УДК 378

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ТЕНЕВОГО ИНТЕРНЕТА ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ

MODERN TRENDS IN THE USE OF MEANS OF THE DARK INTERNET IN COMMISSION OF CRIMES IN THE SPHERE OF ILLEGAL DRUG TRAFFICKING

Петухов Андрей Юрьевич,
старший преподаватель кафедры оперативно-разыскной деятельности в органах внутренних дел Краснодарского университета МВД России (г. Краснодар), кандидат педагогических наук

petuhow—andrey@mail.ru

Куликов Кирилл Сергеевич,
курсант 4 курса Краснодарского университета МВД России (г. Краснодар)

kylikova_23_97@mail.ru

Ключевые слова:
теневой Интернет, глубинный Интернет, анонимные сети, незаконный оборот наркотиков, бесконтактный сбыт наркотических средств и психотропных веществ.

В статье рассматриваются современные тенденции использования средств теневого Интернета при совершении преступлений в сфере незаконного оборота наркотиков, проводится анализ основных механизмов использования информационных технологий преступными группировками с целью маскировки своей преступной деятельности.

Keywords:
dark Internet, deep Internet, anonymous networks, illegal drug trafficking, contactless sale of narcotic drugs and psychotropic substances.

The article considers the current trends in the use of means of the dark Internet in the commission of crimes in the sphere of illegal drug trafficking; the main mechanisms of the use of information technologies by criminal groups in order to disguise their criminal activities are analyzed.

Сеть Интернет вошла в нашу жизнь за какие-то пятьдесят с лишним лет настолько прочно, что на сегодняшний день мы просто не представляем себе жизнь без данного ресурса. При этом многие пользователи Всемирной паутины используют лишь малый объем всей информации, предоставляемой этим ресурсом.

В настоящее время классический Интернет делят на три условных части:

1. Открытый Интернет (Clear Net) – составляет примерно 4-5% от общего объема информации, эта часть Интернета доступна и открыта для всех пользователей с применением стандартных браузеров. Получить информацию можно с использованием общеизвестных поисковых систем (Google, Yandex и другие);

2. Глубинный Интернет (Deep Net) – составляет примерно 90-91% от общего объема информации, в основном это сайты или страницы, которые не индексируются, то есть которые не видимы в общеизвестных поисковых системах. Они доступны в определенных браузерах, либо по прямым ссылкам и размещаются на соответствующих ресурсах. Эти сайты предоставляют особого уровня значащую информацию в виде архивов, баз данных и т.д.;

3. Темный Интернет (Dark Net) – в среднем это 5% от общего объема информации, предоставляемой сетью. Dark Net является частью Deep Net, но его выделяют в отдельную категорию в основном по причине его общественной опасности и содержащейся в нем асоциальной информации.

С точки зрения предмета правоохранительной деятельности наибольший интерес представляют возможности последних двух групп, особенно при использовании их в преступной деятельности, а в частности сбыте наркотических средств бесконтактными способами и посредствам интернет-магазинов в сегменте темного или глубинного Интернета.

По самым скромным подсчетам, «дарквебом» – рынком нелегальной торговли – анонимно пользуются 2 миллиона человек в день по всему миру. С помощью криптовалюты и Tor-браузера здесь можно купить все: от марихуаны до документации к американским дронам. При этом покупки и транзакции невозможно отследить, а значит и предъявить обвинения. Администраторы и продавцы торговых точек зарабатывают на подпольном рынке до полумиллиона долларов ежемесячно. Государственные правоохранительные органы пытаются, но не могут заблокировать сайты «дарквеба», это технически невозможно. В 2015 году, после двух лет безуспешных попыток ФБР задержали Росса Ульбрихта, администратора первого известного подпольного рынка Silk Road. Суд приговорил его к пожизненному заключению. Однако ситуация не изменилась к лучшему: произошла децентрализация нелегальной торговли и на месте Silk Road появились сотни других торговых площадок. Кроме того, возникли отдельные движения, вдохновленные идеей «дарквеба». [1]

Для того чтобы воспользоваться ресурсами глубинного Интернета преступники используют соответствующий инструмент, обеспечивающий доступ, таким инструментом может выступать, к примеру, браузер The Onion Router или TOR. Это бесплатная программа, которая была разработана в Исследовательской лаборатории Военно-морских сил США в середине 90-х годов для защиты онлайн-коммуникаций спецслужб США. TOR имеет многоуровневую структуру, которая позволяет пользователю перемещаться в сети, переходя с одного уровня на другой, при этом пользователь защищен криптографическим алгоритмом, который позволяет скрыть его IP-адрес. При этом используется принцип «луковой» маршрутизации, который заключается в использовании цепи случайно выбранных компьютеров в различных частях мира, для того чтобы затруднить возможность определения местонахождения пользователя и, что более важно, установить личность пользователя.

