

СЕРТИФИКАЦИЯ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ: НОРМАТИВНО-ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ

Федосеев С.В.¹

Ключевые слова: центр обработки данных (ЦОД), сертификация, технико-правовые стандарты, технические регламенты, сертификат соответствия, статус, объект регулирования, характер применения технического регламента и национального стандарта, резервирование систем, инженерная инфраструктура, операционная модель эксплуатации, международные системы сертификации ЦОД.

Аннотация

Цель работы: обоснование научно-методического подхода к решению задач применения отечественной модели сертификации ЦОД и национальных технико-правовых стандартов, определяющих требования к ЦОД.

Методы: концептуально-логическое моделирование правовых отношений и информационных связей, определяемых отечественной системой классификации и сертификации ЦОД, выполнением требований национальных технико-правовых стандартов; системный анализ взаимосвязи предметной области правовой сферы, объектов сферы информационных сетевых технологий, сферы разработки и эксплуатации центров обработки данных, математических алгоритмов и основных объектов и методов теории принятия решений и теории множеств.

Результаты: выполнен анализ возможностей применения технических регламентов и национальных технико-правовых стандартов и определены различия между ними по признакам: статус, объект применения, характер применения, аспекты регулирования; проведен анализ международных систем сертификации центров обработки данных; рассмотрены требования технико-правовых стандартов в отношении инженерной инфраструктуры, стадий создания, операционной модели эксплуатации, классификации ЦОД; выявлены перспективы использования системы добровольной сертификации «РосЦОД», обоснована процедура сравнения ЦОД.

DOI: 10.21681/1994-1404-2023-2-14-25

Введение

Вопросам совершенствования отечественной системы сертификации центров обработки информации (ЦОД) придается в последнее время большое значение. Это связано прежде всего с тем, что все возрастающие объемы информации разного уровня закрытости начинают размещаться и обрабатываться с использованием ЦОД. Так, электронная цифровая подпись (ЭЦП) превращается в «облачную» ЭЦП с переносом всех вычислительных операций на внешний сервис, а государственные структуры становятся пользователями коммерческих ЦОД. Очевидно, что в таком цифровом пространстве на первый план выходят проблемы обеспечения защиты информации [7—10], разработки новых инфраструктурных технических решений [3] и правового регулирования информационных отношений [2, 11].

Если в течение предыдущих 10—15 лет в Российской Федерации классификация и сертификация ЦОД

осуществлялась только с использованием международных и иностранных стандартов (национальных технических стандартов по ЦОД просто не существовало), то за последние два года разработаны и введены в действие четыре национальных российских стандарта, напрямую определяющие требования к ЦОД.

Применение технических регламентов и национальных стандартов для сертификации ЦОД

В настоящее время вопросы проектирования, строительства, оснащения и функционирования ЦОД определяют следующие нормативные правовые акты.

– Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». В мае 2022 г. приняты поправки к этому закону, которые законодательно определяют ЦОД и операторов ЦОД, закрепляют в качестве основной деятельности оператора ЦОД оказание услуги размещения оборудования, обеспечивающего обработку/хранение данных. Это позволяет

¹ Федосеев Сергей Витальевич, кандидат технических наук, доцент, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.
E-mail: fedsergvt@mail.ru

использовать инфраструктуру коммерческих поставщиков услуг ЦОД для оказания сервисов государственным ведомствам и организациям.

- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», одним из основных требований которого является размещение систем обработки и хранения персональной информации граждан Российской Федерации только на территории РФ и соответствие этих систем требованиям законодательства в области безопасности информации [10].
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», согласно которому служебная информация в правоохранительных, финансовых, государственных и других структурах может обрабатываться только с использованием программного обеспечения, сертифицированного Федеральной службой по техническому и экспортному контролю (ФСТЭК).

Требования к ЦОД по вопросам обеспечения защиты информации и персональных данных содержатся также в следующих документах:

- Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Наибольшее значение при проведении сертификации современных ЦОД имеют два типа документов: технические регламенты и национальные технико-правовые стандарты.

Технический (технико-правовой) **регламент** определяется как документ, который «устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, налад-

ки, эксплуатации, хранения, перевозки, реализации и утилизации)»².

Такой документ может быть: международным договором РФ, подлежащим ратификации или ратифицированным; указом Президента РФ; постановлением Правительства РФ; нормативным правовым актом федерального органа исполнительной власти по техническому регулированию (Федеральное агентство по техническому регулированию и метрологии — Росстандарт).

В качестве органа по сертификации может выступать «юридическое лицо или индивидуальный предприниматель, аккредитованные в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации для выполнения работ по сертификации»³.

Сертификат, выдаваемый органом сертификации, подтверждает соответствие объекта требованиям технико-правовых регламентов, документов по стандартизации, условиям договоров.

Национальный стандарт — «документ по стандартизации, который разработан участником или участниками работ по стандартизации, в отношении которого проведена экспертиза в техническом комитете по стандартизации или проектом технического комитета по стандартизации и в котором для всеобщего применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы в отношении объекта стандартизации»⁴.

Вопросами, связанными с разработкой национальных стандартов для ЦОД, занимается технический комитет ТК 120 при Росстандарте. Национальный стандарт проходит официальную регистрацию в Федеральном агентстве по техническому регулированию и метрологии.

