УТВЕРЖДЕНЫ
приказом ФСТЭК России
от « 27 » октября 2022 г. № 187

Зарегистрирован Минюстом России
« 22 » декабря 2022 г. № 71774

Требования по безопасности информации к средствам виртуализации (выписка)

1. Настоящие Требования являются обязательными требованиями в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа[1] (далее – требования по безопасности информации), предъявляемыми к программным средствам, обеспечивающим создание и функционирование изолированных программных сред, состоящих из виртуального оборудования, гостевых операционных систем и прикладного программного обеспечения (далее – виртуальные машины), в информационной (автоматизированной) системе (далее – средства виртуализации).

2. Выполнение настоящих Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности информационных технологий, организуемых ФСТЭК России в пределах своих полномочий в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063) (с изменениями, внесенными приказом ФСТЭК России от 5 августа 2021 г. № 121 (зарегистрирован Минюстом России 27 октября 2021 г., регистрационный № 65594) и приказом ФСТЭК России от 19 сентября 2022 г. № 172 (зарегистрирован Минюстом России 19 октября 2022 г., регистрационный № 70614).

3. Настоящие Требования применяются к средствам виртуализации, реализующим функциональные возможности по созданию образов виртуальных машин, формированию среды выполнения виртуальных машин, запуску виртуальных машин и управлению ими, по идентификации и

1 Статья 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, № 52, ст. 5140; 2007, № 19, ст. 2293; 2011, № 49, ст. 7025; 2016, № 15, ст. 2066).

аутентификации пользователей в средстве виртуализации и централизованному управлению образами виртуальных машин, виртуальными машинами и организацией взаимодействия между виртуальными машинами.

4. Для дифференциации требований по безопасности информации к средствам виртуализации устанавливается 6 классов защиты. Самый низкий класс – шестой, самый высокий – первый.

Средства виртуализации, соответствующие 6 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 3 категории значимости[2], в государственных информационных системах 3 класса защищенности[3], в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности[4], в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных[5].

Средства виртуализации, соответствующие 5 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 2 категории значимости, в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных.

Средства виртуализации, соответствующие 4 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 1 категории значимости, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости

---

2 Статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204; 2019, № 16, ст. 1955).

3 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933) и приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924).

4 Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 32919) (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071) и приказом ФСТЭК России от 15 марта 2021 г. № 46 (зарегистрирован Минюстом России 1 июля 2021 г., регистрационный № 64063).

5 Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257).

обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса[6].

5. Настоящие Требования включают требования по безопасности информации, предъявляемые к:

уровню доверия средства виртуализации;

хостовой операционной системе, в среде которой функционирует средство виртуализации (далее – хостовая операционная система);

составу функций безопасности средства виртуализации;

доверенной загрузке виртуальных машин;

контролю целостности в средстве виртуализации;

регистрации событий безопасности в средстве виртуализации;

управлению доступом в средстве виртуализации;

управлению потоками информации в средстве виртуализации;

защите памяти;

ограничению программной среды;

резервному копированию виртуальных машин;

идентификации и аутентификации пользователей в средстве виртуализации;

централизованному управлению образами виртуальных машин и виртуальными машинами.

6. Средство виртуализации должно соответствовать Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59772) (с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 г. № 68 (зарегистрирован Минюстом России 20 июля 2022 г., регистрационный № 69318).

Устанавливается следующее соответствие классов защиты средств виртуализации уровням доверия:

средства виртуализации 6 класса защиты должны соответствовать 6 уровню доверия;

средства виртуализации 5 класса защиты должны соответствовать 5 уровню доверия;

средства виртуализации 4 класса защиты должны соответствовать 4 уровню доверия.

---

6 Требования о защите информации, содержащейся в информационных системах общего пользования, утвержденные приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 (зарегистрирован Минюстом России 13 октября 2010 г., регистрационный № 18704).

