5. Антивирусная защита (ФСТЭК МД 14.06.2012)

Требования к средствам антивирусной защиты применяются к программным средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом.

Требования предназначены для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств защиты информации, заявителей на осуществление сертификации продукции, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты информации на соответствие обязательным требованиям безопасности информации.

Выполнение Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности информационных технологий, применяемых для формирования государственных информационных ресурсов, организуемых ФСТЭК России в пределах своих полномочий.

Требования к средствам антивирусной защиты включают общие требования к средствам антивирусной защиты и требования к функциям безопасности средств антивирусной защиты.

Для дифференциации требований к функциям безопасности средств антивирусной защиты установлено шесть классов защиты средств антивирусной защиты. Самый низкий класс – шестой, самый высокий – первый.

Средства антивирусной защиты, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов\*.

Средства антивирусной защиты, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса\*.

Средства антивирусной защиты, соответствующие 4 классу защиты, применяются в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса\*, а также в информационных системах общего пользования II класса\*\*.

Средства антивирусной защиты, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Также выделяются следующие типы средств антивирусной защиты:

тип «А» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для централизованного администрирования средствами антивирусной защиты, установленными на компонентах информационных систем (серверах, автоматизированных рабочих местах);

тип «Б» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на серверах информационных систем;

тип «В» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автоматизированных рабочих местах информационных систем;

тип «Г» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автономных автоматизированных рабочих местах.

Средства антивирусной защиты типа «А» не применяются в информационных системах самостоятельно и предназначены для использования только совместно со средствами антивирусной защиты типов «Б» и (или) «В».

Методические документы ФСТЭК России, содержащие профили защиты средств антивирусной защиты 4, 5 и 6 классов защиты размещены на официальном сайте ФСТЭК России www.fstec.ru в разделе «Информационно-справочная система по документам в области технической защиты информации. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации».

Основными угрозами, для противостояния которым используются САВЗ (любого из типов) , являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и(или) съемных машинных носителей информации, вредоносных компьютерных программ (вирусов)(КВ). В САВЗ должны быть реализованы следующие функции безопасности:

* разграничение доступа к управлению САВЗ;
* управление работой САВЗ;
* управление параметрами САВЗ;
* управление установкой обновлений (актуализации) базы данных
* признаков вредоносных компьютерных программ (вирусов) (БД ПКВ) САВЗ;
* аудит безопасности САВЗ;
* сигнализация САВЗ.

В среде, в которой САВЗ функционирует, должны быть реализованы следующие функции безопасности среды:

* обеспечение доверенной связи (маршрута) между САВЗ и пользователями;
* обеспечение доверенного канала получения обновлений САВЗ;
* обеспечение условий безопасного функционирования;
* управление атрибутами безопасности.