Министерство образования и науки РФ
Алтайский государственный университет
Юридический институт

ПРАВА ЧЕЛОВЕКА И КРИМИНАЛИЗАЦИЯ

Том 2. Взгляд в будущее: трибуна молодого ученого

Материалы Международной научно-практической конференции 12–14 мая 2022 года

Барнаул

Издательство
Алтайского государственного
университета
2022

УДК 343.2
ББК 67.408
П 68

Рецензенты:
доктор юрид. наук, профессор Васильев Антон Александрович
доктор юрид. наук, профессор Детков Алексей Петрович
Ответственный редактор:
Коренная Анна Анатольевна, кандидат юридических наук, адвокат, доцент кафедры уголовного права и криминологии Алтайского государственного университета, директор Автономной некоммерческой организации реализации социальных проектов «Территория успеха»

П 68 **Права человека и криминализация. Том 2. Взгляд в будущее: трибуна молодого ученого** : материалы международной научно-практической конференции / отв. ред. А.А. Коренная ; Министерство науки и высшего образования РФ, Алтайский государственный университет. — Барнаул : Изд-во Алт. ун-та, 2022. — 150 с.

ISBN 978-5-7904-2665-0.

Настоящий сборник составлен по материалам Международной научно-практической конференции, состоявшейся 12–14 мая 2022 года в Барнауле. В сборник вошли статьи профессорско-преподавательского и научного состава вузов России, практикующих юристов, сотрудников специализированных министерств, правоохранительных органов, а также магистрантов и студентов.

Сборник будет востребован преподавателями и студентами высших и средних специальных учебных заведений в рамках программ основного образовательного цикла, а также программ дополнительного образования, курсов повышения квалификации.

УДК 343.2
ББК 67.408

ISBN 978-5-7904-2665-0

15. Цифровые финансовые активы: первая компания включена в реестр // https://clck.ru/gkhLR — дата обращения 02.05.2022;

16. О включении сведений об ООО «Лайтхаус» в реестр операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов // https://clck.ru/gkhKz — дата обращения 02.05.2022;

17. О включении сведений о ПАО Сбербанк в реестр операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов // https://clck.ru/gkhKi — дата обращения 02.05.2022;

18. Россия вошла в десятку самых влиятельных стран по майнингу криптовалют // https://clck.ru/gkhKG — дата обращения 02.05.2022.

Информация об авторе: Корепанова Екатерина Сергеевна, г. Ижевск, Институт права, социального управления и безопасности ФГБОУ ВО «Удмуртского государственного университета». Адрес электронной почты: katkorepanova@mail.ru.

Information about the author: Korepanova Ekaterina Sergeevna, Izhevsk, Institute of Law, Social Management and Security of the Udmurt State University. Email address: katkorepanova@mail.ru.

УДК 34

Широбокова Е. С.

ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-АНОНИМАЙЗЕРОВ

Аннотация: статья посвящена проблеме отграничения законного использования программ-анонимайзеров, имеющих целевое назначение от использования данных программ с нарушением требований, а также от незаконного их использования. Наличие регулятивного законодательства, касающегося программ-анонимайзеров, в полной мере не разрешает проблемы, связанные с обращением данных программ. Предлагается включить в порядок обращения программ-анонимайзеров требование

об обязательном лицензировании указанных ресурсов. Также обосновывается необходимость криминализации деяний, связанных с незаконным использованием программ-анонимайзеров.

Ключевые слова: программа-анонимайзер, прокси-сервер, VPN, SIP-телефония, блокирование сайтов.

Shirobokova E. S.

CRIMINAL LIABILITY PROBLEMS FOR CRIMES USING ANONYMIZER PROGRAMS

Annotation: the article is devoted to the problem of distinguishing the legitimate use of anonymizer programs that have a purpose from the use of these programs in violation of the requirements, as well as from their illegal use. The existence of regulatory legislation concerning anonymizer programs does not fully solve the problems associated with the circulation of these programs. It is proposed to include a requirement for mandatory licensing of these resources in the procedure for contacting anonymizer programs. The necessity of criminalization of acts related to the illegal use of anonymizer programs is also justified.

