AKASHI

KHAN DATA CENTER

明石

UNBELIEVABLE KAZAKHSTAN

UBELIEVABLE DATA CENTER

ЦОД:

Системы защиты центра обработки данных

AKASHI
KHAN DATA CENTER

Как обеспечить безопасность ЦОД?

Основная задача любого провайдера услуг ЦОД – обеспечить физическую и виртуальную безопасность своего дата-центра. Безупречная защита помогает свести к минимуму ущерб от любых внешних и внутренних воздействий, сформировать доверие со стороны клиентов и поддерживать репутацию ЦОД на самом высоком уровне.

AKASHI
KHAN DATA CENTER

Источники угроз

Для того чтобы обеспечить безопасность центра обработки данных, необходимо знать, что может представлять для него угрозу. Список факторов риска включает:

- Форс-мажорные обстоятельства (природные катаклизмы, террористические акты и т. д.);
- Техногенные чрезвычайные ситуации и их последствия;
- Проникновение злоумышленников с целью кражи информации или вывода оборудования из строя;
- Нарушения регламентов внутри предприятия (непреднамеренные или злонамеренные действия сотрудников);
- Сервисные сбои/аварии и т. д.

Все эти факторы угрожают информационной и физической безопасности ЦОД в той или иной степени и могут повлечь за собой последствия разного масштаба – от простоя в работе до полной потери данных без возможности их восстановления.
При составлении плана по обеспечению безопасности центра обработки данных важно учитывать степень вероятности и критичности чрезвычайной ситуации: от этого будет зависеть конкурентные действия и бюджет, необходимые для того, чтобы ее предотвратить. Рассмотрим подробнее физический уровень защиты. Пожарная безопасность и обеспечение виртуальной безопасности предмет отдельного обсуждения.

AKASHI
KHAN DATA CENTER

Физическая безопасность и контроль доступа в дата-центр

Основные задачи системы безопасности ЦОД:

- предотвратить проникновение на территорию дата-центра посторонних людей,
- обеспечить катастрофоустойчивость объекта (защитить его от затопления, землетрясения, а также других природных и техногенных катаклизмов).

AKASHI
KHAN DATA CENTER

Физическая безопасность и контроль доступа в дата-центр

Наиболее надежный способ обеспечить физическую безопасность ЦОД — построить многоуровневую защиту с несколькими периметрами безопасности. Базовый контур защиты — это круглосуточная охрана и охраняемый периметр. За внешней территорией и всеми посетителями дата-центра ведется тщательное наблюдение. Любой из них должен иметь ограниченный доступ к оборудованию и сопровождаться сотрудником ЦОД. Данные о приходах и уходах посетителей фиксируются в специальном журнале.

В центрах обработки данных нет стеклянных окон, но любая дверь (даже металлическая) представляет потенциальную «лазейку» и должна быть надежно защищена. Для контроля зоны прохода в дата-центре используются тамбур-шлюзы с переговорными устройствами, установлены датчики движения, ведется круглосуточное видеонаблюдение.

AKASHI
KHAN DATA CENTER

Дополнительная защита инженерных компонентов

Помимо выбора местоположения существует множество других способов обеспечить физическую безопасность здания и инженерных компонентов ЦОД. Усиление защиты может включать:

- Железобетонные стены и конструкции, способные защитить объект от внешних воздействий;
- Гидравлические выдвижные препятствия для автомобилей и противоподкопные сооружения;
- Рамки металлодетекторов и химические датчики, проверяющие наличие у посетителей отравляющих веществ;
- Серверные шкафы и клетки, которые крепятся к фундаменту и несущим конструкциям;
- Индивидуальные ограждения и замки;

AKASHI
KHAN DATA CENTER

Поставщики услуг ЦОД обязаны:

- обеспечить физическую и информационную безопасность;
- предоставить соответствующий уровень сервиса;
- обеспечить круглосуточную работу высококвалифицированного персонала

AKASHI
KHAN DATA CENTER

+77059663455 | salem@akashi.pro | akashi.pro