

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

ТРЕБОВАНИЯ К ДАТАЦЕНТРАМ. ИНФРАСТРУКТУРА И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

O'ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
HAZORAT.H. ABUOF.ILYOSHOV
AXBOROT TEXNOLOGIYALARI
JAMIY SHARH BOY-BOYLARI

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр развития и внедрения компьютерных и информационных технологий UZINFOCOM (ГУП Центр UZINFOCOM)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи, информатизации и телекоммуникационных технологий № 7

3 ПРИНЯТ Постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 05.12.2014 № 05-592

4 Настоящий стандарт разработан с учетом требований ANSI/TIA-942-A-2012 Telecommunications Infrastructure Standard for Data Centers (Телекоммуникационная инфраструктура центров обработки данных)

5 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

Содержание

1 Область применения.....	1
2 Нормативные ссылки.....	1
3 Термины, определения и сокращения.....	2
4 Проектирование.....	4
5 Инфраструктура кабельных систем.....	7
6 Требования и структура телекоммуникационных пространств.....	8
7 Кабельные системы датацентров.....	28
8 Кабельные каналы, фальшполы и потолочные лотки.....	33
9 Избыточность (резервирование) инфраструктуры, систем, провайдеров доступа.....	35
10 Обеспечение информационной безопасности.....	39
Приложение А (справочное) Выбор местонахождения и проектов зданий для датацентров.....	59
Приложение В (справочное) Примеры проектов датацентров.....	62
Приложение С (справочное) Площади для датацентров.....	67
Приложение D (справочное) Уровни инфраструктуры датацентров.....	68
Приложение E (справочное) Проектирование кабельной системы.....	107
Приложение F (справочное) Согласование проектов датацентров с поставщиками (провайдерами) услуг и доступа.....	115
Приложение G (справочное) Согласование планов размещения оборудования с персоналом, обслуживающим датацентры.....	121
Библиография	122

O'ZSTANDART AGENTLIGA
 STANDARTLARNI TAYYARLASH VA
 MAZKURAT K. DAVLAT QURILMALARIGA
 AHBOROT TEXNOLOGIYALARINI
 JORIY ETISH BO'YICHA MAS'ALALARI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологиялари ДАТАЦЕНТРАЛАР УЧУН ТАЛАБ. ИНФРАТУЗИЛМА ВА АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ

Информационная технология ТРЕБОВАНИЯ К ДАТАЦЕНТРАМ. ИНФРАСТРУКТУРА И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Information technology. Datacenters requirements.
Infrastructure and ensuring of information security

Дата введения 11.12.2014

1 Область применения

Настоящий стандарт устанавливает требования по проектированию и монтажу датацентров, включая планировку помещения, технологическую структуру, с учетом требований по обеспечению информационной безопасности.

Настоящий стандарт предназначен для применения всеми хозяйствующими субъектами, имеющими датацентр или принимающими участие в разработке проектной документации на строительство датацентра.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

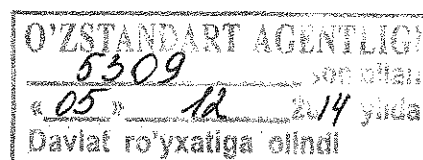
O'z DSt 1047:2003 Информационные технологии. Термины и определения

O'z DSt 1059:2010 Техника пожарная. Огнетушители переносные. Общие технические требования. Методы контроля

O'z DSt 2141:2011 Волоконно-оптические системы передачи. Термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов на территории Узбекистана по соответствующему указателю стандартов, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Издание официальное



3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по О'z DSt 1047, О'z DSt 2141, а также следующие термины с соответствующими определениями:

3.1.1 **главная распределительная зона:** Пространство в датацентре, где расположена основная (главная) коммутационная панель.

3.1.2 **горизонтальная распределительная зона:** Пространство в датацентре, где расположена горизонтальная коммутационная панель.

3.1.3 **датацентр:** Специализированное здание (площадка) для размещения серверного и коммуникационного оборудования и подключения к каналам сети Интернет.

3.1.4 **кабелепровод:** Трасса или структура, предназначенная или используемая для прокладки и монтажа телекоммуникационных кабелей.

3.1.5 **кабельный канал:** Устройство для размещения кабеля связи.

3.1.6 **коробка для кабелепротяжки:** Полость (коробка, кожух), устроенная на отрезке кабельного канала для размещения провода или кабеля.

3.1.7 **магистраль:** Устройство (например, кабельный канал, кабель или постоянное соединение) для прокладки кабельной подсистемы 2 и кабельной подсистемы 3.

3.1.8 **модульный разъем:** Телекоммуникационный разъем с направляющим ключом или без него, имеющий контактные либо бесконтактные позиции.

3.1.9 **перемычка:** Сборка (жгут) из проводов «витая пара» без соединителей (разъемов), используемая для соединения линий связи на кросс-панели.

3.1.10 **провайдер доступа:** Оператор любого устройства, используемого для передачи сигналов связи к помещению пользователя и обратно.

3.1.11 **промежуточная распределительная зона:** Пространство в датацентре, где расположена промежуточная коммутационная панель.

3.1.12 **прямое соединение:** Схема соединения, при которой используется соединительная арматура (кабельные оконцеватели) для непосредственного соединения кабеля с кабелем, без шнура переключения или перемычки.

3.1.13 **соединительная арматура:** Устройство, обеспечивающее механическое оконцевание кабеля (кабельный оконцеватель).

3.1.14 **сплайс:** Соединение проводников, предполагаемое постоянным.

3.1.15 **среда передачи:** Провод, кабель, проводники, радиорелейные линии, используемые для связи.

3.1.16 инфраструктура телекоммуникаций: Совокупность компонентов системы связи, исключая оборудование (аппаратуру), которые совместно обеспечивают базовую поддержку распределения всей информации в здании.

3.1.17 телекоммуникационное помещение: Помещение и пространство, предназначенное для размещения распределительных пунктов, соединительного и телекоммуникационного активного оборудования.

3.1.18 точка разграничения: Точка, где меняется операционное управление или право собственности.

3.1.19 фальшпол: Система, состоящая из полностью съёмных и взаимозаменяемых плиток пола, опирающихся на регулируемые стойки или стрингеры (либо и на то, и на другое) и открывающих доступ к пространству под полом.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

ИБП - источник бесперебойного питания;

ЛВС - локальная вычислительная сеть;

ОВиК - отопление, вентиляция и кондиционирование;

СУБД - система управления базами данных;

СКУД - система контроля управления доступом;

ССХД - сеть системы хранения данных;

BNC (Bayonet Neill Concelman) - коаксиальный радиочастотный разъём;

CEPT (Conference of European Post and Telecommunications) - Европейская конференция администраций почтовых служб и служб связи;

DS (Digital Signal) – цифровой сигнал;

DSX (Digital Signal Cross-Connect) - кроссирование цифровых сигналов;

FDDI (Fiber Distributed Data Interface) - волоконно-оптический интерфейс передачи данных;

FTP (File Transfer Protocol) - протокол передачи файлов;

HIPS (Host-based Intrusion Prevention System) - система предотвращения вторжений для отдельных хостов;

HTTP (Hyper Text Transfer Protocol) - протокол передачи гипертекста;

IDC (Insulation Displacement Connector) - разъём, смещающий изоляцию;

IDS (Intrusion Detection System) - система обнаружения вторжений;

IMAP (Internet Message Access Protocol) - протокол прикладного уровня для доступа к электронной почте;

IP (Internet Protocol) - межсетевой протокол;

IPS (Intrusion Prevention System) - система предотвращения вторжений;

ISDN (Integrated Services Digital Network) - цифровая сеть с интеграцией служб;

KVM (Keyboard, Video, Mouse) - клавиатура, видео, мышь;

OSI (Open Systems Interconnection) - взаимодействие открытых систем;

PDU (Power Distribution Unit) - распределитель питания;

POP3 (Post Office Protocol Version 3) - протокол почтового отделения, версия 3;

SMB (Server Message Block) - сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия;

SMTP (Simple Mail Transfer Protocol) - простой протокол передачи почты;

SONET (Synchronous Optical Network) - синхронная оптическая сеть;

SPAN (Switch Port Analyzer) - возможность коммутатора зеркалирования трафик определенного порта или несколько портов;

SSL (Secure Sockets Layer) - уровень защищённых сокетов;

STM (Synchronous Transport Module) - синхронный транспортный модуль;

VPN (Virtual Private Network) - виртуальная частная сеть.

4 Проектирование

4.1 Общие положения

Описанные ниже этапы процесса проектирования относятся к проекту нового датацентра или расширению существующего. Проект телекоммуникационной кабельной системы, план размещения оборудования по этажам, планы электропроводки, архитектурная планировка, системы отопления/вентиляции/кондиционирования, безопасности, освещения должны быть координированы между собой. Данный процесс должен выглядеть так:

а) примерно оценивают требования к телекоммуникациям, пространству, энергоснабжению и охлаждению датацентра при его работе с полной нагрузкой. Предположительно оценивают будущие тенденции развития телекоммуникаций, роста энергопотребления и необходимости в охлаждении за весь срок жизни датацентра;

б) предъявляют архитекторам и инженерам требования к пространству, электропитанию, охлаждению, нагрузкам на этажные перекрытия, заземлению, электрозащите и др. Предусматривают требования для операционного центра, погрузочной платформы, складских помещений, подготовительной зоны и других подсобных пространств;

с) координируют предварительные планы расположения датацентра, полученные от архитектора и инженеров. При необходимости предлагают изменения;

д) разрабатывают поэтажные планы размещения аппаратуры, включающие в себя расположение главных помещений и пространств под комнаты ввода, главных распределительных зон, промежуточных распределительных зон, горизонтальных распределительных зон, места зонного распределения и аппаратные. Сообщают инженерам-строителям ожидаемую потребность в электропитании, охлаждении, требования к нагрузке на перекрытия от аппаратуры. Предусматривают требования к кабелепроводам для телекоммуникаций;

е) получают от инженеров обновлённый план, где указаны кабелепроводы, электрооборудование и механическое оборудование, добавленное к поэтажным планам датацентра из расчёта его работы с полной загрузкой;

ф) проектируют телекоммуникационную кабельную систему, исходя из потребностей оборудования, которое установлено или подлежит установке в датацентре.

Информационная безопасность датацентров обеспечивается путем выполнения требований нормативно-правовых актов и государственных стандартов Республики Узбекистан по информационной безопасности.

Дополнительная информация о факторах, учитываемых при проектировании датацентра, приведена в приложении А.

Примеры проектов датацентра приведены в приложении В.

4.2 Взаимосвязи помещений датацентра и прочих площадей здания

На рисунке 1 показаны основные помещения типичного датацентра, их взаимосвязи друг с другом и с помещениями, расположенными вне датацентра. Сведения, касающиеся зон размещения телекоммуникаций внутри датацентра, приведены в разделе 5.

Настоящий стандарт регламентирует инфраструктуру телекоммуникаций для помещений датацентра, которыми являются серверная и соответствующие подсобные пространства.

Дополнительные требования к площади для датацентра приведены в приложении С.

ЎЗБЕКИСТАН АГЕНЛИГИ
STANDARTLAR VA TEX. QANUNLARI
HISOBAT VA TADQIQOT BOSHQARMASI
Axborot-Tekhnika Markazi
DSTU 2875:2014

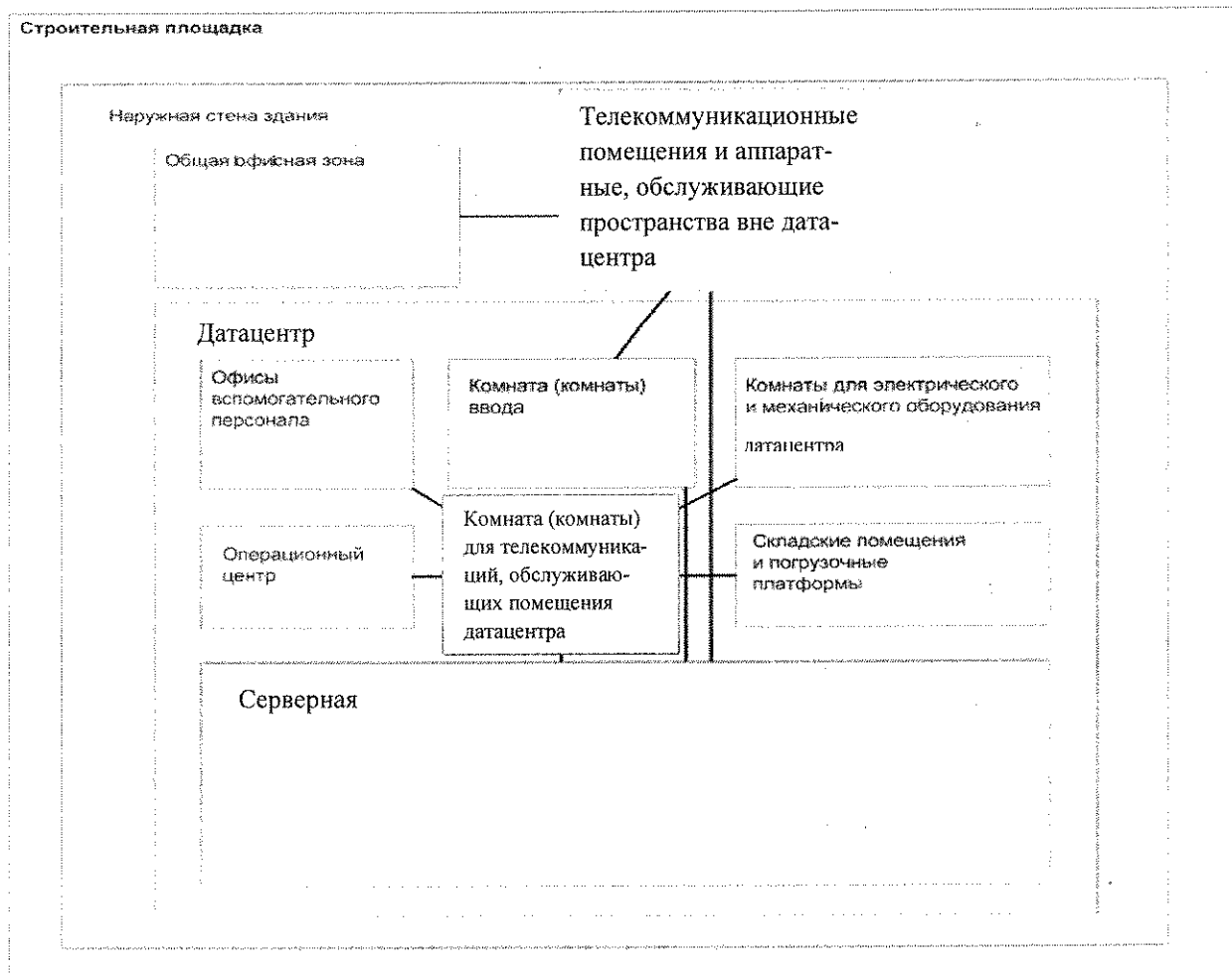


Рисунок 1 - Взаимосвязи между помещениями в датацентре

4.3 Уровни

Настоящий стандарт содержит сведения о четырёх уровнях, относящихся к разной степени готовности и обеспечения безопасности инфраструктуры средств телекоммуникаций датацентра. Более высокие уровни соответствуют более высокой степени готовности и защищённости. Подробные сведения для каждого из четырёх уровней приведены в приложении D.

4.4 Привлечение профессионалов

Проектируемые датацентры должны будут работать с большим числом вычислительного и оборудования телекоммуникаций. Поэтому с самого начала проекта следует привлекать к участию в нём профессионалов и спецификаторов (описателей) по телекоммуникациям и информационным технологиям. Кроме требований к пространствам, микроклимату, смежности и рабочим характеристикам компьютерного и оборудования телекоммуникаций, в проектах датацентров необходимо учитывать требования к

телекоммуникационным кабелепроводам и пространствам, предписанные настоящим стандартом.

5 Инфраструктура кабельных систем

На рисунке 2 изображена представительная модель, в которой различные функциональные элементы составляют кабельную систему для некоего датацентра. Модель определяет взаимосвязи между этими элементами и показывает, как они конфигурируются для создания общей системы. Базовыми элементами кабельной системы датацентра являются:

- a) горизонтальная кабельная система (кабельная подсистема 1 - пункт 7.1);
- b) магистраль (кабельная подсистема 2 и кабельная подсистема 3 - подпункт 7.2);
- c) коммутационная панель в комнате ввода или главной распределительной зоне (распределитель С, распределитель В или распределитель А);
- d) основная (главная) коммутационная панель в главной распределительной зоне (распределитель С, распределитель В или распределитель А);
- e) необязательные промежуточные кросс-панели в промежуточной распределительной зоне или главной распределительной зоне;
- f) горизонтальная коммутационная панель в телекоммуникационном помещении, горизонтальной распределительной зоне или главной распределительной зоне (распределитель С, распределитель В или распределитель А);
- g) консолидационная точка в месте зонного распределения (необязательно);
- h) розетка в аппаратной или в месте зонного распределения.

O'ZSTANDART AGENTLIGA
 STANDARTLASH, TEX. RAJLAT
 NAZORAT VA QURILMASTIRISH VA
 AQBOQOT TEXNOLOGIYALARI
 JORIY ETISH BOSHQARMASI

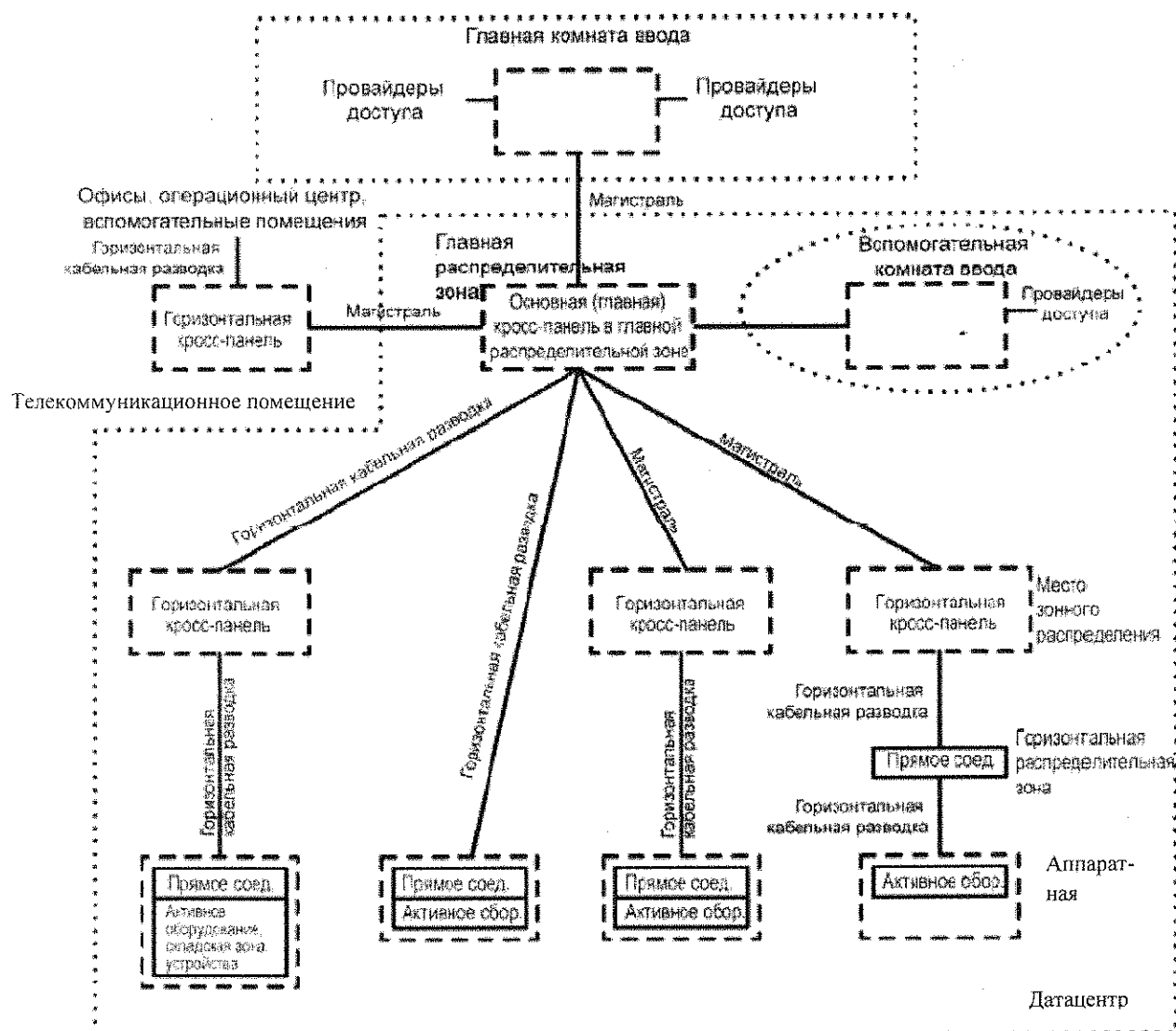


Рисунок 2 - Топология датацентра

6 Требования и структура телекоммуникационных пространств

6.1 Общие положения

В датацентре должны быть места, специально выделенные для поддержки инфраструктуры телекоммуникаций. Эти места должны поддерживать кабельную систему и аппаратуру телекоммуникаций. В типовом случае в пределах датацентра обычно имеются: комната ввода, главная распределительная зона, промежуточная распределительная зона, горизонтальная распределительная зона, место зонного распределения и аппаратная. В зависимости от размеров датацентра не все эти зоны могут использоваться в структуре. Эти зоны могут иметь, а могут и не иметь стен либо иных ограждений для отделения их от других пространств серверной.

UZBEKISTAN RESPUBLICA
STATESTANDARDS AUTHORITY, DAYLAT
MAGISTRAL: HUROFICOLASHTIRISH TA
AKHBOZOT TEXNOLOGIYALARI
2014 YIL 07 AY 01 KUNIGI

6.2 Структура датацентра

6.2.1 Основные элементы

К телекоммуникационным зонам датацентра относятся: комната ввода, главная распределительная зона, промежуточная распределительная зона, горизонтальная распределительная зона, место зонного распределения и аппаратная. Комната ввода – это место, используемое для сопряжения структурированной кабельной системы датацентра и междомовых кабелей, как принадлежащих провайдеру доступа, так и потребителю. В этом месте находятся принадлежащие провайдеру разграничительная арматура и оборудование. Комната ввода может располагаться вне серверной, если датацентр размещён в здании, где находятся офисы общего назначения или помещения, не входящие в пределы датацентра. Комната ввода может быть расположена вне серверной также из соображений повышения безопасности, т.к. в этом случае исключается необходимость впуска в серверную обслуживающего персонала провайдера доступа. Датацентры могут иметь не одну, а несколько комнат ввода, с целью обеспечения дополнительного резервирования или для того, чтобы избежать превышения максимальной длины участков кабеля, идущего к проводке, предусмотренной провайдером.

Комната ввода сопрягается с серверной через главную распределительную зону. Комната ввода может располагаться рядом с главной распределительной зоной или может быть объединена с ней.

Главная распределительная зона содержит основную (главную) коммутационную панель, которая является центральным пунктом распределения структурированной кабельной системы и может содержать горизонтальную коммутационную панель, когда аппаратные обслуживаются прямо из главной распределительной зоны. Это место находится внутри серверной; в многопользовательских датацентрах оно может располагаться в специально выделенной комнате из соображений безопасности. Каждый датацентр должен иметь хотя бы одну главную распределительную зону. Центральный маршрутизатор, центральный коммутатор ЛВС, центральный коммутатор ССХД, а также учрежденческую автоматическую телефонную станцию часто размещают в главной распределительной зоне, поскольку это место является ядром кабельной инфраструктуры датацентра. Принадлежащее провайдеру доступа подготовительное оборудование (например, мультиплексоры M13) также часто располагается в главной распределительной зоне, а не в комнате ввода, это исключает необходимость выделять вторую комнату ввода из-за ограничений, накладываемых на длину контура.

Главная распределительная зона может обслуживать одну или несколько горизонтальных распределительных зон или аппаратных в пределах датацентра и одну или несколько телекоммуникационных помещений, расположенных вне датацентра и предназначенных для поддержки вспомо-

могательных офисных комнат, операционного центра и других вспомогательных помещений.

Горизонтальная распределительная зона используется для обслуживания аппаратных в тех случаях, когда горизонтальная коммутационная панель не находится в главной распределительной зоне. Поэтому, когда она используется, горизонтальная распределительная зона может включать в себя горизонтальную коммутационную панель, которая является центральным распределительным пунктом для кабельной системы к аппаратным. Горизонтальная распределительная зона находится внутри серверной, но может располагаться в специально выделенной комнате внутри серверной с целью обеспечения дополнительной безопасности. В горизонтальной распределительной зоне обычно находятся коммутаторы локальных сетей, коммутаторы ССХД, а также KVM-коммутаторы для окончного оборудования, размещённого в аппаратных. Датацентр может содержать части серверной, находящиеся на нескольких этажах, причём каждый этаж обслуживается своей собственной горизонтальной коммутационной панелью. Небольшие датацентры могут не нуждаться в горизонтальной распределительной зоне, поскольку всю серверную в целом сможет обслуживать главная распределительная зона. Однако типичный датацентр будет иметь несколько горизонтальных распределительных зон.

Допускается иметь в горизонтальной кабельной системе опциональную точку прямого соединения, которая называется местом зонного распределения. Это место располагается между зоной горизонтального распределения и аппаратной, что позволяет часто осуществлять реконфигурацию и повышает гибкость системы.

6.2.2 Типовая топология датацентра

Типовой датацентр содержит одну комнату ввода внешних сервисов, возможно, одну или несколько телекоммуникационных помещений, одну главную распределительную зону и несколько горизонтальных распределительных зон. Топология такого датацентра представлена на рисунке 3.

STANDART ASENTLIG
STANDARTLASHUVICH, TUVLET
KIZIRATIM! KUYUGIOLASHUVICHKA
AKHOBOT TEXNOLOGIYALARIGI
JOSIY ETISH BOSQARMAQ!

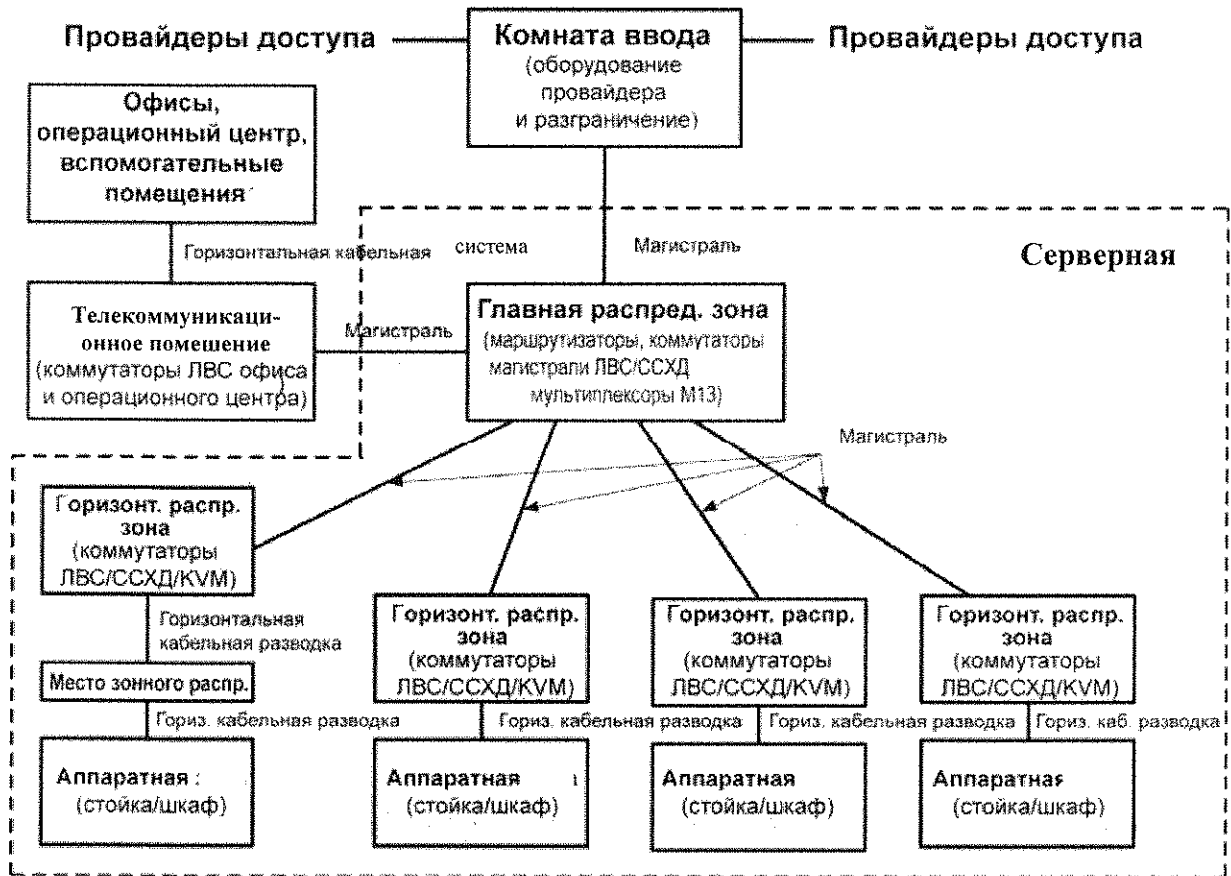


Рисунок 3 - Пример базовой топологии датацентра

6.2.3 Редуцированные топологии датацентров

Проектировщики датацентра могут консолидировать основную (главную) коммутационную панель и горизонтальную коммутационную панель в единую главную распределительную зону, возможно, совсем небольшую – один шкаф или одну стойку. Телекоммуникационное помещение и комната ввода могут быть также объединены с главной распределительной зоной, в этом случае будет датацентр с редуцированной топологией. Такая топология для небольшого датацентра приведена на рисунке 4.

