Архитектура параллельных вычислительных систем

к.т.н., доцент
Костичев Сергей Валентинович

Инфраструктура суперкомпьютерных центров

snenv@mail.ru

Учебные вопросы:

1. **Центр обработки данных**
   Требования, предъявляемые к ЦОД
2. **Уровни надежности ЦОД**
   Характеристики уровней надежности
3. **Сертификация ЦОД**

4. **Структура ЦОД и этапы построения**

Прогноз Allied Market Research:

к 2022 году рынок центров обработки данных вырастет до 71,2 млрд долларов.

1. Центр обработки данных

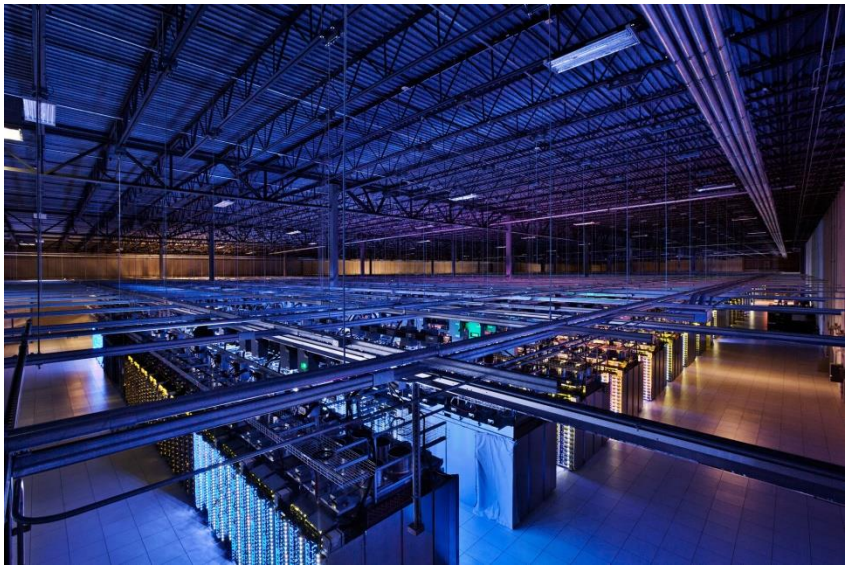
Центр обработки данных (ЦОД) = дата-центр — это отказоустойчивая комплексная централизованная система, обеспечивающая автоматизацию бизнес-процессов с высоким уровнем производительности и качеством предоставляемых сервисов.

ЦОД - это сложный комплекс

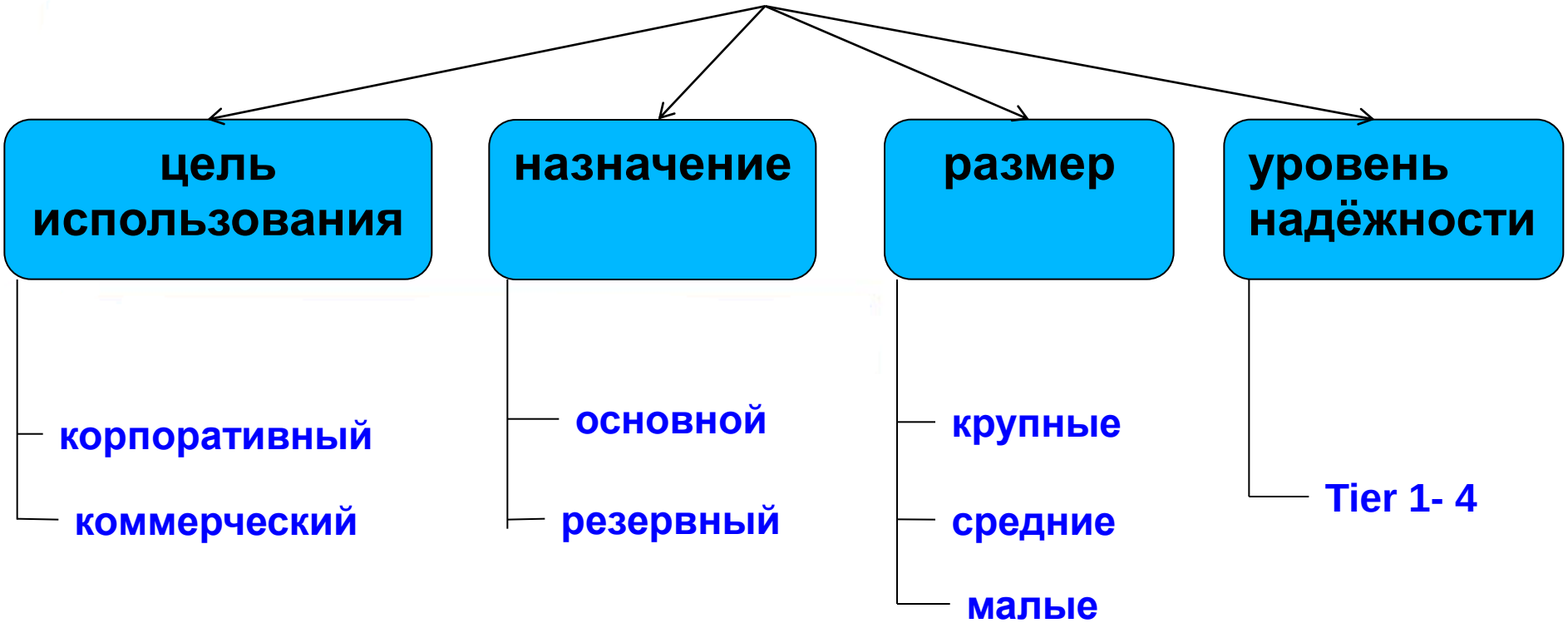
- IT решений,
- высокотехнологичного оборудования,
- строительных и инженерных конструкций

Основные функции ЦОД:

- хранение,
- быстрая обработка любого объема данных,
- передача и выдача информации в стандартизированном виде пользователю



Центры обработки данных



Центр обработки данных

Основные разновидности:

- **Внутренние (корпоративные)**

  В рамках конкретного предприятия.

