исключающей совершение им преступных деяний; постоянный превентивный контроль за действиями профилактируемого; постановка на профилактический учет.

Большая роль при осуществлении оперативно-розыскной профилактики принадлежит индивидуально-профилактической беседе.

Беседа – способ речевого общения оперативного сотрудника с профилактируемым лицом с целью выяснения сведений о личности последнего и иных данных, необходимых для достижения цели профилактики, а также доведения до него определенной информации предупреждающего характера. Индивидуальное профилактическое воздействие в форме беседы оказывается с применением метода убеждения и, как правило, содержит в себе: разъяснение причины проведения беседы; получение объяснений в письменной форме с согласия профилактируемого лица или в устной форме об обстоятельствах и мотивах совершения правонарушений; предупреждение о возможных последствиях в случае реализации преступных намерений.

Для проведения индивидуальной профилактической работы используются, как правило, служебные помещения правоохранительных органов, обстановка и условия в которых должны отвечать требованиям безопасности и способствовать достижению цели профилактики.

Ключевая роль в оперативно-розыскной профилактике общеуголовных преступлений принадлежит подразделениям уголовного розыска органов внутренних дел.

Сотрудники подразделений уголовного розыска выявляют при проведении оперативно-розыскных мероприятий причины и условия, способствующие совершению преступлений, принимают в пределах своей компетенции меры по их устранению; проводят оперативно-розыскные мероприятия по выявлению лиц, занимающихся приготовлением или покушением на преступление, принимают к ним меры, предусмотренные законодательством РФ; поддерживают взаимодействие с участковыми уполномоченными полиции, сотрудниками подразделений по делам несовершеннолетних, направленное на выявление преступлений, совершаемых несовершеннолетними, лицами, ранее судимыми, и лицами, ведущими аморальный образ жизни; осуществляют розыск лиц, скрывшихся от органов дознания, следствия и суда, без вести пропавших и несовершеннолетних, занимающихся бродяжничеством; участвуют в осуществлении мероприятий по предупреждению преступлений террористического характера и экстремистской направленности; осуществляют в пределах своей компетенции оперативно-розыскные мероприятия в отношении лиц, осужденных к наказаниям, не связанным с лишением свободы, и представляющих оперативный интерес.

УДК 343.97

В.К. Кирвель

СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

На семинаре-практикуме по преступлениям, связанным с использованием компьютерной сети (A/CONF.187/10), Десятого конгресса ООН по предупреждению преступности и обращению с правонарушителями (Вена, 2000) было предложено определение киберпреступности. Под ней понимается любое преступление, которое может осуществляться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети либо против компьютерной системы или сети.

На основании анализа зарубежных и национальных публикаций мы делаем вывод о том, что одним из направлений противодействия правоохранительных органов новым технологическим трендам в сфере киберпреступности способно стать противодействие искусственному интеллекту (ИИ) или искусственным нейронным сетям (ИНС), которые могут быть применены в криминальных целях.

Сегодня активно обсуждается использование в СМИ и информационных ресурсах интернета ИНС, умеющих генерировать видео- или аудиофальшивки. Эта технология получила название глубоких фейков (deepfake). По нашему мнению, она уже сейчас представляет реальную угрозу для граждан, юридических лиц и государства.

Глубокие фейки являются продуктом ИИ, известным как глубокое обучение, в котором набор алгоритмов, называемых ИНС, обучается понимать правила и воспроизводить модели путем обработки большого объема данных. Пары алгоритмов сводятся друг с другом в генеративные соперничающие сети (ГСС). В таких ИНС один алгоритм, называемый генератором, создает контент, смоделированный на основе исходных данных (например, искусственные изображения людей на основе реальных фотографий из банка данных), в то время как второй алгоритм, именуемый дискриминатором, пытается выявить искусственно созданный контент (в нашем случае – искусственные изображения людей). Поскольку каждый алгоритм постоянно учится противостоять другому, подобное сопряжение ведет к быстрому прогрессу, позволяющему ГСС искусственно генерировать высокореалистичные изображения людей на фото или видео либо встраивать изображения людей в существующие видеозаписи.

