О правотворчестве и правовых новациях в части защиты от утечек персональных данных

Булочников Станислав Юрьевич, Тамбовский государственный университет им. Г. Р. Державина, Институт права и национальной безопасности (Тамбов, Российская Федерация)
студент 3-го курса специалитета;
e-mail: bulochnikov03@mail.ru
ORCID: 0009-0001-7619-0643.

Научный руководитель:
Харин Вадим Витальевич, Тамбовский государственный университет им. Г. Р. Державина, Институт права и национальной безопасности; кафедра специальной подготовки и обеспечения национальной безопасности (Тамбов, Российская Федерация)
старший преподаватель;
e-mail: harin@tsutmb.ru

Аннотация
Статья посвящена анализу правовых новаций и законодательных изменений в области защиты персональных данных от утечек, вызванных вызовами цифровизации и глобализации. Автор подчеркивает рост киберугроз и необходимость совершенствования законодательства для противодействия этим вызовам.
В исследовании использован сравнительно-правовой анализ законодательства, а также рассмотрены последние изменения в нормативно-правовых актах, направленные на усиление защиты персональных данных. Автор анализирует ключевые проблемы, такие как рост утечек данных, и предлагает меры по их устранению, включая введение киберстрахования и усиление ответственности за утечки.
Выявлены основные проблемы в области защиты персональных данных, такие как увеличение числа утечек и незаконное использование данных с помощью технологий Deepfake. Предложены меры по улучшению законодательства, включая введение киберстрахования и усиление административной и уголовной ответственности за утечки данных. Также рассмотрены правовые механизмы борьбы с технологиями Deepfake.
Результаты исследования могут быть использованы для дальнейшего совершенствования законодательства в области защиты персональных данных, а также для повышения осведомленности граждан о киберрисках. Предложенные меры, такие как киберстрахование и усиление ответственности, могут способствовать снижению числа утечек данных и повышению уровня информационной безопасности. Исследование также подчеркивает необходимость гармонизации законодательства и повышения компетенций специалистов в области IT и права.
Ключевые слова: персональные данные, цифровизация, киберстрахование, киберриски, утечки данных, правотворчество, технология распознавания лиц, защита изображения лица, искусственный интеллект, информация.

On Law-making and Legal Innovations in Terms of Protection against Personal Data Leaks

Stanislav Yu. Bulochnikov, Derzhavin Tambov State University, Institute of Law and National Security (Tambov, Russian Federation)
specialized student;
e-mail: bulochnikov03@mail.ru
ORCID: 0009-0001-7619-0643.

Academic Supervisor:
Vadim V. Harin, Derzhavin Tambov State University, Institute of Law and National Security; Department of Special Training and National Security (Tambov, Russian Federation)
Senior Lecturer;
e-mail: harin@tsutmb.ru

Abstract
The paper deals with the analysis of recent legal innovations and amendments in the legislation related to personal data protection against the leaks caused by digitalization and globalization challenges. The author emphasizes the increasing number of cyber threats as well as the need for improved legislation to address these challenges.
The research employs a comparative legal analysis of existing legislation, as well as some recent amendments to regulatory legal acts aiming to strengthen personal data protection. The author examines such key issues as the growth of data breaches, and proposes some measures to address them, including implementing cyber insurance and increasing liability for data leaks.
The main issues in the area of personal data protection have been identified, including the increase in data breaches and illegal use of information through the employment of Deepfake technologies. To address these issues, measures have been proposed, such as improving legislation through the introduction of cyber insurance and increasing administrative and criminal penalties for data breaches. Additionally, legal mechanisms to combat Deepfake technologies have been considered.
The research findings can be utilized to further refine the legislation in the realm of personal data protection and raise the citizens' awareness of cyber risks. The suggested measures, including cyber insurance and heightened accountability, can be instrumental in reducing the frequency of data breaches and enhancing information security. Furthermore, the study emphasizes the necessity for harmonizing legislation and enhancing the skills of IT professionals and legal experts.

