МОДЕЛЬ КЛАССИФИКАЦИИ ЦОДов

Разработчик: АНО КС ЦОД

Версия: 2.4 (19.09.2022)

Содержание

1. Введение

Широкое применение информационных систем во всех сферах общества, развитие глобальных сетей передачи данных, систем хранения и обработки данных обуславливает рост числа инженерных объектов, обеспечивающих функционирование таких сетей и систем. Такие объекты, называемые центрами обработки данных (далее– ЦОД), используются как операторами телекоммуникационных сетей, так и государственными и коммерческими предприятиями. Ключевыми требованиями к этим объектам являются требования по надежности, готовности, физической защищенности, предъявляемые используемыми информационными системами и обеспечивающие непрерывность предоставляемых сервисов для их конечных потребителей. Такие требования существенно влияют на применяемые в ЦОДах проектные, технические решения, а также на процессы эксплуатации и обслуживания ЦОДов.

В настоящем документе рассматриваются уровни готовности и физической защищенности ЦОДов в зависимости от применяемых технических решений.

1.2. Назначение документа

Настоящий документ описывает модель классификации ЦОДов применительно к их уровню готовности и физической защищенности и дает рекомендации по организации подобных объектов для обеспечения нужд государственных и частных компаний, использующих информационные системы разного уровня критичности.

Настоящий документ разработан в целях обеспечения единого унифицированного подхода к организации ЦОДов, служащих для работы государственных информационных систем (ГИС) и иных информационных ресурсов.

Основания для разработки: Законопроект № 1195296-7 «О внесении изменений в Федеральный закон "О связи"» (в части регулирования деятельности центров обработки данных). Принят Государственной Думой в первом чтении 6 апреля 2022 года.

1.3. Перечень терминов и сокращений

Центр обработки данных (ЦОД) – сооружение связи с комплексом систем инженерно-технического обеспечения, спроектированное и используемое для размещения оборудования, обеспечивающего обработку или хранение данных, и соответствующее утвержденной классификации (из Проекта Законопроекта № 1195296-7 «О внесении изменений в Федеральный закон "О связи"»).

Технологическая площадка – выделенная территория, имеющая периметр безопасности, на которой расположено одно или несколько зданий ЦОДа, эксплуатируемых одним оператором.

Готовность (Availability) – свойство находиться в работоспособном состоянии в определенный момент (период) времени.

Отказоустойчивость – возможность непрерывного предоставления сервисов на базе данного ЦОДа при единичном отказе любого компонента основных инженерных систем.

Резервирование – способ обеспечения надежности объекта за счет использования дополнительных средств и/или возможностей сверх минимально необходимых для выполнения требуемых функций (ГОСТ Р 27.102-2021).

Доступность ЦОДа – состояние, в котором работоспособность инженерных систем и линий связи ЦОДа обеспечивает условия и значения параметров, необходимые для работы размещаемых в нем ИС абонентов, в соответствии с заявленными характеристиками ЦОДа.

Технологическая мощность ЦОДа – величина, характеризующая способность ЦОДа разместить оборудование, обеспечивающее обработку и (или) хранение данных, и зависящая от технических возможностей комплекса систем инженерно-технического обеспечения в соответствии с утвержденной классификацией центров обработки данных; технологическая мощность ЦОДа определяется двумя основными показателями: подведенной мощностью и числом стойко-мест в нем.

Номинальная мощность стойки – максимальная активная мощность, потребляемая стойкой в любом режиме; является основной проектной характеристикой машинного зала; ограничение величины потребляемой мощности значением номинала стойки является ответственностью абонента ЦОДа; превышение значения номинальной мощности не допускается и может повлечь за собой аварийное отключение стойки и/или выход значений параметров электропитания и среды в машинном зале за границы диапазонов, гарантируемых оператором ЦОДа.

Секционирование – разнесение или конструктивная изоляция взаимно резервирующих компонентов, трубопроводов, трасс таким образом, чтобы единичная авария, включая пожар в отдельном помещении, не могла привести к одновременному отказу взаимно резервирующих компонентов или трасс.

Инженерная инфраструктура ЦОДа – комплекс систем и их оборудования, обеспечивающий бесперебойное функционирование систем и оборудования ИТ-инфраструктуры ЦОДа. Примечание: состав инженерной инфраструктуры определяется требованиями к ее функционированию со стороны оборудования ИТ-инфраструктуры и требованиями к обеспечению безопасной работы всего ЦОДа. Как правило, в состав инженерной инфраструктуры входят системы электроснабжения, поддержания климата, связи и управления, комплекс систем безопасности (ГОСТ Р 58811-2020).

Система электроснабжения – совокупность электроустановок и электрических устройств, предназначенных для обеспечения электроэнергией потребителей электрических сетей (ГОСТ 32144-2013).

Система распределения электропитания – совокупность устройств и путей для передачи и распределения электроэнергии между потребителями электрической сети.

Система холодоснабжения – комплекс оборудования и устройств для производства холода (охлаждаемой среды) и подачи его в воздухоохладители приточных установок и кондиционеров (ГОСТ 22270-2018, пункт 2.85).

Непрерывное охлаждение – поддержание климатических параметров в критичных помещениях ЦОДа при переходе с основных на резервные источники электроснабжения и обратно.

Система вентиляции – комплекс функционально связанных между собой оборудования, установок, устройств, воздуховодов, обеспечивающий обмен воздуха в помещениях для удаления избытков теплоты, влаги, вредных веществ и замену его наружным с целью поддержания допустимых метеорологических условий и чистоты воздуха в обслуживаемой или рабочей зонах.

Физическая безопасность ЦОДа – комплекс мер и технических решений, направленных на обеспечение должного контрольно-пропускного режима и правил нахождения в ЦОДе людей, а также защиту объекта от внешних (природные стихийные катастрофы, результаты негативного воздействия происшествий техногенной и антропогенной природы) и внутренних (задымления, возгорания, пожары, нарушение правил безопасности объекта и пр.) негативных воздействий.

Комплексная система безопасности – система безопасности, одновременно выполняющая несколько функций безопасности, которые снижают риски, обусловленные несколькими видами и/или источниками опасностей (ГОСТ Р 53195.1-2008: «Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения»).

Система контроля и управления доступом (СКУД) – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью (ГОСТ Р 51241-2008).

Система охранной сигнализации – совокупность совместно действующих технических средств для обнаружения несанкционированного проникновения на охраняемый объект, передачи, сбора, обработки и представления информации в заданном виде (Р 78.36.018-2011. «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»).

Система тревожной сигнализации – комплекс устройств, обеспечивающих выдачу сигнала «Тревога» при возникновении угрозы персоналу или угрозы повреждения оборудования путем нажатия кнопки тревожной сигнализации с идентификацией места сигнала «Тревога».

Система видеонаблюдения – совокупность функционирующих видеоканалов, программных и технических средств записи и хранения видеоданных, а также программных и/или технических средств управления, осуществляющих информационный обмен между собой (ГОСТ Р 51558-2014).

Система пожарной безопасности (СПБ) – комплекс организационных мероприятий и технических средств, направленных на предотвращение пожара и ущерба от него (ГОСТ 12.1.004-91).

Обособленная территория – территория, границы которой обозначены ограждением (объектами искусственного происхождения), прилегающая к зданию (строению, сооружению), в котором расположен ЦОД.

