Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет юридический
Кафедра теории и истории государства и права
Направление подготовки 40.04.01 – Юриспруденция
Направленность (профиль) образовательной программы: Теория и история государства и права, история правовых учений

ДОПУСТИТЬ К ЗАЩИТЕ
И.о. зав. кафедрой
_____ Е.Ю. Титлина
«3» июля 2023 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему: Трансформация правовой реальности в цифровую эпоху

Исполнитель
студент группы 121 ом _____ (подпись, дата) М.А. Катаев

Руководитель
канд.юрид.наук, доцент _____ (подпись, дата) А.В. Швец

Руководитель научного
содержания программы
магистратуры
док.филос.наук, профессор _____ (подпись, дата) И.Ю. Куляскина

Нормоконтроль _____ (подпись, дата) О.В. Громова

Рецензент _____ (подпись, дата) Д.А. Лисниченко

Благовещенск 2023

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет юридический
Кафедра теории и истории государства и права

УТВЕРЖДАЮ
И. о. зав. кафедрой
Е. Ю. Титлина
«10» октября 2021 г.

З А Д А Н И Е

К выпускной квалификационной работе студента Катаева Максима Александровича .

1. Тема выпускной квалификационной работы: Трансформация правовой реальности в цифровую эпоху (утверждена приказом от 24.04.2023 г. № 974-уч).

2. Срок сдачи студентом законченной работы: 20.06.2023 г.

3. Исходные данные к выпускной квалификационной работе: Конституция РФ, иные правовые акты, учебная и научная литература, публикации в периодических изданиях.

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов): история цифровизации в юридической сфере; преимущества и недостатки цифровизации в юридической отрасли; роль искусственного интеллекта в юридической отрасли; трансформация правовой реальности в цифровую эпоху; правовая культуры при цифровой трансформации; проблемы безопасности данных и конфиденциальности в цифровую эпоху юриспруденции; пути совершенствования прина и способов адаптации юристов к цифровой эпохе.

5. Перечень материалов приложения (наличие чертежей таблиц графиков схем программных продуктов иллюстрированного материала и т.п.): нет.

6. Консультанты по выпускной квалификационной работе (с указанием относящихся к ним разделов): нет.

7. Дата выдачи задания: 04.10.2021 г.

Руководитель выпускной квалификационной работы: Швец Александр Витальевич, канд. юрид. наук, доцент.

Задание принял к исполнению (дата): 04.10.2021 г. _____
(подпись студента)

2

РЕФЕРАТ

Магистерская работа содержит 65 с., 4 рисунка, 3 таблицы, 55 источника.

ЦИФРОВИЗАЦИЯ, ПРАВО, ПРАВОВАЯ СФЕРА, ЦИФРОВОЕ ПРАВО, ТРАНСФОРМАЦИЯ ПРАВОВОЙ РЕАЛЬНОСТИ, ЦИФРОВАЯ ЭКОНОМИКА, БОЛЬШИЕ ДАННЫЕ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Цель магистерской работы – выявление и обоснование теоретических и практических аспектов цифровизации права, выявление преимуществ и потенциальных недостатков трансформации правовой реальности в цифровую эпоху, включая проблемы конфиденциальности и безопасности данных.

В работе рассмотрены теоретические и правовые основы цифровизации права. Проведен анализ наличия цифровых технологий в юридической сфере и их влияния на работу юристов, а также рассмотрены исторические примеры внедрения цифровизации в юридическую отрасль. Выявлены проблемы цифровизации права и предложены пути решения данных проблем.

Практическая значимость работы. Содержащиеся в работе положения могут быть положены в основу дальнейших исследований в сфере трансформации правовой реальности в цифровую эпоху.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Трансформация правовой реальности в цифровую эпоху является актуальной темой из-за растущей потребности в эффективной и быстрой обработке больших объёмов данных, а также ускорения процессов в сфере юриспруденции. В условиях развития цифровых технологий исчезает необходимость в бумажном документообороте, что облегчает работу юристов и судей. Она позволяет автоматизировать рутинные задачи, ускоряет процесс принятия решений и уменьшает вероятность ошибок. Кроме того, цифровые технологии могут помочь в борьбе с коррупцией и неэффективностью судебной системы. Все это позволяет улучшить качество правосудия и обеспечить быстрое и справедливое решение юридических вопросов.

Цифровизация права является одной из наиболее актуальных тем в современном мире, поскольку она непосредственно связана с технологическими изменениями и новыми возможностями, которые они предоставляют.

Цель магистерской работы – выявление и обоснование теоретических и практических аспектов цифровизации права, выявление преимуществ и потенциальных недостатков трансформации правовой реальности в цифровую эпоху, включая проблемы конфиденциальности и безопасности данных.

В соответствии с поставленной целью были определены **следующие задачи:**

1. Анализ истории цифровизации в юридической сфере.
2. Анализ изменений законов и правил, регулирующих использование технологий в юридической сфере.
3. Определение преимущества и выявление недостатков цифровизации в юридической отрасли.
4. Рассмотрение влияния цифровизации на юридическое образование.
5. Определение будущего цифровизации в юридической отрасли.
6. Анализ трансформации правовой реальности в цифровую эпоху.
7. Рассмотрение правовой культуры при цифровой трансформации.

8. Оценка влияния цифровизации на юридическую отрасль и граждан.

9. Изучение проблем безопасности данных и конфиденциальности в цифровую эпоху юриспруденции.

10. Определение путей совершенствования права и способов адаптации юристов к цифровой эпохе.

Объектом исследования является общественные отношения, возникающие при воздействии цифровизации на правовую реальность.

Предметом исследования являются новые технологии в юридической отрасли, их применение и влияние на работу юристов, изменения в законодательстве и правилах, возможности цифровизации процессов в юридической сфере, методы обеспечения безопасности данных клиентов при использовании новых технологий и способы использования новых технологий для повышения эффективности работы в юридической сфере.

Степень изученности.

Теоретико-методологическая основа диссертационного исследования представлена различными группами научных методов: общенаучными, общелогическими, частно-научными.

В исследовании используются метод анализа и синтеза, а также метод индукции.

В диссертации используется герменевтический метод, который плодотворно применяется в историко-правовых исследованиях.

Также в работе применялись такие методы, как: описание; статистический метод; графический метод; сравнительный метод.

Основные положения, выносимые на защиту:

1. Цифровизация правовой реальности является неизбежным процессом в современном обществе, в следствии которой возникает необходимость пересмотра и изменения существующих правовых норм и механизмов регулирования цифровых отношений.

2. В цифровой эпохе возникают новые правовые проблемы, связанные с защитой личных данных, киберпреступностью, электронно-цифровыми подпи-

сями и другими аспектами цифровых технологий.

3. Одной из основных задач правовой реформы в цифровую эпоху является обеспечение баланса между защитой прав и свобод граждан в цифровой среде и необходимостью обеспечения безопасности и стабильности цифровой инфраструктуры.

4. Для успешной трансформации правовой реальности в цифровую эпоху необходимо учитывать интересы всех заинтересованных сторон, включая государственные органы, бизнес-сообщество, научное сообщество и гражданское общество.

5. Применение цифровых технологий позволяет автоматизировать повседневные задачи, сокращает время на принятие решений и снижает вероятность ошибок. Кроме того, применение цифровых технологий может помочь в борьбе с коррупцией и неэффективностью судебной системы.

6. Цифровизация приносит значительные изменения в юридическую отрасль, повышая эффективность и доступность юридических услуг.

Научная новизна диссертационного исследования заключается в том, что на основе проведенного многоаспектного, целостного, теоретико-правового анализа содержательной специфики трансформации правовой реальности в цифровую эпоху определены пути совершенствования права и способов адаптации юристов к цифровой эпохе.

Теоретическая и практическая значимость исследования:

1. Теоретическая значимость исследования заключается в том, что оно позволяет раскрыть сущность и особенности трансформации правовой реальности в цифровую эпоху. Это помогает лучше понимать изменения, которые происходят в правовой системе и влияют на жизнь людей.

2. При проведении анализа реализации цифровых технологий, юристы могут оценить их преимущества, такие как быстрота и доступность юридической помощи, более эффективное управление документами. Кроме того, цифровизация может обеспечить лучшую прозрачность процесса работы и повысить уровень доверия граждан к юридическим услугам.

3. Практическая значимость исследования заключается в том, что оно может быть использовано для разработки новых правовых норм и принятия решений в сфере права. Также оно может помочь компаниям и организациям адаптироваться к новым технологиям и изменениям в правовой системе.

4. Разработка рабочих процессов, которые учитывают потенциальные уязвимости цифровых сервисов и платформ, обучение юристов работе с безопасностью данных, а также использование специализированных технологий и инструментов защиты.

5. Исследование имеет большое значение для общества, так как позволяет лучше понимать, как изменения в технологиях и информационных системах влияют на правовую систему и как право должно адаптироваться к новым условиям.

Структура диссертации определена характером исследуемых в ней проблем и следует логике их изложения. Работа состоит из введения, трех глав, включающих в себя 10 параграфов, заключения и библиографического списка.

1 СТАНОВЛЕНИЕ И РАЗВИТИЕ ЦИФРОВИЗАЦИИ В ЮРИДИЧЕСКОЙ СФЕРЕ

1.1 История цифровизации в юридической сфере

Историю цифровизации в юридической профессии можно проследить с 1970-х годов, когда компьютеры впервые появились в юридических фирмах. В то время компьютеры использовались в основном для обработки текстов и документооборота. Однако по мере развития технологий компьютеры становились все более сложными, а их возможности расширялись.

В 1990-х годах Интернет стал широко доступен, и юридические фирмы быстро осознали потенциал этой новой технологии. Интернет позволил юридическим фирмам общаться с клиентами и другими специалистами в области права в режиме реального времени, повышая скорость и эффективность юридических услуг.

Внедрение облачных вычислений в начале 2000-х годов стало еще одной важной веткой в развитии юридической отрасли. Облачные вычисления позволили юридическим фирмам хранить и получать доступ к данным и документам из любого места и в любое время. Эта технология позволила специалистам в области права сотрудничать и обмениваться информацией с клиентами и другими специалистами в области права по всему миру.

После появления компьютеров и интернета было принято множество законов, которые регулируют их использование.

Закон об авторском праве в цифровую эпоху (Digital Millennium Copyright Act) - принятый в США в 1998 году для того, чтобы регулировать использование авторских прав в онлайн-среде. Он устанавливает ответственность за нарушение авторских прав, включая запрет на обход технологий защиты авторских прав, таких как шифрование.

Закон об информационной безопасности (Federal Information Security Management Act) - принятый в США в 2002 году для того, чтобы обеспечить защиту информации в государственных организациях. Он требует от государ-

ственных организаций установки мер безопасности для защиты конфиденциальной информации и регулярного аудита систем безопасности.

Европейский закон о защите персональных данных (General Data Protection Regulation) - принятый в 2018 году, он устанавливает правила сбора, хранения и использования персональных данных пользователей в Европейском Союзе. Он требует согласия пользователей на обработку и использование их данных, а также обязует компании обеспечивать безопасность и конфиденциальность этих данных.

Законы о киберпреступлениях, принятые в различных странах, устанавливают ответственность за киберпреступления, такие как хакерство, фишинг, распространение вредоносного программного обеспечения и другие виды информационных преступлений. Он предусматривает штрафы и наказания для лиц, совершивших такие действия.

По Уголовному кодексу Российской Федерации от 13.06.1996 № 63-ФЗ[1] преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). В 2012 году в Уголовный кодекс Российской Федерации были введены статьи, регламентирующие уголовную ответственность за различные виды кибермошенничества (статьи 159.3 и 159.6 УК РФ), формально не относящиеся к 28 главе Уголовного кодекса.

Законы об электронной коммерции, приняты в различных странах. Они устанавливают правила проведения бизнеса в онлайн-среде, включая правила продажи товаров и услуг, защиты потребителей и т.д. Они также требуют от компаний соблюдать правила конфиденциальности и безопасности при обработке персональных данных пользователей.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 13.06.2023) (с изм. и доп., вступ. в силу с 24.06.2023) [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

В соответствии с законодательством Российской Федерации, существуют документы, которые регулируют электронную торговлю:

1) федеральный закон "О контрактной системе в сфере закупок" от 05 04.2013 г № 44-ФЗ[2];

2) федеральный закон "О защите прав потребителей" от 07.02.1992 г. № 2300-1[3];

3) федеральный закон "Об электронной подписи" от 06.04.2011 № 63-ФЗ[4];

4) федеральный законом "О техническом регулировании" от 27.12.2002 г. № 184-ФЗ[5].

