

ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ  
(ФСТЭК РОССИИ)

УТВЕРЖДАЮ  
Директор ФСТЭК России

В.Селин

«\_\_\_» февраля 2014 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**РЕКОМЕНДАЦИИ ПО ОБНОВЛЕНИЮ СЕРТИФИЦИРОВАННЫХ  
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

**(ПРОЕКТ)**

1. Настоящий методический документ ФСТЭК России разработан и утвержден 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, Положением о сертификации средств защиты информации, утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608, и пунктом 9 Положения об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, утвержденного постановлением Правительства Российской Федерации от 15 мая 2010 г. № 330 и предназначен для заявителей на осуществление сертификации средств защиты информации (далее – заявители), испытательных лабораторий и органов по сертификации, при проведении ими работ по обеспечению соответствия сертифицированных средств защиты информации (далее – средства защиты информации) требованиям безопасности информации, а также для пользователей сертифицированных средств защиты информации (далее - пользователи).

Положения настоящего методического документа предназначены для использования при разработке конструкторской и эксплуатационной документации на средства защиты информации, а также при заключении договоров на проведение сертификационных испытаний и инспекционного контроля.

2. Заявитель при необходимости разрабатывает и организует обновление пользователем средств защиты информации.

В случае если заявитель не является разработчиком средства защиты информации, он своевременно получает обновления от разработчика и обеспечивает их качество.

3. В зависимости от степени влияния на безопасность средства защиты информации устанавливаются следующие типы его обновления:

1 тип - обновление баз данных, необходимых для реализации функций безопасности средства защиты информации (обновление баз сигнатур вирусов средств антивирусной защиты, баз сигнатур уязвимостей средств контроля (анализа) защищенности, баз решающих правил систем обнаружения вторжений и других);

2 тип - обновление, направленное на устранение уязвимостей средства защиты информации;

3 тип - обновление, направленное на добавление функции (функций) безопасности средства защиты информации, на совершенствование реализации функции (функций) безопасности средства защиты информации, на расширение числа поддерживаемых программных и аппаратных платформ;

4 тип - обновление, не влияющее на безопасность средства защиты информации (изменение интерфейса средства защиты информации, иных функций, не влияющее на функции безопасности средства защиты информации).

4. Заявитель, разработав или получив обновление средства защиты информации, определяет его тип в соответствии с пунктом 3 данного методического документа.

5. Если определен 1 тип обновления, заявитель осуществляет гарантированное доведение до пользователей информации о необходимости обновления и предоставляет возможность его получения по каналу, который обеспечивает его целостность и доступность (далее – доверенный канал).

Максимальный срок доведения обновления 1 типа до пользователей по доверенному каналу указывается в эксплуатационной документации.

Пользователь при получении указанной информации осуществляет в указанный срок получение обновления средства защиты информации и в течение одних суток с момента получения применяет его.

Заявитель ежегодно организует проведение инспекционного контроля средства защиты информации с полным пакетом обновлений 1 типа в испытательной лаборатории.

Испытательная лаборатория в течение 15 дней проводит инспекционный контроль средства защиты информации с указанным пакетом обновлений и представляет техническое заключение по результатам инспекционного контроля заявителю.

6. Если заявителем определен 2, 3 или 4 тип обновления средства защиты информации, заявитель представляет в испытательную лабораторию обновление средства защиты информации, при необходимости само средство защиты информации, необходимую документацию (извещения о внесении изменений в документацию) на средство защиты информации, исходные тексты программного обеспечения средства защиты информации в случае необходимости проверки на отсутствие недеklarированных возможностей.

Испытательная лаборатория, проведя предварительный анализ представленных заявителем обновления средства защиты информации и документации, не позднее 3 дней с момента обращения заявителя уточняет тип обновления и сообщает об этом заявителю.

