

Аварии ЦОД.

Внешний сервисный байпас.

01 декабря 2015 г.

По иронии судьбы авария, о которой ниже пойдет речь, произошла спустя всего три месяца, после того как заказчик и генпроектировщик получили от нашей компании предупреждающее письмо с рекомендацией установить внешний сервисный байпас на источник бесперебойного питания. Но никакой реакции на предупреждение не последовало.

В ходе строительства дата-центра нашей компанией была поставлена и смонтирована флагманская блочная система ИБП Trinegy мощностью 1 МВт. Хотя данный ИБП и оснащен встроенным сервисным байпасом, мы все же порекомендовали головной организации сделать внешний общий сервисный байпас на систему — на случай аварии, чтобы при неблагоприятном развитии событий можно было бы обслужить этот источник полностью, не прерывая питания нагрузки. Но специалисты генподрядчика возразили, что ИБП уже оснащен сервисным байпасом, который позволит обслужить внутренние компоненты системы в любой ситуации. Ничто не предвещало плохого, и случается, чтобы новая система целиком была выведена из строя, не предвиделось.

Идеология подхода Uptime Institute к обеспечению отказоустойчивости в соответствии с требованиями Tier III подразумевает использование внешнего байпаса, для того чтобы была возможность обслужить внутренний байпас. Но в данном случае этим принципом пренебрегли. От комплектации системы внешним байпасом специалисты головной организации отказались либо из-за ограниченности бюджета, либо из-за желания увеличить маржу.

А между тем объект проектировался и строился в уже имеющемся здании, которое приспособлялось под нужды ЦОДа. Причем реконструировался объект, как всегда, в спешке. Гидроизоляция в старом здании была сделана плохо, но переделывать ее не стали. Спустя три месяца после инсталляции оборудования весенние талые воды начали заливать ИБП, при этом подтопление шло не снизу, а сверху, фактически из-под потолка. Воды просочилось довольно много — в ИБП произошло короткое замыкание, источник, «громко бабахнув» (со слов очевидцев), сгорел.

И только в этот момент стало понятно, что починить его и сделать гидроизоляцию без отключения всего ЦОДа просто невозможно: источник централизованно питал дата-центр по своему встроенному байпасу. В итоге, несмотря на высокий уровень резервирования (блочная система, резервирование по схеме N+2), после выхода из строя двух силовых блоков питание ЦОДа перестало быть бесперебойным, и все стали заложниками этой ситуации.

Следует заметить, что сама система ИБП проявила себя с наилучшей стороны. Система устояла, она не «бросила» нагрузку. Сгорели лишь те силовые блоки, на которые больше всего пролилось воды, а оставшиеся три силовых модуля, на которые воды

пролилось меньше, остались в работоспособном состоянии. Но, поскольку источник централизованно держал на себе весь ЦОД, то есть через него шло все питание объекта, а внешнего сервисного байпаса не было, для устранения повреждений силовых блоков пришлось проводить полное отключение ИБП.

В результате, как это было ни болезненно для заказчика, пришлось выбрать время и останавливать ЦОД, после чего работоспособность ИБП была полностью восстановлена, а сам источник оснащен внешним сервисным байпасом. Для компании, владеющей ЦОДом, его остановка была очень критична, болезненна.

В данном случае у аварии несколько причин. Первая — это спешка при строительстве и плохая гидроизоляция. Аккумуляторные батареи стояли на архивных стеллажах с фанерными полками, то есть в ЦОДе наблюдалась полная эклектика: соседство самого передового оборудования и «артефактов» конца прошлого века.

В терминах Uptime Institute система, спроектированная по требованиям Tier II, не подразумевает обслуживания любого элемента без отключения нагрузки, что прекрасно и продемонстрировал этот случай. Данная авария относится к такого рода инцидентам, которые без остановки ЦОДа ликвидированы быть не могут.

Это хрестоматийный случай, когда заказчика предупреждают о возможных рисках, но он предпочитает отмахнуться, а потом происходит ситуация, о которой его предупреждали! При этом уровень затрат на блок сервисного байпаса для источника мощностью 1 МВт несопоставимо мал по сравнению с убытками от остановки ЦОДа.

В итоге в течение длительного времени (больше полугода), пока выбирали момент для остановки ЦОДа, все ИТ-системы работали вообще без защиты! Такой вот риск-менеджмент. Ну и надо понимать, что, как и любая машина-«утопленник», ресурс наработки на отказ системы ИБП после такой аварии резко снизился: различные ее компоненты стали выходить из строя чаще, чем этого можно было бы ожидать от системы, не пережившей подобный стресс.

Авторы: Сергей Ермаков, Станислав Ильенко