Аварийное освещение – освещение, предназначенное для использования при нарушении питания рабочего освещения (ГОСТ Р 55842-2013 (ИСО 30061:2007)).

Служба эксплуатации ЦОДа – организация или ее подразделение, в обязанность которым вменяется проведение работ по эксплуатации систем и оборудования ЦОДа (ГОСТ Р 58812-2020).

Автоматизированная система диспетчеризации и управления (АСДУ) – комплекс средств, обеспечивающих централизованный мониторинг, диспетчеризацию и автоматическое управление оборудованием инженерных систем, обеспечивающих функционирование объекта.

ФЗ – федеральный закон Российской Федерации

ИТ – информационные технологии

ГИС – государственная информационная система

ИБП - источник бесперебойного питания

ДГУ – дизель-генераторная установка

ГРЩ – главный распределительный щит

БРП – блок распределения питания стойки

PDU – Power Distribution Unit, то же, что БРП

СБЭ – система бесперебойного электроснабжения

СГЭ – система гарантированного электроснабжения

САО – система аварийного освещения

САПС – система автоматической пожарной сигнализации

СПА – система противопожарной автоматики

СОУЭ – система оповещения и управления эвакуацией

АУПТ-- автоматическая установка пожаротушения

СГПТ – система газового пожаротушения

ВОЛС – волоконно-оптическая линия связи

MMR – Meet-me-room, выделенное место в пределах ЦОДа, где телекоммуникационные компании могут физически коммутироваться между собой и осуществлять обмен данными.

1.4. Используемые нормативные и прочие документы

Для составления настоящего документа использованы следующие нормативные документы, правила и нормы:

- «Правила устройства электроустановок» (ПУЭ), версия 7
- Стандарт ГОСТ Р 53987-2010 (ИСО 8528-1-2005) «Электроагрегаты генераторные переменного тока с приводом от двигателя внутреннего сгорания. Часть 1. Применение, технические характеристики и параметры»
- Свод правил СП 60.13330.2020 «Отопление, вентиляция и кондиционирование воздуха. СНиП 41-01-2003»
- Свод правил СП 12.13130.2009 «Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности»
- ГОСТ Р 27.102-2021. «Надежность в технике»
- Федеральный закон № 116-ФЗ «О промышленной безопасности опасных производственных объектов»
- Стандарт ГОСТ Р 52551-2016 «Системы охраны и безопасности. Термины и определения»
- Сборник рекомендаций Р 78.36.018-2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»
- Стандарт ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний»
- Федеральный закон ФЗ № 123 «Технический регламент о требованиях пожарной безопасности»
- Свод правил СП 486.1311500.2020 «Свод правил. Системы противопожарной защиты. Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения и системами пожарной сигнализации»
- Свод правил СП 3.13130.2009 «Свод правил. Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре»
- Свод правил СП 485.1311500.2020 «Свод правил. Системы противопожарной защиты. Установки пожаротушения автоматические. Нормы и правила проектирования»
- СП 20.13330.2016 «Свод правил. Нагрузки и воздействия. Актуализированная редакция СНиП 2.01.07-85» (ред. от 28.01.2019)
- Постановление Правительства РФ № 390 «О противопожарном режиме» (с изменениями на 7 марта 2019 года)

- Постановление Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСБ N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
- Приказ ФСТЭК № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Кроме того, учитывались рекомендации следующих международных стандартов:

- Серия стандартов CEN/CENELEC EN 50600-2012
- Стандарт Uptime Institute Tier Standard: Topology
- Стандарт Uptime Institute Tier Standard: Operational Sustainability
- Руководство ASHRAE TC 9.9-2016 Data Center Power Equipment Thermal Guidelines and Best Practices.

2. Классификация ЦОДов

В зависимости от применяемых технологических решений, архитектуры построения инженерных систем и подходов к обеспечению физической защищенности ЦОДы могут быть классифицированы по степени их надежности и физической защищенности в отношении исполняемых ими функций (реализуемых сервисов).

Классификация ЦОДов:

- Класс A (Высший);
- Класс B (Средний);
- Класс C (Низший).

Данные уровни надежности различаются по подходам к организации (архитектуре) и резервированию основных инженерных систем, т.е. инженерных систем, обеспечивающих принципиальную возможность функционирования ЦОДа (система электропитания, система холодоснабжения), а также по степени их физической защищенности, оснащению противопожарными системами, по общим характеристикам здания ЦОДа, места его расположения, организации линий связи.

Для Класса C основным принципом реализации инженерной архитектуры является резервирование всех активных компонентов основных инженерных систем.

Для Класса B основным принципом реализации инженерной архитектуры является обеспечение возможности выполнения операций по техническому обслуживанию, ремонту, замене любого компонента основных инженерных систем без перерыва в предоставлении сервисов на базе данного ЦОДа.

Для Класса A основным принципом реализации инженерной архитектуры является отказоустойчивость, понимаемая как возможность непрерывного предоставления сервисов на базе данного ЦОДа при единичном отказе любого компонента основных инженерных систем.

2.1. Критерии соответствия

ЦОД признается соответствующим определенному классу при следующих условиях:

- Организация электрических систем ЦОДа, включая внешние линии электроснабжения, резервные источники электроснабжения, внутреннюю систему электропитания и систему распределения электропитания, соответствует минимальным требованиям для данного класса, приведенным в разделе «3. Система электроснабжения»;
- Организация механических систем ЦОДа, включая все компоненты систем холодоснабжения и промышленного кондиционирования, элементы контуров охлаждения, соответствует минимальным требованиям для данного класса, приведенным в разделе «4. Система холодоснабжения»;
- Организация каналов связи ЦОДа с внешними по отношению к нему объектами соответствует минимальным требованиям для данного класса, приведенным в разделе «5. Телекоммуникационная инфраструктура»;
- Организация внутренних пространств ЦОДа, характеристики здания ЦОДа, место его расположения соответствуют минимальным требованиям для данного класса, приведенным в разделе «6.1. Общие требования к зданию, сооружению (помещениям) ЦОДа»;

- Организация физической, в том числе пожарной, безопасности ЦОДа соответствует минимальным требованиям для данного класса, приведенным в разделе «6. Физическая безопасность».

Оценка соответствия ЦОДа указанным критериям классификации проводится уполномоченными (аккредитованными) организациями в соответствии с порядком проведения технического аудита центров обработки данных с целью определения их класса согласно программе и методике проведения оценки.

Безотносительно к вышеприведенной классификации все инженерные системы ЦОДа, свойства и характеристики здания ЦОДа, а также все процессы эксплуатации ЦОДа должны отвечать всем соответствующим требованиям и нормам, действующим на территории Российской Федерации.

3. Система электроснабжения

Система электроснабжения ЦОДа является основной и наиболее значимой инженерной системой объекта, обеспечивающей его принципиальную работоспособность. Пропадание внешнего электроснабжения, просадки напряжения и помехи в электрической сети – наиболее частые причины отключения оборудования и прекращения работы сервисов, предоставляемых потребителям ЦОДов. Система электроснабжения ЦОДа должна быть организована таким образом, чтобы минимизировать или устранить риски отключения его потребителей.