И иными федеральными законами и нормативными правовыми актами Российской Федерации, а также соглашениями сторон.

Эти документы содержат конкретные и узконаправленные рекомендации по проведению торгов по тем или иным вопросам. Для создания общей базы ведения электронной торговли разрабатывался отдельный проект закона, который был внесен на рассмотрение 3 октября 2000 года, однако до сих пор не принят.

Это лишь некоторые примеры законов, которые были приняты после появления компьютеров и интернета.

Идея создания электронного правительства в России появилась еще в 2000-х годах, когда начали разрабатываться первые проекты государственных порталов и информационных систем. В 2010 году была принята Федеральная целевая программа «Электронная Россия», которая предусматривала создание единой информационной среды для государственных органов и населения.

В 2002 году был принят закон "Об электронной подписи", который уста-

---

[2] Федеральный закон от 05.04.2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

[3] Федеральный закон от 07.02.1992 г. № 2300-1 «О защите прав потребителей» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

[4] Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

[5] Федеральный закон от 27.12.2002 г. № 184-ФЗ «О техническом регулировании» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

новил правила использования электронных документов и подписей в государственных органах и между гражданами и организациями.

Использование электронной подписи в электронных документах регулируется законодательством Российской Федерации. Основными правовыми документами, которые регулируют использование электронной подписи, являются:

1) федеральный закон «Об электронной подписи» от 10 января 2002 года № 63-ФЗ;

2) постановление Правительства РФ «Об утверждении Правил использования электронной подписи при осуществлении государственных и муниципальных услуг» от 6 февраля 2002 года № 81[6];

3) приказ Министерства экономического развития РФ «Об утверждении требований к созданию, использованию и проверке электронной подписи» от 6 февраля 2015 года № 54[7].

Согласно законодательству РФ, электронная подпись имеет такую же юридическую силу, как и собственноручная подпись на бумажном документе. Это означает, что электронный документ, подписанный электронной подписью, имеет юридическую силу и может использоваться в судебных процессах.

Для того чтобы использовать электронную подпись, необходимо получить квалифицированный сертификат ключа подписи у аккредитованного удостоверяющего центра. Квалифицированный сертификат ключа подписи является основным документом, который подтверждает личность владельца электронной подписи и его право подписывать электронные документы.

Без процедуры аутентификации невозможно гарантировать информационную безопасность, а использование мобильных устройств и облачных технологий подвергает этот принцип риску. Аутентификация — это процедура, подтверждающая подлинность субъекта в информационной системе на основе

[6] Постановление Правительства РФ от 6.02.2002 г. № 81 «Об утверждении Правил использования электронной подписи при осуществлении государственных и муниципальных услуг» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

[7] Приказ Министерства экономического развития РФ от 6.02.2015 г. № 54 «Об утверждении требований к созданию, использованию и проверке электронной подписи» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

идентификатора, которая предоставлена на рисунке 1.

Рисунок 1 - Идентификация и аутентификация с точки зрения применяемых технологий

Кроме того, законодательство устанавливает требования к созданию, использованию и проверке электронной подписи. Например, для создания электронной подписи необходимо использовать криптографические алгоритмы, которые обеспечивают надежную защиту от подделки или изменения электронного документа.

Также законодательство предусматривает ответственность за незаконное использование электронной подписи. Например, если владелец электронной подписи передал ее третьим лицам без разрешения или использовал ее для подписания документов, которые не имеют юридической силы, то он может быть привлечен к ответственности в соответствии с законодательством.

15 декабря 2009 года был создан Федеральный портал государственных услуг[8], который стал центральным элементом электронного правительства. К концу 2011 года на портале госуслуг было размещено 34 319 услуг, включая оформление паспорта, регистрацию автомобиля, подачу налоговой декларации и многое другое.

[8] Портал государственных услуг Российской Федерации [Электронный ресурс]. URL : https://www.gosuslugi.ru/ (дата обращения : 01.03.2023).

Использование государственных услуг через портал государственных услуг регулируется Федеральным законом «Об организации предоставления государственных и муниципальных услуг» от 27 июля 2010 года № 210-ФЗ[9]. В соответствии с этим законом, государственные органы и организации обязаны предоставлять государственные и муниципальные услуги через портал госуслуг.

Пользователи имеют право на получение информации о порядке предоставления услуг, а также на обращение в государственные органы и организации через портал госуслуг. Закон также устанавливает требования к качеству предоставляемых услуг и обеспечению безопасности информации, а также правила использования электронной подписи.

В случае нарушения прав пользователей или несоблюдения законодательства Российской Федерации, государственные органы и организации могут быть привлечены к ответственности в соответствии с законодательством.

В 2016 году была запущена новая версия Федерального портала государственных услуг, которая стала более удобной и функциональной. Также была запущена система электронных очередей в государственные органы, которая позволяет избежать долгих ожиданий и ускорить получение государственных услуг.

Сегодня электронное правительство в России продолжает развиваться и совершенствоваться. Оно позволяет ускорить и упростить получение государственных услуг, сократить бюрократию и повысить прозрачность работы государственных органов.

Вместе с этим продолжается цифровизация в юридической сфере, и новые технологии, такие как искусственный интеллект и блокчейн. Искусственный интеллект может помочь юристам автоматизировать рутинные задачи, такие как анализ документов и поиск информации в базах данных. Блокчейн — это технология распределенного реестра, которая позволяет сохранять данные в

[9] Федеральный закон от 27.07. 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг [Электронный ресурс] : Доступ из справ.-правовой системы «КонсультантПлюс».

цепочке блоков, каждый из которых содержит информацию о предыдущем блоке. Это обеспечивает безопасность и надежность хранения данных, так как любые изменения в блокчейне должны быть подтверждены всеми участниками сети. В юридической сфере блокчейн может использоваться для хранения данных о сделках и контрактах, а также для обеспечения безопасности при работе с данными клиентов и контрактах.

Блокчейн-система предусматривает проведение транзакций в несколько этапов. Пользователь отправляет запрос на проведение операции, используя специальный зашифрованный ключ, содержащий информацию о типе операции, ее целях и сторонах. Затем данные отправляются в P2P-сеть, состоящую из узлов сети, которые подтверждают достоверность информации.

P2P-сеть (peer-to-peer) — это сеть, в которой компьютеры взаимодействуют друг с другом напрямую, без центрального сервера. Каждый компьютер в сети может быть одновременно и клиентом, и сервером, т.е. он может как запрашивать информацию у других компьютеров, так и предоставлять ее. В P2P-сетях нет централизованного управления, что делает их более устойчивыми к отказам и более сложными для блокировки и контроля со стороны внешних организаций. P2P-сети широко используются для обмена файлами, музыкой, видео и другой информацией.

Сеть проверяет транзакцию по определенному алгоритму и позволяет осуществить передачу информации, например, сделку в криптовалюте. После успешного подтверждения транзакции в цепочку блоков добавляется новый блок, содержащий сведения об операции и ссылку на предыдущий блок. Каждый блок содержит неизменяемую информацию, что обеспечивает надежность и безопасность проведенных транзакций. Все это позволяет обеспечивать прозрачность, надежность и безопасность при проведении операций в блокчейн-системе.

Подробная схема использования блокчейн технологий для проведения транзакций, с описанием каждого этапа, предоставлена на рисунке 2. Варианты применения блокчейн технологий предоставлены на рисунке 3.

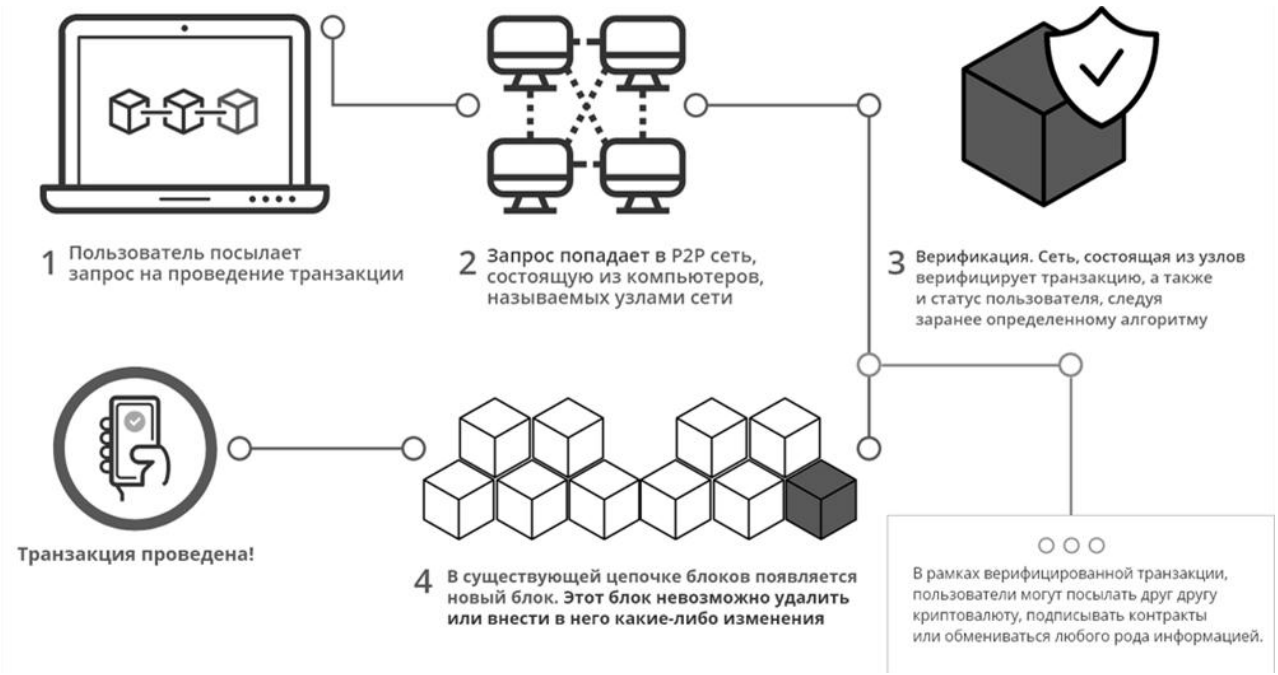

Рисунок 2 - Схема использования блокчейн технологий для проведения транзакций.

Рисунок 3 – Варианты применения блокчейн технологий.

Примером использования новых технологий служит компания LegalTech — это технологические решения, применяемые в сфере права, которые позволяют автоматизировать и ускорить процессы юридической работы. В России LegalTech начал активно развиваться в последние годы, и сейчас на рынке представлено множество стартапов и компаний, которые предлагают различные

решения для автоматизации юридических процессов.

Одним из наиболее популярных направлений LegalTech в России является электронная подпись и документооборот. Например, компания DocuSign предлагает решения для электронной подписи документов, а компания Pravo.ru[10] - сервис для электронного документооборота между юридическими лицами.

Также в России развиваются LegalTech-платформы, которые позволяют автоматизировать процессы поиска и анализа юридической информации. Например, компания LexisNexis предлагает онлайн-базу данных юридической информации, содержит законодательство, комментарии, судебные дела, онлайн-книги и формы договоров. Экспертная организация Автономная некоммерческая организация «Право Роботов» осуществляет научную и аналитическую работу в области развития российского законодательства. Основная цель АНО «Право Роботов» - повышение качества законодательства, обеспечение его соответствия современным вызовам и потребностям общества, а также поддержание правовой стабильности и предсказуемости в России. Для достижения этой цели организация проводит исследования, анализирует законодательные акты и предлагает свои рекомендации и решения по улучшению существующих правовых норм. Кроме того, АНО «Право Роботов» занимается информационной поддержкой процесса правотворчества и обеспечением доступа к актуальной правовой информации для широкой аудитории.

В целом, LegalTech в России только начинает свой путь, но уже сейчас можно сказать, что это перспективное направление, которое будет активно развиваться в ближайшие годы.

Цифровизация юридической профессии позволяет увеличить эффективность работы юристов, сократить время на выполнение задач и повысить качество услуг. Однако для успешной реализации цифровизации необходимо учитывать все проблемы и препятствия, которые могут возникнуть на этом пути.

[10] Законодательство, судебная система, новости и аналитика. Все о юридическом рынке [Электронный ресурс]. URL : https://www. pravo.ru. (дата обращения : 15.03.2023).

Важно обеспечить безопасность данных, обучить кадры работе с новыми технологиями и использовать доступные решения для малых и средних юридических фирм.