7. В случае функционирования средства виртуализации в среде хостовой операционной системы, хостовая операционная система должна быть сертифицирована на соответствие Требованиям в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требованиям безопасности информации к операционным системам), утвержденным приказом ФСТЭК России от 19 августа 2016 г. № 119 (зарегистрирован Минюстом России 19 сентября 2016 г., регистрационный № 43691), и Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76.

Средство виртуализации 6 класса защиты должно функционировать в среде хостовой операционной системы, соответствующей 6 классу защиты и 6 уровню доверия.

Средство виртуализации 5 класса защиты должно функционировать в среде хостовой операционной системы, соответствующей 5 классу защиты и 5 уровню доверия.

Средство виртуализации 4 класса защиты должно функционировать в среде хостовой операционной системы, соответствующей 4 классу защиты и 4 уровню доверия.

8. В средстве виртуализации должны быть реализованы следующие функции безопасности:

доверенная загрузка виртуальных машин;

контроль целостности;

регистрация событий безопасности;

управление доступом;

резервное копирование;

управление потоками информации;

защита памяти;

ограничение программной среды;

идентификация и аутентификация пользователей.

централизованное управление образами виртуальных машин и виртуальными машинами.

9. К доверенной загрузке виртуальных машин предъявляются следующие требования:

9.1. Средство виртуализации 6, 5 классов защиты должно блокировать запуск виртуальной машины при выявлении нарушения целостности конфигурации виртуального оборудования данной виртуальной машины.

9.2. Средство виртуализации 4 класса защиты наряду с требованиями, установленными подпунктом 9.1 пункта 9 настоящих Требований, дополнительно должно блокировать запуск виртуальной машины при выявлении нарушения целостности файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины) и (или) исполняемых файлов гостевой операционной системы.

10. К контролю целостности в средстве виртуализации предъявляются следующие требования:

10.1. Средство виртуализации 6 класса защиты должно:

контролировать целостность в процессе загрузки и динамически в процессе функционирования средства виртуализации объектов контроля самостоятельно или с применением сертифицированных хостовой операционной системы или средства доверенной загрузки;

информировать администратора безопасности средства виртуализации о нарушении целостности объектов контроля;

контролировать целостность конфигурации виртуального оборудования виртуальных машин.

10.2. Средство виртуализации 5 класса защиты наряду с требованиями, установленными подпунктом 10.1 пункта 10 настоящих Требований, дополнительно должно контролировать целостность исполняемых файлов и параметров настройки средства виртуализации.

10.3. Средство виртуализации 4 класса защиты наряду с требованиями, установленными подпунктами 10.1 и 10.2 пункта 10 настоящих Требований, дополнительно должно обеспечивать целостность сведений о событиях безопасности.

11. К регистрации событий безопасности в средстве виртуализации предъявляются следующие требования:

11.1. Средство виртуализации 6, 5 классов защиты должно:

обеспечивать регистрацию событий безопасности, связанных с функционированием средства виртуализации;

оповещать администратора безопасности средства виртуализации о событиях безопасности;

выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;

осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили.

Регистрация событий безопасности в средстве виртуализации должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации»[7].

Для каждой функции безопасности в средстве виртуализации должен быть определен перечень событий, необходимых для регистрации и учета.

Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться номер (уникальный идентификатор) события, дата, время, тип события безопасности.

Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

Журнал событий безопасности средства виртуализации должен быть доступен только для чтения. При исчерпании области памяти, отведенной под журнал событий безопасности средства виртуализации, должно осуществляться архивирование журнала с последующей очисткой высвобождаемой области памяти.

Регистрации подлежат как минимум следующие события безопасности:

успешные и неуспешные попытки аутентификации пользователей средства виртуализации;

доступ пользователей средства виртуализации к виртуальным машинам;

создание и удаление виртуальных машин;

запуск и остановка средства виртуализации с указанием причины остановки;

запуск и остановка виртуальных машин с указанием причины остановки;

изменение ролевой модели;

изменение конфигурации средства виртуализации;

изменение конфигураций виртуальных машин;

факты нарушения целостности объектов контроля.

