

ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ

Научная статья

УДК 343.98; 004; 005.7 DOI: 10.61260/2074-1626-2024-4-91-110

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ВЕДОМСТВЕННЫХ ВУЗОВ: ГАРМОНИЗАЦИЯ НОРМАТИВНОЙ ПРАВОВОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

✉ Уткин Николай Иванович;

Шеншин Виктор Михайлович;

Шестаков Александр Викторович.

Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия

✉ utkinnick@mail.ru

Аннотация. Цифровая трансформация во всех сферах деятельности в Российской Федерации является в настоящее время основным вектором развития страны, в том числе федеральных органов исполнительной власти, их подведомственных структур и образовательных организаций, которая осуществляется в непростых условиях информационного и технологического воздействия на различные области, в том числе информационную безопасность. Необходимость регуляторных изменений и гармонизации нормативной правовой базы при реализации мероприятий и работ по цифровой трансформации многоуровневых организационных систем различного типа очевидна, а проблематика, несомненно, актуальна. В области информационной безопасности гармонизация регламентирующих документов должна осуществляться не по факту полученного результата или организации и проведения работ соответствующего этапа или стадии цифровой трансформации, а с определенным опережением, применительно ко всем компонентам и составляющим организационных систем. Подведомственные образовательные организации находятся в специфических вертикалях нормативных правовых отношений, реализуемых уровнями образования в соответствии с федеральным законодательством, ведомственных организационных структур управления, а применительно к информационной безопасности – в системе мегарегулирования технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации, что обуславливает комплексное исследование обеспечения информационной безопасности посредством гармонизации нормативной базы цифровой трансформации ведомственных образовательных организаций.

Ключевые слова: гармонизация нормативной базы, цифровая трансформация, образовательная организация, информационная безопасность

Для цитирования: Уткин Н.И., Шеншин В.М., Шестаков А.В. Цифровая трансформация ведомственных вузов: гармонизация нормативной правовой базы информационной безопасности // Право. Безопасность. Чрезвычайные ситуации. 2024. № 4 (65). С. 91–110. DOI: 10.61260/2074-1626-2024-4-91-110.

Scientific article

DIGITAL TRANSFORMATION OF DEPARTMENTAL UNIVERSITIES: HARMONIZATION OF THE REGULATORY FRAMEWORK FOR INFORMATION SECURITY

✉ Utkin Nikolai I.;

Shenshin Viktor M.;

Shestakov Alexander V.

Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia

✉ utkinnick@mail.ru

Abstract. Digital transformation in all spheres of activity in the Russian Federation is currently the main vector of development of the country, including federal executive authorities, their subordinate structures and subordinate educational organizations, which is carried out in difficult conditions of information and technological impact on various areas, including information security. The need for regulatory changes and harmonization of the regulatory framework in the implementation of measures and works on the digital transformation of multilevel organizational systems of various types is obvious, and the issue is undoubtedly relevant. In the field of information security, harmonization of regulatory documents should be carried out not upon the fact of the result obtained or the organization and conduct of work at the appropriate stage or stage of digital transformation, but with a certain advance, in relation to all components and components of organizational systems. Subordinate educational organizations are located in specific verticals of regulatory legal relations implemented by levels of education in accordance with federal legislation, departmental organizational management structures, and in relation to information security – in the system of mega-regulation of technological independence and security of the critical information infrastructure of the Russian Federation, which determines a comprehensive study of information security through harmonization of the regulatory framework of digital transformation of departmental educational organizations.

Keywords: information security competencies, competence models, competence deficit, assessment of competence deficit

For citation: Utkin N.I., Shenshin V.M., Shestakov A.V. Digital transformation of departmental universities: harmonization of the regulatory framework for information security // *Pravo. Bezopasnost'. Chrezvychajnye situacii* = Right. Safety. Emergency situations. 2024. № 4 (65). P. 91–110. DOI: 10.61260/2074-1626-2024-4-91-110.

Введение

Цифровая трансформация во всех областях жизнедеятельности человека, в том числе в области образования, затронула не только организационные и технологические аспекты, но и объективно обусловила возникновение проблем правового и технического регулирования обеспечения защиты информации от неправомерных действий или кибербезопасности, доступа к информации, а также обеспечения конфиденциальности и целостности персональных данных в цифровой среде (интернет-среде, цифровой образовательной среде, цифровой научно-образовательной среде и другим подобным).

Правовые аспекты кибербезопасности, соответственно, можно рассматривать в контексте обеспечения цифровой безопасности применительно к цифровой трансформации:

- 1) правовым нормам – в регламентации ограниченной и запрещенной к распространению информации, а также мер ответственности за нарушение правовых норм;
- 2) институциональным основам – в регулировании полномочий системы органов в сфере безопасности (суды, Роскомнадзор, ФСТЭК России, Минцифры России и др.);
- 3) техническим средствам – в регламентации разработки, внедрения и эксплуатации технических средств и информационных технологий (ИТ) противодействия цифровым угрозам (антивирусные программы, программы-фильтры, системы обнаружения вторжений, технические средства контроля) в создаваемых в ходе цифровой трансформации цифровых средах.

Цифровая защита от чрезвычайных ситуаций при таком семантическом подходе может рассматриваться как правовое регулирование в области кибербезопасности информационных инфраструктур различного назначения или защищенности российского ИТ-ландшафта при угрозе возникновения и возникновении чрезвычайных ситуаций, что налагает особую значимость проблематики для образовательных организаций, подведомственных федеральному органу исполнительной власти (ОИВ), осуществляющих функции в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, обеспечения пожарной безопасности и безопасности людей на водных объектах [1].

Теоретические основы и методы исследования

Теоретическую основу исследования составляют методы онтологического анализа соответствия предметно-регуляторной области и формального описания терминологических структур на пространстве нормативных правовых документов, регулирующих отношения информационной безопасности (ИБ) при цифровой трансформации ведомственных образовательных организаций высшего образования. Объектом данного исследования выступает проблема гармонизации нормативно-правового обеспечения ИБ при цифровой трансформации ведомственных образовательных организаций на примере МЧС России.

Результаты и обсуждение

Цифровая трансформация отрасли – комплексное преобразование деятельности участников отрасли и ОИВ Российской Федерации, связанное с переходом к новым бизнес-моделям, каналам коммуникаций, а также процессам и культуре, которые базируются на новых подходах к управлению данными с использованием цифровых технологий.

Подведомственные вузы, в том числе МЧС России, находятся под влиянием двух регуляторных векторов цифровой трансформации:

- первый – регулирование цифровой трансформации федеральных ОИВ и соответствующих отраслей экономики по линии МЧС России;
- второй – регулирование цифровой трансформации науки и образования по линии Минобрнауки России и Минпросвещения России.

Термины и перечень правовых документов, которыми определены основные контрольные макропоказатели цифровой трансформации государственного управления и порядок оценки достижения «цифровой зрелости» отраслей экономики и федеральных ОИВ, представлены в табл. 1.

