлений: проблемы и пути их решения. – 2018. – № 3. – С. 78–82.

77. Верина, Г.В. Об истоках современных концепций объекта преступления [Текст] / Г.В. Верина // Уголовное право. – 2016. – № 1. – С. 4-7.

78. Верник, А.Г. Цензура в Интернете: исторический аспект, современный опыт и перспективы [Текст] / А.Г. Верник // Дискуссия. – 2014. – № 11. – С. 174-182.

79. Вишневецкий, К.В. Механизм виктимологической детерминации [Текст] / К.В. Вишневецкий // Теория и практика общественного развития. – 2014. – № 10. С.154-157.

80. Вишневецкий, К.В. Социальный аспект криминальной виктимологии [Текст] / К.В. Вишневецкий // Гуманитарные, социально-экономические и общественные науки. – 2021. – № 3. – С. 136-140.

81. Вишневецкий, К.В. Влияние инновационных технологий на сферу предупреждения преступности [Текст] / К.В. Вишневецкий, А.А. Кашкаров// Гуманитарные, социально-экономические и общественные науки. – 2021. – № 3. – С. 136-140.

82. Вишневецкий, К.В. Виктимологическая характеристика личности жертвы доведения до самоубийства [Текст] / К.В. Вишневецкий, В.В. Доев // Гуманитарные, социально-экономические и общественные науки. 2020. № 6. С. 109-113.

83. Воронцова, С.В. Киберпреступность: проблемы квалификации преступных деяний [Текст] / С.В. Воронцова // Российская юстиция. – 2011. – № 2. – С. 14.

84. Городничев, С.В. Система социального рейтинга в Китае [Текст] /

С.В. Городничев, П.Г. Герасимова // Вестник Тульского филиала Финуниверситета. – 2020. – № 1. – С. 134-136.

85. Графов, Д.Б. Система социального рейтинга в КНР как информационно-коммуникационная технология поощрения и наказания [Текст] / Д.Б. Графов // Власть. – 2020. – № 2. – С. 250-259.

86. Давитадзе, М.Д. Современные проблемы уголовной политики [Текст] / М.Д. Давитадзе // Вестник Московского университета МВД России. – 2018. – № 6. – С. 123-127.

87. Долженко, Н.И. К вопросу о содержательных аспектах киберпреступности [Текст] / Н.И. Долженко, И.Г. Хмелевская // Nomothetika: Философия. Социология. Право. – 2020. – Т. 45. – № 2. – С. 315-322.

88. Егоров, Н.С. Человек в социальных сетях киберпространства [Текст] / Н.С. Егоров, В.Г. Туркина // Современные научные исследования и разработки. – 2018. Т. 1. – № 4. – С. 196-198.

89. Желудков, М.А. Особенности противодействия киберпреступности в России и зарубежных странах [Текст] / М.А. Желудков, А.М. Попов, М.М. Дубровина // Вестник Волгоградской академии МВД России. – 2018. – № 3. – С. 97-102.

90. Жихарева, Л.В. Особенности эмоциональной привязанности у подростков, склонных к девиантной виктимности [Текст] / Л.В. Жихарева // Научный результат. Педагогика и психология образования. – 2018. – Т. 4, № 4. – С. 96-106.

91. Зайцев, И.Н. Тотальность медийного пузыря [Текст] / И.Н. Зайцев // Научная сессия ГУАП: сб. докл. научной сессии, посвященной Всемирному дню авиации и космонавтики. В 3 ч. / под общ. ред. Ю.А. Антохиной. – СПб., 2019. – С. 99-103.

92. Зинцова, А.С. Социальная профилактика кибербуллинга [Текст] / А.С. Зинцова // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. – 2014. – № 3. – С. 122-128.

93. Ищенко, Е.П. О криминалистическом обеспечении раскрытия и расследования киберпреступлений [Текст] / Е.П. Ищенко // Деятельность правоохранительных органов в современных условиях: сб. матер. 20 междунар. науч.-практ. конф. (28-29 мая 2015 г.). В 2 т. Т. 1. – Иркутск: Изд-во Вост.-Сиб. ин-та МВД России, 2015. С. 336-341.

94. Калиниченко, В.Н. Принцип работы блокчейн [Текст] / В.Н. Калиниченко, В.Ю. Кондратьев // Цифровизация экономики: направления, методы, инструменты. сб. ст. по матер. II всерос. науч.-практ. конф. – Краснодар, 2020. – С. 219-221.

95. Качурова, Е.С. Современные возможности индивидуального виктимологического предупреждения преступности // Проблемы современного законодательства России и зарубежных стран: матер. VIII междунар. науч.-практ. конф. [Текст] / Е.С. Качурова. – Иркутск: Иркутский институт (филиал) ВГУЮ (РПА Минюста России), 2019. – С. 320-323.

96. Клещина, Е.Н. Понятие, значение и структура личности жертвы преступления [Текст] / Е.Н. Клещина // Вестник Московского университета МВД России. – 2010. – № 4. – С. 129-130.

97. Климович, А.П. Влияние цифровых технологий на современное общество. Пример системы рейтинга социального кредита в Китае [Текст] / А.П. Климович // Цифровая социология. – 2020. – Т. 3. – № 3. – С. 35-44.

98. Козлов, А.В. Проблемы правового ограничения анонимности граждан в сети Интернет [Текст] / А.В. Козлов // Стратегические коммуникации в современном мире: сб. матер. по результатам науч.-практ. конф.: Пятой и Шестой междунар. науч.-практ. конф., Четвертой и Пятой всерос. науч.-практ. конф. – Саратов: Саратовский источник. – 2018. – С. 172-178.

99. Козлова, О.Е. Перспективы применения положительного опыта зарубежных стран в борьбе с киберпреступностью в Российской Федерации [Текст] / О.Е. Козлова, А.В. Самойлова, Э.В. Твердохлебова // Актуальные научные исследования в современном мире. – 2020. – № 8-5. – С. 42-47.

100. Короткова, Н.А. Виктимологическая профилактика преступлений против половой неприкосновенности несовершеннолетних, совершаемых с использованием сети Интернет [Текст] / Н.А. Короткова // Научные достижения и открытия современной молодёжи: сб. ст. по матер. II междунар. науч.-практ. конф. – Новосибирск, 2017. – С. 225-228.

101. Кот, Я.И. Нравственные аспекты свободы в киберпространстве [Текст] / И.Я. Кот // Гуманитарный вестник. – 2018. – № 11. – С. 1.