В зависимости от степени критичности и требований к непрерывности работы размещенных в ЦОДе информационных систем его система электроснабжения может быть организована различным образом. При этом каждый из уровней готовности системы электроснабжения предполагает свой минимальный набор требований.

В общем случае система электроснабжения ЦОДа зависит как от характера внешнего энергоснабжения объекта (наличия источников генерации электроэнергии на объекте), так и от применяемой системы распределения электропитания в пределах объекта.

3.1. Энергоснабжение ЦОДа

Система энергоснабжения для ЦОДа должна предусматривать наличие нескольких независимых источников энергоснабжения, в качестве которых могут выступать внешние источники энергоснабжения, локальные источники генерации электроэнергии, используемые ЦОДом, или любая их комбинация, в соответствии с требованиями, приведенными в табл. 3.1. Для повышения надежности рекомендуется, чтобы линии электропередачи от любых из этих источников были разнесены территориально. Мощность источников электроснабжения следует выбирать таким образом, чтобы их резервирование было не ниже N при пропадании электроснабжения от любого из источников.

В случае нескольких внешних источников энергоснабжения линии электропередачи должны быть проложены от разных питающих центров (электростанций/подстанций/распределительных пунктов) или от разных ячеек одной подстанции (в этом случае обязательным условием является запитывание линий электропередачи от разных секций/систем шин с применением АВР).

Запрещается осуществлять технологическое присоединение ЦОДа к бесхозяйным сетям либо к сетям организаций, не оказывающих услуги по передаче электроэнергии и не являющихся сетевыми организациями (внутренние сети зданий и сооружений, садовые и гаражные кооперативы и т.п.), за исключением опосредованного присоединения (присоединения по субабонентской схеме, когда субабонентом является лицо, чьи энергоустановки не присоединены непосредственно к сетям энергоснабжающей организации), а также присоединения к сетям объектов по производству электроэнергии, имеющих, в свою очередь, присоединение к Единой энергосистеме.

Табл. 3.1. Организация энергоснабжения ЦОДа

Характеристика	Класс C	Класс B	Класс A
Число независимых источников электроэнергии, не менее чем	Два	Два	Два
Автоматическое переключение между источниками энергоснабжения	Требуется	Требуется	Требуется
Автоматический запуск генераторной установки (при наличии)	Требуется	Требуется	Требуется
Мин. запас топлива генераторной установки (при наличии), в часах работы	2	4	12
Разделение групп электроприемников, относящихся к технологическому циклу ЦОДа, и групп электроприемников сторонних организаций, вынесение электрических нагрузок ЦОДа на отдельные центры питания (трансформаторные подстанции/группы, секции/системы шин РУ, РП, генераторные установки)	Рекомендуется	Обязательно	Обязательно

3.2. Система внутреннего распределения электропитания ЦОДа

Система внутреннего распределения электропитания в ЦОДе служит для передачи электрической энергии от питающих линий (в том числе генераторных станций) различным группам потребителей в пределах ЦОДа. Среди потребителей электроэнергии можно выделить следующие группы нагрузок:

- Критичные ИТ-нагрузки;
- Некритичные ИТ-нагрузки;
- Критичные нагрузки инженерных и вспомогательных систем здания;
- Некритичные нагрузки инженерных и вспомогательных систем здания.

К критичным видам нагрузок относят те нагрузки, перебои в работе которых не допускаются или должны быть минимизированы (например, ИТ-оборудование информационных систем, СПБ, СКУД, СВН, АСДУ, САО и др.). К некритичным видам нагрузок относят все прочие нагрузки здания ЦОДа.

Электропитание критичных видов нагрузок должно осуществляться от системы бесперебойного питания, построенной на статических или динамических ИБП, имеющих достаточный уровень резервирования (табл. 3.2).

При использовании статических ИБП время автономной работы от батарей при полной нагрузке (в аварийном режиме, т. е. в конфигурации N) принимается не менее 5 мин в конце срока эксплуатации батарей.

Для систем электроснабжения и электрораспределения ЦОДа Класса А взаимно резервирующие элементы систем электроснабжения должны располагаться в отдельных помещениях и быть физически изолированы друг от друга, взаимно резервирующие трассы доставки электропитания на всем их протяжении внутри ЦОДа, от ввода кабелей в здание до оконечного ИТ-оборудования, должны проходить в разных лотках.

Вторичное распределение питания после СБЭ к ИТ-нагрузке надлежит выполнять в соответствии с требованиями к заданному классу ЦОДа, приведенными в табл. 3.2.

Оконечное ИТ-оборудование, размещаемое в ЦОДе, следует подключать к блокам распределения питания (БРП, PDU) с учетом распределения нагрузки по независимым вводам питания (если применимо). Для оборудования с одним блоком питания рекомендуется предусмотреть наличие АВР/ATS.

Мощности трансформаторов, ДГУ, ИБП и других компонентов электроустановки должны выбираться таким образом, чтобы обеспечить электроснабжение соответствующих групп потребителей ЦОДа с учетом резервирования. Коэффициент использования следует принять за 1 (единицу).

В ЦОДе должна быть обеспечена возможность мониторинга показателей электропитания на уровне ГРЩ, ДГУ, ИБП.

Основные требования к системе распределения электроэнергии приведены в табл. 3.2.

Табл. 3.2. Организация системы внутреннего распределения электропитания ЦОДа

Характеристика	Класс C	Класс B	Класс A
Уровень резервирования для компонентов системы электроснабжения	N+1 для всех активных компонентов	N+1 для любого компонента	N для любого компонента после любого отказа
Минимальное число контуров распределения электропитания	Один	Два активных	Два активных
Техническая возможность подключения оконечного ИТ-оборудования одновременно к двум независимым линиям электропитания	Рекомендуется	Требуется	Требуется
Особые требования по физическому размещению компонентов системы электропитания	Нет	Рекомендовано размещение СБП вне машинных залов	Секционирование всех компонентов по числу резервных элементов для каждой секции

4. Система холодоснабжения

Система холодоснабжения центра обработки данных является одной из основных инженерных систем ЦОДа, обеспечивает необходимые климатические параметры в его помещениях, оказывает критически важное влияние на работоспособность установленного в нем оборудования. Критичные нагрузки ЦОДа, как правило, требовательны к таким параметрам окружающей среды, как температура и влажность. Отклонение этих параметров от границ требуемого диапазона значений может повлечь за собой перегрев оборудования, сбои и отказы в его работе, выход оборудования из строя. Во избежание подобных инцидентов система холодоснабжения и кондиционирования ЦОДа должна быть организована таким образом, чтобы минимизировать или устранить вышеуказанные риски.

В зависимости от степени критичности и требований к непрерывности работы размещенных в ЦОДе информационных систем, а также учитывая значительную вариативность существующих технологических решений для обеспечения требуемого климатического режима эксплуатации, системы кондиционирования и холодоснабжения ЦОДа могут быть организованы различным образом, при условии соблюдения требований к системе охлаждения, приведенных в табл. 4.1.

