Требования к средствам доверенной загрузки

ФСТЭК № 119

Общие Положения

Требования применяются к программным и программно-техническим средствам, в целях обеспечения ИБ , содержащей гос тайну и иную конф информацию.

Документ для организаций осуществляющих работы по созданию СЗИ, заявителей на осуществлении сертификации и испытательных лабораторий.

Общие требования

Средства Доверенной загрузки должны обеспечивать безопасность при:

НСД к информации при загрузки нештатной операционной системы и обхода правил разграничения доступа штатной операционной системы

Несанкционированная загрузка штатной и получения НСД к информации

Нарушение целостности программной среды

Типы СДЗ (средств доверенной загрузки):

1. Средства доверенной загрузки уровня базовой системы ввода-вывода
2. Средства доверенной загрузки уровня платы расширения
3. Средства доверенной загрузки уровня загрузочной записи

СДЗ уровня ввод-вывод должны обеспечивать:

1. Получение управления в процессе выполнения базовой системы ввода-вывода до передачи управления для загрузки операционной системы
2. Самотестирование СДЗ
3. Идентификация и аутентификация пользователя с использованием портов ввод-вывод
4. КЦ среды функционирования
5. Продолжение выполнения базовой системы ввода-выводы с последующей загрузкой ОС в случае + аутентификации
6. Блокировка загрузки в случае – аутентификации
7. Регистрация событий ИБ

СДЗ уровня платы расширения:

1. Получение управление от базовой системы ввода-вывода
2. Самотестирование СДЗ
3. Идентификация и аутентификация пользователя с использованием портов ввод-вывод платы расширения
4. КЦ среды функционирования
5. загрузка ОС в случае + аутентификации
6. Блокировка загрузки в случае – аутентификации
7. Регистрация событий ИБ

СДЗ уровня загрузочной записи:

1. Получение управления до загрузки ОС
2. Идентификация и аутентификация пользователя
3. Обеспечение доступности разделов жесткого диска
4. Блокировка загрузки в случае превышения числа неудачных попыток
5. Регистрация событий ИБ

Шесть классов СДЗ:

6 класс: ГИС 3 класс защищенности, АСУП и ТП 3 класс защищенности, ИСПДн 3 и 4 уровня защищенности

5 класс: ГИС 2 класс, АСУП и ТП 2 класс, ИСПДн 2 уровня защищенности

4 класс: ГИС 1 класс, АСУП и ТП 1 класс, ИСПДн 1 уровня защищенности, ИС общего пользования 2 класса

3 класс: секретные сведения

2 класс: совершенно секретные сведения

1 класс: сведения особой важности

Для обеспечения ФБ должны быть след условия:

1. Установка и управление СДЗ
2. Совместимость компонентов СДЗ
3. Физическая защита компонентов СДЗ

Требования к ФБ:

1. Требования к составу ФБ СДЗ
2. Требования к составу функциональных возможностей СДЗ
3. Требования к реализации функциональных возможностей СДЗ
4. Требования доверия к СДЗ

|  |  |
| --- | --- |
| Условное обозначение реализуемой функции безопасности | Состав функциональных возможностей средств доверенной загрузки |
| Условное обозначение семейства |
| ФБ 1 | FMT\_SMF |
| FMT\_MOF |
| FMT\_MTD |
| FMT\_SMR |
| ФБ 2 | FMT\_MOF |
| ФБ 3 | FMT\_MTD |
| ФБ 4 | FAU\_GEN |
| FAU\_SAR |
| FAU\_ARP |
| FAU\_STG |
| ФБ 5 | FIA\_AFL |
| FIA\_SOS |
| FIA\_UAU |
| FIA\_UID |
| ФБ 6 | FTP\_TST |
| ФБ 7 | FDP\_SDI |
| FTL\_SVT\_EXT |
| ФБ 8 | FTL\_BLC\_EXT |
| ФБ 9 | FDP\_ACC |
| FDP\_ACF |
| ФБ 10 | FAU\_ARP |
| ФБ 11 | FTP\_FLS |
| ФБ 12 | FMT\_MTD |
| FTL\_RIP\_EXT |
| FTP\_PHP |