102. Курицына, Е.В. Преступность в советском обществе в 1953–1964 гг. (социально–криминологический аспект) [Текст] / Е.В. Курицына // Известия Пензенского государственного педагогического университета им. В.Г. Белинского. – 2007. – № 3. – С. 115-120.

103. Лопашенко, Н.А. Административной преюдиции в уголовном праве – нет! [Текст] / Н.А. Лопашенко // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2011. – № 3. – С. 64-71.

104. Лунтовская, М.А. Технологии блокчейн: понятие и принципы работы [Текст] / М.А. Лунтовская // Ученые записки Российской Академии предпринимательства. – 2020. – Т. 19, № 2. – С. 72-80.

105. Мавричев, А.А. Система социального рейтинга в Китае: миф или реальность [Текст] / А.А. Мавричев, Е.А. Макаров, А.В. Дьяконенко, М.Б. Хрипунова // Наука Красноярья. – 2021. – Т. 10. – № 4-2. – С. 59-66.

106. Майоров, А.В. Виктимологический аспект мошенничества [Текст] / А.В. Майоров Н.Е. Яременко // Виктимология. – 2019. – № 3. – С. 36-41.

107. Моторина, И.Е. Позитивные и негативные аспекты становления инфосферы [Текст] / И.Е. Моторина // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2011. – № 8-4. – С. 134-137.

108. Нестерова, А.А. Психологические особенности детей, склонных к виктимности в ситуации школьной травли [Текст] / А.А. Нестерова // Личность в экстремальных условиях и кризисных ситуациях жизнедеятельности. – 2015.

– № 5. – С. 277-285.

109. Никулин, Д.В. Профилактика мошенничества в сфере глобальной сети Интернет и средств массовой информации. Виктимологический аспект [Текст] / Д.В. Никулин // Аллея науки. – 2018. – Т. 6, № 6. – С. 786-794.

110. Номоконов, В.А. Киберпреступность как новая криминальная угроза [Текст] / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 1. – С. 45–55.

111. Пацкевич, А.П. Криминалистическое исследование способа совершения карманных краж [Текст] / А.П. Пацкевич // Борьба с преступностью: теория и практика: тез. докл. IX междунар. науч.-практ. конф. – Могилев, 2021. – С. 261-264.

112. Пинкевич, Т.В. Легализация криптовалюты в россии: за и против [Текст] / Т.В. Пинкевич // Уголовная политика и правоприменительная практика : сб. матер. V междунар. науч.-практ. конф. – СПб.: Петрополис, 2018. – С. 292-302.

113. Пушмин, И.И. Детерминанты виктимизации жертв мошенничеств [Текст] / И.И. Пушмин // Научный форум: юриспруденция, история, социология, политология и философия: сб. ст. по матер. XVII междунар. науч.-практ. конф. – 2018. – № 4. – С. 69-76.

114. Роговский, Е.А. Политика США по обеспечению безопасности киберпространства [Текст] / Е.А. Роговский // США и Канада: экономика, политика, культура. – 2012. – № 6. – С. 3-22.

115. Родина, Е.А. Общесоциальная профилактика криминогенной виктимизации пользователей сети Интернет [Текст] / Е.А. Родина // Вестник Саратовской государственной юридической академии. – 2022. – № 3. – С. 197-206.

116. Родина, Е.А. Киберпространство как криминологическая категория [Текст] / Е.А. Родина // Вестник Казанского юридического института МВД России. – 2021. – № 1. – С. 66-71.

117. 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 2021 г.). – М.: МФЮА, 2021. – С. 163-172.

118. Родина, Е.А. Виктимологическое предупреждение преступлений в киберпространстве [Текст] / Е.А. Родина // Актуальные проблемы государства и права. – 2021. – № 19. – С. 510-524.

119. Сабитов, Р.А. Соотношение понятий «потерпевший от преступления», «пострадавший от преступления» и «жертва преступления» [Текст] / Р.А. Сабитов // Виктимология. – 2014. – № 1. – С. 17-26.

120. Савиных, Е.В. Основные направления и проблемы виктимологической профилактики преступности [Текст] / Е.В. Савиных // Виктимология. – 2014. – № 1. – С. 51-54.

121. Сафуанов, Ф.С. Особенности личности жертв противоправных посягательств в Интернете [Текст] / Ф.С. Сафуанов, Н.В. Докучаева // Психология и право. – 2015. – Т. 5, № 4. – С. 80–93.

122. Свищёв, А.В. Понятие распределенных реестров и принцип работы блокчейн [Текст] / А.В. Свищёв, А.В. Хлоповская // Моя профессиональная карьера. – 2021. – Т. 1, № 23. – С. 210-216.

123. Семерикова, А.А. Криминологический анализ жертвы сексуального насилия [Текст] / А.А. Семерикова // Юридические исследования. – 2018. – № 7. – С. 28-41.

124. Сидоренко, Э.Л. Криптовалюта как новый юридический феномен [Текст] / Э.Л. Сидоренко // Общество и право. – 2016. – № 3. – С. 193-197.

125. Сидоренко, Э.Л. Наркотики и криптовалюта: мировые криминологические тренды [Текст] / Э.Л. Сидоренко // Наркоконтроль. – 2018. – № 2. – С. 8-13.

126. Ситкова, О.Ю. Современное состояние зарубежных научных исследований о безопасности детей в информационно-коммуникационной среде [Текст] / О.Ю. Ситкова, Л.В. Шварц // Правовая политика и правовая жизнь. – 2020. – № 2. – С. 76-87.

127. Скурихина, А.А. Виктимность в сфере компьютерных преступлений [Текст] / А.А. Скурихина, О.С. Ронжина // Виктимология. – 2014. – № 2. – С. 48-50.

128. Скоков, И.Е. Элементы оперативно-розыскной характеристики карманных краж // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований: матер. регион. науч.-практ. конф. [Текст] / И.Е. Скоков – СПб.: Изд-во Санкт-Петерб. ун-та МВД России, 2020. – С. 203-207.

129. Уразалиев, М. Вопросы криминализации общества в условиях пандемии – новые угрозы и вызовы [Текст] / М. Уразалиев // Review of law sciences. – 2020. – С. 192-197.

130. Фадеев, В.Н. Причинность в криминологии и детерминация преступности [Текст] / В.Н. Фадеев // Криминология: вчера, сегодня, завтра. – 2017. – № 3. – С. 21-27.

