DOI 10.37882/2223–2974.2022.03.33

ЗАПРЕТ АНОНИМНОСТИ В СЕТИ ИНТЕРНЕТ КАК МЕРА ПРОФИЛАКТИКИ МОШЕННИЧЕСТВА

Семенова Наталья Александровна
Аспирант, Бурятский государственный университет имени Доржи Банзарова
624559@list.ru

Аннотация. В настоящей статье проводится анализ законодательного введения запрета на анонимность в сети Интернет, как меры профилактики мошенничества, раскрываются виды и смысл анонимности в сети интернет. Автором предпринята попытка дать криминологическую оценку анонимности в сети Интернет, раскрыть её сильные и слабые стороны, проанализировать целесообразность запрета анонимности в сети интернет в качестве меры по профилактике мошенничества. Для этого предлагается выяснить, каким образом анонимность используется для совершения интернет-мошенничества, насколько эффективным будет её запрет и в каких случаях. При написании статьи использовался сравнительно-аналитический метод исследования. В заключении делается вывод, что эффективность предупреждения интернет-мошенничества зависит от проведения сбалансированной политики борьбы с киберпреступностью со стороны государства и общества.

Ключевые слова: интернет-мошенничество, мошенничество в сети Интернет, анонимность интернета, информационная безопасность, компьютерное мошенничество.

PROHIBITION OF ANONYMITY ON THE INTERNET AS A MEASURE TO PREVENT FRAUD

N. Semenova

Summary. This article analyzes the possibility of legislative introduction of a ban on anonymity on the Internet, as a fraud prevention measure, reveals the types and meaning of anonymity on the Internet. The scientific novelty of the article lies in the fact that the author makes an attempt to give a criminological assessment of anonymity on the Internet, to reveal its strengths and weaknesses. The expediency of banning anonymity on the Internet as a measure to prevent fraud is also analyzed. To do this, the author intends to find out exactly how anonymity is used to commit Internet fraud and how effective its ban will be and in what cases. Comparative-analytical research method is used in the analysis. In conclusion, it is concluded that the effectiveness of preventing Internet fraud depends on the implementation of a balanced policy to combat cybercrime by the state and society.

Keywords: internet-fraud, Internet fraud, internet anonymity, information security, computer fraud.

Слово анонимность происходит от греч. *ἀνωνυμία* «безымянность» от *ἀνώνυμος* «безымянный», неизвестный. Идея анонимности заключается в невозможности идентифицировать субъекта, однако анонимность может быть связана с понятиями конфиденциальности, свободы и безопасности.

Вопрос о целесообразности запрета анонимности в сети интернет, с правовой точки зрения остаётся мало изученным. Запрет анонимности, вызывает массовые споры, критику и даже протесты. Некоторые сторонники анонимности в интернете, справедливо опасаются, что такой запрет затронет их право на конфиденциальность персональных данных, личную и коммерческую тайну. В обоснование своих доводов они приводят понятие анонимности как способа защиты от противоправных действий третьих лиц, в том числе и мошенников.

Так по мнению Кецко К.В, для субъектов электронной коммерции, анонимность в сети Интернет, с одной стороны является преимуществом, с другой вызывает

опасения участников, несет определенные риски. Это, в частности, доступность внешнего проникновения, спам-атаки, создание сайтов-дубликатов [1, с. 58].

Другие авторы относят анонимность в сети Интернет к проблемам правового регулирования цифровых технологий, связанным с реализацией прав и свобод граждан. Они утверждают, что анонимность пользователя — это его конституционная гарантия, обеспечивающая охрану тайн его личной жизни. При этом авторы не исключают ограничение анонимности, когда она используется во вред охраняемым законом, общественным отношениям [2, с. 5].

Сторонники запрета анонимности в сети интернет, считают, что тем самым, можно снизить количество преступлений в виде мошенничества в сфере компьютерной информации. Как доказательство своей точки зрения, они приводят тот факт, что анонимность, затрудняет поиск лиц, совершивших мошеннические действия и сбор доказательств по соответствующим преступлениям.

Идея о запрете анонимности в интернете является не новой. Ее ещё в 2011 году подержал один из ведущих мировых специалистов в сфере информационной безопасности Евгений Касперский. Однако в настоящее время на сайте https://www.kaspersky.ru пользователям предлагают услуги, маскирующие уникальный IP-адрес и гарантирующие полную анонимность в интернете.

