



DOI: <https://doi.org/10.15688/lc.jvolsu.2024.1.19>

UDC 343.85
LBC 67.410.2



Submitted: 29.01.2024
Accepted: 28.02.2024

THE MAIN DIRECTIONS OF USING INFORMATION TECHNOLOGY IN SOLVING DRUG TRAFFICKING CRIMES

Ivan N. Arkhiptsev

Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin,
Belgorod, Russian Federation

Alexander V. Sarychev

Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin,
Belgorod, Russian Federation

Anna B. Beloshapko

Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin,
Belgorod, Russian Federation

Introduction: modern society is conditioned by the growth of drug trafficking, which leads to an expansion of the scale and an increase in the rate of narcotization of the most able-bodied and reproductive age groups. Thus, the National Security Strategy of the Russian Federation has determined that one of the sources of threats to state and public security is the activities of criminal organizations and groups engaged in drugs trafficking and psychotropic substances. The use of information technology is crucial in the distribution of narcotic drugs. In order to identify and prevent crimes committed in this way the employees of law enforcement agencies, and primarily, the employees of operational units, need special knowledge in the field of information technology. The improvement of special knowledge used in operational investigative activities, as well as in the preliminary investigation of drug trafficking crimes, is due to the need to develop the methodological recommendations and implement them in practice. The **purpose** of the study is to identify relevant theoretical and applied problems of methodological support for detecting and solving drug trafficking crimes committed using information technology and systems based on the use of forensic knowledge about the latest computer technologies and information resources. To achieve this goal, it is necessary to solve the following tasks: 1) to consider the main characteristics of crimes related to drug trafficking on the Internet; 2) to investigate the mechanism of activity of online stores selling narcotic drugs; 3) To analyze the problems of counteraction to the contactless method of distribution of narcotic drugs using information technology; 4) to study the main directions of using information technology in solving drug trafficking crimes. Research **methods:** the nature of the issues under consideration determined the application of a set of complementary research methods: theoretical and empirical. The theoretical methods: the study and analysis of literature, Internet resources. The empirical methods: on the basis of periodicals and in electronic publications on the Internet, to study the latest methods and characteristics of committing crimes in the field of information technology, as well as the methods of their detection and investigation using information and telecommunication technologies and systems by employees of operational units. Generalization method: the conclusions are drawn based on the results of the work as a whole.

Key words: drug trafficking, information technology, Internet, law enforcement agencies, counteraction.

Citation. Arkhiptsev I.N., Sarychev A.V., Beloshapko A.B. The Main Directions of Using Information Technology in Solving Drug Trafficking Crimes. *Legal Concept = Pravovaya paradigma*, 2024, vol. 23, no. 1, pp. 139-148. (in Russian). DOI: <https://doi.org/10.15688/lc.jvolsu.2024.1.19>

**ОСНОВНЫЕ НАПРАВЛЕНИЯ
ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА
НАРКОТИЧЕСКИХ СРЕДСТВ**

Иван Николаевич Архипцев

Белгородский юридический институт МВД России им. И.Д. Путилина, г. Белгород, Российская Федерация

Александр Викторович Сарычев

Белгородский юридический институт МВД России им. И.Д. Путилина, г. Белгород, Российская Федерация

Анна Борисовна Белошапко

Белгородский юридический институт МВД России им. И.Д. Путилина, г. Белгород, Российская Федерация