131. Федотов, М.А. Киберпространство как сфера обитания права [Текст] / В.Н. Федотов // Бюллетень ЮНЕСКО по авторскому праву. – 1998. – № 2 (т. XXXII).

132. Харитонов, А.О. Системный подход к исследованию корпоративной виктимизации [Текст] / А.О. Харитонов, Н.М. Александрина // Современная экономика: актуальные вопросы, достижения и инновации: сб. ст. IX междунар. науч.-практ. конф. – Пенза: МЦНС «Наука и Просвещение», 2017. – С. 228-230.

133. Хмель, П.С. Правовое регулирование медицинского киберпространства [Текст] / П.С. Хмель // Актуальные вопросы современной медицины: матер. II Дальневосточного медицинского молодежного форума /

под ред. Е.Н. Сазоновой. – Хабаровск: Изд-во Дальневосточного гос. мед. ун-та (Хабаровск), 2018. – С. 147-149.

134. Хромой, Б.П. История развития вычислительной техники и связи [Текст] / Б.П. Хромой // T-Comm: Телекоммуникации и транспорт. – 2016. – Т. 10, № 3. – С. 82-88.

135. Чекменёва, Т.Г. Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты [Текст] / Т.Г. Чекменёва, Б.А. Ершов, С.Д. Трубицын, А.А. Остапенко // Бюллетень социально-экономических и гуманитарных исследований. – 2020. – № 7. – С. 78-97.

136. Шабаев М.Б. Как работает VPN и обзор лучших VPN провайдеров [Текст] / М.Б. Шабаев, М.М. Матыгов // Тенденции развития науки и образования. – 2020. – № 68-1. – С. 140-142.

137. Шалагин, А.Е. О приоритетных направлениях деятельности органов внутренних дел по предупреждению преступлений и административных правонарушений [Текст] / А.Е. Шалагин // Вестник экономики, права и социологии. – 2014. – № 2. – С. 153-157.

138. Шалагин, А.Е. Предупреждение преступлений в эпоху цифровизации [Текст] / А.Е. Шалагин, А.Д. Идиятуллов // Державинские чтения: сб. ст. XVI междунар. науч.-практ. конф. – М., 2021. – С. 385-387.

139. Шалагин, А.Е. Детерминирующие факторы противоправного поведения подростков и молодежи [Текст] / А.Е. Шалагин, А.Д. Идиятуллов, И.А. Шалагин// Евразийское Научное Объединение. – 2021. – № 7-2. – С. 154-158.

140. Шалагин, А.Е. Криминологическая характеристика и предупреждение преступлений, связанных с побуждением к суициду, совершаемых с использованием информационно-коммуникационной сети «Интернет» [Текст] / А.Е. Шалагин, А.Д. Идиятуллов // Ученые записки Казанского юридического института МВД России. – 2018. – Т. 3. – С. 82-88.

141. Шаргородский, М.Д. Преступность, ее причины и условия в

социалистическом обществе [Текст] / М.Д. Шаргородский // Преступность и ее предупреждение: сб. ст. – Л.: Лениздат, 1966. – С. 20-58.

142. Шаров, Д.В. соотношение уголовно-процессуального и уголовно-правового понятий потерпевшего: проблемы и пути их решения [Текст] / Д.В. Шаров // Вестник Московского университета МВД России. – 2013. – № 7. – С. 79-81.

143. Шведова, В.О. Цифровые идентификаторы личности как новый источник социальной дискриминации [Текст] / В.О. Шведова // Социальная интеграция и развитие этнокультур в евразийском пространстве. – 2020. – Т. 3. – № 9. – С. 239-244.

144. Шейнов, В.П. Разработка теста «психологические факторы риска виктимизации взрослого индивида [Текст] / В.П. Шейнов // Системная психология и социология. – 2018. – № 3. – С. 14-25.

145. Шкорубская, Е.Г. Коммуникативное пространство сети Интернет: бунт против анонимного избытка информации [Текст] / Е.Г. Шкорубская // Учёные записки Крымского федерального университета имени В.И. Вернадского. Философия. Политология. Культурология. – 2018. – Т. 4 (70). – № 4. – С. 86-99.

146. Яковлев, А.М. Об изучении личности преступника [Текст] / А.М. Яковлев // Советское государство и право. – 1962. – № 11. – С. 109-110.

Диссертации и авторефераты диссертаций

147. Бытко, С.Ю. Эффективность предупредительного воздействия уголовного наказания на преступность: теоретический и прикладной аспекты: дис. … д-ра юрид. наук [Текст] / С.Ю. Бытко. – Саратов, 2018. – 471 с.

148. Бытко, С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис. ... канд. юрид. наук [Текст] / С.Ю. Бытко. – Саратов, 2002. – 190 с.

149. Демидова-Петрова, Е.С. Преступность несовершеннолетних в современной России: теоретико-методологические и прикладные проблемы ее

познания и предупреждения: дис. … д-ра юрид. наук. [Текст] / Е.С. Демидова-Петрова. – Казань, 2019. – 625 с.

150. Комаров, А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: автореф. дис. … канд. юрид наук [Текст] / А.А. Комаров. – Саратов, 2011. – 25 с.

151. Новиков, В.П. Физические и юридические лица как потерпевшие по делам об административных правонарушениях: автореф. дис. … канд. юрид. наук [Текст] / В.П. Новиков. – М., 2004. – 22 с.

152. Простосердов, М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. [Текст] / М.А. Простосердов. – М., 2016. – 232 с.

153. Семченков, И.П. Объект преступления: социально-философские и методологические аспекты проблемы: автореф. дис. ... канд. юрид. наук [Текст] / И.П. Семченков. – М., 2003. – 24 с.

154. Тропина, Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. ... канд. юрид. наук [Текст] / Т.Л. Тропина. – Владивосток, 2005. – 26 с.

155. Шатилов, А.В. Особенности криминологической характеристики и предупреждения мошенничества, совершаемого организованными преступными формированиями: дис. ... канд. юрид. наук [Текст] / А.В. Шатилов. – Саратов, 2019. – 210 с.

156. Шевченко, Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … канд. юрид. наук [Текст] / Е.С. Шевченко. – М., 2016. – 249 с.