На сегодняшний день можно выделить следующие этапы развития цифровизации в юриспруденции, которые предоставлены в таблице 1.

Таблица 1 - Этапы развития цифровизации в юриспруденции

Технологии	Влияние на юридическую сферу
1. Автоматизация рутинных задач.	Юристы начинают использовать программы для автоматизации рутинных задач, таких как заполнение форм и документов, подготовка документации и т.д.
2. Облачные технологии.	Юридические фирмы начинают использовать облачные технологии для хранения и обмена документами, что упрощает работу с клиентами и позволяет получать доступ к документам из любой точки мира.
3. Искусственный интеллект.	Новые технологии, такие как искусственный интеллект, помогают юристам автоматизировать рутинные задачи, такие как анализ документов и поиск информации в базах данных.
4. Блокчейн.	Блокчейн позволяет обеспечить безопасность и надежность хранения данных о сделках и контрактах, что повышает уровень доверия к услугам юридических фирм.
5. Цифровые подписи.	Введение цифровых подписей позволяет сократить время на подписание документов и повысить уровень безопасности при работе с документами.
6. Виртуальные помощники.	Юридические фирмы начинают использовать виртуальных помощников для работы с клиентами и обработки запросов.
7. Big Data и аналитика.	Анализ больших данных помогает юристам принимать более обоснованные решения и предсказывать возможные проблемы в будущем.
8. Мобильные приложения.	Развитие мобильных технологий позволяет юристам работать удаленно и получать доступ к документам и базам данных из любой точки мира.
9. Обучение кадров.	Обучение кадров работе с новыми технологиями становится необходимостью для успешной реализации цифровизации в юриспруденции.

Продолжение таблицы 1

Технологии	Влияние на юридическую сферу
10. Развитие экосистемы цифровых сервисов для юридических фирм.	Развитие экосистемы цифровых сервисов для юридических фирм позволяет использовать доступные решения для малых и средних юридических фирм и повышает эффективность работы всей отрасли.

1.2 Преимущества и недостатки цифровизации в юридической отрасли

Цифровизация принесла множество преимуществ юридической отрасли. Одним из наиболее значимых преимуществ является повышение эффективности. Цифровизация позволила специалистам в области права работать более эффективно, сокращая время и расходы, связанные с традиционными бумажными системами. Например, электронные системы подачи документов сократили время и расходы, связанные с подачей документов и состязательных бумаг.

Цифровизация в юридической отрасли имеет множество преимуществ:

1. Ускорение процессов: электронные системы позволяют сократить время на обработку документов и ускорить процессы рассмотрения дел.

2. Улучшение качества услуг: цифровые технологии позволяют сократить количество ошибок и повысить точность рассмотрения дел.

3. Снижение затрат: использование электронных систем позволяет сократить расходы на бумажную документацию, пересылку почтой и другие затраты.

4. Удобство для пользователей: электронные системы позволяют получать услуги в любое время и из любой точки мира, что делает процесс получения услуг более удобным для пользователей.

5. Увеличение прозрачности: цифровые системы позволяют увеличить прозрачность работы государственных органов и обеспечить доступность информации для граждан.

6. Улучшение безопасности: использование электронных систем позво-

ляет обеспечить защиту от несанкционированного доступа к информации и предотвратить возможные фальсификации документов.

Таким образом, цифровизация в юридической отрасли является важным шагом к повышению качества и доступности юридических услуг, ускорению процессов и повышению прозрачности работы государственных органов.

Цифровизация также повысила доступность юридических услуг. С ростом использования цифровых платформ доступ к юридическим услугам теперь можно получить удаленно, что облегчает людям доступ к юридическим услугам независимо от их местонахождения. Это позволило юридическим фирмам расширить сферу своей деятельности и предложить свои услуги более широкой аудитории.

Несмотря на многочисленные преимущества цифровизации, существуют и потенциальные недостатки, которые необходимо учитывать. Проблемы конфиденциальности и безопасности данных - одна из самых серьезных проблем, связанных с цифровизацией в юридической отрасли. Юридические документы содержат чувствительную и конфиденциальную информацию, и если эта информация попадет в чужие руки, это может иметь серьезные последствия.

Еще одним потенциальным недостатком цифровизации является риск ошибок и сбоев. Цифровые системы не являются совершенными и в них могут возникать ошибки. Если эти ошибки останутся незамеченными, они могут привести к серьезным последствиям.

Например, ошибки в финансовых системах могут привести к потере денег или конфиденциальной информации, что нанесет ущерб компании и ее клиентам. Также сбои в цифровых системах могут привести к остановке производства, ошибках в медицинских диагнозах или даже к авариям на дорогах, если речь идет о системах автоматизированного управления транспортом. Поэтому очень важно следить за качеством и надежностью цифровых систем и своевременно выявлять, и устранять возможные ошибки или сбои.

На примере портала «Госуслуги» можно увидеть самые частые проблемы, такие как технические сбои и ошибки на сайте, не позволяющие пользователю

зарегистрироваться или оформить заявку, недостаточная информация о процессе оформления заявки или услуги, что может привести к запутанности в процессе использования сервиса, отсутствие оперативности в предоставлении информации о статусе заявки, приводит к длительным ожиданиям, недостаточная обратная связь, отзывчивость и внимание к клиентам со стороны службы технической поддержки. Общая доля частых проблем портала «Госуслуги» предоставлена на рисунке 4.

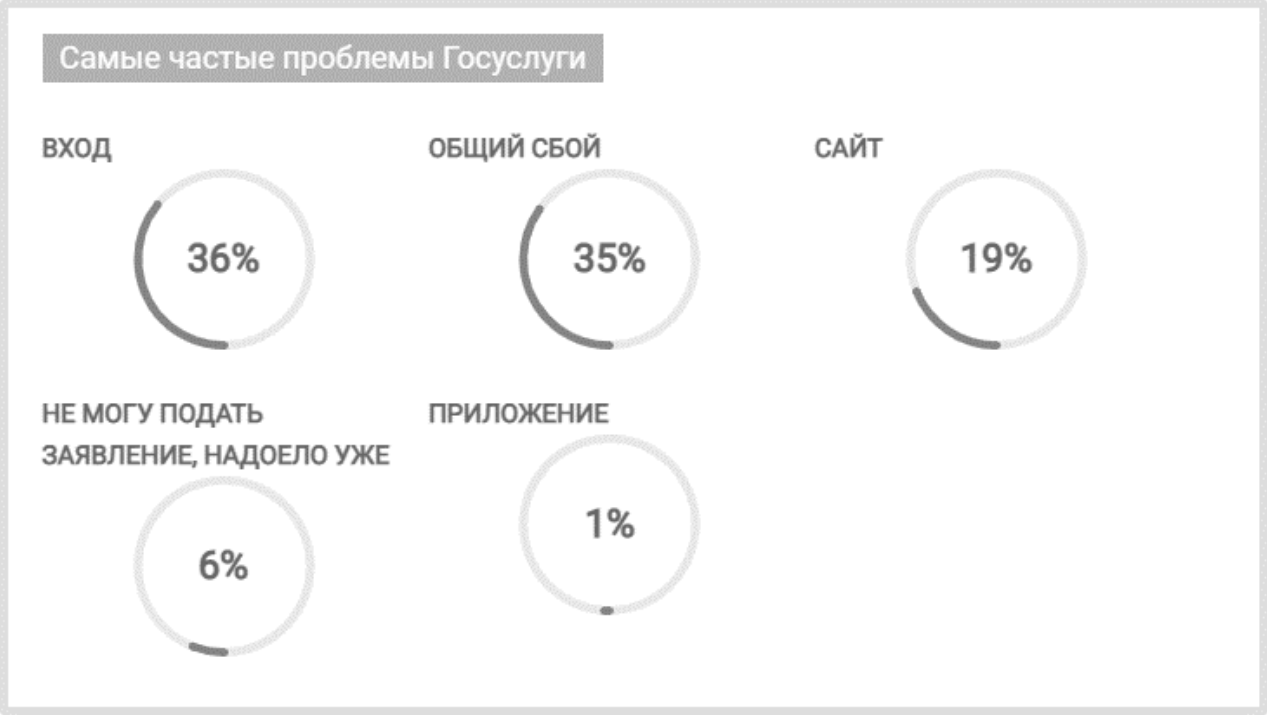

Рисунок 4 - Самые частые проблемы портала «Госуслуги».

Несмотря на множество преимуществ, цифровизация в юридической отрасли также имеет некоторые недостатки:

1. Необходимость обучения: внедрение электронных систем требует обучения персонала и пользователей, что может занять время и стоить дополнительных затрат.

2. Риск потери данных: использование электронных систем может повысить риск потери данных из-за возможных технических сбоев или кибератак.

3. Необходимость обновления: электронные системы требуют постоянного обновления и совершенствования, что также может стать дополнительной

нагрузкой для организаций.

4. Недоступность для некоторых пользователей: не все пользователи могут иметь доступ к электронным системам из-за отсутствия технической возможности или навыков работы с ними.

5. Риск ошибок: автоматизация процессов может привести к возникновению ошибок из-за неправильной настройки или программирования систем.

6. Нарушение конфиденциальности: использование электронных систем может привести к нарушению конфиденциальности информации, если не будут соблюдены соответствующие меры безопасности.

Таким образом, при внедрении цифровых технологий в юридическую отрасль необходимо учитывать как их преимущества, так и недостатки, чтобы обеспечить более эффективную и безопасную работу организаций.

2 СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В ЮРИСПРУДЕНЦИИ

2.1 Роль искусственного интеллекта в юридической отрасли

В последние годы искусственный интеллект становится все более распространенным в юридической отрасли. искусственный интеллект используется для автоматизации повторяющихся задач, таких как анализ документов, юридические исследования и анализ договоров. Эта технология способна значительно повысить эффективность и точность юридических услуг.

Однако использование искусственный интеллект в юридической отрасли также вызывает опасения по поводу перемещения рабочих мест. Некоторые специалисты в области права беспокоятся, что растущее использование искусственный интеллект может привести к сокращению рабочих мест в отрасли.

Существует также опасение, что искусственный интеллект может привести к снижению качества юридических услуг. Так же, использование искусственного интеллекта может включать риски и ограничения, такие как недостаток этических стандартов или ошибки в алгоритмах обработки данных. Поэтому искусственный интеллект, необходимо использовать с осторожностью и учитывать возможные риски при его применении в юридической практике.

Искусственный интеллект играет все более важную роль в юридической отрасли, ускоряя и упрощая процессы и повышая точность принятия решений. Вот некоторые из областей предоставлены в таблице 2, в которых искусственный интеллект уже может использоваться в юридической практике.

Таблица 2 – Возможности использования искусственного интеллекта

Область применения	Возможности использования
1. Автоматизация документооборота	Использование для автоматизации процессов создания, хранения и поиска документов, что упрощает работу юристов и повышает эффективность.
2. Анализ доказательств	Использование для анализа большого количества доказательств и выявления связей между ними, что помогает юристам принимать более точные решения.
3. Анализ судебных решений	Использование для анализа судебных решений и предсказания исхода дел на основе предыдущих судебных решений, что помогает принимать более обоснованные решения.

Продолжение таблицы 2

Область применения	Возможности использования
4. Работа с большими данными	Использование для анализа больших объемов данных, что позволяет юристам выявлять тенденции и паттерны в данных, которые могут помочь им принимать более обоснованные решения.
5. Юридический чат-бот	Использование для создания чат-ботов, которые могут отвечать на юридические вопросы клиентов, что упрощает работу юристов и повышает удобство для клиентов.

В целом, использование искусственного интеллекта в юридической отрасли позволяет ускорить процессы, повысить точность принятия решений и повысить эффективность работы юристов. Однако, необходимо учитывать возможные риски и ограничения использования искусственного интеллекта в юридической практике, такие как недостаток этических стандартов или ошибки в алгоритмах обработки данных.

2.2 Влияние цифровизации на юридическое образование

Цифровизация повлияла не только на юридическую практику, но и на юридическое образование. Юридические факультеты теперь включают цифровые инструменты и платформы в свои учебные программы, готовя студентов к цифровой эпохе юриспруденции. Это позволило студентам юридических факультетов развить навыки и знания, необходимые для успешной работы в цифровизированной юридической отрасли.

Цифровизация также оказывает значительное влияние на юридическое образование, изменяя способы обучения и требуя новых навыков и знаний у будущих юристов. В частности, цифровые технологии позволяют использовать новые методы обучения, такие как онлайн-курсы и виртуальные классы, которые упрощают доступ к знаниям и повышают гибкость обучения.

