



Пожаробезопасность в Дата-центре

Максим Амзараков

Дата центр и безопасность

Дата-центры в современном мире довольно новое явление, также как и мобильные телефоны, компьютеры и все приборы, оборудование, системы работающие с информацией и данными.

Вопрос о безопасности данных обычно сводится к проблемам сохранности их конфиденциальности. Дата-центры, как хранилище данных, также не лишены комплексов средств для предотвращения нарушения конфиденциальности.

Однако, Дата-центр, в первую очередь, обеспечивает другую характеристику безопасности данных - их доступность и сохранность. К мероприятиям, обеспечивающим сохранность данных в Дата-центре на случай пожара, относятся также периодическое копирование данных на ленты, хранимые вне Дата-центра.

Все современные Дата-центры в обязательном порядке комплектуются той или иной системой пожаротушения. Системы пожаротушения в Дата-центре призваны не только спасти данные, накопленные в вычислительных системах и системах хранения, но и оборудование, их обрабатывающее. Применение систем пожаротушения в Дата-центрах совместно с системами раннего обнаружения, позволяет сохранить данные и оборудования от последствий воздействия огня.

Данные мероприятия позволяют обеспечить сохранность данных, но не их доступность.

После срабатывания системы пожаротушения необходимо выключить системы кондиционирования и вентиляции, а при повторном срабатывании полностью обесточить Дата-центр. Серверные залы Дата-центров и технологические помещения изобилуют электрическими приборами и системами, каждая из которых может являться источником возгорания. Произвести повторное включение Дата-центра возможно лишь после восполнения огнетушащего состава и устранения причины возгорания.

На поиск причин и замену баллонов систем пожаротушения уходят дни, а в некоторых случаях, недели.

Именно пожар в Дата-центре является наиболее опасным, с точки зрения последствий, событием. И именно против пожара в Дата-центре очень сложно застраховаться.

Оценка пожаробезопасности

Многочисленные риски необходимо учитывать при оценке пожаробезопасности.

Основной риск возникновения пожара - это возгорание кабелепроводов, которое может возникнуть в результате перегрева кабелей и/или компонентов. Данный перегрев может привести к возгоранию кабельной изоляции, бумаги и т.д. Временной период между началом (перегревом) и видимым возгоранием является длительным. Он может занять часы, дни или даже недели в зависимости от набора многочисленных условий. Большинство инцидентов не приводят к возникновению пожара вообще. Считается, что в хорошо управляемом (с технической и организационной точек зрения) дата-



центре вероятность возникновения пожара минимальна. Отсутствие достоверных данных и непрозрачность отношений между оператором дата-центра и пользователями его услуг не позволяют дать количественную оценку рисков возникновения пожара

Имитационные испытания в серверных стойках указывают на то, что перегретый компонент через определенный период времени приведет к возникновению возгорания в сервере. Данное возгорание будет развиваться медленно и в определенный момент времени данный сервер начнет выделять тепло нагревая окружающее оборудование, например, сервер, находящийся сверху или снизу. Возгорание близлежащего оборудования может перейти к неконтролируемому горению, а проще говоря - пожару, который охватит весь Дата-центр. Это будет кошмаром для Дата-центра и устранение этого «непредвиденного» риска в Дата-центре обязательно и необходимо.

Эксперименты и испытания указывают на то, что при нормально осуществляемом управлении дата-центром быстрое распространение огня в помещении Дата-центра практически не возможно. Процесс возникновения пожара занимает достаточно времени, в сравнении с возможностью его очень раннего обнаружения.

Обнаружение отклонений

Экспериментально было доказано, что, так называемая, аспирационная система обнаружения всегда на самой-самой ранней стадии предупредит о том или ином отклонении. При круглосуточном наличии персонала на объекте, сотрудники дата-центра успеют на ранней стадии выявить причину отклонения и предпринять необходимые действия. В настоящий момент риск возникновения пожара практически полностью отсутствует.

Оценка риска

Риск это произведение вероятности возникновения события и масштабности его последствий.

$$Risk = Chance * Effect$$

Эффект (последствия пожара в Дата-центре) безусловно оценивается большим. Шанс (вероятность) возникновения пожара в Дата-центре сведена к минимуму, однако, зачастую вероятность возникновения пожара недооценивается. Ниже будет рассмотрены вероятность (или шанс) возникновения пожара в Дата-центре.

Вероятность перегрева какого-либо компонента ИТ оборудования или сервера в отдельности считается довольно низкой. Вероятность перегрева увеличивается экспоненциально с увеличением количества ИТ оборудования в Дата-центре (сложением вероятностей возникновения пожара в каждой единице оборудования).