Keywords: personal data, digital transformation, cyber insurance, cybersecurity risks, data breaches, deep fake, legislative process, innovations, globalization, facial recognition technologies, face image protection, artificial intelligence, information.

ВВЕДЕНИЕ

Правовые новации в сфере новых и развивающихся технологий включают изменения и обновления законодательства, направленные на адаптацию правовых норм к современным экономическим и социальным условиям. Эти изменения разрабатываются и принимаются государственными органами в рамках правотворческого процесса, который направлен на совершенствование правового регулирования.

Правотворчество — это процесс разработки, принятия, изменения или отмены правовых норм компетентными государственными органами. В сфере частного права правотворчество играет ключевую роль в обеспечении актуальности и эффективности правового регулирования. Оно позволяет своевременно реагировать на изменения в экономике, социальной сфере и технологиях, обеспечивая защиту прав и интересов участников гражданского оборота [5].

По мнению С. С. Вашуриной, государство для регулирования новых процессов и технологий в эпоху цифровизации вводит лишь программно-стратегические акты, а не полноценные законы или иные систематизированные и конкретные нормы [3]. Однако

в последние годы в законодательстве произошел ряд значительных изменений, направленных на улучшение правового регулирования и создание более благоприятных условий для развития бизнеса и экономики в условиях цифровизации. Примеры последних изменений отражены в таблице 1.

Таблица 1*

Вид изменений	Суть изменений
Изменения в Гражданском кодексе Российской Федерации	Внесены поправки в отношении недвижимости, наследства, интеллектуальной собственности, которые уточнили и упростили правовые нормы в этих сферах[1]
Принятие новых законов	В недавнее время были приняты новые законы, регулирующие отношения в сфере электронной торговли, кредитных историй, защиты данных и других областях[2]
Развитие нормативно-правовых актов	Разработаны и приняты новые подзаконные акты, уточняющие и конкретизирующие нормы федеральных законов в различных сферах частного права[3]

* *Составлено (разработано) автором.*

Конечно же, современные правовые новации неразрывно связаны с развитием новых технологий. Цифровизация охватывает всё больше сфер жизни, способствуя развитию экономических отношений, в этой связи роль информационно-телекоммуникационной системы Интернет сложно переоценить [7]. Для пользователей Интернета остро стоит вопрос о безопасности персональных данных. Эти данные часто становятся мишенью для киберпреступников.

РОСТ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИИ

По данным InfoWatch (российской компании, специализирующейся на информационной безопасности), в 2023 году количество утечек конфиденциальных данных в мире увеличилось в 2,4 раза. Число скомпрометированных записей персональных данных возросло в 6 раз и достигло 18,3 миллиарда. В России этот показатель составил 705 миллионов[4].

Более того, по данным центра противодействия кибератакам Solar JSOC (ГК «Солар»), злоумышленники сформировали базу персональных данных на каждого жителя страны. Это может привести к активизации преступности в цифровой и информационной среде. В частности, повысится уровень мошенничества, шантажа, кибератак и число обзвонов граждан для введения их в заблуждение[5]. В ноябре 2024 года президент ПАО «Ростелеком» Михаил Осеевский заявил, что персональные данные абсолютно всех россиян уже продолжительное время находятся в открытом доступе[6].

---

[1] См. напр., Федеральный закон «О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» от 24.07.2023 № 339-ФЗ.

[2] См., напр., Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ.

[3] См., напр., Постановление Правительства Российской Федерации «Об утверждении Правил ведения реестра лиц, осуществляющих майнинг цифровой валюты, и Правил ведения реестра операторов майнинговой инфраструктуры» от 31.10.2024 № 1464.

[4] Доклад компании InfoWatch об утечках персональных данных в 2023 году. – URL: https://www.infowatch.ru/company/presscenter/news/chislo-utechek-personalnykh-dannykh-v-mire-uvelichilos-v-2-4-raza (дата обращения: 14.01.2025).

[5] ТАСС. Эксперт предупредил о возможном наличии базы почти на всех россиян у хакеров. – URL: https://tass.ru/ekonomika/21982447 (дата обращения: 14.01.2025).

