Казанский
инновационный
университет имени
В. Г. Тимирясова

Министерство цифрового развития
государственного управления,
информационных технологий
и связи Республики Татарстан

# ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
I Международной научно-практической конференции

23 сентября 2022 г.
г. Казань

В шести томах
Том 2

Казань ■ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ■ 2022

Kazan
Innovative University
named after
V. G. Timiryasov

Ministry of Digitalization of Public
Administration, Information
Technologies and Communications
of the Republic of Tatarstan

# DIGITAL TECHNOLOGIES AND LAW

Collection of scientific articles
of the I International Scientific and Practical Conference

September 23, 2022
Kazan

In 6 volumes
Volume 2

Kazan ■ KIU "POZNANIYE" PUBLISHERS ■ 2022

**УДК 004:34(063)**
**ББК 67с51я43**
**Ц75**

*Печатается по решению редакционно-издательского совета*
*Казанского инновационного университета имени В. Г. Тимирясова*



**Ц75** **Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции** (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 2. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 556 с. EDN: JSIXFM. DOI: http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556
**ISBN 978-5-8399-0767-6**
**ISBN 978-5-8399-0769-0** (Том 2)

Вошедшие в сборник научные труды приурочены к Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 23 сентября в Казани в рамках Международного форума Kazan Digital Week 2022, организуемого Кабинетом Министров Республики Татарстан под эгидой Правительства Российской Федерации.

Широкий круг рассмотренных на конференции теоретико-методологических и практикоориентированных, междисциплинарных и отраслевых вопросов связан с приоритетами правового развития цифровых технологий, перспективами правового регулирования цифрового профилирования, экспериментальными и специальными правовыми режимам в сфере создания цифровых инноваций, интеллектуальными правами, трудовыми и связанными с ними отношениями, блокчейн-технологиями, криптовалютой, децентрализованными финансами в правовых реалиях, искусственным интеллектом, робототехникой и др.

Научные труды представленного тома систематизированы по современным трендам развития цифровых технологий в системе уголовно-правовых, международно-правовых и частноправовых (цивилистических) отношений.

Нашедшие отражение в этом и иных томах сборника идеи и предложения в своей совокупности являются ключом к пониманию интеллектуальной карты смыслов, которые будут интересны ученым-правоведам и экспертам в области цифровых технологий, практикующим юристам, представителям правотворческих и правоприменительных органов, государственным служащим и участникам реального сектора экономики, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0767-6
ISBN 978-5-8399-0769-0 (Том 2)

**UDC 004:34(063)**
**LBC 67c51я43**
**Ц75**

*Published by the decision of the Editorial-Publishing Board*
*of Kazan Innovative University named after V. G. Timiryasov*



**Ц75** **Digital Technologies and Law: collection of scientific articles of the I International Scientific and Practical Conference** (Kazan, September 23, 2022) / eds.: I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova. In 6 vol. Vol. 2. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2022. – 556 p. EDN: JSIXFM. DOI: http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556
**ISBN 978-5-8399-0767-6**
**ISBN 978-5-8399-0769-0** (Volume 2)

The research works included into the collection are correlated with International Scientific and Practical Conference "Digital Technologies and Law" which took place on September 23 in Kazan during the International Forum Kazan Digital Week 2022, organized by the Cabinet of Ministers of the Republic of Tatarstan under the aegis of the Government of the Russian Federation.

The broad range of theoretical and methodological, practice-oriented, interdisciplinary and sectoral issues is related to the priorities of juridical development of digital technologies, prospects of legal regulation of digital profiling, experimental and special legal regimes in the sphere of digital innovations, intellectual rights, labor and adjacent relations, blockchain technologies, cryptocurrency, decentralized finance in legal realities, artificial intelligence, robotics, etc.

The research works included in this volume are systematized by the modern trends of digital technologies development in the system of criminal-legal, international-legal and private-legal (civilistic) relations.