Таблица 1

Нормативная правовая база в области цифровой трансформации

Документ	Данные документа	Содержание
1	2	3
Нормативная правовая база в области цифровой трансформации отраслей и ОИВ Российской Федерации		
1. О национальных целях развития Российской Федерации на период до 2030 г.	Указ Президента Российской Федерации от 21 июля 2020 г. № 474 (утратил силу, 2024 г.)	В качестве одного из целевых показателей национальной цели «цифровая трансформация» указано достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы

1	2	3
2. О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных ОИВ и органов управления государственными внебюджетными фондами	Постановление Правительства Российской Федерации от 10 октября 2020 г. № 1646 (с изм. от 1 июля 2024 г.)	Порядок разработки, утверждения и реализации федеральными ОИВ и органами управления государственными внебюджетными фондами ведомственных программ цифровой трансформации
3. Об утверждении стратегического направления в области цифровой трансформации государственного управления	Распоряжение Правительства Российской Федерации от 22 октября 2021 г. № 2998р (утратило силу, 2024 г.)	Достижение «цифровой зрелости» ключевых отраслей экономики, социальной сферы, в том числе здравоохранения и образования, а также государственного управления; доля массовых социально значимых услуг, доступных в электронном виде; увеличение вложений в отечественные решения в сфере ИТ
4. Об утверждении стратегического направления в области цифровой трансформации государственного управления	Распоряжение Правительства Российской Федерации от 16 марта 2024 г. № 637р	Сокращение сроков предоставления госуслуг в онлайн-формате, переход на электронный документооборот органов местного самоуправления, государственных и муниципальных учреждений, а также на автоматизацию и упрощение модуля ввода/вывода
5. О национальных целях развития Российской Федерации на период до 2030 г. и на перспективу до 2036 г.	Указ Президента Российской Федерации от 7 мая 2024 г. № 309	П. 1. Национальная цель – цифровая трансформация государственного и муниципального управления, экономики и социальной сферы. П. 9. До 1 сентября 2024 г. представить национальные проекты... «Экономика данных и цифровая трансформация государства»
Нормативная правовая база в области цифровой трансформации МЧС России		
6. Нормативная правовая база в области цифровой трансформации МЧС России	Распоряжение МЧС России от 25 июля 2022 г. № 800	Срок действия: 1 января 2022 г. – 31 декабря 2024 г. Целей – 6. Показателей – 250. По состоянию на 1 декабря 2024 г. «доля должностных лиц МЧС России, участвующих в цифровой трансформации и прошедших обучение в области ИБ, составила 21 %»

Следует отметить, что в 2024 г. Правительством Российской Федерации и федеральными органами исполнительной власти проводится актуализация ранее принятых подходов и регламентов и, соответственно, изменений в нормативной правовой базе.

В МЧС России цифровая трансформация проводится в соответствии с Ведомственной программой на 2022 г. и на плановый период 2023 и 2024 гг. Программой определены шесть целей и более 250 показателей. К ним, в частности, относятся показатели обучения должностных лиц в области цифровой трансформации и ИБ. Срок ее действия заканчивается 31 декабря 2024 г. В настоящее время идет активная работа профильных департаментов и руководства МЧС России по согласованию целей и показателей Ведомственной программы с Минцифры России и профильными департаментами Правительства Российской Федерации с учетом результатов разработки показателей национальных проектов «Экономика данных и цифровая трансформация государства».

В январе 2024 г. Правительством Российской Федерации был подготовлен рейтинг цифровой трансформации федеральных министерств, в котором 18 ведомств показали высокий результат эффективности, остальные – средний и ниже среднего [2].

Критериями оценки были: исполнение бюджетных обязательств по реализации задач цифровой трансформации; выполнение ключевых показателей эффективности; сроки и качество выполнения поручений Правительства Российской Федерации руководителями цифровой трансформации федеральными органами власти. При оценке эффективности и результативности цифровой трансформации учитывалась степень достижения более 20 показателей рейтинга эффективности и результативности руководителей цифровой трансформации, а также выполнения ключевых результатов реализации ведомственных программ цифровой трансформации, в том числе переход ведомства на использование единого коммуникационного сервиса госслужащего [3].

ВЫСОКАЯ РЕЗУЛЬТАТИВНОСТЬ ФРЦТ					
	ВАРЕНЦОВ Михаил Александрович	РОСГВАРДИЯ		ХАБАРОВ* Александр Владимирович	ФСИН РОССИИ
	ШЕРЕДИН Роман Валериевич	РОСИМУЩЕСТВО		МАРТЫНОВА Елена Валерьевна	РОСРЕЕСТР
	ГЕРАСИМОВ Антон Андреевич	МЧС РОССИИ		ТИТОВ Максим Александрович	МИНСЕЛЬХОЗ РОССИИ
	КОЧЕТОВА Светлана Михайловна	РОСОБРНАДЗОР		ВАСИЛЬЧЕНКО Юрий Леонтьевич	РОСАЛЬКОГОЛЬТАБАККОНТРОЛЬ
	ПАВЛЮКОВ Дмитрий Юрьевич	РОСЗДРАВНАДЗОР		ХОЛОДОВ* Алексей Викторович	РОСПРИРОДНАДЗОР
	ШЕРЕМЕТЦЕВ Эдуард Михайлович	МИНЭНЕРГО РОССИИ			

* 2023 год – исполняющий обязанности РЦТ

* 2023 ГОД – ИСПОЛНЯЮЩИЙ ОБЯЗАННОСТИ РЦТ

Рис. 1. Результаты цифровой трансформации федеральных ОИВ [3]

Как заявлено вице-премьером Дмитрием Чернышенко, кадровая ротация руководителей цифровой трансформации по итогам 2023 г. составит более 15 % [2]. Впервые в истории рейтинга цифровой трансформации Лидером среди федеральных ОИВ, МЧС России – на третьем месте, уступив Росгвардии и Росимууществу. При составлении рейтинга 2024 г. будут учитываться импортонезависимость программного обеспечения, ИБ, переход на платформу «ГосТех».

В аспекте цифровой трансформации в подведомственной образовательной организации (Санкт-Петербургский университет ГПС МЧС России, далее – Университет) с 2018 по 2024 г. последовательно выполнялись программы развития Университета в сфере информатизации, направленные на повышение качества образования и формирование

эффективной системы управления образовательным процессом на основе использования информационных и телекоммуникационных технологий. Цифровая трансформация Университета является комплексным преобразованием его деятельности, связанным с переходом к новым бизнес-моделям цифрового Университета, каналам коммуникаций, а также процессам и культуре, которые базируются на новых подходах к управлению данными с использованием цифровых технологий. По направлению цифровой трансформации Университета программные мероприятия развития на период 2024–2028 гг., которые утверждены МЧС России, реализуются по четырем стратегическим целям («Развитие цифровых сервисов»; «Модернизация инфраструктуры»; «Обеспечение информационной безопасности»; «Обеспечение антитеррористической защищенности»). Мероприятиями предусмотрен ежегодный нарастающий (в среднем 10-процентный) прирост основных показателей развития цифровых сервисов, инфраструктуры с учетом обеспечения ИБ и импортозамещения.

Цифровая трансформация подведомственных вузов осуществляется под непрерывным руководством федерального ОИВ, в том числе по направлению организации документооборота и служебных мессенджеров, регламентация которых гармонизирована с действующей нормативной правовой базой в части электронного документооборота [4–6], межведомственного взаимодействия [7], мессенджеров [8].