Введение: современное общество характеризуется ростом незаконного оборота наркотических средств, который приводит к расширению масштабов и увеличению скорости наркотизации представителей наиболее трудоспособных и репродуктивных возрастных групп населения. Так, Стратегия национальной безопасности Российской Федерации определила, что одним из источников угроз государственной и общественной безопасности является деятельность преступных организаций и группировок, занимающихся незаконным оборотом наркотических средств и психотропных веществ. При распространении наркотических средств определяющее значение оказывает использование информационных технологий. Для выявления и предотвращения преступлений, совершаемых данным способом, от сотрудников правоохранительных органов, в первую очередь сотрудников оперативных подразделений, необходимы специальные познания в сфере использования информационных технологий. Совершенствование специальных познаний, применяемых в оперативно-розыскной деятельности, а также при производстве предварительного следствия по преступлениям, связанным с незаконным оборотом наркотических средств, обусловлено необходимостью разработки методических рекомендаций и внедрением их в практическую деятельность. **Цель** исследования – выявление актуальных теоретических и прикладных проблем методического обеспечения обнаружения и раскрытия преступлений в сфере незаконного оборота наркотических средств, совершаемых с использованием информационных технологий и систем на основе применения теоретических знаний о новейших компьютерных технологиях и информационных ресурсах. Для достижения поставленной цели необходимо решить следующие **задачи:** 1) рассмотреть основную характеристику преступлений, связанных с незаконным оборотом наркотиков в сети Интернет; 2) исследовать механизм деятельности интернет-магазинов по продаже наркотических средств; 3) разобрать проблемы противодействия бесконтактному способу распространения наркотических средств с помощью информационных технологий; 4) изучить основные направления использования информационных технологий при раскрытии преступлений в сфере незаконного оборота наркотических средств. **Методы исследования.** Характер рассматриваемых вопросов определил применение комплекса взаимодополняющих методов исследования: теоретических и эмпирических. Теоретические методы: изучение и анализ литературы, интернет-ресурсов. Эмпирические методы: на базе периодических изданий и в электронных публикациях изучить новейшие способы и характеристики совершения преступлений в сфере информационных технологий, а также методы их выявления и расследования при помощи информационно-телекоммуникационных технологий и систем сотрудниками оперативных подразделений. Метод обобщения: сделаны выводы по результатам работы в целом.

Ключевые слова: незаконный оборот наркотических средств, информационные технологии, Интернет, правоохранительные органы, противодействие.

Цитирование. Архипцев И. Н., Сарычев А. В., Белошапко А. Б. Основные направления использования информационных технологий при раскрытии преступлений в сфере незаконного оборота наркотических средств // Legal Concept = Правовая парадигма. – 2024. – Т. 23, № 1. – С. 139–148. – DOI: <https://doi.org/10.15688/lc.jvolsu.2024.1.19>

Введение

В настоящее время наблюдается рост незаконного оборота наркотических средств, который обусловлен появлением новых способов совершения преступлений посредством использования информационно-телекоммуникационных технологий и систем, а также последующего сокрытия ими личности преступника. Представители преступного сообщества используют теневые интернет-сегменты, мессенджеры, позволяющие мгновенно обмениваться сообщениями и геолокацией, а также безвозвратно удалять не только текст сообщения, но и контактные данные отправителя или получателя сообщений. Использование интернет-кошельков обеспечивает анонимность их владельцев при оплате запрещенного или ограниченного в гражданском обороте товара, а также возможности создания указанных средств платежа на подставных лиц с целью вывода денежных средств, полученных преступным путем. Важнейшим направлением по борьбе с незаконным оборотом наркотиков стоит отметить обеспечение совершенствования владения сотрудниками правоохранительных органов знаний и навыков в сфере информационно-телекоммуникационных технологий и искусственного интеллекта. Это делается с той целью, чтобы искоренить проблему, которая связана с тем, что интернет-магазины, создаваемые на вышеуказанных платформах, осуществляют свою деятельность и управляются в основном не с территории России, что существенно затрудняет их отслеживание, приостановление деятельности и последующее закрытие, поскольку преступники используют способы сокрытия своего местонахождения путем применения программного обеспечения, позволяющего подменить или скрыть используемый в действительности IP-адрес, анонимайзеров, VPN-сервисов. Применение преступником VPN-программ, получивших в настоящее время большое распространение, позволяет получать доступ к скрытой сети DarkNET, Tor и др.

Так как происходит внедрение новейших достижений науки и техники в процесс по незаконному распространению наркотических средств, каждый второй преступник, занимающийся этой деятельностью, использует информационные технологии.

Комплекс поисковых мероприятий при раскрытии преступлений в сфере незаконного оборота наркотических средств

На сегодняшний день российское общество развивается в условиях внедрения цифровых технологий в различные сферы жизнедеятельности общества и интеграции информационных технологий в общественную жизнь, в рамках чего должны обеспечиваться основные потребности государства. Так, Президент РФ в последние годы подписал ряд указов, задающих направление ускоренного технологического развития страны и ее цифровой трансформации [4; 5]. Достижение целей, содержащихся в данных нормативных правовых актах, будет способствовать развитию страны в таких сферах, как экономика, политика, культура и социальное обеспечение населения.