6. STANDART AGENTURA
 STANDART AGENTURA, PAVLAT
 NAZAROV, PAVLAT AGENTURA
 AGENTURA AGENTURA AGENTURA
 AGENTURA AGENTURA AGENTURA
 AGENTURA AGENTURA AGENTURA

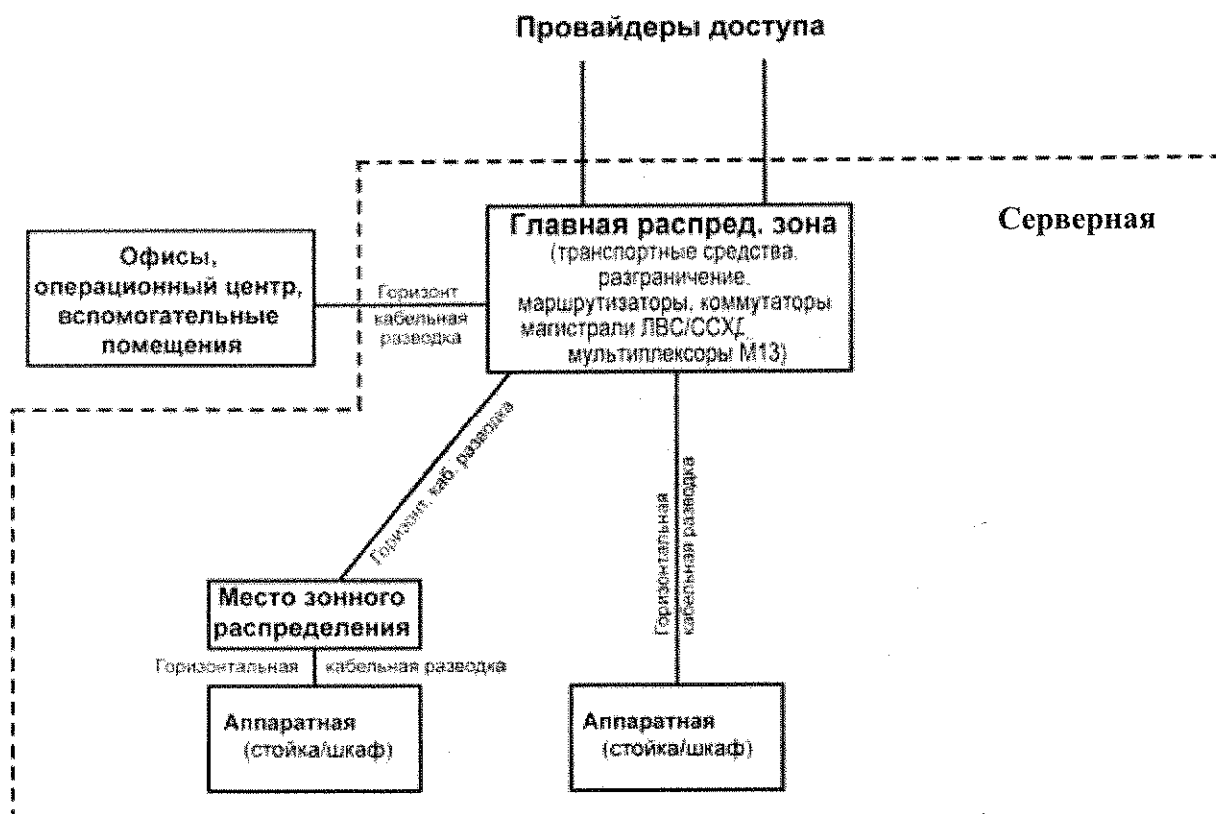


Рисунок 4 - Пример редуцированной топологии датацентра

6.2.4 Датацентры с распределённой топологией

Для больших датацентров, расположенных на нескольких этажах или в нескольких комнатах, потребуются промежуточные кросс-соединения, расположенные в промежуточной распределительной зоне. На каждом этаже или в каждой комнате может быть одна или несколько промежуточных распределительных зон.

Датацентрам с большими по площади или далеко разнесёнными друг от друга офисными и вспомогательными помещениями могут понадобиться несколько телекоммуникационных помещений.

Дистанционные ограничения (на длину участка кабеля) могут потребовать устройства нескольких комнат ввода для очень крупных датацентров. Топология датацентра с несколькими комнатами ввода показана на рисунке 5. Главная комната ввода не должна иметь прямых соединений с горизонтальными распределительными зонами.

Наличие кабельной системы от вспомогательной комнаты ввода непосредственно к горизонтальным распределительным зонам в некоторых случаях допустимо с тем, чтобы удовлетворить некоторым требованиям ограничения длины линии и необходимого резервирования.

Составитель: А.А.А.А.
 Стадия: Проектная
 Издатель: Издательство
 Адрес: 1234567890
 Дата: 01.01.2014



Рисунок 5 - Пример распределённой топологии датацентра с несколькими комнатами

6.3 Требования к серверной

6.3.1 Выбор помещения серверной

Выбор помещения серверной производится на основании следующих положений:

- серверную рекомендуется располагать в помещении, не имеющем внешних стен здания;
- в помещении серверной должно быть достаточно места для беспрепятственной установки, эксплуатации и технического обслуживания основного оборудования, средств поддержки вычислительной техники, носителей данных, а также свободного перемещения обслуживающего персонала;
- несущие конструкции здания в помещении серверной, где планируется к размещению оборудование, должны выдерживать расчетную нагрузку, включающую вес компьютерного и оборудования телекоммуникаций, оборудования систем инфраструктуры, а также свободного перемещения обслуживающего персонала.

ВВЕДЕНИЕ
ОБЩИЕ ПОЛОЖЕНИЯ
ТРЕБОВАНИЯ К ПОМЕЩЕНИЮ
ТРЕБОВАНИЯ К ЭЛЕКТРОСНАБЖЕНИЮ
ТРЕБОВАНИЯ К ВОЗДУХООЧИЩЕНИЮ
ТРЕБОВАНИЯ К ВОЗДУХОПОДАВАНИЮ
ТРЕБОВАНИЯ К ВОЗДУХОУВЛАЖНЕНИЮ
ТРЕБОВАНИЯ К ВОЗДУХОПОДАВАНИЮ
ТРЕБОВАНИЯ К ВОЗДУХОУВЛАЖНЕНИЮ
ТРЕБОВАНИЯ К ВОЗДУХОПОДАВАНИЮ
ТРЕБОВАНИЯ К ВОЗДУХОУВЛАЖНЕНИЮ

6.3.2 Требования к дверным проемам и окнам

Помещение должно быть, по возможности, без оконных проемов с глухими стенами. В помещении серверной, а также на пути транспортировки оборудования ширина дверей должна быть не менее 910 mm.

6.3.3 Требования к отделке помещения

К отделке помещений серверной предъявляются следующие требования:

- в серверной, при необходимости, рекомендуется установка фальшпола;
- просвет между фальшполом и фальшпотолком должен быть не менее 2500 mm;
- расстояние между строительным полом и фальшполом должно быть не менее 300 mm (рекомендуемое 400 mm);
- крутизна устанавливаемого на входе в серверную пандуса не должна превышать значение 1:10;
- конструкция фальшпола должна выдерживать расчетные нагрузки и состоять из легкоъемных модулей (плиток). При этом необходимо учитывать то, что отдельные устройства вычислительной системы могут создавать точечную нагрузку на пол до 455 kg;
- материал покрытия пола должен иметь электрическое сопротивление относительно земли от 1,0 MΩ (минимум) до 20 MΩ (максимум) при изменениях относительной влажности от 20% до 60% и температуры от +18°C до +24°C, а также обладать повышенной износостойкостью, низкой возгораемостью, повышенной стойкостью к царапанью. В серверной запрещается использование ковровых покрытий;
- поверхности под фальшполом должны окрашиваться или герметизироваться для предотвращения отслаивания и пыления штукатурки или бетона перекрытия;
- в строительном перекрытии под фальшполом необходимо сделать дренаж для оттока воды в случае аварийного протекания.

6.3.4 Требования при прокладке коммуникаций в помещении серверной

При прокладке коммуникаций в помещении серверной не должно проходить никаких магистралей и ответвлений инженерных систем, включая общую хозяйственную канализацию, холодное и горячее водоснабжение, общую вентиляцию и кондиционирование, распределительную сеть электропитания и освещение и другие слаботочные системы, за исключением технологических систем, располагаемых в самой серверной.

ЎЎЎЎЎЎЎЎЎЎЎЎЎЎ
ЎЎЎЎЎЎЎЎЎЎЎЎЎЎ
ЎЎЎЎЎЎЎЎЎЎЎЎЎЎ
ЎЎЎЎЎЎЎЎЎЎЎЎЎЎ
ЎЎЎЎЎЎЎЎЎЎЎЎЎЎ
ЎЎЎЎЎЎЎЎЎЎЎЎЎЎ

6.3.5 Система электропитания, освещения и заземления

6.3.5.1 Подсистема гарантированного электропитания

Подсистема гарантированного электропитания предусматривает наличие двух вводов электропитания от разных электрических подстанций и одну автоматическую дизельную электростанцию. Все три источника электроэнергии подаются на автоматический ввод резерва, осуществляющий автоматическое переключение фидеров при пропадании электропитания на основной (резервный) фидер.

Параметры линий электропитания, автоматической дизельной электростанции и автоматического ввода резерва определяются исходя из суммарной потребляемой мощности оборудования и подсистем серверной и должны обеспечивать не менее 10% запаса по мощности.

Линии внешнего электропитания должны быть выполнены по пятипроводной схеме с жилами неравного сечения.

6.3.5.2 Подсистема бесперебойного электропитания

Подсистема бесперебойного электропитания предусматривает электроснабжение оборудования и систем серверной через ИБП.

Мощность и конфигурация ИБП рассчитываются с учетом всего запитываемого оборудования и запаса для будущего развития.

Время автономной работы от ИБП рассчитывается с учетом потребностей, а также с учетом необходимого времени для перехода на резервные линии, автоматическую дизельную электростанцию и обратно.

ИБП серверной должен иметь 100% резерв в виде второго аналогичного ИБП.

Каждый ИБП должен обеспечивать не менее 30% запаса по мощности для развития оборудования серверной.

6.3.5.3 Подсистема распределения электропитания по потребителям

Подсистема распределения электропитания по потребителям включает в себя распределительные щиты серверной и линии питания до потребителей.

Основные требования к подсистеме:

- все потребители электропитания разбиваются на группы, чтобы обеспечить возможность проводить работы без отключения общего электропитания;

- каждая группа должна иметь свою автоматическую защиту сети;

- потребители могут иметь свою отдельную автоматическую защиту сети. К каждой стойке с оборудованием (телекоммуникационному шкафу) подводится два кабеля питания, по одному от двух ИБП (основного и резервного);

- внутри стоек (шкафов) устанавливаются модули распределения питания для оборудования стойки;

- все соединения без использования стандартных розеток производятся в распределительных щитах, расположенных в помещении серверной;

- кабели питания по серверной прокладываются в металлических лотках в полостях фальшпола/фальшпотолка.

Подсистема технологического заземления серверной выполняется отдельно от защитного заземления здания.

Сопротивление технологического заземления должно быть менее 1Ω .

Присоединение технологического заземления к защитному заземлению здания производится непосредственно у защитных электродов, расположенных в грунте.

Все металлические части и конструкции серверной должны быть заземлены. Каждый шкаф (стойка) с оборудованием заземляется отдельным проводником.

Несварные металлические конструкции серверной должны иметь заземляющие шайбы в болтовых соединениях, улучшающие электрический контакт между частями конструкции.

6.3.5.4 Подсистема электрического освещения

Освещенность помещения серверной должна быть не менее 500 lx на высоте 1 m от уровня пола.

Для освещения серверной допустимо применять обычные или галогенные лампы накаливания. Применение газоразрядных ламп недопустимо из-за наличия электромагнитных помех при их работе.

Питание подсистемы электрического освещения осуществляется от системы гарантированного электропитания серверной.

6.3.6 Система обеспечения микроклимата

Основные требования к подсистеме кондиционирования и вентиляции:

а) в помещении серверной должны соблюдаться следующие климатические условия:

- температура воздуха в помещении: $18-24^{\circ}\text{C}$;
- допустимые отклонения температуры: $\pm 2^{\circ}\text{C}$;
- относительная влажность воздуха: $40-50\%$;
- точность поддержания влажности: $\pm 1\%$;

б) фактическая холодильная мощность системы кондиционирования воздуха должна превышать суммарное тепловыделение всего оборудования и систем, размещенного в помещении серверной;

в) система кондиционирования воздуха серверной выполняется с использованием 100% резервирования (минимум два независимых кондиционера, каждый способен самостоятельно обеспечить температурный режим помещения);

Q. STANDART AGENTLARI

STANDARTLASHTIRISH, DAVLAT

STANDARTLASHTIRISH VA

d) система кондиционирования должна обеспечивать возможность удаленного мониторинга;

e) для помещения серверной необходим приток свежего воздуха с обеспечением фильтрации (класс EU4) и подогревом поступающего воздуха (в зимний период). Причем давление в помещении должно быть положительным относительно давления в остальных помещениях здания;

f) на воздуховодах приточной и вытяжной вентиляций необходимо устанавливать защитные клапаны, управляемые автоматикой установки газового пожаротушения;

g) необходимо предусмотреть отключение систем кондиционирования и приточно-вытяжной вентиляции по сигналу пожарной сигнализации и пожаротушения;

h) электропитание кондиционеров серверной должно осуществляться от подсистемы бесперебойного электропитания.

Основные требования к подсистеме:

a) система контроля параметров предназначена для контроля климатических и других параметров в серверных шкафах и телекоммуникационных стойках. В каждом шкафу устанавливаются датчики для контроля следующих параметров:

- температура воздуха;
- запыленность воздуха;
- скорость потока воздуха;
- задымленность воздуха;
- открытие/ закрытие дверей шкафов;

b) данная подсистема осуществляет оперативный температурный контроль внутри шкафов и управляет климатическим оборудованием для надежного отвода рассеиваемой мощности.

6.3.7 Система организации оборудования и кабельного хозяйства

6.3.7.1 Подсистема телекоммуникационных шкафов и стоек

Все оборудование серверной размещается в закрытых шкафах или открытых стойках. Количество стоек (шкафов) определяется исходя из имеющегося оборудования и его типоразмеров, способов монтажа.

Для улучшения температурного режима размещение шкафов (стоек) организуют рядами, с образованием «горячих» и «холодных» коридоров.

Промежутки между шкафами не допускаются.

Для удобства монтажа оборудования и прокладки кабелей проходы между рядами шкафов или стоек не должны быть слишком узкими. Расстояние между передними сторонами стоек или шкафов (соседних рядов) - 1,2 m, а минимальное - 0,9 m. Расстояние между задними сторонами стоек или шкафов (опять же соседних рядов) должно составлять 0,9 m, а минимальное - 0,6 m.

Размещать ряды стоек или шкафов нужно так, чтобы можно было снимать плиты фальшпола спереди и сзади ряда. Таким образом, все шка-

фы следует выравнивать вдоль краев плит фальшпола. Чтобы резьбовые стержни, которыми монтажные стойки крепятся к межэтажным перекрытиям, не попадали на крепежные элементы плит фальшпола, стойки устанавливаются ближе к центру этих плит.

Распределение оборудования по шкафам (стойкам) осуществляется с учетом совместимости (возможного взаимного влияния), оптимального распределения потребляемой мощности (а значит и тепловыделения), оптимальности коммуникаций, габаритов и массы оборудования.

Закрытые шкафы, в отличие от стоек, позволяют организовать дополнительные ограничения на доступ к оборудованию. Доступ внутрь таких шкафов может осуществляться с использованием подсистемы контроля доступа.

Закрытые шкафы нуждаются в дополнительных мерах по обеспечению требуемого температурного режима. Для этого применяются дополнительные вентиляторы, встраиваемые системы охлаждения, модули отвода горячего воздуха.

6.3.7.2 Подсистема организации коммуникаций

Все коммуникационные кабели внутри серверной должны быть организованы в лотки, проложенные в нишах фальшпола или фальшпотолка.

Лотки силовых и слаботочных кабелей должны быть разнесены на расстояние до 500 mm. Допускается пересечение трасс под углом 90 градусов.

Вводные каналы в телекоммуникационные шкафы и стойки должны обеспечивать свободную протяжку требуемого количества кабелей вместе с оконечными разъемами.

Коэффициент заполнения кабельных каналов и закладных не должен превышать от 50 % до 60%.

Внутри стоек и шкафов необходимо использовать кабельные организаторы, предотвращающие свешивание лишней длины кабеля.

Для упрощения коммуникаций и исключения поломки разъемов оборудования необходимо применять патч-панели.

Все кабели, кроссовые коммуникации и патч-панели должны иметь маркировку, позволяющую однозначно идентифицировать каждый кабель (разъем, порт).

6.4 Требования к комнате ввода

6.4.1 Общие положения

Комната ввода представляет собой пространство, предпочтительно выполненное в виде отдельной комнаты, в которой оборудование, принадлежащее провайдеру доступа, сопрягается с кабельной системой датацентра. Здесь обычно находится аппаратура провайдера и именно здесь про-

вайдеры доступа обычно передают линии связи пользователю. Эта точка передачи называется точкой разграничения.

В комнате ввода будут находиться внешние кабельные каналы, защитные блоки для медных внешних кабелей, оборудование провайдера доступа и терминирующее оборудование для кабельной системы, идущей к серверной.

6.4.2 Местоположение

Комнату ввода следует размещать таким образом, чтобы длина линий от точки разграничения с провайдером доступа до окончного оборудования не превышала максимально допустимого значения. Максимальная длина включает в себя весь путь кабеля, в том числе шнуры переключения и разность высот между перекрытиями и в пределах стоек или шкафов. Конкретные значения длины линии (от точки разграничения до окончного оборудования) для учёта при планировании размещения комнаты ввода приведены в приложении Е.

Примечание - Для линий, превышающих значения длины, указанные в приложении Е, можно использовать повторители (репитеры).

Комнаты ввода могут быть расположены как внутри, так и вне серверной. Из соображений безопасности комнаты ввода следует размещать вне серверной во избежание допуска техников провайдера в серверную. Однако, в крупных датацентрах из-за ограничений по длине линий, возможно размещение комнаты ввода в серверной.

Для кабельной системы в комнатах ввода следует использовать такую же кабельную систему (верхнего расположения или подпольную), что и в серверной; это позволит минимизировать длину кабелей, поскольку исключит переход от кабельных лотков верхнего расположения к подпольным кабельным лоткам.

6.4.3 Число комнат ввода

Для крупных датацентров могут потребоваться несколько комнат ввода с целью обслуживания линий некоторых типов при их прохождении через пространство серверной и/или с целью обеспечения дополнительного резервирования.

Вспомогательные комнаты ввода могут иметь свои собственные кабелепроводы для линий специального назначения от провайдера доступа или же могут быть вторичными по отношению к главной комнате ввода, в этом случае подающие кабели от провайдера подводятся сюда из главной комнаты ввода.

6.4.4 Прокладка внешнего кабельного канала под фальшполом

Если комната ввода расположена на территории серверной, то внешний кабельный канал следует размещать так, чтобы он не пересекался с воздушным потоком, трубопроводом охлаждённой воды и с другими кабелями, проложенными под фальшполом.

6.4.5 Помещения провайдера доступа и поставщика услуг

Помещения провайдера доступа и поставщика услуг для датацентра обычно находятся либо в комнате ввода, либо в серверной.

Помещения провайдера доступа и поставщика услуг в комнате ввода датацентра обычно не требуют перегородок, поскольку доступ в комнату ввода датацентра тщательно контролируется. Однако, провайдер доступа и поставщик услуг, которые арендуют площадь в серверной, обычно требуют безопасного доступа к своим помещениям.

6.4.6 Архитектурный проект

6.4.6.1 Общие положения

При выборе для ввода внешних сервисов закрытого помещения или открытой зоны следует исходить из соображений безопасности (учитывая при этом как санкционированный, так и случайный доступ), необходимости установки настенных предохранительных устройств, размеров комнаты/пространства ввода и физического местоположения.

6.4.6.2 Размеры

Размеры комнаты необходимо выбирать с учетом существующих и предполагаемых максимальных требований к:

- пространству возле задней панели и рамы для оконцевания кабелей провайдера доступа и кампусных кабелей;
- стойкам провайдера доступа;
- принадлежащей пользователю аппаратуре, которую нужно разместить в комнате ввода;
- разграничительным стойкам вместе с оконцевателями для кабельной системы, идущей к серверной;
- кабельным каналам.

Требуемая площадь в большей степени зависит от числа провайдеров доступа, количества и типа линий, терминируемых в этой комнате, чем от размеров датацентра.

Для определения первоначальных и перспективных требований к площадям, необходимо согласовать данный вопрос с провайдерами доступа и персоналом, обслуживающим датацентры. В приложении F приведены сведения о координации и разграничении с провайдерами доступа. В приложении G приведены сведения по согласованию планов размещения оборудования с персоналом, обслуживающим датацентры.

Следует также предусмотреть место для кабелей кампусной системы. Кабели, содержащие металлические элементы (кабели с медными парами, коаксиальные кабели, оптические кабели с металлическими компонентами), должны терминироваться с предохранителями в комнате ввода. Эти предохранители могут быть как настенного, так и рамного монтажа. Место установки предохранителей должно находиться как можно ближе к точке ввода кабелей в здание. Допускается терминировать кампусные оптические

ские кабели в основной (главной) кросс-панели, а не в комнате ввода, если они не содержат металлических компонентов (например, оболочка кабеля или несущий элемент).

6.4.6.3 Фанерные задние панели

В тех помещениях, где должны быть предусмотрены настенные оконцеватели для предохранителей, стены следует облицевать жёстко закреплёнными фанерными листами толщиной 19 mm, высотой 2,4 m, предпочтительно из непористой фанеры, способной выдержать прикреплённую к ней соединительную арматуру. Фанера должна быть огнестойкой или покрытой в два слоя огнезащитной краской.

Если огнестойкую фанеру будут красить, то не следует закрашивать штамп, подтверждающий огнестойкость, пока не закончится проверка, проводимая пожарной инспекцией. Чтобы уменьшить коробление, огнестойкая фанера должна быть высушена в печи с тем, чтобы её влажность не превышала 15%.

6.4.6.4 Освещение

Должна быть обеспечена освещённость не менее 500 lx в горизонтальной плоскости и 200 lx в вертикальной плоскости, при измерениях на высоте 1 m над чистым полом в середине всех проходов между шкафами.

Осветительные приборы не следует запитывать от тех же распределительных щитов питания, что и оборудование телекоммуникаций в серверной. Не следует применять выключатели с реостатами для регулирования света ламп. Аварийное освещение и надписи (знаки, символы) должны быть размещены в надлежащих местах таким образом, чтобы отсутствие основного освещения не помешало найти аварийный выход.

6.4.6.5 Двери

Двери должны быть шириной не менее 1 m и высотой не менее 2,13 m, без порогов, они должны быть или открывающимися наружу, или раздвигающимися в стороны (сдвижными), или съёмными. Двери должны быть снабжены замком и либо не иметь центральной стойки, либо иметь съёмную центральную стойку, чтобы облегчить доставку крупногабаритного оборудования.

6.4.6.6 Надписи, знаки, символы

Надписи (знаки, символы) следует размещать в соответствии с планом обеспечения безопасности здания.

6.4.7 Система противопожарной защиты

Системы противопожарной защиты и ручные огнетушители должны соответствовать требованиям O'z DSt 1059. В серверных следует устанавливать спринклерные системы предупреждающего действия.

6.4.8 Проникновение воды

В местах, где существует риск проникновения воды, должны быть предусмотрены меры по удалению воды из данного места (например, спусковое отверстие в полу). Любые водопроводные и сливные трубы, которые проходят через комнату, следует располагать в удалении от оборудования и не прямо над ним.

6.5 Главная распределительная зона

6.5.1 Общие положения

Главная распределительная зона – это центральное место, где находится точка распределения для структурированной кабельной системы в датацентре. Датацентр должен иметь, по крайней мере, одну главную распределительную зону. Центральные маршрутизаторы и центральные коммутаторы сетей датацентров зачастую размещают в главной распределительной зоне или вблизи неё.

В датацентрах, используемых несколькими организациями, например датацентрах, где хранятся базы данных Интернета или практикуется совместное размещение оборудования, главную распределительную зону следует располагать в безопасном месте.

6.5.2 Местоположение

Для главной распределительной зоны следует выбрать центральное расположение, чтобы не выйти за пределы дистанционных ограничений для поддерживаемых приложений, в том числе не превысить максимально допустимую длину участков кабелей для линий провайдера доступа, обслуживаемых из комнаты ввода.

6.5.3 Требования к помещению

Если главная распределительная зона находится в закрытом помещении, необходимо предусмотреть возможность выделения специально для этой зоны собственной системы ОВиК, отдельного распределительного щита питания и силовых панелей со своим ИБП.

Если главная распределительная зона имеет собственную систему ОВиК, то линии регулирования температуры для кондиционеров следует питать и контролировать с того же распределительного щита или панели питания, которые обслуживают аппаратуру телекоммуникаций, установленную в главной распределительной зоне.

Требования к архитектурному проекту, механическому и электрическому оборудованию главной распределительной зоны совпадают с требованиями к проекту серверной.

SECRET
STRATEGIC INFORMATION, TAYLOR
NATIONAL INTELLIGENCE SECURITY
AGENCY
1997 RELEASE UNDER E.O. 13526

6.6 Промежуточная распределительная зона

6.6.1 Общие положения

Промежуточная распределительная зона - это пространство, которое поддерживает промежуточный кросс. Он может быть использован, для того чтобы обеспечить второй уровень кабельной подсистемы (кабельная подсистема 2) в слишком больших датацентрах, в которых недостаточно размещения только кабельной подсистемы 3 и кабельной подсистемы 1.

6.6.2 Расположение

Промежуточная распределительная зона должна быть расположена централизованно, чтобы избежать превышения максимальной длины кабеля для схем провайдеров доступа, обслуживаемых вне комнаты ввода.

6.6.3 Требования к помещению

Требования к помещению такие же, что и для помещения горизонтальной распределительной зоны (6.7.3).

6.7 Горизонтальная распределительная зона

6.7.1 Общие положения

Горизонтальная распределительная зона - это пространство, которое поддерживает кабельную систему, идущую к аппаратной. В этой же зоне обычно располагаются коммутаторы локальных сетей, коммутаторы ССХД, пульт управления, а также KVM-коммутаторы, которые поддерживают оконечное оборудование. Главная распределительная зона может выполнять функции горизонтальной распределительной зоны для близко расположенного оборудования или даже для всей серверной, если серверная невелика.

На каждом этаже должна быть, по крайней мере, одна горизонтальная распределительная зона. Для поддержки оборудования, находящегося за пределами ограничений, накладываемых на длину горизонтального кабеля, могут потребоваться дополнительные горизонтальные распределительные зоны.

Максимальное число подключений к одной горизонтальной распределительной зоне следует выбирать исходя из возможностей кабельных лотков, с учётом свободного места, оставляемого в лотках для разводки кабелей в будущем.

В датацентрах, используемых несколькими организациями, например датацентрах, где хранятся базы данных Интернета или практикуется совместное размещение оборудования, горизонтальную распределительную зону следует располагать в безопасном месте.

6.7.2 Местоположение

Горизонтальные распределительные зоны следует располагать так, чтобы не выйти за пределы ограничений на максимальную длину магистральных кабелей, идущих от главной распределительной зоны, и на максимальное расстояние для среды передачи данного типа.

6.7.3 Требования к помещению

Если горизонтальная распределительная зона находится в закрытом помещении, следует рассмотреть возможность выделения специально для этой зоны собственной системы ОВиК, отдельных распределительных щитов питания и силовых панелей со своим ИБП.

Линии регулирования температуры и кондиционеры следует питать и контролировать с иных распределительных щитов питания или панелей, чем те, которые обслуживают аппаратуру телекоммуникаций, установленную в горизонтальной распределительной зоне.

Требования к архитектурному проекту, механическому и электрическому оборудованию горизонтальной распределительной зоны совпадают с требованиями к проекту серверной.

6.8 Место зонного распределения

Место зонного распределения следует ограничивать обслуживанием не более 288 соединений коаксиальных или медных кабелей во избежание скопления кабелей, особенно в полостях, которые будут задействованы над фальшпотолками или под плитками фальшпола с размерами 600 mm x 600 mm.

В местах зонного распределения не допускается использовать соединения типа кроссконнект. В пределах одного участка горизонтального кабеля допускается использовать только одно место зонного распределения.

В месте зонного распределения не допускается размещать активное оборудование, за исключением силового оборудования постоянного тока.

6.9 Аппаратные

Аппаратные – это места, выделенные для окончного оборудования, в том числе для компьютерных систем и аппаратуры телекоммуникаций.

Оконечное оборудование – это обычно оборудование напольной установки или оборудование, монтируемое в шкафах или стойках.

Горизонтальные кабели терминируются в аппаратных на оконцевателях, смонтированных в шкафах или стойках. Для каждого шкафа или стойки с оборудованием необходимо предусмотреть достаточное число сетевых розеток и оконцевателей, с тем, чтобы минимизировать длину шнуров переключения и шнуров питания.

Между единицами оборудования, находящимися в аппаратной, допускается прямое кабельное соединение «точка-точка». При таком соединении единиц оборудования в аппаратной необходимо применять кабели длиной не более 15 м, причём их необходимо использовать только между единицами оборудования, находящимися в соседних стойках или шкафах в одном и том же ряду.

6.10 Телекоммуникационные помещения

В датацентрах телекоммуникационные помещения — это место, где происходит разводка кабелей к зонам вне серверной, но при необходимости его можно объединить с главной распределительной зоной или горизонтальной распределительной зоной.

В датацентре может быть расположено несколько телекоммуникационных помещений, если подлежащие обслуживанию зоны невозможно поддерживать из одного помещения.

6.11 Вспомогательные зоны датацентра

Вспомогательные (подсобные) зоны датацентра — это места вне серверной, которые предназначены для поддержки оборудования датацентра. К ним относятся операционный центр, офисы обслуживающего персонала, комнаты охраны, комнаты электриков, механиков, складские помещения, помещения для подготовки оборудования перед монтажом, погрузочные платформы.

Операционный центр, комната охраны и офисы обслуживающего персонала должны быть снабжены кабельной системой. Для пультов операционного центра и пультов охраны потребуется большее число кабелей, чем для стандартных рабочих мест. Операционный центр может потребовать также кабельной системы для больших стенных или потолочных дисплеев (мониторов или телевизионных экранов).

В комнатах электриков, комнатах механиков, складских помещениях, комнатах для подготовки оборудования к монтажу и у погрузочных платформ следует установить хотя бы по одному настенному телефону на каждое помещение. Комнаты электриков и механиков должны иметь также, по крайней мере, одно подключение для передачи данных для доступа к системе управления объектом.

6.12 Стойки и шкафы

6.12.1 Общие положения

Стойки должны быть снабжены боковыми монтажными направляющими, к которым монтируются оборудование и арматура. Шкафы могут иметь боковые монтажные направляющие, боковые стенки, верхнюю па-

нель-крышку, переднюю и заднюю дверцы, и они зачастую снабжаются замками.

