УДК 343.3/.7
DOI: 10.17238/issn2686-9241.2019.2.133-155

Цифровизация и ее уголовно-правовые риски

А.И. Чучаев*, Ю.В. Грачева, С.В. Маликов****

** Крымский филиал, ФГБОУВО «Российский государственный университет правосудия», г. Симферополь, Россия*
*** ФГБОУВО «Московский государственный юридический университет имени О.Е. Кутафина» (МГЮА), г. Москва, Россия*
moksha1@rambler.ru, uvgracheva@mail.ru, s.v.malikov@yandex.ru

Введение. Значимость изменений и их беспрецедентная динамика изменяют характер угроз собственности, жизни и здоровью человека, организациям, социуму и государству. Противодействие киберугрозам ставит новые задачи перед специалистами по информационной безопасности, требует выработки механизмов правовой защиты, которые позволят опережающими темпами реагировать на криминогенные угрозы в цифровой среде. К сожалению, отечественный законодатель опаздывает в принятии решений; уголовно-правовые нормы, целью которых является противодействие преступлениям в информационной сфере, страдают пробельностью, неспособны охватить все возможные общественно опасные деяния и их последствия.
Теоретические основы. Методы. Общеметодологическую основу работы составляет всеобщий диалектический метод, базирующийся на законах и категориях диалектического и исторического материализма. Также использованы частные и специальные методы научного познания: системно-структурный, формально-логический, сравнительно-правовой и статистический анализ, контент-анализ, непосредственное наблюдение.
Результаты исследования. В статье проводится анализ сфер жизнедеятельности, на которые инновационные технологии воздействуют или будут оказывать наибольшее влияние. Тем самым преследуется в первую очередь пропедевтическая цель – создание необходимого теоретического фундамента для последующего рассмотрения специальных уголовно-правовых вопросов. К таким сферам отнесены: цифровая медицина, цифровая логистика, электронная коммерция и умные дома.
Обсуждение и заключение. Защита от киберугроз требует как постоянно интегрируемого и автоматизируемого подхода к кибербезопасности, так и адаптации законодательства к таким угрозам. Подготовка нормативных правовых актов, регулирующих вопросы цифровизации в определенной сфере (медицина, персональные данные, экономика, логистика, жилищно-коммунальные услуги и др.), должна сопровождаться оценкой возможных рисков с целью безотлагательной разработки (корректировки) уголовно-правовых норм, охраняющих соответствующие общественные отношения. В частности, можно говорить о следующих «пробелах» в уголовном законодательстве: ненаказуема пропаганда либо реклама наркотических средств, совершенных с использованием информационно-телекоммуникационных сетей (сети Интернет); не проводится усиления ответственности за распространение оружия и торговлю людьми, совершаемые посредством сети Интернет; сложностью при противодействии преступлениям, связанным с электронной коммерцией, является использование криптовалюты; односторонней представляется позиция законодателя по вопросу охраны персональных или идентифицирующих физических и юридических лиц данных; отсутствуют уголовно-правовые средства реагирования в случаях цифровизации медицинской деятельности и управления беспилотными транспортными средствами.

Ускоренная цифровизация всех сфер жизнедеятельности человека требует усиленной правовой защиты, одним из аспектов которой может выступить формирование новой главы Уголовного кодекса Российской Федерации, посвященной информационной безопасности. Содержание такой главы может объединить так называемые компьютерные преступления и иные деяния, связанные с незаконным использованием информации, сопровождающиеся причинением материального ущерба, вреда здоровью и жизни.

Ключевые слова: цифровая медицина, цифровая логистика, умный город, электронная коммерция, риски цифровизации, противодействие преступности

Для цитирования: Чучаев А.И., Грачева Ю.В., Маликов С.В. Цифровизация и ее уголовно-правовые риски // Правосудие. 2019. Т. 1, № 2. С. 133–155. DOI: 10.17238/issn2686-9241.2019.2.133-155

Digitalisation and its Criminal-Legal Risks

Alexandr I. Chuchaev*, Yulia V. Gracheva, Sergey V. Malikov****

** Crimea Branch, Russian State University of Justice, Simferopol', Russia*
*** Kutafin Moscow State Law University, Moscow, Russia*
For correspondence: moksha1@rambler.ru, uvgracheva@mail.ru, s.v.malikov@yandex.ru

Introduction. The significance of changes and their unprecedented dynamics changes the nature of threats to property, life and health, organizations, society and the state. Countering cyber threats poses new challenges for information security specialists, and requires the development of legal protection mechanisms that will allow them to respond at a faster pace to criminal threats in the digital environment. Unfortunately, the domestic legislator is late in making decisions; criminal law norms, the purpose of which is to counteract crimes in the information sphere, suffer from a gap, unable to cover all possible socially dangerous acts and their consequences.
Theoretical Basis. Methods. The General methodological basis of the work is the universal dialectical method based on the laws and categories of dialectical and historical materialism. Private and special methods of scientific cognition are also used: system-structural, formal-logical, comparative-legal and statistical analysis, content analysis, direct observation.
Results. The article analyzes the spheres of life on which innovative technologies affect or will have the greatest impact. Thus the propaedeutic goal is pursued in the first place-the creation of the necessary theoretical Foundation for the subsequent consideration of special criminal law issues. These areas include digital medicine, digital logistics, e-Commerce and smart homes.
Discussion and Conclusion. Protection against cyber threats requires both a constantly integrated and automated approach to cybersecurity and the adaptation of legislation to such threats. The preparation of normative legal acts regulating the issues of digitalization in a certain area (medicine, personal data, economy, logistics, housing and communal services, etc.) should be accompanied by an assessment of possible risks in order to urgently develop (adjust) criminal law norms that protect the relevant public relations. In particular it is possible to speak about the following "gaps" in the criminal law: propaganda or advertising of narcotic drugs committed using information and telecommunication networks (Internet) is not punishable; there is no strengthening of responsibility for the proliferation of weapons and human trafficking committed through the Internet; the difficulty in countering crimes related to e-Commerce is the use of cryptocurrency; the position of the legislator on the protection of personal or identifying data of individuals and legal entities is one-sided; there are no criminal legal means of implementation in cases of digitalization of medical activities and management of unmanned vehicles.
The accelerated digitalization of all spheres of human activity requires enhanced legal protection, one of the aspects of which is the formation of a new Chapter of the criminal code devoted to information security. The content of such a Chapter can unite the so-called computer crimes

and other acts associated with the illegal use of information, accompanied by causing material damage, harm to health and life.