.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Компонент | Класс защиты | | | | | |
| 6 | 5 | 4 | 3 | 2 | 1 |
| Средства доверенной загрузки уровня базовой системы ввода-вывода | | | | | | |
| FAU\_GEN.1 |  |  | + | = | = | = |
| FAU\_ARP.1 |  |  | + | = | = | = |
| FIA\_AFL.1 |  |  |  | + | + | + |
| FIA\_SOS.1 |  |  |  | + | = | = |
| FIA\_UAU.2 |  |  |  | + | = | = |
| FIA\_UAU.5 |  |  |  | + | = | = |
| FIA\_UAU.7 |  |  |  | + | = | = |
| FIA\_UID.2 |  |  |  | + | = | = |
| FDP\_SDI.1 |  |  | + | = | = | = |
| FMT\_MOF.1 |  |  | + | = | = | = |
| FMT\_MTD.1 |  |  | + | = | = | = |
| FMT\_MTD.2 |  |  | + | + | = | = |
| FMT\_SMF.1 |  |  | + | = | = | = |
| FTP\_TST.1 |  |  | + | = | = | = |
| FTL\_BLC\_EXT.1 |  |  | + | + | = | = |
| FTL\_RIP\_EXT.1 |  |  |  | + | = | = |
| FTL\_SVT\_EXT.1 |  |  |  | + | = | = |
| Средства доверенной загрузки уровня платы расширения | | | | | | |
| FAU\_GEN.1 |  |  | + | = | = | = |
| FAU\_SAR.1 |  |  | + | = | = | = |
| FAU\_SAR.3 |  |  | + | = | = | = |
| FAU\_ARP.1 |  |  | + | = | = | = |
| FAU\_STG.1 |  |  | + | = | = | = |
| FAU\_STG.3 |  |  | + | = | = | = |
| FIA\_AFL.1 |  |  |  | + | + | + |
| FIA\_SOS.1 |  |  |  | + | = | = |
| FIA\_UAU.2 |  |  |  | + | = | = |
| FIA\_UAU.5 |  |  |  | + | = | = |
| FIA\_UAU.7 |  |  |  | + | = | = |
| FIA\_UID.2 |  |  |  | + | = | = |
| FDP\_SDI.1 |  |  | + | = | = | = |
| FMT\_MOF.1 |  |  | + | = | = | = |
| FMT\_MTD.1 |  |  | + | = | = | = |
| FMT\_MTD.2 |  |  | + | + | = | = |
| FMT\_SMF.1 |  |  | + | = | = | = |
| FMT\_SMR.1 |  |  | + | = | = | = |
| FTP\_TST.1 |  |  | + | = | = | = |
| FTP\_FLS.1 |  |  |  | + | = | = |
| FTP\_PHP.2 |  |  |  |  |  | + |
| FTL\_BLC\_EXT.1 |  |  | + | + | = | = |
| FTL\_BLC\_EXT.2 |  |  | + | + | = | = |
| FTL\_RIP\_EXT.1 |  |  |  | + | = | = |
| FTL\_RIP\_EXT.2 |  |  |  | + | = | = |
| FTL\_SVT\_EXT.1 |  |  |  | + | = | = |
| СДЗ уровня загрузочной записи жёсткого диска | | | | | | |
| FAU\_GEN.1 |  | + |  |  |  |  |
| FIA\_AFL.1 | + | = |  |  |  |  |
| FIA\_SOS.1 |  | + |  |  |  |  |
| FIA\_UAU.1 | + |  |  |  |  |  |
| FIA\_UAU.2 |  | + |  |  |  |  |
| FIA\_UAU.7 |  | + |  |  |  |  |
| FIA\_UID.1 | + |  |  |  |  |  |
| FIA\_UID.2 |  | + |  |  |  |  |
| FDP\_ACC.1 | + | = |  |  |  |  |
| FDP\_ACF.1 | + | = |  |  |  |  |
| FMT\_MOF.1 |  | + |  |  |  |  |
| FMT\_MTD.1 | + | = |  |  |  |  |
| FMT\_SMF.1 | + | = |  |  |  |  |
| FMT\_SMR.1 | + | = |  |  |  |  |
| FTL\_RIP\_EXT.1 |  | + |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс защиты | 6 | 5 | 4 | 3 | 2 | 1 |
| Тип СДЗ |  |
| СДЗ уровня ввод-вывод | | - | - | ИТ.СДЗ.  УБ4.П3 | ИТ.СДЗ.  УБ3.П3 | ИТ.СДЗ.  УБ2.П3 | ИТ.СДЗ.  УБ1.П3 |
| СДЗ уровня платы расширения | | - | - | ИТ.СДЗ.  ПР1.П3 | ИТ.СДЗ.  ПР3.П3 | ИТ.СДЗ.  ПР2.П3 | ИТ.СДЗ.  ПР1.П3 |
| СДЗ уровня загрузочной записи | | ИТ.СДЗ.  ЗЗ6.П3 | ИТ.СДЗ.  ЗЗ5.П3 | - | - | - | - |