Стандартизация в РФ основывается на *принципе добровольности*, при этом законодательно определены исключения. Согласно этим исключениям, обязательность применения документов по стандартизации возникает в следующих случаях:

1. В отношении объектов стандартизации, определенных ст. 6 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации», которая определяет в качестве таких объектов:
 - оборонную продукцию по государственному оборонному заказу;
 - продукцию, используемую в целях защиты сведений, составляющих государственную тайну;
 - продукцию, сведения о которой составляют государственную тайну;
 - продукцию, связанную с обеспечением безопасности в области использования атомной энергии.

² Ст. 2 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

³ Там же.

⁴ Ст. 2 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации».

Технический регламент и национальный стандарт

Признаки \ Документ	Технический регламент	Национальный стандарт
Статус	Федеральный закон, или указ Президента РФ, или постановление Правительства РФ, или нормативный правовой акт	Документ в области стандартизации
Объект регулирования	Продукция. Процессы жизненного цикла, связанные с требованиями к продукции	Продукция. Работы (услуги). Процессы жизненного цикла продукции на после-производственных стадиях
Характер применения	Обязательный	Добровольный (в общем случае)
Общая характеристика требований. Аспекты регулирования	Требования к характеристикам безопасности продукции. Требования к оценке соответствия (подтверждение соответствия, государственный контроль и надзор)	Требования ко всем техническим (потребительским) качествам и характеристикам продукции. Обеспечение безопасности продукции в развитие общих требований технического регламента

Порядок стандартизации в отношении продукции устанавливается Правительством РФ.

2. В отношении изготовителя и (или) исполнителя в случае публичного заявления о соответствии продукции национальному стандарту, в том числе в случае применения обозначения национального стандарта в маркировке, в эксплуатационной или иной документации, и (или) маркировки продукции знаком национальной системы стандартизации⁵.

Очевидным является то, что технико-правовой регламент обладает более весомым юридическим статусом по сравнению с национальным стандартом (табл. 1).

Вместе с тем в некоторых случаях применение на добровольной основе стандартов и (или) сводов правил является достаточным условием соблюдения требований соответствующих технических регламентов.

Выполнение этого условия обеспечивается следующими позициями⁶:

1. Своевременное утверждение и опубликование перечня документов по стандартизации, в результате применения которых на добровольной основе обеспечивается соблюдение требований принятого технического регламента. В перечень могут включаться стандарты: национальные РФ, международные, региональные, иностранных государств, а также своды правил иностранных государств при условии их регистрации в Федеральном информационном фонде технических регламентов и стандартов.

2. Применение на добровольной основе стандартов и (или) сводов правил, включенных в указанный перечень. При этом оценка соответствия объектов сертификации требованиям технических регламентов осуществляется на основании подтверждения соответствия

таких стандартов и (или) сводов правил техническим регламентам согласно указанному выше перечню.

3. Применение на добровольной основе документов, не входящих в указанный перечень. В этом случае допускается использование предварительных национальных стандартов РФ, стандартов организаций и (или) иных документов, которые должны подтверждать соответствие объекта сертификации требованиям соответствующих технических регламентов. Такую доказательную базу формирует заявитель. В нее могут быть включены результаты испытаний, исследований, техническая документация.

Анализ международных систем сертификации центров обработки данных

До настоящего времени наиболее авторитетной в РФ системой классификации и сертификации ЦОД была система, созданная американской частной компанией *Uptime Institute* и состоящая из следующих разделов: сертификация специалистов, сертификация проектной документации, сертификация построенных объектов, сертификация эксплуатационных процессов уже действующих ЦОД.

Компания *Uptime Institute* проводит проверку и классификацию ЦОД на основе разработанных ею показателей и выдает сертификат соответствия по одному из четырех уровней *Tier*⁷.

Tier 1 предполагает наличие у инженерной инфраструктуры ЦОД (ИИ ЦОД) только базовой функциональности, которая обеспечивается наличием систем бесперебойного электропитания и охлаждения при отсутствии системы резервирования. Отказы и сбои систем и оборудования приводят к остановкам в работе всего ЦОД. Проведение профилактических и ремонтных работ также

⁵ Ст. 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации».

⁶ Ст. 16.1 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

⁷ От англ. tier — ярус.

Сравнение требований стандартов сертификации ЦОД в отношении систем электроснабжения

Уровень	Стандарт EN 50600	Стандарт TIA-942	Стандарты Uptime Institute
1	Одноканальная система без резервирования компонентов	N (нерезервированные модули)	N (нерезервированные модули)
2	Одноканальная система с резервированием компонентов	N+1	N+1
3	Многоканальная система (резервирование систем)	N+1	N+1
4	Многоканальная система (резервирование систем)	2N	2(N+1)

Обозначения: *N* — необходимое количество элементов в системе; *N+1* — предусмотрен один резервный элемент, который подключается при отказе или сбое; *2N* — используется две параллельные системы, делящие нагрузку из расчета 50/50 (в случае выхода из строя одной из систем, вторая полностью берет на себя нагрузку); *2N+1* — две параллельные системы и один резервный элемент; *2(N+1)* — две параллельные системы, в каждой из которых есть резервный элемент.

приводит к остановке ЦОД. Коэффициент готовности по критичным системам должен быть не ниже 0,99671.

Tier 2 подразумевает начальный уровень резервирования, который достигается введением дополнительных каналов электропитания и охлаждения. Коэффициент готовности — не ниже 0,99749.