Приказом МЧС России от 14 мая 2021 г. № 315 «Об утверждении Инструкции по делопроизводству в территориальных органах Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, учреждениях и организациях, находящихся в ведении Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий» [9] определено, что:

- 1) документы поступают в территориальные органы, организации МЧС России посредством почтовой, фельдъегерской, специальной связи и по каналам электронной связи;
- 2) каналы электронной связи включают в себя систему электронного документооборота (СЭД), интегрированную с системой межведомственного электронного документооборота МЭДО [7], единой системой межведомственного электронного взаимодействия (СМЭВ) в целях предоставления государственных и муниципальных услуг в электронной форме;
- 3) по каналам СЭД, МЭДО, СМЭВ, а также по каналам сети «Интернет» (сопряженным с СЭД) поступают электронные документы или их электронные копии;
- 4) по каналам СЭД производится обмен документами между центральным аппаратом МЧС России, территориальными органами, организациями МЧС России, их структурными подразделениями.

В Университете для ведомственной компоненты СЭД развернуты выделенные автоматизированные рабочие места. Для их возможного использования в других информационных процессах Университетом в июле – августе 2024 г. были организованы и успешно проведены испытания (проверки) модернизированных средств защиты информации компании Конфидент, которые позволяют реализовать дополнительные функции.

Распоряжением Правительства Российской Федерации от 16 марта 2024 г. № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» [8] предусмотрено создание автоматизированного рабочего места госслужащего с отечественным программным обеспечением (КС АРМ ГС) (рис. 2). Сервисы содержат обмен сообщениями, электронную почту, видеоконференцсвязь и другие актуальные услуги. В 2024 г. проведен ребрендинг названия КС АРМ ГС на название «Среда». Соответствующими документами МЧС России определен переход должностных лиц МЧС России и подведомственных образовательных организаций на новый защищенный мессенджер, который более функционален, чем ранее традиционно используемые. В сервисе «Среда» применяется защита данных, соответствующая требованиям приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [10], требованиям, регламентируемым Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [11], а также обеспечивающая безопасность персональных данных не ниже третьего уровня защищённости. Реализовано шифрование при передаче пользовательских данных: для подключения пользователей используется протокол «https», для подключения инфраструктуры – средства криптографической защиты информации [12].

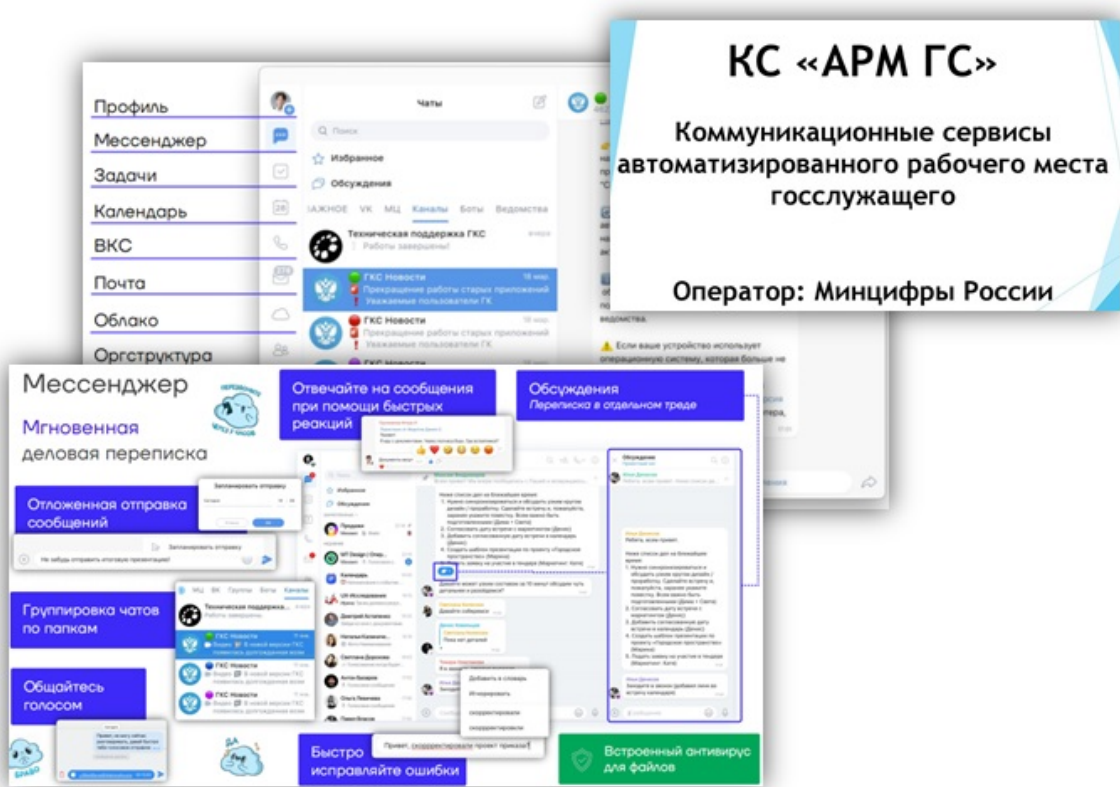


Рис. 2. Цифровая трансформация коммуникаций с применением Коммуникационного сервиса «Автоматизированное рабочее место государственного служащего» [12]

Основные нормативные правовые документы второго вектора цифровой трансформации по линии науки и образования представлены в табл. 2. В соответствии с ними гармонизированы ведомственные документы и локальные акты Университета.

Таблица 2

Нормативная правовая база цифровой трансформации в области образования

Документ	Данные документа	Содержание
1	2	3
1. О национальных целях развития Российской Федерации на период до 2030 г.	Указ Президента Российской Федерации от 21 июля 2020 г. № 474 (утратил силу, 2024 г.)	В качестве одного из целевых показателей национальной цели «цифровая трансформация» указано достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы

1	2	3
2. Об утверждении стратегического направления в области цифровой трансформации науки и высшего образования (для подведомственных вузов Минобрнауки России)	Распоряжение Правительства Российской Федерации от 21 декабря 2021 г. № 3759р	Проекты: «Датахаб», «Архитектура цифровой трансформации», «Цифровой университет», «Единая сервисная платформа науки», «Маркетплейс ПО и оборудования», «Цифровое мышление», «Сервис хаб»
3. Стратегия цифровой трансформации отрасли науки и высшего образования (для подведомственных вузов Минобрнауки России)	Утверждена Минобрнауки России 29 декабря 2022 г.	Пять треков (направлений): Архитектура ЦТ; Развитие цифровых сервисов; Управление данными; Модернизация инфраструктуры; Управление кадровым потенциалом (отрасли)
4. О национальных целях развития Российской Федерации на период до 2030 г. и на перспективу до 2036 г.	Указ Президента Российской Федерации от 7 мая 2024 г. № 309	П. 1. Национальная цель – цифровая трансформация государственного и муниципального управления, экономики и социальной сферы. П. 9. До 1 сентября 2024 г. представить национальные проекты... «Экономика данных и цифровая трансформация государства»

В рамках проекта «Единая сервисная платформа науки» [13] будут использоваться технологии искусственного интеллекта (ИИ) в части формирования рейтингов научных организаций и вузов, верификации исследований, формирования портфолио научных организаций и вузов, а также технологии распределенного реестра в части верификации исследований. В рамках проекта «Маркетплейс программного обеспечения и оборудования» будут использоваться технологии интернета вещей в части мониторинга за состоянием оборудования научных организаций и вузов, а также технологии ИИ для анализа данных, поступающих от устройств, подключенных к интернету вещей. Базовое событие процесса цифровой трансформации в сфере науки и высшего образования – это формирование и распространение новых, с точки зрения содержания, моделей работы организаций. В их основе – комбинация непрерывного профессионального развития, новых цифровых сервисов и инструментов, инфраструктурных и организационных условий для внедрения изменений, сопровождение участников при освоении новых ролей и методов рабочего взаимодействия.