Выделим основные направления использования информационных технологий и систем при раскрытии преступлений в сфере незаконного оборота наркотических средств:

1. Проведение комплекса поисковых мероприятий в системе Интернет с целью установления сайтов и теневых сегментов Интернета и получения оперативно-значимой информации о продавцах, сбытчиках и покупателях наркотических средств.

2. Использование средств и технологий, связанных с раскрытием личности в информационном пространстве.

Рассмотрим каждое из названных направлений более подробно.

Комплекс поисковых мероприятий может включать в себя методы, которые способны более оперативно выполнять определенные задачи и способы поиска. К ним относятся: целевой поиск, нецелевой поиск, тематический поиск, персонифицированный поиск.

Целевой поиск – мониторинг, используется в тех случаях, когда сотрудникам правоохранительных органов известны интернет-сайты, на которых ранее осуществлялся сбыт наркотических средств или психотропных веществ, то есть уже известный перечень интернет-сайтов, торгующих наркотиками.

Целевой поиск как правило происходит с помощью защищенных от внешнего воздействия ЭВМ, доступ к которым ограничен.

Данные технические средства способны просматривать логи серверов и интернет-сайтов с помощью информации, предоставляемой провайдером сети.

Информацию, которую получают сотрудники оперативных подразделений в сети Интернет, передают в органы ФСБ с целью организации дальнейших совместных действий для решения задач по нейтрализации канала сбыта незаконного распространения наркотиков.

Нецелевой поиск – установление объектов, имеющих характерные признаки для наркотических средств и психотропных веществ в сети Интернет, в частности такие сайты и форумы, где обсуждается изготовление, культивирование, а также сырье для изготовления наркотических средств.

В ходе нецелевого поиска происходит вербовка людей, которые ведут активную жизнь в сети DarkNET. С помощью своих агентов сотрудники правоохранительных органов получают всю необходимую информацию в сети DarkNET, узнают про каналы сбыта наркотических средств и веществ, раскрывают иные форумы и объекты, которые связаны с незаконным распространением наркотических средств.

Тематический поиск – проведение поисковых мероприятий, направленных на проверку и подтверждение имеющейся оперативной информации. В данном методе поиска используются общие ресурсы Интернета, а также поисковые системы, позволяющие обнаруживать информацию, фигурирующую в новостных сайтах.

Персонализированный поиск – информационный поиск в отношении установленного лица и или преступной группы, в которой имеются идентифицированные личные данные.

Персонализированный поиск проводится с помощью технических средств аудио- и видеозаписи посредством наблюдения, собирается и документируется вся информация о деятельности лица с целью выявления фактов совершения преступления. Кроме того, если необходимо с помощью технических средств записать сообщения от просматриваемого лица или установить специальные видеокamеры для слежения за ним, на помощь приходит подразделение МВД России БСТМ, в котором осуществляют деятельность со-

трудники, обученные работать с техническими средствами связи, аудио- и видеозаписи, в сети Интернет и т. д.

Введение усовершенствованных программно-технических средств

Определение личности в информационной среде является одним из основных средств установления личности преступника. Однако универсального программно-технического обеспечения (программы, приложения) на сегодняшний день не разработано. Вместе с тем существует принципиальная возможность устранения данного пробела посредством установления IP-адресов и доменных имен, проверки банковских карт и расчетных счетов получателей и отправителей денежных средств, IMEI номеров телекоммуникационных устройств, открытых данных, содержащихся в поисковых системах государственных органов, поисковых системах Yandex и Google, специализированного поиска в социальных сетях посредством мониторинга.

В частности, сервис Muip.net, размещенный на интернет-ресурсе, предлагает функционал для определения интернет-провайдера, который предоставлял услуги доступа в сеть по конкретному IP-адресу, браузеру и операционной системе. В сфере информационных технологий используются и другие данные, которые помогают идентифицировать пользователя, осуществившего выход в Интернет в определенный момент времени с использованием известного сотрудникам правоохранительных органов IP-адреса телекоммуникационного устройства [8].

Сервис Xinit.ru обладает возможностью определения местоположения точки доступа к сети Интернет, используя данные MAC-адреса сетевой карты. Кроме того, данный сервис содержит важные аналитические материалы, касающиеся вопросов информационной безопасности [9].

Цифровая платформа «Инфосфера» предоставляет возможность получать информацию о физических и юридических лицах, а также ином имуществе с помощью сбора данных из более чем 70 открытых источников. К последним относятся сайты государственных органов, поисковые базы данных для по-

иска работы, социальные сети, объявления и резюме. При помощи данной платформы становится возможным определить владельца телефона или электронной почты, а также получить информацию об автомобилях [7].