Keywords: digital medicine, digital logistics, smart city, e-Commerce, risks of digitalization, combating crime

For citation: Chuchaev, A.I., Gracheva, Yu.V. and Malikov, S.V., 2019. Digitalisation and its criminal-legal risks. *Pravosudie* = Justice, 1(2), pp. 133–155. DOI: 10.17238/issn2686-9241.2019.2.133-155

Введение

Усиление деловой, социальной активности в киберпространстве, цифровая трансформация предпринимательской деятельности и деятельности государственных и муниципальных служб обусловливают актуальность проблем трансформации права в условиях развития цифровых технологий. В Стратегии развития информационного общества в Российской Федерации указано на широкое распространение и доступность мобильных устройств, беспроводных технологий, сетей связи, создание системы предоставления государственных и муниципальных услуг в электронной форме, к которой подключились более 34 млн россиян[1]. Последние данные свидетельствуют, что в России почти 110 млн пользователей интернета, из них 70 млн активно пользуются социальными сетями и практически 60 млн используют мобильные приложения[2].

Тема цифровизации в настоящее время весьма актуальна среди исследователей, в том числе в области уголовного права. Внимание отечественных ученых узконаправлено и акцентировано на так называемых компьютерных преступлениях и защите информации, что обусловлено существующей структурой уголовного законодательства, обособившего преступления в сфере компьютерной информации и включающего квалифицирующие признаки в отдельные составы преступлений [Букалерова, Л.А., 2009; Гузеева, О.С., 2015; Козаев, Н.Ш., 2015; Степанов-Егиянц, В.Г., 2016; Тропина, Т.Л., 2009]. Иной взгляд характерен для криминологических исследований, однако работ в этой области немного [Косынкин, А.А., 2013; Овчинский, В.С., 2018; Соловьев, В.С., 2017]. Предметом изучения в данной статье выступили риски в отдельных сферах жизнедеятельности человека, сопровождающиеся или имеющие значительный потенциал для внедрения цифровых технологий и недостаточно исследуемые в отечественной науке. Наряду с прогнозированием отдельных рисков и угроз кратко характеризуется сама сфера и ее преимущества.

---

[1] См.: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». Доступ из справочной правовой системы «КонсультантПлюс».

[2] См.: The new Global Digital Statshot report. URL: https://wearesocial.com/blog/2019/07/global-social-media-users-pass-3-5-billion

Теоретические основы. Методы

Общеметодологическую основу исследования составляет всеобщий диалектический метод, базирующийся на законах и категориях диалектического и исторического материализма. Помимо этого используются частные и специальные методы научного познания: системно-структурный, формально-логический, сравнительно-правовой и статистический анализ, контент-анализ, непосредственное наблюдение и др.

Теоретическая основа исследования, выводы и предложения базируются на научном осмыслении трудов и результатов исследований отечественных и зарубежных ученых в области уголовного права и криминологии, научных работ в специализированных изданиях, материалов по результатам проведения научно-практических мероприятий (конгрессов, конференций, круглых столов).

Результаты исследования

Электронная коммерция. Электронная коммерция – это покупка и продажа товаров или услуг через интернет, а также передача денежных средств и информации, необходимых для выполнения этих транзакций. Электронный бизнес относится ко всем аспектам ведения бизнеса в интернете, тогда как электронная коммерция обозначает транзакции именно товаров и услуг. Проблемы правового регулирования электронной коммерции начали разрабатываться сравнительно недавно: сначала в западных странах [Paton, D., 2002; Voss, G., et al., 2012; Beurskens, F., 2003; Asplin, T., 2002], а затем и в России [Рассолов, И.М., 2003; Шамраев, А.В., 2003; Тедеев, А.А., 2002]. Основными проблемами правового регулирования данной сферы являются: соотношение государственного регулирования и саморегулирования; правомерность распространения государственного суверенитета на виртуальное пространство; выработка единообразного понятийного аппарата в сфере электронной коммерции; идентификация участников электронной коммерции, электронного документооборота и электронной сделки; юрисдикция и применимое право в сфере электронной коммерции; обеспечение безопасности информационного обмена [Нугаев, Ш.Р., 2010].

Электронная коммерция имеет множество преимуществ по сравнению с обычными методами ведения торговли. Потребители могут легко осуществлять поиск товаров по базе данных товаров и услуг, а также видеть фактические цены, формировать заказ на определенную дату и даже создавать «списки пожеланий», надеясь, что кто-то заплатит за выбранный товар. Клиенты интернет-магазинов могут сравнивать цены одним щелчком мыши и покупать необходимый продукт после сравнения его цены со всеми ценами, представленными в интернете.

Интернет-продавцы в свою очередь тоже получают определенные преимущества. Интернет и его поисковые системы предоставляют клиентам возможность найти товар даже в тех магазинах, которые не мо-

гут позволить себе дорогостоящую рекламную кампанию. Благодаря распространению интернета небольшие интернет-магазины также выходят на мировые рынки. Кроме того, веб-технологии позволяют отслеживать предпочтения клиентов и осуществлять персонализированные маркетинговые инициативы.

Кроме явных преимуществ перед другими формами торговли электронная коммерция сопряжена с определенными проблемами: уязвимость и риски, присущие всем информационным системам; влияние на покупательскую активность; возможности, которые анонимная электронная коммерция дает правонарушителям, и др.

Во-первых, электронная коммерция оказывает воздействие на потребительское поведение:

– использование информации поведенческих паттернов позволяет влиять на покупателя и фактически скрыто вынуждать делать покупки;

– информация о геолокации потенциального покупателя дает возможность использовать его склонности к импульсивным покупкам.

Правовой статус подобного влияния не определен, но интеллектуальное навязывание приводит к росту объемов продаж на сотни миллионов рублей. Отсутствие правовой защиты не позволяет покупателям жаловаться, они винят себя, хотя становятся жертвами манипуляций.

Во-вторых, такая торговля способствует незаконным продажам товаров:

– возможность создавать интернет-магазины в анонимной зоне, где ни продавец, ни покупатель не предоставляют сведения друг о друге, приводит к росту объемов электронных продаж запрещенных товаров (наркотиков, оружия), оказания интимных услуг и т. д.;

– оборот виртуальных валют направлен на сокрытие факта и назначения оплаты запрещенного товара.

В-третьих, электронная коммерция используется при отмывании полученных преступным путем денег. Виртуальные товары и криптовалюты имеют ценность в виртуальной среде, что дает возможность использовать их как объект спекуляции и после ряда операций скрывать происхождение преступно полученных денежных средств.

В-четвертых, электронная коммерция сопряжена с рисками нарушения безопасности:

– при оплате товара в электронных магазинах профиль покупателя, содержащий реквизиты и пин-код банковской карты, может быть взломан в целях последующего хищения денежных средств;

– взлом вирусом системы «клиент – банк» позволяет скопировать сертификат электронной подписи, при помощи которого формируются распоряжения о переводе денежных средств при оплате товара;

– злоумышленник, путем взлома получивший доступ к личному кабинету интернет-магазина, может заказать товар на фальшивый адрес;

– имея сведения о покупке некоторых товаров, злоумышленник может пойти на шантаж; в первую очередь это касается данных об определенных видах лекарств.

