УДК 343. 98

О НЕКОТОРЫХ ВОПРОСАХ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Новоселов Н.Г.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматривается деятельность преступников в информационно-коммуникационном пространстве, в том числе в скрытом сегменте сети Интернет – DarkNet. Анализируется система блокчейн как один из элементов эффективного раскрытия киберпреступлений, а также способы просмотра денежного электронного оборота с учетом данных технологий. Высказываются предложения по совершенствованию деятельности органов внутренних дел в рассматриваемой сфере.

Ключевые слова: информационно-телекоммуникационные технологии, киберпреступления, криптовалюта, блокчейн, криптобиржа, транзакции.

ON SOME ISSUES OF DISCLOSURE OF CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

Novoselov N.G.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article examines the activities of criminals in the information and communication space, including in the hidden segment of the DarkNet Internet. The blockchain system is analyzed as one of the elements of effective disclosure of cybercrimes, as well as ways to view monetary electronic turnover taking into account these technologies. Proposals are made to improve the activities of the internal affairs bodies in this area.

Keywords: information and telecommunication technologies, cyberstalks, cryptocurrency, blockchain, crypto exchange, transaction.

Информационно-телекоммуникационные технологии практически ежедневно используются в различных сферах деятельности человека и имеют большое значение в жизни каждого члена современного общества. Такая многофункциональная и универсальная система не осталась без внимания различного вида преступников. Появление современных средств телекоммуникаций, социальных сетей и мессенджеров кардинально изменило механизм осуществления преступной деятельности членов организованных преступных групп, переведя эту деятельность в режим онлайн.

Так, за 10 месяцев 2022 года на территории Российской Федерации совершено 429 245 преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, 285 830 из которых остаются нераскрытыми. Процент раскрываемости рассматриваемого вида преступлений составил всего 29,2% [3].

Рассматривая преступную деятельность отдельных лиц, совершаемую с использованием информационно-коммуникационных технологий необходимо отметить, что она обладает характерными, свойственными только этому виду преступлений особенностями, к которым можно отнести:

– конспиративность и анонимность деятельности преступников;

– широкую географию распространения и использования преступных контентов;

– наличие специальных знаний в области IT-технологий;

– использование в своей противоправной деятельности криптовалюты.

Деятельность преступников в информационно-коммуникационной сфере начинается с создания определенного интернет-ресурса, где размещаются соответствующие предложения или реклама. Как правило, информация находится не в привычной сети, а в скрытом сегменте Интернета – DarkNet, в который невозможно попасть при использовании стандартного браузера, к тому же DarkNet обладает высокой степенью шифрования IP-адресов пользователей.

Для того чтобы посетить страницу контента, необходимо воспользоваться особым прокси-сервисом (один из наиболее популярных вариантов – сеть «Тор» и «Тор Браузер», которые изначально были созданы Министерством Обороны США для передачи зашифрованной информации через информационно-компьютерных посредников). Суть работы этой площадки заключается в том, что отследить IP-адрес отправителя представляется практически невозможным. О популярности данной площадки свидетельствует то, что уже с начала 2020 года, ежедневно «Тор» пользуются более 324 000 человек из России, или 14,7% аудитории [1].

Одним из главных преимуществ данного сегмента является анонимность, а соединение в нем устанавливается между участниками в зашифрованном виде, с использованием нестандартных портов и протоколов. Основной валютой DarkNet является криптовалюта биткоин.

На современном этапе развития технологий система проверки транзакций, так называемый блокчейн, является одним из элементов эффективного раскрытия киберпреступлений. Система блокчейн состоит из разных блоков, включающих в себя структурированную схему информации о сведениях, которые напрямую вводятся ее пользователями. Эти сведения содержат в себе информацию о различных транзакциях, переводах, заключенных сделках и договорах. Все они позволяют выстроить ту самую цепочку, исходя из ранее введенных данных. Суть системы также состоит в том, что при появлении нового блока сведений он автоматически присоединяется к предыдущему. Таким образом, упомянутая система содержит в себе всю информацию, относящуюся к определенному пользователю, и делает прозрачной всю активность действий.