В общем случае выбор системы охлаждения ЦОДа зависит от характера и набора требований его критичных потребителей, а также от природных климатических условий, в которых располагается ЦОД. При проектировании системы охлаждения необходимо предусматривать обеспечение необходимого климатического режима эксплуатации для всех критичных видов нагрузок, а также для иного инженерного технологического оборудования, чувствительного к среде эксплуатации, такого как ИБП, аккумуляторные батареи, компоненты СГПТ, СКУД, СВН и пр. С целью обеспечить необходимый климатический режим эксплуатации следует руководствоваться требованиями производителя оборудования критичных потребителей ЦОДа к показателям температуры, относительной влажности, градиента температуры, высоты над уровнем моря; положениями Свода правил СП 60.13330.2020 «Отопление, вентиляция и кондиционирование воздуха. СНиП 41-01-2003»; рекомендациями ASHRAE TC9.9-2016 по организации климатических режимов для соответствующего класса ИТ-оборудования (A0-A4), а также сведениями о среднегодовых температурах и температурных минимумах и максимумах в регионе размещения ЦОДа.

Чтобы обеспечить подпиточную воду в установках холодоснабжения, если перерыв в подаче воды приводит к критичной потере холодопроизводительности, следует предусмотреть основной и резервный источник ее подачи. Для систем увлажнения воздуха резервирование подпитки водой не является обязательным.

При построении системы охлаждения ИТ-нагрузки, размещенной в машинных залах ЦОДа, с помощью периметральных или внутрирядных блоков кондиционирования воздуха следует предусмотреть резервирование таких блоков по схеме не ниже N+1 на помещение.

При расчете тепловых нагрузок необходимо исходить из номинальных мощностей стоек и максимальных (паспортных) показателей для инженерного оборудования.

Необходимо предусмотреть возможность контроля температурного и влажностного режима для всех критичных потребителей ЦОДа.

Табл. 4.1. Организация системы охлаждения ЦОДа

Характеристика	Класс C	Класс B	Класс A
Минимальный уровень резервирования для компонентов систем холодоснабжения и кондиционирования	N+1 для всех активных компонентов	N+1 для любого компонента	N для любого компонента после любого отказа
Минимальное число контуров с теплоносителем системы холодоснабжения (при наличии таковых)	Один	Два активных	Два или более активных (авария на одном из контуров не должна приводить к нарушению работоспособности системы холодоснабжения)
Непрерывное охлаждение	Не требуется	Не требуется	Требуется
Особые требования по физическому размещению компонентов системы холодоснабжения	Не требуется	Не допускается прокладка транзитных трубопроводов в пределах машинного зала или над ним	Требования к классу B + секционирование всех компонентов по числу резервных элементов для каждой секции

5. Телекоммуникационная инфраструктура

ЦОД не только обеспечивает возможность функционирования ИТ-оборудования, отвечающего за обработку и хранение данных и размещение информационных систем, но и несет на себе функции объекта связи, предоставляющего возможность передачи информации, являющегося узлом распределенной сети передачи данных и обеспечивающего связность с точками сбора данных, а также пользователями информационных систем, работающих в ЦОДе.

Для реализации функций связи ЦОД должен иметь телекоммуникационную инфраструктуру, включающую в себя элементы волоконно-оптических линий связи (ВОЛС), которые обеспечивают связность ЦОДа с внешними по отношению к нему объектами. Проектом ЦОДа или технологической площадки должны быть предусмотрены линейно-кабельные сооружения, обеспечивающие прокладку линий связи как при строительстве ЦОДа, так и в ходе его дальнейшей эксплуатации в достаточном объеме и с достаточным резервированием, соответствующим классу ЦОДа. При невозможности реализации ВОЛС допустимо использовать альтернативные способы организации каналов связи (например, спутниковую связь).

Надежность связи ЦОДа с другими объектами может быть повышена за счет применения резервирующих линий связи, в том числе принадлежащих различным поставщикам услуг связи. Целесообразна организация нескольких точек коммутации и размещения телекоммуникационного оборудования (комнат ввода, Meet-Me-Room) внутри ЦОДа и обеспечение возможности прокладки линий связи к ним от вводных колодцев различными маршрутами внутри здания ЦОДа.

Поставщиком услуг связи может являться как владелец (оператор) ЦОДа, так и сторонняя по отношению к ЦОДу организация. Целесообразно использовать услуги различных поставщиков связи, в том числе для прокладки ВОЛС.

При организации точек размещения телекоммуникационного оборудования ЦОДа в помещениях, не служащих для размещения основного ИТ-оборудования (машинных залах), требования к организации таких помещений аналогичны требованиям к машинным залам с учетом наличия и мощности активного оборудования.

Характеристики, топология ВОЛС и пропускная способность каналов связи определяются проектировщиком на основании предполагаемого (расчетного) объема трафика между размещенными в ЦОДе информационными системами и их пользователями.

Требования к организации телекоммуникационной инфраструктуры ЦОДа приведены в табл. 5.1.

Табл. 5.1. Организация телекоммуникационной инфраструктуры ЦОДа

Характеристика	Класс С	Класс В	Класс А
Минимальное числонезависимых трасс ВОЛС (иных линий связи, при невозможности прокладки ВОЛС)	Одна	Две, допустима прокладка единым маршрутом	Две, различными непересекающимися маршрутами
Число точек размещения телекоммуникационного оборудования внутри здания ЦОДа	Одна	Одна, рекомендовано две	Две, обязательно
Число телекоммуникационных вводов в здание/ на технологическую площадку и минимальное расстояние между ними (если применимо)	Один	Один, рекомендовано два с расстоянием не менее 20 м между вводами	Два, с расстоянием не менее 20 м между вводами
Прокладка линий связи внутри здания от телекоммуникационных вводов до точек размещения телекоммуникационного оборудования разными непересекающимися маршрутами	-	Рекомендуется	Требуется

6. Физическая безопасность

Под физической безопасностью ЦОДа понимается комплекс мер и технических решений, направленных на обеспечение должного контрольно-пропускного режима и правил нахождения в ЦОДе людей, а также защиту объекта от внешних (природные стихийные катастрофы, результаты негативного воздействия происшествий техногенной и антропогенной природы) и внутренних (задымления, возгорания, пожары, нарушение правил безопасности объекта и пр.) негативных воздействий.

6.1. Общие требования к зданию, сооружению (помещениям) ЦОДа

ЦОД должен размещаться на территории Российской Федерации. При выборе места размещения ЦОДа рекомендовано учитывать риски, связанные с возникновением природных или техногенных катастроф, а также степень подверженности влиянию следующих негативных факторов:

- нахождение в сейсмически активной зоне;
- наводнения внешнего происхождения;
- снежные бураны/сильные ветра/ураганы/торнадо;
- повышение уровня воды в реках/водоемах/озерах, приводящее к затоплению значительных территорий;
- пожары внешнего происхождения;
- повышенное электромагнитное излучение, вибрации, взрывы;
- нахождение на территории с экстремальными значениями температурных минимумов и максимумов;
- нахождение на территории с высоким уровнем относительной влажности воздуха;
- нахождение на территории, расположенной на значительной (более 1500 м) высоте над уровнем моря;
- близость аэропортов (нахождение в зоне глиссад воздушного транспорта), дамб, других опасных объектов;
- близость зон скопления людей (вокзалы, порты, аэропорты, ТПУ, торговые центры, зоны массовых гуляний и пр.);
- близость детских, спортивных, учебных, медицинских, исправительных учреждений/сооружений, иных объектов социальной значимости;
- близость производственных, складских и иных объектов, вызывающих значительное загрязнение воздуха, в том числе агрессивными парами и газами;
- близость лесных массивов, пашных земель;
- близость опасных производственных объектов (такие объекты определяются согласно Федеральному закону № 116-ФЗ «О промышленной безопасности опасных производственных объектов»);
- близость надземных и подземных магистральных водо-, нефте-, газо-, теплопроводов, хранилищ взрывоопасных и пожароопасных веществ.

