ФСТЭК приказ 638 “Требования к системам обнаружения вторжений”

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.

3 класс – секретные сведения

2 класс – совершенно секретные сведения

1 класс – сведения особой важности

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.



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. N 638.

Системы обнаружения вторжений могут быть:

Пассивные – обнаруживать только факт воздействия на защищаемую информационную систему

Активными - обнаруживать воздействия и выполнять ответные действия по противодействию вторжению

Реализуются следующие методы обнаружения вторжения :

Сигнатурный метод

Эвристические методы

И иные методы обнаружения

Типы систем обнаружения вторжений

1. Системы обнаружения вторжений уровня сети
2. Системы обнаружения вторжений уровня узла(хоста)

Условия для реализации ФБ:

1. Установка, конфигурирование и управление СОВ в соответствии с эксплуатационной документацией
2. Предоставление доступа СОВ к контролируемым объектам ИС
3. Совместимость компонентов СОВ с элементами контролируемой ИС
4. Физическая защита элементов ИС на которых установлены компоненты СОВ
5. Синхронизация по времени между компонентами СОВ а также между СОВ и средой ее функционирования

Требования к ФБ:

1. Требования к составу реализуемых ФБ СОВ и сред, в которых эти средства функционируют
2. Требования к составу функциональных возможностей СОВ, обеспечивающих реализацию ФБ
3. Требования к реализации функциональных возможностей СОВ
4. Требования доверия к безопасности СОВ
5. Требования из ГОСТ Р ИСО/МЭК 15408

На базе ИСО МЭК 15408-2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Компонент | 6 | 5 | 4 | 3 | 2 | 1 |
| FAU\_GEN.1 | + | = | = | = | = | = |
| FAU\_GEN.2 |  | + | = | = | = | = |
| FAU\_SAR.1 | + | = | = | = | = | = |
| FAU\_SAR.2 |  | + | = | = | = | = |
| FAU\_SAR.3 |  | + | = | = | = | = |
| FMT\_MOF.1 | + | = | = | = | = | = |
| FMT\_MTD.1 | + | = | = | + | = | = |
| FMT\_MTD.2 |  | + | = | = | = | = |
| FMT\_MTD.3 |  |  |  |  | + | = |
| FMT\_SMR.1 | + | = | = | = | = |  |
| FMT\_SMR.2 |  |  |  |  |  | + |
| FMT\_SMR.3 |  |  |  |  |  | + |
| FPT\_TST.1 |  | + | = | + | = | = |

Для Систем обнаружения вторжений уровня сети

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Компонент | 6 | 5 | 4 | 3 | 2 | 1 |
| FID\_COL\_EXT.1 | + | = | = | = | = | = |
| FID\_ANL\_EXT.1 | + | = | = | = | = | = |
| FID\_MTH\_EXT.1 | + | = | = | = | = | = |
| FID\_MTH\_EXT.2 | + | = | = | = | = | = |
| FID\_SEL\_EXT.1 |  |  |  |  | + | = |
| FID\_RCT\_EXT.1 | + | = | = | + | = | = |
| FID\_RCT\_EXT.2 |  |  |  |  | + | + |
| FID\_PCL\_EXT.1 | + | = | = | = | = | = |
| FID\_CON\_EXT.1 | + | = | = | = | + | = |
| FID\_CON\_EXT.2 |  |  |  |  |  | + |
| FID\_MSK\_EXT.1 |  |  |  | + | + | = |
| FID\_UPD\_EXT.1 | + | = | = | = | = | = |
| FID\_INF\_EXT.1 | + | = | = | + | = | = |

Для Систем обнаружения вторжений уровня узла

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Компонент | 6 | 5 | 4 | 3 | 2 | 1 |
| FID\_COL\_EXT.2 | + | = | = | = | = | = |
| FID\_ANL\_EXT.2 | + | = | = | = | + | + |
| FID\_MTH\_EXT.1 | + | = | = | = | = | = |
| FID\_MTH\_EXT.2 | + | = | = | = | = | = |
| FID\_SEL\_EXT.1 |  |  |  |  | + | = |
| FID\_RCT\_EXT.1 | + | = | = | + | = | + |
| FID\_RCT\_EXT.2 |  |  |  |  | + | = |
| FID\_RSC\_EXT.1 |  |  |  | + | + | = |
| FID\_PCL\_EXT.1 | + | = | = | + | = | = |
| FID\_CON\_EXT.1 | + | = | = | = | + | = |
| FID\_CON\_EXT.2 |  |  |  |  |  | + |
| FID\_MSK\_EXT.1 |  |  |  | + | + | = |
| FID\_UPD\_EXT.1 | + | = | = | = | = | = |
| FID\_INF\_EXT.1 | + | = | = | + | = | = |

+ - усиленные требования по сравнению с предыдущим классом

= - требования совпадают с предыдущим классом

Требования доверия в соответсвии с ИСО МЭК 15408-3

Профили защиты

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Тип системы вторжений | 6 | 5 | 4 | 3 | 2 | 1 |
| Уровень сети | ИТ.СОВ.С6.ПЗ | ИТ.СОВ.С5.ПЗ | ИТ.СОВ.С4.ПЗ | ИТ.СОВ.С3.ПЗ | ИТ.СОВ.С2.ПЗ | ИТ.СОВ.С1.ПЗ |
| Уровень узла | ИТ.СОВ.У6.ПЗ | ИТ.СОВ.У5.ПЗ | ИТ.СОВ.У4.ПЗ | ИТ.СОВ.У3.ПЗ | ИТ.СОВ.У2.ПЗ | ИТ.СОВ.У1.ПЗ |