[6] ТАСС. Глава «Ростелекома» считает, что личные данные всех россиян уже утекли в сеть – URL: https://tass.ru/ekonomika/22439315 (дата обращения: 14.01.2025).

Безусловно, привлечение всеобщего внимания к проблеме защиты информации и персональных данных частных лиц способствует запуску процессов изменений и в других сферах. Так, наряду с необходимостью внесения изменений в гражданское, уголовное, административное и законодательство сфере страхования неизбежные изменения произойдут в экономических отношениях между государством и гражданами, государством и коммерческими структурами, оказывающими комплексные услуги страхования. Это подтверждает Е. В. Михайлова, которая выделяет не только позитивные стороны цифровых ресурсов, но и отрицательные, например, новые способы уклонения от уплаты налогов и нарушения авторских прав [9]. Очевидно, что субъектам законотворчества необходимо реагировать на эти изменения и принимать соответствующие меры.

Одновременно с этим достижение успеха невозможно без привлечения компетентных специалистов в IT-отрасли, а также повышения соответствующих навыков у юристов и адвокатов.

МЕХАНИЗМ СТРАХОВАНИЯ КИБЕРРИСКОВ (КИБЕРСТРАХОВАНИЕ)

Законодатель пытается урегулировать распространение персональных данных в цифровой среде. Так, в 2024 году сенаторы предложили ввести понятие «киберстрахование» — страхование от киберрисков, связанных с утечкой и неправомерным использованием персональных данных. С помощью этого механизма граждане России могут начать получать компенсации в случае утечек своих персональных данных из ФГИС «Госуслуги». Выплачивать компенсации будет Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры РФ) из собственных средств, поскольку является оператором персональных данных. Важно, чтобы операторы, работающие с персональными данными, имели финансовое обеспечение для выплаты компенсаций в случае утечек данных и ущерба, причиненного гражданам. Что касается государственных организаций, то компенсации в пользу граждан также возможны: их могут выплачивать либо из бюджета, либо из финансовых средств непосредственного виновника утечки[7].

Компенсация за утечки данных — это важный аспект в области защиты данных и приватности. В современном цифровом мире, где персональная информация может быть скомпрометирована из-за кибератак, утечек данных или других сбоев в безопасности, компенсация является механизмом, который позволяет пострадавшим получить возмещение ущерба, понесенного в результате таких инцидентов.

В. Ф. Бадюков в своих работах приводит несколько исследований, подтверждающих опасность и перспективность вопросов утечек персональных данных еще в 2020 году. Отмечалось, что в силу отсутствия проработанной нормативно-правовой базы интерес российских компаний и предприятий к рынку страхования утечек персональных данных практически отсутствовал [1].

Западные страны разработали и применяют политику информационной безопасности как комплекс законотворческих, социально-экономических и общественных реформ, что, в свою очередь, позволяет нам рассуждать над используемыми понятиями: «киберриски», «киберпреступление» и «киберстрахование» [6].

Одно из коммерчески популярных решений за рубежом, которое позволяет защищать предприятия и частных лиц от финансовых потерь, вызванных подверженностью киберрискам, является киберстрахование (англ. cyber insurance). В частности, бизнес-решения

[7] РИА Новости. Россияне могут начать получать компенсации от «Госуслуг» за утечки данных. – URL: https://ria.ru/20240320/kompensatsii-1934374284.html (дата обращения: 14.01.2025).

в области киберстрахования диверсифицируют своих клиентов по типу киберрисков (высокий, средний, низкий). Кроме того, они позволяют покрывать свои собственные расходы и ответственность перед третьими лицами (например, ответственность электронных СМИ, сетевая безопасность, предотвращение утечек персональных данных и ответственность за конфиденциальность) [10].

Нужно отметить, что и в Российской Федерации делаются существенные шаги в решении указанных проблем. В течение всего 2024 года депутаты Государственной Думы ФС РФ обсуждали и принимали законопроекты, ужесточающие ответственность за утечки персональных данных. Теперь мера административной ответственности будет сопряжена с количеством незаконно распространенных сведений и информации о конкретном человеке[8]. В таблице 2 представлены количество субъектов (идентификаторов) и ответственность за неправомерную передачу информации (предоставление, распространение, доступ).

