

СОВЕРШЕНСТВОВАНИЕ ЗАКОНОДАТЕЛЬСТВА NOVUS LEX

DOI: 10.17803/1729-5920.2020.158.1.145-159

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

Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения¹

Аннотация. Противодействие киберугрозам ставит новые задачи перед специалистами по информационной безопасности, требует выработки механизмов правовой защиты, которые позволят с опережением реагировать на криминогенные угрозы в цифровой среде. Выбранный отечественным законодателем путь противодействия преступлениям в информационной сфере страдает запаздыванием, пробельностью и неспособностью охватить все возможные общественно опасные деяния и их последствия. В статье проводится анализ сфер жизнедеятельности, на которые инновационные технологии воздействуют или будут оказывать наибольшее влияние, тем самым преследуется пропедевтическая цель — создание необходимого теоретического фундамента для последующего рассмотрения специальных уголовно-правовых вопросов. К таким сферам отнесены: социальные сети, электронная коммерция, цифровая медицина, экономика совместного потребления, Индустрия 4.0.

Авторы приходят к выводу, что цифровизация многих сфер жизнедеятельности сопровождается положительным эффектом, но и несет новые угрозы и риски, не получающие отражения в уголовном законода-

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16158.

© Грачева Ю. В., Коробеев А. И., Маликов С. В., Чучаев А. И., 2020

* *Грачева Юлия Викторовна*, доктор юридических наук, профессор, профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
uvgracheva@mail.ru

** *Коробеев Александр Иванович*, доктор юридических наук, профессор, заведующий кафедрой уголовного права и криминологии Дальневосточного федерального университета, заслуженный деятель науки Российской Федерации
Ул. Суханова, д. 8, г. Владивосток, Россия, 690091
korobeev.ai@dvfu.ru

*** *Маликов Сергей Владимирович*, кандидат юридических наук, старший преподаватель кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
s.v.malikov@yandex.ru

**** *Чучаев Александр Иванович*, доктор юридических наук, профессор, профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
moksha1@rambler.ru

тельстве. В подобной ситуации требуется пересмотр уголовно-правовой политики и выработка унифицированного подхода.

Ключевые слова: социальные сети, электронная коммерция, цифровая медицина, экономика, совместное потребление, Индустрия 4.0, риски цифровизации, противодействие преступности.

Для цитирования: Грачева Ю. В., Коробеев А. И., Маликов С. В., Чучаев А. И. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения // Lex russica. — 2020. — Т. 73. — № 1. — С. 145—159. — DOI: 10.17803/1729-5920.2020.158.1.145-159.

Criminal and Legal Risks in the Field of Digital Technologies: Problems and Suggestions²

Yuliya V. Gracheva, Dr. Sci. (Law), Professor, Professor of the Department of Criminal Law at Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
uvgracheva@mail.ru

Aleksandr I. Korobeev, Dr. Sci. (Law), Professor, Head of the Department of Criminal Law and Criminology at the Far Eastern Federal University, Honored Worker of Science of the Russian Federation
ul. Sukhanova, d. 8, Vladivostok, Russia, 690091
korobeev.ai@dvfu.ru

Sergey V. Malikov, Cand. Sci. (Law), Senior Lecturer of the Department of Criminal Law at Kutafin Moscow State University of Law (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
s.v.malikov@yandex.ru

Aleksandr I. Chuchaev, Dr. Sci. (Law), Professor, Professor of the Department of Criminal Law at Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
moksha1@rambler.ru

Abstract. Countering cyber threats poses new challenges for information security specialists, and requires developing legal protection mechanisms that will allow them to respond to criminal threats in the digital environment ahead of time. The path chosen by the national legislator to counteract crimes in the information sphere suffers from a delay, a gap and an inability to cover all possible socially dangerous acts and their consequences. The paper analyzes the spheres of life that innovative technologies affect or will have the greatest impact on, thus pursuing a propaedeutic goal — creating the necessary theoretical foundation for further consideration of special criminal law issues. These areas include social networks, e-commerce, digital medicine, sharing economy, industry 4.0.

The authors conclude that the digitalization of many spheres of life is accompanied by a positive effect, but also carries new threats and risks that are not reflected in criminal legislation. In such a situation, it is necessary to review the criminal law policy and develop a unified approach.

Keywords: social networks, e-commerce, digital medicine, economy, shared consumption, industry 4.0, risks of digitalization, crime prevention.

Cite as: Gracheva YuV, Korobeev AI, Malikov SV, Chuchaev AI. Uголовно-правовые риски в сфере tsifrovyykh tekhnologiy: problemy i predlozheniya [Criminal and legal risks in the field of digital technologies: Problems and suggestions]. *Lex russica*. 2020;73(1):145-159. (In Russ.). DOI: 10.17803/1729-5920.2020.158.1.145-159.

² The reported study was funded by RFBR according to the research project No. 18-29-16158.

Введение

Увеличение активности в киберпространстве, цифровая трансформация предпринимательской деятельности, деятельности государственных и муниципальных служб определяют актуальность рассмотрения вопроса модификации права в условиях развития цифровых технологий. Прорывное развитие цифровых технологий приводит к появлению новых видов нематериальных и трансформации традиционных материальных активов, образованию важных прямых и обратных зависимостей между объектами виртуального (киберпространства) и реального мира. Значимость преобразований и их беспрецедентная динамика изменяют характер угроз собственности, жизни и здоровью человека, функционированию организаций, социума и государства.

Угрозы цифровой среды, создающие опасность для личности, общества и государства, исследуются как совокупность причин и факторов, обусловленных применением цифровой технологии, от которой зависит вероятность нанесения ущерба, и сферы жизнедеятельности, определяющей характер и размер ущерба.

Внимание отечественных ученых акцентировано главным образом на так называемых компьютерных преступлениях, или защите информации, что обусловлено существующей структурой уголовного законодательства, обособившего преступления в сфере компьютерной информации и включающего соответствующие квалифицирующие признаки в отдельные составы преступлений³. Иной взгляд характерен для криминологических исследований, однако работ в этой области немного⁴.