Tier 3 подтверждает более высокую степень резервирования: используется несколько каналов электропитания и охлаждения. Профилактические и ремонтные работы не приводят к прерыванию работы ЦОД. Коэффициент готовности — не ниже 0,99982.

Tier 4 предполагает полное резервирование всех систем, что делает возможным производить любые работы в ЦОД без остановки его работы.

Коэффициент готовности — не ниже 99,995.

Стандарт TIA-942 Ассоциации телекоммуникационной отрасли — *Telecommunication Industry Association* Института американских национальных стандартов также достаточно широко применяется в РФ.

Требования, изложенные в стандарте *TIA*, относятся к области строительства, системам резервирования, безопасности, электроснабжения, охлаждения, применению *структурированных кабельных сетей* (СКС), обеспечению ремонтнопригодности и ввода в эксплуатацию.

Стандарты EN 50600 разработаны организацией *CENELEC* — *European Committee for Electrotechnical Standardization* и содержат модели эксплуатации, требования по экологическому контролю, к системам информационной безопасности, охлаждения, электроснабжения, СКС.

Каждый из рассмотренных стандартов использует собственную модель сертификации. Но если стандарты *EN 50600* и *TIA-942* предполагают привлечение для аттестации ЦОД сторонних организаций, получивших у них аккредитацию, то компания *Uptime Institute* проводит такую аттестацию исключительно сама.

Сравнение требований стандартов *Uptime Institute*, *TIA-942* и *EN 50600* по обеспечению надежности систем электроснабжения⁸ приведено в табл. 2.

BICSI 009 2019 — еще один достаточно известный стандарт в рассматриваемой области, разработанный Международной консультативной службой строительной отрасли — *Building Industry Consulting Service International*.

Этот стандарт по большому количеству позиций совпадает с *TIA-942*, но отличается от других стандартов тщательной проработкой технических требований к инженерной инфраструктуре ЦОД.

Отечественные технико-правовые стандарты сертификации центров обработки данных

В течение долгого времени в России отсутствовали отечественные технические стандарты, определяющие систему сертификации ЦОД, и использовались для этого, как правило, стандарты *Uptime Institute* — **Tier и Management&Operations**.

Однако взаимодействие с международными организациями, выполняющими сертификацию ЦОД, в современных условиях становится практически невозможным. По этой причине возникает необходимость разработки и применения отечественных технических стандартов, создания отдельной системы сертификации.

Следует принимать во внимание, что лучшие мировые практики в области проектирования и эксплуатации ЦОД уже представлены в открытых международных и иностранных стандартах: *ISO/IEC TS 22237*; *EN 50600*; *TIA-942*. В связи с этим национальный стандарт может быть разработан просто на основе адаптации перечисленных документов под реальные отечественные условия.

⁸ Сертификатам *Uptime* найдут бюджетную замену. URL: https://www.cnews.ru/reviews/rynok_inzhenernoj_itinfrastruktury/articles/sertifikatam_uptime_najdut_byudzhetnuyu

В Российской Федерации выбран другой путь — разработка собственных национальных технических стандартов сертификации ЦОД, что объясняется следующими причинами:

- перманентное изменение нормативной правовой базы, связанное с возрастанием требований регуляторов, прежде всего Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю, Банка России, Министерства связи и массовых коммуникаций;
- открытые отечественные стандарты позволяют понизить стоимость услуги по сертификации ЦОД, сделать ее более доступной для небольших дата-центров;
- расширяющее использование государственными структурами средств обработки информации ЦОД делает нежелательным применение иностранных стандартов.

Отличительной характеристикой отечественной системы технических стандартов по сертификации ЦОД должен стать менее глубокий аудит по сравнению, например, со стандартами *Uptime Institute*.

Первые национальные технические стандарты сертификации ЦОД были введены в действие только в 2020 г. Проекты этих стандартов подготавливает некоммерческая организация «Ассоциация участников

отрасли центров обработки данных», которая функционирует в составе Технического комитета «Центры обработки данных» (ТК 120) Федерального агентства по техническому регулированию и метрологии.

Техническим комитетом разработана комплексная программа стандартизации отрасли ЦОД, включающая стандартизацию всех объектов этой отрасли: процессов, продукции, услуг. В соответствии с этой программой к настоящему времени разработаны и введены в действие следующие технические стандарты.

ГОСТ Р 58811-2020 «Центры обработки данных. Инженерная инфраструктура. Стадии создания»

Этот стандарт определяет стадии и этапы жизненного цикла создания инженерной инфраструктуры ЦОД (ИИ ЦОД) (табл. 3).

Как следует из табл. 3, каждая стадия разбивается на несколько этапов и для каждого из них определены цели и содержание работ. Например, цель этапа 8.1 «Проведение предварительных испытаний» заключается в определении соответствия реализованных технических решений для частей и систем ИИ ЦОД требованиям технического задания на создание ИИ ЦОД и частных технических заданий на создание частей и систем ИИ ЦОД.