Цифровая трансформация приемной кампании в образовательных организациях Российской Федерации (рис. 3) обеспечивается посредством специально созданного цифрового сервиса Единого портала государственных услуг¹ «Суперсервис поступление в вуз онлайн» (ЕПГУ ССПВО) для организации удаленной регистрации абитуриентов, online-поддачи заявлений, вывода пофамильных списков и экрана подачи заявлений, доступ образовательных организаций к которому организуется с применением сертифицированных отечественных программных средств, например, компании ООО «Лаборатория ММИС» – «Модуля интеграции с ФИС ГИА и Приема» для обмена данными приемной кампании с федеральными информационными системами (ИС) государственно итоговой аттестации и приема граждан [14].

¹ Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг» (ЕПГУ)

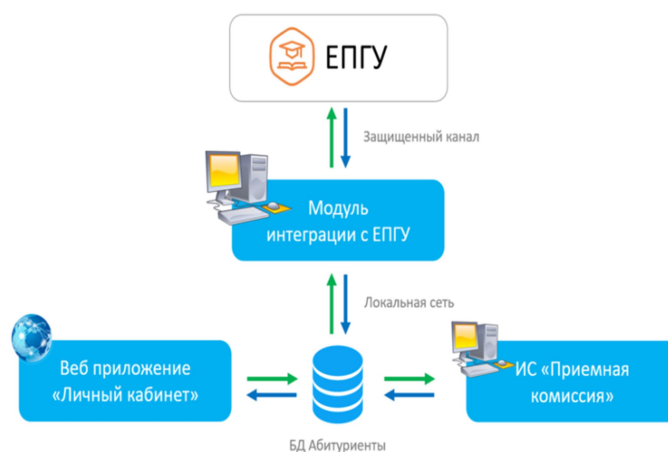


Рис. 3. Цифровая трансформация приемной компании образовательной организации через государственный портал [14]

Процедуры подключения к ЕПГУ ССПВО и работы пользователей в ней гармонизированы с правовыми, нормативно-техническими и эксплуатационными документами организации подключения к продуктовым средам ЕСИА², ЕПГУ и Технологическому portalу [15–17].

Цифровая трансформация вузовских структурных подразделений общего образования и среднего профессионального образования (рис. 4) организуется в рамках реализации мероприятий федерального проекта «Цифровая образовательная среда» национального проекта «Образование» [18, 19] посредством подключения подразделений к региональным компонентам, например, к Комплексной автоматизированной информационной системе каталогизации ресурсов образования Санкт-Петербурга (КАИС КРО – Электронный Дневник) [20], регламентация которого гармонизирована нормативными документами и локальными актами ОИВ субъекта Российской Федерации.

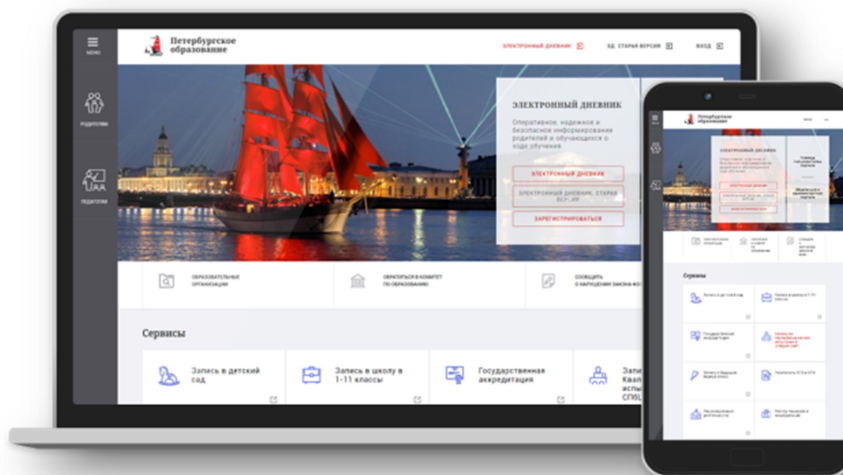


Рис. 4. Цифровая трансформация общеобразовательной организации через цифровую образовательную среду [21]

² Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА).

Цифровая трансформация образовательного процесса образовательной организации высшего профессионального образования должна соответствовать действующим нормам законодательства в области образования [22] на основе гармонизированных локальных актов организации и обеспечиваться применением сертифицированных отечественных программных средств, например, «1С: Университет», разработанных на технологической платформе «1С: Предприятие 8.3», которое позволяет реализовать различные модели ведения приемной кампании, планирование учебного процесса, расчет и распределение нагрузки, управление контингентом, работа с приказами, учет платных услуг. Для организации системы дистанционного обучения (LMS) предусматривается комплексирование нескольких программных продуктов на платформе «1С: Предприятие 8.3», для корпоративного применения – как представлено на рис. 5, а для образовательной организации – на рис. 6 [23].



Рис. 5. Организация системы дистанционного обучения на базе решений 1С [23]



Рис. 6. Электронная информационная образовательная среда на базе решений 1С [23]

Возможности цифровой трансформации дистанционной образовательной среды университета расширены за счет реализованной государственной системы «Современная цифровая образовательная среда», которая развернута в соответствии с требованиями нормативных правовых актов Правительства Российской Федерации [18]. Обеспечивается доступ по принципу «одного окна» к онлайн-курсам, реализуемым различными образовательными организациями и платформами. Для обучающихся по программам высшего и дополнительного профессионального образования предусмотрены формирование и ведение реестра онлайн-курсов, организация централизованного учета результатов обучения на них, учет образовательных программ и результатов их освоения, подключение пользователей с помощью ЕСИА.

Цифровая трансформация ведомственных образовательных организаций проходит в условиях масштабных атак на информационную инфраструктуру Российской Федерации. За первое полугодие 2024 г. [24]:

- уровень атак на вузы в период приемной кампании с 1 по 15 июля 2024 г. возрос в 4,5 раза (4–700 тыс. запросов/с, длительность атак 4–53 мин);
- атаки продолжились против «облачных» сервисов государственных информационных систем; DDoS-атаки на ВТБ, Альфа-Банк, Росбанк, Газпромбанк, СПБ, Сбербанк (24 июля 2024 г.), Центробанк России (29 июля 2024 г.);
- атаки зафиксированы на технологические системы ЖКХ (программное обеспечение SCADA-систем) через коммуникации Starlink, в частности, на устройства управления лифтами (контроллеры).

В этот же период вступили в действие нормативные правовые документы, регламентирующие переход сервисов государственных организаций публично-правовой сферы на единые технологические платформы [25], опубликованы проекты о запрещении информации о VPN-сервисах [26], изменений требований о защите информации, не составляющей государственную тайну, и по обеспечению безопасности значимых объектов критической информационной инфраструктуры [27, 28].

