конфиденциальной информации за пределы контролируемой зоны за счёт электромагнитных полей побочного характера и наводок.

Экранирование позволяет защитить от нежелательных воздействий электромагнитных сигналов и излучений собственных электромагнитных полей, а также ослабить или исключить паразитное влияние внешних излучений.

Электростатическое экранирование заключается в замыкании силовых линий электростатического поля источника на поверхность экрана и отводе наведённых зарядов на массу и на землю. Такое экранирование эффективно для устранения ёмкостных паразитных связей. Экранирующий эффект максимален на постоянном токе и с повышением частоты снижается.

Магнитостатическое экранирование основано на замыкании силовых линий магнитного поля источника в толще экрана, обладающего малым магнитным сопротивлением для постоянного тока в области низких частот. Электромагнитное экранирование ослабляет поле образующимися в толще экрана вихревыми токами. Заземление аппаратуры и её элементов используются для отвода наведённых сигналов на землю. Фильтрация применяется для подавления или ослабления сигналов при их возникновении или распространении, а также для защиты систем питания аппаратуры обработки информации.

Развязка представляет собой разделение различных электрических цепей с помощью специальных схем.

СОЗДАНИЕ МОДЕЛИ БЕЗОПАСНОСТИ ДЛЯ СОВРЕМЕННЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

А.С. ПОТЕТЕНКО

Центры обработки данных (ЦОД) привлекают внимание многих злоумышленников. Исходя из анализа современных угроз безопасности информации, хранимой и обрабатываемой в ЦОД, для создания устойчивой модели безопасности необходимо предпринять следующие меры:

– определить зоны безопасности и установить для каждой из них уровни безопасности;

– провести оценку текущей ситуации в сфере безопасности для выявления уязвимостей и рисков нарушения безопасности;

–внедрить сетевую систему обнаружения вторжений для важных сетевых сегментов.

– ввести контроль межзонального доступа с использованием межсетевых экранов и маршрутизаторов;

– установить ограничения доступа, путем внедрения VLAN на уровне маршрутизаторов.

Принять меры по защите сети хранения данных выполнением следующих пунктов:

– защита сети хранения данных от внешних угроз, таких как атаки злоумышленников;

– защита сети хранения данных от внутренних угроз, таких как несанкционированный доступ сотрудников или доступ с использованием взломанных устройств;

– защита сети хранения данных от непреднамеренных угроз нарушения безопасности со стороны авторизованных пользователей, таких как неправильная конфигурация или ошибка пользователя;

– защита и изоляция среды каждого хранилища данных от других, даже если они находятся в пределах одной физической сети.

Внедрить средства эффективного управления и мониторинга для поиска и устранения неисправностей компонентов системы, обеспечения безопасности и функций программного обеспечения.