6.12.2 «Горячие» и «холодные» проходы

Шкафы и стойки должны быть расположены по чередующейся схеме, с тем, чтобы передняя сторона шкафов/стоек в каждом ряду была обращена к передней же стороне другого ряда, создавая «горячие» и «холодные» проходы.

«Холодными» называют проходы вдоль передней стороны шкафов/стоек. Если в «холодных» проходах устроен фальшпол, то здесь под полом, на плите перекрытия, следует уложить силовые кабели.

«Горячими» являются проходы вдоль задней стороны шкафов/стоек. При наличии в «горячих» проходах фальшпола под ним следует проложить кабельные желоба (короба) для телекоммуникационной кабельной системы.

Пример «горячих» проходов, «холодных» проходов и размещения шкафов приведен на рисунке 6.

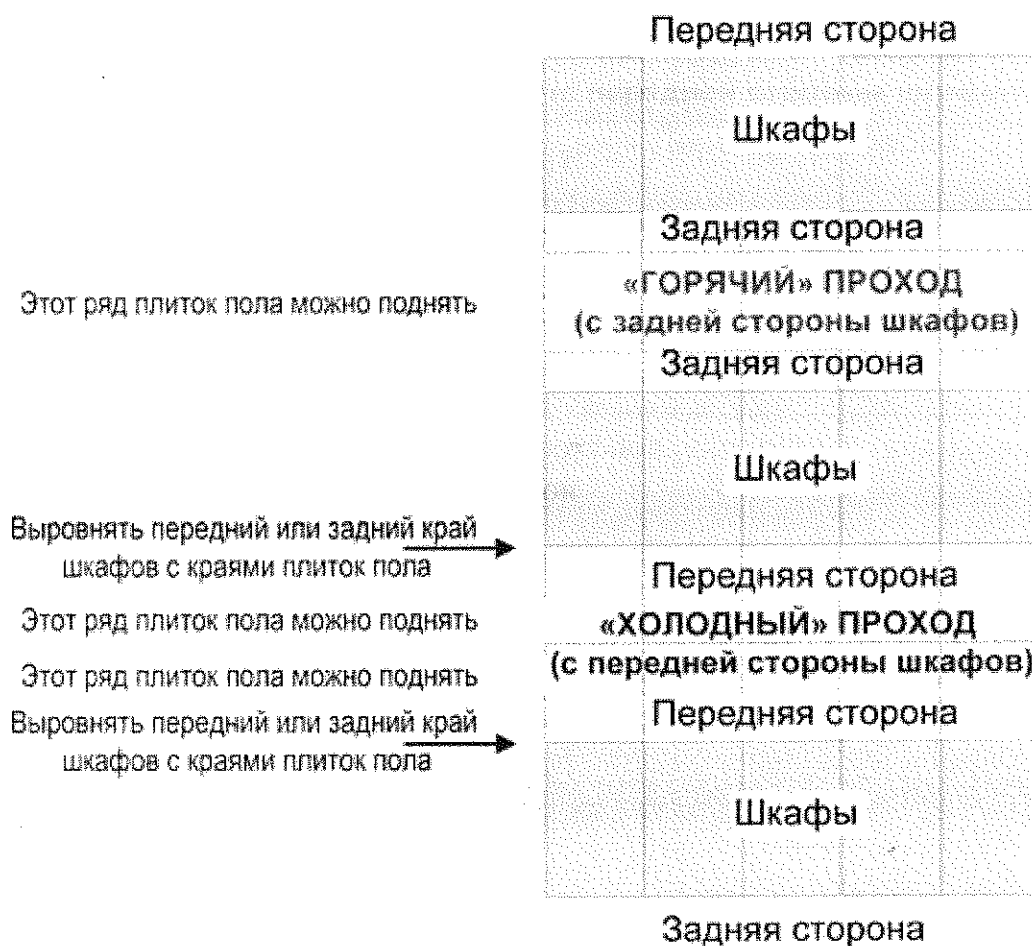


Рисунок 6 - Пример «горячих» проходов, «холодных» проходов и размещения шкафов

6.12.3 Размещение относительно плиток фальшпола

При размещении на фальшполах шкафы и стойки должны быть поставлены так, чтобы они не мешали поднимать плитки пола с передней и задней стороны шкафов и стоек.

Шкафы следует выровнять либо по передней, либо по задней кромке ряда уложенных плиток пола. Стойки следует ставить так, чтобы резьбовые стержни, которыми стойка крепится к плите перекрытия, не проходили сквозь стрингеры фальшпола.

6.12.4 Вырезы в плитках фальшпола

Вырезы (прорезы) в плитках фальшпола не следует делать большего размера, чем это необходимо. В вырезы плиток следует вставлять вентиляционные решётки с клапаном или щётки, чтобы уменьшить потери воздуха через отверстия в плитках пола. Вырезы плиток пола должны иметь отделку или уплотнения по всем кромкам.

Вырезы в плитках пола для шкафов следует размещать под шкафами или в другом месте, где не возникнет опасность споткнуться о такой вырез.

Вырезы в плитках пола для стоек следует размещать либо под вертикальными кабельными организаторами между стойками, либо под стойкой (у отверстия между нижними уголками). Обычно первый вариант размещения предпочтителен, поскольку позволяет устанавливать оборудование в нижней части стойки.

6.12.5 Стойки и шкафы в комнате ввода внешних сервисов, главной, промежуточной и горизонтальной распределительных зонах

В комнате ввода, главной, промежуточной и горизонтальной распределительных зонах для размещения оборудования и панелей переключения следует использовать стойки размером 480 mm. Поставщики услуг могут устанавливать своё оборудование в комнате ввода как в стойках размером 585 mm, так и в шкафах собственной конструкции.

В комнате ввода внешних сервисов, главной, промежуточной и горизонтальной распределительных зонах перед каждой парой стоек и у обоих концов каждого ряда стоек должен быть установлен вертикальный кабельный организатор. Эти устройства должны иметь ширину не менее 83 mm. В местах установки единичных стоек вертикальные кабельные организаторы должны иметь ширину не менее 150 mm. В тех случаях, когда стойки поставлены в один или несколько рядов, необходимо предусмотреть возможность установки вертикальных кабельных организаторов шириной 250 mm между стойками и шириной 150 mm по обоим концам ряда стоек. Эти вертикальные организаторы должны быть такой же высоты, что и стойки.

В комнате ввода внешних сервисов, главной, промежуточной и горизонтальной распределительных зонах над и под каждой панелью переключения следует устанавливать горизонтальные кабельные организаторы.

Предпочтительное отношение числа горизонтальных кабельных организаторов к числу панелей переключения 1:1.

Управление кабелями с помощью вертикальных и горизонтальных кабельных организаторов и резерв кабеля должны быть достаточными для того, чтобы обеспечить аккуратную заделку кабелей и выполнение требований к радиусу изгиба.

7 Кабельные системы датацентров

7.1 Горизонтальная кабельная система

7.1.1 Общие положения

Горизонтальная кабельная система – это часть телекоммуникационной кабельной системы от механического оконцевателя в аппаратной до горизонтальной кросс-панели в горизонтальной распределительной зоне либо до основной (главной) кросс-панели в главной распределительной зоне.

При проектировании горизонтальной кабельной системы следует учитывать следующее:

- голосовую, модемную и факсимильную связь;
- коммутационное оборудование помещений;
- соединения для управления (администрирования) вычислительной сетью и сетью связи;
- KVM-соединения;
- информационные коммуникации;
- глобальные сети;
- локальные сети;
- ССХД;
- прочие сигнальные системы здания (системы автоматизации здания, например система противопожарной защиты, система охраны, система энергоснабжения, ОВиК, система управления электропотреблением и т.д.).

Горизонтальная кабельная система должна планироваться с целью снижения расходов на ее обслуживание и внесение изменений, а также с учетом возможного расширения парка активного оборудования и появления новых сервисов. Следует уделить внимание таким вопросам, как восприимчивость системы к разнообразию пользовательских приложений, с тем, чтобы сократить или исключить вероятность изменений в кабельной системе по мере развития потребностей оборудования. Доступ к горизонтальной системе для её реконфигурирования можно обеспечить через фальшпол или через систему кабельных лотков верхнего расположения. Однако в правильно спланированном помещении вмешательство в горизонтальную систему случается только при добавлении новых кабелей.

7.1.2 Топология

Горизонтальная кабельная система должна иметь топологию звезды, как показано на рисунке 7. Каждый механический оконцеватель в аппаратной должен быть соединён горизонтальным кабелем с горизонтальной коммутационной панелью в горизонтальной распределительной зоне или с основной (главной) коммутационной панелью в главной распределительной зоне.

Горизонтальная кабельная система должна содержать не более одной консолидационной точки в месте зонного распределения между горизонтальной коммутационной панелью в горизонтальной распределительной зоне и механическим оконцевателем в аппаратной.

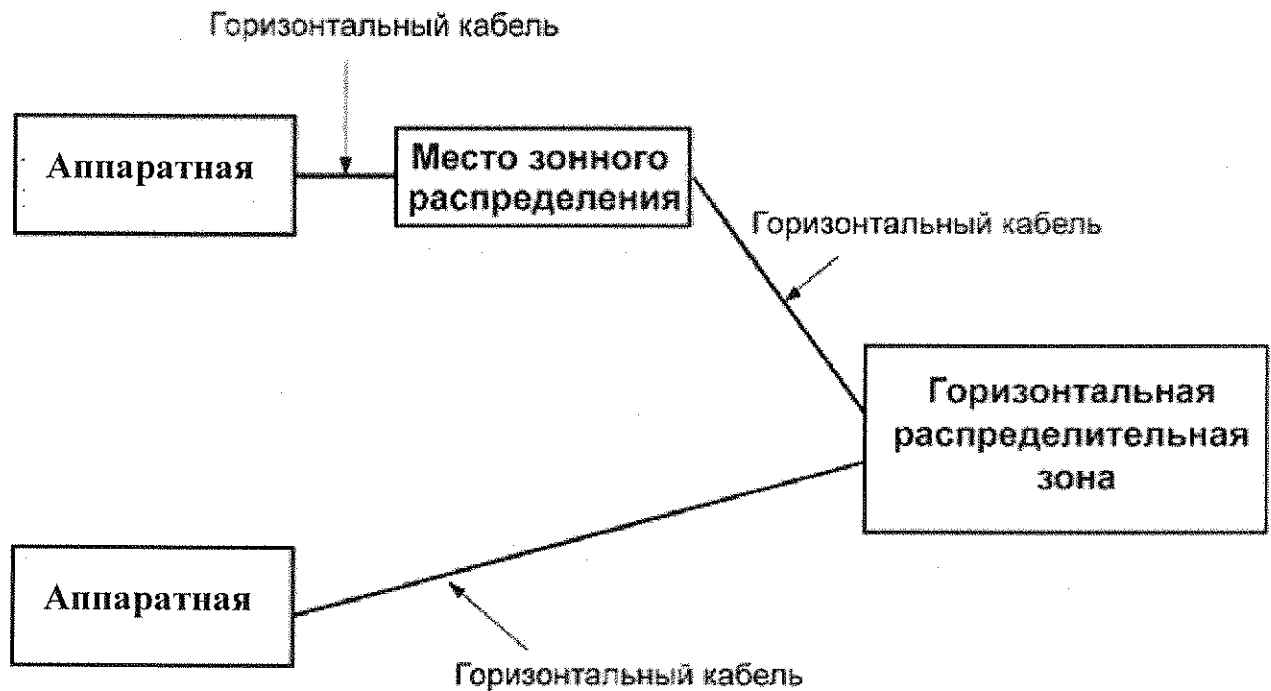


Рисунок 7 - Типовая схема горизонтальной кабельной системы с топологией звезды

7.1.3 Длина горизонтальной кабельной системы

Длина горизонтальной кабельной разводки — это длина кабеля от механического окончания носителя на горизонтальной кросс-панели в горизонтальной распределительной зоне или в главной распределительной зоне до механического окончания носителя в аппаратном помещении. Максимально допустимая длина горизонтальной кабельной разводки равна 90 м, вне зависимости от типа кабельного носителя. Максимально допустимая длина канала связи с учётом соединительных шнуров равна 100 м. Максимально допустимая длина кабельной разводки в датацентре, не имеющем горизонтальной распределительной зоны, равна 300 м для оптического канала с учётом соединительных шнуров, 90 м для медного кабеля без учёта

соединительных шнуров и 100 m для медного кабеля с учётом соединительных шнуров.

Дополнительные сведения по длинам кабельной системы для разных случаев применения приведены в приложении Е.

7.2 Магистраль

7.2.1 Общие положения

Назначение магистрали – обеспечить соединения между главной распределительной зоной, горизонтальной распределительной зоной и помещениями ввода внешних сервисов в кабельной системе датацентра. Магистраль состоит из магистральных кабелей, основных (главных) кросс-панелей, горизонтальных кросс-панелей, механических оконцевателей и шнуров переключения или перемычек, используемых для кросс-соединений «магистраль-магистраль».

Ожидается, что магистраль будет обслуживать потребности пользователей датацентра в течение одного или нескольких планируемых периодов, каждый из которых занимает отрезок времени, измеряемый днями или месяцами. В течение каждого планируемого периода магистраль должна обеспечивать возможность возрастания и изменения пользовательских потребностей в обслуживании без установки дополнительной кабельной системы. Длительность планируемого периода полностью зависит от материально-технического обеспечения проекта, включая закупку материалов, транспортировку, контроль монтажа и технического состояния.

Магистраль должна допускать реконфигурирование и будущее расширение без вмешательства в магистральную кабельную систему. Магистраль должна поддерживать разные требования к связности, включая связность, как с сетями, так и с физическими консолями, например, должна обеспечивать соединение с локальными сетями, глобальными сетями, сетями систем хранения данных, компьютерными каналами и пультами управления оборудованием.

7.2.2 Топология

7.2.2.1 Топология типа «звезда»

Магистральная система должна использовать иерархическую топологию типа «звезда» (рисунок 8), в которой каждая горизонтальная коммутационная панель в горизонтальной распределительной зоне соединена кабелем непосредственно с основной (главной) коммутационной панелью в главной распределительной зоне. Магистральная кабельная система должна содержать не более одного иерархического уровня кросс-соединения. На пути от горизонтальной кросс-панели к другой горизонтальной кросс-панели сигнал должен преодолевать не более одной кросс-панели.

СТАНДАРТЫ И ТЕХНИЧЕСКИЕ УСЛОВИЯ
ИЗДАНИЕ 1-е 2014 г.
АКТИВНО УТВЕРЖДЕНО
ИЗДАНИЕ 1-е 2014 г.



Рисунок 8 - Типовая магистраль, построенная по топологии типа «звезда»

Наличие горизонтальной кросс-панели не является обязательным. Когда горизонтальные кросс-панели отсутствуют, кабельная система от основной (главной) кросс-панели к механическому оконцевателю в аппаратной считается горизонтальной системой. Если такая горизонтальная система проходит через зону горизонтального распределения, необходимо в горизонтальной распределительной зоне предусмотреть запас длины кабеля, допускающий движение кабелей при их перемещении к какой-нибудь кросс-панели.

Кросс-панели магистральной кабельной системы могут располагаться в телекоммуникационных помещениях, в главных распределительных зонах, промежуточных распределительных зонах, горизонтальных распределительных зонах или в комнатах ввода внешних сервисов.

7.2.2.2 Восприимчивость к конфигурациям, не использующим топологию типа «звезда»

Топология, приведенная на рисунке 8, благодаря использованию соответствующих межсоединений, электроники или адаптеров в распределительных зонах, датацентров, зачастую может включать в себя системы, спроектированные на основе иной топологии – использующие конфигурацию типа «кольцо», «шина» или «дерево».

Между горизонтальными распределительными зонами можно организовать кабельную систему для обеспечения резервирования и во избежание превышения ограничений по длине в связи с использованием существующей кабельной системы.

7.2.3 Избыточные топологии кабельной системы

Избыточные топологии могут включать в себя параллельную иерархию с резервными распределительными зонами. Эти топологии являются дополнениями к топологии типа «звезда».

7.2.4 Длина магистральной кабельной системы

Максимально допустимые значения длины зависят от условий применения и типа кабельных носителей. Максимальные значения длины магистрали приведены в приложении Е. Чтобы свести к минимуму длину кабельной системы, зачастую выгодно располагать основную (главную) коммутационную панель примерно в середине вычислительного центра. Кабельные сети, которые превышают эти ограничения по длине, можно разделить на некие зоны, каждая из которых может обслуживаться магистральной системой в соответствии с настоящим стандартом. Межсоединения между такими отдельными зонами, которые выходят за пределы области применения настоящего стандарта, могут быть выполнены с помощью оборудования и технологий, обычно применяемых в глобальных сетях.

Общая длина магистральной кабельной системы, выполненной из многопарного симметричного кабеля с сопротивлением 100 Ω категории 3 и поддерживающей прикладные системы тактовой частотой до 16 MHz, должна быть не более 90 m.

Общая длина магистральной кабельной системы, выполненной из многопарного симметричного кабеля с сопротивлением 100 Ω категорий 5 и 6, должна быть не более 90 m. Эта длина допускает дополнительно подключать к магистрали с обоих концов соединительные кабели (шнуры) длиной 5 m.

В датацентрах обычно используются шнуры переключения длиной более 5 m. В датацентрах, использующих такие кабели, максимальная длина магистральной системы должна быть соответственно уменьшена, чтобы не были превышены максимально допустимые значения длины канала.

7.3 Выбор кабельного носителя

Кабельная система в соответствии с настоящим стандартом применяется для разных прикладных задач, которые выполняются в среде данного датацентра. Выбор кабельных носителей следует делать в зависимости от характеристик индивидуальной задачи. Делая этот выбор, нужно учитывать перечисленные ниже факторы:

- а) гибкость по отношению к поддерживаемым сервисам;
- б) требуемый срок службы кабельной системы;
- с) размеры помещений/всего вычислительного центра и число пользователей;

д) пропускную способность канала в пределах этой кабельной системы;

е) рекомендации или спецификации поставщика оборудования.

В случае если один тип кабеля не удовлетворяет всем требованиям конечного пользователя, необходимо использовать в магистральной кабельной системе кабели нескольких типов. В таких случаях разные кабельные носители должны использовать ту же архитектуру помещений с тем же самым расположением кросс-панелей, механических оконцевателей и т.д.

8 Кабельные каналы, фальшполы и потолочные лотки

8.1 Кабельные каналы датацентров

Телекоммуникационную кабельную систему датацентра не допускается проводить через пространства, доступные для посторонних лиц или для персонала здания, если кабели не заключены в закрытый кабельный трубопровод или иной безопасный кабельный канал. Все смотровые люки, коробки для кабелепротяжки и сплайс-коробки должны быть снабжены замками.

Внешний кабель для датацентров не следует прокладывать через общие аппаратные.

Любые смотровые люки, как относящиеся собственно к зданию, так и контролируемые владельцем датацентра, следует держать на замке и под наблюдением системы охраны датацентра, с использованием видеокамеры, дистанционного устройства тревожной сигнализации или того и другого вместе.

Доступ к коробкам для кабелепротяжки для кабельной системы датацентров (будь то подводящие кабели или кабельная система между частями датацентра), расположенным в общедоступных местах или в помещениях совместного пользования с другими обитателями здания, следует контролировать. Коробки для кабелепротяжки также следует держать на замке и под наблюдением системы охраны датацентра, с использованием видеокамеры, дистанционного устройства тревожной сигнализации или того и другого вместе.

Все сплайс-коробки для кабельной системы датацентра, находящиеся в общедоступных местах, следует держать на замке и под наблюдением системы охраны датацентра с использованием видеокамеры, дистанционного устройства тревожной сигнализации или того и другого вместе.

Вход в тоннели коммунальных служб, используемые в качестве коммун. ввода внешних телекоммуникаций и для других кабельных разводов датацентров, следует держать под замком. Если эти туннели используются несколькими сотрудниками здания или если их нельзя запереть, кабели для

датацентров должны быть заключены в жёсткий кабельный трубопровод или иной безопасный кабельный канал.

8.2 Фальшполы

8.2.1 Общие положения

Системы фальшполов, называемых также съёмными полами, следует использовать в датацентрах, обслуживающих оборудование, к которому кабели подводятся снизу.

Кабели под фальшполом должны быть терминированы, по крайней мере, одним концом в главной распределительной зоне либо в горизонтальной распределительной зоне или же их нужно удалить.

Дополнительные сведения об установке стоек и шкафов на фальшполы приведены в 6.12.

8.2.2 Кабельные лотки для телекоммуникационной кабельной системы

Телекоммуникационная кабельная система под фальшполом должна размещаться в вентилируемых кабельных лотках, которые не препятствуют потоку воздуха.

Маршруты прокладываемых под полом кабельных лотков следует уже на стадиях планирования координировать с другими системами, которые также будут находиться под полом.

8.2.3 Требования к эксплуатационным качествам фальшполов

Фальшполы для датацентров должны иметь собранное на болтах стрингерное основание, поскольку такие фальшполы более устойчивы, чем бесстрингерные. Кроме того, для повышения устойчивости стрингеры фальшполов должны иметь длину 1,2 m и расстановку типа «ёлочка». Для дополнительной устойчивости подставки следует закрепить болтами к чёрному полу.

8.2.4 Кромки вырезов плиток фальшпола

Вырезы в плитках фальшпола должны иметь окантовку или уплотнения по всей длине кромок. Если окантовка или уплотнения возвышаются над поверхностью фальшпола, их необходимо установить так, чтобы они не мешали размещению стоек и шкафов. Окантовку или уплотнения не допускается размещать там, где стойки и шкафы нормально контактируют с поверхностью фальшпола. В тех случаях, когда система ОВиК выпускает воздух через пол, вырезы в плитках пола следует ограничить как по размерам, так и по количеству, чтобы обеспечить надлежащий воздушный поток. Рекомендуются выполнять надлежащую балансировку системы ОВиК, когда все стойки с оборудованием, шкафы и пр. будут установлены на свои

места. При добавлении вырезов в полу, стоек, шкафов и т.п. систему ОВиК следует балансировать заново.

8.3 Потолочные лотки

Потолочные лотки могут уменьшить потребность в устройстве фальшполов в тех датацентрах, где не применяются напольные системы, требующие подвода кабелей снизу.

Потолочные лотки могут быть смонтированы в несколько ярусов, чтобы обеспечить достаточную пропускную способность. Обычно используют двухъярусный или трёхъярусный монтаж потолочных лотков, один ярус для силовых кабелей и один или два – для телекоммуникационной кабельной системы. Один из ярусов потолочных лотков обычно имеет кронштейны на той стене, которая несёт заземляющую структуру датацентра. Эти потолочные лотки часто дополняются системой кабельных трубопроводов или лотков для оптических кабелей переключения. Трубопровод или лоток для оптического кабеля может быть закреплён к тем же самым висячим стержням, которые используются в качестве опоры для потолочных лотков.

Кабели в навесных кабельных коробах нельзя оставлять без внимания. Кабели должны быть терминированы, по крайней мере, одним концом в главной распределительной зоне либо в горизонтальной распределительной зоне, или же их нужно удалить.

В проходах и других общих пространствах в датацентрах потолочные лотки должны иметь сплошное дно либо должны располагаться на высоте не менее 2,7 m над готовым полом, для того чтобы ограничить доступ к ним, либо же они должны быть иным образом защищены от случайного и/или намеренного повреждения.

Рекомендуемая максимально допустимая глубина любого кабельного короба равна 0,15 m.

9 Избыточность (резервирование) инфраструктуры, систем, провайдеров доступа

9.1 Общие положения

Датацентры, которые оборудованы разнотипными телекоммуникационными устройствами, способны продолжать работу даже при чрезвычайных обстоятельствах. Настоящий стандарт устанавливает четыре уровня, соответствующих разной степени готовности инфраструктуры датацентра. Сведения об уровнях инфраструктуры приведены в приложении D. На рисунке 9 представлены различные резервные компоненты инфраструктуры телекоммуникаций, которые можно добавить к базовой инфраструктуре.

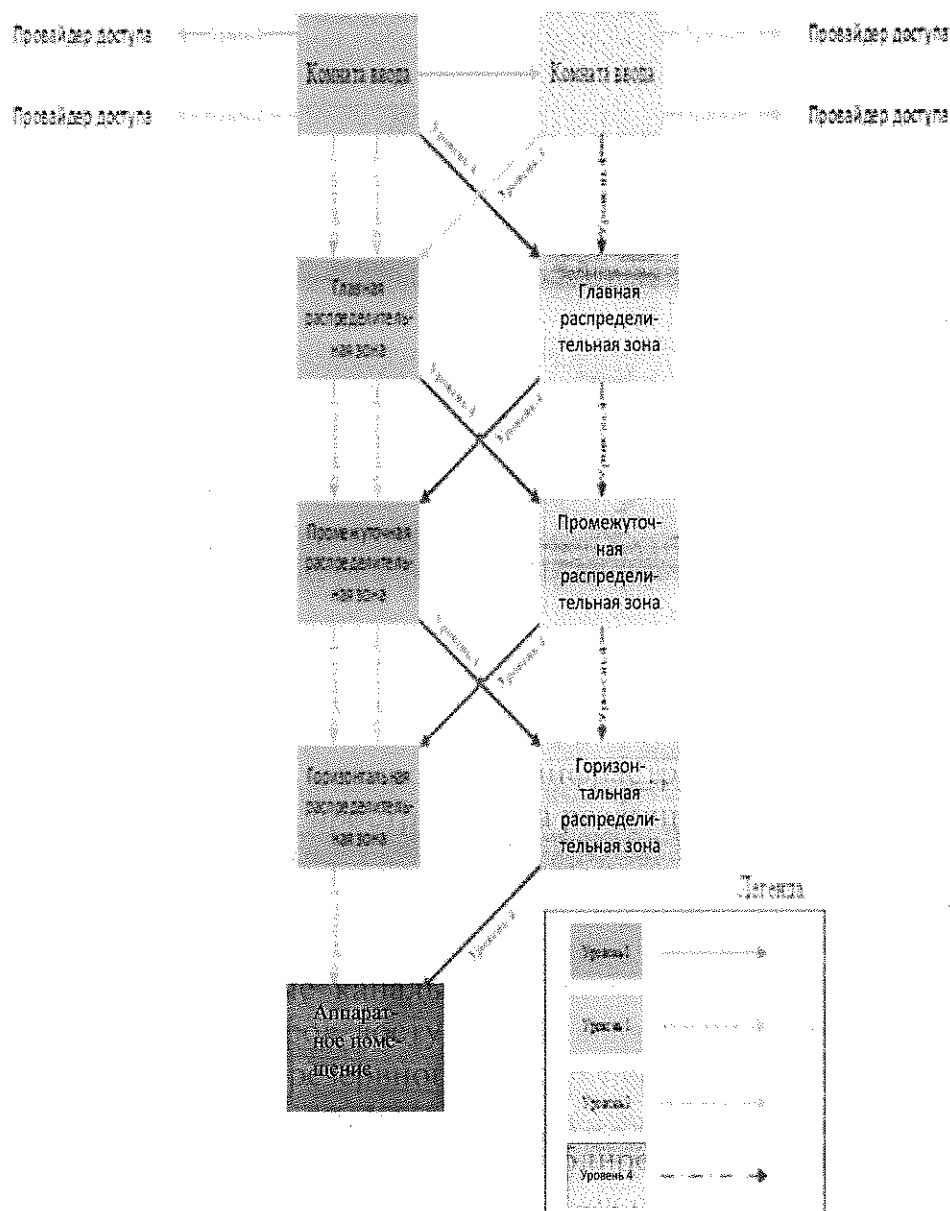


Рисунок 9 - Резервирование инфраструктуры телекоммуникаций и пространств на различных уровнях

Надёжность инфраструктуры телекоммуникаций можно повысить, предусмотрев резервные зоны перекрёстного соединения и физически разделённые кабельные каналы. Для датацентров свойственно наличие нескольких провайдеров доступа, поставляющих услуги, а также резервных маршрутизаторов, резервного центрального распределения и окончательных коммутаторов. Такая топология сети обеспечивает определённый уровень резервирования, но одно только дублирование сервисов и аппаратуры не обеспечивает исключения единых точек отказов.

9.2 Резервные смотровые люки и внешние кабельные каналы

Наличие нескольких внешних кабельных каналов от собственной линии провайдера к комнате (комнатам) ввода исключает единую точку отказа для провайдерских сервисов, входящих в здание. Эти кабельные каналы должны иметь принадлежащие пользователю смотровые люки в тех случаях, когда жёсткие металлические кабельные каналы (кабельные трубопроводы) провайдера не заканчиваются у стены здания. Смотровые люки и внешние кабельные каналы должны находиться с противоположных сторон стены здания и должны быть удалены друг от друга, по крайней мере, на 20 м.

В датацентрах с двумя комнатами ввода и двумя смотровыми люками нет необходимости устанавливать кабельные трубопроводы от каждой комнаты ввода к каждому из двух смотровых люков. При такой конфигурации от каждого провайдера доступа обычно требуют установить два внешних кабеля, один к главной комнате ввода через главный смотровой люк и один - к вспомогательной комнате ввода через вспомогательный смотровой люк. Кабельные трубопроводы от главного смотрового люка к вспомогательной комнате ввода и от вспомогательного смотрового люка к главной комнате ввода обеспечивают гибкость, но не являются обязательными.

В датацентрах с двумя комнатами ввода допускается устанавливать кабельные трубопроводы между двумя комнатами ввода с целью обеспечения прямого пути для кабелей провайдера доступа между этими двумя комнатами, например чтобы выполнить кольцо для сети SONET или SDH.

9.3 Резервные сервисы провайдеров доступа

С целью обеспечения непрерывности услуг телекоммуникаций, предоставляемых датацентру провайдерами доступа, можно привлечь несколько провайдеров, использовать несколько провайдерских центральных офисов, а также предусмотреть несколько разных кабельных трасс от провайдеров доступа к датацентру.

Наличие нескольких провайдеров обеспечит непрерывность связи в случае масштабной аварии у провайдера или в случае его финансового краха, способного повлиять на сервис.

Но всё же одно лишь использование нескольких провайдеров доступа не гарантирует непрерывности сервиса, поскольку провайдеры часто сообща занимают площадь в центральных офисах и совместно используют кабельные трассы.

Пользователю следует обеспечить такое положение, при котором сервисы поставляются из разных провайдерских центральных офисов и кабельные трассы к этим центральным офисам идут по разным маршру-

там. Эти трассы должны быть физически отдалены друг от друга на расстояние не менее 20 m во всех точках по всей длине этих трасс.

9.4 Резервирование комнат ввода

Несколько комнат ввода можно устроить с целью резервирования, а не только для того, чтобы обойти ограничения на максимальную длину линии. Наличие нескольких комнат ввода повышает степень резервирования, но усложняет организационное управление.