Общеизвестным является факт, что основная проблема профилактики интернет-мошенничества заключается в том, что способы совершения мошенничества меняются с огромной скоростью.

Предупреждение интернет-мошенничества во многом зависит от того, насколько известен способ его совершения. Сегодня, правоохранители не успевают проанализировать все способы и предложить соответствующие меры профилактики, тем более довести эти профилактические меры до широкого круга лиц, которые потенциально могут стать жертвами интернет-мошенников.

Фактически профилактикой интернет-мошенничества занимаются как правоохранительные органы и государственные структуры, так и медиа и IT гиганты, такие как Google, Yandex, другие. Кроме того, профилактикой занимаются и субъекты предпринимательской деятельности — это банки, крупные корпорации, операторы сотовой связи, организации, занимающиеся разработками IT продуктов, другие организации и физические лица, так или иначе заинтересованные в информационной безопасности в сети Интернет.

Возможности социальных методов профилактики интернет-мошенничества ограниваются восприятием субъектами профилактики профилактической информации и невозможностью раскрыть и донести до широкого круга пользователей, не только все схемы интернет- мошенничества, но и даже основные паттерны социальной инженерии используемые мошенниками. В человеческих отношения, возможно всё, что угодно, восприятие людей сложно сориентировать на распознавание мошенничества, поэтому мошенники без особого труда находят своих жертв.

Что касается технических способов профилактики интернет-мошенничества, то речь идет о разнообразных программных методах, призванных защитить устройства, выходящие в сеть Интернет от различного рода атак злоумышленников. Сюда можно отнести различные антивирусные программы, сервисы типа CheckShortURL, используемые для проверки сайта на наличие вредоносных программ. Например, когда человек собирается перейти по ссылке на сайт.

Несмотря на разнообразие и всеобъемлющий характер профилактических мер, направленных профилактику и борьбу с мошенничеством в сети интернет, практика показывает, что сегодня, этих мер уже недостаточно, уровень интернет-мошенничеств за последние два года резко возрос. Как следует из отчета Центробанка, всего за период времени с января по март 2021 года мошенники украли путем несанкционированных переводов у граждан и компаний в России 2,9 миллиардов рублей, что на 57% больше, чем в первом квартале 2020 года [3].

Профилактика мошенничества в сети Интернет в криминологическом аспекте, имеет некоторые затруднения вызванные тем, что интернет-мошенничество представляется, как мошенничество с использованием интернета как глобальной виртуальной сети, а также мошенничество с использованием интернет-связи. В последнем случае — это технология подключения к глобальной сети Интернет. При обсуждении вопроса анонимности в сети Интернет, понимание этих нюансов в контексте интернет-мошенничества необходимо для правильной квалификации деяний, образующих состав преступления.

Говоря об анонимности в сети, необходимо разграничивать анонимность в обыденном понимании, анонимность данных и анонимность в техническом аспекте. Эти аспекты хотя и связаны между собой, всё же имеются существенные различия по содержанию.

Что касается анонимности в обыденном понимании, речь идет, прежде всего, о возможности использова-

ния псевдонимов, вымышленных имен, создания в социальных сетях страниц, не содержащих личных данных, таких как имя, фамилия, другой информации, в том числе фотографий, позволяющей идентифицировать пользователя или опознать его. Не всегда такие страницы создаются с целью совершения мошенничества. Для многих это шанс пообщаться без идентификации, возможность будучи не опознанным, просматривать чужие страницы, выражать свои мысли, без боязни быть, в чем либо уличённым, или в иных целях. Это так называемые, «технические» аккаунты.

В данном случае анонимность пользователей довольно условна, если речь идет о добропорядочных гражданах, ведь для регистрации в социальной сети, добропорядочным пользователям приходится оставлять какие-либо данные о себе.

Другое дело, когда в социальных сетях и на торговых площадках, например, «Авито», под вымышленными именами скрываются профессиональные мошенники, которые регистрируют страницы по сим-картам, оформленным на подставных лиц, а в сеть выходят, используя специальные программы анонимайзеры, что существенно затрудняет их поиск. Однако, сами социальные сети, сайты знакомств и торговые площадки довольно быстро реагируют на такие подозрительные страницы, блокируя их деятельность.

