

Правоотношения, возникающие при проведении контролируемой поставки, неизбежно затрагивают интересы и сферу ответственности целого ряда государственных органов, уполномоченных на осуществление контрольной, надзорной и правоохранительной деятельности, а также организаций, осуществляющих свою деятельность в сфере перемещения предметов, документов, веществ железнодорожным, морским, автомобильным и авиасообщением. В случаях если канал поставки организован из-за рубежа и имеет конечный пункт на территории нашего государства, а также уходит за границу или проходит транзитом через территорию Республики Беларусь, о проведении контролируемой поставки через государственную границу письменно уведомляются таможенные органы и органы пограничной службы Республики Беларусь, прокурор или его заместитель.

В этой связи успешное достижение целей и задач по результатам проведения контролируемой поставки находится в прямой зависимости от созданных условий для надлежащей координации действий между заинтересованными государственными органами и организациями Республики Беларусь, а также обеспечения необходимого уровня взаимодействия с правоохранительными органами зарубежных стран.

Данное взаимодействие подлежит детальному регламентированию в законодательстве Республики Беларусь и международных договорах с наделением заинтересованных и привлекаемых к проведению контролируемой поставки субъектов соответствующими возможностями и полномочиями. Однако в настоящее время вопросы организации и проведения контролируемой поставки изложены лишь в декларативно-рамочной форме в некоторых актах законодательства, относящихся к сфере деятельности таможенных органов. При этом их абсолютное большинство использует понятие «контролируемая поставка» исключительно как метод выявления лиц, участвующих в совершении преступления, получения доказательств и обеспечения уголовного преследования.

В целях организации проведения контролируемой поставки специальными нормативными правовыми актами требуется установить порядок информирования о проведении указанного оперативно-розыскного мероприятия, привлечения необходимых сил и средств взаимодействующих сторон, проведения оперативно-розыскных и иных мероприятий вспомогательного и обеспечивающего характера, организации удаленного доступа и обмена между заинтересованными сторонами информацией из специализированных банков, баз данных и информационных массивов, предоставления и использования материалов ОРД.

Следует также учитывать, что при подготовке и проведении контролируемой поставки через государственную границу Республики Беларусь неизбежно возникнет необходимость обмена на международном уровне сведениями, составляющими государственные секреты. При этом в Законе Республики Беларусь от 19 июля 2010 г. № 170-3 «О государственных секретах» закреплено, что государственные органы и иные организации могут принять решение о передаче сведений, составляющих государственные секреты, иностранным государствам, международным организациям, межгосударственным образованиям только при наличии соответствующего международного договора Республики Беларусь о защите государственных секретов.

Отсюда можно сделать вывод о необходимости подготовки и издания актов законодательства Республики Беларусь, подписания международных договоров, подробно регламентирующих организацию взаимодействия по вопросам подготовки и проведения контролируемой поставки, информационного обмена между органами, осуществляющими ОРД, международными организациями, правоохранительными органами, специальными службами иностранных государств, а также обеспечения защиты государственных секретов.

УДК 343.085:004.9

П.Л. Боровик

ПРОБЛЕМНЫЕ ВОПРОСЫ ДЕАНОНИМИЗАЦИИ ЛИЦ, СОВЕРШАЮЩИХ БЕСКОНТАКТНЫЙ СБЫТ НАРКОТИКОВ В СКРЫТОМ СЕГМЕНТЕ СЕТИ ИНТЕРНЕТ (DARKNET)

Повышенная скрытность реализации механизма сбыта наркотиков в сети Интернет обеспечивается не только за счет полного исключения прямых контактов субъектов преступной деятельности между собой, но и за счет сложной сетевой инфраструктуры используемого при этом скрытого сегмента сети (DarkNet). Это существенно усложняет применение сотрудниками оперативных подразделений традиционных средств выявления и документирования преступлений.

Указанные обстоятельства обосновывают актуальность и необходимость выработки научно-обоснованных практических рекомендаций, направленных не только на выявление признаков преступлений в сети DarkNet, но и на установление (деанонимизацию) лиц, их совершающих.

Изучение открытых источников, посвященных данной проблематике, показало, что существуют некоторые возможности деанонимизации пользователя сети DarkNet (далее – резидента сети). Все они условно делятся на три основные группы: воздействие на браузер резидента сети; воздействие на соединение; анализ сетевой активности резидента сети.

Первая группа способов основывается на использовании средств эксплуатации уязвимостей к браузеру Firefox, с помощью которого осуществляется доступ к сети DarkNet (далее – Tor Browser). Так, например, использование программной библиотеки WebRTC, предназначенной для обмена данными в режиме реального времени между браузерами без промежуточных серверов, позволяет установить реальный IP-адрес резидента сети (несмотря на использование им технологий VPN и Proxy).

Вместе с тем подобный подход не всегда позволяет осуществлять эффективную поисковую работу в сети DarkNet. Это связано с тем, что жизненный цикл уязвимостей составляет всего от недели до нескольких месяцев, а существование версий Tor Browser, содержащих конкретную уязвимость, компрометирует весьма ограниченный круг резидентов сети, использующих скрытый сегмент интернета в противоправных целях.