Цифровая медицина. Медицина – один из самых сложных и ответственных видов деятельности. Развитие цифровых технологий сильно повлияло на качество и доступность медицинских услуг, позволило лучше лечить, предотвращать развитие многих заболеваний, повышать качество жизни хронических больных и даже изменять восприятие здорового образа жизни у огромного числа людей [Кантемирова, М.А. и Аликова, З.Р., 2019; Афонасков, О.В., и др., 2018; Романова, И., 2013; Brown, B., 2011; Alshahrani, W., 2018; Tavazzi, L., 2019; Kohl, S.E., 2019].

Одной из приоритетных задач, поставленных ООН перед своими членами, является создание системы всеобщего здравоохранения[3]. В соответствии с определением, данным Всемирной Организацией Здравоохранения, эта система подразумевает прежде всего равный доступ к медицинским услугам, включая лечебную, реабилитационную, профилактическую, паллиативную медицинскую помощь, при этом их качество должно способствовать улучшению здоровья и не зависеть от финансовых возможностей обратившихся за ними.

Самое значительное влияние цифровизация оказала на:

– диагностику, улучшив ее качество за счет использования систем больших данных и машинного обучения;

– оценку влияния на организм новых препаратов благодаря предсказательной аналитике и системам искусственного интеллекта;

– трансплантологию – появились новые виды умных имплантов и даже кибернетические органы (обучаемые руки, ноги) вследствие достижений в области роботизации и искусственного интеллекта;

– качество и оперативность применения мер при мониторинге состояния (давления, уровня сахара и др.) пациентов с хроническими заболеваниями;

– развитие систем ранней диагностики благодаря возможности собирать и анализировать данные, получаемые с IoT-устройств – трекеров активности, пульсометров, умных весов;

– взаимодействие между пациентом и врачами-специалистами – за счет появления телемедицины;

– платформы и маркетплейсы медицинских услуг, обеспечивающие возможность выбрать специалиста по результатам его исследований.

Россия довольно активно движется в направлении цифровизации медицины, разрабатывается соответствующая законодательная база[4].

---

[3] См.: United Nations. Resolution adopted by the General Assembly on 25 September 2015. 70/1. Transforming our world: the 2030 Agenda for Sustainable Development // UN. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E; United Nations. Sustainable Development Goals. 17 Goals to transform our world // UN. URL: http://www.un.org/sustainabledevelopment/health.

[4] См.: Федеральный закон от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам примене-

В частности, утверждено Положение о единой государственной информационной системе, которая будет включать 13 подсистем, в том числе: федеральный регистр медицинских работников, федеральный реестр медицинских организаций, федеральную электронную регистратуру, федеральную интегрированную электронную медицинскую карту, федеральный реестр электронных медицинских документов, подсистему ведения специализированных регистров пациентов по отдельным нозологиям и категориям граждан, мониторинга организации оказания высокотехнологичной медицинской помощи и санаторно-курортного лечения, подсистему мониторинга и контроля в сфере госзакупок лекарственных препаратов[5].

Изменения технологий и способов взаимодействия открывают и новые возможности для совершения медицинскими работниками преступлений, таких как мошенничество, подделка данных цифровой диагностики для обоснования трат и запроса компенсаций у страховых компаний. В условиях цифровизации по-другому нужно оценивать врачебные ошибки: при наличии доказанного эффективного метода и его доступности пренебрежение им следует рассматривать как преступление. Встает вопрос о допустимом количестве врачебных ошибок каждого врача. Технологии позволяют проводить мониторинг и оценку эффективности работы индивидуально и в целом медицинского учреждения как структурной единицы. Другим аспектом этой проблемы является то, что в традиционной схеме разделения ответственности ошибка – это результат деятельности конкретного врача, а в условиях применения цифровых методов ставится вопрос об ответственности архитекторов диагностических систем и лиц, вносящих в такие системы информацию о пациенте, симптомах заболевания и др. Искажение вносимой информации может породить череду ошибочных диагнозов.

Использование информационных систем для сбора всеобъемлющей информации о пациентах и врачах создает определенные риски, которые могут исходить от медицинского персонала, IT-персонала, внешних злоумышленников, самих пациентов.

Мошенничество со страховыми выплатами. Это умышленное искажение данных руководством медицинского учреждения, предпринимаемое для того, чтобы повысить страховые выплаты. В настоящее время в зарубежных странах имеет место судебная практика, согласно которой для искажения работы диагностического алгоритма врачи ме-

ния информационных технологий в сфере охраны здоровья». Доступ из справочной правовой системы «КонсультантПлюс».

[5] См.: Постановление Правительства Российской Федерации от 5 мая 2018 г. № 555 «О единой государственной информационной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»). Доступ из справочной правовой системы «КонсультантПлюс».

няли пиксели в снимке МРТ. В результате система искусственного интеллекта определяла признаки болезни, которой на самом деле не было. Такого рода преступления снижают скорость распространения автоматизированных систем проверки заявок на страховые выплаты, поскольку есть риск, что недобросовестные должностные лица будут пытаться обмануть эти системы ради получения одобрения. В конечном счете от подобного мошенничества страдает здоровье пациентов, поскольку автоматизированная система повысила бы скорость ответа и, как следствие, качество медицинского вмешательства.

Неквалифицированная медицинская помощь. Новые формы взаимодействия с пациентом через сайт продаж медицинских услуг и услуг телемедицины создают риски появления ситуаций, в которых подтверждение личности врача не обеспечено, в результате чего лица с неподтвержденной квалификацией ведут удаленное консультирование, чтобы получить денежное вознаграждение. Это провоцирует риски нанести вред здоровью пациентов, получающих неквалифицированную медицинскую помощь.

Риски врачебных ошибок. Некоторые методы машинного обучения подразумевают использование прошлого опыта (ретроспективных данных о лечении и его результатах) для оптимизации алгоритмов и для самонастройки. Эти данные актуализируются после принятия системы в эксплуатацию, для обучения в системе задействованы данные, которые заносят соответствующие врачи, работающие в конкретной организации. Если подавляющее большинство специалистов из-за своей низкой квалификации будут вводить в систему некорректные заключения или данные о результатах лечения будут внесены в искаженном виде, то система с некоторой вероятностью пройдет самообучение и начнет генерировать ошибочные заключения в соответствии с загружаемой информацией.

Таким образом, корректность ввода сведений об одном пациенте влияет на точность диагностики другого, следующего за первым. Трудность контроля ручного занесения информации создает риски появления врачебных ошибок не только у одного врача в отношении одного пациента, но и у всех пользующихся системой диагностики для всех последующих обследуемых пациентов.