В данном случае можно говорить об ограничении или запрете анонимности с целью профилактики мошеннических действий, при которых потерпевшие лица, подвергшись обману, сами передают, принадлежащие им денежные средства мошенникам, например в счёт оплаты несуществующих товаров или услуг, на благотворительность, в долг или на другие цели.

Безопасность пользователей в социальных сетях, на сайтах знакомств, а также на торговых площадках, в большей степени зависит от выполнения ими несложных правил, касающихся общения и обращения с денежными средствами. Полностью исключить обман и обезопасить каждого пользователя таких сайтов, запретив регистрацию анонимных страниц, представляется нам маловероятным. Добропорядочные граждане будут предоставлять паспортные данные при регистрации, предоставлять биометрические данные, а мошенники найдут способы, например, вскрыть чужие «настоящие» страницы и, как это практикуется сейчас, совершать преступные действия через них. Формально, запрет анонимности в социальных сетях и на торговых площадках повысит уровень доверия пользователей, в результате чего, мошенники только выиграют. В правовом плане, на выше упомянутые платформы будут возложены дополнительные обязанности по контролю и выявлению, ещё на стадии регистрации, недобросовестных пользователей, что неминуемо приведет к дополнительным затратам, которые скажутся на обычных пользователях, в отдельных случаях регистрация может стать платной или цена на регистрацию, если она была платной, возрастёт.

Когда речь идет об анонимности данных, то имеется ввиду идентификация анонимных данных конкретного лица в сети Интернет. Необходимо отметить, что в настоящее время возможности идентификации данных физических и юридических лиц в сети Интернет весьма велики без применения каких-либо специфических технических методов. Например, в социальных сетях, многие пользователи добровольно выкладывают информацию о себе. Здесь можно говорить об имени, дате рождения, семейном положении, номере телефона, транспортных средствах, включая государственные номера, данные геолокации и другую информацию, которую мошенники могут использовать в своих целях. Юридические лица так же выкладывают в сеть свои данные, используя которые можно узнать большинство интересующей информации. Но когда речь идет о защите персональных данных, коммерческой тайны или данных, которые физическое или юридическое лицо не хотело бы придать огласке, например данные о наличии счетов в банках и тому подобные, необходимо иметь ввиду, что для сохранности этих данных применяются технологии анонимизации данных. Анонимизация является способом обработки данных, в результате которого происходит преобразование идентификационной информации таким образом, чтобы по полученным данным нельзя было определить их принадлежность тому или иному субъекту. Анонимность данных рассматривается в качестве меры безопасности и должна, неукоснительно соблюдаться всеми субъектами оперирующими этими данными. Однако, как показывает практика, утечки данных происходят даже в крупных корпорациях. Попадая в руки мошенников они используются ими в своих преступных целях. В этой связи необходимо учесть, что утечка данных происходят во многом благодаря тому, что они недостаточно анонимизированы, и вообще не защищены, часто они хранятся в незашифрованном виде, поэтому в определённых условиях становятся лёгкой добычей мошенников.

Так в феврале 2022 года в Бурятии завершилось расследование уголовного дела против 22-летнего жителя республики, обвиняемого в совершении преступлений предусмотренных частью 2 статьи 138 Уголовного кодекса РФ — «Нарушение тайны переписки, телефонных переговоров и иных сообщений граждан, совершённое с использованием служебного положения», частью 3 статьи 272 «Неправомерный доступ к охраняемой законом компьютерной информации» и частью 3 статьи 183

УК РФ — «Незаконное получение и разглашение сведений, составляющих коммерческую тайну». По данным следствия, 8 февраля 2021 года молодой человек устроился продавцом-консультантом в торговую точку дилера оператора сотовой связи. На следующий день он разместил в нескольких группах в популярном мессенджере объявления о том, что имеет доступ к конфиденциальной информации абонентов и готов предоставить её всем желающим за определённое денежное вознаграждение. В последующие несколько дней злоумышленник по запросам анонимных пользователей передал им сведения с детализацией телефонных звонков и сообщений восьми клиентов из разных регионов. За это ему заплатили 21 тысячу рублей [4].

Данный пример свидетельствует, о том, как отсутствие анонимизации данных, способствует совершению разнообразных преступлений. Становиться очевидным, что если данные попадают к мошенникам, то число мошенничеств неизбежно растет.

В целях профилактики такого вида преступности, необходимо возложить на компании повышенную ответственность за неправильное и незащищенное хранение персональных данных, стимулируя их, тем самым, применять более строгие меры к отбору сотрудников, имеющих доступ к персональным данным. Например, предлагать им проходить проверки на полиграфе при приёме на работу.