Следует весьма внимательно распределить линии между комнатами ввода.

Провайдеры доступа должны установить своё оборудование в обеих комнатах ввода таким образом, чтобы линии всех требуемых типов можно было подготовить к работе (инициировать) из каждой комнаты. Иницирующее оборудование провайдера в одной комнате ввода не должно быть подчинённым по отношению к оборудованию в другой комнате ввода. Оборудование провайдера в каждой из комнат ввода должно быть способно работать в случае отказа в другой комнате ввода.

Две комнаты ввода следует отодвинуть друг от друга на расстояние не менее 20 м и разместить в отдельных огнезащитных зонах. Комнаты ввода не должны иметь общих распределительных щитов питания и общего оборудования для кондиционирования воздуха.

9.5 Резервная главная распределительная зона

Второстепенная распределительная зона обеспечит дополнительное резервирование, но при этом усложнится организационное управление. Основные маршрутизаторы и коммутаторы следует распределить между главной распределительной зоной и второстепенной распределительной зоной. Линии также следует распределить между двумя этими зонами.

Устраивать второстепенную распределительную зону не имеет смысла, если серверная представляет собой единое пространство, поскольку пожар в одной части датацентра потребует, вероятно, отключения всего датацентра целиком.

9.6 Резервная магистральная система

Резервная магистраль защищает от общего выхода из строя вследствие отказа магистральной кабельной системы. Резервная магистраль может быть устроена по-разному, в зависимости от желаемой степени защиты.

Магистральная система между двумя зонами, например, между горизонтальной распределительной зоной и главной распределительной зоной может быть выполнена путём укладки двух кабелей между этими зонами,

предпочтительно по двум разным маршрутам. Если датацентр имеет главную распределительную зону и второстепенную распределительную зону, то укладывать резервирующую магистральную систему к горизонтальной распределительной зоне нет необходимости, однако кабели к главной распределительной зоне и второстепенной распределительной зоне следует проложить по разным маршрутам.

9.7 Резервная горизонтальная система

Горизонтальную кабельную систему к критически важным системам можно проложить по разным маршрутам, чтобы повысить степень резервирования. При выборе маршрутов следует соблюдать осторожность, чтобы не превысить максимально допустимую длину горизонтального кабеля.

Для критически важных систем можно предусмотреть две разные горизонтальные распределительные зоны, если только не превышать ограничений на максимальную длину кабелей. Но такая степень резервирования, возможно, не обеспечит намного более надёжную защиту, чем укладка горизонтальной системы по разным маршрутам, если две эти горизонтальные распределительные зоны находятся в одной и той же огнезащитной зоне.

10 Обеспечение информационной безопасности

10.1 Комплекс технических (аппаратно-программных) средств защиты

10.1.1 Общие положения

Комплексы технических средств защиты информации в основном включают в себя программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации (временных файлов), тестового контроля системы защиты и др.

10.1.2 Применение систем обнаружения и предотвращения атак (IDS/IPS)

Система обнаружения и предотвращения вторжений (IDS/IPS) - это программное или программно-аппаратное средство, предназначенное для выявления, предотвращения или блокировки аномалий в сетевом трафике. Детектируются отклонения от поведения сетевых приложений в реальном времени, а также факты неавторизованного доступа (вторжения или сетевые атаки) в компьютерную систему или сеть. IDS/IPS служат как дополнение к межсетевым экранам, работа которых происходит на основе политики безопасности, IDS/IPS служат механизмами мониторинга и наблюдения подозрительной активности. Они могут обнаружить атакующих, которые обошли межсетевой экран и выдать отчет об этом инциденте.

Выбор IPS/IDS основывается исходя из масштаба сетевой инфраструктуры, а также пропускной способности интерфейсов коммуникационного оборудования (маршрутизаторов, коммутаторов, линии связи) датацентра.

10.1.3 Режимы (размещения) систем обнаружения и предотвращения атак (IPS/IDS)

Режим inline IPS/IDS подразумевает, что сенсор находится в разрыве потока анализируемого трафика, тем самым может непосредственно в момент обнаружения угрозы заблокировать опасный пакет или соединение. Простой в таком расположении, при выходе из строя полностью устройства (например, обесточено), может привести к потере связи (если, конечно, канал не зарезервирован). Аналогичная ситуация случится, если устройство настроено в режиме fail-close.

В режиме promiscuous (неразборчивый) IPS/IDS работают как сниффер, это отдельное устройство, на которое копируется трафик с помощью SPAN сессии с коммутатора. Устройство также может блокировать вредоносный трафик, управляя пакетными фильтрами на подконтрольных маршрутизаторах/устройствах безопасности, но это действие уже может быть запоздалым, т.к. начальные пакеты будут уже переданы. В этом режиме выход из строя устройства IPS/IDS фактически не приведет к потере связи.

В зависимости от поставленных задач, применяется анализ полной копии всех пакетов либо информации о каждом установленном сетевом соединении/обмене. Полная копия пакетов, обрабатываемых управляемым коммутатором, направляется на выделенный SPAN-порт, к которому подключается сетевой сенсор. В зависимости от производителя, версии аппаратной платформы и программного обеспечения коммутатора, возможно выборочное копирование входящих/исходящих пакетов определенных физических либо логических интерфейсов на SPAN-порт. Для эффективного анализа пропускная способность SPAN-порта и, соответственно, сетевого сенсора, должна быть не менее пиковой суммарной нагрузки на анализируемые интерфейсы.

10.1.4 Указания по эксплуатации систем обнаружения и предотвращения атак (IPS/IDS)

Установка устройства недостаточной мощности вызовет ухудшение параметров работы инфраструктуры, либо, не будет выполнять свои функции.

Система обнаружения и предотвращения атак при вводе в действие должна пройти предварительные испытания, предусмотренные нормативно-техническими документами, для определения ее работоспособности и принятия решения о возможности передачи IPS/IDS в опытную эксплуатацию.

При проведении приемочных испытаний с использованием средств телекоммуникаций общего пользования или других ведомств и организаций в состав приемочной комиссии включаются их представители. В случае осуществления доставки, установки и наладки IPS/IDS внешними исполнителями, продолжительность опытной эксплуатации IPS/IDS согласовывается между заказчиками и исполнителями.

По результатам приемочных испытаний и опытной эксплуатации комиссия составляет акт о вводе в действие IPS/IDS. Датой ввода в действие IPS/IDS считается дата подписания акта приемочной комиссией.

10.1.5 Применение межсетевых экранов и выделение демилитаризованных зон

Под межсетевым экраном понимается комплекс аппаратных или программных средств управления доступом, защищающее внутренние сети от внешних атак, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Межсетевой экран устанавливается на границе между внешней и внутренней сетью.

Все межсетевые экраны можно разделить на три типа:

- пакетные фильтры;
- сервера прикладного уровня;
- сервера уровня соединения.

Все типы могут одновременно встретиться в одном межсетевом экране.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также межсетевые экраны часто называют фильтрами, так как их основная задача пропускать или не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. Межсетевые экраны рекомендуются внедрять для решения следующих задач:

- контроля отдельных веб-приложений;
- обнаружения вторжений по наиболее популярным протоколам, таким как HTTP, SMTP и POP3;
- создания VPN-соединений для удаленного подключения (мобильных) пользователей;
- оптимизации сетевого взаимодействия;
- защита от распределенных атак;
- организация выделенных зон безопасности;
- построение отказоустойчивых VPN с балансировкой нагрузки.

10.1.6 Схема подключения межсетевого экрана

Основной схемой подключения межсетевого экрана является схема с использованием двух и более сетевых интерфейсов.

Межсетевые экраны с двумя сетевыми интерфейсами. Межсетевой экран имеет два сетевых интерфейса, подключенных к двум различным сетям. Это наиболее распространенная схема подключения межсетевого экрана. Большинство межсетевых экранов рассчитаны именно на эту схему подключения. Межсетевой экран осуществляет физическое и логическое разделение двух сетей, принимая решение о возможности установления соединения (передачи пакетов) между ними. Как правило, со стороны внешней сети межсетевой экран подключен к маршрутизатору (чаще всего к маршрутизатору провайдера). Внешний маршрутизатор должен пропускать только пакеты, принадлежащие адресному IP-пространству межсетевого экрана или внутренней сети. Если маршрутизатор поддерживает функции фильтра пакетов, то для повышения производительности межсетевого экрана на маршрутизаторе могут быть заданы первичные правила фильтрации входящего трафика. Например, иногда целесообразно с помощью маршрутизатора блокировать (IP-пакеты с подделанным адресом отправителя IP-spoofing) неиспользуемые порты. Внутренний маршрутизатор используется в больших корпоративных сетях или для усиления политики безопасности. Чаще всего после межсетевого экрана располагают сетевой коммутатор или концентратор Ethernet.

Демилитаризованная зона. В некоторых межсетевых экранах допускается использование нескольких сетевых интерфейсов с установлением различных политик безопасности между подключаемыми к ним сетям. Существует возможность образования так называемой демилитаризованной зоны. В демилитаризованных зонах размещают службы, которые должны быть доступны и клиентам сети Интернет, и клиентам защищенной сети. Поскольку доступ к сервисам демилитаризованных зон должен осуществляться из открытой сети, то в демилитаризованной зоне определяются менее жесткие требования к сетевой безопасности, но достаточные для организации защиты от внешних угроз. Демилитаризованная зона может быть образована и путем подключения серверов перед межсетевым экраном. Если в сети используются группы пользователей с четким разграничением доступных сервисов или различными уровнями конфиденциальности обрабатываемой информации, то межсетевой экран может контролировать сетевые потоки не только во внешние сети, но и между внутренними сегментами сети. Такая возможность достигается за счет использования дополнительных интерфейсов и установки соответствующих правил.

Выделение демилитаризованных зон, а также поддержка нескольких сетевых интерфейсов межсетевым экраном позволяют вести централизованное управление защитой сетевых ресурсов с различными принятыми политиками безопасности.

10.1.7 Указания по эксплуатации межсетевого экрана

Межсетевой экран обеспечивает конфиденциальность и защиту от несанкционированного доступа при реализации организацией следующих предварительных организационно-распорядительных мер. Должны быть приняты следующие меры:

- обеспечена физическая сохранность (целостность) оборудования;
- предусмотрена защита от электромагнитного, акустического и других видов излучения;
- представлены документы производителя, подтверждающие проведение тестирования межсетевого экрана на соответствие требований сертификата.

При проведении приемочных испытаний с привлечением других ведомств и организаций в состав приемочной комиссии включаются представители их организаций. В случае осуществления доставки, установки и наладки межсетевого экрана внешними исполнителями, продолжительность опытной эксплуатации межсетевого экрана согласовывается между заказчиками и исполнителями.

По результатам приемочных испытаний и опытной эксплуатации комиссия составляет акт о вводе в действие межсетевого экрана. Датой ввода в действие межсетевого экрана считается дата подписания акта приемочной комиссией.

10.1.8 Постоянный централизованный антивирусный мониторинг

Антивирусная защита должна представлять собой масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети рабочих станций и серверов.

В рамках всего датацентра должны использоваться единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие персональные компьютеры, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус).

Антивирусные средства должны включать:

- лицензионный файл ключа;
- программные средства антивирусной защиты рабочих станций и серверов;
- программные средства централизованного управления, мониторинга и обновления операционной системы;
- обновляемые базы данных сигнатур вредоносных программ и атак;
- эксплуатационную документацию.

СЕРТИФИКАТ АССЕРТАЦИИ
СТАНДАРТИЗАЦИИ, ПАТЕНТ
ИЗДАТЕЛЬСТВА
АККРЕДИТОВАННЫЙ
ЦЕНТР

10.1.9 Требования к программным средствам антивирусной защиты серверов

Программные средства антивирусной защиты файловых серверов должны обеспечивать реализацию следующих функциональных возможностей:

- резидентный антивирусный мониторинг;
- антивирусное сканирование по команде пользователя или администратора;
- антивирусное сканирование по расписанию;
- защита от еще неизвестных вредоносных программ на основе эвристического анализа;
- обнаружение руткитов (скрытых файлов/системных аномалий);
- антивирусная проверка и лечение файлов, упакованных программами;
- содержит HIPS для предотвращения попыток внешнего воздействия, а также для мониторинга процессов, файлов и ключей реестра;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- защита от вредоносных сценариев, загружаемых с веб-страниц и распознавание фишинг-сайтов;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- регулировка распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;
- настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта;
- блокировка сменных носителей информации и устройств;
- интеграция с центром безопасности операционной системы;
- самозащита антивирусных продуктов от вредоносных программ, злоумышленников или неквалифицированных пользователей;
- проверка трафика по протоколам IMAP, POP3 независимо от используемого почтового клиента;
- защита HTTP-трафика - проверка всех объектов, поступающих на компьютер пользователя по протоколу HTTP и FTP;
- защита зашифрованного трафика – протоколы HTTPS, POP3s;
- автоматическое скрывание уведомлений при работе антивируса в полноэкранном режиме;
- наличие множества путей уведомления администраторов о важных событиях, происходящих на серверах и рабочих станциях (почтовое сообщение, всплывающее окно, запись в журнал событий);
- наличие системы централизованного сбора с клиентских рабочих мест потенциально опасных образцов вредоносного кода и возможность

централизованно или вручную отправлять образцы вредоносного кода вирусным экспертам.

10.1.10 Требования к системе управления антивирусной защитой

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:

- масштабируемое решение;
- централизованная установка/обновление/удаление программных средств антивирусной защиты, настройки, администрирования;
- централизованный сбор информации и создание отчетов о состоянии антивирусной защиты;
- автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;
- доставка обновлений на рабочие места пользователей сразу после их получения;
- построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на носителях информации;
- механизм оповещения о событиях в работе установленных приложений антивирусной защиты и возможность настройки рассылки почтовых уведомлений о них;
- наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную;
- отсутствие дополнительных модулей (клиентов) на удаленном сервере/персональном компьютере для обеспечения удаленного администрирования;
- поддержка баз данных;
- осуществляет проверку актуальности критически важных обновлений.

10.1.11 Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- типы обновлений: обновление база данных сигнатур вирусов, программных компонентов, обновление ядра;
- пакеты обновления зеркала можно загружать двумя способами: по протоколу HTTP (рекомендуется) и с помощью общего сетевого диска (SMB);

– осуществляется проверка целостности и подлинности обновлений средствами электронной цифровой подписи.

10.1.12 Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать следующие документы:

- руководство пользователя (администратора);
- руководство администратора средств удаленного администрирования.

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты, а также изменений настроек.

10.1.13 Применение средств антивирусного контроля

Обновление антивирусных средств должно происходить в автоматическом режиме при загрузке вычислительной техники. Допускается работа антивируса с обновлениями не больше 72 часов.

Антивирусный контроль всех дисков и файлов вычислительной техники должен проводиться еженедельно в автоматическом режиме.

Внеочередной антивирусный контроль всех дисков и файлов вычислительной техники должен выполняться:

- непосредственно после установки (изменения) программного обеспечения на вычислительной техники;
- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);
- на каждой вычислительной технике в резидентном режиме должен быть запущен антивирусный монитор.

Обязательному антивирусному контролю подлежит любая информация (текстовые, файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях.

Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема.

Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на выделенной рабочей станции на отсутствие вирусов, после чего устанавливаться на сервер.

10.1.14 Применение систем резервного копирования данных

10.1.14.1 Требования к системе хранения данных

Требования к системе хранения данных:

- 1) наличие двух высокодоступных дисковых массивов;
- 2) резервирование критичных компонентов системы (блоки питания, жесткие диски, вентиляторы и т.д.) с возможностью горячей замены;
- 3) наличие не менее двух дисковых накопителей горячей замены;
- 4) иметь модульную архитектуру;
- 5) поддерживать возможность подключения серверов с различными операционными системами через одни и те же каналы Fibre Channel;
- 6) обеспечивать возможность одновременного использования дисков различного объема в одном дисковом массиве;
- 7) обеспечивать возможность балансировки нагрузки между каналами подключения для каждого из подключаемых к массиву серверов;
- 8) обеспечивать возможность балансировки нагрузки на дисковые накопители;
- 9) возможность динамической смены ролей томов и направления передачи данных без проведения ресинхронизации данных;
- 10) возможность реализации собственными аппаратно - программными средствами дисковых массивов локального и удаленного копирования данных без использования ресурсов внешних серверов;
- 11) поддерживать передачу данных в резервный центр в синхронном режиме;
- 12) иметь возможность добавления поддержки асинхронного режима. Предоставлять возможность мгновенного переключения между синхронным и асинхронным режимом для любой пары томов;
- 13) в случае множественного сбоя дисковых накопителей, хранящих основной том, обеспечивать автоматическое получение данных из резервной системы хранения через основную систему хранения прозрачно для серверов;
- 14) наличие не менее двух независимых путей подключения дисковых массивов к серверам кластерных узлов;
- 15) данные из кэш-памяти должны быть защищены от длительного потери питания;
- 16) возможность создания моментальных снимков дискового пространства с целью восстановления работоспособности системы в случае сбоя в кратчайшие сроки. Копии не должны занимать столько же дискового пространства, как основные тома, сохраняя только измененные на основном томе данные. Необходимо описать процедуру создания момен-

тальных снимков дискового пространства, их отображения и процедуру восстановления данных с их использованием;

17) иметь конфигурацию, программное обеспечение и лицензии на его использование, позволяющие осуществлять мониторинг состояния массива и изменение его конфигурации, осуществлять мониторинг производительности массива, коммутаторов Fibre Channel и подключенных серверных платформ, управление правами доступа к логическим томам в системе хранения;

18) наличие резервного объема дискового пространства равного двукратному объему промышленной базы данных;

19) возможность наращивания дискового пространства в 3-4 раза путем добавления дисковых накопителей, дисковых корзин, контроллеров массива, увеличения объема кэш-памяти и каналов ввода/вывода;

20) наличие необходимого количества коммуникационного оборудования сети хранения данных;

21) возможность замены или добавления любого компонента, а также смены версии системного программного обеспечения без прекращения доступности дискового массива.

10.1.14.2 Требования к системе резервного копирования и архивирования

Требования к системе резервного копирования и архивирования следующие:

1) наличие типовой стратегии резервного копирования и восстановления СУБД приложений датацентра для реализуемой конфигурации программно-аппаратных средств, согласованных со службой технической поддержки и обеспечивающую восстановление бизнес - данных «на момент сбоя» за минимальное время;

2) должна быть предусмотрена возможность обеспечения резервного копирования базы данных без остановки СУБД;

3) наличие заявленного соотношения между прогнозируемым временем восстановления и объемами восстанавливаемых данных СУБД (необходимо указать);

4) время восстановления баз данных при сбое не должно превышать 2 часов;

5) минимальная производительность ленточной библиотеки при чтении или записи компрессированных данных не менее 1 Tbite/h;

6) должна быть подключена к сети хранения данных напрямую через Fiber Channel и передавать данные напрямую со всех серверов, подключенных к дисковой системе хранения;

7) наличие необходимого количества программного обеспечения резервного копирования и лицензий к нему;

8) наличие необходимого количества ленточных библиотек резервного копирования исходя из необходимости хранения как минимум 5 резервных копий;

9) наличие оборудования долговременного хранения данных на внешних носителях информации (юридическое архивирование). Данное оборудование должно обеспечивать запись на носители информации (желательно перезаписываемые), имеющие гарантийный срок хранения информации не менее 10 лет.

Наличие в программном обеспечении управления комплексом юридического архивирования механизма создания минимум двух копий информации с возможностью извлечения из библиотеки и транспортировки одной из копий на удаленную площадку, а также механизма поиска и восстановления архивированной информации.

10.1.14.3 Виды резервного копирования

Полное резервное копирование. Полное копирование обычно затрагивает всю систему и все файлы. Еженедельное, ежемесячное и ежеквартальное резервное копирование подразумевает создание полной копии всех данных. Обычно копирование выполняется по пятницам или в течение выходных, когда копирование большого объема данных не влияет на работу датацентра. Последующие резервные копирования, выполняемые с понедельника по четверг до следующего полного копирования, могут быть дифференциальными или инкрементными, главным образом для того, чтобы сохранить время и место на носителе. Полное резервное копирование следует проводить, по крайней мере, еженедельно.

Дифференциальное резервное копирование. При разностном (дифференциальном) резервном копировании каждый файл, который был изменен с момента последнего полного резервного копирования, копируется каждый раз заново. Дифференциальное копирование ускоряет процесс восстановления. Все, что необходимо - это последняя полная и последняя дифференциальная резервная копия.

Инкрементное резервное копирование. При добавочном («инкрементном») резервном копировании происходит копирование только тех файлов, которые были изменены с тех пор, как в последний раз выполнялось полное или добавочное резервное копирование. Последующее инкрементное резервное копирование добавляет только файлы, которые были изменены с момента предыдущего. В среднем, инкрементное резервное копирование занимает меньше времени, так как копируется меньшее количество файлов. Однако, процесс восстановления данных занимает больше времени, так как должны быть восстановлены данные последнего полного резервного копирования, плюс данные всех последующих инкрементных резервных копирований. При этом, в отличие от дифференциального копирования, изменившиеся или новые файлы не замещают старые, а добавляются на носитель независимо.

Клонирование. Клонирование позволяет скопировать целый раздел или носитель (устройство) со всеми файлами и директориями в другой раздел или на другой носитель. Если раздел является загрузочным, то клонированный раздел тоже будет загрузочным.

Резервное копирование в виде образа. Образ - точная копия всего раздела или носителя (устройства), хранящаяся в одном файле.

Резервное копирование в режиме реального времени. Резервное копирование в режиме реального времени позволяет создавать копии файлов, директорий и томов, не прерывая работу, без перезагрузки компьютера.

10.1.15 Дополнительные требования

Комплекс технических (аппаратно-программных) средств защиты дополнительно могут включать:

- локальное резервное копирование данных для их быстрого восстановления;
- удаленное резервное копирование данных для обеспечения катастрофоустойчивости;
- разделение трафика с помощью виртуальных сетей, построенных с использованием коммутаторов;
- использование авторизованных сертификатов SSL;
- средства аутентификации пользователей и элементов (рабочих станций, задач, элементов баз данных и т.п.);
- средства поиска и обнаружения уязвимостей;
- средства защиты от несанкционированного доступа.

10.1.16 Ответственность

Лица, имеющие доступ к средствам защиты (технические, аппаратно-программные) датацентра несут ответственность за:

- надлежащее выполнение функциональных обязанностей сотрудников и ответственных за обеспечение информационной безопасности датацентра;
- обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации в рамках своей компетенции.

10.2 Правила доступа пользователей и обслуживающего персонала в датацентр

10.2.1 Общие положения

Данный пункт описывает порядок доступа обслуживающего персонала (администратор, техник, электрик и пр.) и пользователей к датацентру (серверам информационной системы организации).

Под «физическим доступом к датацентру организации» подразумевается любой доступ, имеющий возможность непосредственного физического контакта с датацентром организации.

Защита физического доступа в помещении датацентра обеспечивается наличием физической охраны, охранной сигнализации, железных дверей, СКУД и системы видеонаблюдения.

Подсистема контроля и управления доступом должна исключить попадание в серверную лиц, в чьи обязанности не входит монтаж, эксплуатация и техническое обслуживание размещённого в серверной оборудования.

Для идентификации допущенных лиц применяются следующие средства:

- ключи от механических замков;
- кодонаборные панели;
- карты и метки электронной идентификации;
- биометрическая идентификация;
- комбинация вышеперечисленных методов.

Для блокирования доступа в помещение могут применяться:

- механические замки;
- электромеханические замки;
- электромагнитные замки;
- комбинация вышеперечисленных средств.

Охранная сигнализация серверной должна быть выполнена отдельно от систем безопасности здания. Сигналы оповещения выводятся в помещение круглосуточной охраны в виде отдельного пульта. Дополнительно сигналы оповещения могут доставляться средствами телекоммуникаций: телефон, Internet и пр.

Контролю и охране подлежат все входы и выходы серверной, объем помещения, оконные проемы (при наличии).

Подсистема охранной сигнализации должна иметь собственный источник резервного питания.

10.2.2 Основные требования

Право доступа в помещение датацентра разграничивается использованием СКУД.

Физический доступ в помещение датацентра осуществляется только на основании списка допуска.

Сотрудники, указанные в списке допуска, должны проходить регистрацию в системе СКУД.

В случае возникновения необходимости доступа в помещение датацентра лицам, не входящим в список допуска, оформляется заявка с обоснованием физического доступа. Данная заявка рассматривается и подписывается руководителем подразделения датацентра, согласовывается с руководителем службы информационной безопасности. При наличии разрешительного документа лица, которым не разрешен физический доступ в

помещение датацентра, должны сопровождаться дежурным администратором.

Для входа в помещении датацентра сотрудники, состоящие в списке допуска, должны использовать карточку системы СКУД

Находясь в помещении датацентра, сотрудник по завершению необходимых работ должен произвести отметку в журнале регистрации посещений помещений датацентра. Выходя, сотрудник должен убедиться в закрытии дверей помещения датацентра.

Для проведения работ в помещении датацентра лица, не входящие в список допуска (таблица 1), должны иметь разрешительный документ. Работы в помещении датацентра указанными лицами разрешается только в сопровождении дежурного администратора. Журнал регистрации посещений помещений датацентра должен содержать данные, в которых отражаются дата, время входа/выхода в помещения датацентра, наименование проводимых работ, фамилия, инициалы и должность, подпись.

Таблица 1 - Перечень работ, требующих физического доступа к датацентру

Наименование работ	Описание	Ответственные за выполнение	Обоснование для физического доступа
Перезагрузка сервера	Выполняется нажатием кнопки Reset на сервере	Дежурный администратор	Невозможность выполнения перезагрузки удаленным способом
Работы по техническому обслуживанию серверов	Замена, установка, переустановка оборудования и программного обеспечения	Дежурный администратор	Работа с серверным оборудованием невозможна без физического контакта
Работы обслуживающего персонала	Уборка серверного помещения	Обслуживающий персонал	Работа непосредственно в помещении с серверным оборудованием, невозможна без физического контакта

Контроль организации порядка доступа работников и анализ данных, полученных от СКУД, журнала учета посещений помещений датацентра и

системы видеонаблюдения проводятся сотрудниками службы информационной безопасности.

10.2.3 Ответственность

Лица, имеющие доступ в помещение датацентра, несут ответственность за:

- надлежащее выполнение функциональных обязанностей сотрудников и ответственных за обеспечение информационной безопасности датацентра;
- обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции.

10.3 Правила видеонаблюдения в помещениях датацентра

10.3.1 Общие положения

Построение системы видеонаблюдения необходимо осуществлять на основе оборудования и с подключением к объектовой системе видеонаблюдения.

Под видеонаблюдением серверной, подразумевается любое наблюдение, имеющее возможность просмотра непосредственного физического контакта с серверами организации.

Защита с видеонаблюдением в помещении датацентра обеспечивается наличием видеокамер.

10.3.2 Основные требования

В целях безопасности, в серверном помещении видеокамеры должны обеспечивать выполнение следующих требований: располагаться таким образом, чтобы избежать мертвых зон и иметь функцию ночного видения. Системы видеонаблюдения должны располагаться таким образом, чтобы в зону их действия не входила территория или объекты, которые не представляют никакого интереса для осуществления контроля.

Разрешения видеокамер должно быть достаточным, чтобы уверенно различать лица сотрудников, обслуживающих технологическое оборудование.

Оборудование должно иметь возможность подключения к нескольким типам каналов передачи данных (основной и резервный), а также должно быть защищено от внешних воздействий и иметь возможность энергонезависимой автономной работы в течение 2 часов с момента прекращения электропитания. В случае отключения основного канала передачи данных видеoinформация должна автоматически передаваться по резервному каналу.

Оборудование должно быть простым в монтаже и демонтаже, а также масштабируемым.

Вероятность безотказной работы средств видеонаблюдения и трансляции видеоизображения при работе должна составлять не менее 0,999 часов (отказ одного объекта из 1000 в течение всего времени работы).

Наработка средств видеонаблюдения и трансляции видеоизображения на сбой должна быть не менее 1000 часов (сбой может произойти не чаще, чем через 1000 часов работы).

Наработка средств видеонаблюдения и трансляции видеоизображения до отказа должна быть не менее 2000 часов (отказ может произойти не чаще, чем через 2000 часов работы).

Средства видеонаблюдения должны быть работоспособны при предельно допустимых отклонениях значений напряжения питания электрической сети 187 V и 242 V.

Средства видеонаблюдения должны быть работоспособны при предельно допустимых значениях температуры окружающего воздуха 0°C и 60°C.

10.3.3 Ответственность

Лица, имеющие доступ к средствам видеонаблюдения датацентра, несут ответственность за:

- надлежащее выполнение функциональных обязанностей сотрудников и ответственных за обеспечение информационной безопасности датацентра;
- обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции.

10.4 Требования к системе охранной сигнализации датацентра

10.4.1 Общие положения

Система охранной сигнализации серверных организации предназначена для обнаружения попыток и (или) фактов проникновения в охраняемые зоны и информирования о данных событиях персонала охраны для осуществления им соответствующих адекватных действий; а также автоматического формирования необходимых команд управления на исполнительные устройства.

10.4.2 Основные требования

Система охранной сигнализации должна обеспечивать ограничение доступа лиц в помещения датацентра.

Система охранной сигнализации должна обеспечивать выполнение следующих требований:

- полный охват контролируемой зоны;
- исключение не обнаруживаемого обхода преграды нарушителем;

- избирательность и чувствительность к присутствию, перемещению и другим действиям нарушителя;
- исключение «мертвых зон»;
- работоспособность в заданных климатических условиях;
- устойчивость к случайным помехам;
- требуемое время обнаружения нарушителя, определяемое регламентами мероприятий по комплексной безопасности;
- возможность централизованного контроля события;
- передача информации в общую охранную сигнализацию здания;
- ведение архива всех событий, происходящих в системе, с фиксацией всех необходимых сведений для их последующей однозначной идентификации (тип и номер устройства, тип и причина события, дата и время его наступления и т.п.);

10.4.3 Ответственность

Лица, имеющие доступ к системе охранной сигнализации датацентра, несут ответственность за:

- надлежащее выполнение функциональных обязанностей сотрудников и ответственных за обеспечение информационной безопасности датацентра;
- обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции.

10.5 Требования назначения системы тревожно-вызывной сигнализации

10.5.1 Общие положения

Система тревожно-вызывной сигнализации в серверных организации предназначена для экстренного вызова групп оперативного реагирования подразделений охраны, выдачи сигнала о работе «по принуждению», а также для контроля жизнедеятельности охраны и контроля прохода патруля по заранее заданному маршруту.