  Достоинства :

  - прямое управлении всей системой,
  - обеспечение безопасности данных и сохранности коммерческой тайны,
  - процесс восстановления поврежденных систем пройдет гораздо быстрее,
  - автономная работа оборудования,
  - быстрое реагирование на различные внештатные ситуации

Причины перехода от внутренних к коммерческим ЦОД .

- **недостаточная надежность** внутреннего ЦОД, не отвечающая требованиям бизнеса (частые отключения электроэнергии).

- **невозможность расширения** инфраструктуры из-за имеющихся ограничений по площадям и/или доступной мощности.

- **невозможность резервирования** интернет-каналов за счет подключения дополнительных операторов. Например, бизнес-центры нередко ограничивают выбор провайдера арендаторами.

Причины перехода от внутренних к коммерческим ЦОД .

- **риски** существующего решения: отсутствие катастрофоустойчивости и недостаточная физическая безопасность оборудования, комплексное несоответствие требованиям TIER 3 (электропитание, охлаждение, пожаротушение, обслуживание в режиме 24*7).

- **высокие капитальные затраты** и длительные сроки строительства внутреннего ЦОД.

Основные разновидности:

- **Коммерческие**.

  Для аренды.

  Характеристики:

  - высокая производительность,
  - максимальная скорость обмена данными,
  - виртуальность ЦОД.

  Достоинства:

  - самостоятельная настройка конфигурации системы,
  - дистанционное управление,
  - экономия средств на строительство и обслуживание собственного ЦОДа

Услуги коммерческих ЦОД

- **Виртуальный сервер.** Предоставление в аренду части дискового пространства, процессорного времени и оперативной памяти (один физический сервер делится между множеством клиентов).

- **Выделенный сервер.** ЦОД предоставляет клиенту в аренду сервер в различной конфигурации.

- **Colocation.** Размещение сервера клиента на площадке ЦОД за плату.

- **Выделенная зона.** Владельцы ЦОД выделяют часть технологических площадей для специальных клиентов,

Основным требованием, предъявляемым к ЦОД является **отказоустойчивость**.

Отказоустойчивость ЦОД определяет **уровень надежности** ЦОД.

При этом подразумевается отключение ЦОД

- на время планово-предупредительных работ и профилактики оборудования,
- внеплановых аварийных ситуаций.

Определения

Надёжность (Dependability).

Это свойство технических объектов сохранять во времени в установленных пределах значения всех параметров, необходимых для выполнения требуемых функций в заданных режимах и условиях применения.

Отказоустойчивость (Fault Tolerance).

Это свойство технической системы сохранять свою работоспособность после отказа одного или нескольких компонентов.

- Определяется количеством любых последовательных единичных отказов элементов системы, после которых сохраняется ее работоспособность в целом.

- Главное назначение отказоустойчивости заключается в способности системы скрывать от пользователя отказ отдельных ее элементов.

Безотказность (**Reliability**) - это способность системы или элемента корректно, безотказно функционировать в заданных условиях в течение установленного периода времени. Иногда **безотказность трактуется как доступность**

Безопасность (**Security**) – это организация защиты объекта от нежелательных действий.

Живучесть (**Survivability**). Живучесть системы характеризует ее способность сохранять полную или частичную работоспособность при действии причин, кроющихся за пределами системы и приводящих к разрушениям или значительным повреждениям некоторой части ее элементов

Иногда **безопасность трактуется как живучесть** системы при любом типе злонамеренных воздействий.

Непрерывность бизнеса. Она включает в себя процессы и методы, направленные на обеспечение безостановочного выполнение критичных бизнес-функций.

Катастрофоустойчивость. Это способность к восстановлению после катастрофы т.е. устойчивость к воздействию аварий и природных катаклизмов.

Комплексная безопасность ЦОД включает защиту от следующих угроз:

- отказ оборудования и программного обеспечения,
- сбои энергопитания,
- пожар и задымление,
- несанкционированный доступ, взлом, кражи,
- вирусы,
- затопление, резкие температурные изменения, пыль,
- частичное разрушение здания,
- электромагнитные излучения.