Согласно закону больших чисел, если установлено много серверов, то вероятность возникновения пожара (в одном из серверов возник пожар) высока. Вначале воздействие данного перегрева незначительно, но, в конечном итоге, вышеуказанное приведет к катастрофическим последствиям, если не предпринимать никаких действий

С точки зрения общего воздействия необходимо учитывать не только само возгорание и прилегающие стойки. Дым распространится по всему залу. Маленькие частицы дыма могут со временем оказать коррозионное воздействие на прочие сервера и/или компоненты



Учитывая важность доступности и надежности функционирования оборудования в Дата-центре, необходимо понимать, что даже небольшой риск возгорания неприемлем для менеджмента дата-центра и его клиентов. Данный риск должен быть устранен автоматической системой противопожарной безопасности для удовлетворения операционных требований.

Огонь. Распространение огня.

Огонь является видимым результатом процесса горения химических элементов и материалов.

Пожар, в бытовом смысле, неконтролируемый процесс горения.

С точки зрения химии процесса, горение - это процесс окисления материалов кислородом. Окисление материалов происходит постоянно в силу наличия кислорода в нашей кислородосодержащей атмосфере. Но для большинства материалов, необходим источник тепла для их окисления.

Кабели электропроводки довольно часто «сгорают» (окисляются) без возникновения пожара. Большой ток, протекающий в проводнике вызывает выделение тепла, которое может быть достаточным для окисления изоляции проводника.

Пожар - это самоподдерживающийся процесс окисления материалов. Это процесс, в котором в результате окисления материала, происходит выделение тепла, необходимого для поддержания этого процесса.

Таким образом, для того, чтобы предотвратить пожар в Дата-центре, необходимо ограничить условия возникновения горения. Т.е. либо прекратить подачу тепла, необходимого для окисления, либо убрать кислород.

При тушении пожара, обычно, выключается электроснабжение, как источник тепла, и ограничивается доступ кислорода в места горения - простым вытеснением по всему объему защищаемого помещения (снижением концентрации кислорода), либо химически в точках горения.

Однако, выключение энергоснабжения Дата-центра может привести к дням и неделям нарушения доступности ИТ систем.

Поэтому для Дата-центров разрабатываются специализированные системы пожарной безопасности, позволяющие продолжать функционирование Дата-центра при возникновении пожароопасных ситуаций.

Пожар в Дата-центре можно разделить на три стадии: возгорание, пожар, поиск причин и устранение.

На каждой стадии необходимо применение специализированных систем и решений по пожарной безопасности.



Решение по противопожарной безопасности

Обнаружение

В силу природы возгорания в Дата-центре (в результате «длительного» воздействия тепла на условно-горючие компоненты), возможно обнаружение не пожара, как самоподдерживающегося процесса, а его раннего начала.

Обнаружение перегрева возможно с помощью высоко чувствительных сенсоров продуктов возгорания. **Titanus Supersens** - прибор раннего обнаружения пожара. Данное устройство позволяет обнаружить начало возгорания на самой ранней стадии (фаза перегрева).

Titanus supersens является аспирационной системой обнаружения возгорания. По принципу работы, система похожа на действия человека, когда он подходит в отдельные уголки помещения и втягивает воздух, чтобы обонятельные сенсоры в носу определили известные частицы горения. Так и система постоянно «вдыхает» воздух через полые трубы, размещенные в защищенном помещении. Система снабжена высокочувствительными датчиками, которые улавливают мельчайшие частицы - продукты горения ранней стадии процесса возникновения пожара. Данный подход, в отличии от традиционного дымового, позволяет обнаружить очаг возникновения пожара задолго до возникновения самоподдерживающейся реакции окисления - горения.

В связи с тем, что данным системам требуется техническое обслуживание, а также они могут выйти из строя, для обеспечения требуемого уровня надежности предусматривается как-минимум две независимые системы. Вышеуказанное, также позволяет устранить риск необнаруженного/скрытого начала возгорания.

Предотвращение пожара и устранение причин

В определенный момент, после первого обнаружения, происходит остановка притока свежего атмосферного воздуха в Дата-центр. Остановка систем приточной вентиляции. В случае использования систем кондиционирования с экономизацией на воздушной стороне (air side economizers) - останов экономизации и переход на внутренний цикл воздухообмена с холодоснабжением на прямом расширении фреона, либо охлажденной воде.

Система «**Quickrelease system**» производит выпуск азота в помещение.

