



КООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

105082, Москва,
2-й Ирининский пер., 3

+7 (495) 150-6424

info@ano-dcc.ru

www.ano-dcc.ru

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
КООРДИНАЦИОННЫЙ СОВЕТ ПО
ЦЕНТРАМ ОБРАБОТКИ ДАННЫХ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ

(АНО КС ЦОД)

УДК 004.03, 004.9

Инв. № МЦОД-2026

«УТВЕРЖДАЮ»
Генеральный директор АНО КС ЦОД
Бедердинов Д.Р.
«26» февраля 2026 года



Научно-исследовательская работа проведена по инициативе АНО КС ЦОД.

Начало работы обязательной госрегистрации не подлежит

ОТЧЕТ

О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

ОТЕЧЕСТВЕННАЯ МОДЕЛЬ КЛАССИФИКАЦИИ ЦОДОВ

(редакция №2)

Руководитель работы

к.г.н.  Бедердинов Д.Р.

«26» февраля 2026 года

Москва, 2026 год

ИСПОЛНИТЕЛИ

Руководитель работы

Бедердинов Дмитрий Рифаитович, кандидат географических наук

Специалисты:

Барсков Александр Георгиевич

Важенин Максим Сергеевич

Вирцер Евгений Владимирович

Вышемирский Сергей Владимирович

Горкавенко Дмитрий Владимирович

Гургенидзе Георгий Редженович

Железнов Видия Александрович

Жиляев Василий Евгеньевич

Кашин Андрей Андреевич

Колмыкова Мария Владимировна

Колосков Евгений Юрьевич

Королев Константин Александрович

Курбатов Ренат Раисович

Мартынюк Александр Викторович, кандидат технических наук

Михеенко Василий Игоревич

Мищук Сергей Юрьевич

Нагорный Константин Дмитриевич

Панышев Дмитрий Олегович

Паршин Николай Сергеевич

Рубцов Сергей Васильевич

Тишкин Александр Викторович

Церулев Максим Владимирович

Чеснов Андрей Александрович

Чирков Тарас Александрович

Шеметов Николай Николаевич

РЕФЕРАТ

Отчет 24 с., 0 рис., 11 таблиц

Работа представляет собой актуализацию первой редакции работы «Отечественная модель классификации ЦОДов». Основанием указанной работы явилось создание первой в России перспективной отечественной системы классификации центров обработки данных (ЦОДов), призванной заполнить вакуум, связанный с отсутствием таких систем классификации и возникновением практических трудностей в использовании классификации стран Запада. С учетом внедрения понятия «ЦОД» в правовое поле, включением указанного понятия в закон «О связи», принятия Правительством РФ правил ведения реестра ЦОД возникла необходимость уточнить результаты ранней работы с целью их гармонизации с имеющимися нормативными правовыми актами.

Результат исследования ориентирован на применение владельцами центров обработки данных, разработчиками технических решений, пользователями (заказчиками услуг), провайдерами облачных услуг, а также заинтересованными государственными органами в качестве эталонной модели классификации, разработанной в России с участием компетентных экспертов и участников рынка ЦОДов.

Исследование выполняется по инициативе разработчика (АНО КС ЦОД), в рамках уставной деятельности по проведению мероприятий, направленных на развитие отечественной отрасли ЦОДов. Исследование выполняется за счет собственных средств АНО КС ЦОД. Бюджетного или договорного финансирования выполнения исследовательских работ не привлекается.

Исследование состоит из одного тома, в котором собраны все основные материалы отчета, таблицы и выводы. Приложения к отчету отсутствуют.

В ходе выполнения работы были исследованы имеющиеся иностранные системы классификации, а также проведены консультации (интервью) с ведущими операторами центров обработки данных Российской Федерации. Был проведен ряд мероприятий по обсуждению разрабатываемой модели классификации между рабочей группой, осуществившей разработку отчета, и профильными специалистами по эксплуатации центров обработки данных, в целях повышения уровня компетентности при выделении категорий.

При проведении исследования использовались методы текстологического анализа, интерполяции и экстраполяции данных.

При построении модели классификации использовались методы факторного и кластерного анализа.

В рамках выполнения исследовательской работы достигнуты следующие результаты:

- Создана модель классификации центров обработки данных применительно к их уровню готовности и физической защищенности и даются рекомендации по организации подобных объектов для обеспечения нужд государственных и частных компаний, использующих информационные системы разного уровня критичности.
- Проверены собственные гипотезы, а также гипотезы участников рынка о возможной значимости тех или иных факторов в контексте их влияния.