Предметом изучения данной статьи 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.

Медиа- и социальные сети

Социальная сеть — это среда взаимодействия при помощи Интернета, в которой пользователи общаются, создают группы, сообщества и коллективы, обмениваются информацией, идеями, сообщениями и другим контентом. Главное отличие социальных сетей от классических сайтов и интернет-дневников заключается в том, что они формируются благодаря контенту, который создают сами пользователи сети. На персональных, корпоративных или новостных сайтах только ограниченный круг людей может публиковать информацию, для них существуют значительные ограничения на типы загружаемой информации. Социальная сеть предоставляет возможность публикации всем участникам⁵.

К указанным сетям относятся IT-сервисы:

- WhatsApp и Viber — приложения для обмена сообщениями;
- Facebook и LinkedIn — платформы на основе информации об участниках;
- видеопорталы (например, YouTube);
- почтовые клиенты (например, GMail) и др.

Онлайн-форумы — это сайты, предназначенные для создания пользователями тем в целях их последующего обсуждения посредством

³ См.: Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М., 2016 ; Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий. М., 2019 ; Гайфутдинов Р. Р. Квалификация преступлений против безопасности компьютерной информации. М., 2019 ; Долгополов К. А. Особенности квалификации и расследования преступлений в сфере компьютерной информации. Ростов н/Д, 2018 ; Мазуров В. А. Преступления в сфере компьютерной информации. Барнаул, 2018.

⁴ См.: Евдокимов К. Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты. Иркутск, 2016 ; Быков В. М. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы. М., 2015 ; Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет. М., 2015 ; Овчинский В. С. Криминология цифрового мира. М., 2018 ; Соловьев В. С. Криминогенный потенциал социальной сети Интернет. М., 2017.

⁵ См.: Монахов В. Н. Социальные сети как объект регулирования. М., 2012 ; Молотников А. Е., Архипов Е. В. Социальные сети и компании-агрегаторы: правовые аспекты деятельности // Предпринимательское право. 2017. № 4. С. 38—47.

размещения сообщений внутри этих тем. Форумы сыграли большую роль в развитии социальных сетей и идеи BBS — электронных досок объявлений, популярных в 1970—1980-х гг. Но, в отличие от BBS, форумы получили удобный интерфейс, что облегчило их использование посетителями без технических навыков. Для создания собственных форумов разработаны разнообразные технологические платформы, например vBulletin и phpBB. Эти платформы до настоящего времени используются владельцами форумов и технически поддерживаются разработчиками. Форумы остаются популярной частью онлайн-культуры.

Сайты знакомств некоторые считают первыми социальными сетями, которые возникли практически одновременно с появлением широкого доступа к Интернету. Они давали возможность пользователям создавать профили (обычно с фотографиями) и связываться друг с другом. Сайты знакомств редко позволяли вести список друзей. Даже, например, один из старейших сайтов Classmates.com в первые годы своего существования не имел такой функции. Полноценными социальными сетями сайты знакомств не являлись. В связи с популярностью соцсетей многие корпорации разных отраслей стали создавать нишевые социальные сети, посвященные своей продукции и образу жизни, который их продукция поддерживает (например, Under Armour).

Социальные медиа не ограничиваются только социальными сетями. Обмен фотографиями, видео и другим мультимедийным контентом также популярен в Интернете. Например, YouTube был запущен в 2005 г. и стал первым крупным сайтом видеохостинга. Пользователи могут загружать видео продолжительностью до 10 минут, делиться ими через YouTube или встраивая их в другие веб-сайты (социальные сети, блоги, форумы и т.п.). В настоящее время на YouTube пользователи могут загружать HD-видео высокого качества. Кроме того, YouTube запустил службу, которая предоставляет телевизионные шоу и фильмы по лицензии от их правообладателей. Основные социальные функции YouTube включают в себя составление рейтингов, комментариев и предоставление подписки на любимые видеоканалы пользователей.

С появлением Twitter в 2006 г. мгновенные обновления статуса (связанные с появлением нового контента) стали новой нормой в социальных сетях. В настоящее время практически

все крупные социальные сети без задержек публикуют обновления в режиме реального времени. Twitter приобрел большую популярность во время конференции SxSW (South by Southwest), поскольку привлек культовую аудиторию и имеет ряд известных пользователей, включая президента США. Twitter также породил ряд сторонних сайтов и приложений, превратившись в платформу для многих сервисов: программы-клиенты Twitter для обновления и управления подписчиками; сервисы, которые отслеживают тенденции в Twitter; сервисы для размещения фотографий и видео прямо в Twitter.

Заполнение профилей социальных сетей, фиксация своей ежедневной активности, убеждений, расовой принадлежности (легко определяемой по фотографии), физического состояния сопряжены с рядом рисков. Последствиями для пользователей социальных сетей могут стать следующие ситуации:

- 1) преследование стalkerами — лицами, которые выбирают в социальной сети жертву; по записям, фотографиям, геолокации определяют часто посещаемые ею места и любимые маршруты и преследуют жертву, чтобы запугать, или проявляют сексуальную агрессию, выплескивают расовую либо политическую ненависть. Facebook и другие сайты социальных сетей часто критиковали за то, что навязчивым преследователям стало легче отслеживать жертв и находить новых. Такое обвинение не является полностью необоснованным, поскольку многие не пользуются настройками конфиденциальности и оставляют свои профили общедоступными;
- 2) использование лицами с психическими отклонениями социальных сетей для знакомств с детьми или подростками и анонимного назначения встреч с ними. Компания MySpace предприняла важный шаг, чтобы запретить незнакомым взрослым дружить с несовершеннолетними. Сети в настоящее время также требуют, чтобы профили подростков в возрасте до 16 лет были закрытыми по умолчанию и другим пользователям не разрешалось их просматривать;
- 3) выявление в социальных сетях физически слабых, тяжело больных людей в целях грабежа, вымогательства, мошенничества;
- 4) определение по геолокации и фотографиям отсутствия хозяев дома, коттеджа, квартиры в целях кражи автомобиля или взлома квартиры, дачи;