10.5.2 Основные требования

Система тревожно-вызывной сигнализации должна обеспечивать выполнение следующих требований:

- информирование персонала системы физической защиты о срабатывании устройств тревожно-вызывной сигнализации;
- определение места вызова;
- скрытность установки и удобство пользования вызывным устройством;
- невозможность отключения устройств тревожно-вызывной сигнализации;

- отличительность сигналов срабатывания устройств, тревожно-вызывной сигнализации от сигналов срабатывания система охранной сигнализации;
- контроль жизнедеятельности операторов пультов управления, охран (техническими средствами или организационными мероприятиями);
- информация, поступающая в центральный пункт управления, локальный пункт управления от устройств тревожно-вызывной сигнализации, должна быть приоритетной по сравнению с сигналами, поступающими от других технических средств физической защиты.

10.5.3 Ответственность

Лица, имеющие доступ к системе тревожно-вызывной сигнализации датацентра, несут ответственность за:

- надлежащее выполнение функциональных обязанностей сотрудников и ответственных за обеспечение информационной безопасности датацентра;
- обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции.

10.6 Подсистема пожарной сигнализации

Подсистема пожарной сигнализации помещения серверной должна быть выполнена отдельно от пожарной сигнализации здания (офиса).

В помещении серверной должны быть установлены два типа датчиков: температурные и дымовые.

Датчики должны контролировать как общее пространство помещений, так и полости, образованные фальшполом и фальшпотолком.

Сигналы оповещения подсистемы пожарной сигнализации выводятся на отдельный пульт в помещение круглосуточной охраны.

Подсистема пожарной сигнализации может быть объединена с подсистемой охранной сигнализации серверной.

10.7 Подсистема газового пожаротушения

Серверная оборудуется автоматической установкой газового пожаротушения, независимой от системы пожаротушения здания.

Модуль подсистемы газового пожаротушения размещается непосредственно в помещении серверной в специально оборудованном для этого шкафу.

Запуск подсистемы газового пожаротушения производится от датчиков раннего обнаружения пожара, реагирующих на появление дыма, а также от ручных извещателей, расположенных у выхода из помещения.

Подсистема газового пожаротушения должна иметь табло оповещения персонала о срабатывании автоматической установки газового пожаротушения, размещаемые внутри и снаружи помещения.

Подсистема газового пожаротушения должна обеспечивать подачу команд на закрытие защитных клапанов подсистемы вентиляции и отключение питания оборудования.

10.8 Подсистема газо-дымоудаления

Подсистема газо-дымоудаления обеспечивает отвод дыма и газа из помещения серверной после срабатывания подсистемы газового пожаротушения.

Подсистема выполняется отдельно от системы вентиляции здания с выводом воздуховода на крышу здания.

Подсистема должна обеспечивать отвод газозвдушной смеси в объеме, втрое превышающем объем серверной.

Допускается использование переносных дымососов

10.9 Мониторинг состояния обеспечения информационной безопасности в датацентре

10.9.1 Основные требования

Система мониторинга состояния обеспечения информационной безопасности в датацентре должна обеспечивать выполнение следующих требований:

- мониторинг состояния программного обеспечения и технических средств;
- мониторинг и управление активным сетевым оборудованием;
- постоянное отслеживание уязвимостей, новых типов атак, оперативное обновление программных средств;
- периодическое тестирование системы безопасности с имитацией различных типов воздействия;
- оперативное реагирование на возникающие угрозы и на попытки вторжения;
- инвентарный учет и управление изменениями в информационной системе;
- контроль и централизованное распространение программного обеспечения;
- консолидация задач мониторинга, корпоративное представление и автоматический анализ (корпоративная консоль);
- автоматизация системы контроля прав доступа пользователей;
- сбор и анализ статистики, отчетность и поддержка принятия решений по обслуживанию программного обеспечения и комплекса технических средств в помещениях датацентра, в том числе для проактивного

управления, т.е. выявление возможных проблем на ранней стадии и недопущение возникновения критических ситуаций;

- автоматизированный мониторинг и учет всех действий персонала и посетителей датацентра.

10.9.2 Ответственность

Лица, осуществляющие мониторинг состояния обеспечения информационной безопасности датацентра, несут ответственность за:

- не надлежащее выполнение функциональных обязанностей сотрудников и ответственных за обеспечение информационной безопасности датацентра;

- не обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции.

Республика Армения
Служба государственной безопасности
Управление по обеспечению безопасности
Информационно-коммуникационных систем
Датум: 10.09.2014

Приложение А (справочное)

Выбор местонахождения и проектов зданий для датацентров

А.1 Архитектурные факторы, учитываемые при выборе объекта

При проектировании датацентра необходимо предусмотреть возможность подъезда к зданию с разных дорог.

У здания должна быть предусмотрена автостоянка (парковка) оптимальных размеров, отвечающая всем требованиям.

Здание должно иметь достаточно большую погрузочно-разгрузочную площадку, грузовой лифт и место для приёма всех ожидаемых поставок расходных материалов и оборудования.

Серверную следует располагать вдали от таких источников электромагнитных и радиационных помех, как рентгеновское оборудование, радиопередатчики и трансформаторы.

Датацентр и всё вспомогательное оборудование должны быть расположены выше самого высокого ожидаемого уровня паводковых вод. Не допускается размещать критически важное электронное, электрическое или механическое оборудование в подвальных этажах.

Помещение должно быть, по возможности, без оконных проемов с глухими стенами. Если в предполагаемом помещении для серверной всё же есть окна, их следует снабдить защитным покрытием, исходя из соображений безопасности и для уменьшения нагрева от солнечных лучей.

А.2 Факторы электроснабжения, учитываемые при выборе объекта

Система электроснабжения должна удовлетворять всем начальным и будущим потребностям датацентра в энергоснабжении. В соответствующих случаях следует предусмотреть возможность и экономическую целесообразность использования дублированных питающих линий, возможно, от разных подстанций общедоступной сети. Если система электроснабжения не может предоставить достаточную мощность, на объекте должна быть предусмотрена возможность поддержки оборудования для самостоятельной, совместной или распределённой выработки электроэнергии. Предпочтительно получать энергию по подземным, а не по воздушным (наземным) питающим линиям, это сводит к минимуму подверженность воздействию молний, деревьев, дорожных аварий и вандализма.

Система электроснабжения должна удовлетворять всем начальным и будущим потребностям датацентра в энергоснабжении. В соответствующих случаях следует предусмотреть возможность и экономическую целесообразность использования дублированных питающих линий, возможно, от разных подстанций общедоступной сети. Если система электроснабжения не может предоставить достаточную мощность, на объекте должна быть предусмотрена возможность поддержки оборудования для самостоятельной, совместной или распределённой выработки электроэнергии. Предпочтительно получать энергию по подземным, а не по воздушным (наземным) питающим линиям, это сводит к минимуму подверженность воздействию молний, деревьев, дорожных аварий и вандализма.

А.3 Физические и механические факторы, учитываемые при выборе объекта

В случае если одно здание арендуют несколько арендаторов, необходимо выделить место на крыше или на уровне земли для установки оборудования для отвода тепла из системы кондиционирования воздуха – конденсоров, башенных охладителей или охладителей с сухим/жидкостным охлаждением.

Если здание имеет действующую систему пожаротушения, её легко модифицировать, превратив в спринклерную систему упреждающего действия, предназначенную для датацентра. Если здание имеет действующую систему кондиционирования воздуха, обслуживающую датацентр, это должна быть система такого типа, который пригоден для датацентров, из расчёта не менее 10 tf/m^2 , включая площадь как серверной, так и подсобных помещений.

А.4 Учёт наличия телекоммуникаций при выборе объекта

Здание должно обслуживаться, по крайней мере, двумя комнатами ввода оптических кабелей, проложенных по разным маршрутам. Эти комнаты ввода должны быть подключены к двум разным офисам провайдера доступа.

Несколько провайдеров доступа должны предоставлять услуги или иметь возможность обслуживать это здание без проведения серьёзных строительных работ или без задержек при получении разрешений.

Датацентр должен обслуживаться специально выделенным оборудованием провайдера доступа, расположенным в помещении датацентра, а не в помещении совместного пользования с другими арендаторами. Внешние кабели провайдера доступа должны быть заключены в кабелепровод внутри здания, оставаясь недоступными для других арендаторов в тех местах, где они проложены в общих с другими арендаторами кабелепроводах. Здание должно иметь специальные кабелепроводы, обслуживающие пространство датацентра.

А.5 Выбор объекта с точки зрения его безопасности

Если охлаждающее оборудование, генераторы, топливные баки или оборудование провайдера доступа располагаются вне помещения, принадлежащего клиенту, то это оборудование должно быть надлежащим образом защищено.

Также владельцу датацентра необходим постоянный круглосуточный доступ к этому месту.

Должно быть обеспечено постоянное наблюдение с помощью видеокамер за зонами общего пользования, включая автостоянки, погрузочно-разгрузочные площадки и входы в здание.

Серверную не следует проектировать в непосредственной близости от автостоянки.

Объект не должен находиться в зоне, где за последние 100 лет случилось наводнение, вблизи активного геологического разлома, на холме, подверженном оползням, у нижнего бьефа плотины или вниз по направлению потока от водонапорной башни. Кроме того, поблизости не должно быть зданий, которые при землетрясении подвержены разрушению.

Объект должен быть не менее чем на 0,8 km удален от железных дорог и крупных автомагистралей, это сведёт к минимуму риск разлива химических реагентов.

Объект должен быть не менее чем на 0,4 km удален от аэропортов, исследовательских лабораторий, химических заводов, мусорных свалок, рек, береговой линии моря и плотин.

Объект должен быть не менее чем на 0,8 km удален от военных баз.

Объект должен быть не менее чем на 1,6 km удален от ядерных реакторов, военных заводов и оборонных (ракетных) установок.

Объект не должен соседствовать с каким-либо иностранным посольством.

Объект не должен быть расположен в районе с высокой преступностью.

А.6 Прочие требования

При выборе участка для размещения датацентра следует учитывать следующие дополнительные критерии:

- риск загрязнения;
- близость пунктов милиции, пожарных частей и больниц;
- общий доступ;
- приказы о районировании;
- вибрации;
- экологические проблемы;
- возможности иного использования здания после того, как отпадёт нужда в датацентре («стратегии выхода»).

JOHN STEPHEN LEGGARD

Приложение В (справочное)

Примеры проектов датацентров

В.1 Пример проекта малого датацентра

Рекомендуется в серверном помещении малого датацентра для вентиляции на «горячем проходе» предусмотреть несколько вентиляционных люков/шахт для предотвращения повышенной влажности воздуха и сокращения количества частиц пыли.

На рисунке В.1 приведена схема планировки серверной с указанием «горячих» и «холодных» проходов.



Рисунок В.1 - Схема планировки серверной с указанием «горячих» и «холодных» проходов

Площадь серверной составляет примерно 1920 м². В нём находятся 73 шкафа с серверами в аппаратных и шесть девятнадцатидюймовых стоек в главной распределительной зоне. Шесть стоек главной распределительной зоны – это шесть стоек с коммутационными панелями и панелями переключений. Главную распределительную зону не обязательно размещать в центре серверной, поскольку отсутствуют ограничения по длине. Однако, разместив главную распределительную зону в центре серверной можно уменьшить длины кабелей и избежать скопления кабелей в проходах, перпендикулярных проходам между шкафами.

Главная распределительная зона поддерживает горизонтальную коммутационную панель, откуда идёт горизонтальная кабельная система к аппаратным. В датацентрах с высокой плотностью кабельной системы к серверным шкафам необходимо организовать горизонтальные распределительные зоны, чтобы свести к минимуму скопление кабелей вблизи главной распределительной зоны.

Ряды стоек и шкафов расположены параллельно направлению воздушного потока под полом, создаваемого кондиционерами для серверной. Каждый кондиционер для серверной расположен навстречу «горячему» проходу, это обеспечивает более эффективный поток возвратного воздуха к каждому кондиционеру.

Серверные шкафы расположены таким образом, что они образуют чередующиеся «горячие» и «холодные» проходы.

Коммуникационные кабели проложены в проволочных лотках (корзинах) в «горячих» проходах. Силовые кабели идут под фальшполом в «холодных» проходах.

Серверная отделена от центра сетевых операций для контроля доступа и во избежание загрязнения воздуха.

В.2 Пример проекта корпоративного датацентра

Ниже приведён пример Интернет датацентра или датацентра Интернет-хостинга, используемого для размещения вычислительного и оборудования телекоммуникаций для нескольких корпоративных веб-сайтов (узлов WWW).

Этот корпоративный датацентр расположен на двух этажах площадью 4140 м² каждый. Этот датацентр является примером датацентра с несколькими горизонтальными распределительными зонами, отличающимися друг от друга главным образом типом систем, которые они поддерживают. В связи с высокой плотностью кабельных линий к серверам на базе персональных компьютеров, эти системы обслуживаются двумя горизонтальными распределительными зонами, каждая из которых поддерживает только 24 серверных шкафа. Запланированы семь дополнительных горизонтальных распределительных зон для поддержки дополнительных серверных шкафов. Таким образом, горизонтальные распределительные зоны могут потребоваться не только для разных функциональных зон, но также для минимизации скопления кабелей в горизонтальной распределительной зоне. Каждая горизонтальная распределительная зона была рассчитана на поддержку не более 2000 четырёхпарных кабелей категории 6.

На первом этаже находятся комнаты электриков, комнаты механиков, складские помещения, погрузочно-разгрузочная площадка, комната для средств обеспечения безопасности, приёмная зона для посетителей, операционный центр и комната ввода внешних сервисов.

Серверная находится на втором этаже и имеет на всей площади фальшполы. Вся телекоммуникационная кабельная система проходит под фальшполом в проволочных лотках. В некоторых местах, где объём кабелей наибольший и где они не препятствуют воздушному потоку, кабельные лотки установлены в два яруса. На рисунке В.2 приведен пример корпоративного датацентра.

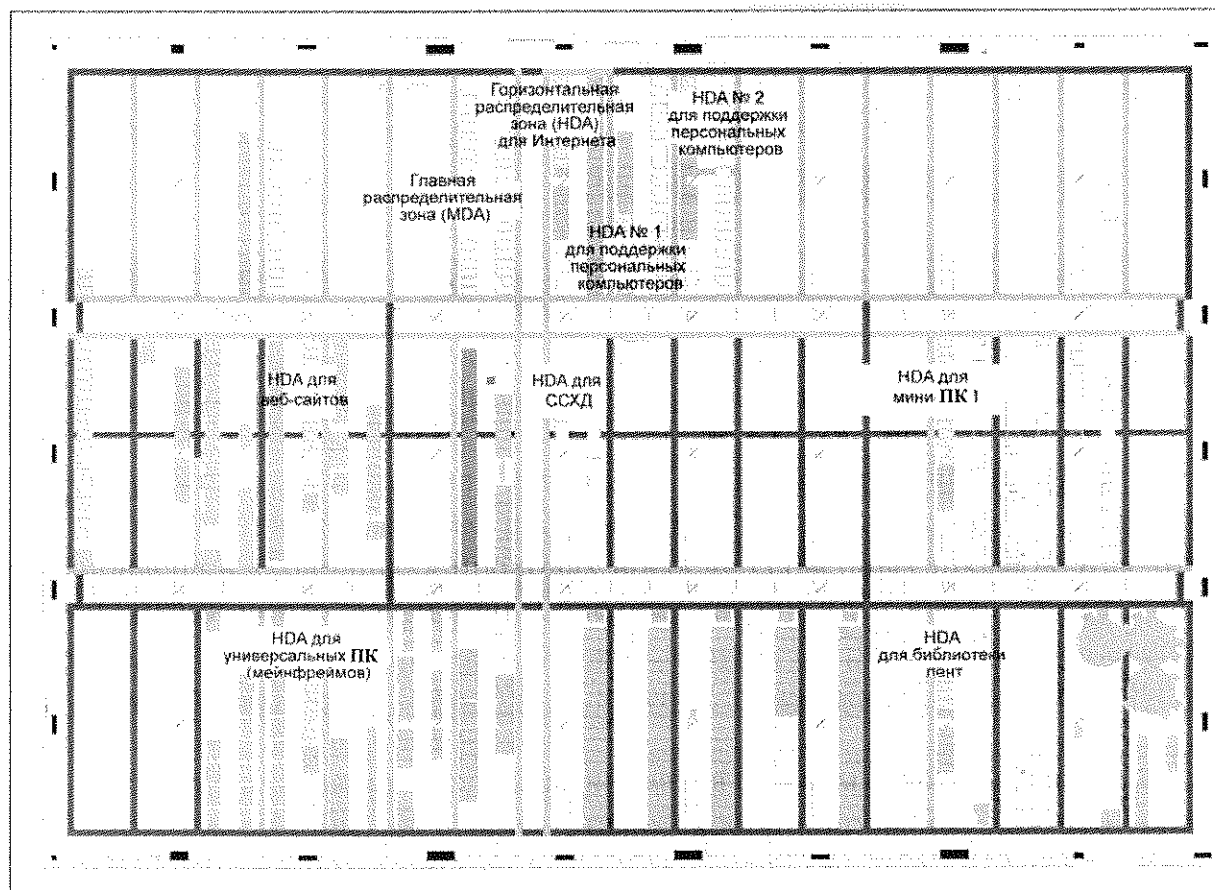


Рисунок В.2 - Пример корпоративного датацентра

Телекоммуникационная кабельная система установлена в «горячих» проходах позади серверных шкафов. Электрическая кабельная система установлена в «холодных» проходах впереди серверных шкафов. Как телекоммуникационные, так и электрические кабели идут вдоль главных проходов в направлении запад/восток, но следуют по отдельным кабелепроводам, сохраняющим отделение силовой и телекоммуникационной разводок.

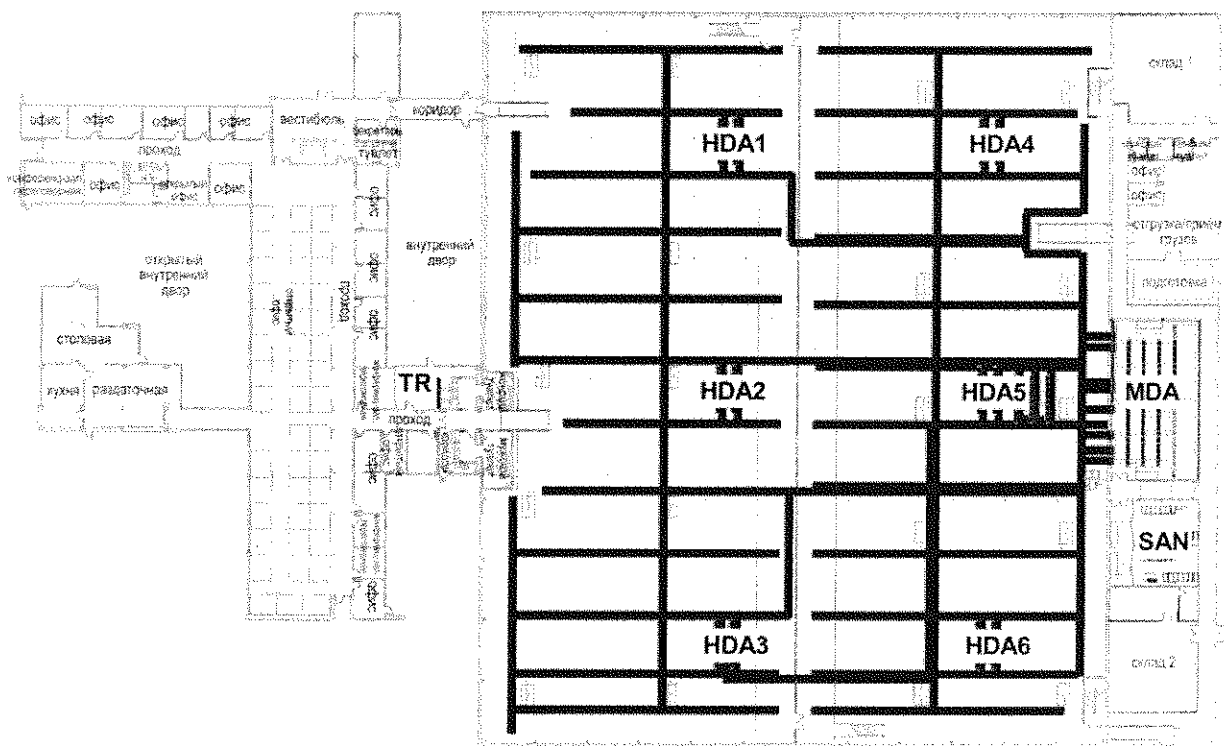
Места размещения комнаты ввода на первом этаже и главной распределительной зоны на втором этаже скоординированы, так что линии Т-1 и Т-3 можно терминировать на оборудовании в любом месте серверной.

Шкафы для серверов стоечного монтажа имеют стандартизованную кабельную систему, здесь применяются многомодовое волокно и неэкранированные кабели «витая пара» категории 6.

В этом датацентре, в связи с большим количеством требований к кабельной системе для напольных систем, было невозможно разработать стандартизованную конфигурацию зонных розеток.

В.3 Пример проекта Интернет-датацентра

Интернет-датацентр в этом примере занимает один этаж площадью около 9500 м² с серверным помещением площадью около 6400 м². Это пример датацентра, в котором горизонтальные распределительные зоны отличаются друг от друга главным образом зонами, которые они обслуживают, а не типом систем, которые они поддерживают. На рисунке В.3 приведен план занимаемого датацентром этажа с кабельными лотками. Стойки главной и горизонтальной распределительных зон приведены, а клиентские стойки и шкафы – нет.



HDA (Horizontal Distribution Area) - горизонтальная распределительная зона,
MDA (Main Distribution Area) - главная распределительная зона

Рисунок В.3 - Пример Интернет-датацентра

Главная распределительная зона включает в себя функции комнаты ввода и основной (главной) кросс-панели. Она вмещает 50 стоек провайдеров доступа и 20 стоек для основной (главной) кросс-панели. Эта комната

поддерживается двумя специально выделенными распределительными щитами питания, двумя специально выделенными кондиционерами и имеет фальшполы. Главная распределительная зона находится в специально выделенном помещении с отдельным входом, что позволяет провайдерам доступа и поставщикам услуг работать в этой комнате, не заходя в компьютерные зоны главной серверной. Места расположения главной и горизонтальной распределительных зон планировались таким образом, чтобы допустимые значения длины линий T-1 и T-3 не были превышены для линий, идущих к любой стойке серверной.

Автоматические библиотеки лент, серверы хранения данных и оборудование управления для систем хранения данных находятся в специально выделенной комнате ССХД, смежной с главной распределительной зоной. Это оборудование поставляется и управляется посторонними организациями, а не владельцами Интернет-датацентра. Отдельная комната для этого оборудования позволяет поставщикам услуг по хранению данных управлять своим оборудованием, не заходя в главную серверную.

Пространство серверной вмещает 4300 клиентских стоек. Клиентское пространство поддерживается шестью горизонтальными распределительными зонами, чтобы ограничить объём кабельной системы в проходящих под полом кабельных лотках. Каждая горизонтальная распределительная зона поддерживает примерно 2000 подключений медных пар. Эти горизонтальные распределительные зоны размещены в средней части обслуживаемых ими зон, чтобы свести к минимуму длины кабелей. Кабельная система от горизонтальной распределительной зоны к клиентским стойкам стандартизована с целью упрощения организационного управления. Однако при необходимости можно проложить дополнительную кабельную систему к клиентским стойкам.

Телекоммуникационная кабельная система к зонам складирования и подготовки поддерживается из главной распределительной зоны. Телекоммуникационная кабельная система к офисам поддерживается из телекоммуникационных помещений.

ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ
ОБЪЕДИНЕННЫЙ ЦЕНТРАЛЬНЫЙ

Приложение С (справочное)

Площади для датацентров

Датацентр должен иметь складское помещение достаточных размеров, чтобы оборудование в ящиках, запасные воздушные фильтры, запасные плитки пола, запасные кабели, запасное оборудование, запасные носители и запасы бумаги можно было хранить вне серверной. Датацентр должен иметь также подготовительную зону для распаковывания и, возможно, тестирования нового оборудования до того, как оно будет установлено в серверной. Есть возможность резко сократить количество частиц пыли в воздухе датацентра, если ввести правило распаковывать всё оборудование в складском помещении здания.

Требуемая площадь помещения тесно связана с планировкой этого помещения, включая не только расстановку стоек и/или шкафов для оборудования, но также кабельные организаторы и другие вспомогательные системы, например, систему электроснабжения, систему ОВиК и систему пожаротушения. Эти вспомогательные системы также предъявляют свои требования к пространству, которые зависят от необходимого уровня резервирования.

Если новый датацентр заменяет один или несколько существующих датацентров, то оценить размеры этого датацентра можно посредством инвентаризации оборудования, которое будет размещено в новом датацентре, и составления поэтажного плана нового датацентра с имеющимся в наличии оборудованием и планируемым к размещению оборудованием, учитывая при этом необходимое расстояние между оборудованием. Поэтажный план должен также учитывать любые планируемые изменения технологии, которые могли бы повлиять на размеры оборудования, подлежащего установке в новом датацентре. В поэтажном плане нового датацентра необходимо учесть вспомогательное электрооборудование и оборудование системы ОВиК.

В связи с тем, что зачастую операционный центр и принтерную комнату необходимо размещать рядом с датацентром, соответственно следует проектировать их вместе с датацентром. Принтерную комнату следует отделить от главной серверной и снабдить отдельной системой ОВиК, поскольку принтеры генерируют бумажную и тонерную пыль, которая губительна для компьютеров.

За пределами серверной следует предусмотреть возможность для выделения отдельных комнат для оборудования таких систем, как система электропитания, система ОВиК, система пожаротушения. Несмотря на то, что при этом пространство используется не столь эффективно, повысится уровень безопасности, поскольку ни поставщикам, ни сотрудникам, обслуживающим это оборудование, не нужно входить в серверную.

Приложение D (справочное)

Уровни инфраструктуры датацентров

D.1 Общие положения

D.1.1 Общее представление о резервировании

Для повышения степени резервирования и надёжности следует исключить точки одиночных отказов как в самом датацентре и в поддерживающей инфраструктуре, так и во внешних сервисах и системе общего энергоснабжения.

Настоящий стандарт рассматривает четыре уровня, связанных с разной степенью готовности инфраструктуры оборудования датацентра.

D.1.2 Общая информация об уровнях

Настоящий стандарт описывает четыре уровня, связанных с разной степенью готовности инфраструктуры оборудования датацентра. Более высокие уровни соответствуют не только более высокой готовности, но также вызывают повышенные строительные затраты. Во всех случаях уровни с более высоким рейтингом включают в себя требования к уровням более низкого рейтинга.

Существуют разные рейтинги уровней для разных частей инфраструктуры датацентра. Например, для электрооборудования может быть рейтинговый уровень 3, но уровень 2 для механического оборудования. Однако общий рейтинг этого датацентра равен самому нижнему уровню по всем частям его инфраструктуры. Таким образом, если датацентр имеет уровень 4 для всех частей инфраструктуры, кроме электрооборудования, где рейтинг равен 2, то весь датацентр получает рейтинг 2. Общий рейтинг датацентра совпадает с рейтингом самого слабого компонента.

Следует уделять внимание поддержанию функциональных возможностей механической и электрической систем на правильном уровне, поскольку нагрузка на датацентр с течением времени возрастает. Датацентр может спуститься с уровня 3 или 4 до уровня 1 или 2 по мере того, как резервированная мощность будет использоваться для поддержки нового вычислительного и оборудования телекоммуникаций.

Чтобы получить оценку какого-либо уровня, датацентр должен соответствовать требованиям, изложенным в настоящем стандарте.

D.2 Резервирование

D.2.1 N - Базовое требование

Система соответствует основным (базовым) требованиям и не имеет резервирования (избыточности).

D.2.2 Резервирование N+1

Резервирование N+1 предусматривает один дополнительный узел, модуль, путь (канала, тракта) или одну систему в дополнение к тому минимуму, который нужен для удовлетворения базового требования. Отказ или ремонт (техническое обслуживание) любого одного узла, модуля или тракта не нарушает работу.

D.2.3 Резервирование N+2

Резервирование N+2 предусматривает два дополнительных узла, модуля, пути (канала, тракта) или две системы в дополнение к тому минимуму, который нужен для удовлетворения базового требования. Отказ или ремонт (техническое обслуживание) любых двух одиночных узлов, модулей или трактов не нарушает работу.

D.2.4 Резервирование 2N

Резервирование 2N предусматривает два комплектных узла, модуля, пути (канала, тракта) или две системы для каждого(-ой) одного(-ой), требуемого(-ой) для базовой системы. Отказ или ремонт (техническое обслуживание) любого одного целого узла, модуля, тракта или системы не нарушает работу.

D.2.5 Резервирование 2(N+1)

Резервирование 2(N+1) предусматривает два комплектных (N+1) узла, модуля, пути (канала, тракта) или две системы. Даже в случае отказа или ремонта (технического обслуживания) любого одного узла, модуля, тракта или системы будет обеспечено некоторое резервирование и работа не будет нарушена.

D.2.6 Возможность параллельного выполнения ремонта и тестирования

Оборудование можно ремонтировать, наращивать и тестировать без прерывания основной работы.

D.2.7 Производительность и масштабируемость

Датацентры и вспомогательную инфраструктуру следует проектировать так, чтобы они могли воспринять будущее наращивание без перерыва или с небольшим перерывом в предоставлении услуг.

D.2.8 Изолированность

Датацентры следует (по возможности) использовать только для тех целей, для которых они предназначены, и следует избавить от второстепенных операций.

