

Tier III по TIA 942 и Tier III по Uptime Institute

Есть два основных документа, которые чаще всего упоминаются при обсуждении стандартов центров обработки данных: это стандарт TIA 942 и классификация по уровням от Uptime Institute. Оба этих документа регламентируют уровни (Tier), что часто приводит к путанице: например, Tier III по TIA 942 и Tier III по Uptime Institute — это две большие разницы.

TIA vs Uptime

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

Этот стандарт разработан ассоциацией телекоммуникационной промышленности США и, в первую очередь, 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»).

Обычно, на соответствие стандарту проверяется только проектная документация.

Однажды реализованный объект не теряет уровень.

Uptime Institute — Tier Classifications Define Site Infrastructure Performance

Этот документ не стандарт, а скорее методология, разработанная специально для нормирования отказоустойчивости ЦОД. Например, телекоммуникационная инфраструктура практически не рассматривается.

Носит обязательный характер (если вы хотите получить сертификат, конечно).

Нет пошаговых инструкций (они быстро устаревают), но есть сформулированные основные принципы проектирования и подходы. «Делай по таким принципам и получишь отказоустойчивый объект».

Сертификация осуществляется только самим Uptime Institute.

Сертифицируется как проект, так и полученный результат (запущенная площадка).

Проверяется, что именно получилось в результате — без особого акцента на том, как был этот результат достигнут, то есть допускается гибкость в плане проектирования в конкретной ситуации (если это играет на результат).

Сначала сертифицируется проект (Tier Certification of Design Documents), потом готовая площадка (Tier Certification of Constructed Facility), а потом регулярно, с периодичностью, например, раз в год, три или пять уже сама эксплуатация (Operational Sustainability Certification) на предмет её соответствия стандарту. Последнее сделано для оценки эксплуатации, наблюдения за ресурсом оборудования и другими вещами, меняющимися в процессе.

При этом именно классификация уровней в ТИА 942 предложена как раз Uptime Institute, и по сути своей они весьма схожи. При этом кардинально разнятся принципы оценки. Ещё раз: ТИА говорит «Делай точно как написано, и всё будет ОК», Uptime Institute говорит «У тебя должно быть всё ОК любыми методами, в соответствии с заданными принципами, а потом мы проверим что оно работает».

Уровни I-IV

Принципиально, и для стандарта ТИА 942, и для методологии Uptime Institute классификация по уровням одинакова. Грубо описать их можно так:

Tier I — без резервирования. Доступность 99.671%.

Tier II — резервирование критических узлов. Доступность 99.741%.

Tier III — резервирование критических узлов, путей получения электроэнергии и трасс доставки холодоносителя. При этом есть возможность вывода любого узла из эксплуатации для его обслуживания с сохранением полной функциональности объекта в целом. Доступность 99.982%

Tier IV — это самый отказоустойчивый уровень, где допускается одна авария (а не плановый вывод узла из эксплуатации) в один момент времени. Как пример аварии — критичная человеческая ошибка. По сути — это два Tier-вторых, которые построены в одном здании вокруг серверных стоек. Доступность 99.995%, что обеспечивает даунтайм всего 26 минут в год.

Как пример: если мы делаем систему с доставкой жидкого теплоносителя по трубам, в Tier III надо делать двойное кольцо, а в Tier II можно обойтись одним. При этом уровень резервирования чиллеров и фанкойлов может быть одинаковым. То же самое касается электропитания и других систем. На уровне IV ещё круче: например, ИБП и трассы питания должны быть не просто задублированы, но ещё и разнесены в разные помещения: если первый блок взорвётся (аварийный случай, а не плановая остановка), то второй не должен пострадать. Если прорывает трубопровод в каком-то месте, это никак не влияет на дублирующую электронику — есть физическое разделение систем.

Если говорить обывательским языком (очень грубо), то уровни выглядят так: первый работает и может отказать, второй в целом нормально работает и выдерживает часть самых распространённых отказов, третий выживает в любых некритичных условиях, четвёртый пригоден для работы в военных условиях.