- Описаны различные факторы, имеющие значение для классификации, разработана шкала оценки в пределах указанных факторов.
- Разработаны предложения по организации ЦОДов для обеспечения нужд государственных и частных компаний, использующих информационные системы разного уровня критичности, с использованием созданной модели классификации.

В рамках исследования впервые предпринята попытка создать отечественную модель классификации центров обработки данных. В рамках второй редакции документа указанная модель гармонизирована с положениями нормативно-правовых актов и может быть использована в том числе для нужд ведения реестра ЦОД.

Результаты исследования могут быть применены любыми заинтересованными лицами для формирования потребительских классов центров обработки данных, а также применены государственными органами для подготовки нормативных актов, относящихся к регулированию деятельности центров обработки данных.

СОДЕРЖАНИЕ

1. Введение.....	6
1.2. Назначение документа.....	6
1.3. Перечень терминов и сокращений	6
1.4. Используемые нормативные и прочие документы	10
2. Основные положения и критерии соответствия	12
3. Система электроснабжения	14
3.1. Электроснабжение ЦОДа	14
3.2. Система внутреннего распределения электропитания ЦОДа.....	15
4. Система технологического охлаждения.....	16
5. Телекоммуникационная инфраструктура	17
6. Физическая безопасность.....	18
6.1. Общие требования к зданию, сооружению (помещениям) ЦОДа.....	18
6.2. Система контроля и управления доступом	20
6.3. Система охранной и тревожной сигнализации.....	21
6.4. Система видеонаблюдения	22
6.5. Система пожарной безопасности	23

Список таблиц:

Табл. 3.1. Требования к системе электроснабжения ЦОДа	14
Табл. 3.2. Требования к системе внутреннего распределения электропитания ЦОДа	15
Табл. 4.1. Требования к системе охлаждения ЦОДа	16
Табл. 5.1. Требования к телекоммуникационной инфраструктуре ЦОДа	17
Табл. 6.1. Требования к месту размещения и зданиям ЦОДа	19
Табл. 6.2. Требования к наличию отдельных вспомогательных технологических помещений в ЦОДе	19
Табл. 6.3. Оснащение ЦОДа системой контроля доступа	20
Табл. 6.4. Оснащение ЦОДа системой охранной сигнализации	22
Табл. 6.5. Оснащение ЦОДа системой видеонаблюдения	22
Табл. 6.6. Оснащение помещений ЦОДа системами сверхраннего обнаружения возгорания	23

1. Введение

Требования к надежности и физической защищенности – ключевые характеристики центров обработки данных, обеспечивающие необходимый уровень непрерывности работы информационных систем. Такие требования существенно влияют на применяемые в ЦОДах проектные, технические решения, а также на процессы эксплуатации и обслуживания ЦОДов.

1.2. Назначение документа

Настоящий документ разработан в целях определения класса центра обработки данных для включения этих сведений в реестр центров обработки данных в соответствии с Постановлением Правительства РФ от 28 ноября 2025 г. № 1932 («Об утверждении Правил формирования и ведения реестра центров обработки данных, расположенных на территории Российской Федерации»).

1.3. Перечень терминов и сокращений

Центр обработки данных (ЦОД) — совокупность зданий, частей зданий или помещений, объединенных единым назначением, включающих комплекс систем инженерно-технического обеспечения, спроектированных и используемых для размещения оборудования, обеспечивающего обработку и (или) хранение данных (из ФЗ «О внесении изменений в статьи 2 и 6 Федерального закона “О связи“»).

Технологическая площадка – территория, имеющая периметр безопасности, на которой расположено одно или несколько зданий (строений, сооружений) ЦОДа.

Выделенная территория – территория с границами, обозначенными ограждением (объектами искусственного происхождения) и оборудованными средствами безопасности, на которой расположено одно или несколько зданий (строений, сооружений) ЦОДа, эксплуатируемых одним оператором.

Технологические помещения ЦОДа – помещения с оборудованием и системами, относящимися к технологическому циклу ЦОДа и обеспечивающими его физическую безопасность.

Машинный зал (машзал) – специализированное технологическое помещение в ЦОДе со специально созданными и поддерживаемыми условиями для размещения и функционирования оборудования, обеспечивающего обработку и (или) хранение данных.

ИТ-оборудование – оборудование, обеспечивающее обработку и (или) хранение данных.