Keywords: anonymizer program, proxy server, VPN, SIP telephony, website blocking.

Анонимайзер — это специальное средство, которое позволяет пользователю скрыть информацию о себе или о своем компьютере от удаленного сервера. Оно может иметь вид специального сайта или отдельной программы, требующей установки на жесткий диск [9, электронный ресурс].

В настоящее время практически все организации озабочены проблемой защиты информации. Последствия взлома систем защиты информации становятся крайне критичными и очень дорогими. Для предотвращения этого организации и граждане используют различные инструменты для защиты информации, которые также увеличивают эффективность и скорость выполнения задач. К числу таких инструментов относится, например, прокси-сервер, который представляет из себя промежуточный сервер между клиентом Интернета и сервера-

ми запрашиваемой информации. Область применения прокси-сервера широка: 1) обеспечение доступа компьютеров в локальной сети к единому соединению с Интернетом — таким образом обеспечивается безопасность оборота информации; 2) сжатие и кэширование данных — это позволяет экономить трафик и ускорять получение запрашиваемой информации; 3) аутентификация и контроль доступа к ресурсам; 4) анонимизация доступа к различным ресурсам, в том числе Интернет-ресурсам — в данном случае, прокси-сервер часто используется для тестирования сайтов, программ после их разработки [3, с. 7–8].

Схожим инструментом является Virtual Private Network (VPN). Технология VPN была разработана таким образом, чтобы позволить удаленным пользователям безопасно получать доступ к корпоративным ресурсам. Для обеспечения безопасности данные проходят через защищенные тунели, а пользователи VPN, обладающие ключами шифрования, должны использовать методы проверки подлинности, включая пароли и другие процедуры идентификации для доступа к VPN-серверу [2, с. 1].

Использование SIP-телефонии (Session Initiation Protocol). Многие организации используют SIP-телефонию как основной источник совершения звонков, что обусловлено меньшей стоимостью тарифов и услуг, чем у других провайдеров связи. Характерной черной SIP-телефонии является виртуальность номеров, с которых осуществляется звонок или передача сообщений. В отличие от обычной линии, SIP-телефония позволят организовать связь между нескольким пользователями, при этом, она может быть, как домашней, так корпоративной, также она позволяет провести аналитику и оценку эффективности работы сотрудников. Принцип работы SIP-телефонии заключается в преобразовании сигналов в цифровые данные, которые сжимаются и разбиваются на пакеты, при этом, избыточная информация: шумы, помехи — не передается, тем самым снижается нагрузка на трафик. Когда сигнал доходит до получателя, цифровые данные преобразуются обратно в голосовые сигналы [1, с. 2–4].

В целях обеспечения полноты защиты информации, пользователями зачастую используется комбинированный метод применения вышеуказанных инструментов. Кроме того, помимо указанных средств существуют и иные технологии, позволяющие засекретить маршруты, трафики в сети.

Указанные программы-анонимайзеры пользуются большим спросом не только для достижения корпоративных целей, но и являются неотъемлемой частью повседневной жизни обычных граждан. При этом, использование таких инструментов можно классифицировать на:

— законное;
— незаконное;
— использование с нарушением требований.

Под законным использованием программ-анонимайзеров принято понимать применение программ-анонимайзеров для получения доступа к разрешенным информационным ресурсам.

Незаконное использование программ-анонимайзеров направлено на получение доступа к заблокированным информационным ресурсам.

Использование программ-аниониамайзеров с нарушением требований безопасности может иметь место в случаях, когда лицо, обеспечивающее доступ к информационному ресурсу, нарушает общие правила информационной безопасности. Так, например, ст. 19.7. КоАП РФ предусматривает ответственность за непредставление либо нарушение сроков и порядка представления сведений о данных о личности владельца анонимайзера или прокси.