- 5) использование лицами, ведущими работу над популяризацией своей личности в медийном пространстве, социального капитала для побуждения к физическому насилию, проведения атак на репутацию в отношении как физических лиц, так и компаний, брендов;
- 6) использование социального капитала и согласованная деятельность оплачиваемых сотрудников для формирования общественного мнения, а также негативного образа физических лиц, политических деятелей, компаний посредством распространения клеветы;
- 7) использование социальных сетей как главного инструмента для призыва к бойкотированию продуктов и компаний по политическим мотивам или другим убеждениям (экология, вегетарианство). Такие бойкоты наносят серьезный финансовый ущерб производителям;
- 8) получение заполненных тестов, сведений об участии в конкурсах, фотографий, персональных данных для прогнозирования поведения человека. При помощи современных технологий по совокупности таких данных легко не просто сегментировать покупателей, но и составлять весьма точные заключения о наличии определенных заболеваний. Сопоставление сведений из социальной сети об активности делает человека подверженным манипуляциям, в частности вымогательству;
- 9) пропаганда применения сквозного метода авторизации Single Sign On — пользователь социальной сети, например Facebook, для доступа на другие сайты задействует логин и пароль Facebook. Таким образом, утечка данных авторизации на одном не очень надежном сайте приведет к компрометации данных доступа ко всем интернет-ресурсам. Ими могут быть интернет-магазины, маркетплейсы с сопоставленными им банковскими картами. Те же самые логин и пароль зачастую используются для доступа к интернет-банкам. Даже если у банка есть до-

полнительная защита СМС-кодом, это преодолимая сложность: данные мобильной связи не шифруются и СМС-код может быть перехвачен злоумышленниками.

Цифровая медицина

Развитие цифровых технологий существенно 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 людей⁶.

Самое значительное влияние цифровизация оказала:

- на диагностику, повысив 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, разраба-

⁶ См.: Информационные технологии в системе здравоохранения (цифровая медицина). Ульяновск, 2018 ; Карпов О. Э., Субботин С. А., Шишканов Д. В., Замятин М. Н. Цифровое здравоохранение. Необходимость и предпосылки // Врач и информационные технологии. 2017. № 3. С. 6—22 ; Муслимов М. И. Цифровое здравоохранение как фактор революционных преобразований в отрасли // Современные проблемы здравоохранения и медицинской статистики. 2018. № 3. С. 63—74 ; Морозова Ю. А. Цифровизация как глобальный, страновой и отраслевой процесс в повышении результативности и эффективности здравоохранения и медицины // Интеллект. Инновации. Инвестиции. 2019. № 4. С. 44—53.

тывается ее законодательная база⁷. 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: в традиционной схеме разделения ответственности ошибка — 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. 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. Среди наиболее значимых рисков можно выделить:

- 1) умышленное искажение данных руководством медицинского учреждения, принимаемое для увеличения сумм страховых выплат. В настоящее время в зарубежных странах есть судебная практика, согласно которой для искажения работы диагностического алгоритма врачи меняли пиксели в снимке МРТ. В результате система искусственного интеллекта определяла признаки болезни, которой на самом деле не было;
- 2) 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;
- 3) возрастают риски врачебных ошибок. Некоторые методы машинного обучения подразумевают использование прошлого опыта (ретроспективных данных о лечении и его результатах) для оптимизации алгоритмов и самонастройки. Эти данные актуализируются после принятия системы в эксплуата-

цию; для обучения в системе задействованы данные, которые вносят врачи, работающие в конкретной организации. Если подавляющее большинство специалистов из-за своей низкой квалификации будут вводить в систему некорректные заключения или если данные в систему о результатах лечения будут внесены в искаженном виде, то система с некоторой вероятностью пройдет самообучение и начнет генерировать ошибочные заключения в соответствии с загруженной информацией;

- 4) наиболее распространенным может стать искажение данных о здоровье и доступ к конфиденциальным сведениям о здоровье, что способно спровоцировать:
 - а) вымогательство денежных средств, совершаемое с угрозой уничтожить медицинские данные;
 - б) шантаж пациентов, для которых утечка сведений о здоровье может привести к отказу в принятии на работу, увольнению, семейным конфликтам с финансовыми последствиями;
 - в) мошенничество в отношении психически нездоровых, одиноких пациентов, психологическое давление и принуждение к передаче активов;
 - г) доведение до самоубийства на основе данных о психическом состоянии;
 - д) противоправные действия в отношении имущества пациентов на основе данных об их перемещениях и местонахождении (больница, санаторий).

В результате нарушения целостности и достоверности данных о здоровье может произойти подмена диагностической информации с целью спровоцировать неадекватное лечение и нанести вред здоровью; для признания невменяемости и принудительного назначения опекунов; с целью получать льготы, которые полагаются инвалидам и другим категориям населения.

Нарушение режима доступа к медицинским данным таит опасность причинения вреда здоровью пациента (и может даже создать угрозу жизни) в результате прерывания сеанса удаленной хирургической операции, недоста-

⁷ Федеральный закон от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»; постановление Правительства РФ 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) // СПС «КонсультантПлюс».

точно 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.

Экономика совместного использования

Под экономикой совместного пользования понимается ряд новых типов бизнес-моделей, платформ и бирж. Она основана на предоставлении информации о товарах и об услугах, ее отличительной характеристикой является децентрализованный обмен товарами и услугами, наличие механизмов рыночного самоуправления, акцент не на передаче, а на доступе к ресурсам. Компании, работающие по модели экономики совместного использования, — это организации, являющиеся в первую очередь информационными посредниками при обмене, а не производителями товара или услуги⁸. Сфера экономики совместного использования активно растет, хотя и вызывает много споров. Повторное использование товаров, простой доступ к рынку услуг через платформы услуг, уничтожение цепочек посредников приводят к серьезным финансовым потерям в отраслях, работающих по традиционным бизнес-моделям.

