распознаванию лиц, что является нарушением Европейской конвенции по правам человека. Теперь полиции запрещено пользоваться этими технологиями.

В Китае после ряда утечек персональных данных в 2019 г. введены жесткие стандарты для приложений, осуществляющих сбор биометрических персональных данных. Так, пользователь должен давать активное согласие на обработку биометрических данных, а оператор должен уведомить субъекта о целях, методах и объеме сбора данных.

Анализируя эту проблематику, нельзя не отметить случаи фальсификации видеоизображений при помощи нейронных сетей. Подделанные таким способом видео обозначаются термином «дипфейк» (от англ. Deep fake). Для борьбы с данным явлением МВД России был заключен контракт, согласно условиям которого к концу 2022 г. ведомство получит программу «Зеркало», позволяющую выявлять признаки внутрикадрового монтажа видеоизображений, произведенного с помощью искусственных нейронных сетей, позволяющих синтезировать видеоизображения людей [5].

Еще одним перспективным направлением развития идентификации, на наш взгляд, является создание мультимодальных биометрических систем, которые могут включать как статические, так и динамические методы, позволяющие одновременно идентифицировать личность человека сразу по нескольким биометрическим параметрам. Например, в ФБР США с 2011 г. реализуется проект NGI (Next Generation Identification), который представляет собой автоматизированную модульную систему идентификации, позволяющую устанавливать тождество объектов. В настоящее время система способна осуществлять идентификацию по отпечаткам пальцев, сетчатке глаза и изображению лица [6, с. 19].

Развитие науки и техники открывает также новые возможности для совершенствования уже применяющихся методов идентификации. Например, Американской ассоциацией рентгенологов (ARRS) была предложена методика биометрической идентификации, которая способна формировать трехмерные модели внутренних слоев отпечатков пальцев, которые практически невозможно подделать. Данный метод открывает новые возможности в системе идентификации, в частности, дает возможность однозначно отличать папиллярный узор живого человека от умершего [7, с. 14].

Резюмируя вышеизложенное, стоит еще раз отметить значимость системы идентификации в различных сферах общественной жизни, особенно в правоохранительной. Помимо традиционных видов идентификации развитие науки и техники открывает возможности по разработке и внедрению новых технологий, существенным образом повышающих результативность исследований. Системы, которые еще

10–15 лет назад могли существовать исключительно в качестве проектов, в настоящее время применяются повсеместно и активно содействуют в решении стоящих перед правоприменителем задач.

1. Чаплыгина, В.Н. Применение лицевой биометрии для информационно-аналитической поддержки розыскных мероприятий / В.Н. Чаплыгина, А.А. Москвичев // Криминалистика: вчера, сегодня, завтра. – 2021. – №1 (21). – С. 177–187.

2. МВД при помощи камер начнет искать преступников по татуировкам и походке [Электронный ресурс] / РБК. – Режим доступа: URL: https://www.rbc.ru/technology_and_media/24/02/2020/5e4fb5af9a7947cfdfd5e1e3 (дата обращения: 14.10.2022).

3. Карамзанова, Ж.В. В Китае камеры начали определять личность людей по походке. Да, даже круче, чем в «Черном зеркале» [Электронный ресурс] / Ж.В. Карамзанова. – Режим доступа: URL: https://medialeaks.ru/0811jkr-you-are-how-you-walk/ (дата обращения: 14.10.2022).

4. Сретенцев, А.Н. Некоторые особенности использования электронных отображений внешности человека в криминалистических целях и перспективы развития систем видеоидентификации / А.Н. Сретенцев // Науч. портал МВД России. – 2021. – № 4 (56). – С. 76–80.

5. МВД к концу 2022 года получит IT-разработку по распознаванию видео с заменой лиц [Электронный ресурс]. – Режим доступа: URL: https://tass.ru/obschestvo/11307705 (дата обращения: 14.10.2022).

6. Сретенцев, А.Н. Возможности и перспективы внедрения систем автоматического распознавания лица человека в процесс раскрытия и расследования преступлений / А.Н. Сретенцев // Рос. следователь. – 2021. – № 1. – С. 17–20.

7. Писарев, Д.Ю. Проблемы применения биометрических систем в раскрытии преступлений : автореф. дис. ... канд. юрид. наук : 12.00.09 / Д.Ю. Писарев ; Кубан. гос. ун-т. – Краснодар, 2012. – 19 с.

