Таким образом, государства Центрально-Азиатского региона стоят перед необходимостью выработки собственной политики и идеологии в правовой, образовательной и информационно-просветительской сферах. Это даст возможность проведения глубокой профилактики распространения радикальной религиозной идеологии, устранения негативных представлений об исламе, имеется также необходимость в модернизации подходов к религиозному и религиоведческому образованию, которые в странах Центральной Азии пребывают не в лучшем состоянии.

Список литературы

1. *Маликов К.* Экстремистские группировки как инструмент влияния геополитических игроков // Материалы итогов проведенного Форума улемов и исламских деятелей Центральной Азии «Согласие и созидание — традиционная основа ислама в Центральной Азии». Бишкек, 2016. С. 74.

2. *Юлдашев М. Б.* Мнения и позиция улемов Центральной Азии о религиозном радикализме и экстремизме // Там же. С. 51.

3. *Ибраев З.* Мусульманское духовенство Центральной Азии объединилось в борьбе против идеологии экстремизма. URL: http://knews.kg/2015/03/musulmanskoe-duhovenstvo-tsentralnoy-azii-obyedinilos-v-borbe-protiv-ideologii-ekstremizma/ (дата обращения: 19.03.2017).

УДК 342.9

Анонимность в глобальных сетях

А. А. Симаков

Защита российского информационного пространства в глобальных сетях от внешней информационной агрессии заставляет с высокой степенью осторожности относиться к правовому регулированию отношений в глобальных анонимных сетях и, в частности, к анонимной пиринговой сети DarkNet. Большинством пользователей глобальных сетей в России востребованы услуги не их анонимности, а защищенности передачи информации (как в правовом, так и в техническом смысле), особенно если эти услуги связаны с электронной коммерцией. Защита от внешних источников угроз по отношению к нашему государству — одна из приоритетных задач национальной безопасности России на современном этапе.

Ключевые слова: анонимность, анонимайзер, прокси-сервер, криптовалюта, туннелирование, информационная безопасность, Интернет.

Анонимность в сети — основная задача компьютерных сетей, построенных на основе анонимных прокси-серверов. Существует круг лиц, которые хотели бы пользоваться возможностями глобальных сетей (желательно, без ограничений) и при этом скрывать свой IP-адрес. Причины такого поведения пользователей весьма разнообразны, причем они необязательно связаны с преступными деяниями. Например, многие понимают, что чем меньше информации о собственном доступе в компьютерную сеть известно другим пользователям сети, тем меньше шансов у злоумышленников удаленно воздействовать на компьютер или использовать его для противоправных действий. Положительным моментом анонимного доступа в сеть можно отнести и сужение каналов доступа на компьютер спама или назойливой рекламы.

Однако действия преступного характера, которые осуществляет анонимный пользователь в глобальной сети, имеют более широкий спектр. Экономические преступления, действия экстремистской направленности, методы информационных войн,

приобретение запрещенной информации — это далеко не весь перечень деяний, направленных против личности, общества, государства.

На современном этапе анонимность, присутствующая в глобальной сети (например, на основе «луковой» маршрутизации Tor), в созданной криптовалюте bitcoin позволяет беспрепятственно осуществлять разнообразные неправомерные сделки и финансовые операции различным экстремистским организациям.