Таблица 2*

Количество субъектов (идентификаторов) персональных данных	Мера административной ответственности
От 1000 до 10 000 субъектов и (или) от 10 000 до 100 000 идентификаторов	Административный штраф на граждан в размере от 100 000 до 200 000 рублей; на должностных лиц — от 200 000 до 400 000 рублей; на юридических лиц — от 3 000 000 до 5 000 000 рублей
От 10 000 до 100 000 субъектов и (или) от 100 000 до 1 000 000 идентификаторов	Административный штраф на граждан в размере от 200 000 до 300 000 рублей; на должностных лиц — от 300 000 до 500 000 рублей; на юридических лиц — от 5 000 000 до 10 000 000 рублей
Более 100 000 субъектов и (или) более 1 000 000 идентификаторов	Административный штраф на граждан в размере от 300 000 до 400 000 рублей; на должностных лиц — от 400 000 до 600 000 рублей; на юридических лиц — от 10 000 000 до 15 000 000 рублей

* *Составлено (разработано) автором.*

Примечательно, что одновременно были внесены и соответствующие поправки в Уголовный кодекс[9]. Отныне за незаконное использование, передачу, сбор или хранение компьютерной информации, содержащей персональные данные, грозит штраф в размере 300 000–400 000 рублей или принудительные работы на срок до четырех лет, либо лишение свободы на срок до четырех лет.

Следует отметить, что государство приспосабливает действующее законодательство к современным реалиям, стремясь удовлетворить потребности общества в защите информации, и особенно — персональных данных граждан.

Однако ни одна из инициатив не сработает, если сами граждане не начнут ответственно относиться к безопасности своих персональных данных. В этой связи перед государством стоит задача не только разъяснить простым обывателям смысл проводимых реформ, но и сформировать у них необходимые компетенции, путем проведения ряда образовательных мероприятий.

Осуществление компенсационных выплат, так называемое страхование киберрисков, из средств бюджета в пользу гражданина, чьи персональные данные стали достоянием общественности, формирует представление о государстве, которое не только признает, но и уважает сведения каждого конкретного взятого гражданина. Киберстрахование в данном случае выступает как правовой и экономических механизм социальной направленности, не связанный с противоправными либо виновными действиями самого государства (государственных организаций и институтов). Этот механизм позволяет минимизировать негативные последствия от утечки персональных данных.

---

[8] Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 30.11.2024 № 420-ФЗ.

[9] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 30.11.2024 № 421-ФЗ.

Остаются неразрешенными вопросы о процедуре оценки страховых рисков и страховых случаев, критериях оценки размера компенсационной выплаты в зависимости от социального статуса потерпевшего гражданина либо от размера причиненного ущерба. Не стоит забывать, что гражданское законодательство и сложившаяся судебная практика испытывают определенные сложности с оценкой размера компенсации морального вреда, например, в сфере защиты авторских прав, либо компенсации вреда вследствие совершенных противоправных действий в отношении личности. Из-за отсутствия четких критериев оценки размера компенсации морального вреда в каждом конкретном случае размер компенсационной выплаты индивидуален[10].

Это же относится и к страховым выплатам, подлежащим выплате в случае кибератак на персональные данные, размещенные (хранящиеся), к примеру, во ФГИС «Госуслуги». В ходе расследования уголовных дел и привлечения виновных к ответственности государство правомочно восполнить бюджет для целей выплаты страховых возмещений, а также развития материально-технической базы и комплексного укрепления информационной безопасности.

Может ли идти речь о страховании, если утечка персональных данных произошла из-за халатного отношения, неисполнения требований информационной безопасности или нарушения положений Федерального закона о персональных данных сотрудниками ФГИС «Госуслуги», а также представителями иных государственных структур (организаций)? В этой связи обсуждению подлежит вопрос о наличии вины в тех или иных действиях (бездействии), вследствие которых произошло разглашение персональных данных, а также о пределах ответственности Минцифры РФ как крупнейшего оператора персональных данных.