УДК 343.98

В.А. Талалаев, О.О. Лемешевский

О НЕКОТОРЫХ ВОПРОСАХ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ИЗУЧЕНИИ КРИМИНАЛИСТИКИ

Образование в Республике Беларусь – это обучение и воспитание в интересах человека, общества, государства, направленное на формирование гармоничной и разносторонне развитой личности. Предметом гордости в Беларуси является система высшего образования, которая успешно функционирует.

С 2020 г. Республика Беларусь превратилась в арену больших геополитических противостояний крупных мировых политических игроков,

став объектом неприкрытого информационного, политического и экономического давления со стороны западных государств [1].

Следует обратить внимание, что обстановка в мире остается крайне напряженной. В связи с этим Президент Республики Беларусь на совещании по вопросам безопасности страны отметил, что «каждый должен заниматься на месте своим делом». Иными словами, дал понять, что необходимо самоотверженно трудиться всем государственным институтам.

Образование на современном этапе играет важную роль в укреплении государства, улучшении его благосостояния. От качества получаемых знаний зависит будущее интеллектуального, управленческого капитала страны. В конкурентоспособности национальных экономик осуществляет важную роль не только добыча природных ресурсов и физический труд, а также знания.

Совершенствование и оптимизация основных направлений подготовки высокопрофессиональных юридических кадров, в том числе для системы органов внутренних дел, обеспечение квалифицированной правовой защиты граждан, повышение правовой культуры общества – актуальные задачи для национальной системы образования Республики Беларусь. Этот факт, в свою очередь, формирует потребность в компетентных юристах, способных решать задачи по предназначению.

О значении проблемы оптимизации существующей системы подготовки и повышения квалификации специалистов юридического профиля свидетельствует тот факт, что Министром образования утверждена Концепция развития юридического образования в Республике Беларусь на период до 2025 года, в которой отмечается, что одной из современных тенденций развития юридического образования является «информатизация юридического образования и усиление роли информационно-коммуникационных технологий в обеспечении процесса образования» [2].

Сущность изложенного выше сводится к тому, что в настоящее время актуально продолжение разработок и внедрения информационно-коммуникационных технологий для дальнейшего формирования специалиста, погруженного в будущую профессию. Обучающийся, находясь в отрыве от аудитории, может быть в контакте с преподавателем и иметь возможность в любое удобное время приступить к той или иной обучающей задаче. Такие приложения можно в определенной степени считать источниками литературы обучающегося и практического направления, объединив в себе несомненные достоинства традиционных учебников и возможности компьютерных технологий.

Образовательные мобильные приложения, например, криминалистической направленности, отличаются от приложений коммерческого типа.

Сфера оказания социальных услуг ушла вперед по сравнению с процессом цифровизации в юридическом образовании. Бытовая техника, продукты питания, автомобильные сервисы и т. п. давно имеют свои мобильные приложения с расширенным функционалом, возможностью доставки товара в любое удобное потребителю время. В случае необходимости мониторинга и приобретения последних редакций учебников, учебных пособий по юридическим дисциплинам, в большинстве случаев приходится прибегать к непосредственному посещению специальных книжных магазинов.

Кроме функции приобретения актуальной юридической литературы, приложения могут выполнять роль помощника обучающимся, при использовании в будущем – специалисту, и ориентированы на выполнение следующих перспективных задач:

помочь обучающемуся получать дополнительную информацию и знания, в том числе благодаря интерактивному взаимодействию с приложением;

ускорить обмен информацией, улучшить взаимодействие между преподавателем и подготавливаемым специалистом;

создавать образовательное сообщество, где каждый участник привносит свой вклад в его развитие;

упростить процесс оценки и контроля знаний;

модернизировать процесс обучения, привлекая максимально возможное количество участников, упростить понимание и усвоение полученной информации и др.

При этом процесс обучения становится интереснее, легче и доступнее, а систематизация базы знаний позволяет своевременно обновлять ее [3].

Примером такого приложения-помощника в рамках изучения учебной дисциплины «Криминалистика» может быть CrimeLib.info – энциклопедия и библиотека криминалистики и уголовного процесса, кроме того, Serious Games – интерактивные симуляторы, тренажеры для экспертно-криминалистической деятельности и т. д.

Справочник CrimeLib.info содержит сведения о различных тактико-технических особенностях производства следственного осмотра; алгоритмы описания отдельных объектов в протоколах следственных действий; перечень объектов, задач и типовых вопросов судебных экспертиз, системы типовых вопросов для допросов; методические рекомендации по расследованию преступлений различных категорий; проблемные вопросы квалификации различных составов преступлений; бланки и образцы заполнения основных процессуальных документов, составляемых следователем (дознавателем); компас и систему регистрации географических координат для ориентирования на местах происшествия, находящихся за чертой населенного пункта.

