ФСТЭК приказ 28 “Требования к средствам антивирусной защиты”

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".

Профили защиты для 4-6 классов по A-Г:

[Ссылка](https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-14-iyunya-2012-g)

Основные условия обеспечения реализации ФБ:

1. Установка конфигурирование и управление средствами антивирусной защиты в соответствии с эксплуатационной документацией
2. Предоставление доступа САЗ к контролируемым объектам ИС
3. Функциональная совместимость средств АЗ к контролируемым ресурсам ИС
4. Физическая защита элементов ИС на которых установлены САЗ
5. Возможность корректной совместной работы САЗ со САЗ других производителей в случае их совместного использования в ИС

+ нужно обеспечить САЗ должны обеспечить обнаружение и блокирование угроз безопасности информации которым подвержены сами САЗ

Требования к ФБ:

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

Состав компонентов можно найти на офф сайте фстэк под каждый класс защиты:

[Ссылка](https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-14-iyunya-2012-g)

На базе ГОСТ 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\_SMR.1 | + | = | = | = | = |  |
| FMT\_SMR.2 |  |  |  |  |  | + |
| FMT\_SMR.3 |  |  |  |  |  | + |

Для А

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Компонент | 6 | 5 | 4 | 3 | 2 | 1 |
| FAV\_ALR\_EXT.2 | + | = | = | + | = | = |
| FAV\_UPD\_EXT.1 | + | = | = | + | = | = |
| FAV\_CLT\_EXT.1 |  |  |  | + | = | = |

Для Б

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Компонент | 6 | 5 | 4 | 3 | 2 | 1 |
| FAV\_DET\_EXT.1 | + | = | = | + | = | = |
| FAV\_DET\_EXT.3 | + | = | = | + | = | = |
| FAV\_MTH\_EXT.1 | + | = | = | + | = | = |
| FAV\_MTH\_EXT.2 | + | = | = | + | = | = |
| FAV\_MTH\_EXT.3 | + | = | = | + | = | = |
| FAV\_ACT\_EXT.1 | + | = | = | = | = | + |
| FAV\_ACT\_EXT.2 |  |  |  | + | = | = |
| FAV\_BLC\_EXT.1 |  |  |  | + | = | = |
| FAV\_BLC\_EXT.2 |  |  |  | + | = | = |
| FAV\_ALR\_EXT.1 |  |  |  | + | = | = |
| FAV\_REC\_EXT.1 |  |  |  | + | = | = |
| FAV\_UPD\_EXT.1 | + | = | = | + | = | = |

Для В

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Компонент | 6 | 5 | 4 | 3 | 2 | 1 |
| FAV\_DET\_EXT.1 | + | = | = |  |  |  |
| FAV\_DET\_EXT.2 |  |  |  | + | = | = |
| FAV\_DET\_EXT.3 |  |  |  | + | = | = |
| FAV\_MTH\_EXT.1 | + | = | = | + | = | = |
| FAV\_MTH\_EXT.2 | + | = | = | + | = | = |
| FAV\_ACT\_EXT.1 | + | = | = | + | = | = |
| FAV\_ACT\_EXT.2 |  |  |  | + | = | = |
| FAV\_BLC\_EXT.1 |  |  |  | + | = | = |
| FAV\_BLC\_EXT.2 |  |  |  | + | = | = |
| FAV\_ALR\_EXT.1 |  |  |  | + | = | = |
| FAV\_REC\_EXT.1 |  |  |  | + | = | = |
| FAV\_UPD\_EXT.1 | + | = | = | + | = | = |

Для Г

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Компонент | 6 | 5 | 4 | 3 | 2 | 1 |
| FAV\_DET\_EXT.1 | + | = | = |  |  |  |
| FAV\_DET\_EXT.2 |  |  |  | + | = | = |
| FAV\_MTH\_EXT.1 | + | = | = | + | = | = |
| FAV\_MTH\_EXT.2 | + | = | = | + | = | = |
| FAV\_ACT\_EXT.1 | + | = | = | + | = | = |
| FAV\_ACT\_EXT.2 |  |  |  | + | = | = |
| FAV\_BLC\_EXT.1 |  |  |  | + | = | = |
| FAV\_ALR\_EXT.1 |  |  |  | + | = | = |
| FAV\_REC\_EXT.1 |  |  |  | + | = | = |
| FAV\_UPD\_EXT.1 | + | = | = | + | = | = |

+ - усиленные требования по сравнению с предыдущим классом

= - требования совпадают с предыдущим классом

Требования доверия в соответсвии с ИСО МЭК 15408-3