УДК 34.096

Вохмянина Анна Сергеевна
Студент 2 курса
заочного факультета, магистратура
направление «Юриспруденция»
АОУ ВО ЛО "ГИЭФПТ"
Россия, г. Гатчина

ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ПРОГРАММ-АНОНИМАЙЗЕРОВ КАК СРЕДСТВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ

Аннотация: *В статье рассмотрена сущность программ-анонимайзеров, дана оценка действующего отечественного законодательства в данной области и дальнейшие перспективы развития правового регулирования. Анализируются основные негативные проявления, связанные с распространением и эксплуатацией программ-анонимайзеров, позволяющих обходить ограничения на доступ к информации и интренет-ресурсам. В настоящей статье рассматриваются возможные средства противодействия использованию информационных технологий в целях совершения киберпреступлений.*

Ключевые слова: *программа-анонимайзер, правовое регулирование в сети «Интернет», киберпреступность, VPN-сервисы.*

Abstract: *The article considers the essence of anonymizing programs, gives an assessment of the current domestic legislation in this area and further prospects for the development of legal regulation. The main negative manifestations associated with the distribution and operation of anonymizer programs, which allow circumventing restrictions on access to information and Internet resources, are*

analyzed. This article discusses possible means of countering the use of information technology to commit cybercrime.

Key words: *anonymizer program, legal regulation on the Internet, cybercrime, VPN services.*

Вопросы правового регулирования деятельности в киберпространстве с каждым годом становятся все более актуальными, основной причиной чему становится развитие информационных технологий. В настоящее время особую важность приобретает вопрос правового регулирования разработки, распространения и использования программ-анонимайзеров, позволяющих пользователю информационно-телекоммуникационной сети «Интернет» получить доступ к ограниченным интернет-ресурсам. Прежде чем анализировать особенности нормативно-правовой базы в данной области, следует в общих чертах ознакомиться с сущностью программ-анонимайзеров, их разновидностями, принципом действия и предназначением.

Программа-анонимайзер – это общее, собирательное название технических средств и способов, позволяющих скрывать данные о пользователе сети «Интернет» и используемых им устройствах. Прежде всего, анонимайзер предназначен для сокрытия личного идентификатор устройства (IP-адрес), предоставляемого оператором информационной системы, то есть интернет-провайдером [4, с. 100]. Принцип действия программ-аннонимайзеров заключается в том, что пользователь указывает интернет-адрес того ресурса, который намеревается посетить. Программа-анонимайзер, обладающая иным сетевым адресом, загружает запрашиваемый интернет-ресурс себе, передавая пользователю фактически копию полученной информации. Следует заметить, что подобным способом пользователю сети «Интернет» предоставляется не только конфиденциальность, но и возможность получения доступа к запрещенным сайтам в сети «Интернет» и информации, распространение которой на территории Российской Федерации

запрещено [2, с. 11]. Таким образом, анонимайзер предоставляет возможность обеспечить конфиденциальность данных пользователя, при этом сведения о его IP-адреса будут сохраняться в тайне как для интернет-провайдера, так и для владельцев тех интернет-ресурсов, которые посещаются пользователем, и будут известны только владельцу программы-анонимайзера. Одной из наиболее известных и популярных среди пользователей программ-анонимайзеров выступает «Tor Browser».

Одной из разновидностью анонимайзеров, отличающихся более сложной системой сокрытия данных пользователя, являются VPN-сервисы, что расшифровывается как «виртуальная частная сеть». Указанные сервисы не просто скрывают от интернет-провайдера и третьих лиц данные о пользователе, посещаемых им интернет-ресурсах, но и шифрует сведения об интернет-соединении. Принцип действия VPN-сервисов заключается в том, что реальное интернет-соединение, создаваемое между пользователем и интернет-ресурсам, маскируется под другие фиктивные соединения. Подобная маскировка осуществляется посредством подключения пользователя к этой частной сети, функционирвоание которой обеспечивается VPN-сервером, расположенного, как правило, в другом государстве [4, с. 101]. Следует заметить, что VPN-серверы располагаются в странах, где цензура в сети «Интернет» минимальна, то есть интернет-провайдеры допускают свободный доступ к любым интернет-ресурсам.

В условиях блокировки многих популярных инетрнет-ресурсов, в том числе социальных сетей «Instagram» и «Facebook», спрос на услуги программ-анонимайзеров в Российской Федерации значительно возрос. Тверской суд города Москвы 21 марта 2022 года удовлетворил иск генеральной прокуратуры и признал социальные сети «Instagram» и «Facebook» экстремистками. Используя VPN-соединение, многие пользователи обходят ограничение на посещение указанных интернет-ресурсов. Справедливо будет

заметить, что подобные намерения пользователей программ-анонимайзеров фактически лишены общественно опасной направленности.

Вместе с тем, эксплуатация программы-анонимайзер, в том числе и VPN-сервисов, может привести сразу к нескольким негативным последствиям. Во-первых, предоставляемая пользователям сети «Интернет», полная конфиденциальность в киберпространстве обеспечивает анонимность злоумышленников, которые совершают киберпреступления. Другими словами, наличие возможности у киберпреступников скрыть свои данные от третьих лиц затрудняет производство оперативно-розыскной деятельности и предварительного расследования в отношении лиц, совершивших преступления в киберпространстве. Во-вторых, VPN-сервисы и иные анонимайзеры дают возможность совершать в сети «Интернет» покупки, которые любой интернет-оператой бы не допустил. Так, в частности, именно программы-анонимайзеры обеспечивают незаконный оборот оружия, наркотических средств, поддельных документов и даже людей. В-третьих, возможность обхода ограничений, установленных правовыми актами Российской Федерации, позволяет пользователям получить доступ к интернет-ресурсам экстремистского содержания. Все негативные последствия этого для общественной нравственности и безопасности конституционного строя Российской Федерации очевидны.