При условии разработки и размещения в свободном доступе на специализированных онлайн-магазинах (Google Play, App Store и др.) данные приложения вызовут обоснованный интерес той категории молодежи, которая готовится к поступлению в учреждения образования юридического профиля и изучает учебную дисциплину «Криминалистика». В этой связи посредством мобильных приложений могут быть с успехом решены отдельные задачи профориентационной работы, информационно-пропагандистской деятельности и иные.

Таким образом, в указанных условиях разработка, использование информационно-коммуникативных технологий, в том числе в виде мобильных приложений, специализированных компьютерных игр (тестов), способствуют более качественной подготовке юридического специалиста, повышению авторитета юридического образования и решению иных, связанных с указанными, задач.

1. О программе патриотического воспитания населения Республики Беларусь на 2022–2025 годы [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 29 дек. 2021 г., № 773 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Концепция развития юридического образования в Республике Беларусь на период до 2025 года [Электронный ресурс] : Концепция М-ва образования Респ. Беларусь, 31 авг. 2017 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

3. Непрерывное дополнительное образование в государствах – участниках СНГ: опыт, приоритеты и перспективы развития : сб. ст. IV Междунар. науч.-практ. конф., посвящ. 20-летию ИПКиП, г. Могилев, 26–27 нояб. 2020 г. / под ред. В.А. Гайсенка, И.В. Шардыко. – Могилев : МГУ им. А.А. Кулешова, 2021. – 352 с.

УДК 343.985.7

А.А. Точилкина

ПРОБЛЕМНЫЕ АСПЕКТЫ ОРГАНИЗАЦИИ ПРОЦЕССА РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ В УСЛОВИЯХ СОВРЕМЕННЫХ СОЦИАЛЬНО-ПРАВОВЫХ РЕАЛИЙ

Развитие современных технологий привносит в нашу жизнь как колоссальные возможности, так и новые угрозы. Преступления, совершаемые с использованием сети Интернет, – одна из серьезнейших проблем современного общества.

В условиях стремительного развития информационных технологий, широкое распространение получает новый вид преступной деятельности – киберпреступность, которая, несомненно, носит трансграничный характер. Киберпреступление – это правонарушение, которое совершено в электронной сфере, направлено на незаконное проникновение в работу компьютерных сетей, программ, устройств, с целью видоизменения данных, их изъятия или добавления ложной информации. Понятия «киберпреступление» и «киберпреступность» будут использоваться в данной статье, так как имеют один и тот же смысл с понятиями «преступление, совершаемое с использованием сети Интернет» и «преступность в сети Интернет» [1].

При расследовании преступлений указанной категории правоохранительные органы сталкиваются с рядом проблем, отдельные из которых подлежат рассмотрению.

В связи с вышеизложенным в первую очередь справедливо отметить, что киберпространство принципиально трансгранично, здесь нет расстояния и часто верно определить местоположение источника кибератаки очень трудно, что приводит к активизации транснациональной киберпреступной деятельности. Из транснационального характера киберпреступлений вытекают трудности их расследования. Одна из трудностей заключается в том, что принцип суверенитета предполагает проведение расследований в определенном государстве только с согласия этого государства. Именно поэтому очень важно сотрудничество между государствами – от этого зависит раскрытие киберпреступлений. Другая трудность связана со временем – оно крайне ограничено (а для совершения киберпреступления часто достаточно нескольких секунд, и следы от киберпреступлений удаляются очень быстро). В связи с этим решающее значение имеет оперативное и своевременное взаимодействие между государствами.

Во-вторых, следует отметить, что в условиях современных социально-правовых реалий киберпреступления становятся все более совершенными, изощренными и скрытными, они наносят крупный экономический и политический ущерб. В связи с этим следует указать, что в киберпространстве действуют разнородные субъекты – и государства, и негосударственные субъекты, что вызывает сложности при разграничении преступной деятельности и политической деятельности государств в киберпространстве. Некоторые негосударственные субъекты могут превосходить кибервозможности государств и способны проводить кибероперации, которые глубоко затрагивают безопасность отдельных государств и международную безопасность. Следовательно, в киберпространстве сглаживаются различия между государством и негосударственными субъектами в отношении ресурсов и кибервозможностей. Распространено мнение, что лишь государства способны прово-