УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 4 июля 2022 г. № 118

Требования по безопасности информации к средствам контейнеризации (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 на основе ядра хостовой операционной системы (далее – контейнеры) в информационной (автоматизированной) системе (далее – средства контейнеризации).

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).

3. Настоящие Требования применяются к средствам контейнеризации, реализующим функциональные возможности по созданию образов контейнеров, формированию среды выполнения контейнеров и обеспечения выполнения их процессов, запуску контейнера и управление данным контейнером, а также дополнительные функциональные возможности по централизованному управлению контейнерами, организации взаимодействия между ними и распространению образов контейнеров.

---

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).

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

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

---

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).

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).

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

уровню доверия средства контейнеризации;

хостовой операционной системе, в среде которой функционирует средство контейнеризации;

составу функций безопасности средства контейнеризации;

изоляции контейнеров средством контейнеризации;

выявлению уязвимостей в образах контейнеров;

проверке корректности конфигурации контейнеров;

контролю целостности контейнеров и их образов в средстве контейнеризации;

регистрации событий безопасности в средстве контейнеризации;

управлению доступом в средстве контейнеризации;

идентификации и аутентификации пользователей в средстве контейнеризации;

централизованному управлению образами контейнеров и контейнерами в средстве контейнеризации.

6. Средство контейнеризации 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 контейнеризации уровням доверия:

средства контейнеризации 6 класса защиты должны соответствовать 6 уровню доверия;

средства контейнеризации 5 класса защиты должны соответствовать 5 уровню доверия;

средства контейнеризации 4 класса защиты должны соответствовать 4 уровню доверия;

7. Хостовая операционная система, в среде которой функционирует средство контейнеризации, 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 контейнеризации 6 класса защиты должно функционировать в среде хостовой операционной системы, соответствующей 6 классу защиты и 6 уровню доверия.

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

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

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

изоляция контейнеров;

выявление уязвимостей в образах контейнеров;

проверка корректности конфигурации контейнеров;

контроль целостности контейнеров и их образов;

регистрация событий безопасности.

В средстве контейнеризации дополнительно могут быть реализованы следующие функции безопасности:

управление доступом;

идентификация и аутентификация пользователей;

централизованное управление образами контейнеров и контейнерами.

9. К изоляции контейнеров средством контейнеризации предъявляются следующие требования:

9.1. Средство контейнеризации 6 класса защиты должно реализовывать механизмы изоляции контейнеров. Способы реализации изоляции контейнеров устанавливаются разработчиком средства контейнеризации.

9.2. Средство контейнеризации 5 и 4 классов защиты наряду с требованиями, установленными подпунктом 9.1 пункта 9 настоящих Требований, дополнительно должно реализовывать следующие механизмы:

изоляция пространств идентификаторов процессов контейнеров;

изоляция пространств имен для межпроцессного взаимодействия контейнеров;

изоляция пространств имен для пользователей и групп контейнеров;

изоляция пространств имен хостов и доменов контейнеров;

изоляция сетевых пространств имен контейнеров;

изоляция пространств имен для иерархии каталогов контейнеров.

10. К выявлению уязвимостей в образах контейнеров предъявляются следующие требования:

10.1. Средство контейнеризации 6 класса защиты должно:

выявлять известные уязвимости при создании, установке образа контейнера в информационной (автоматизированной) системе и хранении образов контейнеров во взаимодействии с сертифицированным средством контроля и анализа защищенности на основе сведений, содержащихся в банке данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541), а также в иных источниках, содержащих сведения об известных уязвимостях;

оповещать о выявленных уязвимостях в образах контейнеров разработчика образов контейнеров и администратора безопасности информационной (автоматизированной) системы.

Средство контейнеризации 6 класса защиты должно осуществлять выявление известных уязвимостей образов контейнеров не реже одного раза в месяц.

10.2. Средство контейнеризации 5 и 4 классов защиты наряду с требованиями, установленными подпунктом 10.1 пункта 10 настоящих Требований, должно запрещать создание образов контейнеров, содержащих известные уязвимости критического и высокого уровня опасности.

Средство контейнеризации 5 и 4 классов защиты должно осуществлять выявление известных уязвимостей образов контейнеров не реже одного раза в неделю.

11. К проверке корректности конфигурации контейнеров в средстве контейнеризации предъявляются следующие требования:

Средство контейнеризации 6, 5 и 4 классов защиты должно обеспечивать:

ограничение прав прикладного программного обеспечения, выполняемого внутри контейнера, на использование периферийных устройств, устройств хранения данных и съемных машинных носителей информации (блочных устройств), входящих в состав информационной (автоматизированной) системы;

ограничение прав прикладного программного обеспечения, выполняемого внутри контейнера, на использование вычислительных ресурсов (оперативной памяти, операций ввода-вывода за период времени) хостовой операционной системы;

монтирование корневой файловой системы хостовой операционной системы в режиме «только для чтения».

12. К контролю целостности контейнеров и их образов в средстве контейнеризации предъявляются следующие требования:

12.1. Средство контейнеризации 6 класса защиты должно:

контролировать самостоятельно или с применением средств контроля целостности хостовой операционной системы и иных сертифицированных средств защиты информации целостность образов контейнеров и исполняемых файлов контейнеров;

информировать администратора информационной (автоматизированной) системы и администратора безопасности средства контейнеризации о нарушении целостности объектов контроля.

12.2. Средство контейнеризации 5 класса защиты наряду с требованиями, установленными подпунктом 12.1 пункта 12 настоящих Требований, должно контролировать целостность параметров настройки средства контейнеризации.