Нарушение конфиденциальности сведений о здоровье может произойти в результате кибератаки, преступных действий медицинских работников, халатности службы информационной безопасности и способно вызвать такие последствия, как:

– вымогательство денежных средств, совершаемое с угрозой уничтожить медицинские данные;

– шантаж пациентов, для которых утечка сведений о здоровье может привести к отказу в принятии на работу (если соискатель зарегистрирован в наркологии, имеет хронические болезни, беременность), увольнению (известны прецеденты с больными гепатитом, СПИДом), семей-

ным конфликтам с финансовыми последствиями (венерические заболевания, беременность);

– мошенничество в отношении психологически нездоровых, одиноких пациентов, психологическое давление и принуждение к передаче активов;

– доведение до самоубийства на основе данных о психическом состоянии;

– противоправные действия в отношении имущества пациентов на основе данных об их перемещениях и местонахождении (больница, санаторий).

Нарушение целостности и достоверности данных о здоровье может иметь определенные последствия:

– подмена диагностической информации в целях спровоцировать неадекватное лечение и нанести вред здоровью;

– подмена информации для признания невменяемости и принудительного назначения опекунства;

– подмена информации в целях получать льготы, которые полагаются инвалидам и другим категориям населения.

Нарушение режима доступа к медицинским данным может привести к нанесению вреда здоровью (и даже к угрозе жизни) пациенту в результате:

– прерывания сеанса удаленной хирургической операции;

– недостаточно оперативного предоставления сведений электронной карты больного или потери этой информации;

– сбоя в работе электронно-управляемого оборудования;

– нарушения передачи информации с датчиков давления, уровня сахара, пульса и т. п.

Цифровая логистика. Логистика – это комплексное планирование, организация, координация, управление, контроль и физическая реализация всех операций движения материальных, финансовых, информационных потоков и потоков трудовых ресурсов. Благодаря цифровым технологиям изменение логистических функций может выйти за рамки простого улучшения существующих процессов и перевести их на новый уровень, позволяя динамически, в режиме реального времени отслеживать не только транспортные средства или крупные сборные грузы, но и каждый конкретный груз или каждого пассажира. Цифровые технологии позволяют не только осуществлять мониторинг, но и управлять движением на каждом участке логистической цепочки, брать под контроль все инфраструктурные составляющие логистических процессов. Телематические сервисы помогают посредством датчиков и разных видов беспроводных соединений постоянно передавать информацию о местонахождении, весе, эксплуатационной пригодности, загруженности, маршруте транспортных средств [Бубнова, Г.В. и Левин, Б.А., 2017; Абдюшева, Д.Р., Меренков, А.О. и Степанов, А.А., 2017; Дмитриев, А.В., 2018; Aktas, E. and Meng, Y., 2017; Francisco, K. and Swanson, D., 2018; Lianguang, C., et al., 2012].

Уже в настоящее время транспортная логистика сильно изменилась под влиянием цифровых технологий, при этом совершенствование цифровых решений продолжается. Среди основных ее трендов можно выделить следующие. Получение «информации в режиме реального времени обо всем и везде» напрямую связано с концепцией интернета вещей. Технология дает возможность отслеживать перемещение людей, объектов (грузов), транспорта, планировать маршруты, контролировать качество поездки или доставки. Объектом цифровизации становится также сама транспортная инфраструктура. Оснащенные датчиками дороги, железные дороги, верфи позволяют владельцам транспортных автомагистралей ежедневно получать информацию об их состоянии. Специальные мобильные датчики-сканеры выступают как системы раннего предупреждения сбоев и критичного износа. Владельцы при обнаружении внезапного дефекта оперативно принимают меры для предотвращения аварий и нештатных ситуаций. Ориентированные на пользователя мобильные сервисы дают людям полный контроль над своими перемещениями. Посредством текущей волны цифровых инноваций при помощи мобильных устройств намечаются все виды поездок. С помощью смартфонов уже планируются пешие маршруты и маршруты автомобильного транспорта, а также приобретаются билеты на самолет или поезд.

Цифровая логистика – не просто один из способов перемещения пассажира из пункта А в пункт Б. Это система, соединяющая режимы, услуги, технологии и конструкции в соответствии с наилучшим вариантом для пассажира. Интегрированные и интеллектуальные транспортные сети будут определять спрос, измерять производительность и контролировать состояние транспортных средств и других активов. Умная инфраструктура и связанные транспортные сети становятся обычным явлением. Повсеместно распространяется аналитика для управления трафиком и реагирования на инциденты в реальном времени. Данные, получаемые от мобильных устройств, лежат в основе аналитического управления транспортом. Анализ больших объемов данных помогает операторам перевозок оптимизировать производительность транспортных сетей, услуг и знаний, управление взаимоотношениями с клиентами.

В настоящее время несчастные случаи на транспорте или складских объектах происходят в основном из-за человеческого фактора. Ошибки водителей, операторов или пилотов – главная причина несчастных случаев на транспорте. Теоретически автономные транспортные средства должны снизить их количество, а с появлением усовершенствованных датчиков транспортные средства станут поддерживать оптимальные расстояние, скорость и курс, отслеживать внешние условия в режиме реального времени. Однако риски несчастных случаев и нанесения материального ущерба не исчезают, а модифицируются в зависимости от технологии, которая лежит в основе того или иного логистического процесса.

В отличие от аварий с участием человека аварии с участием беспилотных транспортных средств (БТС) могут происходить по целому ряду причин, последствия от аварий могут быть самыми разнообразными – от порчи имущества и срыва сроков доставки до травм и человеческих жертв. Причинами аварий БТС являются:

– ошибки управляющих систем;

– несанкционированный доступ, т. е. доступ несанкционированного оператора к системе управления. В случае физического доступа, если оператор не знаком с оборудованием, связанным с роботизированной средой, он может оказаться в опасной и потенциально смертельной зоне. В случае удаленного доступа неквалифицированные действия могут нанести материальный ущерб;

– механические неисправности;

– сбой в системе питания (повреждение, преднамеренное отключение источников питания; возможны столкновения и травмы, падение, например беспилотных летательных аппаратов);

– неправильная установка при настройке складского робота.

Кроме рисков, вызванных непосредственно технологическими сбоями, БТС создают новые возможности для совершения традиционных преступлений:

– использование БТС наркокурьерами (даже в случае пресечения такой деятельности отправитель с высокой вероятностью останется анонимным, а доставка наркотиков в зоне видимости при помощи дрона позволяет конечным распространителям снизить риски; все это затрудняет контроль со стороны правоохранительных органов за распространением наркотиков);

– использование самоуправляемых машин для террористических атак (доставка взрывчатых веществ перестанет представлять прямую угрозу для жизни террористов, что повысит угрозу террористических актов);

– политическая борьба с представителями органов власти, которая станет анонимной и децентрализованной (противники политического режима, оснащенные автономными средствами доставки, могут использовать идеологию точечного устранения противника).