ИТ – информационные технологии.

Зона ЦОДа – совокупность помещений и (или) выделенных системой ограждающих конструкций частей помещений для размещения и функционирования инженерно-технических, коммуникационных систем ЦОДа, а также оборудования, обеспечивающего обработку и (или) хранение данных.

Отказ – событие, заключающееся в нарушении работоспособного состояния объекта (ГОСТ Р 27.102-2021).

Отказоустойчивость – возможность непрерывной работы информационных систем 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). Резервирование предполагает определенную избыточность компонентов объекта, что дает возможность использовать их при отказе какого-либо базового компонента — без прерывания работы объекта в целом. Базовую модель резервирования описывают формулой $N + R$, где N (от англ. Normal) — число элементов, необходимых для нормальной работы, а R (от англ. Redundant) — число избыточных компонентов.

Технологическая мощность – величина, характеризующая способность ЦОДа разместить оборудование, обеспечивающее обработку и хранение данных, и зависящая от технических возможностей систем инженерно-технического обеспечения, которая определяется электрической мощностью, подведенной и доступной непосредственно для электропитания оборудования, обеспечивающего обработку и хранение данных, измеряемой в киловаттах (кВт).

Независимый источник электроэнергии — это источник, который не имеет общих точек отказа с другим источником (другими источниками) и обеспечивает подачу электроэнергии с регламентированными характеристиками при ее исчезновении на другом источнике (других источниках).

Локальная система генерации – комплекс вырабатывающего электроэнергию оборудования, расположенного в месте нахождения потребителя или ближе к потребителю, чем генерирующие объекты централизованного энергоснабжения.

Номинальная мощность стойки – максимальная мощность, потребляемая стойкой в любом режиме.

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, технологического охлаждения, связи и управления, комплекс систем безопасности.

ИТ-инфраструктура – комплекс систем и их оборудования, обеспечивающий функционирование информационных систем.

Основные инженерные системы – инженерные системы, отключение которых приведет к нарушению функционирования оборудования ИТ-инфраструктуры; к таким системам относят, в частности, системы электроснабжения и технологического охлаждения.

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.

Критически важная нагрузка – оборудование, система, элемент системы или иной объект, отключение которых приведет к остановке выполнения функций ЦОДа.

Система технологического охлаждения — инженерная система, которая отводит тепло от оборудования или технологического процесса и поддерживает температуру в диапазоне, необходимом для нормальной работы техники.

Нормальный режим работы – стандартная ситуация, при которой оборудование работает с расчетными параметрами.

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 помещениях с критически важными нагрузками ЦОДа при переходе с основных на резервные источники электроснабжения и обратно.

Система вентиляции – комплекс функционально связанных между собой оборудования, установок, устройств, воздухопроводов, 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.

Активное оборудование (компоненты) системы электроснабжения — устройства, выполняющие преобразование и/или регулирование параметров электрической энергии, управляющие режимами работы и обеспечивающие бесперебойность/резервирование питания.

Пассивное оборудование (компоненты) системы электроснабжения — элементы, обеспечивающие распределение и передачу электроэнергии без преобразования ее параметров.

Активное оборудование (компоненты) системы охлаждения — оборудование, обеспечивающее получение холода и/или принудительную циркуляцию воздуха/теплоносителя и автоматическое регулирование параметров микроклимата за счет энергопотребляющих узлов (компрессор, вентилятор, насос, электроприводы).

Пассивное оборудование (компоненты) системы охлаждения — элементы системы, предназначенные для транспортировки и распределения воздуха/теплоносителя и не содержащие энергопотребляющих узлов.

Помещение узла взаимной коммутации (Meet-Me-Room) – выделенное место в пределах ЦОДа, где расположено оборудование телекоммуникационных компаний (провайдеров), а также осуществляется коммутация и, при необходимости, обмен трафиком.

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).

ЗИП – набор запасных частей, инструментов, принадлежностей и расходных материалов, необходимых для функционирования, технического обслуживания и ремонта.

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

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) – помещение узла взаимной коммутации.