Существует два способа просмотра денежного оборота по технологии блокчейн: ручной и при помощи специального программного обеспечения (далее – СПО).

Ручной способ заключается в просмотре по адресу кошелька всех денежных операций, с которых поступают средства в кошелек, однако данный способ затрачивает больше времени, чем анализ информации с использованием СПО. Этот способ позволяет установить информацию о принадлежности кошелька к тому или иному сервису. Так, например, при анализе кошелька в системе блокчейн, сотрудник правоохранительных органов, располагающий информацией о том, что на него поступали биткойн-транзакции для оплаты запрещенных орудий, средств, веществ, предметов, через сервер СПО узнает, что на конкретный кошелек поступали биткойн-средства мелкими суммами с другого кошелька, в отношении которого у СПО-сервиса имеются данные о принадлежности этого кошелька к конкретной криптобирже.

Далее сотрудник делает запрос в криптобиржу, в котором просит администрацию предоставить информацию о владельце кошелька. Биржа присылает ответ с информацией о пользователе, которая содержит в себе фамилию, имя, отчество, номер телефона, электронную почту и т.д. Таким образом, сотрудник устанавливает личность самого преступника или подставного лица.

Подобным образом 14 июля 2022 года сотрудниками органов внутренних дел стало известно о легализации почти 2 млрд рублей, приобретенных в результате сбыта наркотических средств посредством использования сети Интернет. В период с 2016 по 2020 год преступники совершали сбыт наркотических и психотропных веществ в крупном и особо крупном размерах путем бесконтактного способа связи с «покупателями». Денежные средства поступали на электронные счета, которые были зарегистрированы на других лиц, не осведомленных о совершении противоправных деяний. В ходе проведения оперативно-разыскных мероприятий сотрудниками правоохранительных органов было выявлено 70 преступлений, квалифицируемых по статье 228.1 УК РФ. Задержано 63 подозреваемых, которым выдвинуто обвинение по статьям 210 и 228.1 УК РФ. На сегодняшний день 32 обвиняемых осуждены. Из незаконного оборота изъято более 22 кг наркотических средств [2].

Для изобличения лиц, совершающих преступления в информационно-коммуникационной среде, органам внутренних дел необходимо проводить свою работу в двух направлениях. Во-первых, следует акцентировать внимание на мониторинге «черного Интернета» и установлении «диспетчерских центров» организованных преступных групп. Во-вторых, упорядочить деятельность оперативных подразделений органов внутренних дел по взаимодействию с администрациями криптобирж и установлению владельцев электронных кошельков, на которые поступали преступные биткойн-транзакции.

Подводя итог, следует отметить, что специфика раскрытия преступлений, совершаемых с использованием информационно-коммуникационных технологий зависит прежде всего от уникальных свойств киберпространства, уровня развития технологий, а также правильного применения оперативно-розыскных мероприятий соответствующими подразделениями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Зачем власти блокируют Tor и можно ли это сделать [Электронный ресурс]. – Режим доступа: https://www.forbes.ru/tekhnologii/448961-zacem-vlasti-blokiruut-tor-i-mozno-li-eto-sdelat (дата обращения: 17.11.2022).

2. Следователем МВД России возбуждено уголовное дело о легализации более 2 млрд рублей [Электронный ресурс]. – Режим доступа: http://www.mvd.ru (дата обращения: 17.11.2022).

3. Состояние преступности в России за январь-октябрь 2022 года [Электронный ресурс]. – Режим доступа: http://www.mvd.ru (дата обращения: 17.11.2022).

УДК 343.985.4:[343.575:004.77](470)

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПРОИЗВОДСТВА ОСМОТРА СРЕДСТВ СОТОВОЙ СВЯЗИ ПО УГОЛОВНЫМ ДЕЛАМ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ

Нугаева Э.Д.,
кандидат юридических наук
(Уфимский юридический институт МВД России)

Аннотация: автором в статье изложены тактические рекомендации по проведению осмотра и процессуальной фиксации сведений, расположенных в электронной памяти сотового телефона на стадиях статистического и динамического осмотра.

Ключевые слова: тактика, осмотр, сотовый телефон, специалист, следователь, наркотические средства, психотропные вещества, информация.