The ideas and proposals reflected in this and other volumes are, taken integrally, a key to understanding the intellectual map of meanings, which would be interesting for legal scientists and experts in the sphere of digital technologies, practicing lawyers, representatives of law-making and law-enforcement agencies, state servants and participants of the real economy sector, young researchers – students, graduates and post-graduates, to all those interested in the issues of mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67c51я43



ISBN 978-5-8399-0767-6
ISBN 978-5-8399-0769-0 (Volume 2)

Подводя итог сказанному, следует отметить, что проблема нормативного закрепления правовой регламентации использования искусственного интеллекта при осуществлении процессуальных действий при осуществлении предварительного расследования требует незамедлительного решения. Основной целью при этом должна стать не попытка заменить человеческий разум компьютерной программой, использующей искусственный интеллект, а оказание помощи правоприменителю в проведении отдельных следственных и процессуальных действий, фиксации материалов расследования в целях оптимизации и повышения эффективности деятельности.

**Список литературы**

1. Указ Президента Российской Федерации от 10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». URL: http:// Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.10.2019, «Собрание законодательства РФ», 14.10.2019, № 41, ст. 5700 (дата обращения: 19.02.2022).

2. Утечки данных. Россия. 2019 год. Аналитический центр Infowatch. URL: https://www.infowatch.ru/analytics/reports/27614 (дата обращения: 19.02.2022).

3. Четверикова О. Цифровой тоталитаризм. Как это делается в России? – М.: Книжный мир. 2019 // URL: https://iknigi.net/avtor-olga-chetverikova/183838-cifrovoy-totalitarizm-kak-eto-delaetsya-v-rossii-olga-chetverikova/read/ (дата обращения: 19.02.2022).

**В. В. Ровнейко,**
кандидат юридических наук, доцент,
Удмуртский государственный университет

## ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ «КРАЖИ ИДЕНТИФИКАЦИИ»

**Аннотация.** Статья посвящена анализу такого понятия как «кража идентификации» и проблемам уголовно-правовой оценки деяний, которые посягают на безопасность цифровой личности. Введение экспериментальных правовых режимов, реализация «пилотных проектов» в «регуляторных песочницах» выявляют новые виды рисков, которые должны быть минимизированы. Так, один из проектов, связанный с использованием биометрических персональных данных при предоставлении банковских услуг, был запущен как регулятивная «песочница» Банка России. Однако «пилот» не взлетел из-за серьезных рисков подделки биометрических данных и документов. Неправомерное использование чужих персональных данных для получения выгоды является «кражей идентификации». Определение понятия «кража идентификации» с учетом положений российского законодательства нуждается в существенной коррекции. Уголовно-правовые средства позволяют рассматривать в качестве основания уголовной ответственности за «кражу идентификации» составы различных преступлений, предусмотренных в УК РФ (например,

о мошенничестве), но необходима разработка системы мер, как уголовно-правового, так и регулятивного характера для обеспечения безопасности цифровой личности.

**Ключевые слова**: уголовное право, цифровые технологии, «кража идентификации», цифровая личность, безопасность цифровой личности, «регуляторные песочницы», экспериментальный правовой режим

## CRIMINAL LAW PROBLEMS OF «IDENTITY THEFT»

**Abstract.** The article is devoted to the "identity theft" and to the problems of criminal law assessment of acts that infringe on the security of a digital identity. The introduction of experimental legal regimes, the implementation of "pilot projects" in "regulatory sandboxes" reveal new types of risks that should be minimized. As a regulatory sandbox of the Bank of Russia one of the projects using biometric personal was related in the provision of banking services. There are serious risks of forgery of biometric and documents in the "pilot". The misuse of other people's personal for profit is "identity theft". The definition of "identity theft", taking into account the provisions of Russian legislation, needs significant correction. In Criminal law there are corpus delicti to criminal liability for "identity theft". The corpus delicti of various crimes provided in the Criminal Code of the Russian Federation (for example, fraud) can be use for "identity theft", but it is necessary to develop a system of measures, criminal and regulatory in nature to ensure the security of a digital identity.