Материалы правоприменительной практики

157. Определение Конституционного Суда РФ от 5 декабря 2019 г. № 3272 «Об отказе в принятии к рассмотрению жалобы гражданина Москалева Михаила Васильевича на нарушение его конституционных прав частью первой статьи 128.1 Уголовного кодекса Российской Федерации и статьей 318

Уголовно-процессуального кодекса Российской Федерации» [Электронный ресурс] // Официальный сайт Конституционного Суда РФ. URL: http://doc.ksrf.ru/decision/KSRFDecision445450.pdf (дата обращения: 24.04.2021).

158. Постановление Девятого арбитражного апелляционного суда г. Москва от 29 июня 2016 г. № 09АП-4829/2016г по делу № А40-120498/1 [Электронный ресурс] // Электронное правосудие. – URL: https://kad.arbitr.ru/Document/Pdf/aefaed33-b367-4655-ab56-43934ee99872/6fae96aa-309b-41ae-80d6-2cf8f5b1dabc/A40-120498-2015_20160629_Postanovlenie_apelljacionnoj_instancii.pdf?isAddStamp=True (дата обращения: 28.12.2020).

159. Определение арбитражного суда г. Москвы от 20 мая 2019 г. № А40-35771/18-71-46Б [Электронный ресурс] // Электронное правосудие. URL: https://kad.arbitr.ru/Document/Pdf/296a7187-edad-4920-acf0-6fedb0a95482/f1f8baf6-4ca6-448e-a231-368566f75c06/A40-35771-2018_20190520_Opredelenie.pdf?isAddStamp=True (дата обращения: 17.08.2021).

160. Решение Кочевского районного суда Пермского края от 24 июня 2019 г. по делу № 2-154/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/KBWb1jyJj8Ya (дата обращения: 17.08.2021).

161. Решение Кировского районного суда г. Астрахани от 28 декабря 2017 г. по делу № 2-4076/2017 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/2rZp67WDk05x/?&regular-judge=&_=1610876551133 (дата обращения: 17.01.2021).

162. Решение Первореченского районного суда г. Владивостока (Приморский край) по делу № 2-2409/2016 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/wYbYK2yGMx1m/?regular-judge=&_=1629717705515 (дата обращения: 23.08.2021).

163. Решение Первореченского районного суда г. Владивостока (Приморский край) по делу № 2-2414/2016 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/amZLetyb8NrT/

?&regular-judge=&_=1629717865756 (дата обращения: 23.08.2021).

164. Уголовное дело № 1/97-2012 // Архив Октябрьского районного суда г. Иркутска за 2012 г.

165. Уголовное дело № 1-368/2018 // Архив Калининского районного суд г.Тюмени за 2018 г.

166. Уголовное дело № 1-400/2016 // Архив Тосненского городского суда Ленинградской области за 2016 г.

167. Уголовное дело № 1-407/2019 1-51/2020 // Архив Центрального районного суда г. Воронежа за 2020 г.

168. Уголовное дело № 1-97/2012 // Архив Октябрьского районного суда г. Иркутска за 2012 г.

169. Уголовное дело № 1-191/2017 // Архив Октябрьского районного суда г. Рязани за 2017 г.

170. Уголовное дело № 1-25/2016 // Архив Ингодинского районного суда г. Читы за 2016 г.

171. Уголовное дело № 1-368/2018 // Архив Калининского районного суда г. Тюмени за 2018 г.

172. Уголовное дело № 1-281/2017 // Архив Калужского районного суда за 2017 г.

173. Уголовное дело № 1-98/2020 // Архив Лазаревского районного суда г. Сочи (Краснодарский край) за 2020 г.

174. Уголовное дело № 1-339/2020 // Архив Усть-Илимского городского суда (Иркутская область) за 2020 г.

175. Уголовное дело № 1-24/2019 // Архив Ленинского районного суда г. Севастополь за 2019 г.

176. Уголовное дело № 1-25/2018 // Архив Судакского городского суда Республики Крым за 2018 г.

Справочная литература

177. Бытко, Ю.И. Сборник нормативных актов по уголовному праву

России X-XX веков [Текст] / Ю.И. Бытко, С.Ю. Бытко. – Саратов: Научная книга, 2006. – 786 с.

178. Даль, В.И. Словарь живого великорусского языка [Текст] / В.И. Даль: в 4 т. Т. 3. – М.: Славянский Дом Книги, 2006. – 896 с.

179. Ожегов, С.И. Толковый словарь русского языка. [Текст] / С.И. Ожегов, Н.Ю. Шведова. – М: ООО «А ТЕМП», 2006. – 944 с.

180. Философский энциклопедический словарь [Текст] – М.: Сов. энциклопедия, 1983. – 840 с.

181. Шапошников, А.К. Этимологический словарь современного русского языка [Текст] / А.К. Шапошников. В 2 т. Т. 1. – М.: Флинта, 2010. – 584 с.

Статьи в средствах массовой информации

182. Warrell, H. Cyber criminals exploit coronavirus disruption. [Текст] / Helen Warrell, Nic Fildes. – Financial Times. – 2020. – March 16.

183. Никифорова, Н. «Фейсбук» – проект ЦРУ... Но разве в этом кто-нибудь сомневается? [Текст] / Н. Никифорова // Взгляд. – 2016. – 27 авг.

184. Фалалеев, М. Запретный секс. Педофилов ловят в сети на «веселые картинки» [Текст] / М. Фалеев // Российская газета. – 2011. – 23 ноября.

185. Варывдин, М. «У нас должна быть обратная связь с людьми». Генпрокурор Игорь Краснов о том, как, надзирая за законностью, помогать гражданам [Текст] / М. Варывдин // Коммерсантъ. – 2019. – № 164.

186. Петров, И. Затишье перед бурей: как COVID-2019 повлияет на преступность [Текст] / И. Петров // Известия. – 2020. – 26 марта.

187. Хвостик, Е. Бедность и низкая компьютерная грамотность тормозят развитие интернета [Текст] / Е. Хвостик // Коммерсант. – 2019. – 5 ноября.

188. У каждого была своя правда. Сергей Иванов открыл мемориальную доску в честь Карла Маннергейма [Текст] // Российская газета. – 2016. – 16 июня.

189. Черноусов, И. Названы основные способы мошенничества по

телефону и в Сети [Текст] // Российская газета. – 2020. – 1 декабря.

Ресурсы сети «Интернет»

190. Barbaschow A. VPNs can still be used in China despite March 31 ban [Электронный ресурс]. – URL: https://www.zdnet.com/article/vpns-can-still-be-used-in-china-despite-march-31-ban/ (дата обращения: 10.08.2021).