Представленные факты указывают на необходимость гармонизации не только нормативной правовой базы в области ИБ с международными документами, но и на необходимость гармонизации ведомственных и локальных вузовских документов в области цифровой трансформации организаций, в области повышения уровня правовых знаний киберкультуры (кибергигиены) и киберграмотности в вузовской среде с нормами обеспечения ИБ, включая вопросы регулирования проведения внутренних аудитов безопасности и подготовки аудиторов.

Масштабное развитие и применение цифровых технологий в государственном управлении, экономике, социальной сфере и техносфере, реализация задачи цифровизации общественной жизни отражаются на правовом регулировании и приводят к изменениям в правовой сфере, созданию правовых норм, регулирующих отношения, связанные с цифровизацией, а также трансформации самого права, правовых явлений и категорий под влиянием цифровизации.

Этот процесс порой развивается не всегда организованно, а порой стихийно, что объективно создает трудности и в сфере функционирования государственных ИС, в том числе МЧС России.

В апреле 2024 г. под эгидой МИД России проведен I форум «Право цифровой безопасности» по актуальным проблемам правовых рисков цифровизации, укрепления цифрового суверенитета и безопасности Российской Федерации.

В рамках программных мероприятий Форума состоялась Стратегическая сессия-практикум «Цифровая защита от чрезвычайных ситуаций», организованная МЧС России, с вкладом Университета в обсуждение обеспечения контроля и аудита состояния защищенности российского ИТ-ландшафта в форме доклада по использованию ведомственного киберполигона, представляющего собой новый класс организационно-технических систем и предназначенного для формирования непрерывной образовательной

киберсреды в области ИБ для должностных лиц, выполняющих профессиональную деятельность в ведомственной системе обеспечения ИБ (СОИБ) [29]. Его место и роль в образовательной организации представлена на рис. 7.



Рис. 7. Электронная информационная образовательная среда на базе решений 1С [23]

Ведомственный киберполигон как организационно-техническая система предоставляет ряд сервисов различных треков, перечень которых приведена в табл. 3.

Таблица 3

Сервисы треков организационно-технической системы класса «киберполигон»

Трек кибертренировок (киберучений)	Трек образовательный	Трек испытательный
1. Сервисы профориентированного образования по направлению ИБ с применением компьютерно-моделирующей среды прототипов и цифровых двойников реальных фрагментов информационной инфраструктуры		1. Сервисы исследования проблемных аспектов кибербезопасности ведомственной информационной инфраструктуры
2. Сервисы формирования групповых компетенций сил обеспечения ИБ	2. Сервисы формирования, апробации и внедрения новых дидактических средств	2. Сервисы формирования документов методического и организационного обеспечения СОИБ
3. Сервисы формирования и регламентированного функционирования киберсреды информационной поддержки СОИБ в текущей деятельности и по программам развития		3. Сервисы технической поддержки компонент ведомственной СОИБ
4. Сервисы сбора, обработки и предоставления сведений о новых инцидентах		
5. Сервисы выработки предложений по мерам киберзащиты		
	6. Сервисы поддержки в актуальном состоянии информации об информационной инфраструктуре	

Наиболее важными являются сервисы, которые направлены на обеспечение гармонизации правовых локальных документов в области ИБ, например, сервисы формирования и регламентированного функционирования киберсреды информационной поддержки СОИБ в текущей деятельности и по программам развития; сервисы формирования документов методического и организационного обеспечения СОИБ. Для их реализации необходимы научно-обоснованные результаты разработки принципов, методологии и элементов технологии решения прикладных задач гармонизации ведомственной нормативной правовой базы в части требований кибербезопасности и ИБ.

Анализ концептуальной идеи о циклических правовых массивах, предложенной учеными Института законодательства и сравнительного правоведения при Правительстве Российской Федерации академиком РАН Т.Я. Хабриевой и профессором Н.Н. Черногором [30, 31], наводит на мысль о том, что многочисленные правовые аспекты ИБ возможно образуют такой правовой массив.

Проблеме гармонизации нормативно-технических документов уделено значительное внимание международными и национальными организациями по стандартизации. Так, например, в ISO 860 даны определения базовым терминам: «гармонизация понятий», «гармонизация системы понятий», «гармонизация терминов»; в ISO 704 определены условия для образования новых терминов в соответствии с принципами и методами терминологии; в ISO 1087 указывается, что результатом стандартизации терминологии является набор обозначений одного понятия, которые принадлежат специальным языкам; в ISO 10241 закрепляется цель регламентации терминологии в соответствии одного понятия одному термину (то есть гармонизация направлена на однозначное толкование и понимание). Исходя из отечественной практики нормативно-технического регулирования в части регламентированных терминов «гармонизированный стандарт», «эквивалентный стандарт», «идентичный стандарт», «модифицированный стандарт», «сопоставимый стандарт» по ГОСТ Р 1.7–2014, при применении этого прецедента к ведомственной нормативно-правовой базе в части требований кибербезопасности и ИБ ряд «негармонизированных» документов может быть отнесен к группам «неэквивалентных» или «сопоставимых».

Следовательно, основная цель гармонизации ведомственной нормативно-правовой базы в части требований кибербезопасности и ИБ заключается в том, чтобы ведомственная система обеспечения ИБ была результативной и экономически более эффективной.

В условиях цифровой трансформации государства, общества и предпринимательства, как показано в работе Т.А. Поляковой, А.В. Минбалева и В.Б. Наумова [32], требуется учитывать опыт разработки концепций и проектов Информационных и Цифровых кодексов.

Известен ряд работ, результаты которых направлены на установление сходства текстовых документов с целью оценки целесообразности последующей гармонизации одного из них. Например, в работе А.А. Хорошилова, А.В. Кан, Е.А. Евдокимова, С.Г. Пицхелаури [33] рассмотрен метод оценки сходства текстов, который основан на анализе сравнения предложений из различных текстов. В работе зарубежных ученых Исламской Республики Иран в области мер сходства попарных документов на основе текущего набора термина [34] указывается, что большинство показателей сходства позволяют судить о сходстве между двумя документами на основе весов терминов и информационного содержания, общего для двух документов.

Проблемы трансформации права в условиях новой цифровой реальности настоятельно требуют совершенствования, интеграции и гармонизации правовых подходов к нормативному регулированию ИБ и защиты информации возможно в таком обособленном циклическом правовом массиве, в целях предупреждения, прогнозирования и смягчения последствий чрезвычайных ситуаций и пожаров, а также осуществление специальных, разрешительных, надзорных и контрольных функций по вопросам, отнесенным к компетенции МЧС России³.

Анализ существующих технологий гармонизации нормативно-правовой базы, которые либо опосредованно, либо непосредственно могут быть распространены на область информационной безопасности, показывает наличие нескольких групп их представлений и реализации:

³ П. 7. Основные задачи МЧС России (согласно «Положению о Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий», Указ Президента Российской Федерации от 11 июля 2004 г. № 868 «Вопросы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий») «4) осуществление нормативного регулирования в целях предупреждения, прогнозирования и смягчения последствий чрезвычайных ситуаций и пожаров, а также осуществление специальных, разрешительных, надзорных и контрольных функций по вопросам, отнесенным к компетенции МЧС России»

- комплекты (сборники) терминов, определений, понятий как предметный тезаурус по нормативно правовой базе в области ИБ;
- методологический аппарат гармонизации документов в зависимости от целей и отраслевых задач;
- технологии формирования непротиворечивых документов;
- технологические платформы и локальные или сетевые сервисы информационной поддержки, формирования и применения в зависимости от целей и задач пользователей (организаций), например, программные решения ОКиДОКи, DocShell 4.0, Альфа-Док; онлайн-платформы docshell.ru, eplat4m.ru.

Вопросы межведомственной и межотраслевой гармонизации правовых норм и подходов к формированию доверенной киберсреды в сфере информационного обеспечения устойчивого функционирования РСЧС и ее функциональных и территориальных подсистем целесообразно предварительно исследовать в рамках отдельных поисковых НИР.

Объективные условия межведомственного взаимодействия при решении совместных задач по предупреждению и ликвидации последствий чрезвычайных ситуаций обуславливают потребность в высоком уровне осведомленности и компетенций должностных лиц в области ИБ и защиты информации различных структурных подразделений МЧС России как аудиторов состояния защищенности цифровых информационных инфраструктур различной принадлежности.

Требуемый уровень осведомленности аудиторов состояния защищенности цифровых информационных инфраструктур различной принадлежности может быть достигнут только за счет непрерывной образовательной среды, построенной и функционирующей на основе ведомственных организационно-технических систем класса «киберполигон».

Существующий уровень правовой защиты и защищенности аудиторов состояния защищенности цифровых информационных инфраструктур недостаточно урегулирован современными нормами права, что обуславливает необходимость проведения межведомственной и межотраслевой гармонизации правовых норм и подходов к формированию доверенной киберсреды в сфере информационного обеспечения устойчивого функционирования государственных ИС, в том числе МЧС России.

Выводы

Результаты проведенного анализа существующего состояния цифровой трансформации ведомственных образовательных организаций и подходов к разрешению проблем гармонизации в области ИБ показывают, что специалистам в области ИБ и защиты информации, а также другим заинтересованным субъектам сегодня невозможно обойтись без знания и исполнения требований соответствующей нормативной правовой базы. На то имеется несколько причин. Формальная состоит в том, что необходимость следования отдельным правилам и выполнять соответствующие требования закреплена законодательно со всеми вытекающими последствиями. Однако наиболее убедительны содержательные причины. Нормативная правовая база – это достаточно специфическая, но все же форма накопления и передачи знаний предметной области: в ее документах зафиксированы апробированные, высококачественные решения и методологии по широкому спектру значимых вопросов. Совместное бесконфликтное сосуществование субъектов с разными интересами в инфосфере в условиях нормативного правового вакуума невозможно: не даром доктринальные документы позиционируют нормативный правовой уровень обеспечения ИБ выше организационно-технического. И наконец, международное и любое другое сотрудничество и/или взаимодействие при выполнении совместных работ и проектов в области ИБ и защиты информации без единой терминологической составляющей нормативной правовой базы будет нерезультативным.

Проведенный категориальный анализ современного состояния и тенденций развития нормативной правовой базы ИБ и защиты информации позволил выявить ее следующие основные противоречия.

Во-первых, с одной стороны, область ИБ и защиты информации является очень динамичной, что требует постоянного обновления ее нормативной правовой базы; а с другой стороны, руководящие документы де-юре должны содержать сведения, полученные де-факто и накопленные годами в процессе «Лучшие практики». Налицо противоречие между устареванием и обновлением нормативной правовой базы обеспечения деятельности в сфере ИБ и защиты информации.

Во-вторых, с одной стороны, область ИБ и защиты информации является очень обширной, что предполагает значительный объем знаний для ее освоения; а с другой стороны, руководящие документы де-юре должны содержать сведения, полученные де-факто и накопленные годами в процессе «Лучшие практики». Налицо противоречие между количеством и качеством «единиц документных текстов» нормативной правовой базы обеспечения деятельности в сфере ИБ и защиты информации.

В-третьих, с одной стороны, область ИБ и защиты информации является транснациональной, что предполагает учет общемировых тенденций; а с другой стороны, вся нормотворческая деятельность должна осуществляться не в ущерб информационному суверенитету Российской Федерации. Налицо противоречие между глобальными и национальными интересами в инфосфере, которое находит свое отражение в нормативной правовой плоскости.

Все перечисленные противоречия не являются антагонистическими («либо» – «либо»), и, следовательно, смягчение их последствий может быть предметом гармонизации. Очевидно, что с учетом этих причин совершенствование нормативного правового (информационного) обеспечения деятельности в сфере ИБ и защиты информации конфиденциального характера в ведомствах является насущной проблемой, разрешение которой лежит в плоскости гармонизации нормативной правовой базы, и, в частности, разработки методологии и специальной ИТ (элементов) решения прикладных задач гармонизации.

Статья подготовлена в рамках выполнения НИР «Киберсреда» и НИР «Гармония» по государственному заданию МЧС России на 2024 г.

Список источников

1. Вопросы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий: Указ Президента Рос. Федерации от 11 июля 2004 г. № 868. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Чернышенко: 15 % ведомств сменят руководителей цифровой трансформации из-за качества работы. URL: <https://tass.ru/ekonomika/10544831> (дата обращения: 29.08.2024).

3. МЧС России вошло в тройку лидеров рейтинга цифровой трансформации среди федеральных органов исполнительной власти. URL: <https://mchs.gov.ru/deyatelnost/press-centr/novosti/5256866> (дата обращения: 29.08.2024).

4. Об утверждении Положения о системе межведомственного электронного документооборота: постановление Правительства Рос. Федерации от 22 сент. 2009 г. № 754. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия: постановление Правительства Рос. Федерации от 24 июля 2021 г. № 1264. Доступ из справ.-правовой системы «КонсультантПлюс».

6. О государственной информационной системе «Типовое облачное решение системы электронного документооборота»: постановление Правительства Рос. Федерации от 15 февр. 2022 г. № 172. Доступ из справ.-правовой системы «КонсультантПлюс».

7. О единой системе межведомственного электронного взаимодействия: постановление Правительства Рос. Федерации от 8 сент. 2010 г. № 697. Доступ из справ.-правовой системы «КонсультантПлюс».

8. Об утверждении стратегического направления в области цифровой трансформации государственного управления: распоряжение Правительства Рос. Федерации от 16 марта 2024 г. № 637-р. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Об утверждении Инструкции по делопроизводству в территориальных органах Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, учреждениях и организациях, находящихся в ведении Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий: приказ МЧС России от 14 мая 2021 г. № 315. Доступ из справ.-правовой системы «КонсультантПлюс».

10. Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18 февр. 2013 г. № 21. Доступ из справ.-правовой системы «КонсультантПлюс».

11. О персональных данных: Федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

12. Сервис «Среда». URL: <https://sreda.digital.gov.ru> (дата обращения: 29.08.2024).

13. Об утверждении стратегического направления в области цифровой трансформации науки и высшего образования: постановление Правительства Рос. Федерации от 21 дек. 2021 г. № 3759-р. Доступ из справ.-правовой системы «КонсультантПлюс».

14. Приемная комиссия. Лаборатория МИИС. URL: <https://www.mmis.ru/programs/pk> (дата обращения: 29.08.2024).