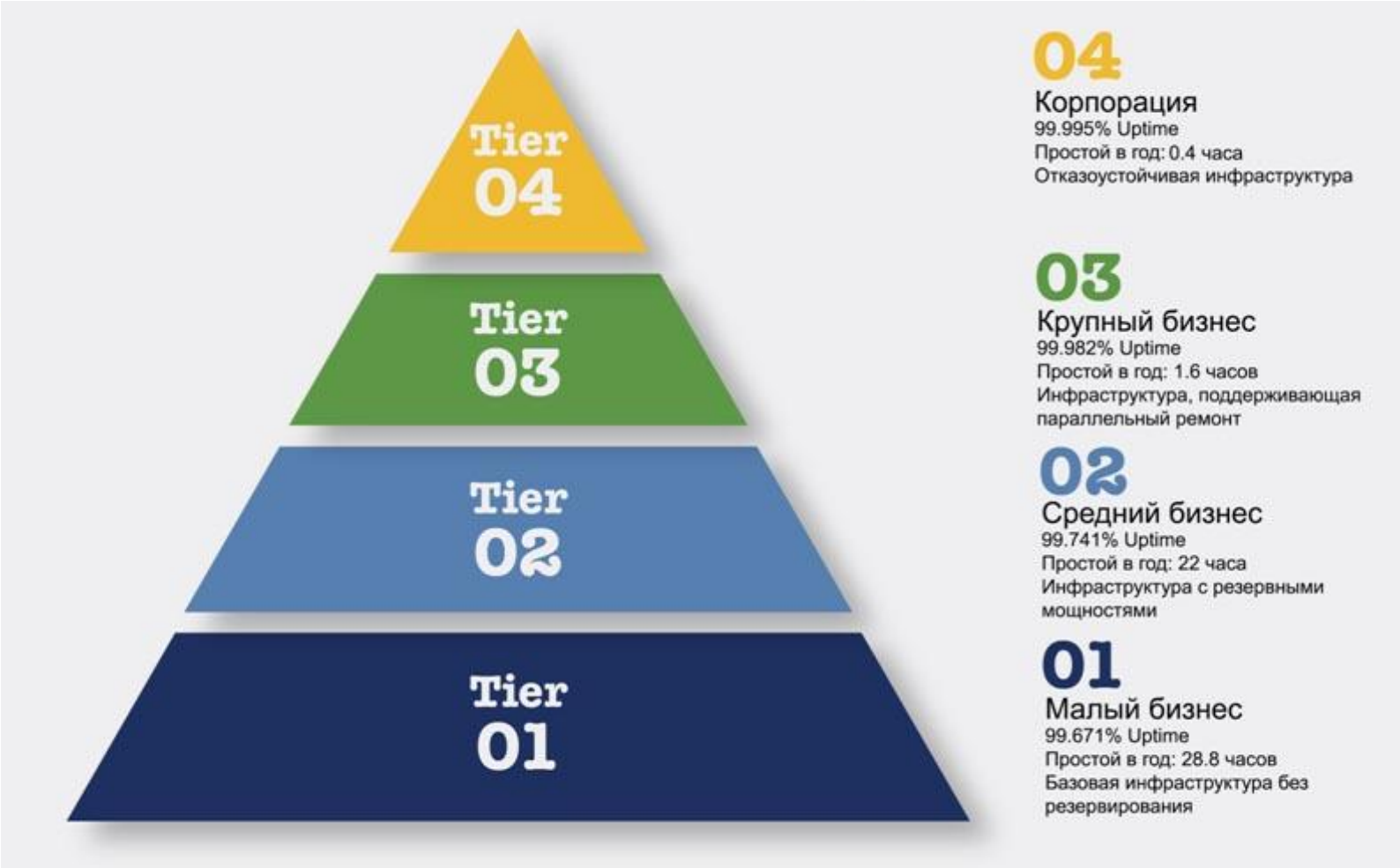
2. Уровни надежности ЦОД

- **Цель** введения классификации по уровням надежности - **избежать неопределенностей**
  - при формировании технического задания к строящимся ЦОД
  - при описании характеристик уже функционирующих ЦОД.

- Понятие отказоустойчивости ЦОД определяет и отказоустойчивость каждой из систем ЦОД. → уровень надежности накладывает определенные требования сразу на всю инфраструктуру ЦОД → **выбранный уровень надежности целиком определяет концепцию ЦОД**.

- В 2000-ных годах были разработаны стандарты надежности ЦОД, от 1-го до 4-го уровня

Четыре уровня надежности ЦОД: Tier 1 - 4 введены организацией Uptime Institute (Институт Бесперебойных Процессов, США).



Tier 1 — первый уровень надежности ЦОД (базовый)

- широко применялся в 1960–1970 годы.
- системы оборудованы в небольших или средних офисах, под них выделено одно помещение
- **главная задача** – поддержка серверной составляющей для обмена информации внутри офиса и передачи ее через интернет другим пользователям.
- **два критерия**, которые относятся к этому уровню:
  - установленные источники бесперебойного питания
  - охлаждение в зависимости от тепловыделения.

Характеристики Tier 1 :

- ошибки или отказ в работе систем или оборудования приводят к сбоям в работе всего ЦОД.
- инженерная инфраструктура способна удовлетворить исключительно текущие потребности, **без резервирования и избыточности ресурсов**.
- время простоя за год - 28,8 часа,
- коэффициент отказоустойчивости - 99,671 %.
- время ввода в эксплуатацию – 3 месяца

Tier 2 — второй уровень надежности ЦОД
(резервирование основных компонентов инфраструктуры)

Для перехода от Tier 1 к Tier 2 **требуется дополнительное (резервное) оборудование**

Характеристики:

- ошибки или отказ в работе систем или оборудования могут привести к сбоям в работе всего ЦОД.
- возможность **резервирования критически важных компонентов**. Стандарт предусматривает наличие избыточных системных ресурсов, улучшенные системы охлаждения и энергоснабжения.
- проведение ремонтных работ требует остановки ЦОД.
- время простоя за год - 22 часа,
- коэффициент отказоустойчивости - 99,741 %.
- время ввода в эксплуатацию от 3 до 6 месяцев

Tier 3 — третий уровень надежности ЦОД
(параллельно обслуживаемая инфраструктура)

Кроме резервных мощностей, **присутствует отдельный канал с питанием и охлаждением.**

Характеристики:

- все ИТ-оборудование имеет двойное электропитание
- не требуется прекращение работы ЦОД для проведения ремонтно-профилактических мероприятий, включая замену оборудования или модернизацию компонентов системы.
- время простоя за год - 1,6 часа
- коэффициент отказоустойчивости - 99,98 %.
- время ввода в эксплуатацию от 15 до 20 месяцев

Tier 4 — четвертый уровень надежности ЦОД (отказоустойчивая инфраструктура)

Стал возможным после появления компьютеров с двумя взаимно резервирующими источниками питания

Характеристики:

- **резервирование** всех систем, повышенная отказоустойчивость
- резервные системы и каналы коммуникаций физически изолированы от основных систем и друг от друга
- требуется **непрерывное охлаждение**
- требуется выделенное пространство, **изолированность**
- не требуется прекращение работы ЦОД, как для плановых, так и внеплановых работ
- время простоя за год - 0,4 часа,
- коэффициент отказоустойчивости - 99,995 %.
- время ввода в эксплуатацию от 15 до 30 месяцев

- Для уровней Tier 3 и 4 **машинный генератор электроэнергии** - основной источник питания. Местное питание от подводящего электрического кабеля считается альтернативой.

- Отключение питания на подводящем кабеле рассматривается как ожидаемое эксплуатационное условие, к которому ЦОД должен быть подготовлен.

Основной показатель, определяющий Tier - возможность проведения профилактических работ без полной остановки ЦОД

Таблица характеристик Tier

Параметр	Tier 1	Tier 2	Tier 3	Tier 4
Год внедрения	1965	1970	1985	1995
Время простоя за год, ч	28.8	22	1.6	0.4
Уровень загрузки оборудования	100 %	100 %	90 %	90 %
Обслуживание без отключения	Нет	Нет	Да	Да
Аварийность	6 аварий за 5 лет	1 авария в год	1 авария за 2,5 года	1 авария за 5 лет
Отказоустойчивость как одиночное событие	Нет	Нет	Нет	Да
Стоимость инфраструктуры евро/кв.м	4800	6500	9700	от 12000

Выводы и следствия

- **в Tier 2 и Tier 3 резкая разница в длительности допустимого простоя за год** (22 и 1.6 часа) при одинаковой схеме резервирования. Это 2 разные категории, связанные с проведением плановых работ:
  - Tier 2 подразумевает, возможность обесточить весь ЦОД,
  - Tier 3 исключает эту возможность.