Системно-программный комплекс Crystal, разработанный компанией Bitfury, обеспечивает возможность получать информацию о транзакциях в блокчейне в режиме реального времени. Он также содержит расширенный инструментарий для аналитических задач и способен выявлять подозрительные транзакции и связанные с ними объекты [3].

Вышеуказанные сервисы позволяют устанавливать местонахождение, время и устройство выхода в сеть Интернет, отслеживать транзакции, получать информацию о лицах. Смоделируем ситуацию использования сервиса Crystal. Например, сотрудник правоохранительных органов проводит анализ и ему известен кошелек «А», на который поступили биткоины в качестве оплаты за покупку наркотических средств. Через систему Crystal сотрудник узнает, что через данный кошелек неоднократно в течении определенного времени поступали мелкие суммы с других различных кошельков.

Однако данные сайты (Сервис Xinit.ru, комплекс Crystal, интернет-ресурс Muip.net) расположены на общедоступных сайтах. Для наиболее эффективной деятельности сотрудников оперативных подразделений по выявлению преступлений в сфере незаконного оборота наркотических средств считаем целесообразной разработку программного обеспечения, позволяющего в режиме реального времени отслеживать транзакции в Blockchain на сторонних ресурсах, передвижение денежных средств посредством использования интернет-кошельков (Qiwi, Yandex Pay и др.), устанавливать местонахождение телекоммуникационных устройств с использованием IP-адресов которых осуществлялся выход в сеть в конкретный момент времени, интернет-провайдеров, операционные системы и браузеры, посредством которых осуществлялся выход в Интернет.

При этом данный сервис будет предоставлять возможность получения информации без запроса в сторонние организации и государственные органы, что будет существенно сокращать временной промежуток получения

сведений и способствовать ускоренному установлению лиц, совершающих производство, сбыт, продажу, покупку и доставку наркотических средств посредством использования информационно-телекоммуникационных технологий.

Предполагается, что доступ к данному сервису будет закрытым и возможность обратиться к нему будут иметь только сотрудники оперативных подразделений по раскрытию преступлений в сфере незаконного оборота наркотиков, получившие специальное разрешение.

Для того чтобы повысить эффективность правоохранительных органов в сфере борьбы с незаконным оборотом наркотических средств, необходимо внедрить программное обеспечение, оснащенное искусственным интеллектом и нейросетями, подключенными к общему блоку информации сети Интернет и базе данных, а также к DarkNET.

В настоящее время в системе Министерства внутренних дел РФ имеется базовое информационно-технологическое оборудование для подразделений по борьбе с незаконным оборотом наркотиков. В процессе разработки программного обеспечения, предназначенного для использования сотрудниками МВД, были внедрены новые системы, которые значительно усиливают информационную и аналитическую поддержку внутриведомственного взаимодействия. Эти системы включают в себя инструменты автоматической информационной поддержки биометрической идентификации личности, а также автоматического поиска и распознавания транспортных средств, движущихся по дорогам. Повышение эффективности внедрения данных средств информатизации прямо зависит от того, насколько качественно формируются оперативно-розыскная и криминалистическая информация, предоставляемая территориальными органами внутренних дел регионального уровня и ГИАЦ МВД России.

Применение искусственного интеллекта в деятельности по борьбе с незаконным оборотом наркотиков

В процессе применения искусственного интеллекта в деятельности по борьбе с незаконным оборотом наркотиков осуществляется