11.2. В средстве виртуализации 4 класса защиты наряду с требованиями, установленными подпунктом 11.1 пункта 11 настоящих Требований, для регистрируемых событий безопасности в каждой записи журнала событий безопасности дополнительно должно регистрироваться описание события безопасности, включающее сведения о его важности.

12. В средстве виртуализации 6, 5, 4 класса защиты должен быть реализован ролевой метод управления доступом с четырьмя ролями

7 Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 13 января 2022 г. № 2-ст (М., «Стандартинформ», 2022).

пользователей: разработчик виртуальной машины, администратор безопасности средства виртуализации, администратор средства виртуализации, администратор виртуальной машины.

12.1 Роль разработчика виртуальной машины должна позволять:

создавать виртуальные машины;

изменять конфигурации виртуальных машин.

12.2 Роль администратора безопасности средства виртуализации должна позволять:

иметь доступ на чтение к журналу событий безопасности средства виртуализации;

формировать отчеты с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности средства виртуализации.

12.3 Роль администратора средства виртуализации должна позволять:

создавать учетные записи пользователей средства виртуализации;

управлять учетными записями пользователей средства виртуализации;

назначать права доступа пользователям средства виртуализации к виртуальным машинам;

создавать и удалять виртуальное оборудование средства виртуализации;

изменять конфигурации виртуального оборудования средства виртуализации;

управлять доступом виртуальных машин к физическому и виртуальному оборудованию;

управлять квотами доступа виртуальных машин к физическому и виртуальному оборудованию;

управлять перемещением виртуальных машин;

удалять виртуальные машины;

запускать и останавливать виртуальные машины;

создавать снимки состояния виртуальных машин, включающих файл конфигурации виртуальной машины, образа виртуальной машины и образа памяти виртуальной машины.

12.4 Роль администратора виртуальной машины должна позволять осуществлять доступ пользователя средства виртуализации к виртуальной машине посредством интерфейса средства виртуализации.

12.5 Средство виртуализации должно обеспечивать возможность определения полномочий для пользователей средства виртуализации в пределах назначенных им ролей.

12.6 В целях обеспечения удаленного доступа пользователей с использованием сетей связи общего пользования к средству виртуализации должны применяться средства криптографической защиты информации,

прошедшие процедуру оценки соответствия в соответствии с законодательством Российской Федерации.

13. К резервному копированию в средстве виртуализации предъявляются следующие требования:

13.1. В средстве виртуализации 6 класса защиты должно обеспечиваться резервное копирование образов виртуальных машин и конфигурации виртуального оборудования виртуальных машин самостоятельно или с применением хостовой операционной системы или сертифицированных средств резервного копирования.

13.2. В средстве виртуализации 5 класса защиты наряду с требованиями, установленными подпунктом 13.1 пункта 13 настоящих Требований, дополнительно должно обеспечиваться резервное копирование параметров настройки средства виртуализации.

13.3. В средстве виртуализации 4 класса защиты наряду с требованиями, установленными подпунктами 13.1 и 13.2 пункта 13 настоящих Требований, дополнительно должно обеспечиваться резервное копирование сведений о событиях безопасности.

14. К ограничению программной среды в средстве виртуализации предъявляются следующие требования:

14.1. Средство виртуализации 6, 5 класса защиты самостоятельно или с привлечением хостовой операционной системы должно осуществлять контроль за запуском компонентов программного обеспечения, обеспечивающий выявление и блокировку запуска компонентов программного обеспечения, не включенных в перечень (список) компонентов, разрешенных для запуска.

14.2. Средство виртуализации 4 класса защиты наряду с требованиями, установленными подпунктом 14.1 пункта 14 настоящих Требований, дополнительно должно осуществлять контроль за запуском компонентов программного обеспечения, обеспечивающий:

выявление и блокировку запуска компонентов программного обеспечения, целостность которого нарушена;

блокировку запуска компонентов программного обеспечения, не прошедших аутентификацию с использованием свидетельств подлинности модулей (в том числе цифровых сигнатур производителя или иных свидетельств подлинности модулей).