Новые способы обучения, такие как онлайн-курсы и виртуальные классы, которые позволяют студентам получать знания и учиться гибко и на расстоянии, предоставляют доступ к качественному образованию в любое время и в любом месте, а виртуальные классы позволяют студентам общаться и сотрудничать с преподавателями и другими студентами, не выходя из дома. Кроме то-

го, новые технологии, такие как виртуальная реальность и дополненная реальность, могут использоваться для создания интерактивных учебных материалов и симуляций, которые помогают студентам лучше понимать сложные концепции и законы.

Кроме того, цифровизация требует от юристов новых навыков в области информационных технологий, таких как анализ больших объемов данных, использование искусственного интеллекта и информационной безопасности. Поэтому, юридические программы должны включать эти темы в свои учебные планы, чтобы подготовить студентов к новым вызовам и требованиям цифровой эры.

В целом, цифровизация оказывает значительное влияние на юридическую отрасль и требует от юристов адаптироваться к новым технологиям и методам работы. Однако, при правильном использовании цифровых инструментов и технологий, юристы могут повысить эффективность своей работы и улучшить качество предоставляемых услуг.

2.3 Будущее цифровизации в юридической отрасли

Цифровизация уже имеет огромное значение для юридической отрасли, улучшая процессы, снижая временные и финансовые затраты и повышая точность. Однако, в будущем, это станет еще более важным.

Ожидается, что цифровые технологии станут еще более интеллектуальными и автоматизированными, что ускорит процессы и уменьшит риски ошибок. Машинное обучение, искусственный интеллект и блокчейн технологии имеют огромный потенциал для преобразования процессов правовых консультаций, анализа договоров и решения конфликтов.

Одним из ключевых преимуществ цифровизации в сфере юриспруденции является доступность для всех – клиенты смогут получать более быстрые и точные решения, а юридические консультанты смогут работать из любой точки мира.

Также ждем расширения области участия роботов-юристов. Они помогут снизить стоимость услуг, ускорить процесс решения конфликтов и освободить

юристов от рутинных задач. Однако, поручение ответственности за юридические решения роботам может привести к правовым проблемам в будущем, поэтому важно не занимать крайнюю сторону.

С другой стороны, цифровизация может привести к сокращению числа рабочих мест для людей в отрасли, что вызовет социальные проблемы. Чтобы преодолеть эти препятствия, заинтересованные стороны должны тесно сотрудничать, чтобы развивать планы и стратегии, учитывающие эти факторы и призванные создать дополнительные возможности для людей в юридической отрасли.

В целом, цифровизация в юридической отрасли предвещает много интересных изменений, но еще важнее будет сохранить преданность справедливости и этике в весь процесс.

Будущее цифровизации в юридической отрасли очень перспективно. По мере развития технологий будут появляться новые возможности для инноваций и роста. В ближайшие годы юридическая отрасль, скорее всего, станет более цифровой, поскольку в ней все чаще будут использоваться и другие цифровые инструменты.

Однако важно помнить, что цифровизация сопряжена с потенциальными рисками. Необходимо решать вопросы конфиденциальности и безопасности данных, а специалисты в области права должны сохранять бдительность, чтобы ошибки и сбои не оставались незамеченными.

Цифровизация уже давно затронула юридическую отрасль, и это только начало. Будущее цифровизации в юридической отрасли будет характеризоваться следующими тенденциями:

1. Использование искусственного интеллекта и машинного обучения для автоматизации процессов юридической работы, таких как анализ документов, подготовка договоров и юридических документов, поиск информации и многое другое.

2. Развитие электронной подписи и использование блокчейн-технологий для обеспечения безопасности и конфиденциальности данных, а также для со-

здания эффективных систем управления правами доступа.

3. Создание облачных платформ для хранения и обмена юридической информацией, которые позволят юристам работать удаленно, обмениваться документами и сотрудничать с клиентами из любой точки мира.

4. Развитие роботизированных процессов и автоматизация рутинной работы, что позволит юристам сконцентрироваться на более сложных задачах, требующих высокой квалификации.

5. Увеличение использования онлайн-сервисов для предоставления юридических услуг, таких как консультации, подготовка документов и подача заявлений.

6. Развитие систем аналитики данных и бизнес-интеллекта, которые помогут юристам принимать более обоснованные решения на основе данных и статистики.

7. Развитие технологий виртуальной и дополненной реальности для создания интерактивных обучающих программ и тренингов для юристов.

В целом, будущее цифровизации в юридической отрасли будет характеризоваться автоматизацией, ускорением процессов и повышением качества предоставляемых услуг. Однако, важно помнить, что технологии не заменят человеческий фактор в юридической работе, а будут лишь инструментом для улучшения ее эффективности.

3 ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПРАВА, ПРОБЛЕМЫИ ПУТИ СОВЕРШЕНСТВОВАНИЯ

3.1 Трансформация правовой реальности в цифровую эпоху

Цифровая трансформация — это:

– процесс внедрения организацией цифровых технологий, сопровождаемый оптимизацией системы управления основными технологическими процессами;

– увеличение эффективности отдельных процессов и деятельности организации в целом;

– отражение реальных процессов и информации в цифровом виде;

– управление на основе реальных данных;

– компетенции каждого сотрудника организации.

Принципы цифровой трансформации:

1) цифровая интеграция;
2) руководство и культура;
3) готовность сотрудников;
4) гибкость процессов;
5) нетерпимость к обособленности;
6) принятие решений на основе данных;
7) системный подход;
8) приведение процессов к общему виду.

Цифровая интеграция — это процесс объединения различных направлений работы в единую целостную систему для улучшения эффективности бизнес-процессов.

Цифровая интеграция позволяет автоматизировать процессы, ускорить принятие решений и повысить качество продукции и услуг. Она также позволяет снизить затраты на обслуживание и управление информацией, что способствует увеличению эффективности.

Примером цифровой интеграции является использование единой плат-

формы для управления всеми бизнес-процессами в работе, включая управление проектами, ресурсами, а так же управление кадрами и финансами.

Это позволяет ускорить принятие решений и повысить эффективность работы всей организации.

Принятие решений на основе данных информационных систем — это процесс анализа данных, полученных из информационных систем, с целью принятия обоснованных и эффективных решений.

Принятие решений на основе данных информационных систем может быть применено в различных сферах деятельности. Для этого используются различные методы и технологии, такие как статистический анализ, машинное обучение, бизнес-анализ и другие.

Преимущества принятия решений на основе данных информационных систем включают:

- более точные и обоснованные решения;
- сокращение времени на принятие решений;
- улучшение эффективности и производительности;
- снижение рисков и ошибок.

Однако, для успешного принятия решений на основе данных информационных систем необходимо уметь правильно интерпретировать данные и использовать соответствующие методы анализа. Также важно учитывать контекст и специфику задачи, чтобы избежать неправильных выводов и решений.

Приведение процессов к общему виду при цифровой трансформации является важным шагом для обеспечения эффективности и согласованности в работе. Это может потребовать значительных изменений в работе, но в конечном итоге поможет достичь поставленных целей и повысить качество.

При цифровой трансформации процессы должны быть приведены к общему виду, чтобы обеспечить эффективность и согласованность в работе организации.

Это может быть достигнуто путем следующих шагов:

1. Анализ процессов. Необходимо провести анализ всех бизнес-

процессов в компании и определить их сильные и слабые стороны. Это поможет выявить процессы, которые нуждаются в изменениях.

2. Определение целей. Необходимо определить цели, которые должны быть достигнуты при изменении процессов. Это может быть улучшение качества продукции или услуг, сокращение времени выполнения задачи или уменьшение затрат.

3. Приведение процессов к общему виду. Необходимо разработать общий шаблон для всех бизнес-процессов в компании. Это поможет обеспечить единообразие и согласованность в работе.

4. Внедрение новых процессов. Необходимо внедрить новые процессы, которые соответствуют общему шаблону. Это может потребовать обучения сотрудников и внедрения новых технологий.

5. Мониторинг и улучшение. Необходимо постоянно мониторить процессы и улучшать их, чтобы достигать поставленных целей и обеспечивать эффективность работы.

Цифровая трансформация не может быть успешной без:

- лидеров, готовых к изменениям;
- принятия принципиальных решений;
- понимания процессов и их разделение;
- переиспользования данных и решений.

Готовность руководства и сотрудников при цифровой трансформации является ключевым фактором для успеха в работе. Руководство должно понимать необходимость цифровой трансформации и готовность внедрять новые технологии и процессы в организацию. Они должны быть готовы к изменениям в бизнес-модели, культуре организации и стратегии.

Ценность перехода к цифровой трансформации не будет иметь долгосрочного эффекта, если игнорировать человеческий фактор.

Сотрудники также должны быть готовы к обучению новым технологиям и процессам, а также к изменению своих рабочих привычек.

Приведение процессов к общему виду при цифровой трансформации яв-

ляется важным шагом для обеспечения эффективности и согласованности в работе. Это может потребовать значительных изменений в работе, но в конечном итоге поможет достичь поставленных целей и повысить качество.

При цифровой трансформации процессы должны быть приведены к общему виду, чтобы обеспечить эффективность и согласованность в работе организации.

Это может быть достигнуто путем следующих шагов:

1. Анализ процессов. Необходимо провести анализ всех бизнес-процессов в компании и определить их сильные и слабые стороны. Это поможет выявить процессы, которые нуждаются в изменениях.

2. Определение целей. Необходимо определить цели, которые должны быть достигнуты при изменении процессов. Это может быть улучшение качества продукции или услуг, сокращение времени выполнения задачи или уменьшение затрат.

3. Приведение процессов к общему виду. Необходимо разработать общий шаблон для всех бизнес-процессов в компании. Это поможет обеспечить единообразие и согласованность в работе.

4. Внедрение новых процессов. Необходимо внедрить новые процессы, которые соответствуют общему шаблону. Это может потребовать обучения сотрудников и внедрения новых технологий.

5. Мониторинг и улучшение. Необходимо постоянно мониторить процессы и улучшать их, чтобы достигать поставленных целей и обеспечивать эффективность работы.

6. Расширение возможностей применения права. Цифровая трансформация в праве помогает расширить возможности применения права, особенно в тех областях, где правовые процессы кажутся слишком дорогостоящими. Она позволяет создавать новые форматы электронных документов и автоматизировать процессы оценки, мониторинга и управления рисками.

7. Создание новых услуг и продуктов. Цифровая трансформация права будет способствовать созданию новых продуктов и услуг, что позволит юри-

стам улучшить свои процессы и сервисы и достичь существенного конкурентного преимущества.

Принятие решений на основе данных информационных систем также может быть основано на системном подходе, который предполагает рассмотрение проблемы или задачи как части более крупной системы. В этом случае анализ данных и принятие решений осуществляется с учетом взаимосвязей и взаимодействий между элементами системы.

Системный подход позволяет более полно и комплексно рассмотреть проблему и учитывать не только ее отдельные аспекты, но и их взаимодействие. Это позволяет принимать более эффективные и устойчивые решения, которые учитывают все факторы и последствия.

Примером применения системного подхода в принятии решений на основе данных может служить анализ судебного производства и решений. При этом необходимо учитывать не только отдельные судебные процессы, но и их взаимодействие друг с другом, а также влияние внешних факторов, таких как изменение экономики, политики, законодательства, региона и т.д.

Некорректно рассматривать «цифру», как обособленные процессы. Цифровизация — это отражение действительности в цифровом виде.

Существует несколько причин, почему сотрудники не используют ресурсы информационных систем:

1. Недостаточное знание о ресурсах: многие могут не знать о том, какие ресурсы доступны в информационных системах и как их использовать. Обычно это происходит из-за того, что люди просто не обращают внимание на обучающие материалы или не проходят достаточное количество обучения.

2. Необходимость в индивидуальном подходе: для того, чтобы получить максимальную пользу от информационных систем, необходимо настроить их на свои индивидуальные потребности.

3. Недостаточное время: Некоторые сотрудники могут ссылаться на недостаток времени, чтобы использовать информационные системы, поскольку они заняты другими делами или считают свои задачи более приоритетными.

Однако если работа связана с обработкой и использованием больших объемов информации в различных системах, то неэффективное взаимодействие с этой информацией может привести к проблемам в принятии важных решений и задержкам в выполнении задач. Для решения этих проблем, необходимо выделить время и усилия, чтобы разобраться в ресурсах информационных систем, в том числе обратиться к специалистам для получения обучения и поддержки и настроить их индивидуально на нужды и потребности своей работы.