**Keywords**: Criminal law, Digital technologies, "Identity theft", Digital identity, digital identity security, "Regulatory sandboxes", Experimental legal regime

Применение в различных сферах деятельности цифровых технологий порождают возникновение социально значимых ценностей (общественных отношений, интересов и благ), находящихся за пределами охраны действующего уголовного законодательства России. Принятие Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [17] и введение «пилотных проектов», «регуляторных (цифровых) песочниц» [6] в различных сферах деятельности породили большое количество вопросов организационного, технического, морального и правового, в том числе и уголовно-правового характера.

Один из таких проектов связан с использованием биометрических персональных данных [12] при предоставлении банковских услуг и запущен как регулятивная «песочница» Банка России (т. е. «механизм для пилотирования, моделирования процессов новых финансовых сервисов и технологий в изолированной среде, требующих изменения правового регулирования») [13]. Восемнадцать российских банков приняли участие в проекте для тестирования возможности открытия счетов новым клиента с применением видеоконференцсвязи без посещения отделения банка физическим лицом. Национальным советом финансового рынка (НСФР) была направлена заявка в Банк России (ЦБ) на пилотирование указанной технологии в регулятивной «песочнице» ЦБ. Данный проект нуждается в тщательном изучении пилотировании в «песочнице» Банка России, так как идентификация лица по

видеосвязи связана с высокими рисками для граждан и финансовых организаций» [19]. «Пилот» не взлетел в связи с серьезными рисками подделки биометрических данных (видео и голоса), а также документов. Работа над проектом продолжается, и банки ищут способы минимизации рисков мошенничества [3].

Хотя указанный проект не был завершен и Банк России не инициировал процедуру создания правовых условий для внедрения сервиса [13], попытка реализации проекта выявила серьезную проблему, связанную с возможной «кражей идентификации» [16] («кражей личности» [2], «кражей идентичности» [10], «похищения цифровой личности» [2] и т. п.) и неправомерным использованием чужих персональных идентификационных данных в своих интересах. Закрепленный в ст. 2 Конституции РФ приоритет интересов личности и возникновение «цифровой личности» обуславливают необходимость обеспечения цифровой безопасности личности уголовно-правовыми средствами и делают необходимым изучение возможностей действующего уголовного законодательства России в этой сфере.

Возникновение новых социально значимых ценностей, в том числе, таких как «цифровая личность», обусловленных применением в различных сферах деятельности цифровых технологий, может повлечь возникновение пробела в уголовном законе. Такой пробел не может восполняться путем применения уголовно-правовых норм по аналогии. В результате некоторые объективно общественно опасные деяния не подпадают под действие уголовно-правовых норм. Нельзя сказать, что все посягательства на такие ценности полностью находятся за пределами действия Уголовного кодекса РФ.

Если рассмотреть риски, которые возникают при удаленной идентификации личности для получения банковских услуг, в уголовно-правовом аспекте, то можно сделать вывод о том, что многие из них формально содержат признаки составов преступлений, предусмотренных в УК РФ. Так, в ходе рассмотрения и анализа возможности применения данного сервиса ЦБ, Минфин и Росфинмониторинг определили пять видов рисков [20].

Необходимо отметить, что большинство из перечисленных в качестве рисков деяний представляет повышенную опасность в связи с техническими сложностями идентификации лица, использующего чужие персональные идентификационные данные. Большая часть из них может быть квалифицирована как мошенничество с учетом разъяснений, содержащихся в постановлении Пленума Верховного Суда РФ о видах и содержании обмана [7], или как отмывание доходов от преступной деятельности [8]. Особая опасность таких действий связана, прежде всего, с возможностью причинения имущественного ущерба как кредитным организациям, так и их клиентам при реализации сервиса по удаленному предоставлению банковских услуг с использованием для идентификации клиентов персональных биометрических данных, лицами, установить которых для последующего привлечения к уголовной ответственности достаточно сложно.