15. О функционировании суперсервиса «Поступление в вуз онлайн» в рамках приемной компании 2024/225 учебного года: постановление Правительства Рос. Федерации от 26 янв. 2023 г. № 89. Доступ из справ.-правовой системы «КонсультантПлюс».

16. Регламент подключения к API Единого портала государственных услуг. Версия 1.4. Минцифры России, 2022. 16 с.

17. Единая система идентификации и аутентификации. Руководство пользователя. Версия 2.79. URL: <https://digital.gov.ru/uploaded/presentations/rukovodstvopolzovatelyaesiamobilversiyanyijprofilv279.pdf> (дата обращения: 29.03.2024).

18. О государственной информационной системе «Современная цифровая образовательная среда»: постановление Правительства Рос. Федерации от 16 нояб. 2020 г. № 1836. Доступ из справ.-правовой системы «КонсультантПлюс».

19. Цифровая образовательная среда. URL: <https://lic-int-pos-im-marshala-zhukovarr38.gosweb.gosuslugi.ru/natsionalnyy-proekt-obrazovanie/tsifrovaya-obrazovatel'naya-sreda> (дата обращения: 29.08.2024).

20. О создании государственной информационной системы Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»: постановление Правительства Санкт-Петербурга от 23 июня 2011 г. № 802. Доступ из справ.-правовой системы «КонсультантПлюс».

21. Электронные услуги в области образования. URL: https://iac.spb.ru/proekty-i-sistemy/detail.php/?ELEMENT_ID=81 (дата обращения: 29.08.2024).

22. О внесении изменений в Федеральный закон «Об образовании в Российской Федерации»: Федер. закон от 8 авг. 2024 г. № 315-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

23. 1С: Электронное обучение. Корпоративный университет. URL: <https://solutions.1c.ru/catalog/elearning-universitycorp/features> (дата обращения: 29.08.2024).

24. Новости информационной безопасности за июль 2024 года. URL: <https://rcngroup.ru/blog/novosti-informacionnoj-bezopasnosti-za-ijul-2024-goda> (дата обращения: 29.08.2024).

25. Об утверждении положения о государственной единой облачной платформе: постановление Правительства Рос. Федерации от 10 июля 2024 г. № 929. Доступ из справ.-правовой системы «КонсультантПлюс».

26. О внесении изменения в Критерии оценки материалов и (или) информации, необходимых для принятия Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»: приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 февр. 2023 г. № 25. Доступ из справ.-правовой системы «КонсультантПлюс».

27. О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ Федеральной службы по техническому и экспортному контролю от 11 февр. 2013 г. № 17. URL: <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=149172#> (дата обращения: 29.08.2024).

28. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ Федеральной службы по техническому и экспортному контролю от 25 дек. 2017 г. № 239. URL: <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=149172#> (дата обращения: 29.08.2024).

29. Право цифровой безопасности: Форум М., 2024. URL: https://mgimo.ru/upload/2024/04/2024-04_digital-law-forum.pdf (дата обращения: 29.08.2024).

30. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1 (253). С. 85–102.

31. Хабриева Т.Я. Циклические нормативные массивы в праве // Журнал российского права. 2019. № 12. С. 5–18.

32. Полякова Т.А., Минбалеев А.В., Наумов В.Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 81–91. DOI: 10.31857/S1026945224010087.

33. Установление сходства текстовых документов / А.А. Хорошилов [и др.] // Моделирование и анализ данных. 2023. Т. 13. № 4. С. 45–58. DOI: 10.17759/mda.2023130403.

34. Oghbaie M., Zanjireh M.M. Pairwise document similarity measure based on present term set // Journal of Big Data. 2018. Vol. 5. № 52. P. 23. DOI: 10.1186/s40537-018-0163-2.

References

1. Voprosy Ministerstva Rossijskoj Federacii po delam grazhdanskoj oborony, chrezvychajnym situacijam i likvidacii posledstvij stihijnyh bedstvij: Ukaz Prezidenta Ros. Federacii ot 11 iyulya 2004 g. № 868. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

2. Chernyshenko: 15 % vedomstv smenyat rukovoditelej cifrovoj transformacii iz-za kachestva raboty. URL: <https://tass.ru/ekonomika/10544831> (data obrashcheniya: 29.08.2024).

3. MCHS Rossii voshlo v trojku liderov rejtinga cifrovoj transformacii sredi federal'nyh organov ispolnitel'noj vlasti. URL: <https://mchs.gov.ru/deyatelnost/press-centr/novosti/5256866> (data obrashcheniya: 29.08.2024).

4. Ob utverzhdenii Polozheniya o sisteme mezhvedomstvennogo elektronnoho dokumentooborota: postanovlenie Pravitel'stva Ros. Federacii ot 22 sent. 2009 g. № 754. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
5. Ob utverzhdenii Pravil obmena dokumentami v elektronnom vide pri organizacii informacionnogo vzaimodejstviya: postanovlenie Pravitel'stva Ros. Federacii ot 24 iyulya 2021 g. № 1264. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
6. O gosudarstvennoj informacionnoj sisteme «Tipovoe oblachnoe reshenie sistemy elektronnoho dokumentooborota»: postanovlenie Pravitel'stva Ros. Federacii ot 15 fevr. 2022 g. № 172. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
7. O edinoj sisteme mezhvedomstvennogo elektronnoho vzaimodejstviya: postanovlenie Pravitel'stva Ros. Federacii ot 8 sent. 2010 g. № 697. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
8. Ob utverzhdenii strategicheskogo napravleniya v oblasti cifrovoj transformacii gosudarstvennogo upravleniya: rasporyazhenie Pravitel'stva Ros. Federacii ot 16 marta 2024 g. № 637-r. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
9. Ob utverzhdenii Instrukcii po deloproizvodstvu v territorial'nyh organah Ministerstva Rossijskoj Federacii po delam grazhdanskoj oborony, chrezvychajnym situacijam i likvidacii posledstvij stihijnyh bedstvij, uchrezhdeniyah i organizacijah, nahodyashchihsya v vedenii Ministerstva Rossijskoj Federacii po delam grazhdanskoj oborony, chrezvychajnym situacijam i likvidacii posledstvij stihijnyh bedstvij: prikaz MCHS Rossii ot 14 maya 2021 g. № 315. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
10. Ob utverzhdenii Sostava i soderzhaniya organizacionnyh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh: prikaz FSTEK Rossii ot 18 fevr. 2013 g. № 21. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
11. O personal'nyh dannyh: Feder. zakon Ros. Federacii ot 27 iyulya 2006 g. № 152-FZ. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
12. Servis «Sreda». URL: <https://sreda.digital.gov.ru> (data obrashcheniya: 29.08.2024).
13. Ob utverzhdenii strategicheskogo napravleniya v oblasti cifrovoj transformacii nauki i vysshego obrazovaniya: postanovlenie Pravitel'stva Ros. Federacii ot 21 dek. 2021 g. № 3759-r. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
14. Priemnaya komissiya. Laboratoriya MIIS. URL: <https://www.mmis.ru/programs/pk> (data obrashcheniya: 29.08.2024).
15. O funkcionirovanii superservisa «Postuplenie v vuz onlajn» v ramkah priemnoj kompanii 2024/225 uchebnogo goda: postanovlenie Pravitel'stva Ros. Federacii ot 26 yanv. 2023 g. № 89. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
16. Reglament podklyucheniya k API Edinogo portala gosudarstvennyh uslug. Versiya 1.4. Mincifry Rossii, 2022. 16 s.
17. Edinaya sistema identifikacii i autentifikacii. Rukovodstvo pol'zovatelya. Versiya 2.79. URL: <https://digital.gov.ru/uploaded/presentations/rukovodstvopolzovatelyaesiamobilversiyanyovijprofilv279.pdf> (data obrashcheniya: 29.03.2024).
18. O gosudarstvennoj informacionnoj sisteme «Sovremennaya cifrovaya obrazovatel'naya sreda»: postanovlenie Pravitel'stva Ros. Federacii ot 16 noyab. 2020 g. № 1836. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
19. Cifrovaya obrazovatel'naya sreda. URL: <https://lic-int-pos-im-marshala-zhukova-r38.gosweb.gosuslugi.ru/natsionalnyy-proekt-obrazovanie/tsifrovaya-obrazovatel'naya-sreda> (data obrashcheniya: 29.08.2024).
20. O sozdanii gosudarstvennoj informacionnoj sistemy Sankt-Peterburga «Kompleksnaya avtomatizirovannaya informacionnaya sistema katalogizacii resursov obrazovaniya Sankt-Peterburga»: postanovlenie Pravitel'stva Sankt-Peterburga ot 23 iyunya 2011 g. № 802. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