- если длительность простоя с учетом плановых работ составляет 22 часа в год, а без учета - 1.6 часа в год, то **простой в связи с плановыми работами должен составить 20.4 часа в год.**

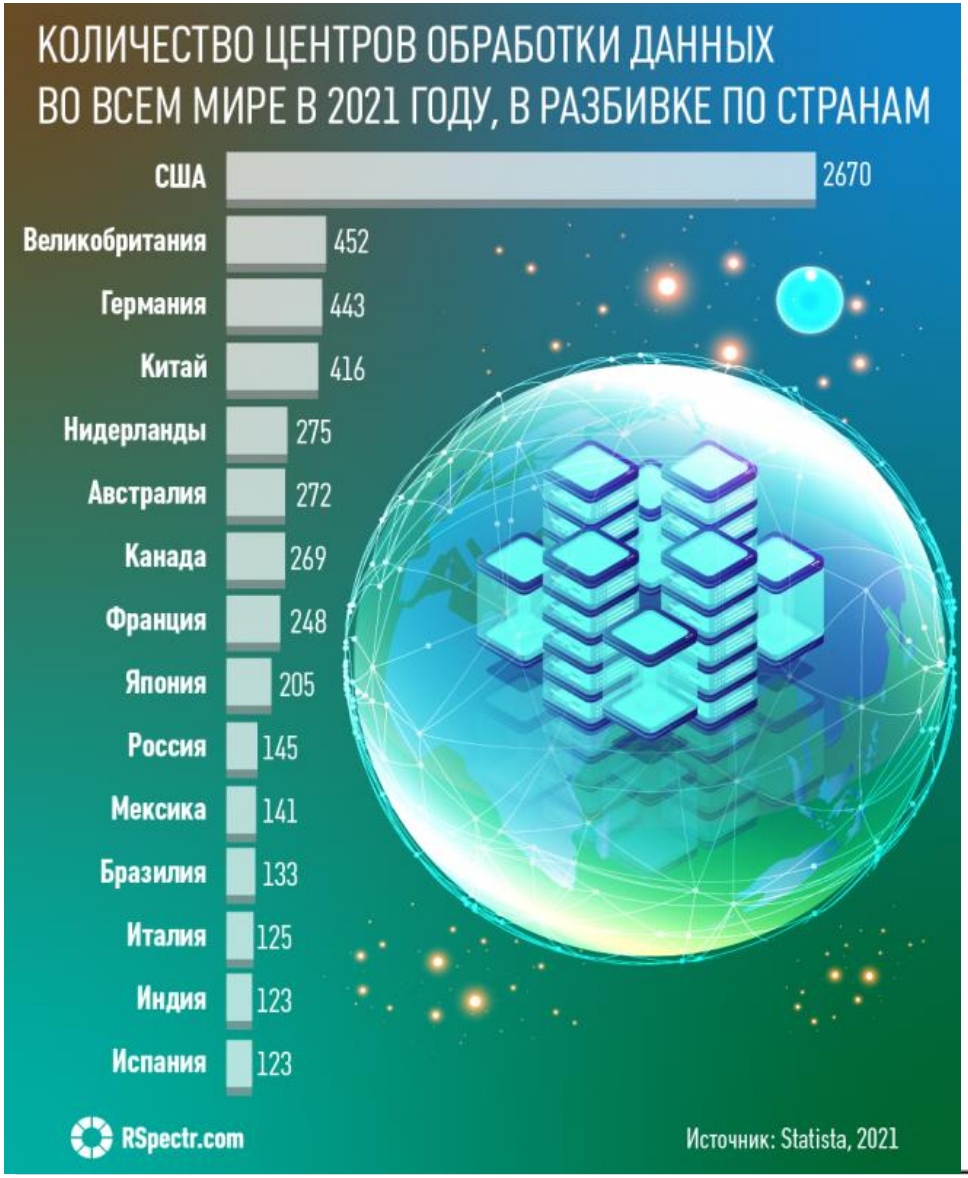
- для ЦОД с системой холодоснабжения на основе чиллеров (водоохлаждающая машина) **Tier 3** требует **резервирования трубопроводов: и прямого и обратного**. Опыт: иногда, стремясь достичь Tier 3, резерв труб не предусматривается

- критичность современных бизнес-процессов велика: простой в 20-25 минут в год приводит к огромным убыткам для компании. → **должен появиться 5-й уровень** надежности ЦОД с характеритиками
    - время простоя за год - 8.8 минут в год,
    - коэффициент отказоустойчивости - 99,999 **%.**

3.Сертификация ЦОД

Сертификация ЦОД проводится организацией Uptime Institute:

- владелец ЦОД обращается в Uptime Institute и предоставляет полный набор документации, включая описание всех систем (электрической, механической, мониторинговой и всех других)
- сотрудники этой организации проводят независимый объективный анализ инфраструктуры, лично посещают ЦОД , сравнивают документацию и реальную ситуацию. Главная задача - **обнаружение слабых мест в реальной инфраструктуре** и изучение недоработок на месте.
- присваивается уровень классификации Tier.



В настоящий момент в мире около 10% ЦОД прошли сертификацию Uptime Institute.

Самый актуальный стандарт проектирования и построения ЦОД — Tier 3

Доля ЦОДов РФ не превышает 5% от всего объема дата-центров

Почему сертифицированные отказоустойчивые ЦОДы аварийно встают?

Два основных документа при обсуждении стандартов ЦОД:

- стандарт **TIA 942** и
- классификация по уровням от **Uptime Institute**.