Q'ZDST 245:2014
STATE STANDARD, DAVLAT
MAZORATI, Q'ZDST 245:2014
AXABBIT TEXNICIYALASCHI
JAHU BILAN KUTUBXONASI

D.2.9 Уровни инфраструктуры датацентра

D.2.9.1 Общие положения

Ниже описаны четыре уровня инфраструктуры датацентров:

1) датацентр уровня I: датацентр базового уровня. Датацентр уровня I подвержен нарушениям нормального хода работы из-за плановых и внеплановых действий. В нем находятся системы распределения электропитания и охлаждения компьютеров, но может не быть фальшполов, ИБП или генератора. Если даже есть ИБП или генераторы, то они представляют собой одномодульные системы и имеют много одиночных точек отказа. Ежегодно инфраструктуру приходится полностью выключать для выполнения работ по планово-предупредительному обслуживанию и профилактическому ремонту. При необходимости могут потребоваться более частые отключения. Ошибки при эксплуатации или самопроизвольные отказы компонентов инфраструктуры объекта будут вызывать перерывы нормального хода работы датацентра;

2) датацентр уровня II: датацентр с резервированными (избыточными) компонентами. Оборудование уровня II с избыточными компонентами несколько меньше подвержено нарушениям нормального хода работы от плановых и от внеплановых действий, чем базовый датацентр. В данном случае имеется фальшпол, ИБП и генераторы, однако проект имеет оценку N+1, что означает однопоточный путь распределения по всей площади. Техническое обслуживание и ремонт критического пути электроснабжения и других частей инфраструктуры объекта потребует остановки процесса обработки данных;

3) датацентр уровня III: датацентр с возможностью параллельного проведения ремонта. Возможности уровня III позволяют осуществлять любую плановую деятельность инфраструктуры объекта без какого-либо нарушения нормального хода работы технических средств серверной. К плановой деятельности относится профилактическое и программируемое техническое обслуживание, ремонт и замена компонентов, добавление или удаление компонентов, влияющих на производительность, тестирование компонентов и систем и пр. Необходимо иметь в наличии достаточную мощность и распределительные возможности, чтобы одновременно нести нагрузку на одном направлении и в то же время выполнять ремонт или тестирование на другом. Внеплановые действия, например ошибки при эксплуатации или самопроизвольные отказы компонентов инфраструктуры объекта всё же будут вызывать перерывы нормального хода работы датацентра. Объекты уровня III зачастую проектируют с перспективой наращивания ресурсов до уровня IV;

4) датацентр уровня IV: отказоустойчивый датацентр. Уровень IV предусматривает возможность проводить любую плановую деятельность без нарушения нормального хода работы. Отказоустойчивая функциональность также обеспечивает способность инфраструктуры объекта выдерживать, по крайней мере, один отказ (или событие) без последствий для кри-

тически важной нагрузки. Это требует одновременной активности путей распределения, обычно в конфигурации «Система+Система». С точки зрения электрооборудования, это означает наличие двух отдельных систем ИБП, в которых каждая система имеет резервирование N+1. При уровне IV всё техническое обеспечение серверной должно иметь двойной подвод питания.

Инфраструктура объекта уровня IV является наиболее совместимой с ИТ-концепцией высокой эксплуатационной готовности, которая использует кластеризацию центральных процессоров, запоминающие устройства с прямым доступом, матрицу независимых дисковых накопителей с избыточностью и дублированные коммуникации с целью достижения надёжности, готовности и ремонтнопригодности.

D.2.9.2 Датацентр уровня I – базового уровня

Датацентр уровня I – это датацентр базового уровня без резервирования (избыточности). Он имеет один путь для распределения электропитания и охлаждения без резервированных (избыточных) компонентов.

Датацентр уровня I подвержен нарушениям нормального хода работы как при плановых, так и при внеплановых действиях. Он имеет системы распределения электропитания и охлаждения компьютеров, ИБП и генераторы представляют собой одномодульные системы и имеют много одиночных точек отказа. Критически важные нагрузки могут быть подвержены отключению во время проведения работ по планово-предупредительному обслуживанию и профилактическому ремонту. Ошибки при эксплуатации или самопроизвольные отказы компонентов инфраструктуры объекта будут вызывать нарушения нормального хода работы датацентра.

D.2.9.3 Датацентр уровня II – с резервированными (избыточными) компонентами

Датацентр уровня II имеет один путь для распределения электропитания и охлаждения, но имеет резервированные (избыточные) компоненты на этом пути распределения.

Оборудование уровня II с избыточными компонентами несколько меньше подвержено нарушениям нормального хода работы от плановых и от внеплановых действий, чем базовый датацентр уровня II. Проектные возможности ИБП и генераторов имеют оценку N+1, что означает однопоточный путь распределения по всей площади. Техническое обслуживание и ремонт критического пути электроснабжения и других частей инфраструктуры объекта потребует остановки процесса обработки данных.

Содержит информацию
об объектах, находящихся в
подчинении, а также
о состоянии их работы
и о состоянии их
технического обслуживания

D.2.9.4 Датацентр уровня III – с возможностью параллельного проведения ремонтов

Датацентр уровня III имеет несколько путей распределения электропитания и охлаждения, но только один путь активен. Поскольку резервированные компоненты имеются не на одном пути распределения, эта система позволяет производить техническое обслуживание и ремонты параллельно с работой датацентра.

Возможности уровня III позволяют осуществлять любую плановую деятельность инфраструктуры объекта без какого-либо нарушения нормального хода работы технических средств серверной. К плановой деятельности относится профилактическое и программируемое техническое обслуживание, ремонт и замена компонентов, добавление или удаление компонентов, влияющих на производительность, тестирование компонентов и систем и пр. В датацентрах, использующих охлаждённую воду, это означает наличие двух независимых комплекта труб. Необходимо иметь в наличии достаточную мощность и распределительные возможности, чтобы одновременно нести нагрузку на одном пути и в то же время выполнять ремонт или тестирование на другом пути. Внеплановые действия, например ошибки при эксплуатации или самопроизвольные отказы компонентов инфраструктуры объекта, всё же будут вызывать нарушения нормального хода работы датацентра. Объекты уровня III зачастую проектируют с перспективой наращивания ресурсов до уровня IV.

Объект должен находиться под управлением человека 24 часа в сутки.

D.2.9.5 Датацентр уровня IV – отказоустойчивый

Датацентр уровня IV имеет несколько активных путей распределения электропитания и охлаждения. Поскольку в датацентре уровня IV, по крайней мере, два пути являются нормально активными, то инфраструктура обеспечивает повышенную степень отказоустойчивости.

Датацентры уровня IV обеспечивают несколько путей подвода электропитания ко всем видам вычислительного и оборудования телекоммуникаций. Уровень IV требует, чтобы всё компьютерное оборудование и оборудование телекоммуникаций имело несколько силовых входов. Оборудование должно быть способно продолжать функционировать, когда один из этих силовых входов отключён. Оборудование, не имеющее нескольких встроенных силовых входов, потребует наличия автоматических переключателей (для перевода на другую электрическую линию) без разрыва тока.

Уровень IV предусматривает возможность проводить любую плановую деятельность без нарушения нормального хода работы. Отказоустойчивая функциональность также обеспечивает способность инфраструктуры датацентра выдержать, по крайней мере, один внеплановый отказ (или событие) без последствий для критически важной нагрузки.

D.3 Телекоммуникации

D.3.1 Уровень I (телекоммуникации)

Чтобы получить, по крайней мере, оценку (рейтинг) «уровень I», инфраструктура телекоммуникаций должна удовлетворять требованиям настоящего стандарта.

Система уровня I должна иметь один принадлежащий клиенту смотровой люк и внешний кабельный канал. Службы провайдера доступа будут терминироваться в одной комнате ввода. Инфраструктура телекоммуникаций будет распределяться из комнаты ввода к главной распределительной зоне и к горизонтальной распределительной зоне по всему датацентру через один кабельный канал. Хотя в топологию сети может быть встроено логическое резервирование (дублирование), но в системе уровня I не будет предусмотрено никакого физического резервирования и никакой диверсификации, т.е. введения разнообразия (для повышения отказоустойчивости системы).

Ниже перечислены некоторые потенциальные одиночные точки отказа системы уровня I:

- отключение провайдера доступа, отключение центрального офиса или нарушение нормального хода работы по длине трассы провайдера доступа;
- отказ оборудования провайдера доступа;
- отказ маршрутизатора или коммутатора, если они не являются резервированными (избыточными);
- какой-либо инцидент в комнате ввода, главной распределительной зоне или смотровом люке, который может нарушить нормальный ход работы всех телекоммуникационных служб для датацентра;
- повреждение магистрали или горизонтальной кабельной системы.

D.3.2 Уровень II (телекоммуникации)

Инфраструктура телекоммуникаций должна соответствовать требованиям уровня I.

Критически важное оборудование телекоммуникаций, временно установленное провайдерское оборудование, промышленно выпускаемые маршрутизаторы и коммутаторы ЛВС и ССХД должны иметь избыточные компоненты (источники питания, процессоры).

Магистральные кабели внутренних ЛВС и ССХД датацентра, идущие от коммутаторов в горизонтальных распределительных зонах к магистральным коммутаторам в главной распределительной зоне должны иметь резервированные оптоволоконные или медные пары внутри общей конфигурации по типу «звезда». Эти резервированные соединения могут быть в одних и тех же или в разных оболочках.

Возможны логические конфигурации, они могут быть в кольцевой или решётчатой топологии, наложенной на физическую конфигурацию типа «звезда».

Система уровня II имеет два принадлежащих клиенту смотровых люка и внешних кабельных канала, идущих к системе. Эти два резервированных внешних кабельных канала будут терминироваться в одной комнате ввода.

Ниже перечислены некоторые потенциальные одиночные точки отказа системы уровня II:

- оборудование провайдера доступа, находящееся в комнате ввода, соединённое с той же самой электрораспределительной системой и поддерживаемое одними ОВиК-компонентами или системами;

- резервированная маршрутизирующая и центральная коммутирующая аппаратура, находящаяся в главной распределительной зоне, соединённая с той же самой электрораспределительной системой и поддерживаемая одними ОВиК-компонентами или системами;

- резервированная распределительная коммутирующая аппаратура, находящаяся в горизонтальной распределительной зоне, соединённая с той же самой электрораспределительной системой и поддерживаемая одними ОВиК-компонентами или системами;

- какой-либо инцидент в комнате ввода или главной распределительной зоне может нарушить нормальный ход работы всех телекоммуникационных служб для датацентра.

D.3.3 Уровень III (телекоммуникации)

Инфраструктура телекоммуникаций должна соответствовать требованиям уровня II.

Датацентр должен обслуживаться, по крайней мере, двумя провайдерами доступа. Обслуживание должно быть обеспечено, по крайней мере, из двух разных центральных офисов или присутственных мест провайдеров доступа. Кабельные каналы из их центральных офисов или присутственных мест должны быть удалены друг от друга на расстояние не менее 29 m по всей длине каналов, чтобы эти каналы можно было считать проложенными по разным маршрутам (диверсифицированными).

Датацентр должен иметь две комнаты ввода, предпочтительно на противоположных торцах датацентра, но физически расстояние между этими двумя комнатами должно быть не менее 20 m. Не допускается совместное использование обеими комнатами ввода предоставленного провайдером доступа оборудования, зон противопожарной защиты, распределительных электрощитов и систем кондиционирования воздуха. Провайдерское оборудование в каждой комнате ввода должно быть способно продолжать работу, если оборудование в другой комнате ввода выйдет из строя.

Датацентр должен иметь дублированные магистральные кабельные каналы между комнатами ввода, главной распределительной зоной и горизонтальными распределительными зонами.

Магистральные кабели внутренних ЛВС и ССХД датацентра, идущие от коммутаторов в горизонтальных распределительных зонах к магистральным коммутаторам в главной распределительной зоне, должны иметь резервированные оптоволоконные или медные пары внутри общей конфигурации по типу звезды. Эти резервированные соединения должны быть в кабельных оболочках, проложенных по разным трассам.

Должен быть предусмотрен «горячий» резерв для всей критически важной аппаратуры телекоммуникаций, для предоставленного провайдером оборудования, для промышленно выпускаемых центральных маршрутизаторов и коммутаторов ЛВС/ССХД.

Все кабели, кросс-панели и шнуры переключений должны быть документированы с использованием электронных таблиц, баз данных или программ, предназначенных для организационного управления кабелями. Документирование кабельной системы является обязательным требованием для того, чтобы датацентру была присвоена оценка «уровень III».

Ниже перечислены некоторые потенциальные одиночные точки отказа системы уровня III:

- какой-либо инцидент в главной распределительной зоне, который может нарушить нормальный ход работы всех телекоммуникационных служб, подведённых к датацентру;
- какой-либо инцидент в горизонтальной распределительной зоне, который может нарушить поставку всех услуг к зоне, которую она обслуживает.

D.3.4 Уровень IV (телекоммуникации)

Инфраструктура телекоммуникаций должна соответствовать требованиям уровня III.

Магистральная кабельная система датацентра должна быть резервирована. Кабельная система между двумя пространствами должна быть проложена по физически разделённым маршрутам, которые совпадают только внутри этих двух конечных пространств. Магистральная система должна быть защищена путём укладки в кабелепровод или путём использования кабелей с заблокированной металлической бронёй.

Должно быть обеспечено автоматическое резервирование для всей критически важной аппаратуры телекоммуникаций, для предоставленного провайдером оборудования, для промышленно выпускаемых центральных маршрутизаторов и коммутаторов ЛВС/ССХД. Сеансы/сетевые соединения должны автоматически переключаться на резервное оборудование.

Датацентр должен иметь главную распределительную зону и второстепенную распределительную зону, предпочтительно на противоположных концах датацентра, но физическое расстояние между этими двумя про-

странствами должно составлять не менее 20 m. Не допускается совместное использование главной распределительной зоной и второстепенной распределительной зоной зон противопожарной защиты, распределительных электрощитов и систем кондиционирования воздуха. Второстепенная распределительная зона является факультативной, если серверная представляет собой единое пространство, в этом случае введение второстепенной распределительной зоны не будет эффективным.

Каждая из этих зон (главная распределительная зона и второстепенная распределительная зона) должна иметь свой кабельный канал к каждой комнате ввода. Должен также быть предусмотрен кабельный канал между главной распределительной зоной и второстепенной распределительной зоной.

Резервированные (избыточные) распределительные маршрутизаторы и коммутаторы должны быть распределены между главной и второстепенной распределительными зонами так, чтобы сети датацентра могли продолжать работать, если главная распределительная зона или второстепенная распределительная зона, или одна из комнат ввода полностью выйдет из строя.

Каждая горизонтальная распределительная зона должна быть связана как с главной, так и с второстепенной распределительными зонами.

Критически важные системы должны иметь горизонтальную кабельную систему к двум горизонтальным распределительным зонам. Дублирующая горизонтальная система является факультативной даже для систем уровня IV.

Ниже перечислены некоторые потенциальные одиночные точки отказа системы уровня IV:

- главная распределительная зона (если отсутствует второстепенная распределительная зона);
- горизонтальная распределительная зона и горизонтальная кабельная система (если не установлена дублирующая горизонтальная кабельная система).

D.4 Требования к архитектуре и конструкции

D.4.1 Общие положения

Конструкции здания должны быть либо железобетонными, либо стальными. Как минимум, каркас здания должен быть спроектирован так, чтобы он противостоял ветровым нагрузкам в соответствии с действующими строительными нормами и правилами для рассматриваемого местоположения и в соответствии с предписаниями для строений, относящихся к весьма важным производственным помещениям.

СЕРТИФИКАТ
СТАНДАРТИЗАЦИИ
НАЦИОНАЛЬНОГО
АКАДЕМИИ
ДЛЯ СЕРТИФИКАЦИИ

D.4.2 Уровень I (архитектура)

В архитектурном отношении датацентр уровня I представляет собой датацентр, к которому не предъявляются никакие требования по защите от физических событий как намеренных, так и случайных, естественных или обусловленных участием человека, которые могли бы привести к отказу датацентра.

D.4.3 Уровень II (архитектура)

Датацентр уровня II должен удовлетворять всем требованиям уровня I. Кроме того, он должен удовлетворять дополнительным требованиям, приведенным в данном приложении. Датацентр уровня II содержит дополнительные минимальные защитные меры против физических событий как намеренных, так и случайных, естественных или обусловленных участием человека, которые могли бы привести к отказу датацентра.

D.4.4 Уровень III (архитектура)

Датацентр уровня III должен удовлетворять всем требованиям уровня II. Кроме того, они должны удовлетворять дополнительным требованиям, приведенным в данном приложении. Датацентр уровня III защищен от большинства физических событий как намеренных, так и случайных, естественных или обусловленных участием человека, которые могли бы привести к отказу датацентра.

D.4.5 Уровень IV (архитектура)

Датацентр уровня IV учитывает все потенциальные физические события, которые могли бы привести к отказу датацентра. Датацентр уровня IV обеспечивает специальные и в некоторых случаях избыточные средства защиты против таких событий. Датацентры уровня IV учитывают потенциальные проблемы, связанные с такими природными катаклизмами, как сейсмические явления, затопления, пожары, ураганы и штормы, а также потенциальные проблемы, связанные с терроризмом.

D.5 Электрооборудование

D.5.1 Уровень I (электрооборудование)

Система уровня I обеспечивает минимальный уровень распределения питания для удовлетворения потребностей электрических нагрузок, с небольшим резервированием или вовсе без него. Электрические системы не имеют резервирования, в них отказ или ремонт/обслуживание какой-либо панели или питающего кабеля вызывает частичное или полное прерывание операций. В месте ввода питания от общедоступной электросети не требуется никакого резервирования.

Генераторы могут быть установлены поодиночке или параллельно с целью повышения мощности, но требование к резервированию не предъ-

является. Обычно используются один или несколько автоматических переключателей, которые реагируют на потерю нормального электроснабжения, инициируют пуск генератора и переключают нагрузки на систему генераторов. Для этой цели используются (но не являются обязательными) автоматические переключатели или автоматические разъединители цепи. Отсутствует необходимость применения постоянно установленных нагрузочных реостатов для тестирования генератора и ИБП. Требуется предусмотреть возможность для подключения переносимых реостатов.

Система бесперебойного электропитания может быть установлена как одиночный блок или в параллель для повышения мощности. Могут быть использованы статические, вращающиеся или гибридные ИБП как двойного преобразования, так и интерактивные. Требуется совместимость системы ИБП с системой генераторов. Система ИБП должна иметь возможность байпаса (обхода), которая позволит сохранить непрерывность работы в период техобслуживания/ремонта системы ИБП.

В датацентрах уровня I для распределения питания к критически важным электронным нагрузкам приемлемыми являются отдельные трансформаторы и щиты. Трансформаторы должны быть рассчитаны на работу с нелинейной нагрузкой, для питания которой они предназначены. Вместо трансформаторов К-типа можно также использовать трансформаторы, погашающие гармоники.

Для распределения питания к критически важным электронным нагрузкам можно использовать распределительные щиты питания или отдельные трансформаторы и панели управления. Допускается использовать любой соответствующий правилам и нормам способ проводки. Для системы распределения не требуется резервирования.

Система заземления должна отвечать минимальным нормативным требованиям.

Текущий контроль электрической и механической системы является факультативным.

D.5.2 Уровень II (электрооборудование)

Системы уровня II должны соответствовать всем требованиям уровня I.

Система уровня II предусматривает наличие модулей ИБП с резервированием (N+1). Требуется наличие генераторной системы, мощность которой должна быть выбрана так, чтобы система справлялась со всеми нагрузками датацентра, хотя резервный комплект генераторов не является обязательным. Отсутствует требование резервирования ввода питания от общей электросети или системы распределения питания.

Требуется предусмотреть возможность подключения передвижных реостатов нагрузок для тестирования генератора и ИБП.

Для распределения питания к критически важным электронным нагрузкам необходимо использовать PDU. Допускается запитывать от PDU

дополнительные панели или «боковые секции» к PDU в тех случаях, когда требуются дополнительные ответвлённые электрические линии. Для обслуживания каждой стойки с компьютерным оборудованием должны быть предусмотрены два резервированных PDU, для каждого предпочтительно питание от отдельной системы ИБП; компьютерное оборудование с одним и с тремя шнурами питания должно быть снабжено смонтированным на стойке быстродействующим или статическим переключателем нагрузки с питанием от каждого PDU. Вместо этого для компьютерного оборудования с одним и с тремя шнурами питания можно предусмотреть устройства PDU со статическим переключателем, имеющим дублированное питание от разных систем ИБП, хотя такая схема предусматривает несколько пониженное резервирование и меньшую гибкость.

Одна линия должна обслуживать не более одной стойки во избежание отказа линии вследствие вредного воздействия нескольких стоек. Для обеспечения резервирования каждая стойка и каждый шкаф должны иметь две специально выделенных электрических линии, питаемых от двух разных PDU или электрических щитков. Рекомендуется, но не требуется, иметь резервированный питающий кабель к распределительному щиту для механической системы.

D.5.3 Уровень III (электрооборудование)

Системы уровня III должны соответствовать всем требованиям уровня II.

Все системы датацентра уровня III должны иметь резервирование не менее (N+1) на уровне модуля, канала и системы, включая системы генераторов, ИБП, систему распределения и все распределительные питающие кабели. При проектировании электрической системы следует учитывать конфигурацию механических систем, чтобы гарантировать, что объединённой электромеханической системе обеспечено резервирование (N+1). Такой уровень резервирования можно получить либо подключением двух источников питания к каждому кондиционеру, либо разделением оборудования для кондиционирования воздуха между несколькими источниками питания. Питающие кабели и распределительные щиты резервированы, благодаря чему отказ или ремонт какого-либо кабеля или панели не вызывает прекращения операций. Должно быть обеспечено достаточное резервирование для того, чтобы была возможность изолировать любую единицу механического или электрического оборудования, которая потребовала бы существенного ремонта. Благодаря использованию распределённой резервированной конфигурации практически исключены одиночные точки отказа, начиная от места ввода питания от энергосистемы общего пользования вплоть до механического оборудования и вплоть до PDU или компьютерного оборудования.

Чтобы повысить доступность питания для критически важной нагрузки, система распределения конфигурируется по распределённой

изолированной резервированной (двухпутной) топологии. Эта топология требует использования автоматических статических переключателей с одной линии на другую либо со стороны первичной, либо со стороны вторичной обмотки трансформатора PDU. Эти переключатели применяются только для нагрузок с одним шнуром питания. Если конструкция нагрузки предусматривает два (или более) шнуров питания, что позволяет непрерывно работать с подачей питания только по одному шнуру, то автоматические статические переключатели не используются, при условии, что шнуры питаются от разных ИБП. Переключатели будут иметь обходную (байпасную) электрическую линию и один выходной выключатель.

Должна быть предусмотрена центральная система текущего контроля и управления питанием и наблюдения за микроклиматом, которая осуществляет текущий контроль за всеми видами крупного электрооборудования, куда относятся главные распределительные устройства, генераторные системы, автоматические переключатели (с одного трансформатора на другой), пункты управления электродвигателями, системы защиты от импульсов напряжения и механические системы. Для управления механической системой, оптимизации её к.п.д. (коэффициент полезного действия), циклического использования оборудования и индикации аварийного состояния должна быть предусмотрена отдельная программируемая система логического управления.

D.5.4 Уровень IV (электрооборудование)

Системы уровня IV должны соответствовать всем требованиям уровня III.

Системы датацентра уровня IV должны иметь конфигурацию с резервированием не менее $2(N+1)$ во всех модулях, системах и каналах. Для всех питающих кабелей и оборудования должна быть предусмотрена возможность ручного обхода (байпаса) для ремонта/техобслуживания или на случай отказа. При любом отказе подача питания к критически важной нагрузке автоматически переключается с отказавшей системы на альтернативную без перерыва питания критически важных нагрузок.

Для обеспечения адекватной работы аккумуляторной батареи должна быть предусмотрена система текущего контроля за аккумуляторной батареей, способная индивидуально контролировать импеданс или сопротивление каждого элемента, температуру корпуса каждого аккумулятора и сигнализировать о приближающемся отказе батареи.

Вводы от сети электроснабжения общего пользования должны быть выделены исключительно для данного конкретного датацентра и изолированы от всех не критически важных устройств.

Здание должно иметь, по крайней мере, два питающих кабеля от сети общего пользования, которые должны быть проложены от двух разных подстанций с целью резервирования.

D.6 Механическое оборудование

D.6.1 Уровень I (механическое оборудование)

Система ОВиК производственного помещения уровня I включает в себя один или несколько кондиционеров с общей холодопроизводительностью, позволяющей поддерживать в критически важном пространстве температуру и относительную влажность в расчётных пределах, без резервных кондиционеров. Если эти кондиционеры обслуживаются системой отвода тепла с помощью воды, например, системой с охлаждённой водой или системой с водяным конденсатором, то компоненты этих систем также подобраны по типоразмерам с тем, чтобы поддерживались расчётные режимы, без резервных компонентов. Система или системы трубопроводов являются однопутными, вследствие чего отказ или ремонт какого-либо участка трубы вызовет частичное или полное прерывание работы системы кондиционирования.

Если предусмотрен электрогенератор, то всё оборудование системы кондиционирования воздуха должно получать питание от резервной системы генераторов.

D.6.2 Уровень II (механическое оборудование)

Система ОВиК производственного помещения уровня II включает в себя несколько кондиционеров с общей холодопроизводительностью, позволяющей поддерживать в критически важном пространстве температуру и относительную влажность в расчётных пределах, с одним резервным агрегатом (N+1). Если эти кондиционеры обслуживаются водяной системой, то компоненты этих систем также подобраны по типоразмерам с тем, чтобы поддерживались расчётные режимы, с одним резервным агрегатом (агрегатами). Система или системы трубопроводов являются однопутными, вследствие чего отказ или ремонт какого-либо участка трубы вызовет частичное или полное прерывание работы системы кондиционирования.

Системы кондиционирования воздуха должны быть рассчитаны на непрерывную работу 7 дней в неделю/24 часа в сутки/365 дней в год и должны иметь резервирование не менее (N+1) для серверной.

Система кондиционирования серверной должна обладать резервированием на уровне (N+1) и иметь не менее одного резервного кондиционера на каждые три или четыре необходимых кондиционеров.

В серверных и других связанных с ними пространствах должно поддерживаться избыточное давление воздуха по сравнению с помещениями, не имеющими отношения к датацентру, и с атмосферным давлением вне помещения.

Всё оборудование для кондиционирования воздуха должно получать питание от резервной системы генераторов.

Линии питания к оборудованию для кондиционирования воздуха должны быть распределены между несколькими панелями управле-

ния/распределительными щитами с целью минимизации влияния отказов электрооборудования на систему кондиционирования воздуха.

Все системы регулирования температуры должны получать питание через специально выделенные резервированные линии от ИБП.

Подача воздуха в датацентр должна быть построена с учётом типов и схем расположения стоек с серверами, которые будут установлены в датацентре. Установка для перемещения воздуха должна иметь достаточную производительность, чтобы противостоять общей проектной тепловой нагрузке от оборудования, освещения и т.д. и поддерживать постоянные уровни относительной влажности в пределах датацентра. Требуемую холодопроизводительность следует рассчитывать исходя из мощности в киловаттах, получаемой от системы ИБП.

Система хранения топлива должна иметь изолированные и резервированные компоненты, чтобы загрязнение топливной системы или её механический отказ не повлияли на систему генераторов в целом.

D.6.3 Уровень III (механическое оборудование)

Система ОВиК производственного помещения уровня III включает в себя несколько кондиционеров с общей холодопроизводительностью, позволяющей поддерживать в критически важном пространстве температуру и относительную влажность в расчётных пределах, с достаточным числом резервных агрегатов для того, чтобы допустить отказ или техническое обслуживание одного электрораспределительного щита. Если эти кондиционеры обслуживаются водяной системой отвода тепла, то компоненты этих систем также подобраны по типоразмерам с тем, чтобы поддерживались расчётные режимы при исключении из работы одного электрического коммутационного щита. Такой уровень резервирования может быть получен либо подводом двух источников питания к каждому кондиционеру, либо распределением кондиционерного оборудования между несколькими источниками питания. Система или системы трубопроводов являются двухпутными, вследствие чего отказ или техобслуживание какого-либо участка трубы не вызовет перерыва в работе системы кондиционирования воздуха.

Для обеспечения электрического резервирования нужно предусмотреть подачу питания к дублирующим агрегатам системы кондиционирования от разных щитов. Все кондиционеры серверной должны быть обеспечены резервным питанием от генератора.

Датацентр должен быть обеспечен специально предназначенным для него холодильным оборудованием с резервированием на уровнях N+1, N+2, 2N или 2(N+1). Должно быть предусмотрено достаточное резервирование для того, чтобы обеспечить изоляцию каждого компонента оборудования, который требует существенного ремонта/техобслуживания.

В соответствии с числом установленных прецизионных кондиционеров и с учётом факторов ремонтпригодности и резервирования, контуры

охлаждения для прецизионных кондиционеров следует подразделять на суб-контуры. Если используются системы с водяным охлаждением или с водяным конденсатором, то каждый суб-контур, специально предназначенный для датацентра, должен иметь независимые насосы, питаемые из централизованной кольцевой системы трубопроводов подачи воды. По периметру датацентра под полом следует проложить петлевой жёлоб, чтобы в него собирались утечки воды со всей зоны, охваченной жёлобом. В этот жёлоб нужно поместить датчики обнаружения утечек (течеискатели). Следует уделить внимание созданию полностью изолированных и резервированных контуров подачи охлаждённой воды.

D.6.4 Уровень IV (механическое оборудование)

Система ОВиК производственного помещения уровня IV включает в себя несколько кондиционеров с общей холодопроизводительностью, позволяющей поддерживать в критически важном пространстве температуру и относительную влажность в расчётных пределах, с достаточным числом резервных агрегатов для того, чтобы допустить отказ или техническое обслуживание одного электрораспределительного щита. Если эти кондиционеры обслуживаются водяной системой отвода тепла, такой как система с водяным охлаждением или с водяным конденсатором, то компоненты этих систем также подобраны по типоразмерам с тем, чтобы поддерживались расчётные режимы при исключении из работы одного электрического коммутационного щита. Такой уровень резервирования может быть получен либо подводом двух источников питания к каждому кондиционеру, либо распределением кондиционерного оборудования между несколькими источниками питания. Система или системы трубопроводов являются двухпутными, вследствие чего отказ или техобслуживание какого-либо участка трубы не вызовет перерыва в работе системы кондиционирования воздуха. Если для системы уровня IV установлены испарительные системы, то необходимо предусмотреть альтернативные ресурсы для бака с запасом воды.

В таблицах D.1 - D.4 приведено руководство по уровням.