Повышенный интерес с точки зрения уголовно-правовой оценки содеянного представляют подмена изображения и подмена личности клиента, которые могут рассматриваться как особый способ совершения преступления. Для обозначения этих общественно опасных действий используется понятие «Identity theft» или «кража

идентификации», под которой понимается причинение вреда путем неправомерного использования персональных данных другого лица. Хотя неправомерному использованию могут подвергнуться данные как физического, так и юридического лица, мы будем рассматривать содержание данного понятия в отношении только физических лиц.

Следует отметить, что характер общественной опасности при «краже идентификации» (Identity theft) не сводится только к причинению имущественного ущерба, хотя в большинстве источников в качестве признака данного вида преступления указана направленность деяния на «получение материальной выгоды» [11]. В других источниках содержится более широкое понятие, в котором в качестве признака «кражи личности (identity theft)» указана направленность на получение любой выгоды [2]. В условиях отсутствия нормативного определения оба подхода имеют равное значение. Но ограничивать количество случаев «кражи идентификации» только корыстной направленностью было бы нецелесообразно.

IT-специалисты выделяют виды «кражи личности» в зависимости от целей последующего использования полученной идентификационной персональной информации. В одной из таких классификаций, например, выделяют в качестве видов кражи личности: 1) финансовые махинации; 2) преступная кража личности (identity theft); 3) кража данных с целью изменения личности; 4) похищение медицинских данных; 5) создание клонов[2].

Данная классификация представляется не вполне корректной, так как ее авторы рассматривают «кражу личности» и как отдельное явление, и как его разновидность (такая кража-кража личности).

В другой классификации авторы тоже выделяют пять видов «кражи идентификации», но немного иначе: 1) кража личных данных; 2) кража финансовой идентичности; 3) кража детской личности; 4) кража личных данных налогоплательщика; 5) кража медицинской идентичности [21].

Таким образом, авторы второй классификации, рассматривая как самостоятельные виды кражу личных данных ребенка и кражу личных данных налогоплательщика, не выделяют в качестве самостоятельного вида создание клонов и кражу личных данных для изменения личности. Представляется, что похищение биометрических персональных данных, которые могут быть использованы для «создания клонов» и «изменения личности», необходимо рассматривать в качестве самостоятельного вида «кражи личности» и с учетом технических особенностей таких действий, а также существование рисков подделки биометрических данных (видео и голоса), например, для дистанционного получения банковских услуг.

Вышеприведенные классификации составлены не юристами, а специалистами в области IT. Имеющиеся правовые исследования в этой сфере не содержат исчерпывающей классификации «краж идентификации», хотя и посвящены правовым проблемам противодействия этому явлению (их немного) [1, 4, 14, 15]. Доктринальные правовые определения понятия «кража идентификации» разнообразны. Одни авторы рассматривают это понятие только в очень узком смысле и приравнивают его к мошенничеству [15]. Другие используют вместо понятия «identity theft» в качестве синонима понятие «digital identity theft» (кража цифровых идентификационных данных), определяя его «доступ к персональной информации

лица, его документам (точнее, их цифровым копиям), данным банковских карт и так далее, в результате чего возникает возможность совершить хищение имущества, принадлежащего такому лицу, либо продать полученные доступы третьим лицам» [1]. Третьи определяют identity theft как кражу личности, и сделку, заключенную, как правило, неустановленным лицом под чужой личиной путем подлога документов и подделки подписей, будь то бумажных или электронных» [14]. Из вышеприведенных точек зрения наиболее обоснованным представляется подход, когда «кража идентификации» рассматривается как «кража цифровых идентификационных данных». Последняя отражает суть анализируемой уголовно-правовой проблемы наиболее точно.

Понятие «кража личности» тесно связано с понятием «цифровой личности». Нормативного определения указанного понятия нет. Давая доктринальное определение в юридической литературе цифровую личность определяют «как совокупность данных о субъекте, отраженная в цифровой форме и содержащая достоверную информацию, включая (но не ограничиваясь) персональные данные субъекта – физического лица или сотрудников юридического лица, финансовую, правовую и банковскую информацию, сведения о его интересах и предпочтениях, историю покупок и перемещений, а также иные сведения, позволяющие осуществить идентификацию субъекта – правообладателя информации или иного лица, связанного с такой информацией» [1].