Оба документа регламентируют уровни (Tier) → путаница: Tier 3 по TIA 942 отличается от Tier 3 по Uptime Institute

TIA 942 — Telecommunications Industry Association — Telecommunications Infrastructure Standard for Data Centers:

- Этот стандарт касается вопросов организации структурированных кабельных систем в ЦОД, и **в меньшей степени вопросов отказоустойчивости** и других инженерных подсистем.
- Носит **рекомендательный** характер.
- Есть пошаговые инструкции и рекомендуемые схемы (помощь инженеру). «Делай как тут написано и получишь хороший результат».
- Соответствие стандарту заявляется владельцем объекта или исполнителем проекта (на уровне «Я делал как вы сказали, *честное слово*»).
- На соответствие стандарту проверяется **только проектная** документация.
- Однажды реализованный объект не теряет уровень.

Uptime Institute — Tier Classifications Define Site Infrastructure Performance

- Этот документ - методология, разработанная специально для нормирования отказоустойчивости ЦОД.
- Носит **обязательный** характер.
- Нет пошаговых инструкций, но **есть сформулированные основные принципы проектирования и подходы**. «Делай по таким принципам и получишь отказоустойчивый объект».
- Сертификация осуществляется **только самим Uptime Institute**.

Uptime Institute — Tier Classifications Define Site Infrastructure Performance (продолжение)

- **Сертифицируется как проект, так и полученный результат** (запущенная площадка). Проверяется, что именно получилось в результате:
  - Tier Certification of Design Documents,
  - Tier Certification of Constructed Facility,
  - **регулярно**, раз в год, три или пять уже сама эксплуатация (Operational Sustainability Certification) на предмет её соответствия стандарту.

Отличаются принципы оценки TIA 942 и Uptime Institute :

TIA : «Делай точно как написано, и всё будет ОК»,

Uptime Institute : «У тебя должно быть всё ОК любыми методами, в соответствии с заданными принципами, а потом мы проверим что оно работает».

Вывод:
есть огромная разница между сертификацией проекта без проверки на месте и сертификацией работающей площадки с конкретной проверкой на месте.

- Иногда (особенно в России) для описания инфраструктуры ЦОДа прибегают к **дробным уровням** (например, Tier 2.5, Tier 3 +, расширенный Tier 3 или Tier 4-lite). Такие обозначения инфраструктуры ЦОДа являются **нелегитимными**.

- Uptime Institute **признает только четыре уровня** (Tier), и отклонение от критериев уровня в любой инженерной подсистеме является запретом для сертификации ЦОДа в целом на этом уровне.

Энергоэффективность

Важный параметр ЦОД — эффективность использования энергии (PUE, Power Usage Effectiveness).

$$PUE = \frac{\text{Общее энергопотребление}}{\text{Энергопотребление IT-оборудования}}$$

- PUE помогает спрогнозировать возможность дальнейшей модернизации ЦОД и переоборудование электроснабжения для повышения эффективности эксплуатации.
- Эталон PUE < 1,25, оптимальный 1,25~1,43, хороший — 1,43~1,67.
- Основной потребитель электроэнергии в ЦОД:
  - 45% система охлаждения.
  - 20% теряется при распределении электроэнергии.

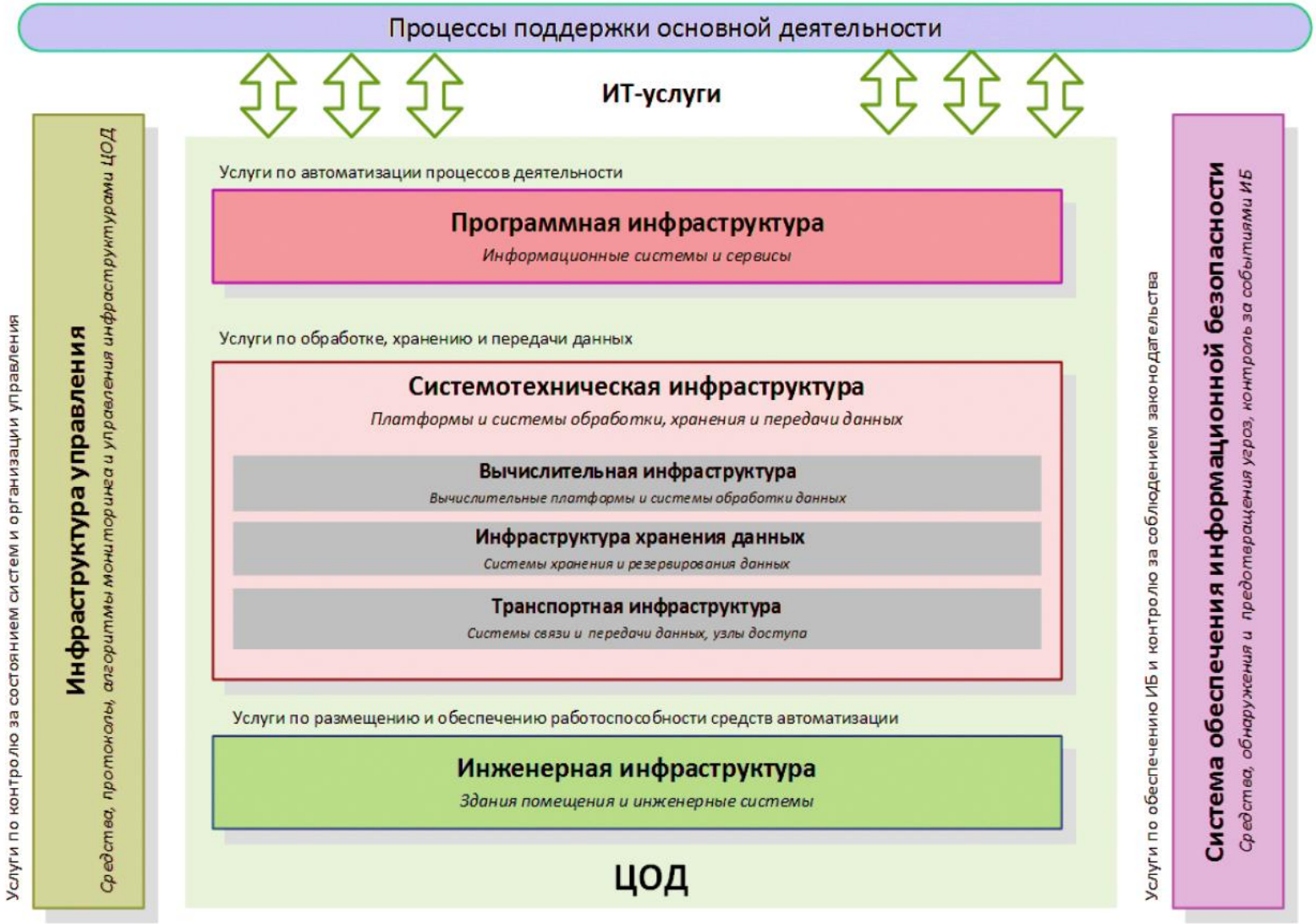
4. Структура ЦОД

Включает 3 технологических блока

- информационный
- телекоммуникационный
- инженерный

и **системы**

- мониторинга, управления и диспетчеризации
- обеспечения безопасности



Структура ЦОД

Информационная инфраструктура:

- высоконадежное серверное оборудование
- системы хранения данных
- системы резервного копирования и восстановления данных

Серверный комплекс ЦОД:

- ресурсные серверы, отвечающих за сохранение и предоставление данных серверам приложений (файл-серверы)
- серверы приложений выполняют обработку данных в соответствии с бизнес-логикой системы
- серверы предоставления информации осуществляют интерфейс между пользователем и серверами приложений (web-серверы)
- служебные серверы обеспечивают работу других подсистем ЦОД (серверы управления системой резервного копирования)

Сетевая и телекоммуникационная инфраструктура

- обеспечивает
  - взаимодействие между серверами,
  - объединяет логические уровни
  - образует каналы связи
    - магистральные соединения с операторами связи
    - каналы, обеспечивающие доступ пользователей к ресурсам ЦОД.
- позволяет осуществлять взаимосвязь элементов ЦОДа, взаимодействие между ЦОДом и пользователями

Информационная и телекоммуникационная инфраструктуры **- сердце ЦОД**, отвечают за производительность, доступность данных и приложений

- В качестве систем хранения данных используются массивы SATA/SSD/SAS

- В качестве серверных процессоров используется линейка серверных процессоров Intel Xeon:
  - в ЦОД начального уровня ставят Intel Xeon класса Silver (модель CPU Intel Xeon Silver 4414 Skylake 2,2GHz с L3-кэшем 14080Kb)
  - в продвинутых конфигурациях Xeon Gold 6254 с L3-кэшем в 25 Mb

Инженерная инфраструктура

Обеспечивает нормальное функционирование основных систем ЦОДа.
Включает **подсистемы контроля** :

- бесперебойного энергообеспечения, а так же фильтрации помехи магистральной сети и стабилизации выходного напряжение
- охлаждения
- климата, кондиционирования **и** вентиляция
- пожаротушения и т.д.

Требования к инженерной инфраструктуре ЦОД

Основные требования

1. Надежность

Достигается за счет:

- использования только современного оборудования ведущих мировых производителей,
- привлечения высококвалифицированных специалистов
- резервирования основных узлов инженерной инфраструктуры.

2. Управляемость

Управление должно позволять прогнозировать все возможные сбои и поломки оборудования для заблаговременного предотвращения аварий.

3. Безопасность

Необходима тщательная проработка всех потенциальных угроз:

- технические сбои,
- любые несанкционированные действия

4. Масштабируемость

Все системы инженерного обеспечения ЦОД должны гибко адаптироваться к растущим потребностям

Дополнительные требования

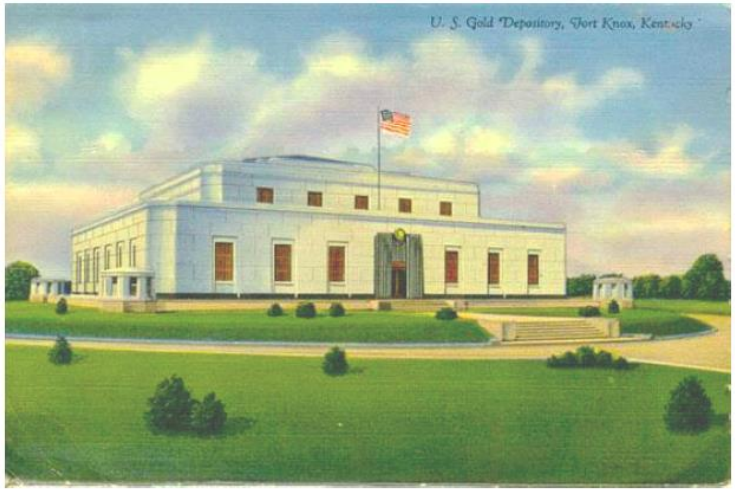
- долгий срок службы
- легкий доступ к отдельным компонентам подсистем для ремонта и диагностики
- бесперебойная подача электроэнергии
- низкая совокупная стоимость владения