Однако наиболее проблемным и спорным аспектом в борьбе с интернет-мошенничеством, на сегодняшний день является инициатива ограничения анонимности в сети Интернет, в техническом аспекте. Идентификация в интернете или локальной сети возможна благодаря IP-адресам. IP означает «Интернет-протокол» — это набор правил, регулирующих формат данных, отправляемых через сеть. IP содержит информацию о местоположении устройства, обеспечивая его доступность для связи. По IP-адресам идентифицируют компьютеры, маршрутизаторы и веб-сайты в сети Интернет. IP-адрес назначается устройству интернет-провайдером. Любое действие в сети, любой запрос будет привязан к этому адресу.

Отбросив технические тонкости про то, какие бывают IP -адреса как они работают, отметим, что скрытие IP-адреса для добропорядочного пользователя — это способ защитить персональные данные и личность в сети Интернет, а для мошенника шанс остаться незамеченным и безнаказанным за совершенные им преступления. Зная IP-адрес, злоумышленники, с помощью специальных программ могут вести сбор статистики пользователя для передачи третьим лицам, определять его месторасположение, получать сведения о каких-либо действиях пользователя, в том числе компрометирующих его. Так, преступник сможет подтвердить чью-либо личность по IP-адресу системы, с целью, например загрузки какого-либо контента с IP-адреса этого пользователя. Такие действия совершаются часто с намерением загружать пиратские фильмы, музыку, видео, что является нарушением условий использования услугами провайдера. Может быть загружен контент, связанный с экстремизмом, терроризмом или детской порнографией, а также контент, способствующий совершению мошенничества, например, объявления о продажах товаров и услуг. Во всех случаях у правоохранительных органов возникают сложности с выявлением исполнителей. Отдельно отметим, что зная IP-адрес пользователя злоумышленники могут взломать устройство, заразить его вредоносными программами и использовать в своих преступных целях.

Мошенники могут использовать социальную инженерию, чтобы обманом заставить пользователя раскрыть IP-адрес. Например, они могут найти субъекта в Skype или аналогичном приложении для обмена мгновенными сообщениями, использующем IP-адреса для связи. Общение с незнакомцами в этих приложениях, предполагает, понимание того, что они могут видеть IP-адрес. Злоумышленники могут использовать инструмент Skype Resolver, позволяющий определить IP-адрес по имени пользователя.

Однако наиболее спорный метод профилактики, предлагаемый в настоящее время — это запрет операторам связи использовать «серые» IP-адреса, то есть публичные сетевые адреса, преобразованные по технологии NAT (Network Address Translation). Сторонники метода ссылаются на то, что технология NAT позволяет преступникам безнаказанно совершать все новые и новые преступления. Поэтому ввиду сложности их изобличения предлагается законодательно запретить операторам связи использовать протокол «Ipv4», а протокол «IPv6» применять как его альтернативу. Полагаем, что внедрение нового протокола может способствовать борьбе с преступлениями в сфере компьютерной информации, поскольку можно будет более точно выявить абонента, оставляющего электронные следы в сети Интернет.

Важно отметить, что данное предложение имеет смысл в долгосрочной перспективе, в ближайшие 10–15 лет, его реализация весьма затруднительна и экономически не обоснована. В настоящее время NAT (Network Address Translation) является базовой фундаментальной технологией и необходима для функционирования сети. А для перехода на протокол «IPv6» необходима замена аппаратно-технологической базы. То есть один IP-адрес должен соответствовать одному

устройству, что на сегодняшний день технологически невозможно воплотить. Попытки же быстро осуществить данную политику могут повлечь обрушению сети Интернет. Кроме того, NAT (Network Address Translation) не является как таковой технологией анонимизации, анонимизация в данном случае, является её побочным продуктом.

К сожалению, что авторы таких предложений часто не приводят достаточных доказательств того, что запрет NAT (Network Address Translation) повысит уровень безопасности сети и снизит уровень преступлений в сфере обращения охраняемой законом информации. Более того, предлагая запретить NAT (Network Address Translation), необходимо ссылаться на исследования о экономической целесообразности такого запрета и провести оценки рисков для безопасности государства.

