УДК 343(575+14) 004.7

ПОЛУЧЕНИЕ ИНФОРМАЦИИ В ИНТЕРЕСАХ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Молоков В.В.,
кандидат технических наук, доцент
(Сибирский юридический институт МВД России)

Аннотация: в статье рассматривается проблема криптографического закрытия информации в телекоммуникационных сетях в контексте возможности её получения правоохранительными органами в интересах раскрытия и расследования преступлений. Приводятся основания для законного получения криминалистически значимой информации и варианты доступа к ней на ресурсах сети Интернет.

Ключевые слова: Интернет, интернет-коммуникации, криптография, криминалистически значимая информация, раскрытие и расследование преступлений.

GETTING INFORMATION IN THE INTERESTS OF THE CRIME DISCLOSURE AND INVESTIGATION UNDER CONDITIONS OF DATA ENCRYPTION IN THE TELECOMMUNICATION SYSTEMS

Molokov V.V.,
Candidate of Technical Sciences, Associate Professor
(Siberian Law Institute of the MIA of Russia)

Abstract: this paper considers the problem of the information encryption in the telecommunication networks in the context of the possibility of its receiving by law enforcement agencies in the interests of disclosing and investigating crimes. The basic for legitimately obtaining forensic information and the options for accessing it on Internet resources are given.

Keywords: Internet, Internet communications, cryptography, forensic information, crime disclosure and investigation.

Современная преступность все чаще использует новейшие достижения в области информационно-телекоммуникационных технологий для осуществления криминальных замыслов [1]. Интернет-технологии используются для управления организованным преступным сообществом, с их помощью совершаются мошеннические действия, осуществляется незаконный сбыт наркотиков и оружия, происходит легализация денежных средств, добытых противоправной деятельностью, и т.п. И эта тенденция не случайна, так как развитие

интернет-коммуникаций осуществляется в сторону анонимизации личности пользователя и скрытия передаваемой в каналах связи информации. В этой связи актуальными являются меры противодействия подобного рода преступным проявлениям, успешной реализации которым может способствовать возможность документирования информации, передаваемой по телекоммуникационным каналам сети Интернет.

Вопрос анонимности пользователей сети Интернет не раз обсуждался в многочисленных публикациях [2]. В основе этого лежат два механизма обезличивания коммутируемого сетевого устройства – это скрытие IP-адреса и закрытие передаваемой информации средствами криптографии. Для этого используются вполне легальные средства, реализующие одну из обозначенных технологий либо представляющие их гибридное сочетание. Тому примеры: анонимные прокси-сервера, VPN-сервисы, SSH-туннели, децентрализованные сети (Tor, P2P и т.п.). На волне всеобщей конфиденциальности наибольшую популярность завоевали интернет-мессенджеры, открыто декларирующие сквозное шифрование, больше известное как end-to-end. Суть данного метода заключается в организации закрытого взаимодействия между участниками информационного обмена без разглашения данных третьим лицам, включая организаторов сервиса. Поэтому так популярны раскрученные мессенджеры Viber, WhatsApp, Telegram. Не секрет, что на каналах Telegram открыто работают площадки по торговле наркотическими средствами и психотропными веществами.

Современную ситуацию на рынке интернет-коммуникаций можно охарактеризовать тотальным господством криптографии. В чем секрет применения сквозного шифрования? Таким вопросом могут задаться большинство рядовых пользователей Интернета. Скорее, дело не в секрете, а в популярности. Классический алгоритм Диффи-Хеллмана использует систему открытых ключей для генерации закрытого симметричного ключа на противоположных сторонах информационного обмена. И такой механизм не компрометирует секретный ключ. Однако существуют некоторые уязвимости оригинального алгоритма Диффи-Хеллмана, например, атака «человек посередине». Поэтому разработано немало модификаций алгоритма, которые лишены данной уязвимости. На текущий момент можно утверждать, что сам принцип сквозного шифрования является достаточно криптостойким и надежно защищает от перехвата данных в канале связи.

Складывается ситуация, что с повышением уровня защиты информации, хранящейся и обрабатываемой в телекоммуникационных системах, растет степень ее конфиденциальности и анонимности. Безусловно, такая тенденция в условиях цифровизации экономических и иных общественных отношений является предпочтительной и оправданной. Однако, как было обозначено ранее, преступность все чаще использует возможности современных средств сетевой коммуникации, зачастую опережая в технической и технологической оснащенности правоохранительные органы.

Таким образом, для успешного противодействия преступлениям, совершаемым с использованием сети Интернет, необходимы мероприятия, связанные с получением значимой в интересах раскрытия и расследования преступлений инфор-

мации. Обозначим, какими возможностями обладают правоохранительные органы для осуществления документирования фактов преступной деятельности.

