



СИСТЕМА "ПОМЕЩЕНИЕ В ПОМЕЩЕНИИ"
С ВЫСОКОЙ СТЕПЕНЬЮ НАДЕЖНОСТИ



Системы информационных технологий на большинстве предприятий являются основой для надежной и эффективной работы. Отказ такой системы или даже сбой в её работе может нанести предприятию существенный ущерб или даже привести его к банкротству. С помощью системы надежной защиты помещения (High Protection Cage) Вы эффективно защищаете свои информационные технологии от таких физических опасностей как пожар, вода, несанкционированный доступ и других потенциальных угроз.

High Protection Cage (HPC) обеспечит Вам максимальную защиту и, тем самым, высокую безопасность в работе предприятия.

Swisste GmbH предлагает Вам с помощью системы HPC обеспечить надежность Ваших информационных технологий по самому высокому стандарту безопасности в соответствии с требованиями стандарта EN 1047-2, сертифицированному Европейским органом сертификации ECB-S*. HPC соответствует высоким требованиям надежности при пожаре; других источниках повышенной опасности таких как электромагнитное поле, несанкционированный доступ, обрушения, пыль и вода. В конкретно описанной методике испытания при сертификации изложены точные условия испытания и предъявляемые требования. Благодаря периодическому контролю качества изготовления и монтажа достигается постоянный уровень качества.

С помощью HPC обеспечивается физическая защита, которую нельзя достигнуть с помощью обычных материалов.

HPC используется там, где требуется высочайшая безотказность и безопасность в эксплуатации, либо применение особых мер защиты вычислительного центра или помещения для серверов.

ИНФОРМАЦИОННЫЙ ЛИСТ. ОПРЕДЕЛЕНИЕ ОСНОВ

В ходе всего испытания органом ECB-S внутри HPC только в одном месте измерения было зарегистрировано повышение температуры на 33 градуса, что существенно ниже установленного предела в 50 градусов и с избытком выполняет заданное условие!

Наряду с требованиями, предъявляемыми стандартом EN 1047-2, система HPC подвергалась и другим тестам и испытаниям с целью выполнения высоких требований к особой надежности и безопасности.

Сфера применения

- Предъявление особо высоких требований и условий, обеспечение супернадежности в эксплуатации при работе серверного помещения или вычислительного центра.
- Невозможность устранения пожароопасности окружающих конструкций, отсутствие технической возможности тушения пожара, либо отсутствие необходимой надежности конструкции здания.

Преимущества

Монтаж нашей надежной и сертифицированной системы HPC гарантирует Вам высокий уровень сохранности данных. Система HPC соответствует самым высоким требованиям BSI (Федеральное ведомство по безопасности информационной техники) или BITCOM.

Признаки

- Проверенная защита от:
 - пожара
 - повышения температуры
 - воды
 - сырости
 - пыли
 - горючих газов
 - электромагнитного поля
 - несанкционированного использования
 - воздействия обрушений.
- Интеграция в Вашу структуру зданий.
- Массивная конструкция, реализуемая как на уровне земли, так и на высших этажах.
- Интеграция всех технических и инфраструктурных компонентов (кондиционер, электрооборудование и т.п.).



СИСТЕМА "ПОМЕЩЕНИЕ В ПОМЕЩЕНИИ" С ВЫСОКОЙ СТЕПЕНЬЮ НАДЕЖНОСТИ

При наличии потенциальных источников опасности вокруг вычислительного центра, которые не представляется возможным устранить, появляется необходимость обязательного использования защитного элемента. В частности, речь может идти, например, о повышенной пожароопасности в связи с близким расположением склада и т.п. Кроме того, НРС применяется там, где имеющаяся структура зданий не обладает должной стабильностью и защищенностью от пожара (например, при расположении серверного помещения в производственном цеху).

Испытание по стандарту ЭН 1047-2 существенно отличается по следующим пунктам от простого испытания строительных материалов и тем самым обеспечивает безусловное преимущество в отношении последующей надежности и защиты чувствительных систем информационных технологий.

- Испытание системного помещения.
- Закрытый корпус (стена, потолок, пол), включая все компоненты (дверь, пропуск, задвижка) подвергается в испытательной печи воздействию обтекающего пламени.
- Повышение температуры внутри закрытого испытательного корпуса в течение всего времени испытания (фаза нагрева и охлаждения) не должно превышать 500 С (Кельвина).
- Влажность воздуха внутри корпуса не должна превышать 85 %.
- Нагретые детали должны через 45 минут после обработки пламенем выдерживать испытание на ударопрочность (3 удара по 200 кг с расстояния 1,5 м).

*ECB-S GmbH – нейтральный и всемирно признанный сертифицирующий орган в соответствии со стандартом EN 4501.
Сайт в Интернете: www.ecb-s.com

§ Иностранное законодательство

"Законодатель возлагает ответственность на руководство предприятием, а в случае ущерба, который можно было предотвратить, возлагает на него также и материальную ответственность."

- **KonTrag** (Закон о контроле и прозрачности на предприятии). Руководство предприятием должно само на самом высоком уровне заботиться об основных направлениях политики предприятия и принимать решения, которые служат защите и продолжению деятельности предприятия и могут быть подтверждены документально.
- В Справочнике по основам безопасности **BSI** (Федерального ведомства по безопасности информационной техники) описана безопасность в области информационной технологии в соответствии с действующим законодательством. Это значит, что предприятие должно соблюдать и применять на практике определенные стандарты безопасности информационной технологии в соответствии с последними техническими достижениями и современными инструкциями и возможностями согласно, например, стандарту **ISO/IEC 27001** и **ISO/IEC 15048**.
- **BASEL III** – руководство для банков по новым правилам акционерного капитала и ликвидности, применяемые на практике стандарты безопасности определяют ранжирование.
- **SOX** (Закон СарбанесОксли), регулирование, добросовестность и задачи менеджмента фирм, имеющих биржевую котировку в США.
- **GRC** (управление, риски и соблюдение законов). Здесь речь идет о внутренних нормах, которые должны обеспечивать постоянство, возможность проверки и документирования с целью надежной работы информационной техники.
- **Solvency II** – регулирует, как и Basel II, риски управления финансовым предприятием. Предприятия подвергаются целому набору рисков, которые необходимо преодолевать, чтобы успешно работать на рынке. В связи с динамическим развитием на финансовых рынках эффективное регулирование предъявляет повышенные требования к менеджерам предприятия, занимающимся контролем и регулированием рисков.
- **Федеральный закон о защите данных** - регулирует порядок обращения с личными данными. Защита систем ИТК и данных в плане безопасности информационных технологий (§ 9 Федерального закона о защите данных).

РЕШЕНИЯ ДЛЯ ВАШЕГО
ВЫЧИСЛИТЕЛЬНОГО ЦЕНТРА С ТОЧНЫМ
УЧЕТОМ ПОТРЕБНОСТЕЙ