Требования к месту размещения, зданиям и помещениям ЦОДа приведены в табл. 6.1 и 6.2.

Табл. 6.1. Общие характеристики размещения ЦОДа

Характеристика	Класс С	Класс В	Класс А
Размещение ЦОДа	В специально спроектированном* для данных целей здании, сооружении (комплексе зданий/сооружений), части или отдельном помещении здания/сооружения	В специально спроектированном* для данных целей здании, сооружении (комплексе зданий/сооружений) или части здания/сооружения	В специально спроектированном* для данных целей здании, сооружении или комплексе зданий/сооружений
Обособленность объекта	Здание/комплекс зданий и сооружений ЦОДа может располагаться на общей территории, через которую могут проходить транзитные коммуникации. Через здание (зону) ЦОДа не проходят транзитные коммуникации сторонних собственников (пользователей), за исключением транзитных коммуникаций инженерных систем других зданий и сооружений ЦОДа, принадлежащих одному собственнику объектов ЦОДа или оператору ЦОДа в составе одного кампуса ЦОДа	Здание/комплекс зданий и сооружений ЦОДа может располагаться на общей территории, через которую могут проходить транзитные коммуникации. Через здание (зону) ЦОДа не проходят транзитные коммуникации сторонних собственников (пользователей), за исключением транзитных коммуникаций инженерных систем других зданий и сооружений ЦОДа, принадлежащих одному собственнику объектов ЦОДа или оператору ЦОДа в составе одного кампуса ЦОДа	Здание/комплекс зданий и сооружений ЦОДа располагается на обособленной территории. Через здание ЦОДа не проходят транзитные коммуникации сторонних собственников (пользователей), за исключением транзитных коммуникаций инженерных систем других зданий и сооружений ЦОДа, принадлежащих одному собственнику объектов ЦОДа или оператору ЦОДа в составе одного кампуса ЦОДа

**Новом, реконструированном или переоборудованном.*

Табл. 6.2. Наличие отдельных вспомогательных помещений в ЦОДе

Назначение отдельного помещения	Класс С	Класс В	Класс А
Распаковка, хранение, тестирование и настройка ИТ-оборудования	Не требуется	Рекомендуется	Требуется
Диспетчерский центр инженерных систем ЦОДа (в пределах технологической площадки)	Не требуется	Требуется	Требуется
Хранение ЗИП (в пределах технологической площадки)	Не требуется	Рекомендуется	Требуется

Здание и/или помещения ЦОДа должны быть оснащены комплексной системой безопасности, которая должна обеспечивать сохранность материальных и информационных ресурсов ЦОДа, а также защиту жизни и здоровья персонала и клиентов ЦОДа.

В состав комплексной системы безопасности входят следующие системы:

- контроля и управления доступом (СКУД);
- охранной и тревожной сигнализации;
- видеонаблюдения;

- пожарной безопасности.

Наличие всех этих систем требуется для любого ЦОДа, независимо от его класса.

Обеспечение режима безопасности в помещениях ЦОДа достигается, в частности, за счет следующих мер:

- оснащение помещений входными дверьми с доводчиками и замками, постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода, а также оборудование помещений техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;
- турникеты для контроля прохода в защищенный периметр;
- оборудование окон помещений, расположенных на первых и (или) последних этажах зданий, а также окон, находящихся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения;
- утверждение правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- утверждение перечня лиц, имеющих право доступа в помещения.

6.2. Система контроля и управления доступом

Система контроля и управления доступом (СКУД) предназначена для технического обеспечения пропускного и внутриобъектового режимов на площадке и в помещениях ЦОДа, разграничения прав доступа, регистрации и архивации событий. Требования к системе контроля доступа приведены в табл. 6.3.

Табл. 6.3. Контроль доступа в ЦОДе

Обеспечение физической защиты	Класс C	Класс B	Класс A
Серверные залы, вспомогательные помещения и оборудование ЦОДа	Требуется	Требуется	Требуется
Подходы к зданию и входы в здание ЦОДа	Не требуется	Требуется	Требуется
Периметр территории, на которой расположен ЦОД	Не требуется	Не требуется	Требуется

Система СКУД должна включать следующие средства:

- контроля пребывания сотрудников и посетителей на территории ЦОДа;
- управления доступом в отдельные помещения и обеспечения режима доступа;
- накопления и дальнейшего анализа событий.

Система СКУД должна обеспечивать:

- санкционированный доступ сотрудников и посетителей во внутренние помещения ЦОДа с разделением по времени и зонам доступа;
- управление пропусками;
- вывод на монитор дежурного охраны и пульт централизованного наблюдения сообщения о несанкционированных событиях в СКУД;
- формирование отчетов по событиям, которые состоялись, с возможной задачей выборки по следующим признакам: тип события, номер пропуска, фамилия владельца пропуска, временной интервал построения выборки с точностью до одной минуты;
- формирование отчетов по оперативной ситуации на объекте: пребывание сотрудников и посетителей с учетом контролируемых зон доступа;

- защиту самой СКУД и информации в ней от несанкционированного доступа;
- автоматическую диагностику состояния аппаратного обеспечения системы;
- прием сигнала «Пожар» (и реагирование на него) от систем пожарной сигнализации и пожаротушения.

В случае возникновения опасности для жизни и здоровья сотрудников и посетителей ЦОДа СКУД должна обеспечивать возможность беспрепятственного покидания помещений ЦОДа с формированием сигнала в охранную сигнализацию.

Оборудование СКУД должно быть обеспечено бесперебойным электропитанием.

При необходимости, а также в целях соблюдения требований соответствующих законов или иных документов, регулирующих деятельность по обработке, передаче и хранению информации, отдельные группы ИТ-оборудования могут выделяться в индивидуальные пространства в пределах машинных залов ЦОДа. Такие индивидуальные пространства, реализуемые в виде клетей, выгородок и пр., также должны оснащаться элементами СКУД, препятствующими несанкционированному доступу к ИТ-оборудованию.

6.3. Система охранной и тревожной сигнализации

Система охранной сигнализации предназначена для своевременного оповещения службы безопасности о проникновении (попытке проникновения) на защищаемую территорию и в защищаемые системой помещения ЦОДа. Требования к такой системе приведены в табл. 6.4.

Система охранной сигнализации должна обеспечивать:

- защиту периметра (ограждения) территории от проникновения в круглосуточном режиме;
- защиту периметра здания (двери, окна, каналы, люки и пр. размером более 150x150 мм);
- защиту периметра и внутренних объемов помещений критической инфраструктуры ЦОДа;
- защиту кровли от несанкционированного проникновения;
- круглосуточный контроль обстановки на охраняемом объекте;
- ведение протокола действий пользователей системы;
- независимую дистанционную постановку/снятие с охраны помещений с выдачей сигнала «Тревога» в случае несанкционированного проникновения в них.

Внешние двери эвакуационных выходов, оснащенные механическими замками, должны иметь возможность открывания только изнутри здания.