191. Coronavirus: The impact on crime and criminal networks [Электронный ресурс]. URL: https://globalinitiative.net/analysis/crime-contagion-impact-covid-crime/ (дата обращения: 14.11.2021).

192. Jason Morris, Ingolf Becker, Simon Parkin. In Control with no Control: Perceptions and Realityof Windows 10 Home Edition Update Features [Электронный ресурс]. – URL: https://www.ndss-symposium.org/wp-content/uploads/2019/02/usec2019_02-5_Morris_paper.pdf (дата обращения: 20.08.2021).

193. Interview mit dem Kannibalen von Rotenburghttps [Электронный ресурс]. – URL: www.welt.de/fernsehen/article1269371/Interview-mit-dem-Kannibalen-von-Rotenburg.html (дата обращения 27.12.2019).

194. Cryptocurrency statistics [Электронный ресурс]. – URL: https://bitinfocharts.com/ (дата обращения: 09.05.2021).

195. Lapidus A. Ann Linde lurad av ryska bluffmakare [Электронный ресурс]. – URL: https://www.expressen.se/nyheter/ann-linde-lurad-av-ryska-bluffmakare/ (дата обращения: 08.08.2021).

196. Lost or Stolen Credit, ATM, and Debit Cards [Электронный ресурс]. – URL: https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards (дата обращения: 28.12.2020).

197. Skills Matter: Further Results from the Survey of Adult Skills, OECD Skills Studies, OECD Publishing, Paris, [Электронный ресурс]. – URL:https://doi.org/10.1787/9789264258051-en (дата обращения: 20.08.2021).

198. Trevor Cradduck LINAC deaths at Zaragoza // The RISKS Digest Volume 11 Issue 18. [Электронный ресурс]. – URL:

http://catless.ncl.ac.uk/Risks/11.18.html#subj6.1 (дата обращения: 20.08.2021).

199. Van Hee C., Jacobs G., Emmery C., Desmet B., Lefever E., Verhoeven B. et al. (2018) Automatic detection of cyberbullying in social media text // PLoS ONE 13(10): e0203794. https://doi.org/10.1371/journal.pone.0203794 [Электронный ресурс]. – URL: https://doi.org/10.1371/journal.pone.0203794 (дата обращения: 12.08.2021).

200. Google передает американским правоохранителям данные о пользователях, находившихся рядом с местами преступлений [Электронный ресурс]. – URL: https://www.newsru.com/hitech/16apr2019/google_data.html (дата обращения: 14.08.2021).

201. Акимов Н. Вынесен приговор следователям ФСБ, бравшим взятку криптовалютой [Электронный ресурс]. – URL: https://legal.report/vynesen-prigovor-sledovatelyam-fsb-bravshim-vzyatku-kriptovaljutoj/ (дата обращения: 09.05.2021).

202. Аналитики сообщили об ускорении роста аудитории платного ТВ в России на 25% [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/4683284 (дата обращения: 18.08.2021).

203. Ахмед Н. Как ЦРУ создавало Google [Электронный ресурс]. – URL: https://d-russia.ru/kak-cru-sozdavalo-google.html (дата обращения: 16.08.2021);

204. Банки и операторы запустят сервисы против подмены номеров мошенниками [Электронный ресурс]. – URL: https://www.rbc.ru/society/12/12/2020/5fd446c49a7947746aba6e19 (дата обращения: 28.12.2020).

205. Березина Е. Facebook будет автоматически блокировать нежелательную информацию [Электронный ресурс]. – URL: https://rg.ru/2016/12/02/facebook-budet-avtomaticheski-blokirovat-nezhelatelnuiu-informaciiu.html (дата обращения: 14.08.2021).

206. Би-би-си узнала о передаче маршрутов первых лиц России через WhatsApp [Электронный ресурс]. – URL:

https://www.rbc.ru/politics/31/12/2020/5fedf4ad9a79470caa864a2f (дата обращения: 17.08.2021).

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

208. В Астрахани мужчина признан виновным в развращении детей. [Электронный ресурс]. – URL: https://astra-novosti.ru/v-astraxani-muzhchina-priznan-vinovnym-v-razvrashhenii-detej/ (дата обращения: 17.01.2021).

209. В ГД внесены законопроекты об использовании QR-кодов в общественных местах и на транспорте [Электронный ресурс]. URL: http://duma.gov.ru/news/52707/ (дата обращения: 14.11.2021).

210. В Китае вступает в силу резонансный закон о кибербезопасности. [Электронный ресурс]. – URL: https://ria.ru/20170601/1495523455.html (дата обращения 21.07.2020).

211. В Приморье экс-борца с наркотиками будут судить за взятку в биткоинах [Электронный ресурс]. – URL: https://ria.ru/20201021/bitkoin-1580777237.html (дата обращения: 09.05.2021).

212. Вершинин И. Операции без согласия клиента банка: практика по предотвращению [Электронный ресурс]. – URL: https://bosfera.ru/bo/operacii-bez-soglasiya-klienta-banka-praktika-po-predotvrashcheniyu (дата обращения: 28.12.2020).

213. Гражданский кодекс КНР / пер. П.В. Бажанова [Электронный ресурс]. – URL: https://chinalaw.center/civil_law/china_civil_code_2020_russian/ (дата обращения: 10.08.2021).

214. Грег Кенн. Насколько сложный программный код у Windows? [Электронный ресурс]. – URL: https://www.zeluslugi.ru/info-czentr/stati/programmnyy-kod-windows (дата обращения: 20.08.2021).

215. Гусев А. В Калужской области снизился возраст пострадавших от

интернет-мошенничеств [Электронный ресурс]. – URL: https://kgvinfo.ru/novosti/obshchestvo/v-kaluzhskoy-oblasti-pomolodel-vozrast-postradavshikh-ot-internet-moshennichestv/ (дата обращения: 27.07.2021).

216. Дикарев В. Цветы, которые нам не нравятся [Электронный ресурс]. – URL: https://craftkino.ru/sostojanie-rossiyskogo-kino/ (дата обращения: 17.08.2021).

217. Ельцин-центр потребовал реабилитации власовцев, назвав их «диссидентами 40-х годов» [Электронный ресурс]. – URL: https://www.rline.tv/news/2016-12-15-eltsin-tsentr-potreboval-reabilitatsii-vlasovtsev-nazvav-ikh-dissidentami-40-kh-godov/ (дата обращения: 17.08.2021).

