ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК РОССИИ)

ИНФОРМАЦИОННОЕ ПИСЬМО
об утверждении требований к системам обнаружения вторжений

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, приказом ФСТЭК России от 6 декабря 2011 г. N 638 (зарегистрирован Минюстом России 1 февраля 2012 г., рег. N 23088) утверждены Требования к системам обнаружения вторжений (далее - Требования), которые вступили в действие с 15 марта 2012 г.

Требования к системам обнаружения вторжений применяются к программным и программно-техническим 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 по 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 системам обнаружения вторжений включают общие требования к системам обнаружения вторжений и требования к функциям безопасности систем обнаружения вторжений.

Для дифференциации требований к функциям безопасности систем обнаружения вторжений установлено шесть классов защиты систем обнаружения вторжений. Самый низкий класс - шестой, самый высокий - первый.

Системы обнаружения вторжений, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов .

Системы обнаружения вторжений, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса .

Системы обнаружения вторжений, 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 .

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

Детализация требований к функциям безопасности систем обнаружения вторжений, установленных Требованиями, а также взаимосвязи этих требований приведены в профилях защиты, утвержденных ФСТЭК России в качестве методических документов в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

Спецификация профилей защиты систем обнаружения вторжений для каждого типа системы обнаружения вторжений и класса защиты системы обнаружения вторжений приведена в таблице.

Класс защиты Тип системы обнаружения вторжений	6	5	4	3	2	1
Система обнаружения вторжений уровня сети	ИТ.СОВ.С6.ПЗ	ИТ.СОВ.С5.ПЗ	ИТ.СОВ.С4.ПЗ	ИТ.СОВ.сз.пз	ИТ.СОВ.С2.ПЗ	ит.сов.с 1.ПЗ
Система обнаружения вторжений уровня узла	ИТ.СОВ.У6.ПЗ	ИТ.СОВ.У5.ПЗ	ИТ.СОВ.У4.ПЗ	ИТ.СОВ.УЗ.ПЗ	ИТ.СОВ.У2.ПЗ	ИТ.СОВ.У1.ПЗ

Таким образом, с 15 марта 2012 г. сертификация средств защиты информации, реализующих функции обнаружения вторжений, в системе сертификации ФСТЭК России проводится на соответствие Требованиям к системам обнаружения вторжений, утвержденным приказом ФСТЭК России от 6 декабря 2011 г. N638.

Обеспечение федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций Требованиями к системам обнаружения вторжений, утвержденными приказом ФСТЭК России от 6 декабря 2011 г. N 638, а также методическими документами ФСТЭК России, содержащими профили защиты систем обнаружения вторжений 3, 2 и 1 классов защиты, производится в соответствии с Временным порядком обеспечения органов государственной власти Российской Федерации, органов местного самоуправления и организаций документами ФСТЭК России (www.fstec.ru).

Методические документы ФСТЭК России, содержащие профили защиты систем обнаружения вторжений 6, 5 и 4 классов защиты размещены на официальном сайте ФСТЭК России www.fstec.ru в разделе «Информационно-справочная система по документам в области технической защиты информации. Специальные нормативные документы».

Примечание: * Устанавливается в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 г., регистрационный N 11462).

Устанавливается в соответствии с Требованиями о защите информации, содержащейся в информационных системах общего пользования, утвержденными приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. N416/489 (зарегистрирован Минюстом России 13 октября 2010 г., регистрационный N 18704).