конфиденциальность персональных данных – подход призван защитить неприкосновенность данных граждан посредством соответствующей архитектуры решений, выбором технологий, процессов, инфраструктуры. Ориентир – это те решения, в которых гражданин является владельцем собственных данных и вправе контролировать доступ к ним (например, банковские и медицинские данные);

сводная платформа анализа и обнаружения киберугроз, которая нацелена на поиск и выявление угроз благодаря работе со множеством городских и ведомственных баз данных, событий, фактического материала. Используя аналитику больших данных, машинное обучение, такая платформа позволяет формировать целостную картину пространства угроз с целью обеспечения правоохранительных органов возможностями сценарного планирования для профилактики различных правонарушений и более оперативного обнаружения и реагирования;

ответ на угрозы и устойчивость к атакам – подготовка, моделирование и проигрывание потенциальных сценариев позволят городам увеличить скорость реагирования и готовить превентивные ответные меры защиты. Устойчивые решения позволяют исключить сбои и отключения связных и высокоуровневых систем по причинам инцидентов на уровне отдельных систем или устройств;

повышение цифровой грамотности и экспертизы в вопросах цифровой безопасности – усложнение и цифровизация городских инфраструктур вызывает необходимость дополнительной и регулярной подготовки сотрудников и руководителей большого перечня ведомств и служб в вопросах кибербезопасности на уровнях физических устройств – персональных и технологических, цифровых баз данных, каналов коммуникаций, цифровых приложений;

согласованная стратегия реализации проектов «умного города» и кибербезопасности. Разрозненные структуры и ведомства с собственными подходами, базами данных, платформами и аналитикой необходимо объединять общими целями, приоритетами и метриками исходя из комплексного подхода к управлению угрозами и рисками, с пониманием взаимосвязей и зависимостей данных, процессов, событий – с возможностями профилактики, предотвращения, обнаружения и реагирования;

формализация согласованного сбора, хранения и управления данными, активами, инфраструктурами и различными технологическими компонентами. Согласованное взаимодействие и работа различных городских структур, ведомств, предприятий позволят объединять возможности по обнаружению, аналитике, профилактике и реагированию на различные угрозы. Важно отметить необходимость построения процессов регулярной интеграции и усиления согласованности взаимодействия городских служб с учетом постоянного усложнения самой городской экосистемы, с одной стороны, ускорения и усложнения цифровизации преступности – с другой;

построение стратегических партнерств и согласованного взаимодействия на различных уровнях цифровой экосистемы города. Это цифровизация на уровне включения физических объектов в цифровую среду, коммуникационные средства и инфраструктуры, базы данных служб и предприятий, цифровые платформы и приложения – цели, средства, программы модернизации и развития.

УДК 343.985

С.И. Бординович

НЕКОТОРЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ, ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «КОНТРОЛИРУЕМАЯ ПОСТАВКА»

Проведение оперативно-розыскного мероприятия «контролируемая поставка» (далее – контролируемая поставка), представляющего собой перемещение гражданином, организацией предметов и документов под контролем должностного лица органа, осуществляющего оперативно-розыскную деятельность (ОРД), в целях получения сведений, необходимых для выполнения задач ОРД, как правило, требует комплексного задействования сил и средств различных государственных органов, организаций, а также граждан, оказывающих содействие на конфиденциальной основе органам, осуществляющим ОРД, посредством участия в проведении указанного оперативно-розыскного мероприятия, содействия в его подготовке и проведении.

В ходе проведения контролируемой поставки осуществляется установление каналов поступления запрещенных к обороту веществ и предметов. Наряду с этим решается задача по установлению их отправителей и получателей, а также лиц, совершивших или совершающих преступления с использованием контролируемых предметов и документов. Для выявления и закрепления доказательства преступной деятельности создаются условия, при которых следы совершаемого преступления отражаются на допускаемых уголовно-процессуальным законом носителях информации.

Согласно Закону Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» контролируемая поставка проводится по постановлению о проведении оперативно-розыскного мероприятия и в рамках дела оперативного учета, представляющего собой обособленное производство, которое включает в себя материалы ОРД в целях систематизации, проверки и оценки сведений, оно заводится по постановлению должностного лица органа, осуществляющего ОРД. Еще одним обязательным условием проведения контролируемой поставки является наличие специального задания, которое объявляется под подпись гражданину, привлекаемому к участию в оперативно-розыскном мероприятии, до начала его проведения.

При проведении контролируемой поставки законодательство допускает полное или частичное изъятие, а также замену перемещаемых вещей, оборот которых представляет повышенную опасность для здоровья граждан и окружающей среды или служащих для изготовления оружия массового поражения.

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-З «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.