

Сертификация средств защиты информации: куда дует ветер?

С.Б. Трошкин

Заместитель директора

*Департамент сертификации и аудита кода
АО «НПО «Эшелон»*

моб.: +7 (985) 929-85-05
mail: s.troshkin@npo-echelon.ru

История

- В апреле 2018 приказом ФСТЭК России №55 утверждено «Положение о системе сертификации средств защиты информации», которое вступило в силу с 1 августа 2018 года.

Изменения для Заявителей

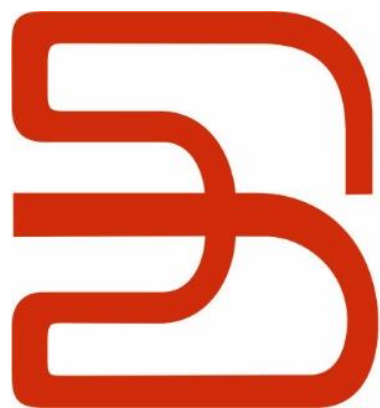
- Положение ограничивает круг компаний, которые могут выступать Заявителями на сертификацию. Заявителями теперь могут выступать либо изготовители СЗИ, которые производят СЗИ и оказывают техническую поддержку, либо конечные пользователи.
- Введены новые обязанности для Заявителей: сделан уклон на устранение уязвимостей и недекларированных возможностей программного обеспечения, с обязательным информированием потребителей об обновлении и доведении обновлений ПО, а также изменений в эксплуатационную документацию
- Схемы сертификации остаются прежними, но единственный образец и партию теперь может сертифицировать только Заявитель, являющийся конечным пользователем, и то только в случае отсутствия серийно производимых сертифицированных аналогов.

Общие изменения внесенные Положением

- Введен предварительный анализ объекта сертификации испытательной лабораторией и органом по сертификации.
- Формализованы сроки работы органа по сертификации и ФСТЭК.
- Увеличен срок действия сертификата, введена возможность использования СЗИ после окончания срока действия сертификата при условии продолжения его поддержки.
- Процедура продления сертификата проводится путем повторной сертификации.
- ФСТЭК получает возможность контроля сроков проведения сертификационных испытаний путем контроля договоров.

Ожидания

- Усиление контроля за поиском и устранением уязвимостей со стороны Заявителя-разработчика, а также испытательных лабораторий.
- Перенятие опыта ФСТЭК Министерством обороны.
- Введение ФСТЭК новой Методики поиска недеklarированных возможностей и проведения анализа уязвимостей (РД НДВ 1999 года утратит силу).
- Расширение круга изделий, попадающих под требования Профилей защиты.
- Контроль выполнения ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования разработчиками.



Эшелон

комплексная безопасность