Безнаказанность противоправных действий такого рода в Интернете дает повод ввести на законодательном уровне запрет анонимайзеров в сети, тем более что в некоторых странах подобная практика существует. Например, в Белоруссии введен запрет на анонимные сети (подобные компьютерной сети Tor) с февраля 2015 г.[1], в КНР установлена действующая по всей стране система «Золотой щит», выполняющая функции глобального firewall[2]. Учитывая напряженную международную обстановку, анонимные компьютерные сети действительно создают серьезную проблему национальной безопасности. Предложение о запрете или ограничении работы анонимайзеров заведомо приводит к вопросу об ограничении свобод в глобальной сети Интернет, а также к вопросу о возможности технической реализации данного проекта. Ограничение свобод в сети Интернет не является предметом рассмотрения данной работы, но даже при поверхностном взгляде можно сделать вывод, что проблема, скорее, искусственно обостряется в пределах определенного социума. Гражданин, пользуясь глобальными сетями, может использовать анонимайзеры лишь с одной целью — обезопасить обращение информации среди участников своего круга. Согласно этой точке зрения функцию защиты информации пользователя можно передать соответствующим государственным органам. Сформированная «государственная» сеть анонимайзеров сможет предоставить гарантии как надежности, так и приватности выхода в глобальную сеть Интернет. Разумеется, ни о какой анонимности со стороны государства речи быть не может, но в действительности для пользователя, который не намерен совершать неправомерные действия в среде Интернет, вряд ли это можно назвать серьезным недостатком. Техническая реализация проекта системы «государственной» сети анонимайзеров вполне осуществима, причем неофициально в целях национальной безопасности сеть анонимайзеров, контролируемая непосредственно государственными структурами, уже существует, о чем не раз сообщалось на различных сайтах глобальной сети.

Рассуждения о широких возможностях, которые предоставляет для граждан система платежей на основе криптовалюты, признаются в Российской Федерации спорными. На законодательном и техническом уровнях в нашей стране вопросы о криптовалюте и технологии blockchain, на которой они построены, ждут своих решений в ближайшее время[3].

Только недавно успели заполнить пробел в законодательстве, определив в Федеральном законе «О национальной платежной системе» статус электронных платежных систем, как предстали «новые денежные суррогаты». По крайней мере, так классифицировал (возможно, небезосновательно) криптовалюту ЦБ РФ[4]. Несмотря на прежние изъяны в понятийном аппарате, понятие «денежные суррогаты» до сих в законодательстве не определено. Кроме того, не решены организационные и технические трудности реализации криптовалюты. Мы согласны с мнением исследователей, указывающих на преждевременность внедрения криптовалюты на территории Российской Федерации, даже в случае их эмиссии непосредственно ЦБ РФ. Однако, столкнувшись с фактом существования незаконных финансовых операций с применением криптовалюты bitcoin, вполне разумно на некоторый период запретить обращение криптовалют на территории Российской Федерации. В дальнейшем, полагаем, нас ожидает рост интереса к криптовалюте. Возможно, в будущем ЦБ РФ изменит свое решение и согласится быть эмитентом «денежного суррогата» — криптовалюты, но для этого предстоит серьезная подготовительная работа в организационной, правовой и технической областях.

Учитывая внешние угрозы информационной безопасности нашей страны, думаем, далеко не последнее место занимает защита информационного пространства глобальной сети Интернет. Наше государство наравне с другими развитыми странами направляет существенные усилия на организационные,

---

[1] *Об утверждении* Положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет : постановление оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 г. № 6/8 // Национальный правовой Интернет-портал Республики Беларусь. 10.06.2015. №7/3059.

[2] *По данным* сайта TorMetrics, «Золотой щит» действует весьма успешно, количество пользователей сети Tor в многочисленном Китае составляет от 500 до 2500 чел. // TorMetrics. URL: https://metrics.torproject.org/userstats-relay-country.html?start=2015-12-23&end=2016-03-22&country=cn&events=off (дата обращения: 25.03.2016).

[3] *Греф* «оплакивает» судьбу криптовалюты в России. URL: http://rueconomics.ru/183565-gref-oplakivaet-sudbu-kriptovalyuty-v-rossii (дата обращения: 6.07.2016).

[4] Там же.

правовые и технические средства защиты информации в глобальной сети Интернет. Так, за последние два года введен значительный перечень ограничений на распространяемую информацию, ее размещение на сайтах [5].

Напряженность международной обстановки прямо пропорциональна активности использования анонимайзеров: методы информационной войны никто не отменял. Данные, которые систематически предоставляет сайт TorMetrics, указывают на то, что с 2014 г. уровень активности использования системы Tor вывел Россию в тройку лидеров вместе с США и Германией (примечателен пик активности в России в сети Tor на февраль 2016 г. — более 270 тысяч человек) [6]. Это тревожный сигнал, ведь утверждение о том, что все граждане России настолько ущемлены в правах и свободе, что только анонимные прокси-серверы системы Tor являются для них «отдушиной», весьма сомнительно. Более правдоподобным выглядит факт, что США еще в начале конфронтации с Россией в информационной войне стали активно использовать в своей подрывной деятельности систему Tor. Например, А. Навальный рекомендует использовать Tor для общения с его фондами, в том числе с Фондом борьбы с коррупцией [7].