Понятие «цифровой личности» может быть в некоторых случаях отождествлено понятию «цифровой профиль», под которым может пониматься «совокупность сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации»» [9]. Полагаем, что с учетом такого определения «цифровой профиль» является более узким понятием по сравнению с «цифровой личностью».

«Кража идентификации» («кража цифровой личности») не ограничивается только корыстной направленностью и, по нашему мнению, должна рассматриваться в широком смысле этого понятия, хотя следует согласиться с тем, что в подавляющем большинстве случаев она совершается в целях получения прямо или косвенно материальной выгоды, но при этом не всегда причиняет вред имущественным правам потерпевшего, хотя всегда нарушает личные права и законные интересы физического лица, чьи персональные данные были похищены. В существующих определениях понятия «identity theft» особое значение придается получению выгоды, а использование неправомерного доступа к цифровому объекту является вторичным. Следует согласиться с мнением, что буквальный перевод на русский язык понятия «identity theft» как «кража идентификации» или «кража цифровой личности» – «представляется не вполне корректным, поскольку фактически происходит завладение не цифровым объектом, а, скорее, доступом к нему» [1].

Необходимо отметить, что уголовно-правовые нормы не предусматривают уголовную ответственность за сам факт «кражи идентификации», т. е. незаконного получения (собирания) или подделки (изготовления) персональных цифровых

идентификационных данных личности. Регулятивное законодательство определяет правовой режим персональных данных. Право на получение персональные данные с последующим внесением их в Единую биометрическую систему имеют самые разные субъекты (и банки, в том числе). В таких условиях, когда получать и собирать информацию могут разные субъекты, и возникает проблема ответственности за их утечку или другие неправомерные действия с такой информацией.

В Российской Федерации формируется Единая биометрическая система (ЕБС), инициаторами создания которой являются банки и ЦБ, а исполнителем – «Ростелеком». Данные, содержащиеся в ЕБС, востребованы в различных сферах жизни, например, в сферах здравоохранения, образования, ритейла, государственных услуг. Наиболее широкое применение ЭБС имеет в финансовой сфере в коммерческих банках [5].

С учетом действующего механизма удаленной идентификации и этапов удаленной идентификации [5], в котором задействованы как вышеуказанные государственные органы, так и физические лица, можно утверждать, что подмена персональных данных может иметь место и при совершении регистрации физического лица в ЕСИА или ЭБС, так и совершении физическим лицом действий по удаленной регистрации.

В отношении идентификационных персональных данных необходимо предусмотреть самостоятельный механизм уголовно-правовой защиты, исходя из того, что «персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)», и с учетом различного вида таких данных (по содержанию, по особенностям правового режима, по источнику и т. п.) [18]. Но, поскольку законно получать и собирать информацию о личности могут разные субъекты, то необходима и дифференциация уголовной ответственности в зависимости от формы вины, целей и мотивов, а также тяжести наступивших последствий (количества потерпевших, характера и размера причиненного им вреда). Кроме того, необходимо учитывать, что многие понятия, которые используются при описании посягательств на информационную безопасность, включая информационную (цифровую) безопасность личности, носят технический характер.

Как известно, корректность и единообразие используемых формулировок позволяет решить многие правовые проблемы. Имеющиеся расхождения в понятиях, имеющих одинаковое (или почти одинаковое содержание), должны учитываться при определении криминообразующих признаков. В сфере информационных технологий общепринятым является использование английских терминов, которые будучи дословно переведенными на русский язык, не могут быть использованы в качестве юридических формулировок сами по себе. Установление уголовной ответственности за «кражу идентификации» предполагает тщательный выбор терминологии и корректное использование специальных технических понятий.

