

5.2.6.2 Подсистема реализуется внедрением программно-аппаратных комплексов сетевого экранирования на границе ЛСВ, классом не ниже 4.

5.2.7 Подсистема обнаружения вторжений.

5.2.7.1 Подсистема обнаружения вторжений предназначена для реализации следующих функций:

- Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений, использующие сигнатурные методы анализа, а также методы выявления аномалий.

- Подсистема обнаружения вторжений проводится для информационной системы, подключённых к сетям международного информационного обмена, путём использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.

5.2.8 Подсистема инструментального анализа защищенности.

5.2.8.1 Подсистема инструментального анализа защищённости предназначена для реализации следующих функций:

- Анализ защищенности проводится путем использования в составе ИСПДн программных или программно-аппаратных средств анализа защищенности.

- Для ИСПДн средствами анализа защищенности должна быть обеспечена возможность выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

5.2.9 Подсистема криптографической защиты.

5.2.9.1 Подсистема криптографической защиты предназначена для реализации следующих функций:

- Приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию. Обеспечена невозможность доступа к ключевым носителям лиц, не назначенных для работы с конкретным ключевым носителем.

- Ключи на ключевых носителях, срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Об уничтожении ключей делается соответствующая запись в Журнале.

6 Пользователи ИСПДн

6.1 В ИСПДн МБДОУ «Детский сад № 105» можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;
- Ответственного за организацию обработки ПДн;
- Операторов (пользователей) обработки ИСПДн.

6.1.1 Администратор ИСПДн.

6.1.1.1 Администратор ИСПДн, работник МБДОУ «Детский сад № 105», ответственный за настройку, внедрение и сопровождение ИСПДн, обеспечивает функционирование ИСПДн и СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент, уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам хранящим персональные данные.

6.1.1.2 Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

- обладает полной информацией о технических средствах и конфигурации ИСПДн;