12.3. Средство контейнеризации 4 класса защиты наряду с требованиями, установленными подпунктами 12.1 и 12.2 пункта 12 настоящих Требований, должно:

контролировать целостность сведений о событиях безопасности самостоятельно или во взаимодействии с хостовой операционной системой и иными сертифицированными средствами защиты информации;

контролировать целостность образов контейнеров и параметров настройки средства контейнеризации при установке образа контейнера в информационной (автоматизированной) системе и далее периодически за счет применения цифровой подписи самостоятельно или во взаимодействии с хостовой операционной системой и иными сертифицированными средствами защиты информации;

блокировать запуск образа контейнера при нарушении его целостности.

13. К регистрации событий безопасности в средстве контейнеризации предъявляются следующие требования:

13.1. Средство контейнеризации 6 класса защиты должно:

регистрировать события, относящиеся к инцидентам безопасности средства контейнеризации, связанные с попытками осуществления несанкционированного доступа к средству контейнеризации;

оповещать администратора безопасности средства контейнеризации и администратора информационной (автоматизированной) системы об инцидентах безопасности;

выполнять действия, являющиеся реакцией на инциденты безопасности;

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

Регистрация событий безопасности в средстве контейнеризации должна осуществляться с учетом требований разделов 5-6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации»[7].

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

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

Записи журнала событий безопасности должны представляться в структурированном виде и содержать информацию о времени события безопасности, взятую из хостовой операционной системы.

Средство контейнеризации должно осуществлять запись событий безопасности контейнеров в журнал событий безопасности информационной (автоматизированной) системы с указанием идентификатора контейнера.

Журнал событий безопасности средства контейнеризации должен быть доступен только для чтения. При исчерпании области памяти, отведенной под журнал событий безопасности средства контейнеризации, средство контейнеризации должно осуществлять архивирование журнала с последующей очисткой указанного журнала.

Регистрации подлежат как минимум следующие события безопасности:

неуспешные попытки аутентификации пользователей средства контейнеризации;

создание, модификация и удаление образов контейнеров;

получение доступа к образам контейнеров;

запуск и остановка контейнеров с указанием причины остановки.

изменение ролевой модели;

модификация запускаемых контейнеров.

13.2. Средство контейнеризации 5 класса защиты наряду с требованиями, установленными подпунктом 13.1 пункта 13 настоящих Требований, должно регистрировать следующие события безопасности:

---

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

выявление известных уязвимостей в образах контейнеров и некорректности конфигурации;

факты нарушения целостности объектов контроля.

Для каждого события безопасности должны регистрироваться:

описание события безопасности;

сведения о критичности события безопасности.

13.3. Средство контейнеризации 4 класса защиты наряду с требованиями, установленными подпунктами 13.1 и 13.2 пункта 13 настоящих Требований, должно обеспечивать запись событий безопасности контейнеров в журнал событий безопасности информационной (автоматизированной) системы с указанием идентификатора пользователя хостовой операционной системы, от имени которого был запущен контейнер.

14. В средстве контейнеризации 6, 5 и 4 классов защиты должен быть реализован ролевой метод управления доступом с тремя ролями пользователей:

разработчик образов контейнеров;

администратор безопасности средства контейнеризации;

администратор информационной (автоматизированной) системы.

14.1. Роль разработчика образов контейнеров должна позволять:

менять установленный администратором безопасности средства контейнеризации для разработчика пароль;

создавать, модифицировать и удалять образы контейнеров.

14.2. Роль администратора информационной (автоматизированной) системы должна позволять:

менять установленный администратором безопасности средства контейнеризации для администратора информационной (автоматизированной) системы пароль;

запускать и останавливать контейнеры.

14.3. Роль администратора безопасности средства контейнеризации должна позволять:

назначать права доступа пользователям средства контейнеризации к образам контейнеров;

создавать учетные записи пользователей средства контейнеризации;

управлять учетными записями пользователей средства контейнеризации;

иметь доступ на чтение к журналу событий безопасности средства контейнеризации;

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

15. К идентификации и аутентификации пользователей в средстве контейнеризации предъявляются следующие требования:

15.1. Первичная идентификация пользователей средства контейнеризации 6 класса защиты должна осуществляться администратором безопасности средства контейнеризации.

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

Средство контейнеризации должно осуществлять аутентификацию пользователей при предъявлении пароля пользователя.

Пароль пользователя должен устанавливаться администратором безопасности средства контейнеризации.

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

При попытке ввода неправильного значения пароля пользователя должно выводиться соответствующее сообщение с приглашением ввести правильный пароль еще раз.

При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя средства контейнеризации должна быть заблокирована средством контейнеризации с возможностью разблокировки администратором безопасности средства контейнеризации.

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

Пароль пользователя средства контейнеризации 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 контейнеризации должно обеспечивать хранение аутентификационной информации пользователя средства контейнеризации в защищенном формате или в защищенном хранилище.

15.2. Пароль пользователя средства контейнеризации 5 класса защиты должен содержать не менее 6 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 8.

15.3. Средство контейнеризации 4 класса защиты наряду с требованиями, установленными подпунктом 15.1 пункта 15 не должно запускать процессы в

---

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

хостовой операционной системе, обладающие привилегиями администратора информационной (автоматизированной) системы и администратора безопасности информационной (автоматизированной) системы.

Пароль пользователя средства контейнеризации 4 класса защиты должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.

16. К централизованному управлению образами контейнеров и контейнерами в средстве контейнеризации предъявляются следующие требования:

16.1. Средство контейнеризации 6 класса защиты должно:

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

обновлять образы контейнеров;

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

16.2. Средство контейнеризации 5 и 4 классов защиты наряду с требованиями, установленными подпунктом 16.1 пункта 16 настоящих Требований, должно:

анализировать возникающие события безопасности в целях выявления инцидентов безопасности;

оповещать администратора безопасности средства контейнеризации о событиях безопасности;

формировать отчеты.