

- Реализация механизмов автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения.
- Проверка на предмет наличия ВП в средствах защиты от ПМВ (при первом запуске средства защиты от ПМВ и с устанавливаемой периодичностью).
- Факт выявления ПМВ должен инициировать автоматическую проверку на предмет наличия ВП.
- Реализация механизма отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.
- На всех технических средствах ИСПДн должен проводиться непрерывный автоматизированный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений ПМВ.
- Проверка целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм.
- Реализация механизмов проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм.
- Восстановление средств защиты от ПМВ, предусматривающая ведение двух копий программных средств защиты, его периодическое обновление и контроль работоспособности.

5.2.5 Подсистема защиты каналов связи.

5.2.5.1 Подсистема защиты каналов связи предназначена для реализации следующих функций:

- Обмен персональными данными, при их обработке в информационной системе, по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) применения технических средств.
- Выделение канала связи, обеспечивающего защиту передаваемой информации.
- Аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.
- Предотвращение возможности отрицания пользователем факта отправки персональных данных другому пользователю.
- Предотвращение возможности отрицания пользователем факта получения персональных данных от другого пользователя.

5.2.6 Подсистема межсетевого экранирования.

5.2.6.1 Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- Фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов).
- Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.
- Идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно – постоянного действия.
- Регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация входа из системы не проводится в моменты аппаратурного отключения межсетевого экрана).
- Контроль целостности своей программной и информационной части.
- Восстановление свойств межсетевого экрана после сбоев и отказов оборудования.
- Регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.