Системы мониторинга, управления и диспетчеризации

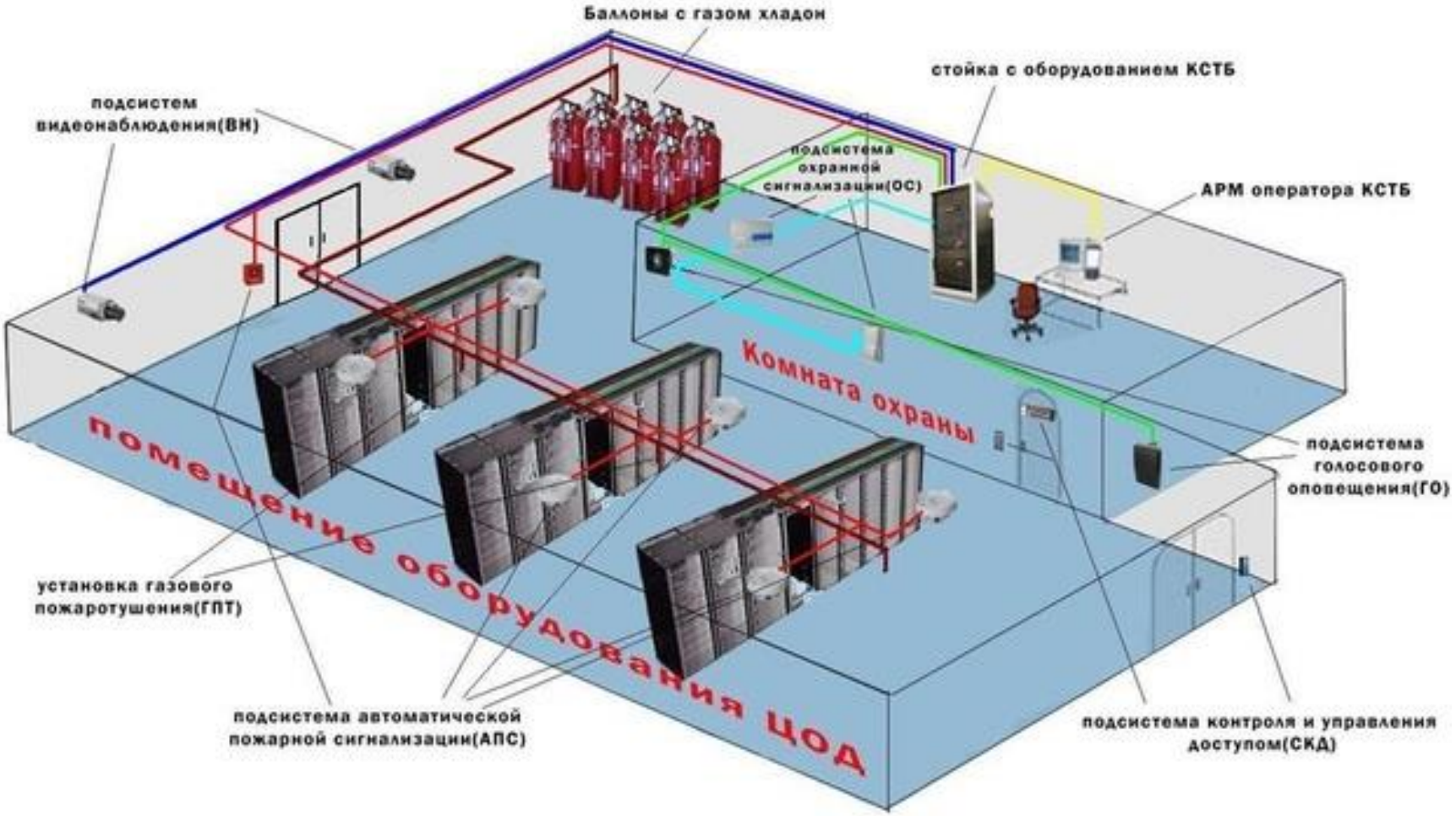
- Включают
  - **подсистему оповещения** и прогнозирования отказов оборудования, критических ситуаций в ЦОДе.
  - **информирование** обслуживающего персонала посредством всех доступных интерфейсов связи: e-mail, sms, автоматический дозвон.
- Позволяют создать в ЦОД централизованный мониторинг параметров систем и их состояний: напряжения электропитания, температуры в стойках, температуры воздуха и т.д.
- Снижает риски возникновения аварийных ситуаций.
- Уменьшают негативное влияния «человеческого фактора».

Системы безопасности ЦОД:

- информационная безопасность
- видеонаблюдение
- система контроля управления доступом (СКУД)
- системы охранной сигнализации и оповещения
- система противопожарной безопасности и пожаротушения (ключевую роль играют инструменты раннего обнаружения дыма)



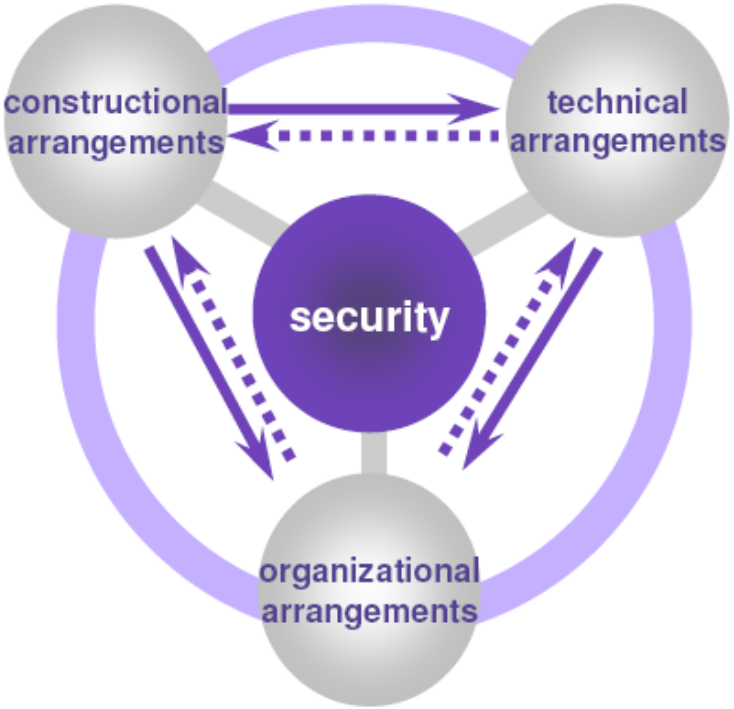
Комплесная система технической безопасности(КСТБ) в центер обработки данных(ЦОД).



