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

19.03.2019 № 240/24/1525

На №_____

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

о Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

В соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, приказом ФСТЭК России от 30 июля 2018 г. № 131 (зарегистрирован Минюстом России 14 ноября 2018 г., регистрационный № 52686) утверждены Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (далее – Требования к уровням доверия).

Требования к уровням доверия предназначены для разработчиков и производителей программных и программно-технических (программно-аппаратных) средств защиты информации, средств обеспечения безопасности информационных технологий, включая защищенные средства обработки информации (далее – средства защиты информации), заявителей на осуществление сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты на соответствие требованиям по безопасности информации.

Выполнение Требований к уровню доверия является обязательным при проведении работ по сертификации средств защиты информации, организуемых ФСТЭК России в пределах своих полномочий.

Требования к уровням доверия устанавливают требования к разработке и производству средств защиты информации, к проведению испытаний средств защиты информации, а также к поддержке безопасности средств

защиты информации в ходе их применения. Для дифференциации указанных требований устанавливается 6 уровней доверия. Самый низкий уровень – шестой, самый высокий – первый.

Средства защиты информации, соответствующие 6 уровню доверия, подлежат применению в значимых объектах критической информационной инфраструктуры 3 категории, в государственных информационных системах 3 класса защищенности, 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 защиты информации, соответствующие 5 уровню доверия, подлежат применению в значимых объектах критической информационной инфраструктуры 2 категории, 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 защиты информации, соответствующие 4 уровню доверия, подлежат применению в значимых объектах критической информационной инфраструктуры 1 категории, 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 защиты информации, соответствующие 1, 2 и 3 уровням доверия, применяются в информационных (автоматизированных) системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Требования к уровню доверия подлежат применению при сертификации средств защиты информации с 1 июня 2019 г.

В связи с утверждением Требований к уровню доверия с 1 июня 2019 г. ФСТЭК России не принимаются к рассмотрению заявки на сертификацию средств защиты информации на соответствие требованиям руководящего документа «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

Кроме того, до внесения соответствующих изменений в нормативные правовые акты ФСТЭК России, устанавливающие требования по безопасности информации к средствам защиты информации, с 1 июня 2019 г. при сертификации не подлежат применению пункт 22 Требований к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638, пункт 22 Требований к средствам антивирусной защиты, утвержденные приказом ФСТЭК России

от 20 марта 2012 г. № 28, пункт 18 Требования к средствам доверенной загрузки, утвержденные приказом ФСТЭК России от 27 сентября 2013 г. № 119, пункт 17 Требований к средствам контроля съемных машинных носителей информации, утвержденные приказом ФСТЭК России от 28 июля 2014 г. № 87, пункт 20 Требований к межсетевым экранам, утвержденные приказом ФСТЭК России от 9 февраля 2016 г. № 9, пункт 18 Требований безопасности информации к операционным системам, утвержденных приказом ФСТЭК России от 19 августа 2016 г. № 119.

Разработчикам и производителям сертифицированных средств защиты информации рекомендуется с привлечением испытательных лабораторий провести оценку соответствия средств защиты информации Требованиям к уровням доверия и представить результаты в ФСТЭК России для переоформления соответствующих сертификатов соответствия. Действие сертификатов соответствия средств защиты информации, в отношении которых указанная оценка соответствия не будет проведена до 1 января 2020 г. на основании пункта 83 Положения о сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. № 55, может быть приостановлено.

В соответствии с главой IV Требований к уровням доверия в отношении средств защиты информации должны быть проведены испытания по выявлению уязвимостей и недекларированных возможностей.

В целях реализации указанного требования в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, ФСТЭК России разработана и утверждена 11 февраля 2019 г. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении (далее — Методика).

В соответствии с Требованиями к уровням доверия и Методикой для дифференциации требований к исследованиям программного обеспечения средств защиты информации по выявлению уязвимостей и недекларированных возможностей устанавливается 6 уровней контроля. Самый низкий уровень – шестой, самый высокий – первый.

Средства защиты информации, соответствующие 6 уровню доверия, проходят исследования по 6 уровню контроля, средства защиты информации, соответствующие 5 уровню доверия – по 5 уровню контроля, средства защиты информации, соответствующие 4 уровню доверия – по 4 уровню контроля, средства защиты информации, соответствующие 3 уровню доверия – по 3 уровню контроля, средства защиты информации, соответствующие 2 уровню доверия – по 2 уровню контроля, средства защиты информации, соответствующие 1 уровню доверия – по 1 уровню контроля.

Обеспечение федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций Требованиями к уровням доверия

самоуправления и организаций Требованиями к уровням доверия и Методикой 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». Организации, имеющие лицензии ФСТЭК России на разработку и (или) производство средств защиты информации, а также аккредитованные ФСТЭК России в качестве органов по сертификации или испытательных лабораторий, могут получить Требования к уровням доверия и Методику, изданные типографским способом, в ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Заместитель директора В.Лютиков