Таким образом, понимание государством негативного влияния использования программ-анимайзеров привело к установлению запрета на их эксплуатацию. Так, в 2017 году были внесены соответствующие изменения в ст. 15.8 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», согласно которым любым интернет-провайдерам и фактически владельцам подобных анонимайзеров было запрещено предоставлять пользователям доступ к информационным ресурсам, доступ к которым ограничен на территории Российской Федерации. Кроме всего прочего, в целях соблюдения данного

ограничения, все программы-анонимайзеры, рассматриваемые законодателем как информационный ресурс, в том числе VPN-сервисы обязаны присоединиться к Государственной информационной системе Роскомнадзора, содержащей перечень информационных ресурсов, доступ к которым ограничен на территории Российской Федерации.

Действующее отечественное законодательство предусматривает возможность привлечения операторов интернет-связи к административной ответственности за несоблюдение установленных ограничений. Так, в частности, ст. 19.7.10 Кодекса РФ об административных правонарушениях устанавливает ответственность за непредоставление Роскомнадзору сведений или предоставление ложных сведений, позволяющих идентифицировать «владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен». Кроме всего прочего, сами владельцы программ-анонимайзеров могут быть привлечены к административной ответственности за неприсоединение к Государственной информационной системе Роскомнадзора и за предоставление пользователям запрещенных материалов и ресурсов, в соответствии со ст. 13.40 КоАП РФ. Помимо всего прочего, в последнее время по требованию Роскомнадзора доступ к некоторым VPN-сервисам, не выполнившим условие о присоединение к Государственной информационной системе, стал ограничиваться.

Так или иначе, фактическое положение дел показывает, что у российских пользователей сохраняется свободный доступ к огромному разнообразию VPN-сервисов и других программ-анонимайзеров, а посредством них – к ограниченным на территории Российской Федерации материалам и интернет-ресурсам. Вместе с тем, на фоне повышения спора на услуги программ, обеспечивающих анонимность в сети «Интернет» и возможность обхода установленных ограничений, обсуждаются самые разнообразные подходы к правовому регулированию. Так, в частности, не

редко предлагается ввести полный запрет на распространение и использование программ-анонимайзеров, вплоть до установления административной ответственности не только для их владельцев, но и пользователей. Реализация подобных предложений представляется невозможной в силу организационных и технических причин. Многие специалисты в области информационных технологий отмечают, что полностью пресечь функционирование анонимайзеров на территории России невозможно, а выявить всех их пользователей с целью привлечения к юридической ответственности тем более [4, с. 102]. Следует признать, что владельцы программ, специализирующихся на обходе различного рода блокировок, найдут способ преодолеть блокировку и своих сервисов.

Вместе с тем, следует учитывать, что не стоит задачи полностью изолировать российский сегмент интернета, как это сделано, например, в Китае, где, кстати, многие VPN-сервисы находят возможность свободно функционировать [3, с. 4]. Более того, бороться следует не с самими программами-анонимайзерами, а с теми негативными явлениями, которые их сопровождают. Учитывая принцип действия VPN-сервисов, а именно то, что информационные серверы располагаются на территории тех государств, законодательство которых не содержит каких-то строгих ограничений в области информации и интернет-ресурсов, единственной возможностью борьбы выступает унификация международно-правовых норм в области информационного права.

Во-первых, следует признать, что киберпреступность является общемировой проблемой, а негативные последствия от совершения преступлений в киберпространстве распространяются на все мировое сообщество. Во-вторых, учитывая активное использование киберпреступностью способов и средств обеспечения анонимности во всемирной сети, бороться с этим необходимо совместными усилиями государств. Эффективным шагом будет разработка международной

конвенции, позволяющей привести в соответствие национального законодательства подписавшихся стран в области ограничения распространения информации и доступа к интернет-ресурсам, которые обеспечивают возможность совершения киберпреступлений, среди которых оборот наркотиков, оружия, поддельных документов, детской порнографии и так далее.

В заключение можно отметить, что в настоящее время в данной сфере действует лишь один международно-правовой акт, а именно Будапештская Конвенция № 185 «О преступности в сфере компьютерной информации», подписанная 23 ноября 2001 года. В 2021 году Российская Федерация внесла в Организацию Объединенных Наций проект новой конвенции, посвященной противодействию совершению преступлений посредством использования информационно-коммуникационных технологий. Таким образом, единственным перспективным направлением в правовом регулировании программ-анонимайзеров на сегодняшний день выступает международный отказ от поддержки соответствующих сервисов, обеспечивающих полную конфиденциальность в сети «Интернет», посредством унификации международно-правовых норм и привидения в соответствие национальных законодательных актов.

Литература:

1. Азизов З.М. Ограничения свободы слова в интернете в целях защиты государственных интересов и конституционного строя страны // Интеллектуальный потенциал XXI века: ступени познания. – 2017. - № 3. – С. 117-121.

2. Гурова М.Е., Исаев М.В. Актуальные проблемы правового регулирования социальных сетей // Скиф. Вопросы студенческой науки. – 2021. - № 7 (59). – С. 7-11.

3. Линь До. Основы правового регулирования и административного контроля интернета в Китае // NB: Административное право и практика администрирования. – 2020. - № 2. – С. 1-7.

4. Сергеев С.М. Некоторые проблемы противодействия использованию в преступленной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник Санкт-Петербургского университета МВД России. – 2017. - № 1 (73). – С. 98-103.

5. Шматкова Л.П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. — 2016. — № 28 (132). — С. 720-723.