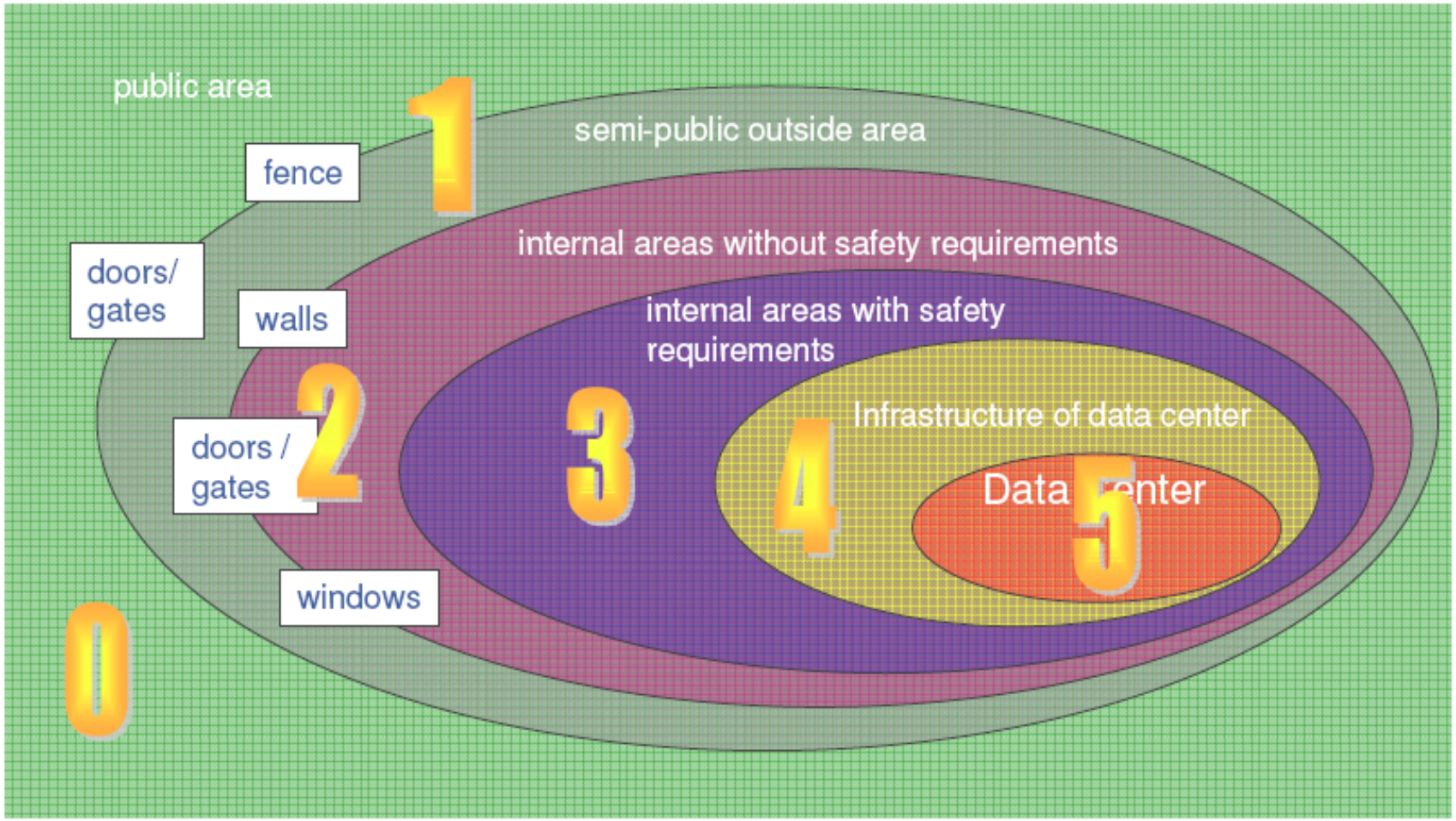
Что же это такое?

Безопасность – это пересечение

- **конструкционных,**
- **технических и**
- **организационных мероприятий**



Безопасность – принцип луковой кожуры



Зона 1

Площади

- Внешние территории
- Парковки

Мероприятия

- Огораживание территории изгородью
- Барьерные растения вокруг парковок
- Контроль доступа охраной
- Видео наблюдения входов
- Защита периметра сенсорными кабелями или лазерными сканерами
- Возможно: распознавание

Зона 2

Площади

- Офисы, не требующие особого режима
- Входы в здание и пути эвакуации

Мероприятия

- Допуск в эти области должен быть контролируемым
- Допуск в здание из внешней области должен быть контролируемым
- Двери во вне должны контролироваться на открывание и запирание противовзломной тревожной сигнализацией

Зона 3

Площади

- Офисы, требующие особого режима безопасности
- Технические помещения безотносительно значимости для ЦОД

Мероприятия

- Строить как отдельную функциональную единицу
- Осуществление допуска только из второй контролируемой зоны
- Двери во вне должны контролироваться на открывание и запирание противовзломной тревожной сигнализацией

Зона 4

Площади

- Техническая инфраструктура ЦОД
- Каналы внутридомовой связи (электричество, телефон, интернет, IT)

Мероприятия

- Строить как отдельную функциональную единицу
- Мероприятия по защите от дыма
- Функциональная целостность в случае пожара на время 90 минут
- Двери в зоне должны контролироваться на открывание и запирание противовзломной тревожной сигнализацией
- Двойной контроль допуска (биометрический, PIN)
- Видео наблюдение дверей
- Детектирование и мероприятия против элементарных повреждений (огонь, вода, газ) и проникновения (датчики движения, тревожные системы)

Зона 5

Площади

- Серверная (компьютерный зал)

Мероприятия

- Все мероприятия для зоны 4
- Ограничение доступа с ловушками
- Помещение не имеет окон и не примыкает вплотную к внешним стенам здания
- Системы пожаротушения или постоянное снижения доли кислорода

Процесс построения ЦОД состоит из четырех этапов:

- **Формирование концепции** (анализ задач и поиск оптимальных решений);
- **Проектирование ЦОД** (разработка проекта и сметной документации, их экспертиза и все необходимые согласования);
- **Строительство ЦОД** (строительно-монтажные работы, установка оборудования, испытания);
- **Ввод объекта в эксплуатацию** (окончательное конфигурирование всех систем и процессов).

➢ По оценкам экспертов, **ЦОД с полным резервированием обходится в 2,5 раза дороже простого ЦОД**, → на уровне предпроектной подготовки надо определиться, какой категории должна соответствовать площадка.

Критерии при постройке ЦОД:

- **Здание**. Это может быть как отдельное помещение в офисе компании, так и полноценное сооружение
- **Подача электроэнергии**. ЦОД не должны простаивать, необходимо сделать так, чтобы энергия подавалась постоянно.
- **Охлаждение помещения**.
- **Защита**. устанавливаются камеры, датчики движения, сигнализация, нанимается специальный персонал.
- **Противопожарная система**. Пена и вода же не подходят, поэтому из комнаты при помощи специального газа вытесняется кислород. Активируется противопожарная система автоматически

Распределение затрат

- системы гарантированного электропитания (34%)
- организация кондиционирования (21%)
- архитектура самого здания (23%).
- коммуникационные сети (7%)
- оборудование газового пожаротушения, систем управления доступом и видеонаблюдения и шкафную инфраструктуру (9%).

Вопросы?