Таблица 3

Стадии и этапы создания инженерной инфраструктуры центра обработки данных

Стадия	Этап работ
1. Предпроектное обследование	1.1. Формирование требований. 1.2. Обследование площадки. 1.3. Оформление отчета об обследовании
2. Задание на разработку технической концепции	2.1. Разработка и утверждение задания на разработку технической концепции
3. Техническая концепция	3.1. Разработка предварительных технических решений. 3.2. Разработка документации для предварительных технических решений
4. Техническое задание	4.1. Разработка и утверждение технического задания
5. Проектная документация	5.1. Разработка проектных решений. 5.2. Разработка проектной документации. 5.3. Разработка заданий на проектирование в смежных частях проекта
6. Рабочая документация	6.1. Разработка рабочей документации
7. Реализация решений	7.1. Поставка оборудования и материалов. 7.2. Монтажные работы. 7.3. Пусконаладочные работы. 7.4. Подготовка объекта к вводу ИИ ЦОД в действие
8. Испытания	8.1. Проведение предварительных испытаний. 8.2. Проведение опытной эксплуатации. 8.3. Проведение комплексных приемочных испытаний
9. Эксплуатация	9.1. Гарантийное обслуживание. 9.2. Послегарантийное обслуживание. 9.3. Сервисное обслуживание

Содержание работ на этом этапе определяется следующим образом:

- испытания частей и систем ИИ ЦОД на работоспособность и соответствие техническому заданию на создание ИИ ЦОД и частным техническим заданиям на создание частей и систем ИИ ЦОД в соответствии с программой и методикой предварительных испытаний;
- устранение замечаний и неисправностей;
- внесение изменений в документацию на ИИ ЦОД, ее части и системы, в том числе эксплуатационную, в соответствии с протоколами испытаний;
- оформление акта о приемке ИИ ЦОД в опытную эксплуатацию.

Рассматриваемый ГОСТ содержит два приложения.

Приложение А содержит рекомендуемые результаты работ по созданию ИИ ЦОД, определяемые как документы, относящиеся к каждому из этапов. Для этапа 8.1 это протоколы проведения предварительных испытаний ИИ ЦОД, ее частей и систем; протоколы устранения замечаний и неисправностей; измененная документация на ИИ ЦОД, ее части и системы; акт о приемке ИИ ЦОД в опытную эксплуатацию.

Приложение В определяет участников, задействованных на конкретных этапах создания ИИ ЦОД. На этапе 8.1 участвуют в работе: заказчик, куратор проекта, генпроектировщик, субпроектировщики, генподрядчик, субподрядчики.

ГОСТ Р 58812-2020 «Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация»

Этот стандарт определяет требования к организации, осуществляющей эксплуатацию инженерных систем ЦОД, с целью обеспечения надлежащего качества их функционирования и предоставления потребителям услуг ИИ ЦОД приемлемого качества. Он способствует формированию и принятию единого *процессного подхода* к организации эксплуатации ИИ ЦОД.

Операционная модель эксплуатации (ОМЭ) определяется в рассматриваемом стандарте как совокупность следующих компонентов: процессов (всего 43 процесса), ресурсов, организационной модели (*рис. 1*).

Для каждого компонента ОМЭ приведены требования и классификация составных частей этих компонентов.

Наиболее важным компонентом ОМЭ являются процессы, которые определяются как регулярно повторяющиеся последовательности взаимосвязанных мероприятий (операций, процедур, действий) по обслуживанию ЦОД.

Каждый из процессов описывается в рассматриваемом техническом стандарте по однотипной схеме:

- наименование процесса (пояснения и общая информация);
- цель процесса, описание требований и рекомендаций;

- эффект от реализации (формулировка ожидаемого эффекта).

Для представленных на *рис. 1* трех категорий процессов приводятся составляющие их группы процессов. Так, для категории «Процессы управления и взаимодействия» выделяются группы: процессы управления обслуживанием, процессы взаимодействия, процессы контроля качества.

В свою очередь, процессы управления обслуживанием подразделяются на диспетчерское управление, управление текущей операционной деятельностью, управление техническим обслуживанием, управление ремонтами, управление жизненным циклом активов.

Последний из перечисленных, процесс «Управление жизненным циклом активов», описан следующим образом.

Цель — повышение эффективности использования оборудования инженерной инфраструктуры ЦОД как производственных активов.

Должны быть сформированы и функционировать следующие *процедуры* процесса управления активами: планирование жизненного цикла активов, отслеживание состояний активов (в рамках жизненного цикла), инициирование изменений состояний активов, предоставление информации.

Должны быть определены *перечень* отслеживаемых активов, их жизненный цикл (который может быть разным для разных активов).

Необходимо осуществлять отслеживание состояния актива с точки зрения жизненного цикла.

Следует выполнять планирование жизненного цикла актива. Действия по изменению состояния активов инициируют в соответствии с планом их жизненного цикла.

Необходимо формировать *требования* к финансированию замены активов (включая собственно закупку нового оборудования и его последующий монтаж, пуск и наладку, а также демонтаж и утилизацию заменяемого оборудования).

Процесс должен предоставлять *значимую информацию* по активам для других процессов, в том числе для управления финансами, ремонтами и др.

Эффект от реализации:

- оптимизация затрат на эксплуатацию;
- рациональное использование технического ресурса оборудования;
- повышение эффективности систем объекта как производственных фондов.

Типовой перечень объектов эксплуатации инженерной инфраструктуры центра обработки данных содержится в справочном приложении стандарта.

