



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)**

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: postin@fstec.ru

10.01.2023 № 240/24/169

На № _____

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

об утверждении Требований по безопасности информации к средствам виртуализации

В соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, приказом ФСТЭК России от 27 октября 2022 г. № 187 (зарегистрирован Минюстом России 22 декабря 2022 г., регистрационный № 71774) утверждены Требования по безопасности информации к средствам виртуализации (далее – Требования).

Указанный документ предназначен для организаций, осуществляющих разработку средств виртуализации, заявителей на осуществление сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты информации на соответствие обязательным требованиям по безопасности информации.

Требования включают минимально необходимые 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.

При включении в средство виртуализации дополнительных функций безопасности требования к таким функциям безопасности должны быть заданы в технических условиях или техническом задании, а полнота и корректность их реализации оценены при проведении сертификации средства виртуализации.

Выполнение 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.

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, в государственных информационных системах 3 класса защищенности², в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных.

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

Средства виртуализации, соответствующие 3 классу защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая

секретные сведения.

Средства виртуализации, соответствующие 2 классу защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая совершенно секретные сведения.

Средства виртуализации, соответствующие 1 классу защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения особой важности.

С 22 декабря 2022 г. сертификация средств виртуализации осуществляется на соответствие Требованиям.

Обеспечение федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций Требованиями производится в соответствии с Порядком обеспечения органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций документами ФСТЭК России, размещенном на официальном сайте ФСТЭК России www.fstec.ru в подразделе «Обеспечение документами» раздела «Документы».

Выписка из Требований для 6, 5 и 4 классов защиты размещена на официальном сайте ФСТЭК России www.fstec.ru в подразделе «Сертификация. Специальные нормативные и методические документы».

Заместитель директора



В.Лютиков