1.4. Используемые нормативные и прочие документы

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

- Федеральный закон № 244-ФЗ «О внесении изменений в статьи 2 и 6 Федерального закона “О связи”»
- Федеральный закон № 116-ФЗ «О промышленной безопасности опасных производственных объектов»
- Федеральный закон № 123-ФЗ «Технический регламент о требованиях пожарной безопасности»
- Постановление Правительства РФ от 28 ноября 2025 г. № 1932 «Об утверждении Правил формирования и ведения реестра центров обработки данных, расположенных на территории Российской Федерации»
- Постановление Правительства РФ № 390 «О противопожарном режиме» (с изменениями на 7 марта 2019 г.)
- Постановление Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСБ № 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».
- «Правила устройства электроустановок» (ПУЭ), версия 7
- Национальный 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»
- Национальный стандарт ГОСТ Р 27.102-2021. «Надежность в технике»
- Национальный 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»
- Национальный стандарт ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний»
- 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»
- Свод правил СП 20.13330.2016 «Свод правил. Нагрузки и воздействия. Актуализированная редакция СНиП 2.01.07-85» (ред. от 28.01.2019)

2. Основные положения и критерии соответствия

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.

Классификация ЦОДов:

- Класс А (Высший);
- Класс В (Средний);
- Класс С (Базовый);
- Класс D (Минимальный)

Данные уровни надежности различаются по подходам к организации (архитектуре) и резервированию основных инженерных систем, а также по степени физической защищенности ЦОДов, их оснащению противопожарными системами, по общим характеристикам здания ЦОДа, места его расположения, организации линий связи.

Для Класса А основным принципом реализации инженерной архитектуры является отказоустойчивость, понимаемая как возможность непрерывной работы информационных систем на базе данного ЦОДа при единичном отказе любого компонента основных инженерных систем.

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

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

В ЦОДах Класса D допускается использование компонентов инженерной инфраструктуры без резервирования.

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 технологического охлаждения, элементы контуров охлаждения, соответствует минимальным требованиям для данного класса, приведенным в разделе 4 («Система технологического охлаждения»).
- 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, а также организация физической, в том числе пожарной, безопасности

ЦОДа соответствуют минимальным требованиям для данного класса, приведенным в разделе 6 «Физическая безопасность».

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 – одна из основных инженерных систем, которая должна быть организована таким образом, чтобы минимизировать или устранить риски отключения его потребителей.

В общем случае построение системы электроснабжения ЦОДа зависит от характера внешнего электроснабжения объекта, наличия собственных источников генерации электроэнергии на объекте, а также от архитектуры применяемой системы распределения электропитания на объекте.

3.1. Электроснабжение ЦОДа

Система электроснабжения для ЦОДа должна предусматривать наличие нескольких источников электроснабжения, в качестве которых могут выступать внешние источники электроснабжения, локальные источники генерации электроэнергии, используемые ЦОДом, или любая их комбинация, в соответствии с требованиями, приведенными в табл. 3.1. Для повышения надежности следует обеспечить территориальное разнесение линий электропередачи от любых из этих источников. 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 электроснабжения 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 бесхозным 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.

Табл. 3.1. Требования к системе электроснабжения ЦОДа

Характеристика	Класс D	Класс C	Класс B	Класс A
Минимальное число источников электроэнергии	Два	Два независимых	Два независимых	Два независимых
Автоматическое переключение между источниками электроснабжения	Не требуется	Требуется	Требуется	Требуется
Автоматический запуск локальной генераторной установки (при наличии)	Не требуется	Требуется	Требуется	Требуется
Мин. запас топлива локальной генераторной установки (при наличии), в часах работы	2	2	4	12
Разделение групп электроприемников, относящихся к системам ЦОДа, и групп электроприемников сторонних организаций, вынесение электрических нагрузок ЦОДа на отдельные центры питания (трансформаторные подстанции/группы, секции/системы шин РУ, РП, генераторные установки)	Не требуется	Не требуется	Требуется	Требуется

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.

Электропитание критически важных нагрузок должно осуществляться от системы бесперебойного питания, имеющей достаточный уровень резервирования (табл. 3.2).

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.

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

Табл. 3.2. Требования к системе внутреннего распределения электропитания ЦОДа

Характеристика	Класс D	Класс C	Класс B	Класс A
Минимальный уровень резервирования для компонентов системы электропитания	N	N+1 для всех активных компонентов	N+1 для любого компонента	N для любого компонента после любого отказа
Минимальное число контуров распределения электропитания	Один	Один	Два активных	Два активных
Техническая возможность подключения оконечного ИТ-оборудования одновременно к двум независимым линиям электропитания	Не требуется	Не требуется	Требуется	Требуется
Особые требования по физическому размещению компонентов системы электропитания	Нет	Нет	Нет	Секционирование всех компонентов по числу резервных элементов для каждой секции*

*Секционирование в рамках машзала не обязательно

4. Система технологического охлаждения

Система технологического охлаждения (далее система охлаждения) ЦОДа – одна из основных его инженерных систем, обеспечивает необходимые климатические параметры в его помещениях, оказывает критически важное влияние на работоспособность установленного в нем оборудования.