Рассматриваемая экономика основана на распространении возможности пользоваться тем, что принадлежит одному участнику обмена, на других участников. Процессы обмена могут быть дву- и более направленными. Такой сценарий товарообмена становится масштабным явлением, которое уже вовлекло в процесс сотни миллионов людей. За последние годы совместное использование возросло таким образом, что было охарактеризовано экспертами как явление, преобразующее индивидуальное и локальное поведение, способное модифицировать и даже уничтожить некоторые традиционные бизнес-модели. Быстрое его развитие в значительной степени обусловлено беспрецедентной популярностью таких платформ, как Uber и Airbnb, которые на ранних этапах при-

менения рассматривались как сама сущность совместного использования (в какой-то момент смена бизнес-модели на модель совместного использования даже получила название «уберизация»).

Предпосылками к развитию этой модели также стали эволюция информационных технологий и распространение социальных сетей, которые, в свою очередь, послужили основой для одноранговых транзакций (без посредников) и прямой связи между потребителями и производителями. Социальным фактором выступила интенсификация социальных отношений, сосредоточенных на совместном использовании активов или пространства для обеспечения возможности не только потребления, но и производства.

Глобальная предпосылка — чрезмерное потребление как главный виновник серьезных экологических проблем, которые в конечном счете вызывают другие проблемы, в том числе истощение природных ресурсов. Экономика совместного использования проявляется в качестве манифеста гиперпотребления, применяя разрушительные методы сотрудничества потребителей.

Как любая экономическая модель, совместное использование саморегулируется. На ранних этапах развития платформ риск получить в попутчики (или водители) сексуального маньяка был существенным. Однако в результате накопления истории взаимодействия и активного применения рейтинговых систем такой риск практически исчез.

Вероятность получить объект, не соответствующий описанию, или быть принужденным оплачивать ремонт повреждений, которые нанес предыдущий пользователь, безусловно, есть и при современных платформах. Популярность последних, не обеспечивающих безопасное использование разделяемого ресурса, быстро снижается. В настоящее время популярные платформы либо берут риски на себя, организуя страхование или давая гарантии возврата денег, либо в явной форме отказываются от принятия рисков, но при этом компенсируют такой отказ низкой стоимостью сервиса.

⁸ См.: Аюшеева И. З. Особенности гражданско-правового регулирования отношений по предоставлению в пользование недвижимого имущества в условиях развития экономики совместного потребления (sharing economy) // Актуальные проблемы российского права. 2019. № 6. С. 40—48; Галлахер Л. Airbnb. Как три простых парня создали новую модель бизнеса / пер. с англ. Е. Деревянко. М., 2019; Головецкий Н. Я., Гребенюк В. В. Фундаментальные основы экономики совместного потребления // Вестник Московского университета имени С. Ю. Витте. Серия 1: Экономика и управление. 2017. № 4. С. 21—26.

Электронная коммерция

Электронная коммерция — это покупка и продажа товаров или услуг через Интернет, а также передача денежных средств и информации, необходимых для выполнения транзакций. Электронный бизнес относится ко всем аспектам ведения бизнеса в Интернете, тогда как электронная коммерция предполагает транзакции именно товаров и услуг. Проблемы правового регулирования электронной коммерции начали разрабатываться сравнительно недавно в западных странах. Основными проблемами правового регулирования 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 обмена⁹.

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 выбранные товары. Клиенты интернет-магазинов могут сравнивать цены одним щелчком мыши и покупать выбранный 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 и в тех магазинах, которые не могут позволить себе дорогостоящую рекламную кампанию. Благодаря распространению Интернета даже небольшие интернет-магазины выходят на мировые рынки. Кроме того, веб-технологии позволяют отсле-

живать предпочтения клиентов и осуществлять персонализированные маркетинговые инициативы.

Кроме преимуществ перед другими формами торговли, электронная коммерция сопряжена с определенными проблемами.

Во-первых, такая торговля способствует незаконным продажам товаров:

- а) 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, предоставления интимных услуг и т.д.;
- б) оборот виртуальных валют направлен на сокрытие факта и назначения оплаты запрещенного товара.

Во-вторых, 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-третьих, высока вероятность нарушения безопасности:

- а) при оплате товара в электронных магазинах профиль покупателя, содержащий реквизиты и пин-код банковской карты, может быть взломан в целях последующего хищения денежных средств;
- б) взлом вирусом системы «клиент — банк» позволяет скопировать сертификат электронной подписи, при помощи которого формируются распоряжения о переводе денежных средств при оплате товара;
- в) злоумышленник, путем взлома получивший доступ к личному кабинету клиента интернет-магазина, может заказать товар на фальшивый адрес;
- г) имея сведения о покупке некоторых товаров, виновный может пойти на шантаж; в первую очередь это касается данных об определенных видах лекарств.

⁹ См.: Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. М., 2016 ; Тедеев А. А. Электронная коммерция (электронная экономическая деятельность). Правовое регулирование и налогообложение. М., 2002 ; Карев Я. А. Электронные документы и сообщения в коммерческом обороте: правовое регулирование. М., 2006.

Индустрия 4.0

Индустрия 4.0 — это название современных тенденций автоматизации и обработки данных в производственных процессах, которые основаны на применении киберфизических систем, интернета вещей, облачных вычислениях, когнитивных вычислениях и других технологиях. Индустрия 4.0 выводит автоматизацию производственных процессов на новый уровень за счет внедрения гибких персонализированных технологий массового производства¹⁰.

В Индустрии 4.0 машина становится независимой производственной единицей, которая собирает данные, анализирует их, формирует команды и выполняет операции. Машины функционируют преимущественно независимо от человека и взаимодействуют с ним не как с участником производственного процесса, а как с заказчиком. Они имеют способность автоматически формировать производственные процессы, ориентированные на клиента. Постоянно автоматически совершенствуются и в конечном счете должны будут восприниматься людьми как сервис. Эти процессы стали возможными благодаря когнитивным технологиям самоаудита, самооптимизации и самонастройки.

Индустрия 4.0 революционизирует производственные процессы, в связи с чем у трансформировавшихся компаний появляются и преимущества перед другими компаниями, и специфические проблемы.