Табл. 6.4. Оснащение ЦОДа системой охранной сигнализации

Объект	Класс C	Класс B	Класс A
Помещения (зоны) для размещения ИТ-оборудования	Требуется	Рекомендуется оборудовать не менее чем двумя рубежами охранной сигнализации	Рекомендуется оборудовать не менее чем двумя рубежами охранной сигнализации
Вспомогательные помещения ЦОДа	Требуется	Требуется	Требуется
Окна и двери	Требуется	Требуется	Требуется
Подходы к зданию	Не требуется	Требуется	Требуется
Периметр территории	Не требуется	Не требуется	Требуется

Помещения (зоны) для размещения критической инфраструктуры ЦОДа рекомендуется оборудовать не менее чем двумя рубежами охранной сигнализации, для чего используются извещатели с разными физическими принципами действия. Для помещений с размещенным внутри ИТ-оборудованием рекомендуется организовать защиту периметра помещения от пролома.

Система тревожной сигнализации должна обеспечивать выдачу сигнала «Тревога» в подразделение охраны при возникновении угрозы персоналу или угрозы повреждения оборудования путем нажатия кнопки тревожной сигнализации с идентификацией места сигнала «Тревога».

Кнопки тревожной сигнализации устанавливаются в отдельных помещениях для размещения ИТ-оборудования, на рабочих местах ответственных лиц, в кабинете руководителя, возле входных дверей, а также на посту охраны. При этом кнопки тревожной сигнализации должны устанавливаться в местах, удобных для использования персоналом ЦОДа и незаметных для посторонних лиц. Кнопки тревожной сигнализации должны иметь защиту от ложного нажатия.

Все тревожные сигналы системы должны отображаться на посту безопасности ЦОДа и на постах субъекта (субъектов) охраны, с которым (которыми) заключен договор об охране ЦОДа.

6.4. Система видеонаблюдения

Система видеонаблюдения должна обеспечивать визуальное наблюдение за охраняемыми зонами в соответствии с классификацией ЦОДа, получение объективной информации о событиях в реальном времени, ведение видеоархива и возможность идентификации субъектов, которые выполняли различные действия. Требования к такой системе приведены в табл. 6.5.

Табл. 6.5. Оснащение ЦОДа системой видеонаблюдения

Объект	Класс С	Класс В	Класс А
Залы (зоны) для размещения ИТ-оборудования	Требуется*	Требуется*	Требуется*
Подходы к ИТ-залам	Определяется на стадии проектирования	Требуется	Требуется
Вспомогательные и технологические помещения	Определяется на стадии проектирования	Требуется	Требуется
Центральный и запасной входы	Требуется	Требуется	Требуется
Посты охраны, КПП	При наличии поста охраны	Требуется	Требуется
Подходы и подъезды к зданию, парковки	Не требуется	Требуется	Требуется
Зоны установки внешних блоков инженерных систем	Требуется	Требуется	Требуется
Периметр территории	Не требуется	Не требуется	Требуется

** При работе системы видеонаблюдения в серверном помещении не должно быть зон, недоступных для просмотра.*

Требования к системе видеонаблюдения:

- удаленное администрирование системы,управление оборудованием и мониторинг его состояния;
- совместимость с программными средствами основных разработчиков видеосистем и периферийного оборудования;
- скорость записи данных видеонаблюдения должна составлять не менее 20 кадров в секунду;
- рекомендована непрерывная видеозапись, возможно включение по детекции движения;
- обеспечение одновременной записи и просмотра ранее записанных изображений;
- глубина видеоархива не менее 90 дней.

Уличные камеры должны обеспечивать работу в климатических условиях площадки ЦОДа, при необходимости оснащаться ИК-прожекторами, детекторами движения, работать в режиме «день-ночь».

Информация от всех видеокамер должна собираться на сервере для хранения видеоинформации, который устанавливается в защищенном помещении (или серверном помещении ЦОДа). Необходимо обеспечить наличие резервной копии видеоархива.

Система видеонаблюдения должна обеспечивать защиту данных и разграничение прав доступа пользователей разного уровня.

6.5. Система пожарной безопасности

Система пожарной безопасности ЦОДа должна соответствовать требованиям ФЗ № 123 «Технический регламент о требованиях пожарной безопасности», а также специализированным Сводам правил и ГОСТам по пожарной безопасности. Требования к оснащению ЦОДа составляющими системы пожарной безопасности приведены в табл. 6.6.

Здания, сооружения и помещения ЦОДа должны быть оснащены системами автоматической пожарной сигнализации (САПС) и противопожарной автоматики (СПА), системой оповещения и управления эвакуацией (СОУЭ), а также автоматическими установками пожаротушения (АУПТ) в соответствии с рекомендациями и требованиями СП 486.1311500.2020 («Свод правил. Системы противопожарной защиты. Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматически установками пожаротушения и системами пожарной сигнализации») и СП 3.13130.2009 («Свод правил. Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре»).

Серверные помещения и помещения ИБП рекомендуется оборудовать системами сверхраннего обнаружения возгорания.

Табл. 6.6. Оснащение помещений ЦОДа системами пожарной безопасности

	Класс C	Класс B	Класс A
САПС	Согласно СП 486.1311500.2020	Согласно СП 486.1311500.2020	Согласно СП 486.1311500.2020
АУПТ	Согласно СП 486.1311500.2020	Согласно СП 486.1311500.2020	Согласно СП 486.1311500.2020
Система сверхраннего обнаружения	На усмотрение проектировщика	В серверных залах рекомендуется	В серверных залах обязательно
СОУЭ	Согласно СП 3.13130.2009	Согласно СП 3.13130.2009	Согласно СП 3.13130.2009

САПС, СПА, АУПТ и СОУЭ должны, в частности, обеспечивать:

- раннее обнаружение пожара по первичному признаку возникновения пожара, характерному для данного типа помещений;
- локализацию места возгорания, объемное пожаротушение, ликвидацию пожара;
- автоматический или ручной запуск автоматики АУПТ;
- вывод сигнала «Пожар» от установок пожаротушения и пожарной сигнализации на центральный пульт наблюдения объекта и городской пульт пожарной охраны (при наличии технической возможности);
- разделение сигналов «Пожар» и «Неисправность»;
- выдачу сигналов управления на закрытие клапанов приточной и вытяжной вентиляции, систем кондиционирования, отключения напряжения от технологического и электротехнического оборудования, силовых и контрольных кабелей от источников электроснабжения при пожаре на вводе в помещение;
- оповещение персонала, находящегося в помещениях ЦОДа, о возникновении пожара с помощью светозвуковых оповещателей;
- подачу сигнала для обеспечения подпора воздуха на путях эвакуации;
- последующее дымо- и газоудаление.

Согласно СП 485.1311500.2020 («Свод правил. Системы противопожарной защиты. Установки пожаротушения автоматические. Нормы и правила проектирования»), тип установки пожаротушения, способ тушения, вид огнетушащего вещества определяются организацией-проектировщиком с учетом пожарной опасности и физико-химических свойств производимых, хранимых и применяемых веществ и материалов, а также особенностей защищаемого оборудования.

Автоматические установки пожаротушения должны быть расположены в специальном выделенном помещении, доступ в которое строго регламентирован, или внутри защищаемых помещений.