На данный момент набирает обороты проектное управление, так как доказало свою эффективность и результативность.

Проектное управление — это особый вид управленческой деятельности, основанный на комплексно-системной модели коллективных действий участников, позволяющий получить в разнообразных отраслях управления - практический результат.

Основные шаги:

1) определить основные процессы и входные-выходные данные, использующиеся обособленным отделом;

2) определить алгоритмы сбора и формирования отчетов;

3) сопоставить данные с возможностями информационной системы, использующихся в организации;

4) при необходимости и возможности проводить доработки информационных систем, с целью обеспечения и получения из нее достоверных данных;

5) обучить сотрудников организации использовать новые инструменты в текущих и будущих задачах;

6) контролировать использование новых инструментов и не допускать возврат к привычному строю работы.

Только такой комплексный анализ позволит принять оптимальное решение по оптимизации процесса деятельности и повышению его эффективности.

3.2 Правовая культура при цифровой трансформации

Правовая культура — это система знаний, ценностей, норм и навыков, связанных с правом, которые формируют поведение и отношение людей к за-

кону и его соблюдению. Данное понятие включает в себя практические навыки по применению законодательства, но также отражает осознание личной ответственности, уважения к правам других людей, понимание правовых принципов и роли правовой системы в обществе.

Правовая культура может быть сформирована разными способами, включая обучение в школах и университетах, практику в профессиональной деятельности, нормативное и пропагандистское воздействие со стороны государства. Она также может быть различной в разных странах, основываясь на исторических, культурных, религиозных и других факторах.

Хорошая правовая культура играет важную роль в стабильном развитии общества, укрепляет правовую государственность, способствует созданию правопорядка и уважению прав и свобод человека.

Цифровая трансформация сильно влияет на правовую культуру общества и, в свою очередь, требует развития и совершенствования правовой культуры для успешной реализации.

Одной из ключевых задач цифровой трансформации является решение задач в области защиты данных и информационной безопасности, поскольку с развитием цифровых технологий все больше информации становится доступной для хранения и обработки на компьютерах и в сети Интернет. В этой связи правовое обеспечение информационной безопасности и защиты данных становится важным компонентом правовой культуры.

Кроме того, цифровая трансформация также влияет на другие области правовой культуры. Например, повышение доступности знаний и информации, связанных с законодательством, может помочь формированию осознанного отношения к правовым нормам и правилам, а также повысить практическую подготовку и навыки в сфере права.

Цифровые технологии также ускоряют процессы правового получения доступа к информации, что облегчает доступ к юридическим услугам и повышает ее доступность для населения. Этот аспект также является важным компонентом правовой культуры.

В целом, цифровая трансформация и правовая культура связаны и взаимосвязаны. Развитие цифровых технологий требует развития новых правовых норм и подходов, а также совершенствования правовой практики в цифровой области, тем самым влияя на развитие правовой культуры общества.

В цифровой эпохе правовая культура играет важную роль в установлении норм и правил поведения в интернете и обеспечении защиты личных данных в онлайн-среде. Знание основ технологий и соблюдение важных правовых требований позволяют пользователям эффективно использовать цифровые ресурсы и сервисы, а также сокращать риски нарушения своих прав и свобод в онлайн-среде.

Развитие правовой культуры в цифровой эпохе позволяет создать условия для формирования этических и правовых стандартов, принятых в онлайн-среде. В связи с этим важно обеспечить доступность справочной информации для пользователей и продвижение публичных образовательных кампаний для формирования верхнего уровня цифровой грамотности и понимания основ правовых норм и принципов, связанных с цифровой безопасностью и защитой личных данных.

Кроме того, направленные на развитие правовой культуры программы обучения на всех уровнях, от школьного образования до профессионального обучения, могут помочь повышению уровня компетентности, а также эффективного применения образования на практике при ведении бизнеса в онлайн-среде.

Важно также снабжать соответствующую информацию и процедуры технической поддержки, использования решений в онлайн-бизнесе на равной основе и для отстаивания своих прав и интересов в сфере высоких технологий.

В целом, правовая культура в цифровой эпохе является ключом к обеспечению эффективного использования цифровых технологий и цифровой безопасности, сформированной методами правовых методов. Она также способствует развитию эффективного цифрового общества, основанного на уважении прав и свобод человека в онлайн-среде.

Цифровая трансформация существенно влияет на формирование правовой культуры. С развитием цифровых технологий меняется восприятие людей о том, что является правильным и неправильным, что дозволено и запрещено, как нужно вести себя в различных онлайн-ситуациях.

Одним из существенных аспектов цифровой трансформации является расширение доступа к информации и знаниям. Люди получают возможность получать и передавать информацию в режиме онлайн, что ведет к умножению знаний в сфере права и повышению юридической грамотности. В результате формируются более высокие стандарты правосознания, что положительно влияет на правовую культуру общества.

Однако, с развитием цифровых технологий появляются новые угрозы, такие как кибербуллинг, цифровое насилие, нарушение авторских прав, кража личных данных и многое другое. Эти явления могут увеличивать уровень правовой неосведомленности и поведения, что негативно влияет на правовую культуру общества.

С одной стороны, расширенный доступ к информации и знаниям в сфере юриспруденции может помочь поднять уровень правосознания общества. С другой стороны, новые технологии ведут к появлению новых нарушений прав человека и норм поведения, что может негативно отразиться на правовой культуре. В связи с этим, важно продвигать образовательные программы и кампании, основанные на этических принципах и правовых нормах, и обеспечить адекватную защиту прав и свобод в онлайн-среде.

3.3 Влияние цифровизации на юридическую отрасль и граждан

С развитием технологий цифровизация стала неотъемлемой частью многих отраслей, включая юридическую. Цифровизация в юридической отрасли включает в себя переход от бумажных документов к электронным, использование новых технологий для обработки и хранения информации, а также автоматизацию процессов. Это приводит к тому, что юридическая отрасль становится более эффективной и доступной для обычных граждан.

Цифровизация имеет огромное влияние на юридическую отрасль. Во-

первых, она позволяет юристам работать более эффективно и быстро. Например, электронные документы могут быть легко найдены и обработаны, что сокращает время на поиск информации. Кроме того, автоматизация процессов позволяет юристам сконцентрироваться на более сложных задачах, в то время как рутинные задачи выполняются автоматически.

Во-вторых, цифровизация делает юридическую отрасль более доступной для клиентов. Электронные услуги позволяют клиентам получать доступ к документам и информации в любое время и из любого места, что удобно для тех, кто не может посетить юридическую компанию лично.

Цифровизация имеет множество преимуществ для юристов. Одним из главных преимуществ является увеличение эффективности работы. Юристы могут быстро и легко находить документы и информацию, что позволяет им сократить время на выполнение задач. Кроме того, автоматизация процессов позволяет юристам сосредоточиться на более сложных задачах, в то время как рутинные задачи выполняются автоматически.

Другим преимуществом цифровизации является улучшение качества работы. Электронные документы и услуги позволяют юристам быстро получать доступ к информации и обрабатывать ее более точно и эффективно. Это повышает качество услуг, что удовлетворяет клиентов и повышает репутацию компании.

Существует множество примеров цифровизации в юридической отрасли. Одним из них является использование электронных документов. Это позволяет юристам быстро находить и обрабатывать документы, а также делиться ими с клиентами.

Другим примером является автоматизация процессов. Это позволяет юристам выполнять рутинные задачи автоматически, что освобождает время для более сложных задач. Кроме того, автоматизация процессов устраняет проблемы с человеческим фактором, такие как ошибки в документах или пропуск важной информации.

Существует множество технологий, способствующих цифровизации в

юридической отрасли. Одной из таких технологий является облачное хранилище данных. Это позволяет юристам быстро и безопасно обмениваться документами и информацией с клиентами.

Другой важной технологией является искусственный интеллект. Он может использоваться для автоматизации процессов, анализа данных и выявления тенденций в правовых вопросах.

Хотя цифровизация имеет множество преимуществ, она также имеет свои проблемы. Одной из главных проблем является безопасность данных. Это особенно важно для юридической отрасли, где конфиденциальность и защита данных являются ключевыми вопросами.

Кроме того, цифровизация может привести к увольнению работников, которые занимаются рутинными задачами. Это может создать проблемы для работников и вызвать социальные проблемы.

Цифровизация меняет юридические услуги для граждан. Они могут получать доступ к документам и информации в любое время и из любого места, что удобно для тех, кто не может посетить юридическую компанию лично. Кроме того, цифровизация позволяет юристам быстро и эффективно решать правовые вопросы.

Цифровизация будет продолжать революционизировать юридическую отрасль в будущем. С развитием новых технологий, таких как блокчейн и машинное обучение, юридическая отрасль будет более эффективной, доступной и безопасной для клиентов.

Чтобы адаптироваться к цифровизации в юридической отрасли, юристы должны быть готовы к изменениям и открыты к новым технологиям. Они также должны обеспечить безопасность данных и защиту конфиденциальной информации.

Цифровизация революционизирует юридическую отрасль, делая ее более эффективной, доступной и безопасной для клиентов. Юристы должны быть готовы к изменениям и открыты к новым технологиям, чтобы успешно адаптироваться к этим изменениям.

3.4 Проблемы безопасности данных и конфиденциальности в цифровую эпоху юриспруденции

Проблемы безопасности данных и конфиденциальности являются одним из наиболее значительных рисков, связанных с цифровизацией в юридической отрасли. Юридические документы содержат личную и конфиденциальную информацию. В то же время если эта информация попадет в чужие руки, это может иметь серьезные последствия.

С ростом использования информационных технологий появляются различные проблемы, связанные с цифровым правом. Некоторые из них включают в себя:

1. Нарушение конфиденциальности данных. Выбросы данных и кибератаки могут привести к незаконному доступу к личной информации пользователя, что может привести к финансовому мошенничеству, краже личности и другим преступлениям.

2. Нарушение авторских прав. В Интернете появляется все больше нелицензионного контента, такого как фильмы, музыка, книги и т.д. Это может нанести ущерб правообладателям и нарушить их авторские права.

3. Низкий уровень осведомленности пользователей. Многие пользователи не знают своих прав в Интернете и не могут защитить свою личную информацию и права.

4. Недостаточная защита детей. Интернет представляет угрозу для детей в виде нецензурного контента, кибербуллинга и контактов с неподходящими людьми.

Для улучшения ситуации и повышения уровня защиты в цифровой эпохе необходимо принимать следующие меры:

1. Создание более строгих правил защиты данных и конфиденциальности.

2. Улучшение законодательства в области авторских прав.

3. Обучение пользователей о своих правах и способах их защиты.

4. Более эффективная регуляция онлайн-продаж и электронной коммер-

ции.

5. Разработка новых технологий, направленных на обеспечение безопасности в Интернете и тщательное тестирование новых продуктов и приложений на отсутствие скрытых уязвимостей.

Юридические фирмы должны принимать меры для обеспечения безопасного хранения и передачи данных. Это включает использование технологии шифрования, ограничение доступа к конфиденциальной информации и применение надежных паролей. Юристы также должны быть бдительными, чтобы не допустить случайного разглашения конфиденциальной информации.

В цифровую эпоху юриспруденции безопасность данных и конфиденциальность стали одними из самых важных вопросов. Судебные органы, адвокаты и другие участники юридического процесса работают с большим количеством конфиденциальной информации, такой как персональные данные, финансовые документы и т.д.

Одним из главных рисков является кибератака или хакерские атаки на системы хранения данных. Часто злоумышленники пытаются получить доступ к информации, чтобы использовать ее в корыстных целях, например, для шантажа или вымогательства.

Для защиты данных и конфиденциальности в цифровую эпоху юриспруденции необходимо применять современные методы шифрования и многофакторную аутентификацию. Кроме того, необходимо обеспечить физическую безопасность серверов и компьютеров, где хранится информация.

Важно также обучать сотрудников правилам безопасности и осведомлять их о новых угрозах. Например, мошенники могут использовать социальную инженерию для получения доступа к системам или информации.

Наконец, необходимо иметь план восстановления после инцидента безопасности. Если все же произойдет нарушение безопасности, необходимо быстро реагировать, чтобы минимизировать ущерб и восстановить работу системы как можно скорее.

Законы, регулирующие информационную безопасность, могут отличаться

в разных странах и регионах. Нормативно-правовые акты и их содержание отображены в таблице 3.