поиск информационных интернет-ресурсов, в частности торговых площадок, социальных сетей, DarkNET и других сайтов на предмет наличия признаков наркопреступлений. Для определения искусственного интеллекта в сфере борьбы с наркотиками применяются основные подходы, включая анализ характеристик химических веществ и оборудования, используемых при производстве наркотиков. Также изучаются специфические термины, применяемые пользователями социальных сетей, анализируются размещенные фото- и видеоматериалы, на которых можно заметить признаки наркотической зависимости или места, связанные с производством и распространением наркотических веществ. Интеллектуальный поиск возможен благодаря информации, доступной наркофорумам, развлекательным игровым порталам, Тог-сетям и социальным сетям, включая «ВКонтакте», «Одноклассники», Facebook и другие платформы. Это позволяет обеспечить выявление, хранение и пресечение предполагаемого производства и распространения наркотических веществ с помощью нейросетей и баз данных, основанных на локальных признаках и местоположении. Так как большая проблема кроется в том, что дальнейшее общение всех участников преступной группы по незаконному обороту наркотических средств осуществляется посредством таких мессенджеров, как WhatsApp, Telegram, Jabber, Brosix и др. Наиболее популярным мессенджером для общения сбытчика, курьера или потребителя является Telegram, поскольку в отличие от своих аналогов он позволяет скрывать номер телефона пользователя. Указание местонахождения наркотического средства, который находится в тайнике или доставляется курьером предварительно, осуществляется посредством таких сервисов, как Postimg, Radikal и другие (OneTimeSecret, Privnote). Основным преимуществом данных сервисов выступает возможность отправителя безвозвратно удалить отправленные им сообщения получателю через установленный промежуток времени, определяемый отправителем.

Таким образом, данный подход к совершению преступления в области незаконного оборота наркотиков с использованием информационных технологий предполагает разме-

щение информации о продаже наркотических средств на различных интернет-ресурсах. Это позволяет преступнику оставаться анонимным и избежать возможности идентификации его как распространителя такой информации. С данной проблемой уже начинает бороться искусственный интеллект, который запрограммирован таким образом, что может идентифицировать скрытого в социальных сетях пользователя по сбыту незаконного вещества.

Кроме того, данное программное обеспечение полезно в процессе использования центральной базы данных наркопреступников через соответствующую среду биометрической идентификации АПК – ГИС «Единый центр хранения данных» и АИС «Единое геоинформационное пространство», а в мегаполисах (в случаях с г. Москва) оно полезно как выступающий в форме элемента интегрированной информационной системы.

С использованием всесторонней городской системы видеонаблюдения и встроенной в нее системы аналитической обработки изображений возможно определить маршруты передвижения и отследить местонахождение разыскиваемых лиц, подозреваемых в хранении или сбыте наркотиков.

При разработке алгоритмов для программного обеспечения фильтрации контента в онлайн-пространстве необходимо учитывать различные эвфемизмы, используемые для обозначения наркотических веществ, такие как «клевер», «божья травка», «сено», «мери джейн», «опилки» и т. д., например для обозначения гашиша.

Дистанционный способ пресечения преступлений в сфере незаконного оборота наркотических средств

С целью сокращения преступлений в сфере незаконного оборота наркотических средств, совершаемых через Интернет с применением специальных инструментов для скрытия личности злоумышленника, представляется целесообразным возложить на провайдеров интернет-услуг обязанность блокировать доступ к информационным ресурсам. Такие ресурсы позволяют злоумышленникам скрывать свою личность и информацию об используемом оборудовании, программном

обеспечении или действиях в сети. Список блокируемых ресурсов будет формироваться на основе предложений оперативно-розыскных органов [1, с. 123].

На сегодняшний день данный механизм частично реализован в положениях Федерального закона «Об информации, информационных технологиях и защите информации» [6] в отношении блокирования доступа к информационно-телекоммуникационным сетям и информационным ресурсам. Используя указанную норму, мы предлагаем расширить ее сферу применения на все программные средства подмены или сокрытия информации о пользователях интернет-ресурсов. Кроме того, считаем целесообразным установить законодательное требование о регистрации пользователей организаторами распространения информации в сети Интернет и подтверждении подлинности предоставленных при регистрации данных. Для этого можно использовать единую систему идентификации и аутентификации, которая успешно применяется при предоставлении государственных услуг в электронной форме и доказала свою эффективность на протяжении длительного времени.

В настоящее время все большее число лиц способно использовать информационные средства для продажи наркотиков, в связи с этим один из самых распространенных способов их реализации – дистанционный. При его применении сложность заключается в том, что раскрыть личность крайне проблематично. Таким образом, необходимо уменьшить размах совершения преступлений, связанных с незаконным оборотом наркотиков, путем сокращения дистанционных методов их совершения. Это поможет привлечь к уголовной ответственности людей, замешанных в разработке программного обеспечения, которое используется для распространения наркотиков, а также владельцев интернет-сайтов и страниц в социальных сетях, на которых размещается информация о сбыте запрещенных средств и веществ.