ГОСТ Р 70139-2022 «Центры обработки данных. Инженерная инфраструктура. Классификация»

Этот стандарт определяет обширный перечень показателей (всего более 200 показателей), характеризующих



Рис. 1. Элементы операционной модели эксплуатации

Таблица 4

Группы показателей безопасности ЦОД

Наименование группы показателей	Описание
Обеспечение стойкости к внешним воздействиям и явлениям	Показатели устойчивости к внешним воздействиям
Обеспечение защиты имущества от нежелательных или несанкционированных физических воздействий	Показатели, связанные с уровнем физической защиты имущества
Обеспечение защиты инженерных систем и ИТ-инфраструктуры от нежелательных или несанкционированных логических воздействий	Показатели, связанные с уровнем информационной защиты
Обеспечение защиты (безопасности) персонала, посетителей и окружающей среды от нежелательных воздействий	Показатели, связанные с уровнем защиты персонала

ющих инженерную инфраструктуру ЦОД, на основе которых становится возможным введение классов ЦОД.

Применение ГОСТ Р 70139-2022 позволяет: формировать требования к ИИ ЦОД и ее отдельным элементам; использовать представленный структурированный перечень показателей ЦОД, их возможных вариантов и интервалов значений для проведения анализа, сравнения, выбора и сертификации ЦОД.

Классификация ЦОД осуществляется в соответствии с попаданием фактических значений показателей ЦОД в установленные допустимые интервалы.

Стандарт определяет основные типы показателей, характеризующих предоставляемые ЦОД услуги: а) показатели назначения; б) показатели надежности; в) показатели безопасности; г) дополнительные показатели.

Каждому типу показателей ставится в соответствие несколько групп показателей. Например, к типу «показатели безопасности» отнесены группы показателей, представленные в табл. 4.

Группу показателей «Обеспечение защиты инженерных систем и ИТ-инфраструктуры от нежелательных или несанкционированных логических воздействий» составляют показатели обеспечения:

- контроля за несанкционированными подключениями к ИТ-инфраструктуре;
- контроля за перемещением носителей информации и их уничтожением;
- защиты инженерной инфраструктуры от компьютерных атак;
- защиты ИТ-инфраструктуры от компьютерных атак.

Диапазон изменения каждого показателя разбит на пять интервалов, для каждого интервала определены требования по значению показателя и соответствующее обозначение класса: от **A** (самые строгие требования) до **E** (самые простые).

Согласно ГОСТ Р 70139-2022, классификация ЦОД выполняется раздельно для двух категорий пользователей:

- 1) органы государственной власти и органы местного самоуправления Российской Федерации;
- 2) хозяйствующие субъекты Российской Федерации других организационно-правовых форм (юридические лица, организации, физические лица).

В первом случае ЦОД, предоставляющие услуги государственным информационным системам (ГИС) [13], подразделяются на следующие классы:

- ГИС-1 (ГИС Специальный);
- ГИС-2 (ГИС Высокий);
- ГИС-3 (ГИС Средний);
- ГИС-4 (ГИС Низкий);
- ГИС-5 (ГИС Минимальный).

Во втором случае используются *многоцелевые центры* (МЦ), которые в отношении инженерной инфраструктуры разделяются на классы:

- МЦ-1 (МЦ Специальный);
- МЦ-2 (МЦ Высокий);
- МЦ-3 (МЦ Средний);
- МЦ-4 (МЦ Низкий);
- МЦ-5 (МЦ Минимальный).

Для каждого из перечисленных классов определен набор соответствующих этому классу характеристик.

Так, например, для ЦОД класса ГИС-1 расчетный коэффициент готовности по критичным системам должен быть не ниже 0,99995, а для ЦОД класса ГИС-5 — не ниже 0,95.

ГОСТ Р 70627-2023 «Центры обработки данных. Инженерная инфраструктура. Документация. Техническая концепция. Требования к составу и содержанию»

Разработка технической концепции является важнейшим этапом создания современных ЦОД. Техническая концепция инженерной инфраструктуры центра обработки данных (ТК ИИ ЦОД) по ГОСТ Р 70627-2023 определяется как документ или комплект документов, в котором содержатся предварительные технические решения и расчет совокупной стоимости владения инженерной инфраструктуры центра обработки данных, приводится обоснование выбора решения для инженерной инфраструктуры центра обработки данных и высокоуровневый план реализации.

В комплект документации ТК ИИ ЦОД входят: пояснительная записка к технической концепции, дополнительные материалы. Основным содержанием стандарта являются *требования* к этим документам.

Пояснительная записка технической концепции должна содержать следующие разделы: Общие сведения,

Основные показатели проектируемого ЦОД, Методика выполнения работ, Описание вариантов технических решений для отдельных систем, Описание вариантов технического решения для реализации комплекса систем, Расчет совокупной стоимости владения ЦОД, Обоснование выбора технического решения для реализации, План реализации выбранного технического решения.

Каждый из приведенных разделов включает в себя несколько подразделов, в которых указываются *требования* по конкретному вопросу. Например, в разделе «Описание вариантов технических решений для отдельных систем» должны быть предусмотрены следующие сведения (подразделы):

- архитектурно-планировочные решения и планировочные решения территории;
- предварительные технические решения для основных систем ИИ ЦОД;
- предварительные технические решения для вспомогательных систем ИИ ЦОД;
- технические показатели для рассматриваемого варианта, отличающиеся от заданных для проектируемого ЦОД.

Приложения к рассматриваемому стандарту содержат сведения, имеющие важнейшее значение при проектировании ИИ ЦОД:

- базовый и расширенный наборы показателей проектируемого центра обработки данных;
- перечень основных и вспомогательных систем инженерной инфраструктуры центра обработки данных.