Говоря об отмене NAT (Network Address Translation) необходимо понимать, что во-первых преступники могут использовать и другие технологии анонимизации, например VPN тоннель (англ. Virtual Private Network — виртуальная частная сеть) или Проект I2P. I2P.

На наш взгляд, для вынесения предложения о законодательном запрете NAT (Network Address Translation) необходимо привлечение экспертов в сфере безопасности сетей к исследованию данного вопроса.

Нельзя игнорировать тот факт, что анонимность в сети Интернет имеет огромное значение для безопасности предприятий, компаний и государственных структур, так как анонимные каналы необходимы для передачи информации благонадежным участникам правоотношений. Именно анонимность в данном контексте, выступает гарантом безопасности от преступных посягательств. Большинство сервисов безопасности используют именно технологии NAT (Network Address Translation).

На практике для того чтобы остаться не идентифицированными в сети Интернет, используется множество разнообразных методов. Например, использование анонимайзеров, вход в интернет с зарубежных IP-адресов, использование серверов, получающих почтовые сообщения и переправляющих их по адресам, указанным отправителем, так называемые ремейлеры, когда при переадресовке, информация об отправителе уничтожается, использование Tor (The Onion Router — луковая маршрутизация) и VPN (Virtual Private Network — виртуальная частная сеть). Использование VPN с Tor обеспечивает максимальную анонимность.

Таким образом, можно сделать вывод, что для профессиональных интернет-мошенников, проблемы преодоления анонимности в сети Интернет не являются столь серьёзными, полагаем, что со временем преступники будут только совершенствоваться в уничтожении следов своей деятельности в сети Интернет. Поэтому, для решения вопроса о законодательном запрете анонимности в сети Интернет, необходима тщательная оценка всех положительных и отрицательных последствий запрета. Для решения этого вопроса должны быть привлечены специалистов из разных сфер деятельности, начиная от IT и заканчивая криминалистами, криминологами и психологами. В противном случае запреты как мера профилактики мошенничества в сети Интернет приведут к ограничению возможностей и прав добросовестных участников правоотношений, что является недопустимым.

Что же касается профилактики интернет-мошенничества, полагаем, прежде всего, необходимо совершенствовать техническую защиту, проводить более глубокую профилактическую работу среди населения. Особенно со стороны субъектов, предоставляющих услуги сотовой сети и интернет, со стороны социальных сетей, торговых площадок. Очень важным является контроль за хранением и обработкой данных. Именно утечка данных даёт наибольшие возможности интернет-мошенникам осуществлять свои преступные намерения.

Эффективность предупреждения интернет-мошенничества зависит от проведения сбалансированной политики со стороны государства и общества в борьбе с киберпреступностью.

Законодательная защита интересов бизнеса, электронной коммерции, неминуемо приведёт к тому, что бизнес-сообщество получит более широкие возможности по укреплению и развитию технологий защиты от интернет-мошенничества и других киберпреступлений.

ЛИТЕРАТУРА

1. Кецко К.В. Преступность в сфере электронной коммерции // Российский следователь. 2021. N9. С. 58–63.
2. Уваров А.А. Проблемы использования цифровых технологий при реализации прав и свобод граждан // Право и цифровая экономика. 2020. N2. С. 5–11.
3. Евгения Чернышова https://www.rbc.ru/finances/09/07/2021/60e845c39a794772e1d0e21e

4. Артемий Иванов https://www.infpol.ru/238278-v-ulan-ude-sotrudnik-salona-sotovoy-svyazi-prodaval-personalnye-dannye-klientov/.
5. Уголовный кодекс Российской Федерации» от 13.06.1996 N63-ФЗ (ред. от 28.01.2022 N3-ФЗ) // Российская газета от 31 января 2022 г. N202.
6. Федеральный закон от 28.12.2009 N381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации» (ред. от 02.07.2021) // Собрание законодательства Российской Федерации от 5 июля 2021 г. N27 (часть I) ст. 51823.
7. Федеральный закон от 27.07.2006 N152-ФЗ «О персональных данных» (ред. от 02.07.2021) // Собрание законодательства Российской Федерации от 5 июля 2021 г. N27 (часть I) ст. 5159.
8. Федеральный закон от 07.07.2003 N126-ФЗ «О связи» (ред. от 30.12.2021) // Собрание законодательства Российской Федерации от 3 января 2022 г. N1 (часть I) ст. 34.

Журнал «Современная наука: актуальные проблемы теории и практики»

Бурятский государственный университет