

грамотность», определив ее как способность эффективно управлять личными цифровыми ресурсами; разбираться в особенностях различных информационных продуктов и услуг, иметь актуальную информацию о ситуации на информационном пространстве; принимать обоснованные решения в отношении безопасности использования информационных ресурсов.

Считаем целесообразным с учетом имеющегося российского опыта принятие Государственной программы Республики Беларусь «Цифровая грамотность», поскольку на сегодня личная цифровая грамотность становится важным условием работы в онлайн-среде. Посещение небезопасных сайтов, невозможность распознать откровенно мошеннические действия и фейковую информацию в сети Интернет приносят серьезные неприятности пользователю и тем самым создают дополнительную нагрузку на правоохранительные органы.

#### Список использованных источников

1. Абламейко, М.С. Правовые проблемы построения информационного общества в Республике Беларусь: теория и практика : автореф. дис... канд. юрид. наук : 12.00.14 / М.С. Абламейко ; Белорус. гос. ун-т. – Минск, 2012. – 28 с.
2. Жуков, А.З. Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права / А.З. Жуков // Проблемы экономики и юрид. практики. – 2019. – № 4. – С. 141–143.

УДК 343

*Р.Р. Насыров*

### **О ПРОТИВОДЕЙСТВИИ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ И ИХ АНАЛОГОВ**

Информационные технологии внедряются во все сферы жизни человека, и преступная сфера не является исключением. Информационно-телекоммуникационная сеть Интернет и информационные технологии позволили наркобизнесу выйти на новый уровень и привлечь внимание огромного количества людей.

Информационно-телекоммуникационные технологии на современном этапе развития активно способствуют развитию и модернизации наркосети, посредством которой осуществляется розничная и оптовая продажа наркотических средств, психотропных веществ и их аналогов. К тому же преступный элемент постоянно повышает меры конспира-

ции, зашифрованность электронных терминалов и сетевых ресурсов, которые служат для перевода денежных средств за наркотики. К наиболее распространенным интернет-площадкам и мессенджерам относятся DarkNet, LegalRC, Iklad, DarkWeb, AlphaBay Market, Daffy Duck, Silkkitie, AS, Lambo, Ramp, Dream Market, Silk Road, Hansa, BigRC.biz, Telegram.

Рассматривая маркетплейсы в теневом сегменте сети Интернет, стоит отметить, что на них перевод денежных средств между продавцом и покупателем допускается посредством платежных систем (например, Яндекс.Деньги, Qiwi, WebMoney и др). Как правило, в Qiwi открывается несколько счетов, на которых аккумулируются денежные средства. Впоследствии данные счета используются для проведения финансовых операций по приобретению различных криптовалютных форм в рублевом эквиваленте на Ethereum, Биткоин, Monero, Litecoin, Zcash, Ripple, Dash. Криптовалюта активно используется лицами, осуществляющими незаконную продажу наркотиков в теневом сегменте сети Интернет. Она обладает огромными преимуществами, так как под ней понимаются виртуальные денежные средства, не имеющие материального выражения и физической формы. Тем самым для криптовалюты характерен уровень анонимности, независимость от национальной валюты, защищенность, необратимость операций, автономность и условность.

Ко всему этому в противодействии криптовалютной наркоторговле большое значение приобретает проблема отсутствия у сотрудников правоохранительных органов необходимых знаний, касающихся криптовалюты и работы с ней. На практике возникает немало вопросов обнаружения и изъятия виртуальных цифровых денежных средств. Именно поэтому важно повышать знания и подготовку сотрудников в области информационных технологий и программирования. Следствием вышеуказанных проблем является отсутствие зарегистрированных случаев изъятия криптовалюты в качестве нелегального дохода от сбыта запрещенных в гражданском обороте средств и веществ.

В Стратегии Государственной антинаркотической политики Российской Федерации на период до 2030 года указано, что возникновение новых и модернизация уже имеющихся способов совершения преступлений организованными группами с использованием инновационных коммуникационных технологий и сетей выступает одной из самых злободневных угроз национальной безопасности в сфере контроля и противодействия незаконному обороту наркотических средств, психотропных веществ и их аналогов (Указ Президента Российской Федерации от 23 ноября 2020 г. № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года»).