218. Запрещённое в России движение АУЕ насчитывает до 34 тыс. приверженцев в 40 регионах [Электронный ресурс]. – URL: https://tass.ru/obschestvo/9218777 (дата обращения: 19.08.2021).

219. Ефимович Е. «Россия 1» стала ударником пятилетки [Электронный ресурс]. – URL: https://www.rbc.ru/newspaper/2020/12/08/5fca6f359a79470a0b53912a (дата обращения: 18.08.2021).

220. Игнатов Г. 20 лет Википедии: как российская Вики превратилась в рассадник лжи и русофобии [Электронный ресурс]. – URL: https://jpgazeta.ru/20-let-vikipedii-kak-rossijskaya-viki-prevratilas-v-rassadnik-lzhi-i-rusofobii/ (дата обращения: 15.08.2021).

221. Как росло количество веб-сайтов в мире [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/4147760 (дата обращения 20.07.2020).

222. Катастрофические последствия программных ошибок [Электронный ресурс]. – URL: https://habr.com/ru/company/mailru/blog/370153/ (дата обращения: 20.08.2021).

223. Клевошин П. Минцифры отказалось от фильтра интернет-трафика для детей [Электронный ресурс]. – URL: https://www.vedomosti.ru/technology/articles/2020/11/22/847846-mintsifri-otkazalos

(дата обращения: 06.05.2021).

224. Козлова, Н. Билетная мафия вместо Большого театра и Мариинки попадет в тюремную камеру [Электронный ресурс]. – URL: https://sledcom.ru/press/smi/item/1537009 (дата обращения: 14.03.2021).

225. Кузнецов И. Apple подтвердила, что будет проверять наши фото. А ещё сообщения и поисковые запросы [Электронный ресурс]. – URL: https://appleinsider.ru/eto-interesno/apple-podtverdila-chto-budet-proveryat-nashi-foto-a-eshhyo-soobshheniya-i-poiskovye-zaprosy.html (дата обращения: 14.08.2021).

226. Лакодин В. «Непокоренные»: как и почему миллиард человек противостоит интернет-рекламе [Электронный ресурс]. – URL: https://texterra.ru/blog/nepokorennye-kak-i-pochemu-milliard-chelovek-protivostoit-internet-reklame.html (дата обращения: 18.08.2021).

227. Можно ли справиться с уязвимостями в программном обеспечении? [Электронный ресурс]. – URL: https://www.kaspersky.ru/blog/mozhno-li-spravitsya-s-uyazvimostyami-v-programmnom-obespechenii/14939/ (дата обращения: 20.08.2021).

228. Мочалова И. Телефонное мошенничество в цифрах: сколько аферисты зарабатывают на обмане россиян [Электронный ресурс]. – URL: https://www.mk.ru/social/2021/04/15/telefonnoe-moshennichestvo-v-cifrakh-skolko-aferisty-zarabatyvayut-na-obmane-rossiyan.html (дата обращения: 13.07.2021).

229. На Кубани с середины года выявили 17 случаев подделки сертификатов о вакцинации [Электронный ресурс]. URL: https://tass.ru/obschestvo/12906209?utm_source=yxnews&utm_medium=desktop&nw=1636888000000 (дата обращения: 14.11.2021).

230. Национальный поисковик «Спутник» запустят до конца весны [Электронный ресурс]. – URL: https://www.forbes.ru/news/255639-natsionalnyi-poiskovik-sputnik-zapustyat-do-kontsa-vesny (дата обращения: 17.08.2021).

231. Некезова К. В России распространился новый вид мошенничества

по телефону [Электронный ресурс]. – URL: https://www.vzsar.ru/news/2020/12/25/v-rossii-rasprostranilsya-novyy-vid-moshennichestva-po-telefony.html (дата обращения: 28.12.2020).

232. Нефедова М. Задержаны мошенники, похищавшие деньги у VIP-клиентов банков с помощью клонов SIM-карт [Электронный ресурс]. – URL: https://xakep.ru/2020/07/16/sin-swap-arrest/ (дата обращения: 23.12.2020).

233. Обвиняемому в убийстве из-за конфликта в школьном чате Арсену Мелконяну продлили арест [Электронный ресурс]. – URL: https://v1.ru/text/criminal/2020/12/21/69646916/ (дата обращения: 23.12.2020).

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

235. ООН признала анонимность в Интернете правом человека [Электронный ресурс]. – URL: http://www.gazeta.ru/tech/news/2015/08/25/n_7509455.shtml (дата обращения: 07.10.18).

236. Петров И. Крах «билетной мафии»: киберворам дали рекордные сроки [Электронный ресурс]. – URL: https://iz.ru/958391/ivan-petrov/krakh-biletnoi-mafii-kibervoram-dali-rekordnye-sroki (дата обращения 27.12.2019).

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

238. По иску Генерального прокурора Российской Федерации Игоря Краснова Верховный Суд Российской Федерации запретил деятельность международного общественного движения «Арестантское уголовное единство» [Электронный ресурс]. – URL: http://genproc.gov.ru/smi/news/genproc/news-1886554/ (дата обращения: 08.07.2021).

239. Пользовательское соглашение сети Facebook [Электронный ресурс].

– URL: https://www.facebook.com/terms.php?locale=ru_RU (дата обращения: 17.01.2021).

240. Пользовательское соглашение социальной сети «ВКонтакте» [Электронный ресурс]. – URL: https://vk.com/terms (дата обращения: 17.01.2021).

241. Постановление Госсовета КНР «О планировании строительства системы социального кредита (2014–2020)» [Электронный ресурс]. – URL: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm (дата обращения: 10.08.2021).

242. Почем сегодня продают уязвимости в программном обеспечении? [Электронный ресурс]. – URL: http://www.aethra.ru/pochem-segodnya-prodayut-uyazvimosti-v-programmnom-obespechenii/ (дата обращения: 20.08.2021).

243. Почему отечественная «Википедия» не взлетит [Электронный ресурс]. – URL: https://cont.ws/@fritzmorgen/1463112 (дата обращения: 17.08.2021).

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

245. Разгорающийся скандал: большой московский слив [Электронный ресурс]. – URL: https://zavtra.ru/events/razgorayushijsya_skandal_bol_shoj_moskovskij_sliv (дата обращения: 28.12.2020).