Настораживающую информацию можно также прочесть в заявлении представителя ФБР США об успешном внедрении специального программного обеспечения в ряд серверов сети Tor для перехвата истинных IP-адресов компьютеров, принадлежащих пользователям данной сети. Цель декларируется в заявлении благая — поимка преступников, распространяющих детскую порнографию, однако интересен сам факт возможности внедрения программного обеспечения такого рода [8]. Другими словами, контроль за серверами сети Tor предоставляет широкие возможности для слежения за пользователями компьютерной сети. Стоит напомнить о сотруднике Агентства национальной безопасности США Э. Сноудене, постоянно поддерживающем один из серверов сети Tor.

Становится понятным желание российских силовых структур отслеживать вход-выход пользователей сети с «луковой» маршрутизацией (вспомним о конкурсе, объявленном в 2014 г. Федеральным казенным учреждением «Научно-производственное объединение „Специальная техника и связь“» Министерства внутренних дел Российской Федерации в Российской Федерации, с призом почти в 4 млн руб. [9]).

В России 2015 г. характеризуется повышенной активностью в борьбе с сайтами сети Tor. Роскомнадзор систематически блокирует занимающиеся противоправными деяниями сайты, которые зарегистрированы в различных странах мира [10].

При кратком рассмотрении компьютерной сети на основе «луковой» маршрутизации можно выделить ряд основных особенностей ее построения.

Большинство анонимных компьютерных сетей используют случайную цепочку узлов при передаче информации от пользователя к ресурсу и обратно. При этом каждому узлу в цепочке известно лишь, от кого пришли данные и куда их передавать дальше, поэтому восстановить всю цепочку и отследить пользователя очень сложно. Например, по такому принципу работают системы Tor и I2P. В сети Tor за счет технологии туннелирования данные пользователей шифруются, что обеспечивает конфиденциальность. «Луковая» маршрутизация, благодаря генерации случайной цепочки прохождения пакетов через серверы сети Tor и шифрования служебной информации для каждого узла отдельно, предоставляет пользователю приватную сессию, т. е. весьма проблематично при использовании такой технологии выявить отправителя информации.

Приблизительно с 2006 г. в сети Интернет стали появляться названия анонимных сетей, такие как DeepWeb (DeepNet), в переводе на русский чаще других употребляется словосочетание «глубинный Интернет (глубинная сеть)», другой термин «DarkNet», обычно определяют как темную часть глубинного Интернета — ту часть, что связана с различными неправомерными и преступными деяниями. И DeepWeb и часть его — DarkNet обеспечивают анонимность пользователей посредством принципа «луковой» маршрутизации. Компьютерная сеть DeepWeb (глубокая сеть) получает в мире все большее распространение. В настоящее время DeepWeb в основном построена на основе «луковой» маршру-

[5] *Об информации*, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ // Рос. газета. 2006. 29 июля.

[6] URL: https://metrics.torproject.org/userstats-relay-country.html?start=2015-12-23&end=2016-03-22&country=ru&events=off (дата обращения: 25.03.2016)

[7] *Фонд* борьбы с коррупцией завел защищенный «черный ящик» для анонимных «сливов» информации о чиновниках. URL: http://www.newsru.com/russia/11jun2014/ blackbox.html (дата обращения: 25.03.2016).

[8] *Создана* более быстрая и надежная альтернатива анонимной сети Tor. URL: http://www.cnews.ru/news/top/sozdana_bolee_bystraya_i_nadezhnaya_alternativa (дата обращения: 25.03.2016).

[9] *МВД* хочет получить доступ к данным пользователей анонимной сети Tor. URL: http://tass.ru/obschestvo/1338815 (дата обращения: 25.03.2016).