Таблица D.1 – Руководство по уровням (телекоммуникации)

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Кабельная система, стойки, шкафы и кабелепроводы отвечают требованиям настоящего стандарта	Да	Да	Да	Да
Проложенные по разным трассам вводы от провайдера доступа и смотровые люки удалены друг от друга минимум на 20 m	Нет	Да	Да	Да

Окончание таблицы D.1

Наименование параметров	Уро- вень I	Уро- вень II	Уро- вень III	Уро- вень IV
Резервированы службы провайдеров доступа – несколько провайдеров, центральных офисов и трасс	Нет	Нет	Да	Да
Вторая комната ввода	Нет	Нет	Да	Да
Вторичная распределительная зона	Нет	Нет	Нет	Фа- куль- татив- но
Резервные магистральные кабелепро- воды	Нет	Нет	Да	Да
Резервная горизонтальная кабельная проводка	Нет	Нет	Нет	Фа- куль- татив- но
Маршрутизаторы и коммутаторы име- ют резервные источники питания и процессоры	Нет	Да	Да	Да
Несколько маршрутизаторов и комму- таторов для резервирования	Нет	Нет	Да	Да

Таблица D.2 – Руководство по уровням (архитектура)

Наименова- ние пара- метров	Уровень I	Уровень II	Уровень III	Уровень IV
Выбор площадки				
Близость к затопляемой зоне	Нет требо- ваний	Не в затоп- ляемой зоне	Не в зоне с риском за- топления раз в 100 лет или ме- нее 91 м от зоны с риском за- топления раз в 50 лет	Не менее 91 м от зоны с риском за- топления раз в 100 лет

ЎЗЎСТАНДАНТ АЎЧЎРАШТИ
СТАНДАРТИЗАЦИОННИЙ ЦЕНТРАЛ
НАЗАРҚАТ ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
АДМИНИСТРАЦИЯСЫ
2014-2015-жылдарда

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Близость к прибрежным или внутренним водным путям	Нет требований	Нет требований	Не менее 91 m	Не менее 0,8 km
Близость к главным магистралям	Нет требований	Нет требований	Не менее 91 m	Не менее 0,8 km
Близость к аэропортам	Нет требований	Нет требований	Не менее 1,6 km	Не менее 8 km
Парковка				
Раздельные парковки для посетителей и сотрудников	Нет требований	Нет требований	Да (физически отделить забором или стеной)	Да (физически отделить забором или стеной)
Отдельно от погрузочно-разгрузочных площадок	Нет требований	Нет требований	Да	Да (физически отделить забором или стеной)
Близость парковки к наружным стенам дата-центра	Нет требований	Нет требований	Минимум 9,1 m	Минимум 18,3 m с физическими барьерами, мешающими машинам подъехать ближе
Наличие арендаторов				
Наличие в здании нескольких арендаторов	Нет ограничений	Можно, если они не создают рисков	Можно, если все арендаторы – это дата-центры или организации телекоммуникаций	Можно, если все арендаторы – это дата-центры или организации телекоммуникаций
Конструкция здания				
Тип конструкции	Нет ограничений	Нет ограничений	Тип II-1hr, III-1hr, IV-1hr	Тип I или II-FR

[illegible]

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Требования к огнестойкости				
Наружные несущие стены	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 4 часа
Внутренние несущие стены	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 2 часа
Наружные ненесущие стены	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 4 часа
Каркас конструкции	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 2 часа
Внутренние перегородки вне серверной	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 1 час
Внутренние перегородки в серверной	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 2 часа
Ограждения шахты	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 2 часа
Полы и полы-потолки	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 2 часа
Компоненты здания				
Крыши и крыши-потолки	По нормам и правилам	По нормам и правилам	Минимум 1 час	Минимум 2 часа
Пароизоляция для стен и потолка серверной	Нет требований	Да	Да	Да
Входы в здание с контрольно-пропускными пунктами	Нет требований	Нет требований	Да	Да
Конструкция панелей перекрытий	-	Нет ограничений	Полностью стальные	Полностью стальные или с заливкой бетоном

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Фундамент	-	Нет ограничений	Стрингеры на болтах	Стрингеры на болтах
Кровля				
Класс	Нет ограничений	Класс А	Класс А	Класс А
Тип	Нет ограничений	Нет ограничений	Негорючий настил (нет систем с механическим креплением)	Двойное дублирование бетонным настилом (нет систем с механическим креплением)
Стойкость к ветровому срыву	Минимальные нормативные требования	FM I-90	Минимум FM I-90	Минимум FM I-120
Уклон крыши	Минимальные нормативные требования	Минимальные нормативные требования	Минимум 1:48	Минимум 1:24
Двери и окна				
Огнестойкость	Минимальные нормативные требования	Минимальные нормативные требования	Минимальные нормативные требования (не менее $\frac{3}{4}$ часа в серверной)	Минимальные нормативные требования (не менее $1\frac{1}{2}$ часа в серверной)

СЕРТИФИКАТ
 ЭЛЕКТРОННО-ЦИФРОВОЙ
 РАССЛАТОВАНИЯ
 КОДИРОВАННО-ПОДПИСАНО
 2014-09-09 10:00:00

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Размеры двери	Минимальные нормативные требования и ширина не менее 1 m, высота не менее 2,13 m	Минимальные нормативные требования и ширина не менее 1 m, высота не менее 2,13 m	Минимальные нормативные требования (ширина не менее 1 m на входе в серверную, комнаты электриков, механиков) и высота не менее 2,29 m	Минимальные нормативные требования (ширина не менее 1,2 m на входе в серверную, комнаты электриков, механиков) и высота не менее 2,49 m
Окна по периметру серверной	Допускаются с минимальными требованиями к огнестойкости	Допускаются с минимальными требованиями к огнестойкости	Допускаются внутренние окна с огнестойкостью 1 час, наружные окна не допускаются	Допускаются внутренние окна с огнестойкостью 1 час, наружные окна не допускаются
Входной вестибюль				
Отгородить от других зон дата-центра	Нет требований	Да	Да	Да
Противопожарная стена от других зон дата-центра	Минимальные нормативные требования	Минимальные нормативные требования	Минимальные нормативные требования (не менее 1 часа)	Минимальные нормативные требования (не менее 2 часов)
Место для охранника	Нет требований	Нет требований	Да	Да

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Средства контроля доступа	Нет требований	Нет требований	Да	Да
Комнаты персонала				
Отгородить от других зон дата-центра	Нет требований	Да	Да	Да
Противопожарные стены от других зон датацентра	Минимальные нормативные требования	Минимальные нормативные требования	Минимальные нормативные требования (не менее 1 часа)	Минимальные нормативные требования (не менее 2 часов)
Комнаты для охраны				
Отгородить от других зон дата-центра	Нет требований	Нет требований	Да	Да
Противопожарные стены от других зон датацентра	Минимальные нормативные требования	Минимальные нормативные требования	Минимальные нормативные требования (не менее 1 часа)	Минимальные нормативные требования (не менее 2 часов)
180-градусные «глазки» на комнатах текущего контроля и средств обеспечения безопасности	Нет требований	Да	Да	Да

СЕРТИФИКАТ
СТАНДАРТИЗАЦИИ, СЕРТИФИКАЦИИ
ИЗДАТЕЛЬСТВО НАЦИОНАЛЬНОГО
АГЕНТСТВА ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ
И СТАНДАРТИЗАЦИИ

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Выделить специальную комнату для средств обеспечения безопасности и контроля	Нет требований	Нет требований	Рекомендуется	Рекомендуется
Операционный центр				
Отгородить от других зон дата-центра	Нет требований	Нет требований	Да	Да
Противопожарные стены от других зон дата-центра	Нет требований	Нет требований	1 час	2 часа
Близость к серверной	Нет требований	Нет требований	Непрямой доступ (максимум одна присоединённая комната)	Прямой доступ
Комнаты отдыха				
Близость к серверной и подсобным зонам	Нет требований	Минимальные нормативные требования	Если совсем рядом, нужен барьер против утечек	Не рядом, но нужен барьер против утечек
Противопожарные стены от серверной и подсобных зон	Минимальные нормативные требования	Минимальные нормативные требования	Минимальные нормативные требования (не менее 1 часа)	Минимальные нормативные требования (не менее 2 часов)

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Комнаты для ИБП и аккумуляторные				
Ширина коридоров для обслуживания, ремонта и перемещения оборудования	Нет требований	Нет требований	Минимальные нормативные требования (не менее 1 m в свету)	Минимальные нормативные требования (не менее 1,2 m в свету)
Близость к серверной	Нет требований	Нет требований	Непосредственно рядом	Непосредственно рядом
Противопожарные стены от серверной и других зон датацентра	Минимальные нормативные требования	Минимальные нормативные требования	Минимальные нормативные требования (не менее 1 часа)	Минимальные нормативные требования (не менее 2 часов)
Требуемые коридоры для выхода				
Противопожарные стены от серверной и других зон датацентра	Противопожарные стены от серверной и других зон датацентра	Противопожарные стены от серверной и других зон датацентра	Противопожарные стены от серверной и других зон датацентра	Противопожарные стены от серверной и других зон датацентра
Ширина	Минимальные нормативные требования	Минимальные нормативные требования	Минимальные нормативные требования и не менее 1,2 m в свету	Минимальные нормативные требования и не менее 1,5 m в свету
Зона отгрузки/приёма грузов				
Зона отгрузки/приёма грузов, отгороженная от других зон датацентра	Нет требований	Нет требований	Да	Да

СЕРТИФИКАТ
 СТАЦИОНАРНЫЙ
 КОДИРОВАННЫЙ
 КОДИРОВАННЫЙ
 КОДИРОВАННЫЙ
 КОДИРОВАННЫЙ

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Противопожарные стены от других зон датацентра	Минимальные требования	Минимальные требования	1 час	2 часа
Физическая защита стен вблизи грузоподъемных операций	Нет требований	Нет требований	Да (обшить фанерой не тоньше 19 mm)	Да (стальные тумбы или подобная защита)
Число погрузо-разгрузочных площадок	Нет требований	1 на 2500 m ² площади серверной	1 на 2500 m ² площади серверной (минимум 2)	1 на 2500 m ² площади серверной (минимум 2)
Зоны для генераторов и топливохранилищ				
Близость к серверной и подсобным зонам	Нет требований	Нет требований	Если внутри здания датацентра, то нужны противопожарные стены двухчасовой огнестойкости со всеми другими зонами	Отдельное здание или всепогодные укрытия, с нормативным расстоянием между зданиями
Близость к общедоступным зонам	Нет требований	Нет требований	Расстояние не менее 9 m	Расстояние не менее 19 m
Безопасность				
Ёмкость ИБП системы центрального процессора	Нет требований	Здание	Здание	Здание + аккумуляторная батарея (минимум 8 часов)

ОБЩЕСТВЕННАЯ КОМПАНИЯ
 СТАНДАРТЫ И ТЕХНИЧЕСКИЕ УСЛОВИЯ
 КОМПЕТЕНТНЫЙ ЦЕНТР
 АДРЕС: ТУ-100-000-000-000
 ЮРИДИЧЕСКИЙ АДРЕС: ТУ-100-000-000-000

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Ёмкость ИБП панелей сбора данных	Нет требований	Здание + аккумуляторная батарея (минимум 4 часа)	Здание + аккумуляторная батарея (минимум 8 часов)	Здание + аккумуляторная батарея (минимум 24 часа)
Ёмкость ИБП полевого устройства	Нет требований	Здание + аккумуляторная батарея (минимум 4 часа)	Здание + аккумуляторная батарея (минимум 8 часов)	Здание + аккумуляторная батарея (минимум 24 часа)
Число охранников в смену	Нет требований	5 дней в неделю в течение рабочих часов	7 дней в неделю, 24 часа в сутки	7 дней в неделю, 24 часа в сутки
Контроль доступа к:				
Генераторам	Промышленный замок	Охранная сигнализация	Охранная сигнализация	Охранная сигнализация
Комнатам ИБП, телефонии	Промышленный замок	Охранная сигнализация	Доступ по карточкам	Доступ по карточкам
Складам оптических кабелей	Промышленный замок	Охранная сигнализация	Охранная сигнализация	Доступ по карточкам
Дверям аварийных выходов	Промышленный замок	Текущий контроль	Задержка выхода по нормативу	Задержка выхода по нормативу
Открыванию досягаемых наружных окон	Нет требований	Охранная сигнализация	Охранная сигнализация	Охранная сигнализация
Центру службы безопасности	Нет требований	Нет требований	Доступ по карточкам	Доступ по карточкам
Сетевому операционному центру	Нет требований	Нет требований	Доступ по карточкам	Доступ по карточкам

СЕРТИФИКАТ
СТАНДАРТИЗАЦИИ
НАЦИОНАЛЬНОГО СТАНДАРТА
АКЦИОНЕРНОГО ОБЩЕСТВА
РОССИИ

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Комнате средств обеспечения безопасности	Нет требований	Охранная сигнализация	Доступ по карточкам	Доступ по карточкам
Дверям в серверным	Промышленный замок	Охранная сигнализация	Карточный или биометрический доступ на вход и на выход	Карточный или биометрический доступ на вход и на выход
Дверям по периметру здания	Нет требований	Охранная сигнализация	Карточный доступ, если двери входные	Карточный доступ, если двери входные
Главной двери на этаже, где расположена серверная	Промышленный замок	Доступ по карточкам	Средства контроля доступа	Средства контроля доступа
Пуленепробиваемые стены, окна, двери				
Место охранника в вестибюле	-	-	Уровень 3 (минимум)	Уровень 3 (минимум)
Наблюдение и контроль с помощью системы закрытой трансляции телевидения				
Периметр здания и парковка	Нет требований	Нет требований	Да	Да
Генераторы	Нет требований	Нет требований	Да	Да
Двери с контролем доступа	Нет требований	Да	Да	Да
Двери серверной	Нет требований	Нет требований	Да	Да
Комнаты ИБП, телефонии	Нет требований	Нет требований	Да	Да

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Система закрытой трансляции телевидения				
Запись любой активности на всех камерах	Нет требований	Нет требований	Да; цифровая	Да; цифровая
Скорость записи, кадры/s	Нет требований	Нет требований	Минимум 20 кадров/s	Минимум 20 кадров/s
Конструкции				
Помещение, предназначенное для сейсмической зоны	Нет ограничений	Нет ограничений	Нет ограничений	В сейсмозонах 0, 1, 2 – по требованиям зоны 3, в зонах 3, 4 – по требованиям зоны 4
Спектр реакций конкретного объекта – уровень местных сейсмических ускорений	Нет	Нет	Рабочее состояние выше 10% при событии, вероятном 1 раз в 50 лет	Рабочее состояние выше 5% при событии, вероятном 1 раз в 100 лет
Коэффициент важности – помогает страховать больше, чем проект по нормативам	$I = 1$	$I = 1,5$	$I = 1,5$	$I = 1,5$

СЕРТИФИКАТ
СТАНДАРТОВ
И ТЕХНИЧЕСКИХ УСЛОВИЙ
НА ПРОДУКТЫ
И УСЛУГИ
СЕРТИФИКАЦИОННО-АНАЛИТИЧЕСКИЙ
ЦЕНТР

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Серверные стойки/шкафы закреплены к основанию или имеют опору и в верхней части, и у основания	Нет	Только основание	Полное крепление	Полное крепление
Ограничение прогибов оборудования телекоммуникаций пределами, приемлемыми для электроарматуры	Нет	Нет	Да	Да
Крепление участков электрических кабелепроводов и кабельных коробов/лотков	По нормативам	По нормативам с коэффициентом важности	По нормативам с коэффициентом важности	По нормативам с коэффициентом важности
Крепление участков крупных воздуховодов механической системы	По нормативам	По нормативам с коэффициентом важности	По нормативам с коэффициентом важности	По нормативам с коэффициентом важности

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Несущая способность перекрытий для наложенной временной нагрузки	7,2 kPa	8,4 kPa	12 kPa	12 kPa
Несущая способность перекрытий для дополнительных грузов, подвешенных снизу	1,2 kPa	1,2 kPa	2,4 kPa	2,4 kPa
Толщина бетонной плиты на уровне земли	127 mm	127 mm	127 mm	127 mm
Толщина слоя бетона на профилированном стальном настиле для перекрытий выше уровня земли; влияет на размер анкеров, которые могут быть установлены	102 mm	102 mm	102 mm	102 mm

СЕРТИФИКАТ АССОЦИИ
 СЕРТИФИКАТ АССОЦИИ
 НАЗНАЧЕНИЕ: АССОЦИАЦИЯ
 АССОЦИАЦИЯ АССОЦИАЦИЯ
 АССОЦИАЦИЯ АССОЦИАЦИЯ

Продолжение таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Система регистрации световых полей здания (стенадиафрагма жёсткости/рама, раскреплённая наклонными или К-образными раскосами/жёсткий пространственный каркас), показывает смещение конструкции	Сталь/бетон, металлический настил	Бетонная стена-диафрагма жёсткости/стальная рама с раскосами	Бетонная стена-диафрагма жёсткости/стальная рама с раскосами	Бетонная стена-диафрагма жёсткости/стальная рама с раскосами
Рассеяние энергии зданием – пассивные клапаны/изоляция основания (энергопоглощение)	Нет	Нет	Пассивные клапаны	Пассивные клапаны/изоляция основания
Пол в комнате ИБП/аккумуляторной в составе здания	Преднапряжённый бетон	Монолитный бетон	Стальной настил с заполнением	Стальной настил с заполнением

Система регистрации световых полей здания (стенадиафрагма жёсткости/рама, раскреплённая наклонными или К-образными раскосами/жёсткий пространственный каркас), показывает смещение конструкции

Окончание таблицы D.2

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Стальной настил с заполнением/преднапряжённый бетон/монолитный бетон	Преднапряжённый бетон	Монолитный бетон	Стальной настил с заполнением	Стальной настил с заполнением

Таблица D.3 - Руководство по уровням (электрооборудование)

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Электрооборудование				
Общие положения				
Система допускает параллельное обслуживание	Нет	Нет	Да	Да
Шнуры питания компьютерного и оборудования телекоммуникаций	1 шнур питания со стопроцентной пропускной способностью по току	2 шнура питания, оба со стопроцентной пропускной способностью по току	2 шнура питания, оба со стопроцентной пропускной способностью по току	2 шнура питания, оба со стопроцентной пропускной способностью по току
Одиночные точки отказа	Одна или более одиночных точек отказа для распределительных систем, питающих электрооборудование или механические системы	Одна или более одиночных точек отказа для распределительных систем, питающих электрические или механические системы	Нет одиночных точек отказа для распределительных систем, обслуживающих электрические или механические системы	Нет одиночных точек отказа для распределительных систем, обслуживающих электрические или механические системы

Продолжение таблицы D.3

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
ИБП				
Резервирование	N	N+1	N+1	2N
Топология	1 модуль или параллельные нерезервированные модули	Параллельные резервированные или распределённые резервированные модули	Параллельные резервированные, распределительные резервированные модули или система с резервированием на уровне блока	Параллельные резервированные, распределительные резервированные модули или система с резервированием на уровне блока
ИБП питают всё компьютерное и оборудование телекоммуникаций	Нет	Нет	Да	Да
Трансформаторы с К-номиналом установлены в распределительный щит питания	Да, но не обязательно, если используются трансформаторы, нейтрализующие гармоники	Да, но не обязательно, если используются трансформаторы, нейтрализующие гармоники	Да, но не обязательно, если используются трансформаторы, нейтрализующие гармоники	Да, но не обязательно, если используются трансформаторы, нейтрализующие гармоники
Заземление				
Система молниезащиты	В соответствии с Правилами (раздел VII) [1]	В соответствии с Правилами (раздел VII) [1]	Да	Да
Нейтраль светильников изолирована от вводов сервисов, питание от трансформатора системы освещения для	Не требуется	Не требуется	Да	Да

Продолжение таблицы D.3

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
изоляции от короткого замыкания на землю				
Инфраструктура заземления в серверной	В соответствии с Правилами (раздел I) [2]	В соответствии с Правилами (раздел I) [2]	В соответствии с Правилами (раздел I) [2]	В соответствии с Правилами (раздел I) [2]
Центральная система текущего контроля и управления питанием и наблюдения за микроклиматом с инженерным дистанционным пультом и ручной блокировкой всех видов автоматического управления и уставок	Нет	Нет	Да	Да
Резервная генерирующая система				
Выбор типоразмера генератора	Типоразмер подбирают только исходя из потребностей компьютерного оборудования и оборудования телекоммуникаций, электрических и механических систем	Типоразмер подбирают только исходя из потребностей компьютерного оборудования и оборудования телекоммуникаций, электрических и механических систем	Типоразмер подбирают только исходя из потребностей компьютерного оборудования и оборудования телекоммуникаций, электрических и механических систем и дополнительно один запасной	Общая нагрузка здания и дополнительно один запасной

Окончание таблицы D.3

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Генераторы на одной шине	Да	Да	Нет	Нет
Техническое обслуживание и текущий ремонт				
Штат обслуживающего технического персонала	На объекте только дневная смена. В остальное время — по вызову	На объекте только дневная смена. В остальное время — по вызову	На объекте круглосуточно в будни. В выходные — по вызову	Круглосуточное дежурство на объекте
Профилактическое обслуживание	Нет требований	Нет требований	Ограниченная программа обучения профилактическому обслуживанию	Полная программа обучения профилактическому обслуживанию
Программы обучения персонала на объекте	Нет требований	Нет требований	Полная программа обучения	Полная программа обучения, включая ручное управление процедурами, если необходимо обойти автоматическую систему управления

Таблица D.4 - Руководство по уровням (механическое оборудование)

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Механическое оборудование				
Общие положения				
Трассы водопроводных и водо-	Разрешено, но не реко-	Разрешено, но не ре-	Не допускается	Не допускается

Продолжение таблицы D.4

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
отводных трубопроводов, не связанных с оборудованием датацентра, в помещениях датацентра	комендуется	комендуется		
Избыточное давление воздуха в серверной и связанных с ней помещениях, по сравнению с наружной атмосферой и помещениями, не относящимися к датацентру	Нет требований	Да	Да	Да
Стоки в полу серверной для сбора конденсата, воды из увлажнителей и воды, выпущенной спринклерами	Да	Да	Да	Да
Механические системы на резервном генераторе	Нет требований	Да	Да	Да
Установка с водяным конденсатором				
Внутренние блоки кондиционеров	Нет резервных кондиционеров	Один резервный кондиционер на каждую критически важную зону	Число кондиционеров достаточно для поддержки критически важной зоны	Число кондиционеров достаточно для поддержки критически важной зоны при

Продолжение таблицы D.4

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
			ны при утрате одного источника электропитания	утрате одного источника электропитания
Регулирование влажности воздуха в серверной	Увлажнение предусмотрено	Увлажнение предусмотрено	Увлажнение предусмотрено	Увлажнение предусмотрено
Подводка электричества к механическому оборудованию	Один путь подачи питания к кондиционерному оборудованию	Один путь подачи питания к кондиционерному оборудованию	Несколько путей подачи питания к кондиционерному оборудованию	Несколько путей подачи питания к кондиционерному оборудованию
Отвод тепла				
Трубопровод охлаждённой воды	Однопутная система охлаждённой воды	Однопутная система охлаждённой воды	Двухпутная система охлаждённой воды	Двухпутная система охлаждённой воды
Насосы охлаждённой воды	Нет резервных насосов охлаждённой воды	Один резервный насос охлаждённой воды	Число насосов охлаждённой воды достаточно для поддержки критически важной зоны при утрате одного источника электропитания	Число насосов охлаждённой воды достаточно для поддержки критически важной зоны при утрате одного источника электропитания
Система трубопроводов конденсаторной воды	Однопутная система трубопроводов конденсаторной воды	Однопутная система трубопроводов конденсаторной воды	Двухпутная система трубопроводов конденсаторной воды	Двухпутная система трубопроводов конденсаторной воды

Продолжение таблицы D.4

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Установка с воздушным охлаждением				
Подводка электричества к механическому оборудованию	Один путь подачи питания к кондиционерному оборудованию	Один путь подачи питания к кондиционерному оборудованию	Несколько путей подачи питания к кондиционерному оборудованию	Несколько путей подачи питания к кондиционерному оборудованию
Регулирование влажности воздуха в серверной	Увлажнение предусмотрено	Увлажнение предусмотрено	Увлажнение предусмотрено	Увлажнение предусмотрено
Система управления ОВиК				
Система управления ОВиК	Отказ системы управления нарушит охлаждение критически важных зон	Отказ системы управления не нарушит охлаждения критически важных зон	Отказ системы управления не нарушит охлаждения критически важных зон	Отказ системы управления не нарушит охлаждения критически важных зон
Источник питания для системы управления ОВиК	Один путь подачи питания к системе управления ОВиК	Резервная подача питания от ИБП к кондиционерному оборудованию	Резервная подача питания от ИБП к кондиционерному оборудованию	Резервная подача питания от ИБП к кондиционерному оборудованию
Водопроводно-водоотводная сеть (для отвода тепла с помощью водяного охлаждения)				
Добавляемая вода	Один источник водоснабжения, на объекте нет резервного запаса воды	Два источника водоснабжения или один источник и запас воды на объекте	Два источника водоснабжения или один источник и запас воды на объекте	Два источника водоснабжения или один источник и запас воды на объекте

Окончание таблицы D.4

Наименование параметров	Уровень I	Уровень II	Уровень III	Уровень IV
Точки подключения к системе конденсаторной воды	Одна точка подключения	Одна точка подключения	Две точки подключения	Две точки подключения
Топливная система				
Резервуары для хранения топлива	Один резервуар	Несколько резервуаров	Несколько резервуаров	Несколько резервуаров
Насосы и трубопроводы резервуаров	Один насос и/или подводящий трубопровод	Несколько насосов, несколько подводящих трубопроводов	Несколько насосов, несколько подводящих трубопроводов	Несколько насосов, несколько подводящих трубопроводов
Пожаротушение				
Система пожарных извещателей	Да	Да	Да	Да
Спринклерная система	Когда требуется	Упреждающего действия (когда требуется)	Упреждающего действия (когда требуется)	Упреждающего действия (когда требуется)
Система раннего предупреждения с помощью дымовых извещателей	Нет	Да	Да	Да
Система течеискателей	Нет	Да	Да	Да

О'ЗДАХСОНТ АСОТЛОН
 СУЛЛАТЛАХСОНТЛАХСОНТ
 АСОТЛОН АСОТЛОН АСОТЛОН
 АСОТЛОН АСОТЛОН АСОТЛОН
 АСОТЛОН АСОТЛОН АСОТЛОН

Приложение Е (справочное)

Проектирование кабельной системы

Е.1 Длины кабелей для работы с разными приложениями

Е.1.1 Общие положения

Максимально допустимые длины кабелей, описываемые ниже, зависят от назначения кабельной системы и от вида кабельного носителя.

Кабель «витая пара» с сопротивлением $100\ \Omega$ (рекомендуется четырёхпарный кабель категории 6) используется в следующих основных случаях применения:

- соединения ЛВС с пропускной способностью 1000 Mbit/s;
- терминирования линий T1 и менее скоростных в зоне окончного оборудования;
- управления и текущего контроля (мониторинга) оборудования;
- управления по дополнительному (вспомогательному) каналу;
- управления энергоснабжением (питанием);
- системы охраны.

Коаксиальный кабель с сопротивлением $75\ \Omega$ (типа 734) используется в основном для подводки линий T-3 от провайдера доступа до зоны окончного оборудования. Современное многомодовое волокно $62,5/125\ \mu\text{m}$ ($160/500\ \text{MHz} \cdot \text{km}$) используется в следующих основных приложениях:

- Ethernet с пропускной способностью 1000 Mbit/s (1000BASE-SX);
- Fibre Channel с пропускной способностью 100 Mbit/s (100-M6-SN-I);
- Fibre Channel с пропускной способностью 200 Mbit/s (200-M6-SN-I).

Современное многомодовое волокно $50/125\ \mu\text{m}$ ($500/500\ \text{MHz} \cdot \text{km}$) используется в следующих основных приложениях:

- Ethernet с пропускной способностью 1000 Mbit/s (1000BASE-SX);
- Fibre Channel с пропускной способностью 100 Mbit/s (100-M5-SN-I);
- Fibre Channel с пропускной способностью 200 Mbit/s (200-M5-SN-I).

Оптимизированное для лазерных излучателей спектрального диапазона 850 nm многомодовое волокно $50/125\ \mu\text{m}$ ($1500/500\ \text{MHz} \cdot \text{km}$; эффективная модальная полоса частот $2000\ \text{MHz} \cdot \text{km}$) используется в следующих основных приложениях:

- Ethernet с пропускной способностью 1000 Mbit/s (1000BASE-SX);
- Ethernet с пропускной способностью $10\ \text{GHz} \cdot \text{km}$ (10GBASE-S);
- Fibre Channel с пропускной способностью 100 Mbit/s (100-M5-SN-I);

- Fibre Channel с пропускной способностью 200 Mbit/s (200-M5-SN-I);
- Fibre Channel с пропускной способностью 1200 Mbit/s (200-M5E-SN-I).

Одномодовое волокно используется в следующих основных приложениях:

- соединения ЛВС и ССХД с пропускной способностью 10 Gbit/s и выше;
- расстояния свыше рекомендуемых значений для многомодового волокна 50/125 μm , оптимизированного для лазерных излучателей спектрального диапазона 850 nm.

Е.1.2 Длины линий Т-1, Е-1, Т-3 и Е-3

В таблице Е.1 указаны максимальные длины кабелей для линий Т-1, Е-1, Т-3 и Е-3 без учёта промежуточных панелей переключений или розеток между точкой разграничения линий и оконечным оборудованием. Эти расчёты предполагают, что между точкой разграничения провайдера доступа (которая может являться коммутационной панелью цифровой связи, т.е. DSX-панелью) и оконечным оборудованием отсутствует коммутационная панель цифровой связи клиента.

Таблица Е.1 - Максимальные длины линий без DSX-панели клиента

Тип линии	Неэкранированная витая пара категории 3	Неэкранированная витая пара категорий 5е и 6	Коаксиал типа 734	Коаксиал типа 735
Т-1	159 m	193 m	-	-
СЕРТ-1 (Е-1)	116 m	146 m	332 m	148 m
Т-3	-	-	146 m	75 m
СЕРТ-3 (Е-3)	-	-	160 m	82 m
Примечание - Длины кабелей по данной таблице относятся к конкретным приложениям, используемым в датацентрах.				

Чтобы протянуть линию на расстояние свыше длин, указанных в таблице, можно использовать повторители.

Эти максимальные длины линий следует скорректировать с учётом потерь на затухание, создаваемых DSX-панелью клиента, расположенной между точкой разграничения провайдера доступа (которая может являться DSX-панелью) и оконечным оборудованием. В таблице Е.2 приведены значения поправок, учитывающих влияние DSX-панелей; эти значения следует вычесть из максимальных длин для линий Т-1, Т-3, Е-1 и Е-3 с официально признанными кабельными носителями.

Таблица Е.2 - Уменьшение максимальных длин линий из-за наличия DSX-панели клиента

Тип линии	Неэкранированная витая пара категории 3	Неэкранированная витая пара категорий 5е и 6	Коаксиал типа 734	Коаксиал типа 735
T-1	11 m	14 m	-	-
СЕРТ-1 (Е-1)	10 m	12 m	64 m	28 m
T-3	-	-	13 m	7 m
СЕРТ-3 (Е-3)	-	-	15 m	8 m

Максимальные длины линий следует скорректировать с учётом потерь на затухание, создаваемых промежуточными панелями переключений и розетками. В таблице Е.3 приведены значения поправок, которые следует вычесть из максимальных длин для линий Т-1, Т-3, Е-1 и Е-3 с официально признанными кабельными носителями.