21. Elektronnye uslugi v oblasti obrazovaniya. URL: https://iac.spb.ru/proekty-i-sistemy/detail.php/?ELEMENT_ID=81 (data obrashcheniya: 29.08.2024).
22. O vnesenii izmenenij v Federal'nyj zakon «Ob obrazovanii v Rossijskoj Federacii: Feder. zakon ot 8 avg. 2024 g. № 315-FZ. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
23. IS: Elektronnoe obuchenie. Korporativnyj universitet. URL: <https://solutions.1c.ru/catalog/elearning-universitycorp/features> (data obrashcheniya: 29.08.2024).
24. Novosti informacionnoj bezopasnosti za iyul' 2024 goda. URL: <https://rcngroup.ru/blog/novosti-informacionnoj-bezopasnosti-za-ijul-2024-goda> (data obrashcheniya: 29.08.2024).
25. Ob utverzhdenii polozheniya o gosudarstvennoj edinoj oblachnoj platforme: postanovlenie Pravitel'stva Ros. Federacii ot 10 iyulya 2024 g. № 929. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
26. O vnesenii izmeneniya v Kriterii ocenki materialov i (ili) informacii, neobhodimyh dlya prinyatiya Federal'noj sluzhboj po nadzoru v sfere svyazi, informacionnyh tekhnologij i massovyh kommunikacij reshenij, yavlyayushchihysya osnovaniyami dlya vklyucheniya domennyh imen i (ili) ukazatelej stranic sajtov v informacionno-telekommunikacionnoj seti «Internet», a takzhe setevyh adresov, pozvolyayushchih identifiциrovat' sajty v informacionno-telekommunikacionnoj seti «Internet», v edinuyu avtomatizirovannuyu informacionnuyu sistemu «Edinyj reestr domennyh imen, ukazatelej stranic sajtov v informacionno-telekommunikacionnoj seti «Internet» i setevyh adresov, pozvolyayushchih identifiциrovat' sajty v informacionno-telekommunikacionnoj seti «Internet», soderzhashchie informaciyu, rasprostranenie kotoroj v Rossijskoj Federacii zapreshcheno»: prikaz Federal'noj sluzhby po nadzoru v sfere svyazi, informacionnyh tekhnologij i massovyh kommunikacij ot 27 fevr. 2023 g. № 25. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».
27. O vnesenii izmenenij v Trebovaniya o zashchite informacii, ne sostavlyayushchej gosudarstvennuyu tajnu, soderzhashchejsya v gosudarstvennyh informacionnyh sistemah: prikaz Federal'noj sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 11 fevr. 2013 g. № 17. URL: <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=149172#> (data obrashcheniya: 29.08.2024).
28. Trebovaniya po obespecheniyu bezopasnosti znachimyh ob"ektov kriticheskoy informacionnoj infrastruktury Rossijskoj Federacii: prikaz Federal'noj sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 25 dek. 2017 g. № 239. URL: <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=149172#> (data obrashcheniya: 29.08.2024).
29. Pravo cifrovoj bezopasnosti: Forum M., 2024. URL: https://mgimo.ru/upload/2024/04/2024-04_digital-law-forum.pdf (data obrashcheniya: 29.08.2024).
30. Habrieva T.Ya., Chernogor N.N. Pravo v usloviyah cifrovoj real'nosti // Zhurnal rossijskogo prava. 2018. № 1 (253). S. 85–102.
31. Habrieva T.Ya. Ciklicheskie normativnye massivy v prave // Zhurnal rossijskogo prava. 2019. № 12. S. 5–18.
32. Polyakova T.A., Minbaleev A.V., Naumov V.B. K voprosu o kodifikacii informacionnogo zakonodatel'stva v usloviyah cifrovoj transformacii // Gosudarstvo i pravo. 2024. № 1. S. 81–91. DOI: 10.31857/S1026945224010087.
33. Ustanovlenie skhodstva tekstovyh dokumentov / A.A. Horoshilov [i dr.] // Modelirovanie i analiz dannyh. 2023. T. 13. № 4. С. 45–58. DOI: 10.17759/mda.2023130403.
34. Oghbaie M., Zanjireh M.M. Pairwise document similarity measure based on present term set // Journal of Big Data. 2018. Vol. 5. № 52. P. 23. DOI: 10.1186/s40537-018-0163-2.

Информация о статье:

Поступила в редакцию: 18.09.2024

Принята к публикации: 20.10.2024

The information about article:

Article was received by the editorial office: 18.09.2024

Accepted for publication: 20.10.2024

Информация об авторах:

Уткин Николай Иванович, профессор кафедры теории и истории государства и права Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор юридических наук, профессор, заслуженный юрист Российской Федерации, e-mail: utkinnick@mail.ru, SPIN-код: 7013-8436

Шеншин Виктор Михайлович, доцент кафедры теории и истории государства и права Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат юридических наук, доцент, e-mail: vitya-shen@mail.ru, SPIN-код: 8769-9940

Шестаков Александр Викторович, ведущий научный сотрудник центра организации научно-исследовательской и редакционной деятельности Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), старший научный сотрудник, доктор технических наук, e-mail: alexandr.shestakov01@yandex.ru, SPIN-код: 5831-5451

Information about the authors:

Utkin Nikolay I., professor of the department of theory and history of state and law of the Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of law, professor, honored lawyer of the Russian Federation, e-mail: utkinnick@mail.ru, SPIN: 7013-8436

Shenshin Viktor M., associate professor of the department of theory and history of state and law of the Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of law, associate professor, e-mail: vitya-shen@mail.ru, SPIN: 8769-9940

Shestakov Alexander V., leading researcher at the center for the organization of research and editorial activities of the Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), senior researcher, doctor of technical sciences, e-mail: alexandr.shestakov01@yandex.ru, SPIN: 5831-5451