Существует одно важнейшее направление в борьбе с незаконным оборотом наркотиков – это повышение компетентности правоохранительных органов в области информационно-телекоммуникационных технологий и искусственного интеллекта. Сотрудники должны осуществлять мониторинг вводимых нов-

шеств, достижений в развитии технологий, а также оценивать риски быстро развивающихся преступлений или появления новых деяний. Анализируя и разрабатывая научно обоснованные рекомендации, учебники и другую литературу, направленную на выявление, раскрытие и расследование преступлений с использованием современных технологий, государство держит свой курс на финансовую и организационную поддержку этих мероприятий в рамках национального проекта «Цифровая экономика Российской Федерации» [2]. В рамках разработки методических положений в системе МВД по выявлению преступлений в сфере незаконного оборота наркотических средств при помощи информационных технологий и систем учитываются факторы, негативно сказывающиеся на деятельности правоохранительных органов, связанной с выявлением рассматриваемой категории преступлений, а именно:

1. Сложность отслеживания письменной и голосовой информации при помощи технических средств, поскольку данная информация отправляется посредством мессенджеров, использующих сквозное шифрование сообщений между пользователями. Электронные ключи создаются и хранятся не на сторонних серверах, как, например, в социальных сетях, а непосредственно в приложении пользователей.

2. Реализация требований Федерального закона «Об информации, информационных технологиях и защите информации» относительно запрета использования программно-технических средств, позволяющих получать доступ к серверам и сайтам, запрещенным на территории Российской Федерации, а также обязательного хранения персональных данных пользователей сети Интернет находится в настоящее время на недостаточном уровне.

3. Возможность произвольного формирования образа личности преступника в цифровом пространстве посредством указания недостоверных данных о личности, фотографии (аватар), что способствует скрытию личности, в действительности совершающей преступные действия.

4. Отсутствие должного контроля со стороны операторов связи за достоверностью данных. Эти же определенные данные указываются при регистрации абонентов сети мо-

бильной связи, что предопределяет факты регистрации абонентов без установления истинных данных о личности и внесения данных о подставных лицах.

5. Широкое распространение технологии анонимных сетевых подключений (подробно описаны нами ранее).

Вышеназванные факторы указывают на основные пробелы, имеющиеся у сотрудников правоохранительных органов при выявлении и расследовании преступлений в сфере незаконного оборота наркотических средств, которые могут иметь свое решение в использовании информационных технологий и систем сотрудниками правоохранительных органов.

Управление «К» МВД России

Стоит отметить, что для эффективной борьбы с преступниками в интернет-пространстве создано такое подразделение в МВД России, как управление «К».

Управление «К» с помощью технических средств и информационных технологий посредством взаимодействия с другими странами занимается предупреждением и раскрытием преступлений в сфере незаконного оборота наркотиков.

Обычно в сферу задач Управления «К» входит работа с иностранными государствами с целью раскрытия личности участников наиболее масштабных преступных сообществ, которые активно занимаются сбытом наркотических средств на территории Российской Федерации.

У Управления «К» присутствуют самые новейшие достижения науки и техники, с помощью которых они выполняют самые засекреченные задания по борьбе с преступностью в сфере оборота наркотиков. На данный момент времени Управление «К» является самым секретным подразделением МВД, которое совместно с ФСБ занимается разработкой дел оперативного учета в отношении крупнейших популярных площадок и маркетплейсов, на которых занимаются продажей наркотических средств.

Заключение

Таким образом, подводя итог сказанному, можно сделать следующие выводы:

1. Выделяют несколько основных направлений, по которым работают сотрудники органов внутренних дел с целью борьбы с незаконным оборотом наркотиков. К таким направлениям относятся: проведение комплекса поисковых мероприятий в системе Интернет с целью установления сайтов и теневых сегментов Интернета и получения оперативно-значимой информации о продавцах, сбытчиках и покупателях наркотических средств, использование средств и технологий, связанных с раскрытием личности в информационном пространстве.

2. В целях более качественного выявления, раскрытия и расследования преступлений в сфере незаконного оборота наркотических средств необходимо обратить внимание на использование всех доступных информационных ресурсов для своевременного получения оперативно-значимой информации и применения ее в оперативно-розыскной деятельности.

3. Разработка программного обеспечения для осуществления деятельности сотрудников оперативных подразделений по контролю за оборотом наркотических средств позволит более качественно и быстро выявлять всех участников незаконного оборота наркотических средств, осуществляемого посредством использования информационных технологий.