Цифровизация управления зданиями и оказания жилищно-коммунальных услуг. Технологии интернета вещей, блокчейн, искусственного интеллекта позволяют перевести управление зданиями на новый уровень. Посредством «цифровых копий» объектов коммунально-инженерной инфраструктуры отслеживается «жизненный цикл» объектов и инженерных систем; фиксируются и прогнозируются поломки инфраструктурных элементов (лифтов, трубопроводов и т. п.), необходимость капитального ремонта зданий и многоквартирных домов. В зданиях со сложными механическими системами отопления, вентиляции и кондиционирования воздуха модернизируются системы управления, которые повышают комфорт и производительность труда находящихся в

них людей. Новые технологии дают возможность исключить человеческий фактор при определении объемов финансирования ЖКХ, мониторинге качества выполнения работ, идентификации проблемных зон, выявлении и предотвращении правонарушений.

Повсеместно распространяются технологии умных зданий, что выходит за рамки просто технологических концепций. Умные здания обладают способностью «соединять» людей с технологиями. Технология умных зданий помогает в управлении объектами, предоставляет ценную информацию об использовании помещений. Например, датчики движения и уровня углекислого газа характеризуют загруженность помещений, что важно для перепланировок. Благодаря подключенным к интернету приборам учета можно по запросу полностью автоматизировать учет и оплату всех услуг ЖКХ, что выявляет неэффективность использования ресурса [Волынсков, В.Э., 2018; Сапир, Ж., 2018; Голенкова, А.А., Шагбазян, С.И. и Степанова, Н.Р., 2017; Meijer, A., 2018; Pagan, J., 2018].

В Российской Федерации в настоящее время развивается аппаратно-программный комплекс «Безопасный город», целью которого является повышение общего уровня общественной безопасности, правопорядка и безопасности среды обитания за счет существенного улучшения координации деятельности сил и служб, ответственных за решение этих задач, путем внедрения на базе муниципальных образований комплексной информационной системы, обеспечивающей прогнозирование, мониторинг, предупреждение и ликвидацию возможных угроз, а также контроль устранения последствий чрезвычайных ситуаций и правонарушений[6]. Внедрение этого комплекса направлено на обеспечение безопасности всего города, а не отдельных зданий и производственных комплексов.

С появлением возможности удаленного цифрового управления механизмами зданий стандартные риски физической безопасности дополнились рисками информационной безопасности:

– совершаются кибератаки на управляющие элементы приборов очистки воздуха и кондиционирования, что вызывает вынужденную перегрузку и выход из строя элементов системы автоматизации зданий;

– кроме механических повреждений нарушения в работе наносят урон здоровью людей, например, нарушения в работе системы кондиционирования зачастую провоцируют астматические приступы, сбои в системе освещения – эпилептические приступы, в системе обогрева (в периоды естественно высокого температурного фона) – тепловой удар;

---

[6] См.: Распоряжение Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса “Безопасный город”». Доступ из справочной правовой системы «КонсультантПлюс».

– выход из строя кондиционера во многих случаях влечет за собой выход из строя оборудования, чувствительного к температурному режиму, например оборудования локального центра обработки данных. Стоимость ущерба от повреждения оборудования иногда составляет несколько миллионов рублей, цена простоя в некоторых случаях достигает сотен тысяч рублей в час, а ценность информации, потерянной в результате сбоя, – нескольких десятков миллионов рублей;

– некорректные данные (ошибочные или искаженные), снимаемые с датчиков, приводят к повышенной нагрузке на оборудование и его преждевременному выходу из строя;

– из-за атак на датчики вынужденно срабатывают системы оповещения о пожаре, критичном превышении нормы вредных веществ в воздухе, что вызывает запуск сигналов к эвакуации, панику, которая может сопровождаться нанесением урона здоровью;

– переход на цифровые датчики потребления создает риски сетевых атак, предпринимаемых для подмены информации, передаваемой счетчиком, когда вместо оригинального счетчика на цифровом хабе – точке сбора информации – авторизуется виртуальный двойник реального, передающий заниженные показатели, а реальный счетчик оказывается в зоне радиоизоляции;

– отказ от физического сервисного контроля также несет в себе определенные риски – датчики IoT передают только то, что они в состоянии измерить, то, для чего они предназначены, и то, что контролировалось визуально. Например, деградация крепления вентилятора к потолку не может контролироваться электроникой вентилятора, что вызывает риски при эксплуатации;

– при создании единой IT-инфраструктуры ЖКХ возникают риски атаки в целях изменения записей о потреблении. С точки зрения одного жильца такая атака слишком сложна и затратна, но для нарушителя – оптового потребителя, например домоуправляющей компании, подобная атака на поставщика может иметь финансовое обоснование;

– в случае использования технологии блокчейн при домовом голосовании возможности тех, кто не имеет доступа к цифровым средствам, будут ограничены, что обоснованно лишит их права голосовать. И встанет вопрос о проведении всех видов голосования, при которых условий для подмены результатов голосования, например на этапе их ручного занесения в блокчейн, станет только больше.

Риски и уголовное право: в порядке обсуждения проблемы

Цифровая трансформация – главный тренд в государственной и корпоративной деятельности – меняет способ ведения бизнеса и государственного управления. Сейчас существует больше потенциальных киберугроз, чем когда-либо прежде, а атаки становятся все более инновационными. Защита от этих угроз требует как постоянно интегриру-

емого и автоматизируемого подхода к кибербезопасности, так и адаптации законодательства к таким угрозам. Подготовка нормативных правовых актов, регулирующих вопросы цифровизации в определенной сфере (медицина, персональные данные, экономика, логистика, жилищно-коммунальные услуги и др.), должна сопровождаться оценкой возможных рисков с целью безотлагательной разработки (корректировки) уголовно-правовых норм, охраняющих соответствующие общественные отношения.

Отечественное уголовное законодательство разделяет преступления в сфере компьютерной информации (глава 28 УК РФ) и иные деяния, в которых под угрозу ставится информационная безопасность (в таких составах преступлений деяние характеризуется как разглашение, распространение, незаконное изготовление, незаконный оборот и т. д.), либо указывается на используемое средство – сеть Интернет. Такой подход обусловлен тем, что информация становится не только целью преступных посягательств, но и средством их совершения. Выбранный законодателем путь конструирования составов преступлений, направленных на противодействие преступлениям в информационной сфере, всегда будет запаздывать, страдать пробельностью и неспособностью охватить все возможные общественно опасные деяния и их последствия. Ускоренное создание «цифровых двойников» человека, предприятий, жилых домов, зданий, а также целых городов требует усиленной правовой защиты, одним из аспектов которой может выступить формирование новой главы Уголовного кодекса Российской Федерации (УК РФ), посвященной информационной безопасности. Содержание такой главы может объединить так называемые компьютерные преступления и иные деяния, связанные с незаконным использованием информации, сопровождающиеся причинением материального ущерба, вреда здоровью и жизни. Тем самым будет осуществлена консолидация правовых инструментов для противодействия преступлениям, совершаемым с помощью информационных технологий, с целью конкретизации существующей угрозы и выработки соответствующих способов их предупреждения, а судебная практика приобретет единство и системность.