Таблица Е.3 - Уменьшение максимальных длин линий в расчёте на каждую панель переключений или розетку

Тип линии	Неэкранированная витая пара категории 3	Неэкранированная витая пара категорий 5е и 6	Коаксиал типа 734	Коаксиал типа 735
T-1	4,0 m	1,9 m	-	-
СЕРТ-1 (Е-1)	3,9 m	2,0 m	4,4 m	2,0 m
T-3	-	-	0,9 m	0,5 m
СЕРТ-3 (Е-3)	-	-	1,1 m	0,5 m

В типичном датацентре имеются всего 3 соединения в магистрали, 3 соединения в горизонтальной кабельной системе и отсутствуют DSX-панели между точкой разграничения провайдера доступа и конечным оборудованием.

Магистраль:

- одно соединение в комнате ввода;
- два соединения в основной (главной) кросс-панели.

Горизонтальная кабельная система:

- два соединения в горизонтальной кросс-панели;
- одно соединение в розетке в аппаратной.

Эта «типичная» конфигурация соответствует типичному датацентру с комнатой ввода, главной распределительной зоной, одной или несколькими

кими горизонтальными распределительными зонами при отсутствии мест аппаратного распределения. Максимальные длины линий для этой типичной конфигурации датацентра приведены в таблице Е.4. Эти максимальные длины линий включают в себя магистральную кабельную систему, горизонтальную кабельную систему и все шнуры переключения или переключки между точкой разграничения провайдера доступа и окончательным оборудованием.

Таблица Е.4 - Максимальные длины линий для типичной конфигурации датацентра

Тип линии	Неэкранированная витая пара категории 3	Неэкранированная витая пара категорий 5е и 6	Коаксиал типа 734	Коаксиал типа 735
T-1	135 m	184 m	-	-
СЕРТ-1 (Е-1)	92 m	134 m	305 m	137 m
T-3	-	-	141 m	72 m
СЕРТ-3 (Е-3)	-	-	153 m	78 m

При максимальных длинах горизонтального кабеля и максимальных длинах шнуров переключения, при отсутствии DSX-панели клиента и отсутствии зонных розеток для «типичного» датацентра, в котором везде к оборудованию можно провести линии T-1, E-1, T-3 и E-3, максимальные длины магистрального кабеля указаны в таблице Е.5. Такая «типичная» конфигурация предполагает, что комната ввода, главная распределительная зона и горизонтальные распределительные зоны разделены, а не совмещены. Максимальная длина магистральной кабельной системы представляет собой сумму длин кабельной системы от комнаты ввода до главной распределительной зоны и от главной распределительной зоны до горизонтальной распределительной зоны.

Таблица Е.5 - Максимальная длина магистрали для типичной конфигурации датацентра

Тип линии	Неэкранированная витая пара категории 3	Неэкранированная витая пара категорий 5е и 6	Коаксиал типа 734	Коаксиал типа 735
T-1	<1 m	46 m	-	-
СЕРТ-1 (Е-1)	<1 m	<1 m	190 m	29 m
T-3	-	-	26 m	0 m

Окончание таблицы Е.5

Тип линии	Неэкранированная витая пара категории 3	Неэкранированная витая пара категорий 5е и 6	Коаксиал типа 734	Коаксиал типа 735
СЕРТ-3 (Е-3)	-	-	38 m	0 m

В этих расчётах предполагалось, что длины шнуров переключения в «типичном» датацентра имеют следующие максимальные значения:

- 10 m для неэкранированной витой пары и оптического кабеля в комнате ввода, главной распределительной зоне и горизонтальной распределительной зоне;

- 5 m для коаксиального кабеля типа 734 в комнате ввода, главной распределительной зоне и горизонтальной распределительной зоне;

- 2,5 m для коаксиального кабеля типа 735 в комнате ввода, главной распределительной зоне и горизонтальной распределительной зоне.

В связи с тем, что для линий Т-1, Т-3, Е-1 и Е-3 разрешены лишь очень короткие длины кабелей «витая пара» категории 3 и коаксиального кабеля типа 735, эти кабели (неэкранированная витая пара категории 3 и коаксиал 735) не рекомендуются для применения в таких линиях.

Длины магистральной кабельной системы можно увеличить путём лимитирования мест, где будут применяться линии Т-1, Е-1, Т-3 и Е-3 (например, только в главной распределительной зоне или в местах, обслуживаемых горизонтальной кабельной системой, терминируемой в главной распределительной зоне).

К числу других возможностей относится проектирование линий от оборудования, расположенного в главной распределительной зоне или в горизонтальной распределительной зоне.

Е.1.3 Консольные соединения RS232 и DB25/DB9

Рекомендуемые максимальные расстояния для консольных соединений типа RS232 и DB25/DB9 с пропускной способностью до 20 kbit/s:

- 23,2 m при использовании неэкранированного кабеля «витая пара» категории 3;

- 27,4 m при использовании неэкранированного кабеля «витая пара» категорий 5е или 6.

Рекомендуемые максимальные расстояния для консольных соединений типа RS232 и DB25/DB9 с пропускной способностью до 64 kbit/s:

- 8,1 m при использовании неэкранированного кабеля «витая пара» категории 3;

- 9,5 m при использовании неэкранированного кабеля «витая пара» категорий 5е или 6.

Рекомендуемые максимальные расстояния при использовании экранированных кабелей «витая пара» вдвое меньше, чем расстояния, разрешённые для неэкранированных кабелей «витая пара».

Е.2 Перекрёстные соединения

В комнате ввода, главной, промежуточной и горизонтальной распределительных зонах переключки и шнуры переключения, используемые для перекрёстного соединения с магистральной системой, должны иметь длину не более 20 м.

Единственным исключением из этого ограничения является применение коаксиальных кабелей с сопротивлением 75 Ω для переключения DS-3, термин, применяемый для обозначения цифровых сигналов с скоростью 45 Mbit/s, передаваемых по линии T-3); в этом случае максимальная длина составляет 5 м для коаксиала типа 734 и 2,5 м – для коаксиала типа 735 в комнате ввода, основной (главной), промежуточной и горизонтальных кросс-панелях.

Е.3 Разделение функций в главной распределительной зоне

Е.3.1 Основная (главная) коммутационная панель для кабелей «витая пара»

Основная (главная) коммутационная панель для кабелей из медных витых пар поддерживает медные кабели, пригодные для работы с широким кругом приложений, куда входят низкоскоростные линии, T-1, E-1, консоли, управление по дополнительному (вспомогательному) каналу, KVM-коммутаторы и ЛВС.

Следует предусмотреть возможность применения кабелей «витая пара» категории 6 для всей медной кабельной системы от основной (главной) кросс-панели до мест прямого соединения и телекоммуникационных помещений, поскольку это обеспечит максимальную гибкость для поддержки широкой номенклатуры приложений. Многопарный магистральный кабель (с числом витых пар 25 и более) категории 3 вполне пригоден для кабельной системы от основной (главной) кросс-панели до горизонтальной кросс-панели и точки разграничения низкоскоростной линии в комнате ввода. Кабельную систему от точки разграничения линий E-1/T-1 в комнате ввода следует выполнить четырехпарным кабелем категории 5е или категории 6.

Тип оконцевания кабелей в основной (главной) кросс-панели (соединительная арматура, предусматривающая контакт с прорезанием изоляции, т.е. IDC - оконцеватели, или же панели переключений) зависит от желаемой плотности и от того, где происходит переход от однопарной и двухпарной кабельной системы провайдера доступа к четырехпарной структурированной кабельной системе серверной:

ЎЗГАЎРАТ АСОЎЛА
ЎЗГАЎРАТ АСОЎЛА
ЎЗГАЎРАТ АСОЎЛА
ЎЗГАЎРАТ АСОЎЛА
ЎЗГАЎРАТ АСОЎЛА
ЎЗГАЎРАТ АСОЎЛА

- если этот переход от однопарной и двухпарной кабельной системы провайдера происходит в комнате ввода, то медный кабель в основной (главной) кросс-панели терминируется обычно на панелях переключений. Это рекомендуемая конфигурация;

- если этот переход от однопарной и двухпарной кабельной системы провайдера происходит в основной (главной) кросс-панели, то заделку медных пар кабеля в основной (главной) кросс-панели следует выполнять на IDC - оконцевателях.

Е.3.2 Основная (главная) коммутационная панель для коаксиальных кабелей

Основная (главная) коммутационная панель для коаксиальных кабелей поддерживает коаксиальные кабели, пригодные для линий Т-3 и Е-3 (два коаксиальных кабеля на каждую линию). Всю коаксиальную кабельную систему следует выполнять коаксиальным кабелем типа 734.

Коаксиальные кабели должны терминироваться на панелях переключений с 75-омными BNC - коннекторами. Как на передней, так и на задней поверхности панели переключений должны быть установлены BNC-коннекторы типа «гнездо».

Е.3.3 Основная (главная) коммутационная панель для оптических кабелей

Основная (главная) коммутационная панель для оптических кабелей поддерживает оптические кабели, пригодные для локальных вычислительных сетей, сетей системы хранения данных, общегородских сетей, компьютерных каналов и линий стандарта SONET.

Заделка оптических кабелей должна выполняться на оптических панелях переключений.

Е.4 Разделение функций в горизонтальной распределительной зоне

В горизонтальных распределительных зонах должны быть отдельные шкафы или стойки для распределения медных кабелей, коаксиальных кабелей и оптических кабелей, кроме тех случаев, когда горизонтальная коммутационная панель невелика и требует лишь одной - двух стоек. Отдельные стойки переключений для кабелей с медными парами, коаксиальных кабелей и оптических кабелей упрощают управление и минимизируют размер стойки каждого типа. Стойки переключений и оборудование необходимо располагать поближе друг к другу для уменьшения длины шнуров переключения.

Использование единого типа кабеля упрощает управление и повышает гибкость в отношении поддержки новых приложений. Существует возможность применения одного типа кабелей «витая пара» для всей гори-

зонтальной системы (например, все кабели неэкранированные с витыми парами категории 5е или же все кабели категории 6), вместо того, чтобы монтировать кабели «витая пара» нескольких разных типов для разных приложений.

Е.5 Кабельная система к оконечному оборудованию

Если кабельная система выполнена медными или оптическими кабелями, то соединительные шнуры от места должны иметь длину не более 22 m.

Если индивидуальные телекоммуникационные розетки находятся на той же аппаратной стойке или в том же шкафу, что и оборудование, обслуживаемое в месте зонного распределения, то длина соединительных шнуров не должна превышать 5 m.

Е.6 Особенности проектирования системы с оптическими кабелями

Высокая плотность размещения оконцевателей может быть достигнута за счёт использования многоволоконных удлинителей и многоволоконных коннекторов (соединителей). Если есть возможность заранее точно подсчитать длины кабелей, то можно сократить затраты времени на монтаж за счёт применения претерминированных многоволоконных ленточных кабельных сборок. В этих случаях следует учитывать влияние дополнительных соединений, чтобы обеспечить общее качество функционирования всей оптоволоконной системы. Оконечное оборудование с высокой скоростью передачи данных можно подключать непосредственно с помощью многоволоконных коннекторов.

Е.7 Особенности проектирования системы с кабелем типа витая пара

Панели переключений должны предоставлять достаточное пространство для маркировки каждой панели переключений её собственным идентификатором, а также маркировки каждого порта.

О'ЗДАСТ 2875
СТАНДАРТИЗАЦИЯ, РАКАТ
ИЗДАТ. Х. В. С. 2014
АДМИТ. Х. В. С. 2014
ДЛЯ СВО. РАКАТ

Приложение F (справочное)

Согласование проектов датацентров с поставщиками (провайдерами) услуг и доступа

F.1 Координация с провайдерами доступа

F.1.1 Общие положения

Проектировщики датацентров должны координировать свои действия с провайдерами доступа, чтобы определить требования провайдеров и обеспечить информирование провайдеров доступа о потребностях дата-центров.

F.1.2 Информация, которую нужно предоставить провайдерам доступа

Обычно провайдеры доступа запрашивают следующие сведения, необходимые для планирования комнат ввода для датацентров:

- адрес здания;
- общие сведения, касающиеся других пользователей здания, включая владельцев, арендаторов;
- планы телекоммуникационных кабельных каналов от внешнего контура владения до комнаты ввода, включая расположение смотровых люков, лазов для руки, коробок для протяжки кабеля;
- выделение кабелепроводов и внутренних лотков для провайдера доступа;
- поэтажные планы помещений ввода;
- назначенные места для принадлежащих провайдеру предохранительных устройств, стоек и шкафов;
- трассы кабелей внутри комнаты ввода (под фальшполами, по лестничным лоткам верхнего расположения и пр.);
- ожидаемое число и тип линий, которые должен предоставить провайдер доступа;
- дата, когда провайдер доступа сможет установить подводящие кабели и оборудование в комнате ввода;
- требуемое место и интерфейс для точки разграничения линий каждого типа, которые будет подводить провайдер доступа;
- требуемая дата сервиса;
- имя, номер телефона и адрес электронной почты контактного лица клиента и контактного лица на объекте.

F.1.3 Информация, которую должны предоставить провайдеры доступа

Провайдер доступа должен предоставить следующую информацию:

- требования к пространству и монтажу для протекторов (предохранительных устройств) на кабелях из медных пар;
- число и размеры стоек и шкафов провайдера доступа;
- требования к электропитанию для оборудования, включая типы штепсельных розеток;
- свободные промежутки для обслуживания;
- график монтажа и обслуживания.

Г.2 Разграничение с провайдером доступа в комнате ввода

Г.2.1 Организация

Комната ввода может иметь до четырёх отдельных зон для разграничения с провайдером доступа:

- разграничения для низкоскоростных кабельных линий из медных витых пар, включая DS-0, ISDN BRI и телефонные линии;
- разграничение для высокоскоростных медных линий DS-1 (T-1 или частичной T-1, ISDN BRI) или CEPT-1 (E-1);
- разграничение для линий на коаксиальном кабеле, включая DS-3 (T-3) и CEPT-3 (E-3);
- разграничение для линий на оптическом кабеле (например, SONET OC-x, SDHSTM-x, FDDI, FastEthernet, GigabitEthernet, 10 GigabitEthernet).

В идеальном случае все провайдеры доступа предусматривают разграничение для своих линий в одном и том же месте, а не на своих собственных стойках. Это упрощает перекрёстные переключения и управление линиями. Централизованное место для разграничения со всеми провайдерами доступа часто называют «зонами встреч» или «стойками встреч». Должны быть отдельные зоны или стойки встреч (разграничения) для линий каждого типа: низкоскоростных, E-1/T-1, E-3/T-3 и оптоволоконных. Кабельная система из серверной к комнате ввода должна терминироваться в зоне разграничения.

Если какой-либо провайдер доступа предпочитает разграничивать свои службы на своих собственных стойках, то клиент может проложить прямые связующие кабели от точки разграничения этого провайдера к желательной зоне встреч/разграничений.

Г.2.2 Разграничение низкоскоростных линий

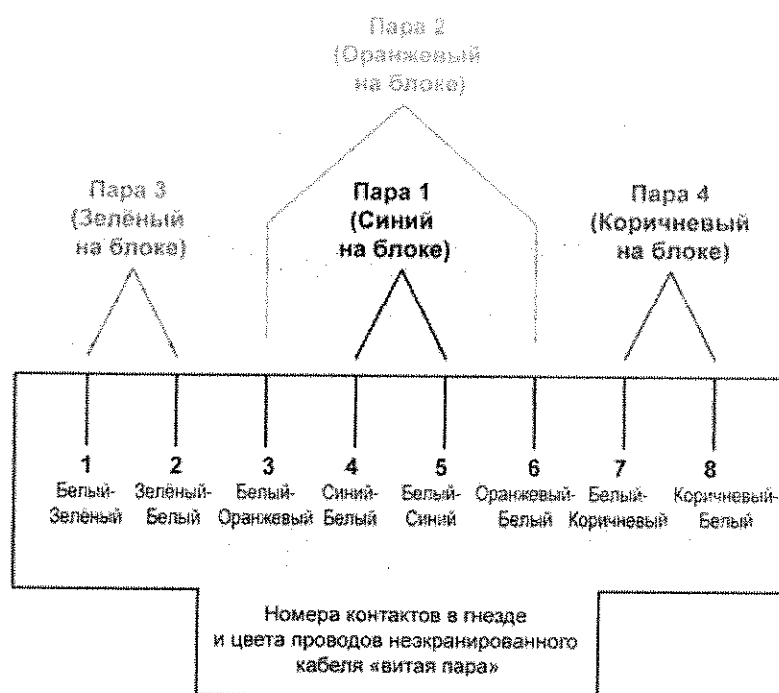
Провайдеры доступа должны обеспечить разграничение низкоскоростных линий на IDC-оконцевателях (соединительная арматура с прорезанием изоляции).

Кабельную систему от зоны разграничения низкоскоростной линии к главной распределительной зоне следует терминировать на IDC-оконцевателях рядом с IDC-оконцевателями провайдера доступа.

Линии от провайдера доступа терминируются в одной или двух парах IDC-оконцевателей. Разные линии имеют разные номера выводов, как показано на рисунках F.1 и F.2.

Каждый четырёхпарный кабель должен терминироваться в восьми-позиционном модульном гнезде в рабочей зоне.

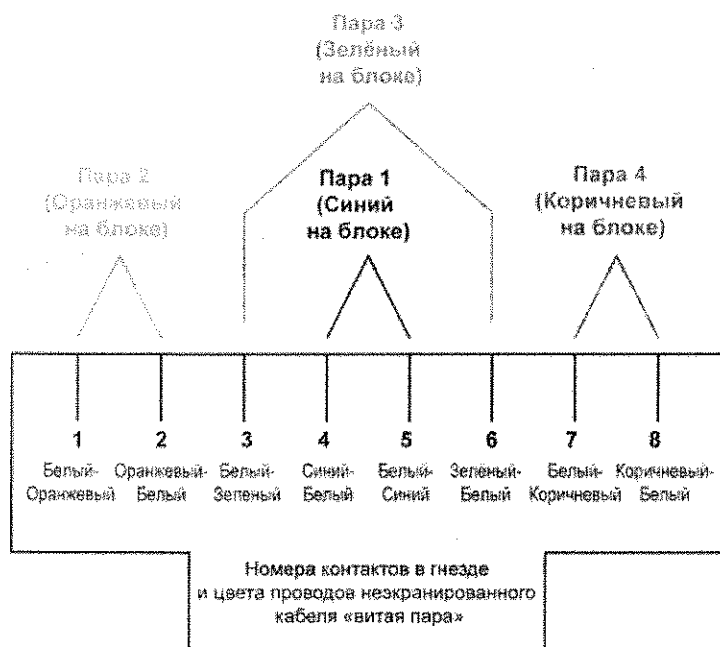
Схема распределения контактов/пар должна соответствовать рисунку F.1 или, как вариант, рисунку F.2, если необходимо приспособиться к определённой восьмиконтактной кабельной системе. Указанные на схеме цвета относятся к кабелю горизонтального распределения. На этих рисунках приведен вид спереди телекоммуникационной розетки/разъёма и показан перечень позиций пар для разных типов линий.



(Вид спереди на гнездо или сзади на разъём – штепсель)

1) телефонные линии однопарное перекрестное соединение с парой 1 (синий); 2) ISDN BRIU-интерфейс (U.S.): однопарное перекрестное соединение с парой 1 (синий); 3) ISDN BRIS/T-интерфейс(Intl.): двухпарное перекрестное соединение с парами 1 и 2 (синий и оранжевый); 4) арендуемая линия 56k/64k: двухпарное перекрестное соединение с парами 3 и 4 (зеленый и коричневый); 5) E1/T1: двухпарное перекрестное соединение с парами 1 и 3 (синий и зеленый); 6) 10Base-T/100Base-T: двухпарное перекрестное соединение с парами 2 и 3 (оранжевый и зеленый)

Рисунок F.1 - Линии кросс-панели к IDC-оконцевателю,
соединённому кабелем с модульными гнездами
в восьмиштырьковом ряду контактов T568A



(Вид спереди на гнездо или сзади на разъём – штепсель)

1) телефонные линии: однопарное перекрестное соединение с парой 1 (синий); 2) ISDNBRIU-интерфейс (U.S.): однопарное перекрестное соединение с парой 1 (синий); 3) ISDNBRIS/T-интерфейс (Intl.): двухпарное перекрестное соединение с парами 1 и 3 (синий и зелёный); 4) арендуемая линия 56k/64k: двухпарное перекрестное соединение с парами 2 и 4 (оранжевый и коричневый); 5) E1/T1: двухпарное перекрестное соединение с парами 1 и 2 (синий и оранжевый); 6) 10Base-T/100Base-T: двухпарное перекрёстное соединение с парами 2 и 3 (оранжевый и зелёный).

Рисунок F.2 - Линии кросс-панели к IDC-оконцевателю,
соединённому кабелем с модульными гнёздами
в восьмиштырьковом ряду контактов T568B

Переход от однопарной и двухпарной кабельной системы провайдера доступа к четырехпарной кабельной системе, используемой в структурированной кабельной системе датацентра, может происходить либо в зоне разграничения низкоскоростных линий, либо в главной распределительной зоне.

IDC-оконцеватели провайдера доступа и клиента могут быть смонтированы на фанерной доске, раме, стойке или в шкафу. Для монтажа большого числа IDC-оконцевателей (более 3000 пар) следует использовать двусторонние рамы.

F.2.3 Разграничение линий T-1

Провайдеры доступа должны передавать линии T-1 на разъемах RJ48X (индивидуальные восьмипозиционные модульные разъемы со шлейфом, предпочтительно на панели переключений DSX-1, смонтированной на принадлежащей клиенту стойке в зоне разграничения DS-1).

Панели переключений от нескольких провайдеров доступа и клиентов могут занимать одну и ту же стойку.

Для индикаторных ламп панелей переключений DSX-1 может потребоваться электропитание. Таким образом, стойки, поддерживающие провайдерские панели переключений DSX-1, должны иметь по крайней мере одну линию питания (20 A, 120 V) и многорозеточную силовую панель.

Место в стойке для панелей переключения, принадлежащих провайдеру доступа и клиенту, должно выбираться с учётом возможности наращивания. Провайдеру доступа может потребоваться место в стойке для размещения выпрямителей для питания панелей переключений DSX-1.

Провайдеры доступа также могут передавать линии DS-1 на IDC – оконцевателях. Эти IDC – оконцеватели можно разместить на той же самой раме, настенной доске, стойке или в том же шкафу, что и IDC – оконцеватели для низкоскоростных линий.

В одном четырехпарном кабеле можно поместить одну передающую и принимающую пару T1. Если же несколько сигналов T1 размещают в многопарном неэкранированном кабеле «витая пара», то передаваемые сигналы следует пустить по одному кабелю, а принимаемые сигналы – по другому.

Если у технического персонала датацентра имеется тестовое оборудование и он умеет диагностировать линии T-1, то в зоне разграничения DS-1 можно использовать панели DSX-1 для терминирования кабельной системы T-1, идущей к главной распределительной зоне. В этих панелях DSX-1 следует использовать либо модульные гнёзда, либо IDC – оконцеватели на задней стороне.

IDC-оконцеватели, панели переключений с модульными гнёздами или панели DSX-1 для кабельной системы к главной распределительной зоне могут находиться как на отдельных, так и в тех же самых стойках, рамах, шкафах, которые используются для панелей переключений DSX-1, принадлежащих провайдеру доступа. Если они отдельные, то их следует располагать рядом со стойками, предназначенными для провайдеров доступа.

Клиент (владелец датацентра) может по своему желанию предусмотреть свои собственные мультиплексоры (типа M13 или подобного типа) с тем, чтобы разделить (демультиплексировать) провайдерские линии T-3 на индивидуальные линии T-1. Эти линии T-1 от принадлежащего клиенту мультиплексора не следует терминировать в зоне разграничения T-1.

Г.2.4 Разграничение линий E-3 и T-3

Провайдеры доступа должны передавать линии E-3 или T-3 на парах BNC-коннекторов (соединителей) типа «гнездо», предпочтительно на панели переключений DSX-3, смонтированной на принадлежащей клиенту стойке, установленной в зоне разграничения E-3/T-3. Панели переключе-

ний от нескольких провайдеров доступа и клиентов могут занимать одну и ту же стойку.

Если у технического персонала датацентра имеется тестовое оборудование и он умеет диагностировать линии E-3 или T-3, то в зоне разграничения E-3/T-3 можно использовать панели DSX-3 для терминирования коаксиальной кабельной системы типа 734, идущей к главной распределительной зоне. В этих панелях DSX-3 следует использовать BNC-коннекторы на задней стороне.

Для индикаторных ламп панелей переключений DSX-3 может потребоваться электропитание. Таким образом, стойки, поддерживающие панели переключений DSX-3, принадлежащие провайдеру доступа, должны иметь, по крайней мере, одну линию питания (20 А, 120 В) и многорозеточную силовую панель.

Место в стойке для панелей переключений, принадлежащих провайдеру доступа и клиенту, должно выделяться с учетом возможности наращивания. Провайдеру доступа может потребоваться место в стойке для размещения выпрямителей для питания панелей переключений DSX-3.

Кабельную систему от зоны разграничения E-3/T-3 к главной распределительной зоне следует выполнить коаксиальным кабелем типа 734. Кабели в зоне разграничения E-3/T-3 можно терминировать на панели переключений, принадлежащей клиенту, с помощью BNC-коннекторов с сопротивлением 75 Ω либо прямо на панелях DSX-3, принадлежащих провайдеру доступа.

Все коннекторы и панели переключений для кабельной системы E-3 и T-3 должны использовать BNC-коннекторы с сопротивлением 75 Ω .

F.2.5 Разграничение оптоволоконных линий

Провайдеры доступа должны передавать оптические линии на оптических панелях, установленных в стойках в зоне разграничения оптоволоконных линий. Оптические панели переключений от нескольких провайдеров доступа и клиентов могут занимать одну и ту же стойку.

Стойки в зоне разграничения оптических линий не требуют электропитания, за исключением, возможно, сетевых розеток для принадлежащего провайдеру доступа и клиенту тестового оборудования.

Кабельная система от зоны разграничения оптических линий к главной распределительной зоне должна быть выполнена таким же типом кабеля, что и кабельная система провайдера доступа.

Приложение G (справочное)

Согласование планов размещения оборудования с персоналом, обслуживающим датацентры

Светильники должны располагаться в проходах между шкафами и стойками, а не прямо над рядами оборудования.

Оборудование и спринклеры в датацентрах должны быть расположены таким образом, чтобы высокие шкафы или кабелепроводы верхнего расположения не мешали разбрызгиванию воды из спринклеров – минимальный свободный зазор по высоте должен составлять 460 mm. Персоналу, обслуживающему датацентр, необходимо знать местоположение шкафов/стоек для оборудования и потребность в электропитании для них. Трассы силовых кабелей и штепсельных розеток должны быть взаимосвязаны с трассами телекоммуникационной кабельной разводки и расположением оборудования.

Персоналу, обслуживающему датацентр, необходимо знать требования к охлаждению шкафов/стоек. Кабельные лотки и телекоммуникационная кабельная разводка должны располагаться таким образом, чтобы обеспечить поддержание достаточного воздушного потока ко всем частям серверной. Воздушный поток от охлаждающего оборудования должен быть направлен параллельно рядам шкафов и стоек. Перфорированные плитки должны быть размещены в «холодных» проходах, а не в «горячих».

Трассы телекоммуникационной кабельной разводки должны быть размещены таким образом, чтобы расстояние кабелей «неэкранированная витая пара» от люминесцентных ламп было не менее 125 mm.

СЪЕДИНИТЕЛЬНЫЕ
СЪЕДИНИТЕЛЬНЫЕ
КАБЕЛИ ИЛИ КАБЕЛЬНЫЕ
КАБЕЛИ ИЛИ КАБЕЛЬНЫЕ
КАБЕЛИ ИЛИ КАБЕЛЬНЫЕ
КАБЕЛИ ИЛИ КАБЕЛЬНЫЕ

Библиография

[1] Правила устройства электроустановок. Раздел VII. Утверждены приказом инспекции «Узгосэнергонадзор» от 23 июня 2006 г. № 105, по согласованию с Министерством юстиции Республики Узбекистан отнесены к техническим документам 18 июля 2006 г., № 20-15-143/14

[2] Правила устройства электроустановок. Раздел I. Утверждены приказом инспекции «Узгосэнергонадзор» от 13 февраля 2004 г. № 84, по согласованию с Министерством юстиции Республики Узбекистан отнесены к техническим документам 27 февраля 2004 г., № 20-15-62/24

[illegible]

УДК 338.49

ОКС 35.020

П 85

Ключевые слова: информационная технология, информационная безопасность, датацентры, серверная, серверное оборудование, кабельная система, телекоммуникационные пространства

СЕРВИС АУДИТОРА
СТ. АУДИТОРА, АУДИТ
ИЗДАНИЕ: 11/01/2014
КАДРОВАЯ КОМПЕТЕНЦИЯ
ЮРИДИЧЕСКОГО

O'z DSt 2014

Заместитель директора
Центра UZINFOCOM

Ведущий специалист
отдела технической
безопасности

Специалист 1-категории
отдела технической
безопасности

Нормоконтроль

СОГЛАСОВАНО

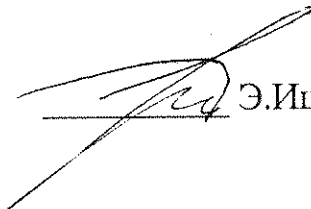
Начальник отдела
информационной безопасности
Государственного комитета
связи, информатизации и
телекоммуникационных
технологий Республики
Узбекистан


А.Гафуров
письмо от 21.01.2014
№ 14-8/357

Начальник отдела
телекоммуникационных
технологий и услуг
Государственного комитета
связи, информатизации и
телекоммуникационных
технологий Республики
Узбекистан

З.Зияев
письмо от 22.01.2014
№ 09-8/365

СЛУЖБА НАЦИОНАЛЬНОЙ
БЕЗОПАСНОСТИ РЕСПУБЛИКИ
УЗБЕКИСТАН
ОТДЕЛ ТЕХНИЧЕСКОЙ
БЕЗОПАСНОСТИ

 Э.Ишимбаев

 Д.Палеев

 О.Каримов

 Л.Шаймарданова
02.07.2014

СОГЛАСОВАНО

Вр.и.о. ГУП Центр научно-
технических и маркетинговых
исследований «UNICON.UZ»

Х.Хасанов
письмо от 17.01.2014
№ 31-05.6/114

СОГЛАСОВАНО

Служба национальной
безопасности Республики
Узбекистан

письмо от 25.06.2014
№ 33/2266