Российская система сертификации ЦОД

Введение в действие рассмотренных выше технико-правовых стандартов свидетельствует об успешном формировании отечественной модели классификации и стандартизации отрасли ЦОД. Для практической реализации этой модели в 2021 г. была создана и зарегистрирована Росстандартом система «РосЦОД» добровольной сертификации ЦОД, являющаяся, по существу, бюджетным аналогом системы *Uptime Institute*.

Организационная структура РосЦод представлена на рис. 2.

Объектами добровольной сертификации в системе РосЦОД являются: продукция, работы и услуги; процессы проектирования, производства, эксплуатации, хранения, перевозки, реализации и утилизации; персонал, участвующий в производстве работ и оказании услуг.

Для определения соответствия при добровольной сертификации в системе РосЦОД могут быть использованы не только документы национальной системы стандартизации, но и межгосударственные, международные стандарты, общероссийские и отраслевые классификаторы (в частности, [1, 12]), стандарты предприятий, условия договоров, своды правил.

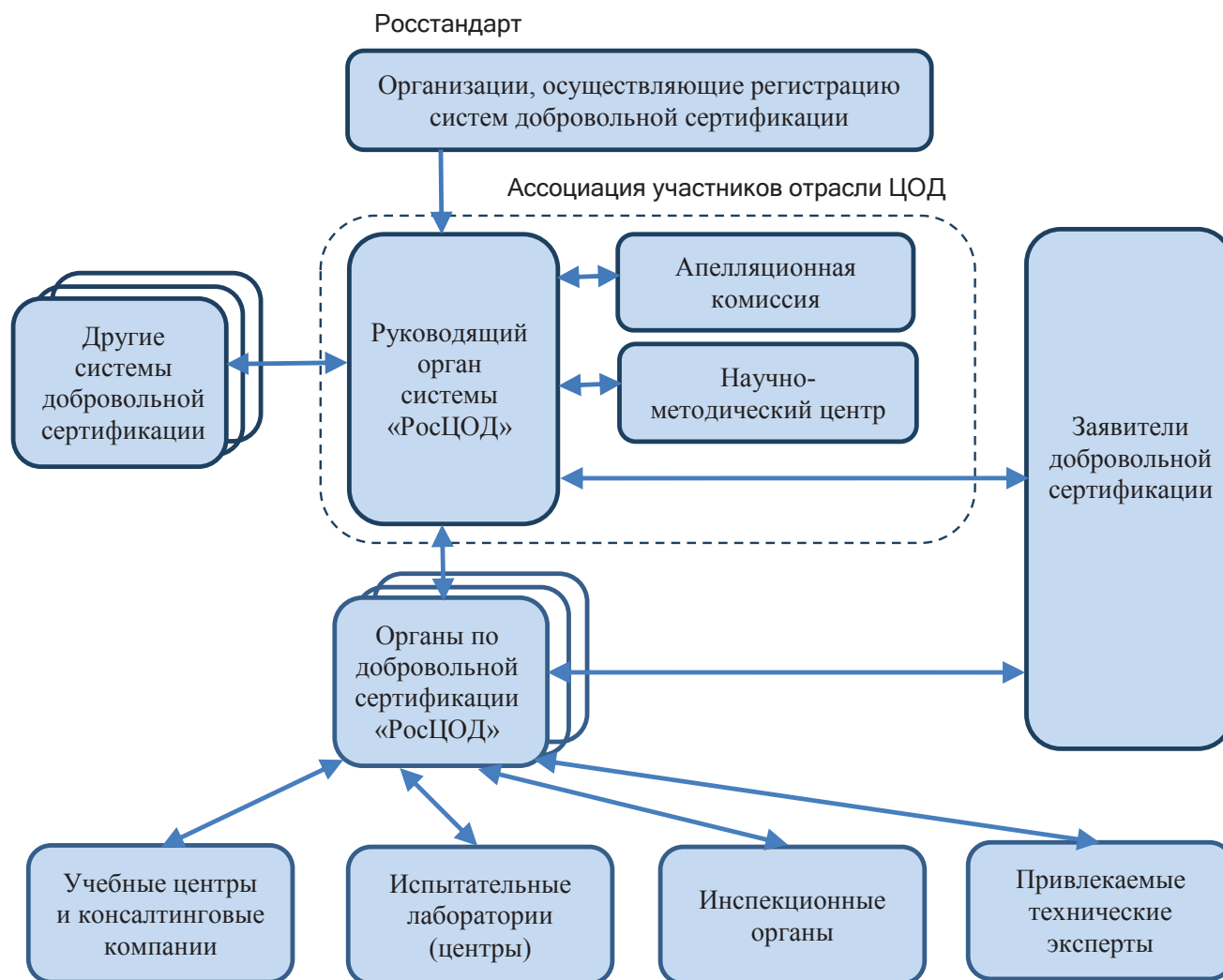


Рис. 2.

Процедура сравнения ЦОД на основе требований ГОСТ Р 70139-2022

Стандартом определена следующая логическая последовательность действий при классификации центров обработки данных.

1. Выбор отдельного показателя для оценки.
2. Оценка выбранного показателя с использованием рекомендованной или собственной методики.
3. Определение класса отдельного показателя на основании Приложения стандарта.
4. Определение класса ЦОД по данному показателю.
5. Определение сводного класса ЦОД по всем показателям, например, по минимальному из классов по показателям.

Каждый из показателей ЦОД оценивается по шкале, имеющей пять классов: от **A** (наивысший класс) до **E** (минимальный). В стандарте приведены правила присвоения сертифицируемому ЦОД определенного класса в категориях ГИС или МЦ.