При этом для США стоимость объекта колеблется так: 30К, 50К, 65К и 100К долларов за стойку (это очень приблизительные цифры, для оценки соотношения затрат между уровнями). В России, обычно ещё дороже. Таким образом, если выбирать между Tier II и Tier III, бюджет увеличивается не очень существенно, а вот аптайм – более чем. Но вопрос даже не в затратах, а том, насколько правильно всё спроектировано и защищено от эксплуатационных проблем на месте.

Зачем нужны эти стандарты?

Задумались о стандартах классификации дата-центров ещё в начале 90-х: тогда в Uptime Institute начали прописывать на бумаге основные принципы строительства отказоустойчивых объектов. Задачей Uptime Institute было изучение методологии строительства безотказных высокотехнологичных объектов и расследование каждой проблемы, которая повлекла за собой отказ в ЦОДе. На момент старта компания имела задокументированный опыт строительства ЦОДов и их «тёплых ламповых аналогов» ещё со времён 70-х, причём те вычислительные центры были очень масштабными и вполне себе отказоустойчивыми. По этим центрам также была статистика основных проблем: начиная от знаменитого мотылька и заканчивая разного рода мелким ремонтами.

В результате примерно в 95-м году была предложена классификация ЦОД по уровням, исходя из их отказоустойчивости. Эта классификация была предложена для того, чтобы заказчики могли выбирать ту инфраструктуру, которая соответствует их нуждам в соответствии с задачей. Грубо говоря, если заказчик строит колл-центр, то ему не обязательно думать про доступность в четыре девятки (99,99% аптайма), а вот если ЦОД, где крутятся системы, критичные для бизнеса банка, то да, тогда стоит. Именно эта классификация была учтена в первой редакции ТИА 942.

В 96-м году появился первый документ описывающий требования к инженерной инфраструктуре вычислительных центров по методологии Uptime Institute. Основные четыре уровня были введены на основе статистики отказов и опыта организации. Уровень отказоустойчивости указывал возможный аптайм, причём без промежуточных этапов: то есть никаких II+ и III+ не было и нет — даже если недотянул из-за одного не задублированного вентиля на не очень важной резервной системе до тройки – всё равно присваивается двойка. Собственно, так присваивается уровень и сейчас, поэтому слова про Tier II+ — это личная фантазия владельца, и она не имеет отношения к самому стандарту.

Основные понятия, которыми оперируют документы — это резервирование, возможность обслуживания узлов без остановки функционирования объекта в целом плюс устойчивость к сбоям и авариям. При этом постулируется ряд весьма необычных для нашей реальности вещей: например, по стандарту Uptime считается, что на уровнях I и II сетевое питание от городской сети может быть основным источником получения электроэнергии, а для уровней III и IV – нет. Город на этом уровне стандарта внезапно перестаёт быть надёжным и рассматривается только как экономически эффективный дополнительный источник питания. При этом система ДГУ должна обеспечивать работу на полной мощности, без ограничений по длительности.

Цель создания ТИА – помощь инженерам-проектировщикам, чтобы они не выдумывали что-то своё, а проектировали так, как предложено в стандарте, учитывающем опыт создания очень многих крупных объектов. Стандарт иллюстрирует и описывает лучшие техники и решения. Со своей стороны, Uptime фокусируется на принципах, при реализации которых можно добиться заданной отказоустойчивости.

Вот в чём разница: ТИА очень детально показывает, как нужно организовывать структурированные кабельные системы, информационные связи и другую инженерку (что логично, поскольку в этих вещах подсказки из best practice довольно важны). При этом Uptime не делает акцента на СКС или электропитании например, а рассматривает влияние всех инженерных систем на отказоустойчивость оборудования в ЦОД в целом. Или ещё (опрровергая одно из самых распространённых заблуждений): Uptime, на самом деле, никак не регламентирует выбор площадки, там есть только приложение в духе «мы заметили, что у Tier IV ЦОДов обычно вот такие площадки, у III вот такие и т.п.»