Сотрудникам необходимо осуществлять мониторинг вводимых новшеств, достижений в развитии технологий, а также оценивать риски быстро развивающихся преступлений или появления новых. Следует анализировать и систематически разрабатывать научно обоснованные рекомендации и другую литературу, направленные на выявление, раскрытие и расследование преступлений, совершенных с использованием цифровых технологий. Предлагается осуществить финансовое и организационное обеспечение реализации указанных мероприятий в рамках государственного проекта «Цифровая экономика Российской Федерации».

В качестве рекомендаций по повышению эффективности борьбы сотрудников правоохранительных органов с незаконным оборотом наркотических средств предлагаем следующее:

1. Повышать уровень квалифицированности и информированности сотрудников в сфере информационных технологий, обучение их работе с сетями Интернет и DarkNET, информирование сотрудников правоохранительных органов о нововведениях в сфере информационных технологий.

2. Для обеспечения большего финансирования операций сотрудников правоохранительных органов, которые пресекают незаконный оборот наркотических средств в сфере информационных технологий, необходимо предоставлять им доступ к самым новейшим разработкам в области программного обеспечения и информационных технологий. Кроме того, важно увеличить материальное обеспечение сотрудников, вовлеченных в деятельность по пресечению незаконного распространения наркотических средств и психотропных веществ, с целью предотвращения «вымывания» квалифицированных кадров в гражданскую, в том числе преступную, сферу (так, на практике известны случаи попыток вербовки сотрудников оперативных подразделений криминальными структурами, занимающимися незаконным распространением наркотических средств и психотропных веществ).

3. Провести программы в образовательных учреждениях по набору наиболее способных студентов и школьников в деятельность по борьбе с незаконным оборотом наркотических средств в сфере информационных технологий, предоставить им возможность работать совместно с сотрудниками органов внутренних дел или в самом ведомстве самостоятельно. Всячески поощрять изучение компьютерных и информационных технологий школьниками, студентами образовательных учреждений, а также сотрудниками правоохранительных органов. Такие кибердружины, по нашему мнению, оказали бы серьезную помощь правоохранительным органам в установлении фактов незаконного оборота наркотиков в информационных сетях.

4. Обеспечить контролирование правоохранительными органами большего количества VPN-серверов для фиксации и записи запрещенной законодательством деятельности лиц в сфере незаконного оборота наркотиков с целью выхода на потенциального сбытчика или поставщика наркотических веществ.

СПИСОК ЛИТЕРАТУРЫ

1. Гаврилин, Ю. В. Совершенствование выявления, раскрытия и расследования хищений, совершенных с использованием информационных банковских технологий (по итогам Всероссийского онлайн-семинара) / Ю. В. Гаврилин, А. Г. Парадников // Труды Академии управления МВД России. – 2020. – № 2 (54). – С. 123–130.

2. Паспорт национального проекта Национальная программа «Цифровая экономика Российской Федерации» (утв. протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7). – URL: <https://docs.cntd.ru/document/564664077?yslid=lj17ztl4o1542770456>

3. Системно-программный комплекс Crystal. – URL: <https://crystalblockchain.com>

4. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.

5. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации (вместе с “Национальной стратегией развития искусственного интеллекта на период до 2030 года”)» (с изм. от 15.02.2024) // Собрание законодательства РФ. – 2019. – № 41. – Ст. 5700.

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. от 12.12.2023) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

7. Цифровая платформа «Инфосфера». – URL: <https://инфосфера.рус/?ysclid=lrpzig4rtl106356900>

8. Myip.net. – URL: <https://myip.ru/?ysclid=lrpztzcc7549754409>

9. Xinit.ru. – URL: <https://antex-e.ru>

REFERENCES

1. Gavrilin Iu.V., Paradnikov A.G. Sovershenstvovanie vyivleniia, raskrytiia i rassledovaniia khishchenii, sovershennykh s ispolzovaniem informatsionnykh bankovskikh tekhnologii (po itogam Vserossiiskogo onlain-seminara) [Improving the Detection, Disclosure and Investigation of Embezzlement Committed Using Information Banking Technologies (Based on the Results of the All-Russian Online Seminar)]. *Trudy Akademii upravleniia MVD Rossii* [Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia], 2020, no. 2 (54), pp. 123-130.