Программы, скрывающие информацию о пользователе, используются для совершения преступлений. Несмотря на то, что программы-анонимайзеры не обеспечивают полную анонимность в сети, они значительно усложняют процесс установления реального IP-адреса компьютера, с помощью которого совершается преступление, позволяют «обойти» запреты на посещение отдельных Интернет-ресурсов, а также используются в иных целях, связанных с введением в заблуждение пользователей информационно-телекоммуникационных ресурсов. В целях конспирации преступной деятельности для затруднения определения местонахождения и идентификации пользователей в сети Интернет преступными группами и сообществами используются программные обеспечения «Tor», «VPN», «VPS», «VDS», SIP-телефония и другие средства анонимизации, что усложняет установление и документирование противоправной деятельности [4, с. 76].

Наиболее распространенными преступлениями, совершаемыми с использованием программ-анонимайзеров, являются преступления, связанные с незаконным обращением предметов, ограниченных или изъя-

тых из гражданского оборота. Так, согласно приговору Октябрьского районного суда г. Мурманска № 1–73/2020 от 28 июля 2020 г. по делу № 1–73/2020, было установлено, что В. Т. Тамазанов, а также иные участники организованной группы при совершении преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, с целью недопущения изобличения правоохранительными органами, всеми участниками организованной группы, по указанию руководителя использовали программы VPN, позволяющие менять IP-адреса при соединении с сетью «Интернет». При этом, участники организованной группы при осуществлении совместной преступной деятельности использовали сим-карты, зарегистрированные на посторонних лиц, не осведомлённых о преступной деятельности организованной группы, которые подлежали систематической смене [5].

Программы-анонимайзеры также используются при совершении преступлений против собственности. Приговором Октябрьского районного суда г. Тамбова № 1–454/2019 от 4 сентября 2019 г. по делу № 1–454/2019 М. В. Тарасов был привлечен к уголовной ответственности за совершение преступлений, преступлений, предусмотренных ч.3 ст. 159 УК РФ. Судом установлено, что для реализации преступного умысла, М. В. Тарасов использовал программные средства (анонимайзеры), предназначенные для подмены и сокрытия реально используемого IP-адреса, а именно, программное средство Avast SecureLine VPN [6, электронный ресурс].

14 марта 2022 года по решению Роскомнадзора началась блокировка социальных сетей «Facebook» и «Instagram». Поскольку использование программ-анонимайзеров не представляет технических сложностей, пользователи социальных сетей, принадлежащих компании Meta имели доступ к данным ресурсам посредством изменения своего IP-адреса. Согласно данным сервиса отслеживания блокировок Globalchek, с момента блокировки до 04.05.2022, доступность «Instagram» варьировалась от 6 до 12%, «Facebook» за тот же период от 3 до 17%. По иску прокуратуры суд признал компанию Meta экстремистской организацией. Соответственно, действия российских пользователей социальных сетей компании Meta, имеющих доступ к данным ресурсам, посредством искажения данных о своем местоположении, можно рассматривать как участие в деятельности общественного или религиозного объединения либо иной ор-

ганизации, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности, за исключением организаций, которые в соответствии с законодательством Российской Федерации признаны террористическими [8, электронный ресурс].

Программы-анонимайзеры, в том числе VPN, прокси-серверы, SIP-телефония, могут выступать средством совершения любого преступления (использоваться при подготовке, совершении преступления или, например, для сокрытия следов преступления и предметов, добытых преступным путем).

Многие составы преступлений предусматривают в качестве признака основного или квалифицированного состава преступления использование ІТТ (например, «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)» (п. «б» ч.2 ст. 228[1] УК РФ) или «с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет»» (п. «б» ч.3 ст. 242 УК РФ)). В данном случае повышенная общественная опасность содеянного связана с использованием СМИ, а также информационных ресурсов, обеспечивающих публичный способ совершения преступления, и с использованием средств совершения преступления, рассчитанных на неопределенно широкий круг лиц. Применение при совершении преступления программ-анонимайзеров с учетом положений действующего УК РФ не влияет на квалификацию преступления. Очевидно, что использование таких ресурсов влияет на характер общественной опасности и повышает степень общественной опасности, что можно аргументировать следующими доводами:

1. Пользователи программ-анонимайзеров, в ходе совершения преступления, помимо общественных отношений, которые являются непосредственным объектом преступления, причиняют вред и посягают на конфиденциальность, целостность и доступность компьютерной информации.