При этом, несмотря поправки, изложенные в Федеральном законе от 29.07.2017 №276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»» в части статьи 15.8 «Меры, направленные на противодействие использованию на территории Российской Федерации информационно-телекоммуникационных сетей и информационных ресурсов, посредством которых обеспечивается доступ к информационным ресурсам и информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации», использование указанных ресурсов в преступной деятельности продолжается. [3]

Под действие закона потенциально попадают все прокси- и VPN-сервисы, а также анонимные сети Tor, I2P и Freenet. В рамках принятого закона владельцам указанных ресурсов предлагается ограничить доступ к сайтам, входящим в реестр запрещенных сайтов Роскомнадзора, при этом контролем за использованием анонимайзеров, Tor и VPN-сервисов, предоставляющих доступ к заблокированным в России сайтам, будут сотрудники ФСБ и МВД.

Браузер TOR имеет свой собственный домен – onion. Он позволяет привязать страницы глубинного Интернета именно к данному браузеру, если ввести ссылку на сайт с доменным именем «.onion». Если проводить эту процедуру в индексируемых (обычных) браузерах, то в качестве результата пользователь получит отказ в доступе. Немаловажным является то, что TOR реализует возможности работы с криптовалютами, в частности bitcoin. Эта криптовалюта является сегодня одной из самых популярных, и ее пытаются добывать все большее количество майнеров по всему миру, наша страна не исключение. Она также является источником информационного «шума» в виртуальном пространстве и СМИ. Вышесказанное обуславливает использование этой валюты в преступных махинациях, так как она позволяет скрытно совершать те или иные незаконные финансовые операции.

Для того чтобы использовать «закрытый» сайт глубинного интернета, необходимо знать соответствующую ссылку, получить доступ к ней возможно на некоторых ресурсах открытого Интернета. В основном это англоязычные сайты, но есть и русскоязычные. Таких сайтов в сети открытого Интернета большое количество, к примеру http://darkach.net или https://rottenswamp.ru. Как и общедоступный Интернет, теневой сегмент имеет свои поисковые системы, почту и интернет-магазины.

В качестве примеров поисковых систем глубинного Интернета можно привести следующие: Grams, not Evil, Torch и многие другие. Следует отметить следующие особенности данных поисковых систем: ссылки между onion-сайтами редки; сайты очень часто меняют адреса; немногие сайты можно найти даже в этих поисковых системах.

Электронная почта представляется такими ресурсами, как Crazy Mail, TempMail, Tor Guard. Отличительными особенностями этих почтовых сервисов являются шифрование, в основном PGP-шифрование, временное ограничение существования ящика (в среднем 10-50 минут), ограниченный объем сообщения.

Отдельно следует обратить внимание на то разнообразие информации, которое располагается в глубинном Интернете. Самыми безобидными являются форумы, на которых люди анонимно обмениваются мнениями, делятся опытом, раскрывают какие-либо секреты и т.п. Еще одним видом сведений глубинного Интернета выступают платформы для продажи персональных данных, продажи поддельных документов, размещения (обмена, предоставления) различной значимой информации во всевозможных сферах.

Таким образом, глубинный Интернет предоставляет возможности осуществления фактически любых финансовых операций в теневом секторе экономики, а также совершения всего спектра компьютерных преступлений. При этом следует подчеркнуть, что глубинный Интернет реализуется все же в сегменте свободного Интернета, свободного от цензуры, авторских прав и т.п.

Самым же опасным, как с точки зрения содержания, так и со стороны совершаемых деяний, является Dark Net. Фактически он использует все те же технологии, что и глубинный Интернет. На просторах темного Интернета можно за определенную сумму приобрести фактически любые запрещенные объекты, новый паспорт и иные документы, оружие, наркотические средства, человеческие органы, высококачественные подделки валют, украденные аккаунты Paypal и других сервисов, и т.п.

Связь с владельцами сайта происходит по электронной почте, посредством которой пересылаются фото и иная необходимая информация. Оплата обозначенного товара, как уже нами упоминалось, происходит при помощи bitcoin, либо других виртуальных валют. Технологии Blockchain, используемые в

данной криптовалюте, позволяют полностью обезличить участников сделки купли-продажи. Суммарные обороты денежных средств в данном сегменте теневого Интернета превышают уже 1,5 млрд долларов с 2012 года. Профильное агентство ООН – UNODC (Управление по наркотикам и преступности) оценивает объем подобных расчетов в несколько процентов от общего денежного оборота криптовалют – то есть мы можем говорить о $1-2 трлн в год. [4]

При обозначении нами возможностей теневого Интернета, безусловно, возникает вопрос о том, каким образом правоохранительным органам организовывать борьбу в данном сегменте, эффективно выявлять преступления, совершаемые с использованием этих технологий. Ведь проведение классических оперативно-розыскных мероприятий, очевидно, будет недостаточным и абсолютно неэффективным средством в такой борьбе.