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 охлаждения ЦОДа могут быть организованы различным образом, при условии соблюдения требований, приведенных в табл. 4.1.

При проектировании системы охлаждения необходимо предусматривать обеспечение необходимого климатического режима эксплуатации для всех критически важных нагрузок, а также для иного инженерного технологического оборудования, чувствительного к среде эксплуатации, такого как ИБП, аккумуляторные батареи, компоненты системы пожарной безопасности и пр. С целью обеспечить необходимый климатический режим эксплуатации следует руководствоваться требованиями производителя оборудования 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.

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

Необходимо предусмотреть возможность контроля температурного и влажностного режима для всех критически важных нагрузок ЦОДа, если они требуют контроля данных показателей.

Табл. 4.1. Требования к системе охлаждения ЦОДа

Характеристика	Класс D	Класс C	Класс B	Класс A
Минимальный уровень резервирования для компонентов систем охлаждения	N	N+1 для всех активных компонентов	N+1 для любого компонента	N для любого компонента после любого отказа
Минимальное число путей подачи теплоносителя системы охлаждения (при наличии таковых)	Один	Один	Два	Два (авария на одном из контуров не должна приводить к нарушению работоспособности системы охлаждения)
Непрерывное охлаждение	Не требуется	Не требуется	Не требуется	Требуется
Особые требования по физическому размещению компонентов системы охлаждения	Не требуется	Не требуется	Не допускается прокладка транзитных трубопроводов в пределах машзала или над ним	Требования к классу B, дополнительно требование секционирования всех компонентов по числу резервных элементов для каждой секции

5. Телекоммуникационная инфраструктура

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, MMR) внутри ЦОДа и обеспечение возможности прокладки линий связи к ним от вводных колодцев различными маршрутами внутри здания ЦОДа.

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

Требования к телекоммуникационной инфраструктуре ЦОДа приведены в табл. 5.1.

Табл. 5.1. Требования к телекоммуникационной инфраструктуре ЦОДа

Характеристика	Класс D	Класс C	Класс B	Класс A
Минимальное число независимых трасс ВОЛС (иных линий связи, при невозможности прокладки ВОЛС)	Одна	Одна	Две, допустима прокладка единым маршрутом	Две, различными непересекающимися маршрутами
Минимальное число точек размещения телекоммуникационного оборудования внутри здания ЦОДа	Одна	Одна	Одна	Две
Минимальное число телекоммуникационных вводов в здание (на технологическую площадку) и минимальное расстояние между ними (если применимо)	Один	Один	Один (в случае нескольких вводов расстояние между ними не менее 20 м)	Два, с расстоянием между вводами не менее 20 м
Прокладка линий связи внутри здания от телекоммуникационных вводов до точек размещения телекоммуникационного оборудования разными непересекающимися маршрутами	Не требуется	Не требуется	Не требуется	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 следует учитывать риски, связанные с возникновением природных или техногенных катастроф, а также степень подверженности влиянию следующих негативных факторов:

- зона сейсмической активности ;
- 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;
- экстремальные значения температурных минимумов и максимумов;
- высокий уровень относительной влажности воздуха;
- значительная (более 1500 м) высота территории 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 и зданиям и помещениям ЦОДа приведены в табл. 6.1 и 6.2.

Табл. 6.1. Требования к месту размещения и зданиям ЦОДа

Характеристика	Класс D	Класс C	Класс B	Класс A
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), 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 (комплексе зданий/сооружений)
Обособленность объекта	Здание/комплекс зданий и сооружений ЦОДа может располагаться на общей территории.	Здание/комплекс зданий и сооружений ЦОДа может располагаться на общей территории.	Здание/комплекс зданий и сооружений ЦОДа может располагаться на общей территории.	Здание/комплекс зданий и сооружений ЦОДа располагается на выделенной территории.
Транзитные коммуникации	Через общую территорию 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	Через общую территорию 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	Через общую территорию 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	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. Требования к наличию отдельных вспомогательных технологических помещений в ЦОДе