2. Используя программы-анонимайзеры, лицо, совершающее преступление, скрывает свое местонахождение (или создает иллюзию своего пребывания в другом в месте), что может затруднить раскрытие преступления и привести к конфликту юрисдикций;

3. Помимо засекречивания трафика, лицо, применяющее программы-анонимайзеры, имеют возможность выдавать себя за иных лиц, то есть добиваться поставленных целей при помощи обмана или введения в заблуждение.

Не представляется возможным внесение изменений в УК РФ, расширяющих перечень квалифицирующих признаков, поскольку применение вышеперечисленных вариантов использования программ-анонимайзеров возможно при совершении любого преступления. В настоящее время единственным способом борьбы с созданием, распространением и предоставлением доступа программ-анонимайзеров является блокирование ресурсов, на которых размещены данные программы.

Перечень оснований для ограничения доступа к сайтам в сети «Интернет», установленный Федеральным законом № 149-ФЗ, широк. К числу оснований относятся, например, решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено, постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети «Интернет», порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица [7, ст. 15.1.].

Еще в 2017 году эксперты информационно-аналитического центра «Сова» пришли к заключению, что решения о блокировке анонимайзеров неправомерны, обосновывая это тем, что программы-анонимайзеры не содержат никакой запрещенной информации, а являются лишь пользовательским инструментом, нет оснований для закрытия доступа к ресурсам, размещающим анонимайзеры [10, электронный ресурс].

11 января 2022 года юристы «Роскомсвободы» подали в интересах The Tor Project Inc. (Tor) апелляционную жалобу на решение Саратовского районного суда, признавшего запрещенной к распространению информацию на главной странице проекта «Tor». «Роскомсвободы» в качестве обоснования указал: «Сами по себе такие технические средства не содержат никакой запрещенной информации, а доступ к запрещенным материалам может быть осуществлен и посредством других инструментов, в том числе через обычную поисковую систему». По-

добной логики придерживается и Европейский суд по правам человека в постановлении «Энгельс против России» [9]. Однако, очевидно, что оставлять без внимания ресурсы, предоставляющие доступ к программам-анонимайзерам нельзя.

В регулятивном законодательстве имеется ряд положений, связанных с использованием программ-анонимайзеров. Так, Федеральный закон «О связи» в ред. Федерального закона от 02.07.2021 N 319-ФЗ в п.9 ст. 46 устанавливает обязанность операторов связи предоставлять в неизменном виде абонентский номер, а также уникальный код идентификации. Данный пункт в новой редакции содержит следующее положение: «Идентификация абонентов, инициирующих соединение для целей передачи голосовой информации в сети передачи данных, осуществляется в порядке, установленном Правительством Российской Федерации».

Федеральным законом от 29.07.2017 N 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» установлен запрет на обеспечение использования в РФ информационно-телекоммуникационных сетей, информационных систем и компьютерных программ для получения доступа к запрещенным информационным ресурсам. На операторов поисковых систем возложена обязанность прекращать выдачу ссылок на заблокированные информационные ресурсы.

Учитывая наличие целевого назначения программ-анонимайзеров, а также применение их гражданами и юридическими лицами в целях защиты информации, повышения скорости и эффективности работы, предлагается произвести четкую грань между законным и незаконным использованием, приобретением, созданием, распространением, предоставлением доступа к программам-анонимайзерам. При этом, основным критерием для признания оборота таких инструментов законным должно выступать наличие лицензии на программу-анонимайзер. Это позволит решить споры о неправомерности блокировки сайтов-анонимайзеров.

