свободы необходимо ввести иное соотношение, чем один день ограничения свободы за восемь часов обязательных работ, так как при сохранении данной пропорции новое наказание, по сути, будет являться более мягким, чем обязательные работы.

Список источников

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)
2. Уголовный кодекс Российской Федерации: федер. Закон от 13.06.1996 № 63-ФЗ: ред. От 20.02.2021. М., Проспект, 2021. 336 с.
3. Уголовно-исполнительный кодекс Российской Федерации: федер. Закон от 25.12.1996 № 63-ФЗ: ред. От 05.04.2021. М., Проспект, 2021. 112 с.
4. Постановление Пленума Верховного Суда № 59 от 22.12.2015 г. "О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации по уголовным делам"

УДК 343.985

НЕКОТОРЫЕ АСПЕКТЫ ОПЕРАТИВНО-РОЗЫСКНОГО ОБЕСПЕЧЕНИЯ РАСКРЫТИЯ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

***В. Ф. Кетурко**, адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь*

В статье рассмотрены актуальные вопросы оперативно-розыскного обеспечения раскрытия мошенничества, совершенного с использованием информационно-коммуникационных технологий. Проанализированы возможности оперативных подразделений при раскрытии данного вида преступлений.

Ключевые слова: информационно-коммуникационные технологии, мошенничество, оперативно-розыскные мероприятия, оперативно-розыскное обеспечение, негласный аппарат.

SOME ASPECTS OF THE OPERATIONAL INSPECTION SUPPORT OF DISCLOSURE OF FRAUD COMMITTED WITH THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

V. F. Keturko, *Adjunct of the Scientific and Pedagogical Faculty of the Academy of the Ministry of Internal Affairs of the Republic of Belarus*

In the abstracts, topical issues of operational and investigative support for the disclosure of fraud committed using information and communication technologies are considered. Analyzed the capabilities of operational units in the disclosure of this type of crime.

Keywords: information and communication technologies, fraud, operational-search measures, operational-search support, secret apparatus.

Современное развитие информационно-коммуникационных технологий, а также доступность к информационным источникам обуславливают не только улучшение жизнедеятельности населения, но и формирование совершенно новых угроз. Переход традиционных преступлений в информационное поле на фоне высокой степени латентности, их многообразия, адаптивности, динамизма способствует необходимости постоянного совершенствования деятельности оперативных подразделений в борьбе с мошенничеством, совершенном с использованием информационно-коммуникационных технологий.

Эффективная деятельность по противодействию преступлений данного вида непосредственно связана с уровнем ее оперативно-розыскного обеспечения, суть которого заключается в комплексном использовании сил и средств оперативных подразделений органов внутренних дел (далее – ОВД) для получения достаточно полной и достоверной информации, которая бы обеспечивала принятие оптимальных и своевременных решений, установление лиц, совершивших преступление.

Различные аспекты оперативно-розыскного обеспечения выявления и раскрытия отдельных видов преступлений были предметом научных исследований А. В. Башана, Н. В. Быкова, О. П. Грибунова, Д. В. Ермоловича, Э. П. Костюковича, Ю. С. Стешенка и др. Однако проблемам оперативно-розыскного обеспечения выявления мошенничества, совершенного с использованием информационно-коммуникационных технологий уделяется фрагментное внимание, что влияет на научное обеспечение вопросов выявления и раскрытия данного вида преступлений. Так как мошенничество, совершенное с использованием информационно-коммуникационных технологий, не относится к преступлениям, против информационной безопасности, а является традиционным преступлением,

информационно-коммуникационные технологии являются лишь способом, а существующие рекомендации и методики разработаны только для традиционных мошенничеств, что не позволяет более эффективно противодействовать данным видам преступлений. Исследование данного вопроса позволит выработать единый подход в борьбе с данной категорией мошенничества.