Практика

В нашей практике подготовки ЦОДов к сертификации по Uptime всплывало несколько «нежданчиков». Например, когда сертифицировали по Tier III собственный дата-центр – потребовалось довольно специфически организовать управление синхронизацией дизель-генераторов (детали есть вот здесь) — на деле в России мало кто об этом даже задумывался. Или вот ещё пример «из неожиданного»: при проектировании систем бесперебойного питания обычно смотрят на тип батареи, ёмкость, герметичность, обслуживаемость и так далее — то есть рассматриваются только основные параметры батарей. На самом деле при проектировании ЦОД следует принимать во внимание и более «тонкие» характеристики. Например у батарей еще и разные кривые разряда (грубо говоря, разная ёмкость при разной скорости разряда) — при частичной нагрузке всё хорошо, но при полной нагрузке система не сможет держать положенное время, ДГУ не успеет выйти на требуемый режим, и произойдет отказ.

А вот пример из практики одного из заказчиков: на бумаге никто не докапывается до состояния дизельного топлива. Грубо говоря, есть генераторы, есть резервные линии доставки топлива, а соляр он и есть соляр, главное, чтобы доливали вовремя. ЦОД может быть оценен как соответствующий требованиям ТИА. Но на практике ДТ в нашей стране обладает парой волшебных свойств, и дизели вполне могут захлебнуться. Это несоответствие проверке на уровне эксплуатации. Грубо говоря, в ТИА никогда не возникнет вопрос «а что если в баке вместо ДТ окажется вода?» и «когда вы в последний раз меняли топливо?». У Uptime Institute есть дебаг-команда, которая призвана проверять такие вещи на практике. Парни учли этот факт и теперь знают не только про то, что топливо может внезапно подвести (по методологии это так), но и учитывают, как конкретно.

Понятно, всё проверить нельзя. Например, всегда есть человеческий фактор, который создаёт крайне непредсказуемые ситуации. В среде инженеров ходит байка, что ещё в двухтысячных годах в Израиле один из ЦОДов крупной ИТ-компании остановился благодаря нашему соотечественнику в новый год. Он отмечал праздник, выпил прямо на смене, потом продолжил. После полуночи питание из города пропало, и врубилась дизели

(участие человека не требовалось, сработала автоматика). Но герою чем-то очень помешал шум, и он вручную аварийно повырубал все генераторы, чтобы продолжить отдых в комфортной обстановке. Официальных подтверждений истории нет, но я почему-то верю в неё хотя бы в качестве примера крайне дикой и нелогичной ситуации.

Автоматика

Ну и напоследок — в стандартах нет рекомендаций по организации автоматике, срабатывающей в аварийных ситуациях и рекомендаций по организации персонала типа аварийных служб. У себя мы применяем старый добрый «советский» подход, когда всё сделано предельно просто и надёжно, чуть ли не на реле: никаких сложных микроконтроллеров с собственной логикой и никакого «восстания машин». Мы выводим автоматику туда, где ситуация однозначна и нужна скорость, превышающая скорость человеческой реакции. При этом всё то, где требуется взвешенное решение, оставляем на ручное управление. Как частный пример – с города на дизель переключает автоматика. Перевод же с дизеля обратно на город (с отключением дизеля) делается строго руками на установке, а не щелчком в интерфейсе. Задача – чтобы важные действия не выполнялись на «автопилоте»: много аварий происходит именно из-за того, что люди сначала делают, а потом думают. Собственно, я считаю, что если в ЦОДе есть профессионал, который хорошо делает свою работу, это куда важнее и, главное, надёжнее самых умных инженерных решений.

Резюме

Итак, почему сертифицированный ЦОД может встать? Ответ — потому что при одинаковом названии уровней (например, Tier II) есть огромная разница между сертификацией проекта без проверки на месте и сертификацией работающей площадки с конкретной проверкой на месте. Если вы не до конца понимаете, как именно сертифицирован ЦОД (по TIA или Uptime), стоит проверить сертификацию.