Кроме того, обращая внимание на наличие повышенной общественной опасности представляется целесообразным криминализировать не деяния, связанные с применением программ-анонимайзеров в качестве средства совершения преступления, а само незаконное обращение

программ-анонимайзеров в качестве самостоятельного противоправного деяния — незаконное использование, приобретение, создание, распространение, предоставление доступа к программам-анонимайзерам. При этом, квалифицировать деяние необходимо по совокупности со статьями Особенной части УК РФ, предусматривающими ответственность за преступление, для совершения которого использовалась программа-анонимайзер.

Ввиду увеличения количества случаев применения программ-анонимайзеров, которое обусловлено различными причинами, в том числе, ограничительными мерами, вызванными covid-19, контролем РПН и большим количеством случаев блокирования Интернет-ресурсов, а также легкостью применения самих программ-анонимайзеров, представляется недостаточным было бы введение лишь административной ответственности за создание, распространение и использование ресурсов, заведомо позволяющих получать доступ к запрещенным ресурсам, необходимо установление ответственности уголовной.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Коммуникационное взаимодействие между пользователями при помощи SIP-телефонии Колмакова В. В., Илющенко А. Н., Глазунова О. Д. В сборнике: Современные инструментальные системы, информационные технологии и инновации. Сборник научных трудов XVII Международной научно-практической конференции. Редколлегия: Разумов М. С. (отв. ред.). Курск, 2022. С. 216–223.

2. Методика расследования незаконного сбыта синтетических наркотических средств, совершенного с использованием Интернет-магазинов: учебное пособие / Земцова С. И., Суров О. А., Галушин П. В. — 2 изд., перераб. и доп. — Красноярск: СибЮИ МВД России, 2019. — 184 с.

3. Организация прокси-сервера Григоренко В. Е., Игрунова С. В. Белгородский государственный национальный исследовательский университет Белгород, Россия. [Электронный ресурс]. URL: https://scienceforum.ru/2018/article/2018005110 (дата обращения 19.04.2022 г.).

4. Организация шифрованного VPN канала для связи с филиалами Николахин А. Ю. В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов конференции РАЕН. 2018. С. 20–22.

5. Приговор № 1–73/2020 от 28 июля 2020 г. по делу № 1–73/2020 Октябрьский районный суд г. Мурманска (Мурманская область). [Электронный ресурс]. URL: https://sudact.ru/regular/doc/Fvk0acfsW5Yv/ (дата обращения 01.05.2022 г.).

6. Приговор № 1–454/2019 от 4 сентября 2019 г. по делу № 1–454/2019 Октябрьский районный суд г. Тамбова (Тамбовская область). [Электронный ресурс]. URL: https://sudact.ru/regular/doc/fzE0R5j7Oigj/

7. The Tor Project и «Роскомсвобода» обжалуют блокировку Tor в суде // Роскомсвобода. 2022. 24 января. [Электронный ресурс]. URL: https://roskomsvoboda.org/post/rks-with-tor/ (дата обращения 01.05.2022 г.)

8. 2021 © GlobalCheck All Rights Reserved [Электронный ресурс]. URL: https://globalcheck.net/ru/monitoring/ru/instagram.com?period=1d (дата обращения 01.05.2022 г.)

9. Лучшие бесплатные анонимайзеры [Электронный ресурс]. URL https://spy-soft.net/luchshie-besplatnye-onlajn-anonimajzery-obzor-vybor-rekomendacii/ (дата обращения 01.05.2022 г.)

10. Блокировки анонимайзеров [Электронный ресурс]. URL: https://www.sova-center.ru/misuse/news/persecution/2016/08/d35307/ (дата обращения 01.05.2022 г.).

Информация об авторе: *Широбокова Елизавета Сергеевна*, г. Ижевск, Институт права, социального управления и безопасности ФГБОУ ВО «Удмуртского государственного университета». Адрес электронной почты: Lizashirobokova@yandex.ru.

Information about the author: Shirobokova Elizaveta Sergeevna, Izhevsk, Institute of Law, Social Management and Security of the Udmurt State University. Email address: Lizashirobokova@yandex.ru.

СОДЕРЖАНИЕ