6. Межсетевые экраны (ФСТЭК МД 12.09.2016)

В соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, 12 сентября 2016 г. ФСТЭК России утверждены методические документы, содержащие профили защиты межсетевых экранов.

Указанные документы содержат детализацию требований, предъявляемых к функциям безопасности межсетевых экранов, а также взаимосвязи этих требований и 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 по безопасности информации при проведении ими работ по сертификации межсетевых экранов на соответствие Требованиям к межсетевым экранам, утвержденным приказом ФСТЭК России от 9 февраля 2016 г. N 9.

Уровни:

* сети (тип «А»)
* логических границ сети (тип «Б»)
* узла (тип «В»)
* веб-сервера (тип «Г»)
* промышленной сети (тип «Д»)

ОО = объект оценки. МЭ = межсетевые экраны.

ОО представляет собой программное или программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков и используемое в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа.

ОО должен обеспечивать нейтрализацию следующих угроз безопасности информации:

* несанкционированный доступ к информации, содержащейся в автоматизированной системе управления;
* отказ в обслуживании автоматизированной системы управления и (или) ее отдельных компонентов;
* несанкционированная передача информации из автоматизированной системы управления в информационно-телекоммуникационные сети или иные информационные системы;
* несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности.

В МЭ не должно содержаться программ, не выполняющих (не задействованных в реализации) функций безопасности или не предназначенных для обеспечения функционирования МЭ (сторонних программ).

В МЭ должны быть реализованы следующие функции безопасности:

* контроль и фильтрация;
* идентификация и аутентификация;
* регистрация событий безопасности (аудит);
* обеспечение бесперебойного функционирования и восстановление;
* тестирование и контроль целостности;
* управление (администрирование).

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

* исключение каналов связи в обход правил фильтрации;
* обеспечение доверенного канала;
* обеспечение доверенного маршрута;
* физическая защита;
* обеспечение безопасного функционирования;
* обеспечение взаимодействия с сертифицированными средствами защиты информации.