В таком случае компенсация причиненного морального вреда и материального ущерба гражданину должна проходить через призму гражданско-правовой ответственности, а не через механизм страховых выплат. Процедура получения пострадавшим гражданином страховых выплат либо возмещение вреда (ущерба) из бюджета представляется надежной, скоротечной и гарантированной.

Данное нововведение является интересным дополнительным механизмом стимулирования государственных органов на примере Минцифры РФ и к повышению обеспечения уровня защищенности персональных данных, особенно в условиях участившихся случаев утечки такого рода информации [4]. Этот прецедент наилучшим образом отразится на изменении отношения государственных и коммерческих организаций к политике обеспечения безопасности персональных данных, а субъектам персональных данных наконец-то дадут возможность получения компенсации материального и морального вреда от неправомерного использования их данных.

Государственная Дума приняла законопроект об обязательном страховании вреда, причиненного искусственным интеллектом (ИИ), в рамках работы экспериментальных правовых режимов (ЭПР). Документ (№ 512628-8) правительство внесло в Государственную Думу в декабре 2023 г. Поправки вносятся в закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в РФ», а в июле 2024 год Президентом был подписан указ о введении этого режима[11].

Сейчас страхование рисков в ЭПР носит добровольный характер. «Программой экспериментального правового режима может предусматриваться требование к субъекту

---

[10] Определение Конституционного Суда РФ «Об отказе в принятии к рассмотрению жалобы гражданки Веретенниковой Анны Александровны на нарушение ее конституционных прав пунктом 2 статьи 1101 Гражданского кодекса Российской Федерации» от 15.07.2004 № 276-О.

[11] Федеральный закон «О внесении изменений в Федеральный закон „Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации“» от 08.07.2024 № 169-ФЗ.

экспериментального правового режима о необходимости страхования им гражданской ответственности за причинение указанного вреда при реализации экспериментального правового режима», — говорится в законе. Эту норму предлагается убрать и сделать страхование обязательным. «Программа ЭПР должна содержать (…) положения о страховании участниками ЭПР своей гражданской ответственности за причинение вреда жизни, здоровью или имуществу других лиц при реализации ЭПР, в том числе в результате использования решений, созданных с применением технологий искусственного интеллекта, а также требования к условиям такого страхования, в том числе к минимальному размеру страховой суммы, перечню рисков и страховых случаев», — говорится в принятом во втором чтении законопроекте.

ТЕХНОЛОГИЯ DEEPFAKE И НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН

Следующая технология, которую необходимо рассмотреть, — это DeepFake (англ. «глубокая подделка»). Она основана на использовании искусственного интеллекта и машинного обучения для создания фальшивых цифровых материалов, таких как видео, аудио или изображения, которые могут реалистично имитировать оригиналы. Очевидно, что в основе этих материалов часто лежат персональные данные граждан, которые с большой долей вероятности используются незаконно [8].

Существует несколько видов технологии DeepFake:

- FaceSwap — замена лица на видео с использованием глубоких нейронных сетей;
- Audio DeepFake — синтез речи, создание фейковых аудиозаписей, имитирующих голос человека;
- Text-to-Speech (TTS) — генерация речи из текстового ввода, с помощью которого можно создавать видео, где люди «произносят» вещи, которые они никогда не говорили.

Эта технология, безусловно, имеет преимущества и может помочь человечеству в решении различных задач. Однако в контексте исследования особый интерес представляют негативные последствия применения DeepFake и правовые механизмы их устранения. А. А. Бычинская и С. И. Иванова выделяют такие последствия, как манипуляции и обман; нарушение приватности; рост киберпреступлений [2].