Очевидно, что при реализации данной последовательности действий может возникнуть такая ситуация, когда к одному классу, в котором заинтересован Заказчик, будут отнесены сразу несколько ЦОД. В этом случае должна быть решена задача выбора лучшей альтернативы из возникшего набора.

Приведем возможный вариант решения этой задачи.

Пусть производится выбор лучшего ЦОД из набора дата-центров, отнесенных в результате проведенной по ГОСТ Р 70139-2022 экспертизы к одному и тому же классу.

Предполагаются заданными:

- исходное множество $X = \{x_j\}, j = \overline{1, K}$ рассматриваемых альтернативных ЦОД мощностью K ;
- множество $W_j = \{\omega_i(x_j)\}, i = \overline{1, m}$ измеренных или полученных экспертным путем значений по каждому i -му показателю из используемого набора для каждого x_j (всего в наборе m показателей);
- диапазон допустимых изменений по каждому i -му показателю $d_i = [\omega_{i2}, \omega_{i1}]$, где ω_{i1} — нижний предел

диапазона изменения i -го показателя, ω_{i2} — верхний (указывается в стандарте);

- коэффициенты $\beta_i, i = (1, m)$ — важности для набора показателей, где β_i — коэффициент важности i -го показателя, определяемый в диапазоне $(0 \leq \beta_i \leq 1)$ [4].

Тогда можно определить нормализованные оценки μ_{ij} i -го показателя для j -го центра обработки данных [5, 6]:

$$\mu_{ij} = \frac{\omega_i(x_j) - \omega_{i1}}{d_i} \quad \text{— для показателя типа «выигрыш»};$$

$$\mu_{ij} = \frac{\omega_{i2} - \omega_i(x_j)}{d_i} \quad \text{— для показателей типа «ущерб»}.$$

Далее следует вычисление, с использованием процедуры свертки значений $\bar{\mu}_j$, осредненных по множеству показателей нормализованных оценок для каждого ЦОД:

$$\bar{\mu}_j = \sum_{i=1}^m \beta_i \mu_{ij}.$$

Наиболее предпочтительным признается центр x^* обработки данных, которому соответствует наибольшее значение $\max \bar{\mu}_j$, осредненной нормализованной оценки:

$$x : \bar{\mu}(x^*) = \max \bar{\mu}_j, \quad j = \overline{1, K}.$$

Если в стандарте для некоторого i -го показателя указывается недопустимый диапазон, а его точное значение и j -й ЦОД при этом такому значению соответствует, то рассматриваемая процедура упрощается, так как значение μ_{ij} становится равным единице.

Рассмотрим следующий численный пример. Обследуются два центра обработки данных x_1 и x_2 , отнесенных к одному и тому же классу **B** по результатам экспертизы, проводимой в соответствии с ГОСТ Р 70139-2022 по установленному общему набору показателей.

Выберем для проведения дополнительной процедуры три показателя, для которых в ГОСТ Р 70139-2022 указаны допустимые диапазоны изменения в каждом из используемых классов **A, B, C, D, E** (табл. 5, 6, 7 ниже).

Зададим численные значения коэффициентов важности рассматриваемых показателей: $\beta_1 = 0,5$; $\beta_2 = 0,3$; $\beta_3 = 0,2$.

Пусть центры обработки данных x_1 и x_2 имеют следующие значения показателей П1, П2, П3:

$$\omega_1(x_1) = 15; \quad \omega_2(x_1) = 1800; \quad \omega_3(x_1) = 15;$$

$$\omega_1(x_2) = 13; \quad \omega_2(x_2) = 2500; \quad \omega_3(x_2) = 12.$$

Показатели П1, П2 относятся к типу «выигрыш», П3 — «ущерб».

Воспользуемся приведенными выше формульными зависимостями и в результате получим:

$$\bar{\mu}_1 = 0,485; \quad \bar{\mu}_2 = 0,561.$$

Отсюда следует, что предпочтительным является x_2 , второй центр обработки данных.

Заключение

Изложенный в статье материал позволяет получить систематизированное представление о направлениях развития отечественной системы сертификации ЦОД и систематизировать основные положения и требования, содержащиеся во вводимых в действие национальных технико-правовых стандартах. Разработанная и представленная процедура сравнения ЦОД является существенным дополнением алгоритма классификации центров обработки данных, содержащегося в стандарте ГОСТ Р 70139.

Проведенный анализ российских национальных технико-правовых стандартов, определяющих вопросы разработки и функционирования ЦОД, а также перспектив использования системы добровольной сер-

Таблица 5

Показатель П1:

Общая доступная мощность электроснабжения, МВт

Класс A	Класс B	Класс C	Класс D	Класс E
Более 20	От 10 до 20	От 3 до 10	От 0,25 до 3	Менее 0,25

Таблица 6

Показатель П2:

Общее количество серверных монтажных шкафов, шт.

Класс A	Класс B	Класс C	Класс D	Класс E
Более 3000	От 801 до 3000	От 201 до 800	От 11 до 200	Не более 10

Показатель ПЗ:
Транспортная доступность и время прибытия экстренных служб, мин

Класс A	Класс B	Класс C	Класс D	Класс E
Не более 10 мин	Не более 20 мин	Не более 40 мин	Данные отсутствуют или не нормируются	Данные отсутствуют или не нормируются

тификации отечественной практики международных и иностранных систем сертификации ЦОД и переходе на отечественные системы.