Так, из всего спектра нелегального оборота запрещенных предметов в сети Интернет законодатель выделил лишь незаконный сбыт наркотиков, который квалифицируется по п. «б» ч. 2 ст. 228[1] УК РФ, в то же время оставив за пределами этой нормы такие деяния, как пропаганда либо реклама наркотических средств, совершенные с использованием информационно-телекоммуникационных сетей (сети Интернет)[7].

---

[7] См.: Проект федерального закона № 108866-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в части усиления ответственности за незаконные пропаганду и рекламу наркотических средств и психотропных веществ». Доступ из справочной правовой системы «КонсультантПлюс».

Непоследовательность очевидна и в ситуации, когда не проводится усиления ответственности за распространение оружия и торговлю людьми, совершаемые посредством сети Интернет. Соответствующих квалифицированных составов преступлений в УК РФ не закреплено, хотя общественная опасность неконтролируемого рынка оружия, а тем более площадок для купли-продажи человека не подлежит сомнению. Вероятно, следует воспринять иной подход, согласно которому может быть криминализирована сама деятельность криптомаркетов, являющихся анонимными платформами для торговли незаконными товарами и услугами, с привлечением к ответственности разработчиков и администраторов таких ресурсов.

Другой сложностью при противодействии преступлениям, связанным с электронной коммерцией, является использование криптовалюты. Основная проблема заключается в господствующем в юридическом сообществе мнении относительно того, что криптовалюта с точки зрения национального права России вообще не является объектом гражданских прав [Ализаде, В.А. и Волеводз, А.Г., 2017, с. 282]. Такой же взгляд на криптовалюту характерен для судебной практики, зачастую не рассматривающей виртуальную валюту в качестве предмета преступления. Исключением пока является позиция Пленума Верховного Суда Российской Федерации, изложенная в Постановлении от 26 февраля 2019 г. № 1, признавшем предметом преступлений, предусмотренных ст. 174 и 174[1] УК РФ, денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления[8]. Однако такое разъяснение применимо лишь к указанной категории дел и не может быть истолковано расширительно.

Односторонней представляется позиция законодателя по вопросу охраны персональных или идентифицирующих физических и юридических лиц данных, весьма широко используемых для противоправных действий: доступ к банковским счетам и картам, фотографиям и контактам, переписке, коммерческой тайне и др. В настоящее время криминализировано лишь хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (ст. 159[6] УК РФ). Количество преступлений, квалифицируе-

[8] См.: Постановление Пленума Верховного Суда Российской Федерации от 26 февраля 2019 г. № 1 «О внесении изменений в Постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 “О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем”» (п. 2). Доступ из справочной правовой системы «КонсультантПлюс».

мых по данной статье, весьма значительно и обусловлено распространенностью таких деяний, связанной с низкой грамотностью населения при использовании цифровых банковских сервисов. В случаях, когда хищение осуществлено не путем обмана, а посредством получения доступа к персональным данным, например через приложение «мобильный банк», содеянное квалифицируется как простая кража [Бархатова, Е.Н., 2016], поскольку специальный состав или квалифицирующий признак законодателем не закреплен.

Установив ответственность за мошенничество в сфере компьютерной информации, законодатель также не закрепил аналогичной нормы (например, ст. 165[1] УК РФ), предусматривающей причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием при отсутствии признаков хищения с использованием информационных технологий, которое может получить распространение в сфере жилищно-коммунального хозяйства, когда собственники жилья или управляющие компании искажают информацию, поступающую с датчиков или приборов, об использовании соответствующих ресурсов.

Отсутствуют уголовно-правовые средства реагирования и в случаях цифровизации медицинской деятельности и управления беспилотными транспортными средствами. Существующий законодательный подход определяет, что ответственность за причинение вреда несет лицо, принимающее решение: врач за преступления против жизни и здоровья, водитель за транспортное преступление. Справедливость такого подхода вызывает сомнение, когда вред причиняется в условиях автоматизации диагностирования и проведения операции, а также движения транспортного средства. Кто должен нести ответственность за причинение вреда здоровью и жизни: разработчик программного обеспечения; лицо, осуществившее незаконный доступ к соответствующей информационной системе; эксплуатант оборудования и (или) транспортного средства? Ответа на подобные вопросы нет ни в главе о преступлениях против безопасности движения и эксплуатации транспорта, ни в главе о преступлениях против жизни и здоровья.

Таким образом, цифровизация многих сфер жизнедеятельности как сопровождается положительным эффектом, так и несет новые угрозы и риски, не получающие отражения в уголовном законодательстве. В подобной ситуации требуются пересмотр уголовно-правовой политики и выработка унифицированного подхода.

Благодарности:

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 18-29-16158 и № 18-29-16162.

Список использованной литературы

Абдюшева Д.Р., Меренков А.О., Степанов А.А. Условия построения маркетинговой системы «цифрового» транспорта и логистики в управлении конкурентоспособностью // Управление. 2018. Т. 3, № 21. С. 60–65.

Aktas E., Meng Y. An Exploration of Big Data Practices in Retail Sector // Logistics. 2017. № 1.

Ализаде В.А., Волеводз А.Г. Судебная практика по делам о преступлениях преступных сообществ (преступных организаций) в сфере незаконного оборота наркотиков, совершенных с использованием информационно-телекоммуникационной сети Интернет и криптовалюты // Библиотека криминалиста. 2017. № 6 (35). С. 281–299.

Alshahrani W. The Role of Digital Medicine on the Improvement of the Healthcare beyond the Hospitals // Health Science Journal. 2018. Vol. 12, № 2.

Asplin T. Going digital: Legal issues for e-commerce, software and the internet // International Journal of Law and Information Technology. 2002. Vol. 10, issue 1. P. 135–138.

Афонасков О.В., Левин В.И., Толстихина А.А., Нугаева Н.Р. Цифровая медицина. Организация автоматизированного рабочего места врача функциональной диагностики в стационаре // Медицинский алфавит. 2018. Т. 2, № 23. С. 29–32

Бархатова Е.Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. 2016. № 9. С. 110–115.

Beurskens F. The Economics of Dot.coms and E-commerce in the Agrifood Sector // Applied Economic Perspectives and Policy. 2003. Vol. 25, issue 1. P. 22–25.

Brown B., Hannan A. The future is already here // BMJ: British Medical Journal. 2011. Vol. 342, № 7805. P. 993.

Бубнова Г.В., Левин Б.А. Цифровая логистика – инновационный механизм развития и эффективного функционирования транспортно-логистических систем и комплексов // International Journal of Open Information Technologies. 2017. Т. 5, № 3. С. 72–78.

Букалерова Л.А. Информационные преступления в сфере государственного и муниципального управления. М. : РПА Минюста России, 2009.

Волынсков В.Э. «Большие данные» – путь к «умным» городам // Градостроительство. 2018. № 5 (57). С. 63–66.

Voss G., Woodcock W., Dumont K., Wells D., Exor I.J., Traça J.L., Embry B., Khan F. Privacy, E-Commerce, and Data Security // The International Lawyer. 2012. Vol. 46, no 1. P. 97–112.