В то же время оперативно-розыскное законодательство вполне четко формулирует исчерпывающий список возможных оперативно-розыскных мероприятий, которые могут проводить правоохранительные органы. В соответствии со статьей 6 Федерального закона от 12.08.1995 №144-ФЗ «Об оперативно-розыскной деятельности» к ним относятся: опрос; наведение справок; сбор образцов для сравнительного исследования; проверочная закупка; исследование предметов и документов; наблюдение; отождествление личности; обследование помещений, зданий, сооружений, участков местности и транспортных средств; контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; снятие информации с технических каналов связи; оперативное внедрение; контролируемая поставка; оперативный эксперимент; получение компьютерной информации. Соответственно, иными средствами документирование преступной деятельности в теневом Интернете просто невозможно.

Указанные проблемы проведения классических оперативно-розыскных мероприятий в совокупности с отсутствием лиц, установленных при их осуществлении в рамках рассматриваемых нами преступлений, демонстрируют достаточно негативную картину. Классические формы выявления преступлений просто не работают в этой плоскости правоотношений. Очевидной является необходимость выработки новых подходов к выявлению и пресечению таких преступлений.

Повысить эффективность работы правоохранительных органов по документированию преступлений в сфере незаконного оборота наркотиков в анонимных сетях вполне возможно. Для этого нужно пересмотреть возможности стандартных оперативно-розыскных мероприятий, методов их проведения применительно к сферам информационных технологий и, следует сказать, такой опыт уже имеется при документировании преступлений, совершаемых в классическом сегменте Интернета при осуществлении преступниками

бесконтактного сбыта наркотических средств. За последнее десятилетие правоохранительными органами накоплен достаточный и положительный опыт проведения таких мероприятий. Собственно, это и послужило причиной использования преступниками возможностей теневого Интернета для осуществления своих преступных замыслов.

Очевидно, что уже сейчас необходима реализация новой формы содействия граждан органам, осуществляющим оперативно-розыскную деятельность. Порой бороться с киберпреступлениями помогают сами преступники. Ведь Dark Net – это банка с пауками. Все эти торговые площадки очень не любят друг друга, а потому активно стараются вытеснить конкурентов. Недавно появились сведения о том, что Dark Net сжался на 85%. Такие подсчеты сделал проект OnionScan. Если в апреле 2016 года в сети Tor насчитывалось примерно 30 тысяч ресурсов, то к началу марта 2017 года осталось только 4,4 тысячи. Исследователи связывают это с прекращением работы популярного в теневом Интернете почтового сервиса Sigaint, а также с хакерской атакой в феврале на крупный хостинг FreedomHostingII. Тогда на десяти с лишним тысячах взломанных «луковых» сайтов появилось одинаковое сообщение, в котором взломщик объяснил, что решил «наказать» хостинг-провайдера за детское порно, которое во множестве обнаружилось на серверах FreedomHostingII. [1] Соответственно, такие факты предоставляют достаточно широкие возможности для правоохранительных органов в направлении реализации содействия граждан.

Необходимо в высокой степени эффективное сочетание (комплексное использование) оперативно-розыскных и уголовно-процессуальных методов фиксации следов преступления и собирания доказательственной базы.

Очевидным видится широкое привлечение возможностей специалистов (экспертов) из соответствующих отраслей знаний при осуществлении документирования и последующего расследования рассматриваемых преступлений на всех стадиях оперативно-розыскной и процессуальной деятельности.

И в конечном счете наиболее эффективной мерой повышения эффективности работы правоохранительных органов в борьбе с незаконным оборотом наркотиков, совершаемым посредством анонимных сетей, будет пересмотр организационно-тактических мер в отношении дел такой категории. Оперативно-розыскное обеспечение должно осуществляться безотрывно, как в рамках расследования уголовного дела, так и в рамках последующего судебного сопровождения.

Библиографический список

1. «Даркнет»: темная сторона Интернета // Официальный интернет-портал Парламентская газета. – URL: https://www.pnp.ru/politics/darknettemnaya-storona-interneta.html (дата обращения: 14.12.2018).

2. Идейная сторона темной паутины. Tor и биткоин. За что борются анархисты «дарквеба» // Официальный интернет-портал ZIMAMAGAZINE. – URL: https://zimamagazine.com/2018/09/darkweb-filosofia-kroptopanki-bitcoin/ (дата обращения: 21.02.2019).

3. О доле криптовалют в мировом обороте незаконных сделок // Официальный интернет-портал HASH TELEGRAPH. – URL: https://hashtelegraph.com/o-dole-kriptovaljut-v-mirovom-oborote-nezakonnyh-sdelok/ (дата обращения: 13.12.2018).