2. *Passport natsionalnogo proekta Natsionalnaia programma «Tsifrovaia ekonomika Rossiiskoi Federatsii» (utv. protokolom zasedaniia prezidiuma Soveta pri Prezidente Rossiiskoi Federatsii po strategicheskomu razvitiuu i natsionalnym proektam ot 4 iyunia 2019 g. № 7)* [Passport of the National Project National Program “Digital Economy of the Russian Federation” (Approved by the Minutes of the Meeting of the Presidium of the Presidential Council for Strategic Development and National Projects Dated June 4, 2019, No. 7)]. URL: <https://docs.cntd.ru/document/564664077?yslid=lj17zt14o1542770456>

3. *Sistemno-programmnyi kompleks Crystal* [Crystal System and Software Package]. URL: <https://crystalblockchain.com>

4. Ukaz Prezidenta RF ot 09.05.2017 № 203 «O Strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017–2030 gody» [Decree of the President of the Russian Federation Dated September 5, 2017, No. 203 “On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030”]. *Sobranie zakonodatelstva RF* [Collection of Legislation of the Russian Federation], 2017, no. 20, art. 2901.

5. Ukaz Prezidenta RF ot 10.10.2019 № 490 «O razvitiu iskusstvennogo intellekta v Rossiiskoi

Federatsii (vmeste s “Natsionalnoi strategiei razvitiia iskusstvennogo intellekta na period do 2030 goda”))» (s izm. ot 15.02.2024) [Decree of the President of the Russian Federation Dated October 10, 2019, No. 490 “On the Development of Artificial Intelligence in the Russian Federation (Together with the ‘National Strategy for the Development of Artificial Intelligence for the Period up to 2030’)” (As Amended on February 15, 2024)]. *Sobranie zakonodatelstva RF* [Collection of Legislation of the Russian Federation], 2019, no. 41, art. 5700.

6. Federalnyi zakon ot 27.07.2006 № 149-FZ «Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii» (s izm. na 12.12.2023) [Federal Law Dated July 27, 2006, No. 149-FZ “On Information, Information Technologies and Information Protection” (As Amended on December 12, 2023)]. *Sobranie zakonodatelstva RF* [Collection of Legislation of the Russian Federation], 2006, no. 31 (pt. 1), art. 3448.

7. *Tsifrovaia platforma «Infosfera»* [Digital Platform “Infosphere”]. URL: <https://инфосфера.рф/?ysclid=lrpxzg4rtl106356900>

8. *Myip.net*. URL: <https://myip.ru/?ysclid=lrpxttzc7549754409>

9. *Xinit.ru*. URL: <https://antex-e.ru>

Information About the Authors

Ivan N. Arkhiptsev, Candidate of Sciences (Jurisprudence), Associate Professor, Department of Criminal Law Disciplines, Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Gorkogo St, 71, 308024 Belgorod, Russian Federation, ArkhiptsevIN@yandex.ru, <https://orcid.org/0000-0003-2307-2712>

Alexander V. Sarychev, Deputy Head of the Course, Faculty of Law Enforcement, Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Gorkogo St, 71, 308024 Belgorod, Russian Federation, w0773@yandex.ru, <https://orcid.org/0000-0002-2115-3191>

Anna B. Beloshapko, Police Private, Cadet, 122 Platoon, Faculty of Interrogator Training, Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Gorkogo St, 71, 308024 Belgorod, Russian Federation, beloshapkoanna27022004@gmail.com, <https://orcid.org/0009-0000-1988-6655>

Информация об авторах

Иван Николаевич Архипцев, кандидат юридических наук, доцент, доцент кафедры уголовно-правовых дисциплин, Белгородский юридический институт МВД России им. И.Д. Путилина, ул. Горького, 71, 308024 г. Белгород, Российская Федерация, ArkhiptsevIN@yandex.ru, <https://orcid.org/0000-0003-2307-2712>

Александр Викторович Сарычев, заместитель начальника курса факультета правоохранительной деятельности, Белгородский юридический институт МВД России им. И.Д. Путилина, ул. Горького, 71, 308024 г. Белгород, Российская Федерация, w0773@yandex.ru, <https://orcid.org/0000-0002-2115-3191>

Анна Борисовна Белошапко, рядовой полиции, курсант 122-го взвода, факультета подготовки дознавателей, Белгородский юридический институт МВД России им. И.Д. Путилина, ул. Горького, 71, 308024 г. Белгород, Российская Федерация, beloshapkoanna27022004@gmail.com, <https://orcid.org/0009-0000-1988-6655>