Назначение отдельного помещения	Класс D	Класс C	Класс B	Класс A
Распаковка, хранение, тестирование и настройка ИТ-оборудования	Не требуется	Не требуется	Не требуется	Требуется
Диспетчерский центр инженерных систем ЦОДа (в пределах технологической площадки)	Не требуется	Не требуется	Требуется	Требуется
Хранение ЗИП (в пределах технологической площадки)	Не требуется	Не требуется	Не требуется	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;
- установка турникетов для контроля прохода на технологическую площадку, в здание или помещение ЦОДа;
- оборудование окон помещений, расположенных на первых и (или) последних этажах зданий, а также окон, находящихся около пожарных лестниц и других мест, откуда в помещения могут проникнуть посторонние лица, 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. Оснащение ЦОДа системой контроля доступа

Объект	Класс D	Класс C	Класс B	Класс A
Машзалы, иные технологические помещения и оборудование ЦОДа	Требуется	Требуется	Требуется	Требуется
Подходы к зданию и входы в здание ЦОДа	Не требуется	Не требуется	Требуется	Требуется
Периметр технологической площадки ЦОДа	Не требуется	Не требуется	Не требуется	Требуется

Система СКУД должна включать следующие средства:

- контроля пребывания сотрудников и посетителей на технологической площадке 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 беспрепятственно покинуть помещения 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 машзалов ЦОДа. Такие индивидуальные пространства, реализуемые в виде клеток, 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) технологической площадки от проникновения в круглосуточном режиме;
- защиту периметра здания (двери, окна, каналы, люки и пр. размером более 150x150 мм);
- защиту периметра и внутренних объемов помещений 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 D	Класс C	Класс B	Класс A
Машзалы (зоны для размещения оборудования, обеспечивающего обработку и (или) хранение	Требуется	Требуется	Требуется	Требуется

данных)				
Иные технологические помещения ЦОДа	Требуется	Требуется	Требуется	Требуется
Окна и двери	Требуется	Требуется	Требуется	Требуется
Подходы к зданию	Не требуется	Не требуется	Требуется	Требуется
Периметр технологической площадки	Не требуется	Не требуется	Не требуется	Требуется

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, выполнявших различные действия. Требования к такой системе приведены в табл. 6.5.

Табл. 6.5. Оснащение ЦОДа системой видеонаблюдения

Объект	Класс D	Класс C	Класс B	Класс A
Машзалы (зоны для размещения оборудования, обеспечивающего обработку и (или) хранение данных)	Требуется*	Требуется*	Требуется*	Требуется*
Подходы к машзалам	Не требуется	Не требуется	Требуется	Требуется
Иные технологические помещения	Не требуется	Не требуется	Требуется	Требуется
Центральный и запасной входы	Требуется	Требуется	Требуется	Требуется
Посты охраны, КПП	Требуется при наличии поста охраны	Требуется при наличии поста охраны	Требуется	Требуется
Подходы и подъезды к зданию, парковки	Не требуется	Не требуется	Требуется	Требуется
Зоны установки внешних блоков инженерных систем	Требуется	Требуется	Требуется	Требуется

Периметр технологической площадки	Не требуется	Не требуется	Не требуется	Требуется
--	--------------	--------------	--------------	-----------

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

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 видеoinформации, который устанавливается в защищенном помещении (или машзале 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 № 123-ФЗ «Технический регламент о требованиях пожарной безопасности», а также специализированным сводам правил и ГОСТам по пожарной безопасности.

Здания, сооружения и помещения ЦОДа оснащаются 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 автоматическими установками пожаротушения и системами пожарной сигнализации») и СП 3.13130.2009 («Свод правил. Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре»).

Отказ от оснащения объекта автоматическими установками пожаротушения (АУПТ) возможен при наличии соответствующего СТУ (специальные технические условия) – документа, разрешающего эксплуатировать объект без АУПТ с учетом его конструктивных, архитектурных и других особенностей.

Требования к оснащению ЦОДа системами сверххранного обнаружения возгорания приведены в табл. 6.6.

Табл. 6.6. Оснащение помещений ЦОДа системами сверххранного обнаружения возгорания

	Класс D	Класс C	Класс B	Класс A
Система сверххранного обнаружения	На усмотрение проектировщика	На усмотрение проектировщика	На усмотрение проектировщика	В машзалах обязательно

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);
- выдачу сигналов управления на закрытие клапанов приточной и вытяжной вентиляции, систем кондиционирования;
- 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.