В сентябре 2024 года в Государственную Думу было внесено сразу два законопроекта, направленных на защиту от дипфейков. Законопроект № 718538-8 «О внесении изменений в УК РФ» предлагает определить использование дипфейков как отягчающее обстоятельство для таких преступлений, как клевета (ст. 128.1), мошенничество (ст. 159), кража (ст. 158) вымогательство (ст. 163) и причинение имущественного ущерба (ст. 165). В случае принятия закона использование дипфейка по указанным выше статьям будет квалифицироваться судом как преступление, совершенное с отягчающими обстоятельствами, по которым наказание может быть увеличено. Например, за клевету штраф может быть поднят до 1,5 млн рублей (без отягчающих обстоятельств штраф за клевету ограничен 500 тыс. рублей), а за мошенничество срок лишения свободы может быть ужесточен до 6 лет (без отягчающих обстоятельств лишение свободы ограничено двумя годами)[12].

Второй законопроект, № 718834-8 «О внесении изменений в часть первую Гражданского кодекса Российской Федерации», вносит в ГК новую статью 152.3. «Охрана голоса

[12] Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности). – URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 14.01.2025).

гражданина»[13]. Она закрепляет за гражданином право распоряжаться записями своего голоса, в том числе и синтезированного с помощью искусственного интеллекта. Правда, предполагаются три исключения, если:

- использование голоса гражданина осуществляется в государственных, общественных или иных публичных интересах;
- голос гражданина записан при видео- или аудиозаписи, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях;
- запись голоса гражданина производилась за плату.

ЗАКЛЮЧЕНИЕ

Развитие новых технологий и способов взаимодействия с персональными данными представляет собой сложный и динамичный процесс, который требует непрерывного внимания и усилий со стороны государства, правоприменителей и самих граждан. Можно сказать, что правовые новации в этой сфере в России являются результатом динамичного процесса правотворчества, который отражает изменения в обществе и экономике. Правотворчество направлено на улучшение правового регулирования и создание более благоприятных условий для развития бизнеса, экономики и безопасности населения в цифровой среде.

На процесс правотворчества влияют как внутренние, так и внешние факторы, включая глобализацию, которая способствует интеграции российского законодательства в международную правовую систему. Государство играет ключевую роль в правотворчестве, обеспечивая разработку и принятие законодательных актов, а также контроль за их соблюдением.

Литература:

1. *Бадюков, В. Ф.* Риски цифровой экономики: особенности и перспективы развития киберстрахования в России / В. Ф. Бадюков, М. Н. Докучаев // Страховое право. – 2021. – № 1 (90). – С. 42–44. – EDN UKGJBK

2. *Бычинская, А. А.* Deepfake: новая реальность / А. А. Бычинская, С. И. Иванова // Новизна. Эксперимент. Традиции (Н.Экс.Т). – 2024. – Т. 10, № 2 (26). – С. 32–39. – EDN TGTRQG

3. *Вашурина, С. С.* Влияние цифровизации на конституционные права граждан / С. С. Вашурина // Теоретическая и прикладная юриспруденция. – 2024. – № 1 (19). – С. 74–83. – EDN EEVHNK

4. *Градобоева, П. А.* Утечка персональных данных в России / П. А. Градобоева // Молодой ученый. – 2024. – № 17 (516). – С. 179–181. – EDN NPTHXJ

5. *Гусева, С. Г.* Правотворчество: основные понятия и принципы / С. Г. Гусева, Т. Я. Коняхина // Вестник экономической безопасности. – 2016. – № 6. – С. 257–259. – EDN YLGJNB

6. *Казарин, О. В.* Современные концепции кибербезопасности ведущих зарубежных государств / О. В. Казарин, А. А. Тарасов // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2013. – № 14 (115). – С. 58–74. – EDN RLYGMT

[13] Законопроект № 718834-8 «О внесении изменений в часть первую Гражданского кодекса Российской Федерации» (об охране голоса). – URL: https://sozd.duma.gov.ru/bill/718834-8 (дата обращения: 14.01.2025).