В научных трудах рассматривается и анализируется точка зрения, которая предполагает внедрение и последующее использование современных технологий интеллектуального анализа в разработке информационно-аналитических сетей, позволяющие осуществить высокоэффективный мониторинг информационно-телекоммуникационной сети Интернет по вопросам наркоситуации в Российской Федерации и выдвигении методик борьбы с данными видами преступлений.

О подобной практике, которая успешно используется в зарубежных странах, пишет И.А. Завьялов в статье «Зарубежный опыт использования искусственного интеллекта в раскрытии преступлений». Так, например, ученые Американского Корнеллского университета в 2017 г. создали программную систему искусственного интеллекта, которая позволяет по публикациям, лайкам и аккаунтам пользователей всемирной сети Интернет установить наличие у них склонности к потреблению алкогольных напитков, табачных изделий, а также наркотических средств, психотропных веществ и их аналогов. Благодаря применению данной системы уже имеются положительные опыты выявления наркозависимых лиц и предупреждения незаконному обороту наркотиков. Следовательно, создание и применение систематизированного механизма нейросетевых технологий позволит правоохранительным органам оперативно и эффективно осуществлять установление даркнет-маркетплейсов и наркомаркетов по продаже наркотиков в сети Интернет. К тому же, это будет способствовать повышению результативности противодействия незаконному обороту наркотических средств и понижению уровня наркотизации населения.

УДК 343

*И.С. Нестер*

### **ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

Современный этап развития общественных отношений характеризуется активным научно-техническим прогрессом, скорость которого постоянно возрастает. Еще 20 лет назад мы вели речь о таком понятии, как «компьютеризация», а сегодня это считается обыденностью.

В настоящий момент на первый план выходит цифровизация, которая представляет собой внедрение цифровых технологий в различные сферы деятельности человека: образование, промышленность, наука, искусство, спорт и т. д. Само понятие цифровизации рассматривается

преимущественно в контексте экономического развития государства, служит своеобразным «драйвером», позволяет ускорить производственные процессы, снизить себестоимость продукции. Тем не менее в последнее время появилось достаточно большое количество научных публикаций о внедрении цифровых технологий в иные сферы, например, образование, здравоохранение и т. д.

В сложившейся ситуации все чаще звучат слова о внедрении цифровых технологий в правоохранительную деятельность. Несмотря на то что методы, используемые для защиты прав и свобод граждан, носят достаточно специфический, иногда карательный характер и не всегда позволяют применять передовые цифровые технологии в полной мере, их проникновение в данную деятельность не остается незамеченным.

Цифровизация правоохранительной деятельности не носит массовый, повсеместный, необдуманный характер. Внедрению современных цифровых технологий предшествует глубокий анализ, в процессе которого определяется множество их особенностей и характерных черт: эффективность технологии, возможность и необходимость ее внедрения, совместимость продукта с уже внедренными достижениями науки и техники, возможность обучения сотрудников правоохранительных органов использованию данных технологий и многое другое. Именно по этой причине уже внедренные средства цифровизации демонстрируют достаточно высокий результат, доказывают тем самым свою эффективность. Примечательным остается тот факт, что правоохранительные органы не останавливаются на достигнутом, анализ новых технологий по обозначенным критериям происходит на постоянной основе.

Ярким примером цифровизации в правоохранительной сфере является внедрение биометрических паспортов. Этот документ позволяет гражданину выполнять отдельные операции (открыть или закрыть банковский счет, покупать товары, оплачивать услуги, получать информацию, содержащую персональные данные в госорганах и многое другое) без непосредственного посещения соответствующего учреждения, т. е. удаленно. При этом идентификация гражданина происходит одновременно несколькими алгоритмами (отпечатки пальцев, распознавание голоса, изображение лица и т. д.). Одновременно с предоставлением гражданам широкого перечня возможностей реализации своих прав, биометрические документы упрощают идентификацию человека.

Немаловажное значение имеет работа правоохранительных органов с гражданами, организациями, общественными объединениями в рамках реализации принципа открытости в своей деятельности. Например, сайт Министерства внутренних дел Республики Беларусь содержит наиболее актуальную информацию о работе данного органа исполнительной власти, позволяет своевременно получать достоверные сведения об измене-