Голенкова А.А., Шагбазян С.И, Степанова Н.Р. Будущее за умными городами // Современные тенденции развития науки и технологий. 2017. № 1, ч. 8. С. 6–8.

Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет : моногр. М. : Акад. Ген. прокуратуры Рос. Федерации, 2015.

Дмитриев А.В. Цифровые технологии в транспортной логистике // РИСК: Ресурсы, Информация, Снабжение, Конкуренция. 2017. № 4. С. 14–18.

Кантемирова М.А., Аликова З.Р. Цифровая экономика: развитие процессов цифровизации медицины в регионе // Вестник Северо-Осетинского государственного университета имени К.Л. Хетагурова. 2019. № 1. С. 92–95.

Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства) : моногр. / под ред. А.В. Наумова. М. : Юрлитинформ, 2015. 224 с.

Kohl S.E., Van Tilburg C., Flaherty G.T. Changing landscape of digital communication in travel medicine // Journal of Travel Medicine Journal of Travel Medicine. 2019. Vol. 26, issue 1. P. 145.

Косынкин А.А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации : моногр. / под ред. Н.А. Подольного. М. : Юрлитинформ, 2013. 213 с.

Lianguang C., Shong-Iee I.Su, Hertz S. Logistics Innovation in China // Transportation Journal. 2012. Vol. 51, no 1. P. 98–117.

Meijer A. Datapolis: A Public Governance Perspective on “Smart Cities” // Perspectives on Public Management and Governance Perspectives on Public Management and Governance. 2018. Vol. 1, issue 3. P. 195–206.

Нугаев Ш.Р. Проблемы правового регулирования электронной коммерции: доктринальные аспекты // Российский юридический журнал. 2010. № 2. С. 182–186.

Овчинский В.С. Криминология цифрового мира : учебник для магистратуры. М. : Норма : Инфра-М, 2018. 352 с.

Pagan J. Smart Cities: The Next Frontier // US Black Engineer and Information Technology. 2018. Vol. 42, № 1. P. 78–80.

Paton D.S., Siegel D., Williams L.V. A Policy Response to the E-Commerce Revolution: The Case of Betting Taxation in the UK // The Economic Journal. 2002. Vol. 112, issue 480. P. F296–F314.

Рассолов И.М. Право и Интернет: теоретические проблемы. М. : Норма, 2003. 336 с

Романова И. Медицина будущего – цифровая медицина : по материалам конференции «Здравоохранение и технологии 2012» // Электроника. Наука, Технология, Бизнес. 2013. № 1 (123). С. 106–110.

Сапир Ж. От регионоведения к «умным городам»: интеллектуальное наследие и возможные проблемы // Экономические и социальные перемены: факты, тенденции, прогноз. 2018. Т. 11, № 3. С. 25–40.

Соловьев В.С. Криминогенный потенциал социального сегмента сети Интернет : моногр. М. : Юрлитинформ, 2017. 176 с.

Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М. : Статут, 2016. 190 с.

Tavazzi L. Big data: is clinical practice changing? // European Heart Journal Supplements. 2019. Vol. 21, issue Supplement_B. P. B98–B102.

Тедеев А.А. Налогово-правовое регулирование электронной экономической деятельности: проблемы терминологии // Законодательство и экономика. 2002. № 2. С. 21–25.

Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : моногр. Владивосток : Изд-во Дальневост. ун-та, 2009. 240 с.

Francisco K., Swanson D. The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency // Logistics. 2018. № 2.

Шамраев А.В. Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. М. : Статут, 2003.

References

Abdyusheva, D.R., Merenkov, A.O. and Stepanov, A.A., 2018. Conditions for building a marketing system of “digital” transport and logistics in the management of competitiveness. *Upravlenie* = [Management], 6(3), pp. 60–65. (In Russ.)

Aktas, E. and Meng, Y., 2017. An Exploration of Big Data Practices in Retail Sector. *Logistics*, 1. (In Eng.)

Alizade, V.A. and Volevodz, A.G., 2017. The court practice on Affairs about crimes of criminal associations (criminal organizations) in the

field of illicit drug trafficking committed with the use of information and telecommunication Internet network and cryptocurrency. *Biblioteka kriminalista* = [Forensic Library], 6(35), p. 282. (In Russ.)

Alshahrani, W., 2018. The Role of Digital Medicine on the Improvement of the Healthcare beyond the Hospitals. *Health Science Journal*, 12(2). (In Eng.)

Asplin, T., 2002. Going digital: Legal issues for e-commerce, software and the internet. *International Journal of Law and Information Technology*, 10(1), pp. 135–138. (In Eng.)

Afonaskov, O.V., Levin, V.I., Tolstikhina, A.A. and Nugaeva, N.R., 2018. Digital medicine. Organization of a hospital functional diagnostician's automated workplace. *Medicinskij alfavit* = [Medical Alphabet], 2(23), pp. 29–32. (In Russ.)

Barkhatova, E.N., 2016. Features of Qualification of Fraud in the Field of Computer Information and Distinction with Other Criminal Offences. *Sovremennoe pravo* = [Modern Law], 9, p. 110–115. (In Russ.)

Beurskens, F., 2003. The Economics of Dot.coms and E-commerce in the Agrifood Sector. *Applied Economic Perspectives and Policy*, 25(1), pp. 22–25. (In Eng.)

Brown, B. and Hannan, A., 2011. The future is already here, *BMJ: British Medical Journal*, 342(7805), p. 993. (In Eng.)

Bubnova, G.V. and Levin, B.A., 2017. Digital logistics is an innovative mechanism for the development and effective functioning of transport and logistics systems and complexes, *International Journal of Open Information Technologies,* 5(3), pp. 72–78. (In Russ.)

Bukalerova, L.A., 2009. *Informatsionnye prestupleniya v sfere gosudarstvennogo i munitsipal'nogo pravleniya* = [Information crimes in the sphere of state and municipal administration]. Moscow: RPA Minjusta Rossii. (In Russ.)

Dmitriev, A.V., 2017. Digital technologies in transport logistics. *RISK: Resursy, Informaciya, Snabzhenie, Konkurenciya* = [RISC: Resources, Information, Supply, Competition], 4, pp. 14–18. (In Russ.)

Francisco, K. and Swanson, D., 2018. The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. *Logistics*, 2. (In Eng.)

Golenkova, A.A., Shagbazyan, S.I. and Stepanova, N.R., 2017. Smart cities are the future. *Sovremennye tendencii razvitiya nauki i tekhnologij* = [Current Trends in Science and Technology], 1(8), pp. 6–8. (In Russ.)

Guzeeva, O.S., 2015. *Prestupleniya, sovershaemye v rossijskom segmente seti Internet* = [Crimes committed in the Russian segment of the

Internet]. Monograph. Moscow: Akad. Gen. prokuratury Ros. Federatsii. (In Russ.)