Рецензент: **Цимбал Владимир Анатольевич**, доктор технических наук, профессор, заслуженный деятель науки РФ, профессор кафедры автоматизированных систем боевого управления Филиала Военной академии им. Петра Великого, г. Серпухов, Российская Федерация.

E-mail: tsimbalva@mail.ru

Литература

1. Борисов Р.С., Ефименко А.А. Классификатор правовых актов для установления правового режима публикуемой информации // Правовая информатика. 2021. № 4. С. 31—45. DOI: 10.21681/1994-1404-2021-4-31-45.
2. Ващекин А.Н. Проблемы правового регулирования отношений в цифровом пространстве // Правосудие. 2020. Т. 2. № 2. С. 126—147.
3. Ефименко А.А., Федосеев С.В. Организация инфраструктуры облачных вычислений на основе SDN сети // Экономика, статистика и информатика. Вестник УМО. 2013. № 5. С. 185—187.
4. Зак Ю.А. Принятие многокритериальных решений. М.: Экономика, 2011. 236 с.
5. Козлов В.Н. Системный анализ, оптимизация и принятие решений. М.: Проспект, 2013. 176 с.
6. Литвак Б.Г. Управленческие решения. М.: Московская финансово-промышленная академия, 2012. 512 с.
7. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74.
8. Ловцов Д.А. Информационная теория эргасистем: монография. М.: РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
9. Ловцов Д.А. Принципы обеспечения защищенности информации в эргасистемах // Правовая информатика. 2021. № 1. С. 36—50. DOI: 10.21681/1994-1404-2021-1-36-50.
10. Ловцов Д.А. Теория защищенности информации в эргасистемах: монография. М.: РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
11. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере. М.: РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
12. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54.
13. Черных А.М. Основные направления интеграции федеральных государственных информационных систем и пространственных данных // Правовая информатика. 2018. № 2. С. 47—56. DOI: 10.21681/1994-1404-2018-2-47-56.

CERTIFICATION OF DATA PROCESSING CENTRES: LEGAL AND TECHNICAL ASPECTS

Sergei Fedoseev, Ph.D. (Technology), Associate Professor, Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.

E-mail: fedsergvit@mail.ru

Keywords: data processing centre (DPC), certification, technical-cum-legal standards, technical regulations, certificate of conformity, status, object of regulation, type of application of the technical regulation and national standard, system redundancy, engineering infrastructure, operational model of operation, international DPC certification systems.

Abstract

Purpose of the work: providing a justification for the research and methodological approach to solving problems of using the domestic DPC certification model and national technical-cum-legal standards determining the requirements for the DPC.

Methods used: logical concept modelling of legal and information relations determined by the domestic DPC classification and certification system and compliance with the requirements of national technical-cum-legal standards, system analysis of relations between the subject area of the legal sphere, objects of the information network technologies sphere, data processing centres development and operation sphere, mathematical algorithms and the main objects and methods of the decision theory and set theory.

Study findings: an analysis of the possibilities of application of technical regulations and national technical-cum-legal standards is carried out and the differences between them are identified, on the basis of the following characteristics: status, object of application, type of application, aspects of regulation. An analysis of international DPC certification systems is carried out. Requirements of technical-cum-legal standards are considered regarding the engineering infrastructure, setup stages, operational model of operation, DPC classification. Prospects for using the RosTsOD DPC Voluntary Certification System are identified, and a justification is given for a DPC comparing procedure.

References

1. Borisov R.S., Efimenko A.A. Klassifikator pravovykh aktov dlia ustanovleniia pravovogo rezhima publikuemoi informatsii. Pravovaia informatika, 2021, No. 4, pp. 31–45. DOI: 10.21681/1994-1404-2021-4-31-45 .
2. Vashchekin A.N. Problemy pravovogo regulirovaniia otnoshenii v tsifrovom prostranstve. Pravosudie, 2020, t. 2, No. 2, pp. 126–147.
3. Efimenko A.A., Fedoseev S.V. Organizatsiia infrastruktury oblachnykh vychislenii na osnove SDN seti. Ekonomika, statistika i informatika, Vestnik UMO, 2013, No. 5, pp. 185–187.
4. Zak Iu.A. Priniatie mnogokriterial'nykh reshenii. M. : Ekonomika, 2011. 236 pp.
5. Kozlov V.N. Sistemnyi analiz, optimizatsiia i priniatie reshenii. M. : Prospekt, 2013. 176 pp.
6. Litvak B.G. Upravlencheskie resheniia. M. : Moskovskaia finansovo-promyshlennaia akademiia, 2012. 512 pp.
7. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66–74. DOI: 10.21681/1994-1404-2017-3-66-74 .
8. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
9. Lovtsov D.A. Printsipy obespecheniia zashchishchennosti informatsii v ergasistemakh. Pravovaia informatika, 2021, No. 1, pp. 36–50. DOI: 10.21681/1994-1404-2021-1-36-50 .
10. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
11. Lovtsov D.A. Sistemologiiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
12. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ograniченного доступа. Pravovaia informatika, 2017, No. 2, pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .
13. Chernykh A.M. Osnovnye napravleniia integratsii federal'nykh gosudarstvennykh informatsionnykh sistem i prostranstvennykh dannykh. Pravovaia informatika, 2018, No. 2, pp. 47–56. DOI: 10.21681/1994-1404-2018-2-47-56 .