Таблица 3 – Нормативно-правовые акты в разных странах и регионах

Нормативно-правовые акты	Содержание
Закон о защите персональных данных (General Data Protection Regulation, GDPR) в Европейском союзе	Цель GDPR - защитить персональные данные граждан Европейского союза и установить единые правила для обработки этих данных. Закон распространяется на любые компании, которые обрабатывают персональные данные граждан ЕС, независимо от того, где эти компании находятся. GDPR предписывает компаниям соблюдать определенные правила при обработке персональных данных, включая согласие на обработку данных, право на доступ к данным, право на удаление данных и право на перенос данных. Компании также должны уведомлять о нарушении безопасности данных в течение 72 часов после его обнаружения. Нарушение GDPR может привести к штрафам до 4% от годового оборота компании или до 20 миллионов евро, в зависимости от того, какая сумма больше.
Закон об информационной безопасности в Китае	Закон обязывает организации и компании, работающие в Китае, хранить данные о китайских гражданах на территории Китая и проходить процедуру сертификации безопасности. Также он запрещает передачу китайских данных за границу без соответствующего разрешения. Закон также требует от операторов сетей и интернет-провайдеров сотрудничать с правительственными органами в борьбе с киберпреступностью и предоставлять им доступ к информации о пользователях. Некоторые эксперты высказывают опасения, что закон может привести к нарушению прав частной жизни и свободы слова в Китае.
Закон о защите информации в России;	Закон устанавливает обязательные требования к организациям и гражданам по защите информации, содержащей государственную тайну. Он также определяет порядок получения и распространения информации, содержащей государственную тайну. Закон о защите информации в России устанавливает ответственность за нарушение правил обращения с информацией, в том числе за незаконное получение, использование и распространение информации. Основная цель закона - обеспечение безопасности информации, сохранение конфиденциальности и защита прав граждан и организаций на ее использование.

Продолжение таблицы 3

Нормативно-правовые акты	Содержание
Закон о информационной безопасности в США	На данный момент, в США нет единого закона о информационной безопасности, но существует ряд законодательных актов, регулирующих область кибербезопасности. Некоторые из них: Закон о кибербезопасности и общественной защите информации (The Cybersecurity and Information Sharing Act, CISA) - принят в 2015 году. Законодательный акт over-shares охрана и распространять информацию о подозрительной или вредоносной активности в Интернете между правительственными агентствами и компаниями. Закон о защите персональных данных (The Personal Data Protection Act) – законодательный акт, который содержит различные ограничения, связанные с сбором, использованием, хранением и раскрытием личной информации. Закон об электронной подписи (The Electronic Signatures in Global and National Commerce Act) - законодательный акт, который регулирует узаконивание электронных подписей в компьютерных системах. Закон о кибервойне (The Cyber Warfare Act) – несколько законодательных актов, навязывающие ответственность за военное использование кибертехнологий.
Закон о защите конфиденциальности и безопасности данных в Австралии	Закон о защите конфиденциальности и безопасности данных в Австралии называется Privacy Act (Закон о конфиденциальности). Этот закон регулирует практику сбора, использования и раскрытия персональных данных в крупных организациях и государственных учреждениях. Согласно Privacy Act, организации, которые обрабатывают персональные данные, должны соблюдать следующие требования: Обеспечить безопасность персональных данных, предпринимая меры для защиты их от несанкционированного доступа, использования, изменения, раскрытия или уничтожения. Уведомлять граждан об использовании и раскрытии их персональных данных. Предоставлять гражданам доступ к их персональным данным и давать возможность вносить изменения. Следить за точностью и актуальностью персональных данных. Использовать персональные данные только для целей, для которых они собраны. В 2018 году были внесены поправки в Privacy Act (PA), которые включают в себя обязательное уведомление регуляторов и пострадавшего в случае наруше-

Продолжение таблицы 3

Нормативно-правовые акты	Содержание
	ния безопасности данных и предоставление большего контроля за персональными данными для граждан.
Закон о защите данных в Японии;	В Японии существует несколько законов, регулирующих защиту данных, однако, наиболее важный из них - это Закон о защите персональных данных, принятый в 2003 году и известный как Personal Information Protection Act (PIPA). Закон обеспечивает защиту прав и свобод граждан в отношении их персональных данных, установленных принципов сбора, использования и обработки. В соответствии с PIPA, пользователи персональных данных должны обеспечивать адекватную защиту персональной информации, которая включает в себя установление целей сбора, получение согласия на сбор и использование данных, доступ к данным, исправление ошибок и защиту данных от утраты, уничтожения, изменения или несанкционированного доступа. Минимальные стандарты, которые должны соблюдаться в ходе защиты данных, включают обязательный контроль и мониторинг систем, регулярный мониторинг технических нарушений безопасности, а также требование окончательной удаления персональных данных после их использования. Кроме того, существуют другие законы, такие как Anti-Phishing Act, которые вводят уголовную ответственность за проведение фишинг-атак и использование незаконной электронной почты и Spam Act, который устанавливает правила отправки коммерческих сообщений, чтобы защитить граждан от спама.

Кроме того, существуют международные стандарты и рекомендации по информационной безопасности, такие как ISO 27001 и NIST Cybersecurity Framework.

В России законодательство о защите информации включает в себя несколько законов, в том числе:

1. Федеральный закон «О защите персональных данных» от 27.07.2006 № 152-ФЗ[11] - определяет правила сбора, хранения, использования и распространения персональных данных граждан России.

[11] Федеральный закон от 27.07.2006 г. № 152-ФЗ «О защите персональных данных» [Электронный ресурс] : Доступ из справ.-правовой системы «КонсультантПлюс».

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ[12] - регулирует вопросы защиты информации в целом, включая конфиденциальность, целостность и доступность информации.

3. Федеральный закон «Об информационной безопасности» от 26.07.2006 № 149-ФЗ - данный закон определяет порядок осуществления информационной безопасности в Российской Федерации, включая защиту информации, информационных систем и информационно-телекоммуникационных сетей.

4. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ[13] - данный закон устанавливает правила организации и функционирования сетей связи, включая защиту информации, передаваемой по сетям связи.

5. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ[14] - определяет правила использования информации, которая может нанести вред детям.

6. Кодекс Российской Федерации «Об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 13.06.2023)[15] – содержит положения, которые предусматривают ответственность за нарушения в области защиты информационной безопасности.

Эти законы охватывают широкий спектр вопросов, связанный с информационной безопасностью в России, и обеспечивают правовое регулирование в этой области.

Кроме того, существуют и другие нормативные акты, регулирующие вопросы информационной безопасности в России, например, постановления Правительства Российской Федерации и инструкции Федеральной службы безопасности Российской Федерации.

---

[12] Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] : Доступ из справ.-правовой системы «КонсультантПлюс».
[13] Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».
[14] Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».
[15] Кодекс Российской Федерации от 30.12.2001 г. № 195-ФЗ (ред. от 13.06.2023) «Об административных правонарушениях» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

Постановления Правительства РФ, которые устанавливают правила и требования по различным вопросам информационной безопасности. Например, Постановление Правительства РФ «Об утверждении Правил обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» от 1 декабря 2003 года № 681[16] устанавливает требования к защите персональных данных при их обработке в информационных системах.

Инструкции Федеральной службы безопасности Российской Федерации— это документы, которые определяют порядок действий и требования к организациям и гражданам по обеспечению информационной безопасности. Например, Инструкция ФСБ РФ «Об утверждении Правил использования защищенных объектов информатизации» от 20 марта 2007 года № 18[17] устанавливает правила использования защищенных объектов информатизации, таких как криптографические средства и защищенные каналы связи.

В целом, законы, постановления и инструкции, регулирующие вопросы информационной безопасности в России, направлены на защиту прав граждан на конфиденциальность и безопасность персональных данных, а также на обеспечение безопасности информации в целом.

Помимо Правительства РФ и ФСБ РФ, вопросы информационной безопасности регулируются также постановлениями и инструкциями Федеральной службы по техническому и экспортному контролю (ФСТЭК). Например, Постановление ФСТЭК России «Об утверждении требований к защите информации при использовании электронной почты» от 18 апреля 2013 года № 21[18] устанавливает требования к защите информации при использовании электронной почты.

Инструкции ФСТЭК РФ также определяют порядок действий и требова-

[16] Постановление Правительства РФ от 01.12.2003 г. № 681 «Об утверждении Правил обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».
[17] Инструкция ФСБ РФ от 20.03.2007 г. № 18 «Об утверждении Правил использования защищенных объектов информатизации» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».
[18] Постановление ФСТЭК России от 18.04.2013 г. № 21 «Об утверждении требований к защите информации при использовании электронной почты» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

ния к организациям и гражданам по обеспечению информационной безопасности. Например, Инструкция ФСТЭК РФ «Об утверждении Правил использования защищенных объектов информатизации в государственных органах и органах местного самоуправления» от 17 июля 2012 года № 21 устанавливает правила использования защищенных объектов информатизации в государственных органах и органах местного самоуправления.

Таким образом, законы, постановления и инструкции, разработанные Правительством РФ, ФСБ РФ и ФСТЭК РФ, являются основными нормативными актами, которые регулируют вопросы информационной безопасности в России. Они направлены на защиту прав граждан и обеспечение безопасности информации в целом.

Кроме того, в России существуют судебные дела, связанные с информационной безопасностью. Например, в 2019 году был рассмотрен судебный иск компании Telegram против ФСБ РФ, связанный с требованием предоставить доступ к зашифрованным сообщениям пользователей. В результате суд вынес решение в пользу ФСБ РФ.

Также в России регулярно проводятся операции по выявлению и пресечению преступлений, связанных с информационной безопасностью. В 2020 году были задержаны несколько человек, обвиняемых в создании и распространении вредоносных программ, а также в краже денежных средств через интернет-банкинг.

В эпоху цифровизации вопросы безопасности данных и конфиденциальности в юриспруденции становятся все более актуальными. Адвокаты и юридические фирмы имеют дело с бесчисленным количеством юридических документов, содержащих конфиденциальную информацию, которую необходимо постоянно защищать. Любой несанкционированный доступ или нарушение конфиденциальности этих данных может привести к серьезным последствиям, включая кражу личных данных и финансовые потери. Поэтому очень важно принять надежные меры безопасности и соблюдать нормативные стандарты для обеспечения сохранности всех конфиденциальных данных. Игнорирование без-

опасности данных может привести к потере доверия со стороны клиентов и репутационному ущербу для юридической отрасли в целом. Специалисты в области права должны уделять первостепенное внимание безопасности данных и конфиденциальности, чтобы сохранить доверие к себе и защитить информацию своих клиентов.

Основные вопросы безопасности данных и конфиденциальности:

1. Какие меры безопасности должны приниматься для защиты конфиденциальных данных клиентов в юридической практике?

2. Какие законы и нормативные акты регулируют сбор, хранение и использование персональных данных в юридической сфере?

3. Какие последствия могут возникнуть при нарушении конфиденциальности данных клиентов юридической фирмы?

5. Какие меры безопасности следует принимать при обмене конфиденциальной информацией с другими юридическими фирмами или организациями?

6. Какие технологии и программное обеспечение помогают обеспечить безопасность данных в юридической практике?

7. Какие меры безопасности следует принимать при удалении или уничтожении конфиденциальных данных клиентов?

8. Какие меры безопасности следует принимать при использовании облачных сервисов для хранения и обработки конфиденциальной информации?

Способы решения и принимаемые меры безопасности в юриспруденции осуществляются в соответствии с действующим законодательством и направлены на защиту прав и интересов всех участников юридических конфликтов.

1. Для защиты конфиденциальных данных клиентов в юридической практике должны приниматься следующие меры безопасности:

– ограничение доступа к информации только уполномоченным сотрудникам;

– использование паролей и других методов аутентификации для защиты доступа к данным;

– шифрование конфиденциальной информации при передаче и хранении;

– регулярное обновление систем безопасности и антивирусного программного обеспечения;

– обучение сотрудников правилам безопасности и контроль их выполнения.

2. Сбор, хранение и использование персональных данных в юридической сфере регулируются законами и нормативными актами, такими как:

– федеральный закон «О защите персональных данных» от 27.07.2006 № 152-ФЗ;

– федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

– постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119[19].

3. При нарушении конфиденциальности данных клиентов юридической фирмы могут возникнуть следующие последствия:

– утечка конфиденциальной информации;

– потеря доверия со стороны клиентов;

– юридические проблемы и судебные разбирательства;

– ущерб репутации юридической фирмы.