Kantemirova, M.A. and Alikova, Z.R., 2019. Digital economy: development of digitalization of medicine in the region. *Vestnik Severo-Osetinskogo gosudarstvennogo universiteta imeni K.L. Hetagurova* = [Bulletin of K.L. Hetagurov North Ossetian State University], 1, pp. 92–95. (In Russ.)

Kohl, S.E., van Tilburg, C. and Flaherty, G.T., 2019. Changing landscape of digital communication in travel medicine. *Journal of Travel Medicine Journal of Travel Medicine*, 26(1), p. 145. (In Eng.)

Kosynkin, A.A., 2013, *Preodolenie protivodejstviya rassledovaniyu prestuplenij v sfere komp'yuternoj informacii* = [Overcoming of counteraction to investigation of crimes in the sphere of computer information]. Monograph. N.A. Podol'nyy, ed. Moscow: Yurlitinform. (In Russ.)

Kozaev, N.S., 2015. *Sovremennye tekhnologii i problemy ugolovnogo prava (analiz zarubezhnogo i rossijskogo zakonodatel'stva)* = [Modern technologies and problems of criminal law (analysis of foreign and Russian legislation)]. Monograph. A.V. Naumov, ed. Moscow: Yurlitinform. (In Russ.)

Lianguang, C., Shong-Iee, I.S, Hertz, S. 2012. Logistics Innovation in China. *Transportation Journal*, 51(1), pp. 98–117. (In Eng.)

Meijer, A., 2018, Datapolis: A Public Governance Perspective on "Smart Cities". *Perspectives on Public Management and Governance Perspectives on Public Management and Governance*, 1(3), pp. 195–206. (In Eng.)

Nugaev, Sh.R., 2010. Problems of legal regulation of e-Commerce: doctrinal aspects. *Rossiyskiy yuridicheskiy zhurnal* = [Russian Law Journal], 2, pp. 182–186. (In Russ.)

Ovchinskiy, V.S., 2018. *Kriminologiya cifrovogo mira* = [Criminology of the digital world]. Textbook for magistracy. Moscow: Norma. (In Russ.)

Pagan, J., 2018. Smart Cities: The Next Frontier. *US Black Engineer and Information Technology*, 42(1), pp. 78–80. (In Eng.)

Paton, D., Siegel, D.S. and Williams, L.V., 2002. A Policy Response to the E-Commerce Revolution: The Case of Betting Taxation in the UK. *The Economic Journal*, 112(480), pp. F296–F314. (In Eng.)

Rassolov, I.M., 2003. *Pravo i Internet. Teoreticheskie problemy* = [Law and Internet. Theoretical problem]. Moscow: Norma. (In Russ.)

Romanova, I., 2013. The medicine of the future is digital medicine. Based on the conference "Health and technology 2012". *Elektronika. Nauka, Tekhnologiya, Biznes* = [Electronics. Science, Technology, Business], 1(123), pp. 106–110. (In Russ.)

Sapir, Zh., 2018. From regional studies to “smart cities”: intellectual heritage and possible problems. *Ekonomicheskie i social’nye peremeny: fakty, tendencii, prognoz* = [Economic and Social Change: Facts, Trends, Forecast], 11(3), pp. 25–40. (In Russ.)

Shamraev, A.V., 2003. *Pravovoe regulirovanie informatsionnykh tekhnologiy (analiz problem i osnovnye dokumenty). Versiya 1.0* = [Legal regulation of information technologies (problem analysis and basic documents). Version 1.0]. Moscow: Statut. (In Russ.)

Solov’ev, V.S., 2017. *Kriminogennyy potentsial sotsial’nogo segmenta seti Internet* [Criminogenic potential of the social segment of the Internet]. Moscow: Yurlitinform. (In Russ.)

Stepanov-Egiyants, V.G., 2016. *Otvetstvennost’ za prestupleniya protiv komp’yuternoy informatsii po ugolovnomu zakonodatel’stvu Rossiyskoy Federatsii* = [Responsibility for crimes against computer information under the criminal legislation of the Russian Federation]. Moscow: Statut. (In Russ.)

Tavazzi, L., 2019. Big data: is clinical practice changing? *European Heart Journal Supplements*, 21(Supplement_B), pp. B98–B102. (In Eng.)

Tedeev, A.A., 2002. Tax and legal regulation of electronic economic activity: problems of terminology. *Zakonodatel’stvo i ekonomika* = [Legislation and Economics], 2, pp. 21–25. (In Russ.)

Tropina, T.L., 2009. *Kiberprestupnost’: ponyatie, sostoyanie, ugolovno-pravovye mery bor’by* = [Cybercrime: concept, state, criminal-legal measures of struggle]. Monograph. Vladivostok : Izd-vo Dal’nevost. un-ta. (In Russ.)

Volynskov, V.E., 2018. Big data-the way to smart cities. *Gradostroitel’stvo* = [City Building], 5(57), pp. 63–66. (In Russ.)

Voss, G., Woodcock, W., Dumont, K., Wells, D., Exor, I.J., Traça, J.L., Embry, B. and Khan F., 2012. Privacy, E-Commerce, and Data Security. *The International Lawyer*, 46(1), pp. 97–112. (In Eng.)

Информация об авторах / Information about the authors:

Чучаев Александр Иванович, профессор кафедры уголовного права Крымского филиала ФГБОУВО «Российский государственный университет правосудия» (295006, Россия, г. Симферополь, ул. Павленко, д. 5) доктор юридических наук, профессор [**Alexandr I. Chuchaev**, Professor of Criminal Law Department, Crimean Branch, Russian State University of Justice (5 Pavlenko St., Simferopol, 295006, Russia), Dr. Sci. (Law), Professor]. E-mail: moksha1@rambler.ru

Грачева Юлия Викторовна, профессор кафедры уголовного права ФГБОУ ВО «Московский государственный юридический университет

имени О.Е. Кутафина (МГЮА)» (125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9), доктор юридических наук, профессор [**Yulia V. Gracheva**, Professor of Criminal Law Department, Kutafin Moscow State Law University (9 Sadovaya-Kudrunskaya St., Moscow, 125993, Russia), Dr. Sci. (Law), Professor]. E-mail: uvgracheva@mail.ru

Маликов Сергей Владимирович, старший преподаватель кафедры уголовного права ФГБОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)» (125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9), кандидат юридических наук [**Sergey V. Malikov**, Senior Lecturer of Criminal Law Department, O.E. Kutafin Moscow State Law University (9 Sadovaya-Kudrunskaya St., Moscow, 125993, Russia), Cand. Sci. (Law)]. E-mail: s.v.malikov@yandex.ru.

Заявленный вклад авторов:

Чучаев Александр Иванович – обзор литературы по исследуемой проблеме; научное руководство.
Грачева Юлия Викторовна – сбор и систематизация данных; анализ и обобщение результатов исследования.
Маликов Сергей Владимирович – сбор и систематизация данных; анализ и обобщение результатов исследования.