Для корректного использования в понятии «кража идентификации» термина «идентификация» следует учитывать, что и она имеет определенное содержание. И с учетом этого содержания нельзя отождествлять идентификацию с другими схожими терминами. Так, в специальной литературе отмечается, что «часто в рос-

сийской практике термином «идентификация» называют три понятия, а именно: собственно идентификацию, верификацию и аутентификацию [5], которые имею близкое по характеру, но все-таки различное содержание, которое необходимо учитывать для понимания правовой природы такого явления как «identity theft». Под идентификацией в узком смысле понимается установление совпадения неизвестного объекта известному; под аутентификацией понимается удостоверение личности; а под верификацией – подтверждение подлинности документов [5].

Таким образом, установление уголовной ответственности за незаконные получение и использование или сбыт персональных данных физического лица, которые позволяют осуществить идентификацию, верификацию и аутентификацию личности является необходимым, исходя из развития инновационных цифровых технологий в различных сферах деятельности.

Некоторые авторы не считают «цифровую личность» новым правовым явлением, нуждающимся самостоятельной правовой охране. Они выделяют два основных аспекта «цифровой личности»:

– «цифровые копии документов, содержащих персональные данные субъекта, его медицинские данные и прочие индивидуальные характеристики, закрепленные в цифровой форме,

– информация о его сетевой активности, история запросов в браузере, предпочтения, интересы и иная информация, которая носит менее формальный характер, нежели первая категория, но также представляет собой высокую ценность, как с точки зрения правомерного коммерческого использования, так и для потенциальных правонарушителей» [1].

С учетом этого подхода и «понимания цифровой личности как цифровой фиксации идентифицирующих документов и прочей информации, содержащей персональные данные о субъекте», ими предлагается «вывод о том, что должен применяться режим, аналогичный бумажным документам,» [1] и «режим конкретных составляющих цифровой личности должен соответствовать потенциальным целям существования информации в той или иной форме: применительно к документам (например, паспорт, ИНН, трудовая книжка, медицинская карта и т. д.)», должен применяться «режим, аналогичный документам в их материальном выражении» [1]. В отношении второй группы информации – персональных данных – должен применяться режим, установленный российским законодательством, согласно которому история поиска и прочая информация, полученная без ведома гражданина, может быть предложена к обработке в рамках режима персональных данных либо коммерческой тайны (в случае обезличенной обработки и использования, например, в рамках формирования статистики)» [1].

Применение к электронным документам (цифровым документам) правового режима, аналогичного применяемому к бумажным документам, общепризнано [22]. Но персональная информация, которая не носит такого формально-документированного характера (например, видео-идентификация) не охраняется нормами уголовного права, если не является личной или семейной тайной [23].

Необходимо отметить, что предлагаемые подходы, применим в области гражданского права, одним из принципов которого является добросовестность и разумность

поведения участников общественных отношений. Задачей уголовного права является охрана прав и свобод личности от общественно опасных действий (бездействия). «Цифровая личность» (digital identity) и цифровые права нуждаются в самостоятельной уголовно-правовой охране, но это возможно только после определения регулятивным законодательством содержания персональных данных («цифровой личности») и режима получения (сбора), хранения, передачи, предоставления, использования и уничтожения персональных данных, позволяющих осуществлять идентификацию, верификацию и аутентификацию личности. Только в этом случае могут быть определены криминообразующие признаки для установления уголовной ответственности за неправомерное использование (а также получение, хранения и т. д.) персональных данных и за нарушение правил использования (а также получения, хранения и т. д.), повлекших их утечку.

Необходимость такого самостоятельного правового регулирования этой сферы деятельности признается даже теми авторами, которые пришли к выводу, что «цифровая личность не представляет собой качественно новое явление, а является новым способом закрепления существующей информации» [1]. По их мнению, все-таки «требуется внесение соответствующих изменений в существующее законодательство для отражения правового режима персонализированной информации посредством цифровой формы. Кроме того, сама категория цифровой личности подлежит детальному рассмотрению в рамках научной и учебной деятельности» [1].