Исходя из названия системы, можно предположить, что выпуск азота происходит очень быстро. Однако, это не так. Взрывообразный выпуск азота из цилиндров высокого давления (300-400 атмосфер) чреват не только возможными повреждениями помещения и нанесением вреда здоровью персоналу Дата-центра. Проведенные исследования показывают, что при резком выпуске газа из баллонов высокого давления может привести к порче жестких дисков серверов из-за резкого акустического удара.

Поэтому, выпуск газа происходит равномерно. Что, в том числе, обеспечивается возможностью системой раннего обнаружения, которая предоставляет дополнительные секунды для работы системы пожаротушения.

Система «**Quickrelease system**» выпуском азота понижает концентрацию кислорода в помещении до 13,5% - 15%.



При такой концентрации кислорода в воздухе персонал Дата-центра может продолжать свою работу без нежелательных последствий для организма. Но материалы, используемые в Дата-центре не могут поддерживать процесс горения, что полностью устраняет возможность возникновения пожара.

Далее в игру включается система **OxyReduct**. Для поддержания заданного уровня пожарной безопасности (пониженное содержание кислорода на уровне 13,5-15%) на протяжении неограниченного периода времени **Oxyreduct** подает в защищаемое помещение азот, вырабатываемый на мембранных фильтрах системы.

Система Oxyreduct постоянно следит за концентрацией кислорода в помещении и обеспечивает его содержание в воздухе на уровне 13-15%.

Таким образом, у персонала Дата-центра появляется неограниченное количество времени для поиска и устранения очага возгорания и перезарядки баллонов системы quickrelease.

Все это время Дата-центр продолжает функционирование без какого-либо снижения заданных характеристик. При этом персонал Дата-центра, а также приглашенные специалисты могут продолжать работу с серверным оборудованием в серверном зале.

Надежность системы

Кроме необходимого уровня надежности элементов системы, которое достигается за счет дублирования критически важных компонент. Одним из элементов системы, как это ни странно звучит, является само помещение.

Любая система газового пожаротушения рассчитывается исходя из известных характеристик помещения, в том числе из расчетной утечки воздуха из помещения (естественного воздухообмена).

Со временем, изначальная герметичность помещения падает, за счет старения здания, дверей, появления дополнительных кабельных вводов и т.д.

Для подтверждения возможности системы пожарной безопасности активно противостоять возгоранию и выполнить свою функцию, необходимо производить периодическую проверку систем. Система Wagner не только производит постоянный контроль своих элементов, но и производит автоматически ежемесячное измерение утечек в помещении.

Гарантии решения

Надлежащая работа и надежность решения по противопожарной безопасности являются неотъемлемой частью общего проектирования дата-центра.

Противопожарная безопасность является составной частью решения по обеспечению физической безопасности Дата-центра, как объекта. Поэтому, проектируемая система должна обладать возможностью интеграции с другими технологическими системами Дата-центра, а проектирование учитывать их особенности.

Гарантии, предоставляемые системой противопожарной безопасности, можно свести к следующему (не ограничивая) списку:

- Возгорание не может возникнуть или развиваться бесконтрольно в Дата-центре;



- Оперативное вмешательство персонала отсутствует или сведено к минимуму.
 - Система взаимодействует с другими подсистемами Дата-центра автоматически.
 - Система поддерживает низкий уровень кислорода до тех пор, пока причина отклонения не обнаружена и не устранена.
- Замена баллонов системы после срабатывания и выпуска газа возможна в течение неограниченного периода времени.
- Отключение электропитания никогда не потребуется.
 - Перегруженный кабель или компонент не может привести к возгоранию или пожару.
- Периодическая автоматическая самодиагностика системы в комплексе (смежные системы, герметичность помещения и т.д.) для обеспечения надлежащей работы на протяжении всей жизни дата-центра.

Для целей обеспечения оптимального функционирования решения необходимо учитывать нижеуказанные факторы:

- Конфигурация помещений и количество кондиционеров в помещении - потоки внутреннего воздухообмена. На основании этих данных определяется количество аспирационных сенсоров системы раннего обнаружения.
- Объем всех защищаемых помещений. Общий объем определяет объем азота (цилиндров), необходимый для снижения уровня кислорода. В зависимости от проекта дата-центра количество баллонов азота может быть изменено.
- Количество дверей и мест утечек. Общие показатели утечек определяют размер системы Oxureduct (производительность азота - м³/h)
- Отсутствие забора свежего воздуха в момент выпуска азота из цилиндров и во время работы системы oxureduct.
- Минимизация возможных утечек воздуха из помещения.

При соблюдении вышеуказанных требований к Дата-центру и системе, оператору Дата-центра можно забыть о таком страшном событии, как пожар.