246. Решение № 1351/2008/ЕС Европейского парламента и Совета Европейского Союза «О создании многолетней программы Сообщества о защите детей при использовании Интернета и других коммуникационных технологий» [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

247. Роскомнадзор разблокировал PornHub [Электронный ресурс]. – URL: https://ria.ru/20170413/1492189250.html (дата обращения: 16.04.2021).

248. Россия потратит два миллиарда рублей на аналог «Википедии»

[Электронный ресурс]. – URL: https://lenta.ru/news/2019/09/26/wikipedia/ (дата обращения: 17.08.2021).

249. Русанова И. Кому принадлежит Яндекс [Электронный ресурс]. – URL: https://brobank.ru/komu-prinadlezhit-yandex/ (дата обращения: 17.08.2021).

250. Саратовец нарвался на мошенников при заказе проститутки в интернете [Электронный ресурс]. – URL: https://www.vzsar.ru/news/2020/11/15/saratovec-narvalsya-na-moshennikov-pri-zakaze-prostitytki-v-internete.html (дата обращения: 28.12.2020).

251. Сбербанк назвал телефонное мошенничество национальным бедствием [Электронный ресурс]. – URL: https://ria.ru/20210707/moshennichestvo-1740256569.html (дата обращения: 17.07.2021).

252. «Сбер» оценил количество мошеннических звонков в России в 15 миллионов с начала 2020 года [Электронный ресурс]. – URL: https://vc.ru/finance/186662-sber-ocenil-kolichestvo-moshennicheskih-zvonkov-v-rossii-v-15-millionov-s-nachala-2020-goda (дата обращения: 28.12.2020).

253. Сбербанк подсчитал, сколько мошенники крадут со счетов россиян в месяц [Электронный ресурс]. – URL: https://ria.ru/20210609/moshenniki-1736229634.html (дата обращения: 17.07.2021).

254. Сотни саратовских подростков изучали АУЕ в соцсетях [Электронный ресурс]. – URL: https://www.vzsar.ru/news/2020/08/11/sotni-saratovskih-podrostkov-izychali-aye-v-socsetyah.html (дата обращения: 12.03.2021).

255. Состояние преступности в России за январь – декабрь 2020 г. [Электронный ресурс]. – URL: http://crimestat.ru/analytics (дата обращения: 13.07.2021).

256. Стаценко Н. Роскомнадзор заблокировал Pornhub на всей территории России [Электронный ресурс]. – URL: https://rb.ru/news/pornhub-down/ (дата обращения: 05.05.2021).

257. Степанов В. Великий колесный путь Власти США закрыли интернет-магазин наркотиков Silk Road [Электронный ресурс]. – URL: https://lenta.ru/articles/2013/10/03/silkroad/ (дата обращения: 16.08.2021).

258. Степовой, В. Дети стали жить «по понятиям» [Электронный ресурс]. – URL: https://mirnov.ru/obshchestvo/problemy-semi-i-vospitanija/deti-stali-zhit-po-ponjatijam.html (дата обращения: 19.08.2021).

259. Телефоны молчат, деньги клиентов утекают: У ВТБ рухнуло все... [Электронный ресурс]. – URL: https://smart-lab.ru/blog/631461.php (дата обращения: 28.12.2020).

260. Теперь в китайских соцсетях регистрируются только по паспорту [Электронный ресурс]. – URL: https://ovesti.ru/other/world/8844-teper-v-kitayskih-socsetyah-registriruyutsya-tolko-po-pasportu.html (дата обращения: 08.08.2021).

261. Токарева А., Биянова Н. Детские долги [Электронный ресурс]. – URL: https://www.banki.ru/news/daytheme/?id=3959932 (дата обращения: 31.12.2020).

262. Условия использования Viber [Электронный ресурс]. – URL: https://www.viber.com/ru/terms/viber-terms-use/ (дата обращения: 17.01.2021).

263. Условия использования сервиса Instagram [Электронный ресурс]. – URL: https://help.instagram.com/478745558852511 (дата обращения: 17.01.2021).

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

265. Френкель Д., Бородихин А. «Мы дали отпор врагу». Иранские власти отключили страну от интернета. [Электронный ресурс]. – URL: https://yandex.ru/turbo/s/zona.media/article/2019/11/20/iran-404 (дата обращения 21.07.2020)

266. Хазов В. Фильтрация интернет-контента для школ. Использование «белых списков» (ACL) [Электронный ресурс]. – URL: https://vasexperts.ru/blog/filtraciya-internet-kontenta-dlya-shkol-ispolzovanie-belyx-

spiskov-acl/ (дата обращения: 06.05.2021).

267. Цифровой юань [Электронный ресурс]. – URL: https://dcep.ru/ (дата обращения: 09.05.2021).

268. Черных, Е. Воронежский след атамана Шкуро [Электронный ресурс]. – URL: https://infovoronezh.ru/News/Voronejskiy-sled-atamana-SHkuro-9876.html (дата обращения: 17.08.2021).

269. Что такое «пузырь фильтров» и как из него выбраться [Электронный ресурс]. – URL: https://habr.com/ru/company/riddut/blog/295714/ (дата обращения: 31.12.2020).

270. Это – гражданская разведка: – пранкер Вован о своих проделках с Лексусом [Электронный ресурс]. – URL: https://www.5-tv.ru/news/199800/ (дата обращения: 24.07.2021).

271. Явная виртуальная угроза [Электронный ресурс]. – URL: https://www.rbc.ru/newspaper/2018/09/24/5ba4d2459a79475744112262 (дата обращения: 15.08.2021).

ПРИЛОЖЕНИЯ

Приложение 1. Результаты анкетирования сотрудников правоохранительных органов

(всего проанкетировано 148 человек)

1. Укажите род Вашей деятельности в правоохранительных органах и общий стаж службы:

а) прокуратура — 48%

б) судебная система — 12,8%

в) органы внутренних дел — 25,7%

г) ФСБ — 6%

2. Какие преступления, на Ваш взгляд, чаще всего совершаются в киберпространстве?

а) мошенничество – 60,8%

б) неправомерный доступ к компьютерной информации – 21,6%

в) распространение вредоносных программ — 8,1 %

г) кража номеров банковских карт и других банковских реквизитов — 43,2%

д) фишинг — 34,5%

е) распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду, и т. п.) – 38,5%

3. Кто чаще всего совершает такие преступления?