Во-первых, в соответствии со ст. 64 Федерального закона № 126-ФЗ «О связи» операторы связи обязаны хранить на территории Российской Федерации данные о фактах передачи информации в течение 3 лет, а сами сообщения и иные пересылаемые данные – в течение 6 месяцев. Это позволяет правоохранительным органам в законодательном порядке запрашивать необходимую информацию у интернет-провайдеров и интернет-компаний, осуществляющих свою деятельность на территории Российской Федерации.

Во-вторых, согласно тому же Закону «О связи» операторы связи должны быть оснащены средствами обеспечения оперативно-розыскных мероприятий. Данные средства позволяют субъектам оперативно-розыскной деятельности осуществлять снятие оперативно значимой информации. Обработка передаваемой по телекоммуникационным каналам информации осуществляется с использованием технологий глубокого анализа трафика, позволяя выделять данные отдельных приложений и абонентов сети Интернет. Вопросы получения оперативно значимой информации в сети Интернет неоднократно обсуждались в контексте противодействия преступлениям в сфере незаконного оборота наркотиков [3].

В-третьих, в связи с принятием Федерального закона от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», больше известного как Закон «О безопасном Интернете», появилась возможность оперативного и эффективного блокирования ресурсов сети Интернет, распространяющих противоправный контент. То есть, операторы связи и интернет-компании, не соблюдающие законодательство Российской Федерации, могут быть блокированы на территории нашей страны.

Получается, что законодательно и технически имеются возможности для получения оперативно и криминалистически значимой информации. Однако это может касаться открытых данных, представленных в виде, удобном для их восприятия и документирования. Имеются проблемы с информацией, закрытой криптографически без возможности расшифровки.

В этих условиях необходимо исходить из уязвимостей, которые обнаруживаются в самих механизмах передачи и трансформации обрабатываемой посредством компьютерных средств информации.

Во-первых, нет необходимости в перехвате шифрованной информации, размещаемой на серверах интернет-компаний, социальных сетей и иных сервисов. Открытую информацию можно законно запрашивать непосредственно у них самих.

Во-вторых, принцип сквозного шифрования в интернет-мессенджерах декларируется исключительно самими разработчиками систем коммуникаций. Непосредственно проверить программный алгоритм на наличие бэкдоров ввиду закрытости исходного кода не представляется возможным. Также странно работает механизм сквозного шифрования на нескольких устройствах, связанных с одной учетной записью. Процесс считывания защищенного кода происходит

однократно, а в дальнейшем передача сообщений дублируется на все устройства. Если постоянно используется один ключ, то это компрометирует его, если сеансовые ключи меняются, то ими управляют. Что также наводит на мысль о необходимости работы по предоставлению значимой информации непосредственно с операторами связи интернет-коммуникаций.

В-третьих, компании, оказывающие услуги связи на территории Российской Федерации, должны соблюдать российские законы, иначе их деятельность может быть ограничена. Соответственно, встает вопрос, как обеспечивается конфиденциальность от правоохранительных органов и специальных служб государства. Значит, необходимо контактировать с такими интернет-компаниями.

В-четвертых, электронное взаимодействие участников пересылки сообщений осуществляется компьютерными устройствами, которые работают с известными и популярными операционными системами типа iOS и Android. При этом сами системы создают резервные копии приложений и данных, сохраняя их на своих облачных серверах. Соответственно, вопрос доступа к информации можно решать через администрации компаний разработчиков операционных систем. Не исключением являются и сами мессенджеры, создающие резервные копии сообщений.

Анализируя представленные доводы, можно сделать выводы относительно предположения, что использование интернет-мессенджерами принципа сквозного шифрования не является безупречным с точки зрения обеспечения полной конфиденциальности сообщений. Правоохранительным органам необходимо в рамках существующего законодательства проводить целенаправленную работу с интернет-компаниями, осуществляющими свою деятельность на территории Российской Федерации, по получению оперативно и криминалистически значимой информации в интересах раскрытия и расследования преступлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Урбан В.В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию // Вестник Восточно-Сибирского института МВД России. 2019. № 1 (88). С. 55–63.

2. Молоков В.В. Средства противодействия раскрытию преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием сети Интернет / Национальный и международный уровни противодействия наркоугрозе и взаимодействие в сфере реабилитации и ресоциализации наркопотребителей: материалы XVIII международной научно-практической конференции. – Красноярск: СибЮИ ФСКН России, 2015. Ч. 2. С. 56–60.

3. Молоков В.В. Программно-технические системы получения оперативно значимой информации в телекоммуникационных каналах сети Интернет / Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXI международной научно-практической конференции: в 2-х ч. – Красноярск: СибЮИ МВД России, 2018. Ч. 2. С. 108–110.