

Например, в 2020 г. по распоряжению Министра юстиции Франции официально была запущена в действие программа по противодействию семейному насилию, легализовавшая применение электронных браслетов нового поколения к супругам-насильникам. Если обладатель браслета приблизится слишком близко, с ним немедленно свяжутся по телефону. И если он не ответит или вновь нарушит границы, то правоохранительные органы предпримут в отношении него более строгие меры, включая арест.

Гийом Ганье – коммерческий директор швейцарской компании Geosatis, которая продает браслеты нового поколения, – считает, что эти продукты компании должны облегчить жизнь людей, за которыми ведется наблюдение.

МВД Республики Беларусь совместно с Минфином, НАН Беларуси, Госкомвоенпромом (ОАО «АГАТ-системы управления») прорабатывается вопрос о возможности приобретения электронных средств контроля производства Российской Федерации и разработки собственного программного обеспечения для их функционирования в целях осуществления контроля за лицами, за которыми установлен превентивный надзор, и осужденными по ст. 77–79 и 117 УК Республики Беларусь.

С учетом того, что в МВД подобные средства контроля отсутствуют, как и предприятия, занимающиеся их разработкой и производством, в Республике Беларусь, проведены маркетинговые исследования аналогичных систем электронных средств контроля разработки Российской Федерации, Китайской Народной Республики и Республики Казахстан.

По результатам исследований установлено, что в Российской Федерации и Китайской Народной Республике имеются соответствующие компании, но их продукция предназначена для удовлетворения внутренних заказов, так как программное обеспечение, разработанное в соответствии с законодательством указанных стран, позволяет обмениваться данными только с правоохранительной системой страны-разработчика.

С учетом изучения рынка компаний, производящих средства электронного контроля, наиболее оптимальным вариантом являются электронные браслеты, производимые в Российской Федерации (АО «Цитос» ФСИН России, стоимость одного устройства составляет около 600–700 долларов США). Вместе с тем для проработки вопроса об их приобретении ОАО «Агат-системы управления» потребуется время и порядка 550 тыс. рублей на реализацию стартовой площадки проекта.

Реализация данного перспективного мероприятия будет продолжена МВД совместно с заинтересованными структурами в первом полугодии 2024 г.

По мнению Верховного Суда, установление поднадзорному обязанности постоянно носить электронные средства контроля фактически будет направлено на обеспечение других установленных в ч. 8 ст. 80 УК Республики Беларусь требований: не покидать свое жилище в определенное время суток, не выезжать за пределы района (города) по служебным и личным делам без согласия органов внутренних дел, и сведется к возложению на лицо, за которым установлен превентивный надзор, дополнительных обязанностей по явке в уголовно-исполнительную инспекцию.

Реализация на законодательном уровне данной обязанности возможна не как требование превентивного надзора, за несоблюдение которого предусмотрена ответственность, а путем корректировки ст. 200 и 201 УИК с одновременным определением конкретных категорий лиц, поведение которых указывает на высокие риски рецидива преступлений. Но данная позиция достаточно спорная ввиду того, что отсутствие ответственности за отказ от ношения электронных средств контроля сведет к минимуму целесообразность их применения для контроля за поднадзорными.

По нашему мнению, целесообразно вернуться к проработке вопроса о возложении на поднадзорных обязанности постоянно носить электронные средства контроля после их практическую внедрения.

Таким образом, можно предположить, что эти направления совершенствования системы исполнения и отбывания наказаний перспективны и не ограничены перечнем задач, которые могут выполняться, так как научно-технологический прогресс постоянно развивается и совершенствуется.

УДК 343

Д.С. Зинченко

О МЕТОДАХ ДЕАНОНИМИЗАЦИИ ЛИЦ, СОВЕРШАЮЩИХ НЕЗАКОННЫЙ ОБОРОТ НАРКОТИКОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Незаконный оборот наркотиков является одним из самых прибыльных видов деятельности организованных преступных групп. Наркопреступность создает угрозу для политического и социально-экономического развития стран во всем мире, подрывает безопасность и стабильность деятельности всех сфер общества. В условиях функционирования цифровой экономики на мировом рынке нелегальный оборот наркотиков трансформируется и переходит на новый этап развития. В результате происходит их цифровая трансформация, которая заключается в переходе от «традиционного» оборота наркотиков к бесконтактному, осуществляемому на различных электронных платформах.

Массовое использование преступными сообществами, занимающимися незаконным оборотом наркотиков, «теневых сегментов» позволяет им сохранять свою анонимность и приватность своих противоправных действий. В этой связи субъектами по противодействию наркопреступности проводится комплекс мероприятий по изучению организационных, тактических и технических возможностей по деанонимизации преступников, совершающих незаконный оборот наркотиков с использованием информационно-коммуникационных технологий.

Под деанонимизацией необходимо понимать комплекс оперативных исследований и технических мер по установлению личности пользователей сетевых ресурсов для решения оперативно-розыскных задач.

Изучение специфики и особенностей функционирования виртуального пространства показывают, что несмотря на использование наркопреступниками теневой части интернета, позволяющей им шифроваться, существуют определенные возможности обработки сетевых ресурсов, которые могут деанонимизировать преступников, совершающих незаконный оборот наркотиков с использованием информационно-коммуникационных технологий. Эти возможности состоят из трех основных методов.