К числу преимуществ можно отнести:

- 1) оптимизация производства. Умная фабрика, содержащая сотни или даже тысячи интеллектуальных устройств, способных к самооптимизации, приведет к почти нулевому времени простоя производства. Это чрезвычайно важно для отраслей, которые используют дорогостоящее производственное оборудование высокого класса, таких как полупроводниковая промышленность. Постоянное производство без простоев принесет дополнительную прибыль компании. Согласно исследованию, результаты которого опубликованы PriceWaterHouseCoopers, цифровые продукты и услуги обеспечивают примерно 110 млрд евро дополнительных

доходов в год для европейской промышленности;

- 2) новые сегменты и новые рынки. Создание гибкого рынка, ориентированного на клиента, поможет быстро и без проблем удовлетворить потребности населения. Это уничтожит разрыв между производителем и потребителем и ускорит процессы производства и доставки;
- 3) активное исследование. Внедрение технологий Индустрии 4.0 стимулирует исследования в разных областях, таких как IT-безопасность, окажет влияние, в частности, на образование. Новая отрасль потребует нового набора навыков. Следовательно, образование и профессиональная подготовка обретут форму, которая обеспечит современную промышленность необходимой квалифицированной рабочей силой.

К числу проблем относятся:

- 1) информационная безопасность. Пожалуй, наиболее сложным аспектом внедрения технологий Индустрии 4.0 являются риски информационной безопасности. Глубокая онлайн-интеграция создаст пространство для нарушения безопасности, утечки данных. Кражи при помощи киберустройств также должны быть приняты во внимание. Решение вопросов безопасности будет стоить производителям денег, а нарушение безопасности может нанести ущерб их активам и репутации. Более того, это проблема не индивидуальная, это проблема всей отрасли, в силу чего исследования в области безопасности имеют решающее значение;
- 2) конфиденциальность собираемых данных. В отрасли, основанной на цифровых взаимосвязях, производители должны непрерывно собирать и анализировать данные. Для частного лица это может выглядеть как угроза его личной жизни. Конфиденциальность данных станет также и проблемой для компаний. Компании, которые ранее никому не передавали свои данные, должны будут перейти к более прозрачной среде, между тем частичное сокрытие информации для многих из них являлось возможностью получать дополнительную выгоду. Сокраще-

¹⁰ См.: Соловова Е. А. Факторы развития экономики совместного потребления в мегаполисах: межстрановое сравнение. М., 2017 ; Куликов Н. А. Юриспруденция в эпоху Индустрии 4.0 // Закон. 2019. № 5. С. 87—92 ; Цифровая экономика и Индустрия 4.0: новые вызовы // Труды научно-практической конференции. СПб., 2018.

ние разрыва между потребителем и производителем станет огромной проблемой.

Говоря о цифровой трансформации в целом, можно выделить ее следующие особенности, приводящие к росту киберугроз:

- увеличение количества потенциальных точек атаки. Чем больше приложений, данных и процессов перемещается в цифровую среду, тем разнообразнее возможности хакеров и других злоумышленников. Становится больше потенциальных точек входа, что затрудняет специалистам по кибербезопасности обнаружение «узких мест» и отслеживание всех угроз.

Кроме того, для хакеров существует возможность атаковать сеть компании не напрямую, не наиболее охраняемые объекты защиты, в частности базы финансового учета, а, например, через внутреннюю социальную сеть компании. Как только хакеры получают доступ к одной системе, они могут использовать данные для авторизации в другой системе, т.е. сеть настолько же безопасна, насколько безопасны ее болевые точки;

- более высокий возможный ущерб. Вероятность повреждения в результате взлома системы или данных сейчас выше, чем когда-либо. Сегодня данные чрезвычайно ценны для бизнеса, все большее число устройств подключено к Интернету, а значит, их можно взломать. Некоторые из устройств и технологий задействованы в критических процессах. Событие, при котором кибератака нарушает некоторые из этих действий, может иметь серьезные последствия. Например, энергосистема, больничное оборудование и транспортные средства содержат цифровые компоненты. Чем сильнее организация зависит от цифровых технологий, тем серьезнее могут быть последствия атаки;

- рост уязвимости из-за использования распределенных сетей. В прошлом многие компании размещали все свое IT-оборудование и организовывали сети исключительно на одной территории. Некоторые компании, особенно крупные или те, которые обрабатывают особо важные данные, все еще делают это. Однако в настоящее время большинство компаний используют внешние цифровые приложения и размещают свои серверы в облаке, т.е. сети этих компаний не изолированы и подключены к общедоступному Интернету. Хотя каналы передачи должны иметь средства защиты, ограни-

чивающие доступ, цифровые технологии создают потенциальную возможность для хакеров взломать эти средства защиты и получить доступ к корпоративным сетям;

- постоянное изменение. Цифровые технологии и другие технологические улучшения увеличили скорость, с которой разработчики создают и обновляют программное обеспечение. Современные технологии быстро меняются. Это дает преимущества, но усложняет отслеживание процессов безопасности. Увеличенная скорость изменений усиливает уязвимость системы безопасности. Кроме того, киберпреступники постоянно придумывают новые методы, в силу чего специалистам по безопасности необходимо постоянно находить новые способы защиты;

- увеличение сложности атак. Методы хакеров не только быстро меняются, но и становятся все более изощренными. Киберпреступники используют искусственный интеллект и другие передовые технологии, как это делают профессионалы в области безопасности. Например, тип атаки с поддержкой искусственного интеллекта, называемый полиморфной атакой, является серьезной проблемой. Подобные атаки киберпреступники трансформируют, чтобы избежать обнаружения при помощи традиционных средств безопасности.

Уголовно-правовые средства противодействия

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, 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 (гл. 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 указывает на используемое средство — сеть

Интернет. Такой подход обусловлен тем, что информация становится не только целью преступных посягательств, но и средством их совершения.

Выбранный отечественным законодателем путь конструирования составов преступлений, направленных на противодействие преступлениям в информационной сфере, всегда будет страдать запаздыванием, пробельностью и неспособностью охватить все возможные общественно опасные деяния и их последствия. Одним из способов устранения подобных пробелов может выступить формирование новой главы Уголовного кодекса РФ, посвященной информационной безопасности, 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.