Технология глубоких фейков позволяет создавать высокореалистичные поддельные видео- и аудиозаписи, например изготавливать прав-

доподобные видеозаписи, в которых пользователи социальных сетей произносят определенные фразы либо сотрудники правоохранительных органов совершают некие действия, с целью оказать нужное психологическое воздействие на граждан и спровоцировать их к совершению противоправных действий или изменить общественное мнение в отношении правоохранительных органов.

Мы полагаем, что технология глубоких фейков может быть использована для совершения следующих видов преступлений, предусмотренных УК Республики Беларусь: разжигание расовой, национальной, религиозной либо иной социальной вражды или розни, реабилитация нацизма (ст. 130 УК), клевета (ст. 188 УК), оскорбление (ст. 189 УК), призывы к действиям, направленным на причинение вреда национальной безопасности Республики Беларусь (ст. 361 УК), и др.

Проблема глубоких фейков в настоящее время уже рассматривается на уровне государственных органов зарубежных стран. В 2018 г. члены Палаты представителей Конгресса США обратились к директору Национальной разведки с просьбой проинформировать конгрессменов и общественность о возможностях использования новых технологий для изготовления фальшивых аудио-, видео- и фотоизображений.

В 2020 г. в Минске прошел круглый стол «Deepfake: новый вызов информационной безопасности», организованный БелТА и Белорусским институтом стратегических исследований, на котором министр информации Республики Беларусь А.Н. Карлюкевич предложил на законодательном уровне разрешить проблему глубоких фейков.

Одним из превентивных методов противодействия криминальному применению глубоких фейков, по нашему мнению, является правовой. Полагаем, что заслуживает внимания российский опыт, а именно принятый в России Федеральный закон от 18 марта 2019 г. № 31-ФЗ «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации».

В соответствии с ч. 1 указанной статьи к глубоким фейкам деструктивной направленности относятся фейковые новости, т. е. недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи. В качестве меры реагирования данный закон предусматривает ограничение доступа к сетевому изданию или иному информационному ресурсу в интернете, которые распространяют недостоверные сведения.

Таким образом, одним из направлений противодействия правоохранительных органов новым технологическим трендам в сфере киберпреступности должно стать противодействие созданию и распространению глубоких фейков, которое требует разрешения не только на законодательном, но и на методическом, организационном, техническом и кадровом уровне.

Не претендуя на бесспорность высказанных суждений и выводов, полагаем, что публикация вызовет интерес у читателей, побудит к дискуссии теоретиков и практиков, а также станет поводом к проведению совместного комплексного научно-практического исследования указанной проблемы.

УДК 343.57:004.7

А.В. Климачков

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ СБЫТУ НАРКОТИЧЕСКИХ СРЕДСТВ, СОВЕРШАЕМОМУ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Международная практика борьбы с наркоманией и наркобизнесом свидетельствует о повсеместном и быстром распространении подпольного производства синтетических наркотических средств, сбыт которых в большинстве случаев происходит с использованием информационно-телекоммуникационных технологий. Наркорынок в России формируется под влиянием тенденций развития международной оперативной обстановки.

Данные официальной статистики МВД Российской Федерации свидетельствуют о том, что в январе – декабре 2020 г. выявлено 189,9 тыс. преступлений, связанных с незаконным оборотом наркотиков, что на 0,2 % меньше, чем за аналогичный период 2019 г.

При этом рост киберпреступности оказывает существенное влияние на криминогенную ситуацию в целом. Практика борьбы с незаконным сбытом наркотических средств свидетельствует о том, что современная наркопреступность в целом характеризуется криминальным профессионализмом, применением изощренных форм и методов совершения