15. Средство виртуализации 6, 5, 4 классов защиты должно обеспечивать управление потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств

управления потоками информации (коммутаторов, маршрутизаторов) и (или) межсетевых экранов, а также контроль взаимодействия виртуальных машин между собой.

16. К защите памяти средством виртуализации предъявляются следующие требования:

16.1. Средство виртуализации 6, 5, 4 классов защиты должно:

очищать остаточную информацию в памяти средства вычислительной техники при ее освобождении (распределении) или блокирование доступа субъектов к остаточной информации;

удалять объекты файловой системы, используемые средством виртуализации, путем перезаписи уничтожаемых (стираемых) объектов файловой системы случайной битовой последовательностью;

размещать код средства виртуализации в области памяти, не доступной одновременно для записи и исполнения;

изолировать области памяти виртуальных машин.

17. При реализации средством виртуализации функций безопасности по идентификации и аутентификации пользователей к средству виртуализации предъявляются следующие требования:

17.1. Первичная идентификация пользователей средства виртуализации 6 класса защиты должна осуществляться администратором средства виртуализации.

Идентификация и аутентификация пользователей в средстве виртуализации осуществляется с учетом требований разделов 4 – 7 ГОСТ Р 58833–2020 «Защита информации. Идентификация и аутентификация. Общие положения»[8].

В случае неуспешной идентификации и аутентификации пользователей в средстве виртуализации их доступ должен быть заблокирован.

Средство виртуализации должно осуществлять аутентификацию пользователей при предъявлении идентификатора и пароля пользователя.

Пароль пользователя для первичной аутентификации должен устанавливаться администратором средства виртуализации.

Средство виртуализации должно обеспечивать возможность смены установленного администратором средства виртуализации пароля пользователя средства виртуализации после его первичной аутентификации.

Средство виртуализации должно обеспечивать невозможность установления одинаковых идентификаторов и паролей для разных пользователей.

---

8 Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 10 апреля 2020 г. № 159-ст (М., «Стандартинформ», 2020).

При попытке ввода неправильного значения идентификатора или пароля пользователя должно выводиться сообщение с приглашением ввести правильный идентификатор и пароль еще раз.

При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя средства виртуализации должна быть заблокирована с возможностью разблокировки администратором средства виртуализации или с возможностью автоматической разблокировки по истечении временного интервала, устанавливаемого администратором средства виртуализации.

Защита пароля пользователя средства виртуализации должна обеспечиваться при его вводе за счет отображения вводимых символов условными знаками.

Пароль пользователя средства виртуализации 6 класса защиты должен содержать не менее 6 символов при алфавите пароля не менее 60 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 10.

Средство виртуализации должно обеспечивать хранение аутентификационной информации пользователя средства виртуализации в защищенном формате или в защищенном хранилище.

17.2. Пароль пользователя средства виртуализации 5 класса защиты наряду с требованиями, установленными подпунктом 17.1 пункта 17 настоящих Требований, дополнительно должен содержать не менее 6 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 8.

Средство виртуализации 5 класса защиты должно обеспечивать взаимную идентификацию и аутентификацию пользователей и средства виртуализации при удаленном доступе с использованием сетей связи общего пользования.

17.3. Пароль пользователя средства виртуализации 4 класса защиты наряду с требованиями, установленными подпунктами 17.1 и 17.2 пункта 17 настоящих Требований, дополнительно должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.

18. При реализации средством виртуализации функций безопасности по централизованному управлению образами виртуальных машин и виртуальными машинами к средству виртуализации предъявляются следующие требования:

18.1. Средство виртуализации 6 класса защиты должно:

создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;

обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности средства виртуализации.

18.2. Средство виртуализации 5, 4 классов защиты должно наряду с требованиями, установленными подпунктом 18.1 пункта 18 настоящих Требований, дополнительно обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.