4. При обмене конфиденциальной информацией с другими юридическими фирмами или организациями следует принимать следующие меры безопасности:

– использование шифрования при передаче данных;

– подписание соглашений о конфиденциальности;

– ограничение доступа к информации только уполномоченным сотруд-

[19] Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

никам.

5. Для обеспечения безопасности данных в юридической практике могут использоваться следующие технологии и программное обеспечение:

– шифрование данных;

– антивирусное программное обеспечение;

– системы контроля доступа;

– системы мониторинга и аудита.

6. При удалении или уничтожении конфиденциальных данных клиентов следует принимать следующие меры безопасности:

– использование специализированных программ для безопасного удаления данных;

– физическое уничтожение носителей информации;

– соблюдение законодательства по защите персональных данных.

7. При использовании облачных сервисов для хранения и обработки конфиденциальной информации следует принимать следующие меры безопасности:

– выбор надежного провайдера облачных сервисов;

– шифрование данных при передаче и хранении;

– регулярный мониторинг систем безопасности провайдера.

3.5 Пути совершенствования права и способы адаптации юристов к цифровой эпохе

Цифровая трансформация оказывает значительное влияние на правовую реальность. С помощью цифровых технологий возможна автоматизация процессов в области юстиции, сокращение времени на обработку документов и улучшение доступности судебной системы.

Одно из преимуществ цифровой трансформации - улучшение доступности судебной системы для граждан. Онлайн-системы позволяют людям получить доступ к электронной версии юридических документов и отслеживать состояние своих дел, не покидая свой дом. Информационные порталы и приложения делают обработку электронных документов проще и более эффективной,

что значительно ускоряет судебные процессы.

Цифровые технологии также применяются для создания децентрализованных блокчейн-баз данных, что может привести к усилению безопасности и конфиденциальности в юридических процедурах. Блокчейн может быть использован для создания глобальных систем идентификации, что поможет продвинуть общественное доверие к судебной системе и устранить возможность нарушения прав и обмана.

В цифровую эпоху требуются существенные изменения и совершенствования правовых норм, так как традиционные способы регулирования недостаточны для защиты информационной безопасности и прав пользователей в сфере информационных технологий. Некоторые пути совершенствования права в цифровую эпоху включают:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ:

— необходимо уточнить процедуру передачи персональных данных граждан в другие страны и задать жесткие требования к подобным передачам;

— требуется расширить понятие персональных данных, с учетом новых технологий сбора и обработки информации;

— необходимо разработать более эффективный механизм контроля за информационной безопасностью в компаниях, осуществляющих обработку персональных данных;

— задача ужесточения наказания за нарушения информационной безопасности, включая штрафы, ограничения на деятельность, а также установление уголовной ответственности.

2. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ:

— требуется увеличить количество данных о личности, которые могут считаться персональными, включая IP-адреса и психологические профили;

— необходимо ужесточить требования по защите персональных данных и вводить обязательную двухэтапную аутентификацию для доступа к личным

данным;

— требуется разработать методы криптографической защиты персональных данных при использовании облачных сервисов;

— необходимо определить ответственность компаний за утечку, несанкционированный доступ к личным данным и их использование.

3. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ:

— необходимо создать единый стандарт для аутентификации пользователей при использовании электронной подписи и введение механизмов защиты от подмены подписи;

— требуется регулировать использование электронной подписи при оформлении договорных отношений и других правоотношений в информационной сфере;

— необходимо разработать механизмы гарантированной защиты от неблагоприятных событий, связанных с использованием электронной подписи.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ:

— определить процедуры и механизмы сбора, хранения, использования и уничтожения информации, необходимых для обеспечения информационной безопасности;

— установить требования по обязательной сертификации компаний, осуществляющих обработку и передачу персональных данных;

— разработать новые и усовершенствовать существующие методы электронной подписи, аутентификации и шифрования данных;

— необходимо ужесточить ответственность за нарушения информационной безопасности, включая введение уголовной ответственности.

5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ:

— введение изменений в сфере защиты персональных данных и информационной безопасности, включая ужесточение мер ответственности за нару-

шения закона;

— для обеспечения более эффективной защиты персональных данных, требуется развитие инструментов контроля и наказания нарушителей.

6. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ:

— необходимо уточнение компетенции специализированных органов для регулирования рынка связи и введение эффективного механизма контроля за функционированием сетей связи;

— разработка и внедрение новых технологий связи, в том числе передачи высокоскоростных данных с использованием оптических технологий.

7. Федеральный закон «О защите конкуренции» от 26.07.2006 № 135-ФЗ[20]:

— необходимо уточнение понятий, касающихся нарушения прав на интеллектуальную собственность в электронном виде;

— введение новых мер, направленных на борьбу с группами, занимающимися монополизацией рынка электронных услуг и продуктов.

8. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ[21] Глава 70. Авторское право:

— уточнение понятий, связанных с авторским правом в виртуальной среде и интернете;

— разработка и внедрение механизмов, обеспечивающих защиту прав на интеллектуальную собственность в цифровой экономике.

Совершенствование права в цифровую эпоху — это непрерывный процесс, требующий регулярного анализа и улучшения законодательной базы. Одни из возможных путей совершенствования права в цифровую эпоху — это создание специализированных законодательных органов.

Например, федеральная служба или комитет, занимающиеся разработкой и координацией законодательства в области цифровых технологий.

---

[20] Федеральный закон от 26.07.2006 г. № 135-ФЗ «О защите конкуренции» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

[21] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

Так же поможет привлечение экспертов в области новых технологий в разработку законов. Экспертное мнение может помочь идентифицировать проблемы и определить лучшие практики в области регулирования цифровых технологий.

Помимо этого, упрощение и объединение законодательства в конкретных областях могут упростить и облегчить правоприменение, а также позволить делать более точные выводы в результате судебных разбирательств. Как правило, законы, регулирующие цифровые технологии, касаются многих разных областей права, включая право интеллектуальной собственности, защиту персональных данных, электронную коммерцию, защиту потребителей, информационная безопасность, ответственность за контент в сети Интернет и т.д.

Упрощение и объединение законодательства в пределах каждой из этих областей поможет судам принимать более точные и последовательные решения при условии снижения количества промежуточных заголовков, обозначений и других технических деталей.

Кроме того, упрощение законодательства может помочь предпринимателям, которые работают в области цифровых технологий, понимать свои права и обязанности лучше, особенно если они работают в разных юрисдикциях. Это может означать сокращение времени и стоимости на правовые консультации, что в свою очередь может сделать бизнес в области цифровых технологий более доступным для тех, кто желает начать свою деятельность на этом рынке.

Расширение международного сотрудничества. Цифровые технологии и интернет не имеют границ, поэтому изучение лучших практик и регулятивов в других странах и международных организациях может помочь улучшить законодательную базу в России и установить стандарты международного уровня.

Внедрение новых технологических средств. Развитие автоматизированных систем, таких как блокчейн технологии, машинное обучение, искусственный интеллект, может помочь ускорить и улучшить процесс правоприменения и устранить ошибки.

В целом, обеспечение эффективной и гибкой законодательной базы в об-

ласти цифровых технологий требует глубокой экспертизы, общественного обсуждения и сотрудничества между национальными и международными организациями. Только так можно обеспечить правовую регламентацию, которая соответствует интересам всех заинтересованных сторон и учитывает быстро меняющиеся технологические тенденции и рассчитывать на длительный результат в этой сфере.

Цифровая эпоха требует от юристов адаптации к новым технологиям и парадигмам в правозащите. Вот несколько способов, которые могут помочь юристам адаптироваться к этому новому реальному миру:

1. Обучение технологиям. Юристы должны получить базовые знания о технологиях, которые используются для обработки, хранения и передачи данных. Это может включать понимание технологий облачных вычислений и мобильных приложений, а также блокчейн технологий, которые используются в процессах цифровой идентификации и контрактов.

2. Юристы должны быть в курсе изменений законодательства в области цифровой среды и знать, как они будут влиять на правоприменение в различных юрисдикциях. Они также должны следить за тенденциями развития технологий и их влиянием на законодательство и правоприменение.

3. Развитие навыков коммуникации. Юристы должны развивать свои навыки коммуникации, чтобы эффективно взаимодействовать с клиентами, предлагать максимально эффективные решения и способствовать распространению знаний о цифровых технологиях и с их помощью связанных с ними рисках.

4. Работа с экспертами. Юристы должны искать помощь у экспертов в области цифровых технологий, чтобы получить дополнительную информацию о них и обеспечить максимальную точность в своей работе.

5. Интеграция технологий. Юристы могут использовать новые технологии, такие как программное обеспечение для управления документами, системы электронной подписи и другие инструменты, чтобы сделать свою работу более эффективной и быстрой.

6. Поддержка инноваций в правоведении. Юристы должны активно стимулировать развитие новых подходов и методологий в правоведении, основанных на цифровых технологиях, таких как юридические боты, аналитические системы и подобные инструменты.

7. Расширение спектра услуг. Юристы могут расширить свой спектр услуг, связанных с цифровой эпохой, например, путем предоставления услуг по защите персональных данных, проведению юридических аудитов информационной безопасности и составлению юридических документов в области цифровой экономики.

8. Работа в команде. Юристы могут работать в команде с программистами, инженерами и экспертами в области технологий, чтобы обеспечить эффективное взаимодействие между правом и технологиями.

9. Обновление знаний. Юристы должны постоянно обновлять свои знания в области цифровых технологий и законодательства, связанного с ними. Это может включать участие в курсах и семинарах, чтение специализированных медиа и постоянную самообразовательную работу.

10. Гибкость мышления. Наконец, юристы должны развивать гибкость мышления и умение быстро адаптироваться к новой информации и требованиям рынка цифровых технологий и услуг. В цифровой эпохе, как в управлении бизнесом, так и в правоохранительных органах, гибкость мышления и умение быстро менять свои подходы являются ключевыми компетенциями.

Итак, адаптация юристов к цифровой эпохе требует от них сочетания таких качеств, как техническая и правовая экспертиза, навыки коммуникации и гибкость мышления. Юристы, которые адаптируются к этому новому миру, получат не только конкурентные преимущества, но и станут ключевыми игроками на рынке правовых услуг в условиях цифровой экономики.

Таким образом, все эти способы могут помочь юристам адаптироваться к цифровой эпохе и продолжать работать со своими клиентами, обеспечивая им общее благополучие, справедливость и соответствие требованиям законодательства.

ЗАКЛЮЧЕНИЕ

Исходя из проведенной работы можно сделать вывод, что тема цифровизации права становится все более актуальной в свете необходимости обработки большого объема информации и ускорения процессов судебной системы. Благодаря развитию цифровых технологий нет необходимости в использовании бумажного документооборота, что значительно облегчает работу юристов и судей.

Применение цифровых технологий позволяет автоматизировать повседневные задачи, сокращает время на принятие решений и снижает вероятность ошибок. Кроме того, применение цифровых технологий может помочь в борьбе с коррупцией и неэффективностью судебной системы. Все это позволяет улучшить качество правосудия, обеспечивая быстрое и справедливое решение юридических вопросов.

Цифровизация принесла значительные изменения в юридическую отрасль, повысив эффективность и доступность юридических услуг. Однако существуют и потенциальные риски, связанные с цифровизацией, включая проблемы конфиденциальности и безопасности данных. Специалисты в области права должны сохранять бдительность, чтобы убедиться, что эти риски учтены и что ошибки и сбои не останутся незамеченными. Принимая цифровизацию и внедряя новые технологии в свою практику, юридические фирмы и адвокаты могут адаптироваться к цифровой эпохе юриспруденции и продолжать оказывать высококачественные юридические услуги.

В работе проанализировано:

1. Влияние современных технологий на юридическую отрасль и их возможности для облегчения и улучшения работы в этой сфере.
2. Изменения, произошедшие в законах и правилах, регулирующих использование электронных технологий в юридической практике.
3. Оценка потенциала цифровизации для улучшения процессов в юридической сфере и повышения эффективности работы юристов.

4. Исследование наиболее эффективных методов защиты конфиденциальных данных клиентов при использовании новых технологий.

5. Как использовать новейшие технологии для оптимизации деятельности в правовой области и достижения лучших результатов.

