**КИС СЗП**

**Корпоративная информационная система** ОАО «СО ЕЭС» – совокупность информационных ресурсов, объединенных локальными вычислительными сетями объектов Заказчика и системами телекоммуникаций между объектами.

КИС имеет территориально распределенную структуру, в состав которой входят объекты федерального (ИА), регионального (ОДУ) и территориального (РДУ) уровней, осуществляющие информационный обмен по телекоммуникационным каналам связи.

Комплекс мер по обеспечению защиты информационных ресурсов ОАО «СО ЕЭС», расположенных в КИС, от несанкционированного доступа со стороны внешних сетей и защиты информационных потоков при передаче данных по каналам корпоративной сети передачи данных включает в себя:

1. Контроль и регистрацию попыток несанкционированного доступа на сетевом уровне, обнаружение сетевых вторжений со стороны каналов связи к информационным ресурсам КИС Заказчика.

2. Конфиденциальность и целостность информации, передаваемой по каналам связи МСС.

3. Возможность обеспечения защищенного удаленного доступа к информационным ресурсам ИА/ОДУ/РДУ из сетей общего пользования.

4. Сбор, корреляцию и анализ событий информационной безопасности с оборудования СЗП КИС.

5. Иерархическое управление политиками безопасности компонентов СЗП КИС.

6. Мониторинг событий ИБ и управление компонентами СЗП КИС, основанный на ролевом принципе распределения полномочий.

7. Аутентификацию, авторизацию и учет доступа операторов и администраторов к активному сетевому оборудованию МСС и компонентам СЗП КИС.

Данная функциональность СЗП обеспечивается следующими подсистемами:

* **межсетевого экранирования** - обеспечивает защиту от несанкционированного доступа и разграничение доступа на сетевом и транспортном уровнях. В данном модуле применяются межсетевые экраны Cisco ASA/PIX, работающие в режиме горячего резервирования.
* **защиты каналов связи** - обеспечивает конфиденциальность и целостность информации, передаваемой по каналам связи МСС. В данной подсистеме применяются выделенные шлюзы безопасности S-Terra CSP VPN Gate 3000, работающие в режиме горячего резервирования.

На межсетевых экранах, подключаемых к ЛВС узла настраиваются туннели (в режиме ESP-null - без шифрования) до межсетевых экранов других узлов в рамках соответствующей магистрали. На криптошлюзах S-Terra CSP настраивается шифрование трафика обмена между межсетевыми экранами по протоколу ESP (шифруется трафик «точка-точка»). Для организации шифрования применяется технология IPSec в режиме туннелирования (ESP). Между магистральными шлюзами безопасности устанавливается туннель (соединение типа «точка-точка») со статическим указанием IP-адресов, участвующих в организации туннеля.

* **защищенного удаленного доступа** - обеспечивает криптографическую защиту удаленных подключений сотрудников ОАО «СО ЕЭС» к информационным ресурсам КИС в узлах ИА/ОДУ/РДУ. В данной подсистеме применяются шлюзы безопасности S-Terra CSP VPN Gate 3000 подсистемы защиты каналов связи.

Процедура защищенного удаленного доступа заключается в следующем. Пользователь использует компьютер, подключенный к сети Интернет с установленным ПО CSP VPN Client.

Шлюз безопасности CSP VPN Gate также подключен к сети Интернет и между VPN-клиентом и VPN-сервером обеспечена IP-связность. Пользователь использует ПО CSP VPN Client для установки защищенного соединения с шлюзом безопасности. Аутентификация пользователя производится на основании его секретного ключа и сертификата открытого ключа, выработанных и используемых в рамках существующей в ОАО «СО ЕЭС» инфраструктуры открытых ключей. Ключевая информация (секретный ключ и сертификат открытого ключа)

хранится на аппаратных носителях (токенах eToken) производства ЗАО «АЛАДДИН Р.Д.», имеющих сертификат соответствия в системе сертификации ФСТЭК России.

* **обнаружения сетевых вторжений** - обеспечивает мониторинг попыток несанкционированной активности в сетевом трафике. В данной подсистеме применяются аппаратно-программные сенсоры обнаружения сетевых атак Cisco IPS серии 4200.

Функциональный модуль (подсистема) обнаружения сетевых атак ресурсов сети состоит из следующих компонентов:

• коммутирующее сетевое оборудование;

• сенсоры обнаружения атак.

Коммутирующее сетевое оборудование обеспечивает выделение копии трафика, проходящего через него, и подлежащего мониторингу сенсорами обнаружения атак. В качестве коммутирующего сетевого оборудования используются на узлах РДУ и РСДУ – коммутаторы Cisco 2960. В качестве сенсоров обнаружения сетевых атак используются сенсоры серии **Cisco IPS 4200 Series** производства Cisco Systems.

* **управления и мониторинга СЗП**, в составе:
* **функциональный модуль мониторинга событий ИБ** - обеспечивает сбор, корреляцию и анализ событий ИБ, получаемых с оборудования СЗП. В данном модуле применяются аппаратно-программные комплексы Cisco Security MARS;
* **функциональный модуль управления средствами обеспечения ИБ** - функционирует на основе ПО Cisco Security Manager, устанавливаемого на выделенный сервер под управлением ОС MS Windows 2003 Server. Сервер предназначен для централизованного управления межсетевыми экранами Cisco ASA/PIX и сенсорами Cisco IPS 4200.;
* **функциональный модуль контроля доступа к сетевому оборудованию** - обеспечивает аутентификацию и разграничение доступа операторов и администраторов активного сетевого оборудования МСС. В данном модуле применяются выделенные серверы аутентификации, авторизации и учета доступа Cisco Secure ACS Solution (основной и резервный).

Сегменты сети и вланы:

1. Inside
2. Outside
3. External
4. Transit
5. Up
6. Control
7. Dmz Internet
8. Dmz untrasted