5.2 СЗПДн имеют различный функционал в зависимости от уровня защищенности ПДн, обрабатываемых в ИСПДн МБДОУ «Детский сад № 105».

5.2.1 Подсистема управления доступом.

5.2.1.1 Подсистема управления доступом предназначена для реализации следующих функций:

- Идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов.

5.2.1.2 Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

5.2.2 Подсистема регистрации и учёта.

5.2.2.1 Подсистема регистрации и учёта предназначена для реализации следующих функций:

- Регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке.
- Учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в Журнал учета с отметкой об их выдаче (приеме).

5.2.3 Подсистема обеспечения целостности.

5.2.3.1 Подсистема целостности предназначена для реализации следующих функций:

- Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных.
- Физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации.
- Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест – программ, имитирующих попытки несанкционированного доступа. .
- Наличие средств восстановления системы защиты персональных данных, предусматривающие ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

5.2.4 Подсистема защиты от программно-математических воздействий.

5.2.4.1 Подсистема защиты от программно-математических воздействий (подсистема антивирусной защиты) предназначена для реализации следующих функций:

- Автоматическая проверка на наличие вредоносных программ (далее – ВП) или последствий программно-математических воздействий (далее – ПМВ) при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа.