



Порядок обновления сертифицированных средств защиты информации

Невыполнение
поддержки

Несвоевременность
поддержки

Проблема
поддержки
СЗИ



Рекомендации по обновлению сертифицированных средств защиты информации предназначены для:

- заявителей (разработчиков, производителей, поставщиков) на осуществление сертификации СЗИ;
- испытательных лабораторий;
- органов по сертификации;
- пользователей сертифицированных СЗИ.

Типы обновлений СЗИ

1 тип
обновление БД,
необходимых для
реализации ФБ СЗИ

2 тип
устранение
уязвимостей СЗИ

3 тип
добавление ФБ СЗИ,
совершенствование
реализации ФБ СЗИ,
расширение числа
поддерживаемых
программных и
аппаратных платформ

4 тип
не влияет на
безопасность СЗИ
(изменение
интерфейса средства
защиты информации,
иных функций, не
влияющее на
функции
безопасности
средства защиты
информации и т.п.)

Возникновение
необходимости
обновления СЗИ



Разработка (или
получение от
разработчика СЗИ)
заявителем
обновления СЗИ



Определение типа
обновления СЗИ
заявителем

Заявителем определен 1 тип обновления (обновление БД, необходимых для реализации ФБ СЗИ)

Порядок обновления

Обеспечение
получения обновления
по доверенному
каналу
пользователями



Доведение до
пользователей
информации о
необходимости
обновления



Получение
пользователем
обновления



Применение
пользователем
обновления

Порядок ИК

Подготовка полного
пакета обновлений типа
1 к инспекционному
контролю ИЛ (ежегодно)



ИК ИЛ СЗИ с полным
пакетом обновлений типа
1 (в течении 15 дней)



Представление
технического
заключению по
результатам ИК
заявителю

Заявителем определен 2, 3 или 4 тип обновления

Представление
заявителем обновления,
при необходимости:
СЗИ, документации,
исходных текстов ПО



Уточнение типа
обновления ИЛ в
течении 3 дней



Информирование
заявителя об
определенном типе
обновления

ИЛ определен 2 тип обновления (устранение уязвимостей СЗИ)

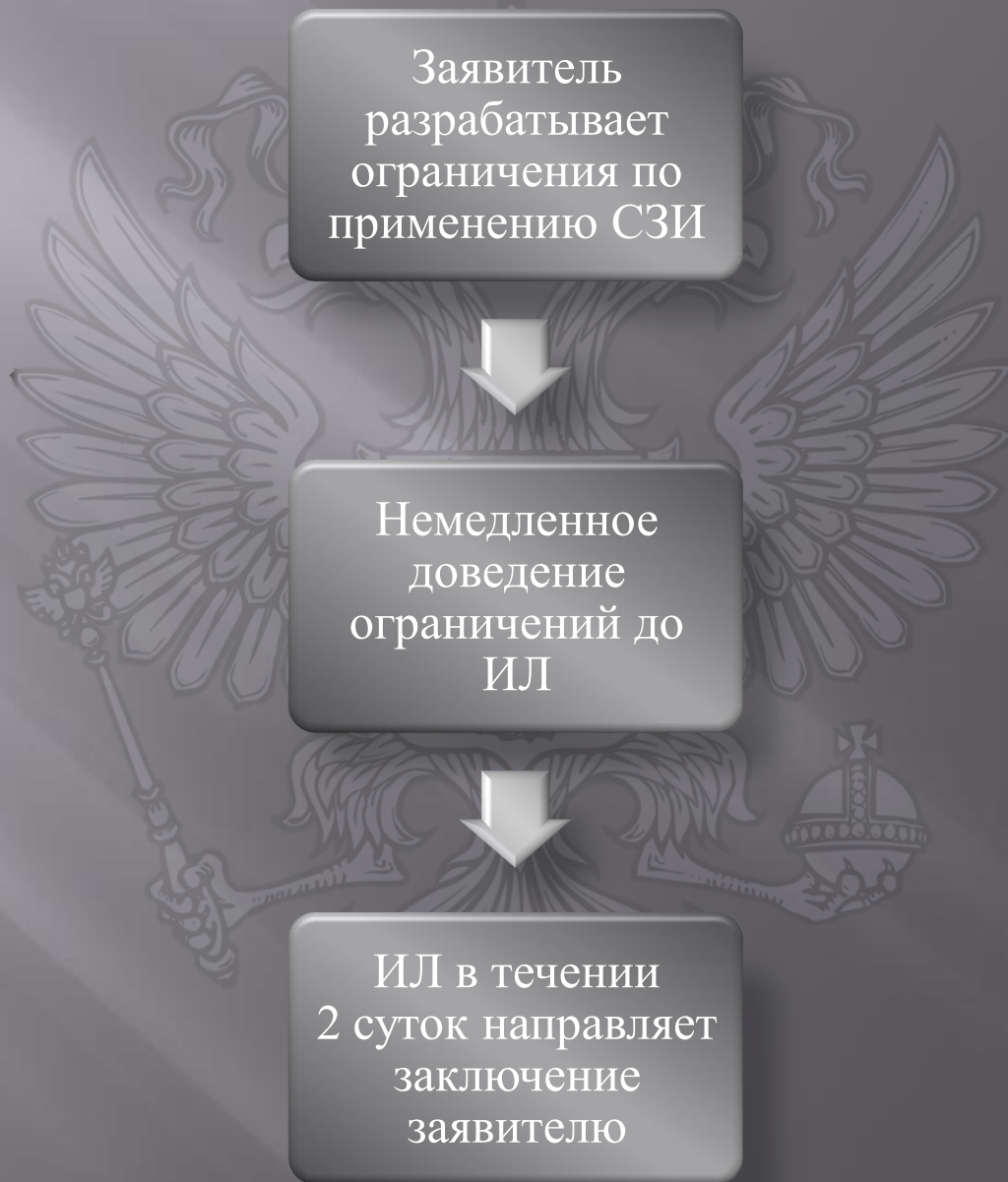
Порядок обновления



Порядок ИК



Невозможно устранить уязвимость СЗИ путем применения обновления



Ограничение по применению СЗИ

устраняет уязвимость

не устраняет уязвимость



ИЛ определен 3 тип обновления (добавление ФБ СЗИ, совершенствование реализации ФБ СЗИ, расширение числа поддерживаемых программных и аппаратных платформ)

12





МД

- Рекомендации по обновлению сертифицированных средств защиты информации

НПА

- Организация и порядок проведения сертификации продукции, используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну

Конструкторская документация СЗИ

Эксплуатационная документация СЗИ

Договоры на проведение сертификационных испытаний и ИК СЗИ



Обновление
ПО



Внешний
контроль ИЛ

Обновление БД



Внешний
контроль ИЛ
ежегодно

ФБ4 СОВ (САВЗ)

- обязательное обновление БД СОВ (САВЗ).

ФБС2 СОВ (САВЗ)

- обеспечение доверенного канала для получения обновлений БД.

ALC_FLR

- Устранение недостатков

AVA

- Оценка уязвимостей

FAV_UPD_EXT

- Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

AMA_SIA_EXT

- Экспертиза анализа влияния обновлений базы данных признаков вредоносных компьютерных программ (вирусов) на безопасность объекта оценки

ALC_FLR

- Устранение недостатков

AVA

- Оценка уязвимостей

ALC_UPI_EXT

- Процедуры обновления базы решающих правил

AMA_SIA_EXT

- Экспертиза анализа влияния обновлений базы решающих правил на безопасность системы обнаружения вторжений

ALC_FLR

- Устранение недостатков

AVA

- Оценка уязвимостей

AMA_SIA_EXT

- Анализ влияния обновлений на безопасность СДЗ

Проект методического документа
«Рекомендации по обновлению сертифицированных
средств защиты информации» размещен на
официальном сайте ФСТЭК России

www.fstec.ru

(раздел «Техническая защита информации»/
«Документы»/«Проекты»)

Предложения направлять
на адрес электронной почты

otd24@fstec.ru

до 20 февраля 2014 г.



Спасибо за внимание !