По данным отдельных исследователей, наибольшая доля приговоров вынесена по факту совершения в социальных сетях общественно опасных деяний, связанных с незаконным оборотом наркотических средств и психотропных веществ. Вторую по величине группу общественно опасных деяний, совершаемых при помощи социальных сетей, составляют преступные посягательства на собственность. В их структуре наибольшую долю образуют мошеннические действия. Кроме того, значительное число деяний, совершаемых при помощи социальных сетей, составляют преступления, связанные с экстремистской и террористической деятельностью, а также незаконное распространение порнографических материалов; деяния, направленные против конституционных прав и свобод человека и гражданина; преступления в сфере компьютерной информации; преступления, связанные с незаконным оборотом сильнодействующих веществ¹¹.

В то же время из всего спектра нелегального оборота запрещенных предметов в сети Интернет законодатель выделил лишь незаконный сбыт наркотиков, который квалифицируется по п. «б» ч. 2 ст. 2281 УК РФ. Непоследовательность очевидна, поскольку, например,

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 криминализована сама деятельность криптомаркетов, являющихся анонимными платформами для торговли незаконными товарами и услугами, с привлечением к ответственности разработчиков и администраторов таких ресурсов.

Отечественное уголовное законодательство характеризуется также наличием определенных пробелов в части установления ответственности за деяния в отношении несовершеннолетних, совершаемые в Интернете и социальных сетях, которые были лишь отчасти устранены в связи с принятием Федерального закона от 29 февраля 2012 г. № 14-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации в целях усиления ответственности за преступления сексуального характера, совершенные в отношении несовершеннолетних»¹². В частности, ст. 242 УК РФ была дополнена квалифицирующим обстоятельством — распространение, публичная демонстрация или рекламирование порнографических материалов или предметов среди несовершеннолетних, а также вовлечение несовершеннолетнего в оборот порнографической продукции, совершенные лицом, достигшим 18-летнего возраста (ч. 2). При этом оставлено без внимания, что многие преступления, включая торговлю детьми, также осуществляются через интернет-площадки, главным образом через социальные сети.

В связи с этим в теории отмечается, что, несмотря на развитие новых способов совершения названных преступлений с использованием информационно-телекоммуникационных сетей, в составах преступлений, предусмотренных ст. 1271, 133, 135, 154, 240, 2401 и 241 УК РФ, квалифицирующий признак «совершение преступления с использованием информационно-

¹¹ См.: Соловьев В. С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 1. С. 60—72.

¹² СЗ РФ. 2012. № 10. Ст. 1162.

телекоммуникационных сетей (в том числе сети Интернет)» до сих пор не выделяется¹³.

Другой сложностью при противодействии преступлениям, связанным, например, с электронной коммерцией, является использование криптовалюты. Проблема заключается в господствующем в юридическом сообществе мнении относительно того, что криптовалюта с точки зрения отечественного права не является объектом гражданских прав. Несмотря на то что ст. 128 ГК РФ предусматривает в качестве объекта гражданского права некое не конкретизированное, специально не обособленное «иное имущество», к которому, если следовать буквальному толкованию закона, и необходимо отнести различные виды криптовалют, складывающаяся правоприменительная практика данное требование закона игнорирует¹⁴. Исключением пока является позиция Пленума Верховного Суда РФ, изложенная в постановлении от 26 февраля 2019 г. № 1, признавшего предметом преступлений, предусмотренных ст. 174 и 174.1 УК РФ, денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления¹⁵. Однако такое разъяснение применимо лишь к указанной категории дел.

Односторонней представляется позиция законодателя по вопросу охраны персональных или идентифицирующих физических и юридических лиц данных, которые весьма широко используются для противоправных действий (доступ к банковским счетам и картам, фотографиям и контактам, переписке, коммерческой тайне и др.). В настоящее время криминализовано 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, квалифицируемых по данной статье, весьма значительно и обусловлено пространностью деяний, связанных в том числе 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, оно квалифицируется как простая кража¹⁶, поскольку специального состава или квалифицирующего признака законодателем не закреплено.

Установив ответственность за мошенничество в сфере компьютерной информации, законодатель не закрепил аналогичной нормы (например, ст. 165.1 УК РФ), предусматривающей ответственность за 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.

По сути, вне поля уголовно-правового воздействия остаются случаи, обусловленные цифровизацией медицинской деятельности. Существующий законодательный подход определяет, что ответственность за причинение вреда несет врач — как за преступление против жизни или здоровья. Смысл такого подхода утрачивается, когда вред причиняется в условиях автоматизации диагностирования и проведения операции. Кто должен нести ответственность за причинение вреда здоровью или жизни: разработчик программного обеспечения; лицо,

¹³ См.: Ключкова А. В., Пристанская О. В. Виктимологические и уголовно-правовые проблемы информационной безопасности детей и их защиты от сексуальной эксплуатации // Вестник Московского университета. Серия 11 : Право. 2017. № 6. С. 86—105.

¹⁴ См.: Перов В. А. Квалификация действий лиц, совершающих преступления с использованием криптовалюты на территории Российской Федерации // Российский следователь. 2018. № 4. С. 54—57.

¹⁵ Постановление Пленума Верховного Суда РФ от 26 февраля 2019 г. № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 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 // СПС «КонсультантПлюс».

¹⁶ См.: Бархатова Е. Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. 2016. № 9. С. 110—115.

осуществившее незаконный доступ к информационной системе; эксплуатант оборудования? Ответа на подобный вопрос уголовное законодательство не содержит.

Таким образом, цифровизация многих сфер жизнедеятельности как сопровождается по-

ложительным эффектом, так и несет новые угрозы и риски, не получающие отражения в уголовном законодательстве. В подобной ситуации требуется пересмотр уголовно-правовой политики и выработка унифицированного подхода.