При использовании газовых огнетушащих веществ (ГОТВ) в помещениях должна быть предусмотрена система газо- и дымоудаления для удаления ГОТВ после ликвидации пожара.

6.6. Система аварийного освещения

Система аварийного освещения предназначена для освещения серверного помещения при отказе основной системы электропитания. Электропитание системы должно осуществляться от распределительных щитов в составе системы бесперебойного электропитания (СБЭ) или от системы гарантированного электроснабжения (СГЭ).

Система эвакуационного освещения должна быть построена на базе светильников с автономными источниками питания (аккумуляторами) со временем автономной работы не менее 60 минут или запитана от СГЭ. Электропитание системы должно осуществляться от щитов СБЭ.

Должно быть предусмотрено наружное освещение комплекса зданий ЦОДа.

Должно также быть обеспечено локальное освещение в серверных помещениях и общих зонах (коридоры).

7. Системы и службы эксплуатации

Автоматизированная система диспетчеризации и управления (АСДУ) предназначена для автоматизации работы диспетчерской службы, специалистов служб поддержки и эксплуатации инженерных систем ЦОДа. Она должна обеспечивать возможность контроля работы оборудования основных инженерных систем и систем жизнеобеспечения, режимов их работы, возникновения аварийных ситуаций, температурно-влажностных режимов технологических помещений, фактов возникновения аварийных ситуаций. Должен также осуществляться сбор информации и отображение текущего состояния инженерных систем ЦОДа в режиме реального времени, хранение данных, обеспечиваться возможность их отображения и анализа (отчеты, графики, тренды) на автоматизированном рабочем месте (АРМ) диспетчера.

В АСДУ должна быть предусмотрена возможность введения пороговых значений для отслеживаемых параметров инженерных систем ЦОДа. Должна быть предусмотрена функция рассылки оповещений об аварийной ситуации (или о достижении отслеживаемыми характеристиками инженерных систем ЦОДа пороговых значений) посредством электронной почты и текстовых сообщений.

АСДУ должна обеспечивать функцию ведения журнала событий и текущих состояний и значений параметров (логов) работы контролируемых систем ЦОДа, а также защиту этих записей от несанкционированного изменения и удаления.

Требования к системам и службам эксплуатации ЦОДа приведены в табл. 7.1.

Табл. 7.1. Оснащение ЦОДа системами и службами эксплуатации

	Класс C	Класс B	Класс A
Наличие (функционирование) дежурной смены эксплуатационного персонала по всем ключевым инженерным системам ЦОДа	Круглосуточно. Допустимо в удаленном режиме	Круглосуточно. С присутствием на объекте	Круглосуточно. С присутствием на объекте
Наличие системы автоматического контроля параметров инженерного оборудования ЦОДа	Требуется	Требуется	Требуется
Наличие системы контроля параметров рабочей среды	Опция	В помещениях ЦОДа	В помещениях ЦОДа и снаружи в зонах установки внешних элементов инженерных систем

8. Порядок проведения технического аудита ЦОДов с целью определения их класса

1. Для обеспечения независимой оценки с целью определения классов центров обработки данных федеральный орган исполнительной власти в области связи определяет некоммерческую организацию, осуществляющую функции технического аудита ЦОДов.

2. Технический аудит проводится некоммерческой организацией, осуществляющей функции технического аудита ЦОДов, на основании договора, заключаемого такой некоммерческой организацией и оператором ЦОДа.

3. Технический аудит ЦОДа осуществляется по инициативе и за счет оператора соответствующего ЦОДа.

4. Для проведения технического аудита оператор ЦОДа направляет в некоммерческую организацию, осуществляющую функции технического аудита ЦОДов, письменное обращение с указанием перечисленных ниже сведений.

   4.1. Информация об операторе ЦОДа:

   - для юридического лица – наименование, адрес местонахождения, государственный регистрационный номер записи о создании юридического лица, а также номер телефона и (если имеется) адрес электронной почты;

   - для индивидуального предпринимателя – фамилия, имя и отчество (при наличии) индивидуального предпринимателя, адрес места жительства, государственный регистрационный номер записи о государственной регистрации индивидуального предпринимателя, а также номер телефона и (если имеется) адрес электронной почты.

   4.2. Информация о ЦОДе, подлежащем техническому аудиту: адрес, кадастровый номер объекта недвижимого имущества (здания, помещения, иного объекта, где расположен ЦОД), площадь, технологическая мощность (ресурс). Оператор ЦОДа вправе указать, какому классу соответствует ЦОД по мнению его оператора, и приложить информацию и документы, обосновывающие это мнение.

5. По истечении трех рабочих дней с момента получения обращения некоммерческая организация, осуществляющая функции технического аудита ЦОДов, подтверждает готовность заключить договор о проведении технического аудита ЦОДа и направляет оператору ЦОДа проект договора либо запрашивает дополнительную информацию, необходимую для подготовки проекта такого договора.
6. Некоммерческая организация, осуществляющая функции технического аудита ЦОДов, не вправе отказаться от заключения договора с оператором ЦОДа на проведение технического аудита. Отказ от заключения договора допускается исключительно в случаях, когда информация и документы, указанные в пункте 4 настоящего Порядка, не представлены либо представлены недостоверные сведения.
7. Технический аудит ЦОДа включает в себя комплексную проверку технических характеристик ЦОДа с целью его соотнесения с определенным классом, установленным Постановлением Правительства РФ от XXX N XXX «О классификации ЦОДов».
8. При проведении технического аудита ЦОДа ставятся следующие вопросы:

8.1. Соответствует ли ЦОД обязательным требованиям, предъявляемым к ЦОДам в Российской Федерации;

8.2. Какому классу соответствует проверяемый ЦОД по совокупности своих характеристик.

9. По результатам технического аудита ЦОДа некоммерческая организация, осуществляющая функции технического аудита ЦОДов, выдает мотивированное заключение, в котором указывается, к какому классу может быть отнесен исследуемый ЦОД.
10. Некоммерческая организация, осуществляющая функции технического аудита ЦОДов, вправе отказать в выдаче заключения по результатам технического аудита, если в результате нарушения оператором ЦОДа своих обязанностей по договору на проведение технического аудита ЦОДа некоммерческая организация, осуществляющая функции технического аудита ЦОДов, не имела возможности провести проверку всех характеристик, имеющих существенное значение для классификации ЦОДа.
11. Если это предусмотрено договором, заключенным некоммерческой организацией, осуществляющей функции технического аудита ЦОДов, с оператором ЦОДа, в отношении которого проводится технический аудит, некоммерческая организация, осуществляющая функции технического аудита, может выдать предварительное заключение с перечислением препятствий для отнесения ЦОДа к более высокому классу. В случае, если оператор ЦОДа готов обеспечить устранение указанных препятствий, по его заявлению технический аудит приостанавливается на период, который требуется оператору ЦОДа для устранения препятствий (но не более 12 месяцев). По заявлению оператора ЦОДа либо по истечении периода приостановления технического аудита ЦОДа такой технический аудит возобновляется, при этом повторной проверке (исследованию) подлежат те характеристики, которые указаны оператором ЦОДа как улучшенные.
12. Некоммерческая организация, осуществляющая функции технического аудита ЦОДов:

12.1. Разрабатывает и согласовывает с федеральным органом исполнительной власти в области связи методику технического аудита ЦОДов (включающую требования к составу и квалификации экспертов, привлекаемых к осуществлению технического аудита), форму договора на проведение технического аудита, порядок определения договорной стоимости технического аудита, форму заключения по результатам технического аудита;

12.2. Заключает договоры на проведение технического аудита ЦОДов, организует проведение технического аудита, в том числе с привлечением субподрядных организаций в случаях необходимости мероприятий, требующих специальных познаний и навыков в области техники и технологий, а также необходимости непосредственного обследования территориально удаленных объектов. Если некоммерческая организация, осуществляющая функции технического аудита ЦОДов, привлекает к проведению технического аудита субподрядные организации, указанным организациям не могут быть переданы функции по принятию решения об отнесении ЦОДа к определенному классу;

12.3. Осуществляет передачу в федеральный орган исполнительной власти в области связи сведений о выдаче заключения об отнесении ЦОДа к определенному классу по итогам технического аудита не позднее 7 дней с даты выдачи заключения;

12.4. Осуществляет деятельность по информированию операторов ЦОДов о состоянии правового регулирования ЦОДов, проводит очные и дистанционные мероприятия, направленные на повышение правовой и технической грамотности административных и технических работников ЦОДов.

13. Некоммерческая организация, осуществляющая функции технического аудита ЦОДов, вправе:

13.1. Самостоятельно в соответствии с принятой методикой формировать программу проведения технического аудита ЦОДа;

13.2. Исследовать в полном объеме техническую (проектную) документацию, связанную с устройством ЦОДа, а также проверять фактическое соответствие ЦОДа такой документации;

13.3. Направлять оператору ЦОДа запросы о предоставлении документов и информации, относящейся к характеристикам ЦОДа;

13.4. Совместно с оператором ЦОДа осуществлять испытания технологических систем ЦОДа с целью подтверждения их наличия и работоспособности в проектных параметрах;

13.5. Осуществлять иные права, предусмотренные законодательством, а также договором о проведении технического аудита ЦОДа.

14. Некоммерческая организация, осуществляющая функции технического аудита ЦОДов, обязана:

14.1. Обеспечивать объективность, всесторонность и полноту технического аудита ЦОДов, а также достоверность и обоснованность выводов, изложенных в заключении по результатам технического аудита;

14.2. По запросу оператора ЦОДа предоставить актуальную информацию о классификации ЦОДов, методике проведения технического аудита ЦОДа, условиях договора на проведение технического аудита, включая стоимость и сроки или порядок их определения;

14.3. Проводить технический аудит ЦОДа в соответствии с условиями заключенного договора на проведение технического аудита ЦОДа;

14.4. При проведении технического аудита ЦОДа руководствоваться согласованной с федеральным органом исполнительной власти в области связи методикой;

14.5. Своевременно передавать в федеральный орган исполнительной власти в области связи информацию о результатах технического аудита ЦОДов.

15. Оператор ЦОДа вправе:

15.1. Самостоятельно принимать решение о проведении технического аудита ЦОДа с целью его отнесения к определенному классу;

15.2. Требовать и получать от некоммерческой организации, осуществляющей функции технического аудита ЦОДов, информацию о классификации ЦОДов, методике проведения технического аудита ЦОДов, условиях договора на проведение технического аудита, включая стоимость и сроки или порядок их определения, а при проведении технического аудита – обоснования замечаний и выводов, которые были сделаны в ходе такого технического аудита;

15.3. По итогам проведения технического аудита получить заключение, указанное в пункте 9 настоящего Порядка.

16. Оператор ЦОДа обязан:

16.1. Содействовать некоммерческой организации, осуществляющей функции технического аудита ЦОДов, в своевременном и полном проведении технического аудита, создавать для этого соответствующие условия, предоставлять необходимую информацию и документацию, предоставить некоммерческой организации, осуществляющей функции технического аудита ЦОДов, возможность проведения испытаний технологических систем ЦОДа с целью подтверждения их наличия и работоспособности;

16.2. Не предпринимать каких бы то ни было действий, направленных на сужение круга вопросов, подлежащих выяснению при проведении технического аудита ЦОДа, а также на сокрытие (ограничение доступа) информации и документации, запрашиваемых некоммерческой организацией, осуществляющей функции технического аудита ЦОДов;

16.3. Своевременно оплачивать проведение технического аудита ЦОДа в соответствии с условиями соответствующего договора.

17. В качестве некоммерческой организации, осуществляющей функции технического аудита ЦОДов, может быть определена некоммерческая организация, соответствующая в совокупности следующим требованиям:

17.1. некоммерческая организация не основана на членстве;

17.2. в состав учредителей некоммерческой организации не входят иностранные граждане, иностранные организации или международные организации.

18. Сведения о некоммерческой организации, осуществляющей функции технического аудита ЦОДов (наименование, адрес местонахождения, адрес электронной почты, фамилия, имя и отчество (при наличии) руководителя), размещаются на сайте федерального органа исполнительной власти в области связи, в информационно-телекоммуникационной сети «Интернет».
19. Срок полномочий некоммерческой организации, осуществляющей функции технического аудита ЦОДов, составляет 10 лет.
20. Полномочия некоммерческой организации, осуществляющей функции технического аудита ЦОДов, могут быть прекращены на основании решения федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, досрочно по заявлению некоммерческой организации, осуществляющей функции технического аудита ЦОДов, а также в случае выявления несоответствия некоммерческой организации, осуществляющей функции технического аудита ЦОДов, требованиям, установленным пунктом 17 настоящего Порядка. Решение о прекращении полномочий некоммерческой организации, осуществляющей функции технического аудита ЦОДов, не позднее семи дней со дня его принятия направляется такой некоммерческой организации и размещается на сайте федерального органа исполнительной власти в области связи в информационно-телекоммуникационной сети «Интернет».
21. Со дня, следующего за днем опубликования на сайте федерального органа исполнительной власти в области связи в информационно-телекоммуникационной сети «Интернет» решения о прекращении полномочий некоммерческой организации, осуществляющей функции технического аудита ЦОДов,

некоммерческая организация, осуществляющая функции технического аудита центров обработки данных, полномочия которой прекращаются, не вправе заключать договоры на проведение технического аудита ЦОДов.

22. Некоммерческая организация, осуществляющая функции технического аудита ЦОДов, полномочия которой прекращаются, не позднее 7 дней с даты опубликования решения о прекращении ее полномочий на сайте федерального органа исполнительной власти в области связи в информационно-телекоммуникационной сети «Интернет», передает в федеральный орган исполнительной власти в области связи информацию о заключенных до даты опубликования на сайте федерального органа договорах на проведение технического аудита ЦОДов.
23. Некоммерческая организация, осуществляющая функции технического аудита ЦОДов, полномочия которой прекращены, вправе завершить технический аудит ЦОДов, договоры на проведение которых были заключены такой некоммерческой организацией в период до прекращения ее права на заключение таких договоров в соответствии с пунктом 21 настоящего Порядка.
24. В качестве экспертов для проведения технического аудита ЦОДа могут выступать лица, обладающие специальными знаниями в области функционирования ЦОДов и доказанным многолетним опытом по профилю экспертизы, при этом указанные лица не должны одновременно быть работниками (в том числе на основании гражданско-правового договора) оператора проверяемого ЦОДа.