**BC/NW 2017 № 1 (30):4.2**

**ОРГАНИЗАЦИЯ ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ В ДАТА-ЦЕНТРЕ**

Чебуреков А.А.

**Актуальность**

Одним из важных компонентов дата-центра является система технической безопасности. Оборудование должно быть защищено от несанкционированного проникновения и возникновения пожара. Обслуживающий персонал дата-центра должен знать, как действовать в непредвиденных и нештатных ситуациях.

Дата-центр – это выделенное место (комната или целое здание) , где размещается серверное и коммуникационное оборудования для подключения абонентов к каналам сети в Интернет.

Основные компоненты технической безопасности дата-центра, в соответствии со стандартом TIA-945[1]:

1. Система видеонаблюдения - используется для контроля и фиксации событий. Позволяет сотрудникам, отдела безопасности, осуществлять дистанционный визуальный контроль над всеми зонами объекта, а также записывать, хранить и просматривать видеоинформацию. Лучше всего установить в комнатах дата-центра IP камеру с датчиком движения. Такие камеры могут без участия человека самостоятельно выполнять наблюдение за отведённым участком, то есть детекция будет срабатывать, только на выбранной зоне. Система видеонаблюдения подаст сигнал оператору безопасности о наличии людей в помещениях дата-центра.
2. Система контроля и управления доступом (СКУД) - предназначена для избирательного доступа, в соответствии с допуском, а также осуществляется регистрация сотрудников в помещение дата-центра. Пример: система контроля и управления доступа «СФИНКС». Данным СКУД можно гибко настроить уровни и порядок доступа персонала, ограничить по времени посещения.
3. Охранно-пожарная сигнализации (ОПС) – основное назначение является оперативное выявление случаев несанкционированного проникновения лиц, выявление очагов на самом раннем этапе возгорания и оповещение об этих событиях службы охраны дата-центра.
4. Система автоматического газового пожаротушения – эффективный элемент комплексной защиты противопожарной защиты помещений различного назначения. Чаще всего в качестве, таких огнетушителей газы являются хладоны. Тушение возгораний хладоном может применяться для электроустановок до 110 КВ, при условии, что горение находится в начальной фазе.
5. Мониторинг – помогает непрерывно контролировать большое количество важных параметров. Вести мониторинг следует за автономными датчиками, оборудованием и системы целиком.
   1. Под автономными датчиками подразумеваются, датчики протечек (используется для систем охлаждения - кондиционеры), температурные датчики (устанавливаются для контроля горячего и холодного коридора), объёма и движения (можно использовать в залах или групп стоек).
   2. По возможности оборудование нужно мониторить всё: ИБП, ДГУ, кондиционеры, камеры и прочее.
   3. Отслеживать систему целиком можно для того, чтобы видеть взаимосвязь оборудования в единой цепочке и легко найти не исправность.
6. Электроснабжение. Каждую стойку следует подключить к двум ИБП. При сбое в работе дата-центра следует подключить к двум блокам автоматического ввода резерва (АВР). При установке только одного АВР приводит к снижению надёжности дата-центра, так как равен одной точке отказа. Переключение из одного источника питания АВР к другому должен быть без малейших скачков электроэнергии и в самые минимальные сроки. Крупные дата-центры (для которых выделено целое здание), следует оснастить резервными источниками питания (дизель-генераторами).
7. Расположение шкафов и стоек должно быть по перемежающей схеме, с тем, чтобы передняя сторона в каждом ряду была обращена к передней стороне другого же ряда, создавая “горячие” и “холодные” коридоры рисунок 1.

Под “холодным” коридором понимают, проходы вдоль передней стороны шкафов/стоек.

Под “горячим” коридором подразумеваются проходы вдоль задней стороны шкафы/стоек.



Рис 1. Расположение проходов между шкафов/стоек

Используя выше описанный стандарт TIA-942, можно провести сравнение с дата-центром, реализованным в Национальном Исследовательском Институте «МЭИ». Дата-центр, который выделен в комнате, обеспечивает следующие основы технической безопасности:

1. Система видеонаблюдения – настроена и налажена под IP-камеру с датчиком движения;
2. Система контроля и управления доступом (СКУД) – настроена система «СФИНКС» под каждого сотрудника;
3. Охранно-пожарная сигнализации (ОПС) – имеются датчики пожарной сигнализации. За доступ в дата-центр отвечает дежурный охранник;
4. Система автоматического газового пожаротушения – имеются хладоновые огнетушители;
5. Мониторинг - каждая стойка оснащена датчиками температуры. Кроме того, контроль температуры ведется коммутаторами Cisco. Контролируется температура воздуха на входе и на выходе системы охлаждения коммутатора. Система мониторинга дата-центра построена на протоколе SNMP (v. 2) и использует свободно-распространяемое программное обеспечение для визуализации состояния оборудования дата-центра.
6. Электроснабжение. Каждая стойка подключена к двум ИБП. Есть возможность обеспечения переключения к АВР и поддержка работы на 20-30 мин. Поскольку дата-центр обслуживает, в основном, Московский энергетический институт, то прекращение электроснабжения оказывает влияние на работоспособность основных пользователей. В таком случае нецелесообразно усложнять систему резервного электропитания.
7. Расположение стоек, установлено в перемежающей схеме образуя “горячие” и “холодные” коридоры.

Автор считает, что в данной работе новыми являются следующие положения и результаты:

– есть возможность провести минимизацию дата-центра МЭИ в доступе посторонних лиц

– используются компьютеры с IPMI, так как для каждого потребителя услуг дата-центра (размещения оборудования) выстраивается пул виртуальных и физических машин через VPN.

– минимизация будет на ведении документации, используя CMDB. Предложенная концепция будет обеспечивать комплексное хранилище данных.

**Литература**

1. Документ SP–3-0092: (Стандарт TIA-942, редакция 7.0, февраль 2005): http://www.upsinfo.ru/etc/tia\_russkii.pdf