Таким образом, выявленные риски «применения систем видеосвязи или иных технических средств для удаленной идентификации клиентов банков в «регуляторной песочнице» ЦБ» были реальными, «поэтому пилот не взлетел» [20]. Такие риски не могут быть минимизированы или устранены путем применения только уголовно-правовых мер. Предпринимаемые меры должны носить комплексный и системный характер. Но выстраивание комплаэнса, направленного на обеспечение цифровой безопасности личности (безопасности цифровой личности) невозможно без использования уголовно-правовых средств противодействия. Закрепление в уголовном законе признаков состава преступления (или составов преступления), которые могут рассматриваться как «кража идентификации», в таких условиях становится необходимой.

Использование цифровых технологий в отношении идентификации, верификации и аутентификации личности при отсутствии средств и гарантий должной защиты личности от неправомерного использования ее биометрических данных является необоснованным риском применения технологий и сервисов, предполагающих сбор и использование того, что может рассматриваться как «цифровая идентификация». Такое использование нуждается в серьезном, глубоком и разностороннем изучении, как с позиций разработки условий правомерности причинения вреда в состоянии обоснованного риска, так и таких понятий, как «цифровая личность», «цифровой профиль» и цифровые права.

«Кража идентификации» предполагает неправомерное получение данных о субъекте, отраженных в цифровой форме, включая персональные данные, которые позволяют осуществить идентификацию (идентификацию, верификацию и аутентификацию) субъекта. Дальнейшее использование такой информации может осуществляться

в самых разных целях и «кражей идентификации» с учетом понятийного аппарата, используемого уголовным правом России, не является. Более корректным было бы в этом случае говорить о «похищении цифровых идентификационных данных».

С учетом действующего российского уголовного законодательства случаи незаконного использования персональных данных можно рассматривать как способы совершения преступлений, уже содержащихся в УК РФ и совершаемых, как правило, путем обмана (мошенничества, умышленного причинения имущественного ущерба при отсутствии признаков хищения и др.). Но представляется возможной дифференциация уголовной ответственности с учетом повышенной общественной опасности таких деяний, совершаемых с использованием незаконно полученных или незаконно используемых цифровых идентификационных данных

В случае установления правового режима «цифровой личности» корректной будет и постановка вопроса об уголовно-правовом значении как предмета самостоятельного состава преступления элементов «цифровой личности» – персональных данных, биометрических персональных данных, медицинских данных, данных налогоплательщика и информация о сетевой активности, история запросов в браузере, предпочтения, интересы и иная личная информация.

## Список литературы

1. Кирсанова Е. Е. Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике: монография. М.: Юстицинформ, 2022. 228 с. / СПС «КонсультантПлюс».

2. Кража личности (Identity theft) // URL: https://www.anti-malware.ru/threats/identity-theft (дата обращения: 19.08.2022).

3. Лекомцева Н. Что такое «регуляторная песочница». Объясняем простыми словами //Энциклопедия. 24 сентября 2021 год. URL: https://secretmag.ru/enciklopediya/chto-takoe-regulyatornaya-pesochnica-obyasnyaem-prostymi-slovami.htm (дата обращения: 19.08.2022).

4. Минаева А. И. Цифровые права как элементы правового статуса личности // Вопросы российского и международного права. 2021. Том 11. № 3А. С. 69–77. DOI: 10.34670/AR.2021.81.43.035 URL: https://www.elibrary.ru/download/elibrary_46126392_10550362.pdf (дата обращения: 19.08.2022).

5. Метревели Е. Г. Перспективы развития цифровой идентификации личности // Современная наука: актуальные проблемы теории и практики. Серия «Экономика и право». № 12, декабрь 2021. С. 71. URL: http://www.nauteh-journal.ru/files/dc428735–3a20–4622-b9dc-4ccf948dda4b (дата обращения: 19.08.2022).

6. Постановление Правительства РФ от 9 марта 2022 г. № 309 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств». URL: https://base.garant.ru/403712648/ (дата обращения: 17.09.2022).

7. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 17.09.2022).

8. Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «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» URL: http://www.consultant.ru/document/cons_doc_LAW_182365/ (дата обращения: 17.09.2022).

9. Проект федерального закона № 747513–7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» (ред., внесенная в ГД ФС РФ, текст по состоянию на 05.07.2019) // СПС «КонсультантПлюс» (дата обращения: 17.09.2022).