БИБЛИОГРАФИЯ

1. Аюшеева И. З. Особенности гражданско-правового регулирования отношений по предоставлению в пользование недвижимого имущества в условиях развития экономики совместного потребления (sharing economy) // Актуальные проблемы российского права. — 2019. — № 6. — С. 40—48.
2. Бархатова Е. Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. — 2016. — № 9. — С. 110—115.
3. Быков В. М. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы. — М., 2015.
4. Гайфутдинов Р. Р. Квалификация преступлений против безопасности компьютерной информации. — М., 2019.
5. Галлахер Л. Airbnb. Как три простых парня создали новую модель бизнеса / пер. с англ. Е. Деревянко. — М., 2019.
6. Головецкий Н. Я., Гребенюк В. В. Фундаментальные основы экономики совместного потребления // Вестник Московского университета имени С. Ю. Витте. Сер. 1 : Экономика и управление. — 2017. — № 4. — С. 21—26.
7. Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет. — М., 2015.
8. Долгополов К. А. Особенности квалификации и расследования преступлений в сфере компьютерной информации. — Ростов н/Д, 2018.
9. Евдокимов К. Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты. — Иркутск, 2016.
10. Информационные технологии в системе здравоохранения (цифровая медицина). — Ульяновск, 2018.
11. Карев Я. А. Электронные документы и сообщения в коммерческом обороте: правовое регулирование. — М., 2006.
12. Карпов О. Э., Субботин С. А., Шишканов Д. В., Замятин М. Н. Цифровое здравоохранение. Необходимость и предпосылки // Врач и информационные технологии. — 2017. — № 3. — С. 6—22.
13. Ключкова А. В., Пристанская О. В. Виктимологические и уголовно-правовые проблемы информационной безопасности детей и их защиты от сексуальной эксплуатации // Вестник Московского университета. Серия 11 : Право. — 2017. — № 6. — С. 86—105.
14. Куликов Н. А. Юриспруденция в эпоху Индустрии 4.0 // Закон. — 2019. — № 5. — С. 87—92.
15. Мазуров В. А. Преступления в сфере компьютерной информации. — Барнаул, 2018.
16. Молотников А. Е., Архипов Е. В. Социальные сети и компании-агрегаторы: правовые аспекты деятельности // Предпринимательское право. — 2017. — № 4. — С. 38—47.
17. Монахов В. Н. Социальные сети как объект регулирования. — М., 2012.
18. Морозова Ю. А. Цифровизация как глобальный, страновой и отраслевой процесс в повышении результативности и эффективности здравоохранения и медицины // Интеллект. Инновации. Инвестиции. — 2019. — № 4. — С. 44—53.
19. Муслимов М. И. Цифровое здравоохранение как фактор революционных преобразований в отрасли // Современные проблемы здравоохранения и медицинской статистики. — 2018. — № 3. — С. 63—74.
20. Овчинский В. С. Криминология цифрового мира. — М., 2018.
21. Перов В. А. Квалификация действий лиц, совершающих преступления с использованием криптовалюты на территории Российской Федерации // Российский следователь. — 2018. — № 4. — С. 54—57.
22. Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий. — М., 2019.
23. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. — М., 2016.

24. Соловова Е. А. Факторы развития экономики совместного потребления в мегаполисах: межстрановое сравнение. — М., 2017.
25. Соловьев В. С. Криминогенный потенциал социальной сети Интернет. — М., 2017.
26. Соловьев В. С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. — 2016. — Т. 10. — № 1. — С. 60—72.
27. Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. — М., 2016.
28. Тедеев А. А. Электронная коммерция (электронная экономическая деятельность). Правовое регулирование и налогообложение. — М., 2002.
29. Цифровая экономика и Индустрия 4.0: новые вызовы // Труды научно-практической конференции. — СПб., 2018.

Материал поступил в редакцию 22 октября 2019 г.

REFERENCES

1. Ayusheeva IZ. Osobennosti grazhdansko-pravovogo regulirovaniya otnosheniy po predostavleniyu v polzovanie nedvizhimogo imushchestva v usloviyakh razvitiya ekonomiki sovmestnogo potrebleniya (sharing economy) [Features of civil law regulation of relations for the provision of real estate for use in the conditions of development of the economy of joint consumption (sharing economy)]. *Aktualnye problemy rossiyskogo prava* [Actual Problems of Russian Law]. 2019;6:40—48.
2. Barkhatova EN. Osobennosti kvalifikatsii moshennichestva v sfere kompyuternoy informatsii i ego razgranichenie s inymi sostavami prestupleniy [Features of the qualification of fraud in the field of computer information and its differentiation from other types of crimes]. *Sovremennoe pravo* [Modern law]. 2016;9:110—115.
3. Bykov VM. *Prestupleniya v sfere kompyuternoy informatsii: kriminologicheskie, ugovovno-pravovye i kriminalisticheskie problemy* [Crimes in the field of computer information: Criminological, criminal law and forensic problems]. Moscow; 2015. (In Russ.).
4. Gayfutdinov RR. *Kvalifikatsiya prestupleniy protiv bezopasnosti kompyuternoy informatsii* [Qualification of crimes against computer information security]. Moscow; 2019. (In Russ.).
5. Gallagher L. *Airbnb. Kak tri prostykh parnya sozdali novuyu model biznesa* [The Airbnb story. How three ordinary guys disrupted an industry, made billions ... and created plenty of controversy]. E. Derevyanko (translated from Eng.). Moscow; 2019. (In Russ.).
6. Golovetskiy NYa, Grebenyuk VV. Fundamentalnye osnovy ekonomiki sovmestnogo potrebleniya [Fundamentals of the economy of joint consumption]. *Vestnik Moskovskogo universiteta imeni S.Yu. Vitte* [Moscow Witte University Bulletin]. Ser. 1: Ekonomika i upravlenie [Economics and management]. 2017;4:21-26. (In Russ.).
7. Guzeeva OS. *Prestupleniya, sovershaemye v rossiyskom segmente seti Internet* [Crimes committed in the Russian segment of the Internet]. Moscow; 2015. (In Russ.).
8. Dolgoplov KA. *Osobennosti kvalifikatsii i rassledovaniya prestupleniy v sfere kompyuternoy informatsii* [Features of qualification and investigation of crimes in the field of computer information]. Rostov on Don; 2018. (In Russ.).
9. Evdokimov KN. *Protivodeystvie kompyuternoy prestupnosti v Rossiyskoy Federatsii: kriminologicheskie i ugovovno-pravovye aspekty* [Counteraction to computer crime in the Russian Federation: criminological and criminal legal aspects]. Irkutsk; 2016. (In Russ.).
10. *Informatsionnye tekhnologii v sisteme zdravookhraneniya (tsifrovaya meditsina)* [Information technologies in the healthcare system (digital medicine)]. Ulyanovsk; 2018. (In Russ.).
11. Karev YaA. *Elektronnye dokumenty i soobshcheniya v kommercheskom oborote: pravovoe regulirovanie* [Electronic documents and messages in commercial circulation: legal regulation]. Moscow; 2006. (In Russ.).
12. Karpov OE, Subbotin SA, Shishkanov DV, Zamyatin MN. *Tsifrovoe zdravookhranenie. Neobkhodimost i predposylki* [Digital healthcare. Necessity and prerequisites]. *Vrach i informatsionnye tekhnologii* [A doctor and information technologies]. 2017;3:6-22. (In Russ.).

