Комплексное решение по физической безопасности IT-ресурсов

Мы настолько привыкли к виртуальному представлению информации, что защита данных ассоциируется только с криптографической защитой файлов от несанкционированного доступа, антивирусными программами, отсутствием на рабочих станциях сотрудников устройств для копирования. Информация в виде битов – такая эфемерная субстанция, что даже большие массивы данных не воспринимаются как что-то осязаемое и материальное. Возможно, именно поэтому самый очевидный уровень защиты – физический – зачастую вообще не рассматривается руководством компаний. О том, почему следует уделять больше внимания данному аспекту защиты информации и о современных подходах к физической защите данных рассказывает Андрей Афоненко, директор Департамента систем безопасности и автоматики компании «ИНСИСТЕМС» (группа компаний ЛАНИТ).

Андрей Афоненко,
ЗАО «Инсистемс»

Информация давно уже стала стратегическим ресурсом, и любая потеря данных может оказать неблагоприятное воздействие на работу компании. В таких условиях центры обработки данных (ЦОД) становятся стратегическим активом, основными требованиями к которому являются соответствие бизнес-задачам компании, правильно организованная инфраструктура и максимальная защита от возможных рисков.

Общеизвестно, что существует как минимум шесть основных факторов риска потери информации от физического воздействия: огонь, вода, дым/коррозийные газы, обрушение (падающие обломки), вандализм и взрывы. Проведенный Data Center Institute анализ показал, что каждый из четырех ЦОДов в течение ближайших пяти лет испытает в своей работе «нарушение», которое может затормозить развитие бизнеса компании. Под термином «нарушение» здесь понимается любое событие, которое вызвало какой-либо сбой в работе системы, включающий в себя одно или несколько событий сразу: потеря питающего напряжения или охлаждения, воздействие огня или воды, естественное бедствие типа землетрясения или урагана, терроризм, ошибка служащего или саботаж, потеря данных или нарушение безопасности. Самое интересное, что в нашей стране голубые экраны и страницы газет пестрят сообщениями о пожарах, возникающих с пугающей регулярностью, при этом все уверены, что данное происшествие с ними не произойдет.

Из всего вышесказанного можно сделать вывод, что подход к созданию на предприятии полноценного ЦОДа, безусловно, требует комплексного рассмотрения рисков, которые могут возникнуть.

В идеале защита данных должна начинаться уже на стадии выбора здания для ЦОДа: оно не должно подвергаться риску, связанному со стихийными бедствиями, его территория должна надежно охраняться и т.д. Но если предположить, что само здание выбрано идеально, а местоположение ЦОДа приближено к геометрическому центру здания и максимально удалено от источников электромагнитных помех, то пора приступать к выбору средств физической защиты.

Являясь авторизованным партнером компании Lampertz – мирового лидера в производстве средств физической защиты оборудования ЦОДов – компания «ИНСИСТЕМС» предлагает различные варианты решений:

- модульные помещения безопасности для центров обработки данных (ЦОД), коммутационных узлов;
- модульные сейфы безопасности для защиты удаленных узлов ИТ-инфраструктуры, коммутационных стоек;
- сейфы для хранения носителей информации;
- специализированные рабочие места для организации безопасных точек контроля, мониторинга и управления системами.

Особое внимание следует обратить на ГОСТ, определяющий требования к физической защите решений для ЦОДов, вступивший в действие на территории РФ в мае этого года. Данный документ является аналогом Европейской нормы EN 1047-2 и полностью подтверждает требования к физической защите ЦОДов, которые уже давно действуют на территории Евросоюза.

Требованиям этого стандарта полностью отвечает оборудование компании Lampertz GmbH & KG. Ноу-хау компании – защищенные модульные помещения (IT Modular Rooms), исключающие наряду с перечисленными и такие факторы риска, как воздействие электромагнитных полей.

Именно поэтому, в своих решениях компания «ИНСИСТЕМС» активно предлагает заказчикам современные разработки по физической защите ЦОДов на базе модулей Lamperz.

Оснастив модульное помещение инженерными системами в составе: газовое пожаротушение, контроль доступа, охранно-пожарная сигнализация, видеонаблюдение, бесперебойное и гарантированное электроснабжение, кондиционирование и вентиляция - мы получим комплексное решение по физической безопасности ИТ ресурсов.

Немаловажным вопросом является организация диспетчеризации и мониторинга работоспособности инженерных систем. Богатый опыт специалистов компании «ИНСИСТЕМС» в построении таких комплексов позволяет создать систему диспетчеризации и мониторинга с нуля или произвести её интеграцию в существующую инфраструктуру здания.

В заключени отмечу, что любой ЦОД – это сложный комплекс сооружений, инженерных и кабельных систем, средств управления и поддержки надежной работы оборудования. Стоит ли создавать отказоустойчивую, масштабируемую, высоконадежную инфраструктуру, в которой изначально минимизированы все потенциальные риски, или ограничиться небольшими текущими затратами, подвергая себя всевозможным угрозам, – такое решение каждая компания принимает сама. Важно знать, что сегодня есть решения, затраты на которые окупаются благодаря высокой степени надежности и бесперебойной работе, которые необходимы современному бизнесу. Создавать решения по стандартам завтрашнего дня можно уже сегодня. И тогда ваш ЦОД станет неприступной крепостью, защищенной и от информационных, и от физических угроз.

Тел. +7 (495) 967-66-75
www.in-systems.ru