Вторая группа способов основана на анализе так называемых записей NetFlow на маршрутизаторах, которые непосредственно являются узлами сети DarkNet или находятся недалеко от них. Как известно, NetFlow – проприетарный открытый протокол, предназначенный для мониторинга трафика в сети. Он предоставляет возможность анализа сетевого трафика на уровне сеансов, делая запись о каждой транзакции TCP/IP.

Несмотря на кажущуюся простоту и эффективность, указанный подход предполагает огромное количество точек присутствия внутри сети DarkNet, требуя наличия огромного пула вычислительных ресурсов, а поэтому также не представляет утилитарной ценности для органов внутренних дел.

Практический интерес представляет третья группа способов, основанная на анализе сетевой активности пользователя. В их основе лежит реализация тега «canvas», позволяющего генерировать растровые изображения при помощи JavaScript на платформе HTML5. Ключевая особенность подхода состоит в том, что рендеринг таких изображений каждый интернет-браузер осуществляет по-разному в зависимости от типа графического адаптера, аппаратно-программной составляющей компьютера, операционной системы и ее конфигурации. Следовательно, параметры отрисованных изображений могут уникально идентифицировать браузер и его программно-аппаратное окружение.

При помощи данного метода могут отслеживаться и другие параметры компьютера резидента сети, например: заголовки браузера и его настройки, программно-аппаратные характеристики экрана (разрешение, поддержка сенсорного ввода), часовой пояс, сведения об операционной системе и др.

Совокупность полученной информации позволяет сформировать так называемый «цифровой отпечаток», имеющий вид 32-битного числа шестнадцатеричной системы (например: b2cf59v35171389elf54d4ab413ac2jb), которое получается в результате обработки всех принятых от браузера данных.

Используя предложенный подход, исследователь может собрать достаточно обширную аналитическую информацию о резидентах сети с определенным цифровым отпечатком, изучив, например, историю его серфинга и авторизаций на сайтах. В последующем это может способствовать установлению круга его общения, социальных связей, интересов и предпочтений.

Дальнейшие действия по деанонимизации лиц, совершающих бесконтактный сбыт наркотиков в сети DarkNet, а также раскрытию соответствующих преступлений связаны с применением всего комплекса оперативно-розыскных сил, средств и методов, позволяющих не только идентифицировать личность конкретного лица, но и выяснить роль каждого из фигурантов, определить места закладок наркотических средств и каналы их сбыта, выявить способы транзакций, обналачивания и распределения денежных средств, а также установить иные обстоятельства, относящиеся к преступной деятельности.

УДК 338.45

А.А. Вишневецкий

О СОДЕРЖАНИИ СТРАТЕГИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Важным фактором обеспечения экономической безопасности государства является успешная интеграция Республики Беларусь в глобальное экономическое пространство, а защита от угроз экономической безопасности должна обеспечиваться полноценной многовекторной внешнеэкономической политикой, что поможет избежать различного рода ограничений для Республики Беларусь, в том числе и в рамках Евразийского экономического союза.

На наш взгляд, для реализации обозначенной цели необходимо создание полноценного правового механизма обеспечения экономической безопасности. В связи с этим представляется целесообразным предложить следующую иерархию нормативных правовых актов, направленных на правовое регулирование общественных отношений в сфере обеспечения экономической безопасности: Концепция национальной безопасности Республики Беларусь; Стратегия обеспечения экономической безопасности Республики Беларусь; Программа обеспечения экономической безопасности Республики Беларусь.

Следует отметить, что Стратегия обеспечения экономической безопасности (далее – Стратегия) должна представлять собой официальную позицию руководства Республики Беларусь в отношении основных целей, задач и направлений противодействия кризисным ситуациям, вызываемым воздействием внешних и внутренних угроз на экономическое развитие страны.

Стратегия призвана обеспечить комплексный подход к обеспечению экономической безопасности Беларуси на основе совершенствования правовых, экономических, финансовых, организационно-управленческих и других механизмов противодействия кризисным ситуациям в экономике и социальной сфере.

Целью Стратегии должно быть повышение качества государственного управления и координация деятельности органов государственной власти, государственных и общественных организаций по защите национальных, экономических интересов и обеспечению безопасности личности, общества и государства.

Задачами Стратегии следует определить: устойчивое социально-экономическое развитие Республики Беларусь на основе объединения материального и интеллектуального потенциала, использования рыночных механизмов функционирования экономики; содействие развитию взаимовыгодного сотрудничества в Беларуси в рамках ЕАЭС, со странами Европейского союза и иными государствами; устранение причин и условий, порождающих коррупцию; обеспечение экономической безопасности и эффективная борьба с преступностью, в том числе экономической.

Стратегия должна строиться на принципах преемственности государственной политики в сфере национальной безопасности, демократии и уважения прав человека, сотрудничества и взаимопомощи, добровольности, добросовестного выполнения взаимных обязательств и на других общепризнанных принципах и нормах международного права. Обеспечение экономической безопасности является составной частью управления экономикой государства.