7. *Михайлова, Е. В.* Цифровизация права в контексте его сущности и применения / Е. В. Михайлова // Теория и практика общественного развития. – 2021. – № 7 (161). – С. 83–86. – EDN OBWWXA
8. Распознавание Deepfake фотографий и видео с помощью глубокого обучения / К. В. Санталов, О. В. Панкратьева, И. Д. Котилевец, И. И. Иванова // Управление в современных системах: сборник трудов XI Всероссийской (национальной) научно-практической конференции научных, научно-педагогических работников и аспирантов. Челябинск, 15 декабря 2021 года. – Челябинск: Южно-Уральский технологический университет, 2021. – С. 332–340. – EDN EKOVHC
9. *Фроленко, Н. А.* Цифровизация права: процессы цифровизации и ее особенности / Н. А. Фроленко, Ю. В. Осипова // Вестник науки. – 2024. – Т. 2, № 2 (71). – С. 184–188. – EDN LAUBTI
10. Ranjan Pal, Peihan Liu, Taoan Lu, and Ed Hua. (2023) How Hard Is Cyber-risk Management in IT/OT Systems? A Theory to Classify and Conquer Hardness of Insuring ICSs. ACM Trans. Cyber-Phys. Syst. 6, 4, Article 35 (October 2022), 31 pages. https://doi.org/10.1145/3568399

References:

1. Badyukov V. F., Dokuchaev M. N. risks of digital economy: features and prospects of development of cyber insurance in Russia. – 2021. – No. 1(90). – Pp. 42–44. – EDN UKGJBK.
2. Bychinskaya A. A., Ivanova S. I. (2024) Deepfake: new reality // Novelty. Experiment. Traditions (N. Ex.T). – Vol. 10, No. 2 (26). – Pp. 32–39. – (In Russ.) – EDN TGTRQG
3. Vashurina S. S. (2024) Influence of digitalization on constitutional rights of citizens // Theoretical and applied jurisprudence. – No. 1 (19). – Pp. 74–83. – (In Russ.) – EDN EEVHNK
4. Gradoboeva P. A. (2024) Utechka personal data in Russia // Young Scientist. – No. 17 (516). – Pp. 179–181. – (In Russ.) – EDN NPTHXJ
5. Guseva S. G., Konyakhina T. Ya. (2026) Pravotvorchestvo: osnovy kontseptsii i principy [law-making: basic concepts and principles]. Vestnik ekonomicheskoi Bezopasnosti [Bulletin of economic security]. – No. 6. – Pp. 257–259. – (In Russ.) – EDN YLGJNB
6. Kazarin O. V., Tarasov A. A. (2013) Sovremennye kontseptsii kiberbezopasnosti vedushchikh zarubezhnykh gosudarstv [modern concepts of cyber security of leading foreign states]. Series: document Science and archiving. Informatics. Information protection and information security. – No. 14 (115). – Pp. 58–74. – (In Russ.) – EDN RLYGMT
7. Mikhailova E. V. (2021) Digitalization of law in the context of its essence and application // Theory and practice of Social Development. – No. 7 (161). – Pp. 83–86. – (In Russ.) – EDN OBWWXA
8. Recognition of deepfake photos and videos with the help of deep learning (2021) / K. V. Santalov, O. V. Pankratieva, I. D. Kotilevets, I. I. Ivanova // Management in modern systems: a collection of works of the XI all-Russian (national) scientific and Practical Conference of scientific, scientific and pedagogical workers and aspirants. Chelyabinsk, December 15, 2021. Chelyabinsk: South Ural Technological University. – Pp. 332–340. – (In Russ.) – EDN EKOVHC
9. Frolenko N. A., Osipova Yu. V. (2024) Digitalization of law: processes of digitalization and its features // Vestnik nauki. – Vol. 2, No. 2 (71). – Pp. 184–188. – (In Russ.) – EDN LAUBTI

10. Ranjan Pal, Peihan Liu, Taoan Lu, and Ed Hua. (2023) How Hard Is Cyber-risk Management in IT/OT Systems? A Theory to Classify and Conquer Hardness of Insuring ICSs. ACM Trans. Cyber-Phys. Syst. 6, 4, Article 35 (October 2022). – 31 p. – https://doi.org/10.1145/3568399

Для цитирования / For citation:
Булочников С. Ю. О правотворчестве и правовых новациях в части защиты от утечек персональных данных // Новизна. Эксперимент. Традиции (Н.Экс.Т). – 2025. – Т. 11. – № 1 (29). – С. 6–15.