Проведя анализ реализации цифровых технологий, юристы могут оценить их преимущества, такие как быстрота и доступность юридической помощи, более эффективное управление документами. Кроме того, цифровизация может обеспечить лучшую прозрачность процесса работы и повысить уровень доверия граждан к юридическим услугам. Это становится особенно важным в условиях современного информационного общества, где граждане ожидают справедливой и прозрачной работы со стороны юристов. Однако для реализации всех преимуществ цифровизации необходимо соблюдать строгие стандарты безопасности, чтобы гарантировать защиту конфиденциальности данных. Это включает в себя разработку рабочих процессов, которые учитывают потенциальные уязвимости, обучение персонала работе с безопасностью данных, а также использование специализированных технологий и инструментов защиты. Таким образом, цифровизация юридической отрасли представляет собой как вызовы, так и возможности для юристов и адвокатов. Юридические фирмы и специалисты, которые готовы адаптироваться к новым технологиям и сохранять высокие стандарты безопасности, получают возможность расширить свою клиентскую базу и улучшить предоставляемые услуги.

Было выявлено несколько проблем, связанных с цифровизацией в юридической отрасли. Одной из главных проблем является риск нарушения конфиденциальности данных клиентов, который возникает при использовании электронных систем управления документами и хранения данных. Кроме того, возможен риск утечки информации в результате кибератак и других форм киберпреступности.

Другой проблемой является нехватка компетентных адвокатов, которые могут эффективно работать с цифровыми технологиями, умеют верно интерпретировать законодательство в данной области, а так же безопасно хранить и

обрабатывать данные.

Для решения этих проблем были предложены следующие пути:

1. Разработка и внедрение более безопасных электронных систем, которые обеспечивают надежную защиту конфиденциальной информации.

2. Обучение специалистов в области права работе с цифровыми технологиями и развитие соответствующих навыков для обеспечения эффективной и безопасной работы.

3. Проведение учебных курсов, которые будут объяснять важность безопасности данных и стандартов для работников юридической сферы.

4. Усиление законодательной базы для обеспечения более жесткой ответственности за нарушение конфиденциальности и безопасности данных.

5. Разработка учебных материалов и обучающих программ для повышения технической грамотности адвокатов в области цифровых технологий.

6. Создание механизма контроля за использованием цифровых технологий с целью обнаружения возможных нарушений.

В целом, учитывая все преимущества, которые может принести цифровизация для юридической отрасли, при условии правильной реализации и обязательной обеспеченности безопасности данных, вопросы информационной безопасности в юридической сфере должны быть приоритетными и привязаны к законодательным процессам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

I Правовые акты

1 Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

2 Инструкция ФСБ РФ от 20.03.2007 г. № 18 «Об утверждении Правил использования защищенных объектов информатизации» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

3 Кодекс Российской Федерации от 30.12.2001 г. № 195-ФЗ (ред. от 13.06.2023) «Об административных правонарушениях» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

4 Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

5 Постановление Правительства РФ от 01.12.2003 г. № 681 «Об утверждении Правил обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

6 Постановление Правительства РФ от 6.02.2002 г. № 81 «Об утверждении Правил использования электронной подписи при осуществлении государственных и муниципальных услуг» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

7 Постановление ФСТЭК России от 18.04.2013 г. № 21 «Об утверждении требований к защите информации при использовании электронной почты» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

8 Приказ Министерства экономического развития РФ от 6.02.2015 г. № 54 «Об утверждении требований к созданию, использованию и проверке элек-

тронной подписи» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

9 Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 13.06.2023) (с изм. и доп., вступ. в силу с 24.06.2023) [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

10 Федеральный закон от 05.04.2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

11 Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

12 Федеральный закон от 07.02.1992 г. № 2300-1 «О защите прав потребителей» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

13 Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

14 Федеральный закон от 26.07.2006 г. № 135-ФЗ «О защите конкуренции» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

15 Федеральный закон от 27.07. 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» [Электронный ресурс] : Доступ из справ.-правовой системы «КонсультантПлюс».

16 Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] : Доступ из справ.-правовой системы «КонсультантПлюс».

17 Федеральный закон от 27.07.2006 г. № 152-ФЗ «О защите персональных данных» [Электронный ресурс] : Доступ из справ.-правовой системы «КонсультантПлюс».

18 Федеральный закон от 27.12.2002 г. № 184-ФЗ «О техническом регу-

лировании» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

19 Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] : Доступ из справ.-правовой системы «Консультант Плюс».

II Специальная литература

20 Аверьянов, М.А. Цифровая трансформация процессов нормативного регулирования: тенденции, подходы и решения / М. А. Аверьянов, О. В. Баранова, Е. Ю. Кочетова, Р. Л. Сиваков // International Journal of Open Information Technologies. – 2018. – Т. 6, № 11. – С. 42-49.

21 Алексеев, С. С. Общая теория права : В 2 томах / С. С. Алексеев. Том 1. – Москва : Издательство "Юридическая литература" Администрации Президента Российской Федерации, 1981. – 360 с.

22 Анисимова, И. А. Уголовно-правовое значение преступного вреда : специальность 12.00.08 "Уголовное право и криминология; уголовно-исполнительное право" : автореферат диссертации на соискание ученой степени кандидата юридических наук / Анисимова Ирина Анатольевна. – Томск, 2008. – 26 с.

23 Антонов, Я. В. Конституционно-правовые перспективы развития электронной демократии в современной России / Я. В. Антонов // Конституционное и муниципальное право. – 2016. – № 9. – С. 17-20.

24 Антонов, Я. В. Проблемы содержания универсальных демократических прав в системе электронной демократии / Я. В. Антонов // Российская юстиция. – 2017. – № 3. – С. 50-53.

25 Арнаутова, А. А. Автоматизация проведения экспертиз проектов нормативных правовых актов / А. А. Арнаутова // Российская правовая система в условиях четвертой промышленной революции : Материалы VI Московского юридического форума XVI Международной научно-практической конференции. В 3-х частях, Москва, 04–06 апреля 2019 года. Том Часть 1. – Москва: Издательство Проспект, 2019. – С. 68-70.

26 Архипов, В. В. Интернет-право : учебник и практикум для вузов / В. В. Архипов. — Москва : Издательство Юрайт, 2023. — 249 с.

27 Архипов, В. В. Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике / В. В. Архипов, В. Б. Наумов // Труды СПИИРАН. – 2017. – № 6(55). – С. 46-62.

28 Архипов, В. В. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности / В. В. Архипов, В. Б. Наумов // Закон. – 2017. – № 5. – С. 157-170.

29 Бачило, И. Л. Информационное право : учебник для вузов / И. Л. Бачило. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 419 с.

30 Бачило, И. Л. О трансформации институтов «государство» и «право» в информационном обществе / И. Л. Бачило, М. А. Шмаков // Государство и право. — 2017. — № 11. — С. 82–83.

31 Бегишев, И. Р. Цифровые технологии и право : Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. Том 2. – Казань: Издательство "Познание", 2022. – 556 с.

32 Беляев, М. А. Модель развития права: от "эволюции" к "взрыву" / М. А. Беляев // Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2016. – № 3. – С. 9-20.

33 Бехманн, Г. Общество знания - трансформация современных обществ / Г. Бехманн // Концепция "общества знания" в современной социальной теории : Сб. науч. тр / Центр социал. науч.-информ. исслед. Отд. социологии и социал. психологии; Отв. ред. Д.В. Ефременко. – МОСКВА, 2010. – С. 39-65.

34 Васильев, А. А. "Умные машины" и искусственный интеллект как вызовы для этики и юриспруденции / А. А. Васильев, О. В. Васильева, Д. Шпопер // Уголовно-процессуальные и криминалистические чтения на Алтае, Барнаул, 10–12 июля 2018 года / Отв. ред. С.И. Давыдов, В.В. Поляков. Том ВЫПУСК

XV. – Барнаул: Алтайский государственный университет, 2018. – С. 44-49.

35 Васильев, А. А. Искусственный интеллект: правовые аспекты / А. А. Васильев, Д. Шпопер // Известия Алтайского государственного университета. – 2018. – № 6(104). – С. 23-26.

36 Васильев, А. А. Искусственный интеллект: этические и правовые аспекты / А. А. Васильев, О. В. Васильева // Правовая мысль в образовании, науке и практике. – 2018. – № 4(8). – С. 9-12.

37 Васильев, А. А. Правовое регулирование робототехники и искусственного интеллекта в Европейском Союзе / А. А. Васильев, Ж. И. Ибрагимов // Российско-азиатский правовой журнал. – 2019. – № 1. – С. 50-54.

38 Васильев, А. А. Развитие науки и технологий: цель или средство прогресса? / А. А. Васильев, О. Е. Зацепина // Управление наукой: теория и практика. – 2022. – Т. 4, № 4. – С. 204-217.

39 Васильев, А. А. Термин "искусственный интеллект" в российском праве: доктринальный анализ / А. А. Васильев, Д. Шпоппер, М. Х. Матаева // Юрислингвистика. – 2018. – № 7-8. – С. 35-44.

40 Васильев, А. А. Этико-правовые аспекты использования «умных машин» / А. А. Васильев, О. В. Васильева // Высшая школа: традиции и инновации : материалы Междунар. науч.-практ. конф., посвященной 20-летию Казахского гуманитарно-юридического университета (16 ноября 2018 г.) : 2 т. — Т. 1 / под науч. ред. Ш.А. Курманбаевой. — Семей: Интеллект, 2018.

41 Гаджиев, Г. А. Может ли робот быть субъектом права? (поиск правовых форм для регулирования цифровой экономики) / Г. А. Гаджиев, Е. А. Войниканис // Право. Журнал Высшей школы экономики. – 2018. – № 4. – С. 24-48.

42 Гоннова, С. М. Национальные системы научно-технической информации - потенциал для развития научной дипломатии в СНГ / С. М. Гоннова, Е. Ю. Разуваева // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2019. – № 12. – С. 1-18.

43 Дайвер, Л. Цифровые технологии и правовая аргументация: влияние статистических юридических технологий на право / Л. Дайвер, П. Макбрайд //

Теоретическая и прикладная юриспруденция. – 2022. – № 3(13). – С. 8-22.

44 Дремлюга, Р. И. Искусственный интеллект — субъект права: аргументы за и против / Р. И. Дремлюга, О. А Дремлюга // Правовая политика и правовая жизнь. — 2019. — № 2. — С. 120–125.

45 Дремлюга, Р. И. Искусственный интеллект как социальный регулятор: за и против / Р. И. Дремлюга, А. С. Кошель // Азиатско-тихоокеанский регион: экономика, политика, право. – 2018. – Т. 20, № 3. – С. 55-68.

46 Дремлюга, Р. И. Правовые аспекты применения предиктивной аналитики в правоохранительной деятельности / Р. И. Дремлюга, В. В. Решетников // Азиатско-тихоокеанский регион: экономика, политика, право. – 2018. – Т. 20, № 3. – С. 133-144.

47 Дремлюга, Р. И. Системы искусственного интеллекта как средство совершения преступления / Р. И. Дремлюга // Информационное право. – 2019. – № 1. – С. 21-25.

48 Жмуров, Д. В. Даркнет как ускользающая сфера правового регулирования / Д. В. Жмуров // Сибирские уголовно-процессуальные и криминалистические чтения. – 2020. – № 1(27). – С. 89-98.

49 Законодательство, судебная система, новости и аналитика. Все о юридическом рынке [Электронный ресурс]. – Режим доступа : https://www. pravo.ru. - 15.03.2023.

50 Корнев, А. В. Цифровые технологии и правовая система Российской Федерации: проблемы и перспективы / А. В. Корнев // Российская правовая система в условиях четвертой промышленной революции : Материалы VI Московского юридического форума XVI Международной научно-практической конференции. В 3-х частях, Москва, 04–06 апреля 2019 года. Том Часть 1. – Москва: Издательство Проспект, 2019. – С. 4-9.

51 Медведев, Е. В. Уголовное право России. Общая часть : учебное пособие для вузов / Е. В. Медведев. — Москва : Издательство Юрайт, 2023. — 178 с.

52 Портал государственных услуг Российской Федерации [Электронный

ресурс]. – Режим доступа : https://www.gosuslugi.ru/. - 01.03.2023.

53 Стрельцов, А. А. Теоретические и методологические основы правового обеспечения информационной безопасности России : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : автореферат диссертации на соискание ученой степени доктора юридических наук / Стрельцов Анатолий Александрович. – Москва, 2004. – 47 с.

54 Танимов, О. В. Цифровое право: основные сущностные аспекты / О. В. Танимов, А. Р. Шевченко // Российская юстиция. – 2019. – № 10. – С. 6-9.

55 Чупров, В. И. Молодежь как субъект социально-экономической трансформации / В. И. Чупров // Аналитический вестник Совета Федерации Федерального Собрания РФ. – 1999. – № 15(103). – С. 21-27.