10. Подлог, связанный с применением компьютеров. URL: https://studref.com/693043/pravo/podlog_svyazannyy_primeneniem_kompyuterov

11. Переход на личности: что такое identity theft. URL: https://www.securitylab.ru/blog/company/infowatch/341488.php (дата обращения: 19.08.2022).

12. Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) о вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки. URL: https://25.rkn.gov.ru/news/news54167.htm (дата обращения: 17.09.2022).

13. Регулятивная «песочница» Банка России. URL: https://cbr.ru/fintech/regulatory_sandbox/ (дата обращения: 19.08.2022).

14. Рудоквас А. Д. О влиянии регистрационной системы на оборот недвижимости // Вестник гражданского права. 2022. № 1. С. 45–58. / СПС «КонсультантПлюс» (система).

15. Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» (2-е издание, переработанное и дополненное). («Статут», 2021) / СПС «КонсультантПлюс».

16. Сазонова Маргарита. Биометрические персональные данные и технологии идентификации: какие правовые проблемы могут возникнуть? // URL: https://www.garant.ru/news/1460152/ (дата обращения: 19.08.2022).

17. Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31.07.2020 № 258-ФЗ (в ред. Федерального закона от 02.07.2021 № 331-ФЗ) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_358738/ (дата обращения: 17.09.2022).

18. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» п. 1 ст. 3 / СПС «Консультант».

19. Чернышова Евгения. «Банки протестируют открытие счетов клиентам по видеосвязи. Но пока ограничат объем операций, которые можно проводить таким способом» // РБК. 09.11.2020. URL: https://www.rbc.ru/finances/09/11/2020/5fa3f7769a79477c927c9189 (дата обращения: 19.08.2022).

20. Чернышова Евгения. ЦБ увидел угрозу при идентификации банковских клиентов по видео. Среди рисков – использование дипфейков и профессионального грима // Финансы, 21 мая 2021 – РБК. URL: https://www.rbc.ru/finances/21/05/2021/60a664d49a79472499fee709 (дата обращения: 19.08.2022).

21. Что такое кража личных данных? URL: https://ru.gofreedommoney.com/what-is-identity-theft (дата обращения: 19.08.2022).

22. Пленум Верховного Суда Российской Федерации принял новое постановление № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324–327.1 УК РФ» URL: https://www.vsrf.ru/documents/own/29494/ (дата обращения: 19.08.2022).

23. Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» URL: http://www.consultant.ru/document/cons_doc_LAW_314616/ (дата обращения: 19.08.2022).

**Г. В. Романова**
кандидат юридических наук,
Казанский институт (филиал) Всероссийского государственного
университета юстиции

## ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

**Аннотация.** В современном мире неизбежно возрастает роль цифровых возможностей и цифровизации услуг в различных сферах жизнедеятельности. В уголовном судопроизводстве появляется и развивается такой вид (источник) доказательства как электронное доказательство. В настоящей статье представлены актуальные вопросы использования электронных доказательств в уголовном судопроизводстве.

**Ключевые слова**: уголовный процесс, компьютерная информация, электронное доказательство, цифровое доказательство

## PROBLEMS OF USING ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

**Abstract**. Digitalization of criminal procedural activity is a complex process that inevitably affects the procedure of proof. One of the most controversial topics in this direction remains the possibility of introducing a new type (source) of evidence – electronic evidence. The article deals with topical issues in criminal proceedings.

**Keywords**: Criminal proceedings, Computer information, Electronic evidence, Digital evidence

Вопросы доказательств и доказывания приобретают процессуальное значение и активно исследуются учеными и правоприменителями в уголовном судопроизводстве.

Представляется, что изучение специального предназначения электронных доказательств в уголовном процессе связана с двумя методологическими проблемами. Во-первых, электронному доказательству придается первостепенное значение, изучается техническая сторона вопроса. Во-вторых, понимание электронного доказательства связано с электронной структурой документа, что затрагивает его особые свойства носителя.