Отдельные авторы, отмечают, что более рациональное изучение анализа оперативной обстановки по направлению противодействия преступлениям, которые совершаются с использованием сети Интернет, указывают на неэффективность привязки к какой-либо территории. Предлагается осуществление анализа посредством имеющихся в ОВД информационных банков данных и учетов, а также доступных открытых источников, в том числе находящихся в сети Интернет. Данный подход в определенной степени является актуальным в борьбе с киберпреступлениями. Однако не стоит отказываться от традиционных подходов в раскрытии преступлений данного вида, так как преступник, совершающий свою противоправную деятельность с использованием сети Интернет, проживает в физическом мире, имеет определенные связи, семью и увлечения.

Необходимо отметить, что мошенники с целью сокрытия своей противоправной деятельности и общения используют соответствующие элементы виртуальной среды, а именно специализированные Интернет-форумы например такие как «RDot, prologic», «happy-hack» и тд, а также Telegram-каналы «AndroHack», «Free Software», «Dark Net» и др. Доступ к перечисленным форумам и Telegram-каналам осуществляется на бесплатной основе, а информация предоставленная на указанных объектах виртуальной среды носит информационный характер о способах и схемах совершения преступлений в сети Интернет. Стоит отметить, что существуют форумы и каналы доступ к которым, осуществляется на платной основе. Верификация на данных платформах позволяет получать подробную инструкцию по использованию новых способов совершения преступлений данной категории, а также при необходимости приобретать вредоносное программное обеспечение, для совершения и сокрытия преступлений. Указанные виртуальные площадки предоставляют возможность общения среди участников, подбор соучастников преступлений, что позволяет организовывать преступные сообщества. Фактически это места сосредоточения преступных элементов и соответственно, обеспечивают потенциальную возможность получения сведений, представляющих оперативный интерес.

Анализ научной литературы свидетельствует об исключительной важности такого элемента, как организация взаимодействия между различными государственными и международными субъектами. Различными исследователями в вопросах противодействия преступлений обозначаются определённые трудности взаимодействия правоохранительных органов, государственных и частных

организаций, а также определённые проблемные вопросы в международном сотрудничестве. Так как, в рамках обеспечения взаимодействия данного направления правоохранительные органы могут осуществлять через НЦБ Интерпола и международную сеть национальных контактных пунктов, стоит отметить, что в большей степени предлагаемый алгоритм актуален лишь для преступлений против информационной безопасности. Мошенничество, данной категории, к данному виду преступлений не относится, а рассматривается как имущественное преступление, что не позволяет получать необходимую оперативную информацию. В виду складывающейся тенденции роста совершения мошенничества, данной категории целесообразно прорабатывать вопрос о внесении изменений в нормативные правовые акты регламентирующие вопросы на различных уровнях взаимодействия не только на преступлениях против информационной безопасности, но и для преступлениях, совершенных с использованием информационно-коммуникационными технологий. Это позволит более оперативно получать необходимую информацию о местонахождении лиц, готовящихся к совершению, совершивших преступления рассматриваемой категории.

Таким образом, можно сделать следующий вывод: проблемам оперативно-розыскного обеспечения деятельности ОВД, в вопросах раскрытия мошенничества, совершенного с использованием информационно-коммуникационных технологий уделяется недостаточное внимание, что негативно влияет на эффективность выполнения правоохранительными органами соответствующих задач.

При раскрытии мошенничества, совершенного с использованием информационно-коммуникационных технологий нет необходимости отказываться от территориально принципа. Однако стоит учитывать, что преступники данного вида, являются специфической группой представителей криминального мира, общение между которыми осуществляется в виртуальной среде. В качестве объектов оперативного обслуживания мошенничества, совершенного с использованием информационно-коммуникационных технологий, целесообразно выделить следующие элементы виртуальной среды: специализированные Интернет-форумы, чаты, Telegram-каналы.

Международное сотрудничество в борьбе с мошенничествами указанной категории нуждается в совершенствовании правового и организационного обеспечения.

С целью раскрытия мошенничества, совершенного с использованием информационно-коммуникационных технологий, рекомендуется проработать вопрос разработки рекомендаций и методик для данного вида преступлений, что позволит выработать единый подход практических подразделений в борьбе с данной категорией мошенничества, обеспечит теорию оперативно-розыскной деятельности.