[10] *Создана* более быстрая и надежная альтернатива анонимной сети Tor. URL: http://www.cnews.ru/news/top/sozdana_bolee_bystraya_i_nadezhnaya_alternativa (дата обращения: 25.03.2016).

тизации, которая на базе системы Tor предоставляет анонимное пользование информационными ресурсами глобальной сети.

Кто является разработчиком технологии «луковой» маршрутизации на основе Tor? Чтобы понять причины быстрого развития данной сети, требуется ответить на еще один вопрос — каковы источники финансирования проекта сети Tor?

Данные о разработчиках в глобальной сети Интернет весьма скудные, хотя и распространены повсеместно, причем очевидны признаки тиражирования некоего одного первоисточника по другим сайтам. Из имеющейся информации известно, что в конце 90-х годов XX в. в Центре высокопроизводительных вычислительных систем Исследовательской лаборатории Военно-морских сил США в рамках проекта FreeHaven совместно с DARPA была разработана система, названная в дальнейшем TheOnionRouter (Tor). Исходя из утверждения, что система разрабатывалась в рамках федерального заказа, можно предположить, что силовым структурам США потребовалась глобальная сеть не только с анонимным входом и выходом, но и защищенная от прослушивания. Создание защищенных каналов связи — это разумное желание для любого сильного государства. Как во времена разработчиков данной сети, так и в настоящее время конфиденциальный канал связи формируется на основе виртуальных туннелей, которые позволяют обеспечить передачу информации в зашифрованном виде. Система Tor не исключение. Но, в отличие от виртуальных частных сетей (VPN), широко использующихся коммерческими организациями, глобальная сеть на основе прокси-серверов системы Tor обеспечивает анонимность в общении. В 2002 г. все результаты проекта Tor были обнародованы вместе с исходными текстами и выпущены клиент-серверные приложения со свободной лицензией.

Вопрос об источниках финансирования требует отдельного исследования, так как очень сложно проследить цепочки взаимосвязей всех коммерческих и некоммерческих организаций, участвующих в проекте создания сети Tor. На официальном сайте TorMetrics можно выделить несколько основных игроков — Министерство обороны США и Государственный департамент США, некоммерческая правозащитная организация Electronic Frontier Foundation (учреждена в США, сейчас имеет свое представительство в Европе), всех других ежегодно меняющихся организаций, как правило, связывает страна регистрации — США.

По большому счету, для рядовых пользователей анонимных сетей анонимность остается скорее мнимой, чем действительной. Во-первых, анонимность периодически нарушается, в том числе в сети, построенной на серверах TOR. Во-вторых, если учесть, что все спецслужбы развитых стран никогда не оставят попыток контролировать в той или иной степени анонимные компьютерные сети, а силовые структуры США принимают непосредственное участие в создании компьютерной сети на основе Tor в глубинном Интернете, также следует принять во внимание факт финансирования этой сети как государственными организациями США, так и сомнительными частными фондами, то можно прийти к выводу о серьезной опасности состояния защищенности пользователя в анонимных сетях, в частности, на основе прокси-серверов Tor.

В целях национальной безопасности нашего государства итогом такого положения дел может быть разумное ограничение вредной, недоброкачественной информации в Интернете (так же, как это осуществляется в других средствах массовой информации) и создание государственной системы анонимных прокси-серверов на основе «луковой» маршрутизации, которая позволит защитить от ряда внешних угроз в глобальной сети не только простых граждан нашей страны, но и государственные, коммерческие и иные организации. Сейчас востребованность большинства наших граждан в надежном и конфиденциальном общении в глобальных компьютерных сетях очень высока, а доверие к отечественной разработке анонимной сети на основе «луковой» маршрутизации, где гарантом выступает наше государство, будет значительно выше, чем к аналогичным проектам, созданным при поддержке силовых структур США. А если ЦБ РФ решится стать гарантом отечественной криптовалюты в ближайшем будущем, то значительная часть преступлений, связанных с несовершенством защиты информации в современных платежных системах, будет заведомо устранена.

Однако передавать в руки государства свою конфиденциальную информацию, в том числе и коммерческую тайну, согласны далеко не все коммерческие организации. Вопрос приватности в глобальной сети Интернет остается открытым.