Секция «LegalTech. Цифровая криминалистика»

Проблемы неправомерного использования информационно-телекоммуникационной сети "Интернет" и развития DarkNet

Научный руководитель – Агаян Виолетта Арсеновна

Ворсинова Александра Владимировна
Студент (бакалавр)
Ростовский юридический институт (филиал) Российской правовой академии Министерства юстиции Российской Федерации, Юридический факультет, Гражданско-правовых дисциплин, Ростов-на-Дону, Россия
E-mail: sasha.vorsinova@yandex.ru

Неправомерное использование информационно-телекоммуникационной сети «Интернет» и развитие DarkNet - площадок стремительно меняет положение и масштабы наркотической угрозы [3]. Именно невозможность правового регулирования трансграничного использования «всемирной паутины» и DarkNet в целях раскрутки наркобизнеса является проблемой мирового масштаба, которая имеет качественный и количественный прирост ежегодно.

Расследование преступлений в сфере цифрового оборота наркотических веществ объективно отстаёт от развития незаконного оборота наркотиков, имеющего сегодня все признаки высокотехнологичного цифрового бизнеса.

Развитие цифровой криминалистики в Российской Федерации является основным способом противодействия распространению наркотических веществ в Сети и повышения эффективности процесса раскрытия подобных преступлений [2].

Акцентируем внимание на основных аспектах популярности цифровых платформ DarkNeta и способах противодействия со стороны правоохранителей с использованием криминалистики в процессе цифровизации в перспективе.

Развитие интернет-площадок ведётся за счёт возможности оставаться анонимным и не привлекать внимание к своей деятельности. Анонимность обеспечивается как сторонними приложениями, так и непосредственно в системе Tor.

Луковичная система маршрутизации является также одной из гарантий анонимности в Сети. А само шифрование представляет собой способ анонимного взаимодействия с использованием компьютерной сети благодаря инкапсулиризации сообщений в несколько слоёв.

Кроме того, многих пользователей «тёмного Интернета» привлекает практически устойчивая защита от DoS-атак, то есть атаки на системные ресурсы с блокировкой доступа или затруднённым доступом.

Для некоторых владельцев ряда маркетплейсов DarkNet отличная площадка для сохранения анонимности за счёт механизма анализа трафика, что позволяет минимизировать скачковые перепады и ввести относительно стабильную торговлю. Например, прокси-сервер I2P используется во многих стандартных сервисах и обеспечивает сингулярную приватность и анонимность.

Некоторые «заинтересованные лица» используют DarkNet из-за мнимой аутентификации, состоящей из нескольких этапов-нодов:

- входная нода - этап, при котором пользователь осуществляя подключение и используя IP-адрес, не видит к чему осуществляется подключение;
- средняя нода - этап самостоятельного подключения, при котором учитывается направление трафика, но не обнаруживается IP-адрес;

- выходная нода - точка, при которой трафик не считывается и только анонимная сеть осуществляет подключение к домену.

Все указанные способы не являются безусловными и имеют свои недостатки и слабые стороны, которые можно использовать для противодействия процветанию наркобизнеса.

С развитием цифровой криминалистики мы сможем раскрывать цифровые площадки DarkNet как киберпространства - место совершения преступления и фиксации наиболее важных цифровых доказательств.

Важно понимать, что противодействие злоумышленникам в DarkNet является весьма долгим и поэтапным процессом, который начинается с установления наблюдения. В данном случае для анализа баз данных, установления связей можно использовать системы искусственного интеллекта для сопоставления данных.

Непосредственно в целях раскрытия и обнаружения наркоторговцев необходимо выявление реальных IP-адресов, которое возможно обнаружить при взаимодействии правоохранителей и технических специалистов. Необходимо развитие программ модификации сетевых узлов для обнаружения системных «пробелов» в программах анонимности DarkNet.

Важно оперативно обнаруживать, фиксировать и приобщать электронные доказательства для составления технической базы, которая позволит расширять возможности противодействия незаконному обороту наркотических веществ в сети Интернет. Использование технических устройств для изъятия информации, содержащей различные клиентские базы и данные о поставщиках и поставках.

Резюмируя вышесказанное, отметим, что развитие цифровизации неизбежно затрагивает и процесс собирания информации о преступлении и лицах его совершивших. Становление цифровой криминалистики определяется не только уровнем изученности, но и, прежде всего, применимости в раскрытии преступлений.

Для противодействия сети DarkNet в целом и распространению наркотических веществ в частности необходимо расширить научную базу исследований возможностей цифровой криминалистики, разрабатывать новые аппаратно-программные комплексы. [1, с.90]

Кроме того, важно осуществлять поэтапное и чёткое взаимодействие специалистов, наращивая опыт в борьбе с преступлениями такого рода. Отметим, что важную составляющую имеет техническое оснащение, в борьбе с наркобизнесом нужно осознавать, что колоссальные денежные суммы тратятся на создание мощных серверов и обеспечение работы современного программного обеспечения.

Источники и литература

1) Ковригина А.Р., Мезенцева А.И. К ВОПРОСУ ОБ ОТДЕЛЬНЫХ ПРОБЛЕМАХ ЦИФРОВОЙ КРИМИНАЛИСТИКИ // Вестник науки. 2021. №12 (45).

2) Хохлов Е. Е. Пронаркотический сегмент в сети «DarkNet»: от истоков до современности // Полицейская и следственная деятельность. 2020. №2.

3) Как Россия стала мировым лидером в торговле наркотиками и кто на этом зарабатывает? [Электронный ресурс]. URL: https://darknark.lenta.ru/article/part2-the-world-leader (Дата обращения: 01.03.2022).