Анализ влиятельной активности на соединении. При использовании сети практически во всех случаях на IP-устройствах (маршрутизаторах, коммутаторах 3-го уровня) работает протокол NetFlow. Система NetFlow – это открытый сетевой протокол, также известный как стандарт IPFIX, предназначенный для учета и анализа сетевого трафика. Анализ данных системы NetFlow позволяет визуализировать не только протоколы TCP/IP (например, IP-адрес источника, протокол, порт), но и дополнительную информацию о входящих и исходящих интерфейсах, сетевом адресе источника, DSCP, области автономных систем в протоколе BGP и др.

Несмотря на очевидную простоту и эффективность этого протокола при его анализе в темной сети из-за большой доли трафика протокол может генерировать большое количество портов существования.

Анализ влияния пользователей сетевых ресурсов на браузер. Для доступа к темной сети злоумышленникам требуется использование специализированного «браузера темной сети». При использовании такого браузера наркопреступникам необходимо пользоваться специальными технологиями, превращающими браузер в оконечный терминал видеоконференцсвязи, например, стандартом WebRTC, который описывает передачу потоковых данных между браузерами в режиме реального времени. Однако такие технологии являются уязвимыми для браузеров, так как WebRTC определяет их реальные IP-адреса, а сохранить анонимность не поможет ни прокси, ни использование «браузера темной сети». И поэтому исследование таких технологий также позволяет деанонимизировать преступников, совершающих незаконный оборот наркотиков с использованием информационно-коммуникационных технологий.

При этом, в связи с тем что жизненный цикл кодеков уязвимостей, например, того же стандарта WebRTC, составляет всего от нескольких недель до нескольких месяцев, данный способ по деанонимизации наркопреступников в темной сети не всегда эффективен.

Анализ сетевой деятельности пользователей сети. В основе этого метода заложено базовое использование тегов «Canvas» при помощи JavaScript на платформе HTML5, позволяющих создать разные объекты, рисунки, фотокомпозиции. Ключевой особенностью является то, что различные браузеры в зависимости от аппаратных и программных компонентов, операционной системы и иных конфигураций представляют изображения по-разному. Таким образом, используя этот способ для деанонимизации наркопреступников, с помощью параметров изображения представляется возможным идентифицировать браузер, его аппаратную и программную среду.

Итак, использование возможностей современных информационных технологий позволяет успешнее противостоять преступности. Злоумышленники используют всевозможные методы для своей анонимности и конфиденциальности. Но при применении компьютерных технологий для совершения преступлений чаще всего остаются виртуальные следы. Следовая картина имеет свою специфику, и традиционные способы их выявления будут не всегда достаточно эффективны.

Соответственно возникает необходимость использования новых методов и средств выявления и фиксации конкретного цифрового следа, в том числе и использование возможностей сетевых ресурсов. А для совершенствования деятельности по деанонимизации преступников, совершающих незаконный оборот наркотиков с использованием информационно-коммуникационных технологий, предлагаем внести дополнения в федеральный проект «Информационная безопасность» национального проекта «Национальная программа «Цифровая экономика Российской Федерации», утвержденный протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 года № 7, содержащие мероприятия по техническому перевооружению подразделений органов внутренних дел, занимающихся противодействием преступности в сфере IT-технологий, оснащению их современными программно-техническими средствами в совокупности с методами искусственного интеллекта и обработки больших объемов неструктурированных данных.

УДК 343.8

С.В. Казак

О ЗАМЕНЕ НАКАЗАНИЙ НА БОЛЕЕ СТРОГИЕ ОСУЖДЕННЫМ, СОВЕРШИВШИМ ПРЕСТУПЛЕНИЯ В ВОЗРАСТЕ ДО ВОСЕМНАДЦАТИ ЛЕТ

Виды наказаний и особенности их назначения лицам, совершившим преступление в возрасте до восемнадцати лет, закреплены в гл. 15 Уголовного кодекса Республики Беларусь (УК). Большинство наказаний, которые могут быть применены к несовершеннолетним, не связаны с изоляцией осужденных от общества: общественные работы, штраф, лишение права заниматься определенной деятельностью, исправительные работы, ограничение свободы. Назначая указанные наказания к данной категории осужденных, суд должен руководствоваться положениями, закрепленными в статьях 110–113, 114¹ УК.

Законом Республики Беларусь от 26 мая 2021 г. № 112-З «Об изменении кодексов по вопросам уголовной ответственности» были декриминализованы деяния, предусмотренные ст. 415–419 УК, которые предусматривали уголовную ответственность за уклонение от отбывания наказаний, не связанных с изоляцией осужденных от общества. Одновременно законодатель дополнил ст. 49–52, 55 УК положениями, закрепляющими правила замены данных наказаний на более строгие наказания в случае, если осужденные злостно уклоняются от их отбывания. Вместе с тем в нормах, регламентирующих наказания, применяемые к лицам, совершившим преступления в возрасте до восемнадцати лет, никаких указаний о возмож-