а) молодые люди, имеющие опыт обращения с компьютерной техникой — 64,9%

б) сотрудники банков, иных финансовых организаций — 12,8%

в) осужденные, отбывающие наказание — 60,8%

д) лица с профессиональным образованием в сфере ИТ — 25,7%

6. Каким способом чаще всего совершаются такие преступления:

а) злоупотребление доверием с добровольной передачей жертвой учётных и личных данных — 82,4%

б) путем распространения вредоносных программ — 38,5%

в) создание сайтов-дублеров — 30,4%

г) перехват интернет-трафика — 8,1%

д) путем распространения недостоверной информации — 12,8%

4. Кто чаще всего становится жертвой?

а) мужчины — 17%

б) женщины — 83 %

5. Укажите типичный возраст потерпевших от мошенничеств в сети Интернет:

а) до 35 — 8,1%

б) 36-40 — 12,8%

в) 41-45 — 16,9

г) 46-50 — 25,7%

д) 51 и старше — 34,5%

6. Укажите причины, по которым люди становятся жертвами мошеннических преступлений (можно указать несколько вариантов)**:**

а) низкий уровень образования — 30,4%

б) излишняя доверчивость — 68,9%

в) низкий уровень интеллекта — 12,8%

г) отсутствие опыта деятельности в сети «Интернет» — 16,9%

д) отсутствие технических познаний о сети «Интернет» — 64,9%

е) анонимность пользователей в сети «Интернет» — 21,6%

7. Можно ли, по Вашему мнению, избежать посягательства в сети Интернет?

а) Нет. Любой может стать жертвой — 35 %

б) Да. Нужно соблюдать правила безопасности — 65%

8. Какие меры предупреждения указанных преступлений вы применяете в своей работе (можно указать несколько вариантов)**?**

а) не применяю — 21,6%

б) профилактические беседы — 16,8%

в) проверка пользователя — 12,8 %

г) не перехожу по подозрительным ссылкам — 25,6%

д) установка антивирусных программ — 34,5%

е) информирование населения о фактах мошенничества — 30,4%

ж) анализ экстремистских групп в социальных сетях — 8%

9. Какие меры, на Ваш взгляд, необходимо применять в борьбе с преступлениями в сети Интернет (можно указать несколько вариантов)**?**

а) блокирование сайтов-дублеров — 30%

б) повышение компьютерной грамотности пользователей — 12,2%

в) проверка сайтов на наличие вредоносных программ — 37,2%

г) информирование населения о видах мошенничества — 49,3%

ж) ужесточение требование компьютерной безопасности — 19,6%

з) усиление контроля над сетью «Интернет» со стороны государства — 28,4%

и) пропаганда законопослушного поведения в сети «Интернет» — 23,6%

к) усиление контроля за сохранностью в тайне конфиденциальной информации о гражданах — 10,1%

л) ужесточение наказаний за киберпреступления — 11,5%

м) применение антивирусных программ

н) отказ от «палочной» системы оценки деятельности правоохранительных органов

10. Хватает ли полученных Вами знаний (в институте, на практике) для борьбы с такими преступлениями?

а) да — 26,4%

б) нет — 73,6%

11. Какие конкретно знания необходимы сотрудникам правоохранительных органов для борьбы с преступлениями в сети Интернет (можно указать несколько вариантов)**?**

а) познания в информационных технологиях — 50%

б) знание компьютерных программ — 29,7%

в) сведения о компьютерной безопасности — 27%

г) о методике противодействия преступлениям в сети «Интернет» — 16,2%

д) повышение квалификации сотрудников — 6,8%

е) более качественная Вузовская подготовка — 6,1%

ж) о методах выявления противоправного контента — 15,5%

Приложение 2. Результаты анкетирования граждан

(всего проанкетировано 204 человека)

1. Пол:

а) мужской – 43,7%

б) женский – 56,3 %

2. Возраст:

а) 18-24 – 57,8%

б) 25-35 – 21,9%

в) 36-50 – 14,1%

г) старше 50 – 21,8%

3. Род деятельности:

а) Школьник – 1,4%

б) Студент – 53,1%

в) Работающий – 39,1%

г) Работающий студент — 1,2%

д) Неработает (пенсионеры, инвалиды, домохозяйки – 4,2%

4. Знаете ли Вы о существовании мошеннических схем в сети Интернет:

а) Да – 96,9%

б) Нет – 3,1%

5. Предпринимались ли в отношении Вас попытки совершения мошенничества в сети Интернет?

а) Да – 82,8%

в) Нет – 17,2%

6. Становились ли Вы когда-нибудь жертвой мошенничества в сети Интернет?

а) Да – 60,9%

б) Нет – 39,1%

7. Жертвой какого вида мошенничества Вы становились?

а) Мошенничество при покупке в сети Интернет – 46,4%

б) Лотерейное мошенничество – 7,1%

в) Фишинг – 42,9%

г) Мошенничество в сфере благотворительности – 10,7%

д) Инвестиции – 3,6%

е) Взлом социальных сетей – 3,6%

ж) Взлом аккаунта и покупка – 3,6%

з) Займы денег – 3,6%

е) Мошенничество при покупке недвижимости – 7,1%

7.Обращались ли Вы за помощью в правоохранительные органы?

а) Да, обращался – 13,3%

б) Нет, ущерб был незначителен – 86,7%

8. Как отреагировали правоохранительные органы на Ваше обращение?

а) Преступление было раскрыто – 0%

б) Преступление не было раскрыто – 30,8%

в) Уголовное дело не было возбуждено – 69,2%

9. Имеется ли у Вас банковская карта?

а) Да – 98,4%

б) Нет – 1,6%

10. Чувствуете ли Вы тревогу за сохранность денежных средств на карте?

а) Да – 56,3%

б) Нет – 43,8%

11. Чем вызвана Ваша тревога?

а) недоверие к банку – 56,8%

б) негативный опыт – 19,4%

в) страх потери банковской карты – 27,8%

г) неумение правильно пользоваться – 11,1%

д) распространенность мошенничеств – 5,6%

12. Слышали ли Вы о мерах безопасности в сети Интернет?

а) Да – 81,3%

в) Нет – 18,8%

13. Из каких источников Вы получаете информацию о преступлениях, связанных с мошенническими действиями, и их профилактике?

а) от знакомых – 75%

б) личный опыт – 40,6%

в) телепередачи – 50%

г) фильмы – 18,8%

д) публикации в Интернете – 84,4%