13. Klochkova AV, Pristanskaya OV. Viktimologicheskie i ugovno-pravovye problemy informatsionnoy bezopasnosti detey i ikh zashchity ot seksualnoy ekspluatatsii [Victimological and criminal legal problems of information security of children and their protection from sexual exploitation]. *Vestnik Moskovskogo universiteta* [Moscow University Bulletin]. Series 11: Law. 2017;6:86-105. (In Russ.).
14. Kulikov NA. Yurisprudentsiya v epokhu Industrii 4.0 [Jurisprudence in the era of Industry 4.0]. *Zakon* [Law]. 2019;5:87-92. (In Russ.).
15. Mazurov VA. *Prestupleniya v sfere kompyuternoy informatsii* [Crimes in the sphere of computer information]. Barnaul; 2018. (In Russ.).
16. Molotnikov AE, Arkhipov EV. Sotsialnye seti i kompanii-agregatory: pravovye aspekty deyatel'nosti [Social networks and aggregator companies: legal aspects of activity]. *Predprinimatelskoe pravo* [Business Law]. 2017;4:38-47. (In Russ.).
17. Monakhov VN. *Sotsialnye seti kak obekt regulirovaniya* [Social networks as an object of regulation]. Moscow; 2012. (In Russ.).
18. Morozova YuA. Tsifrovizatsiya kak globalnyy, stranovoy i otraslevoy protsess v povyshenii rezultativnosti i effektivnosti zdravookhraneniya i meditsiny [Digitalization as a global, country and industry process in improving the efficiency and effectiveness of health and medicine]. *Intellekt. Innovatsii. Investitsii* [Intellect. Innovations. Investment]. 2019;4:44-53. (In Russ.).
19. Muslimov MI. Tsifrovoe zdravookhraneniye kak faktor revolyutsionnykh preobrazovaniy v otrasli [Digital healthcare as a factor of revolutionary transformations in the industry]. *Sovremennye problemy zdravookhraneniya i meditsinskoy statistiki* [Current problems of health care and medical statistics]. 2018;3:63—74.
20. Ovchinsky VS. *Kriminologiya tsifrovogo mira* [Criminology of the digital world]. Moscow; 2018. (In Russ.).
21. Perov VA. Kvalifikatsiya deystviy lits, sovershayushchikh prestupleniya s ispolzovaniem kriptovalyuty na territorii Rossiyskoy Federatsii [Classification of actions of persons who commit crimes using cryptocurrency on the territory of the Russian Federation]. *Rossiyskiy sledovatel* [Russian Investigator]. 2018;4:54-57. (In Russ.).
22. Russkevich EA. *Ugovno-pravovoe protivodeystvie prestupleniyam, sovershaemym s ispolzovaniem informatsionno-kommunikatsionnykh tekhnologiy* [Criminal and legal counteraction to crimes committed using information and communication technologies]. Moscow; 2019. (In Russ.).
23. Savelyev AI. *Elektronnaya kommertsiya v Rossii i za rubezhom: pravovoe regulirovanie* [E-Commerce in Russia and abroad: legal regulation]. Moscow; 2016. (In Russ.).
24. Solovova EA. *Faktory razvitiya ekonomiki sovmestnogo potrebleniya v megapolisakh: mezhstranovoe sravnenie* [Factors of development of the economy of shared consumption in megacities: cross-country comparison]. Moscow; 2017. (In Russ.).
25. Solovev VS. *Kriminogennyy potentsial sotsialnoy seti Internet* [Criminogenic potential of the Internet social network]. Moscow; 2017. (In Russ.).
26. Solovyov VS. Prestupnost v sotsialnykh setyakh Interneta (kriminologicheskoe issledovanie po materialam sudebnoy praktiki) [Crime in social networks (criminological research based on the materials of judicial practice)]. *Kriminologicheskii zhurnal Baykalskogo gosudarstvennogo universiteta ekonomiki i prava* [Criminology Journal of Baikal National University of Economics and Law]. 2016;10(1):60-72. (In Russ.).
27. Stepanov-Egiyants VG. *Otvetstvennost za prestupleniya protiv kompyuternoy informatsii po ugovnomu zakonodatel'stvu Rossiyskoy Federatsii* [Responsibility for crimes against computer information under the criminal law of the Russian Federation]. Moscow; 2016. (In Russ.).
28. Tedeev AA. *Elektronnaya kommertsiya (elektronnaya ekonomicheskaya deyatel'nost). Pravovoe regulirovanie i nalogooblozhenie* [E-Commerce (e-economic activity). Legal regulation and taxation]. Moscow; 2002. (In Russ.).
29. Tsifrovaya ekonomika i Industriya 4.0: novye vyzovy [Digital economy and industry 4.0: new challenges]. *Trudy nauchno-prakticheskoy konferentsii* [Proceedings of the scientific and practical conference]. St. Petersburg; 2018. (In Russ.).