7. Если испытательной лабораторией установлен 2 тип обновления, заявитель незамедлительно осуществляет гарантированное доведение до пользователей информации о необходимости обновления (с подтверждением её получения) и предоставляет возможность его получения по доверенному каналу.

Максимальный срок доведения обновления 1 типа до пользователя по доверенному каналу указывается в эксплуатационной документации.

Пользователь при получении указанной информации осуществляет в указанный срок получение обновления средства защиты информации

инезамедлительно применяет его, о чем делает соответствующую отметку в эксплуатационной документации (формуляр или паспорт) с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.

Испытательная лаборатория в течение 30 суток с момента получения обновления осуществляет инспекционный контроль и представляет техническое заключение по его результатам заявителю.

Испытательная лаборатория представляет указанное техническое заключение, а также другие материалы инспекционного контроля в ФСТЭК России.

ФСТЭК России при необходимости вносит изменения в сертификат соответствия на средство защиты информации.

Заявитель, получив в ФСТЭК России сертификат соответствия с внесенными изменениями, доводит его копию, а также изменения в эксплуатационную документацию до всех пользователей.

При невозможности устранения уязвимостей средства защиты информации, в том числе путем применения обновления, заявитель разрабатывает ограничения по применению средства защиты информации, которые незамедлительно доводит до испытательной лаборатории.

Испытательная лаборатория в течение двух суток с момента обращения заявителя направляет свое заключение заявителю.

Если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, заявитель незамедлительно и гарантированно с подтверждением доводит его до пользователя.

Пользователь реализует указанное ограничение по применению средства защиты информации. Если пользователь не может реализовать ограничение по применению средства защиты информации он прекращает его применение.

Заявитель вносит необходимые изменения в эксплуатационную документацию и направляет её совместно с заключением испытательной лаборатории в ФСТЭК России.

ФСТЭК России при необходимости вносит изменения в сертификат соответствия на средство защиты информации в части, касающейся указанного ограничения по применению.

Заявитель, получив сертификат соответствия с внесенными изменениями, доводит его копию, а также изменения в эксплуатационную документацию до всех пользователей.

Если уязвимость не устраняется путем установления ограничений по применению, заявитель незамедлительно и гарантированно, с подтверждением, сообщает об этом всем пользователям и в ФСТЭК России.

Пользователи прекращают применение средства защиты информации.

ФСТЭК России прекращает действие сертификата соответствия (аннулирует сертификат соответствия), вносит изменения в Государственный реестр сертифицированных средств защиты информации и размещает на официальном сайте Службы информационное сообщение об указанном событии.

8. Если испытательной лабораторией установлен 3 тип обновления, она в течение срока, определенного в договоре с заявителем, проводит инспекционный контроль средства защиты информации с указанным обновлением.

Техническое заключение и материалы инспекционного контроля испытательная лаборатория направляет в ФСТЭК России.

ФСТЭК России рассматривает материалы инспекционного контроля и при необходимости вносит изменения в сертификат соответствия на средство защиты информации.

Заявитель, получив в ФСТЭК России сертификат соответствия с внесенными изменениями, доводит его копию, а также изменения в эксплуатационную документацию до всех пользователей, осуществляет

доведение до пользователей информации о возможности обновления средства защиты информации и предоставляет возможность его получения по доверенному каналу.

Пользователь при получении указанной информации принимает решение о необходимости применения обновления.

Пользователь, в случае применения обновления, делает соответствующую отметку в эксплуатационной документации (формуляр или паспорт) с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.

9. Если испытательной лабораторией установлен 4 тип обновления она в течение срока, определенного в договоре с заявителем проводит инспекционный контроль средства защиты информации с указанным обновлением.

Техническое заключение по результатам инспекционного контроля испытательная лаборатория направляет заявителю.

Заявитель направляет указанное техническое заключение и изменения в конструкторскую и эксплуатационную документацию в ФСТЭК России.

Заявитель осуществляет доведение до пользователей информации о возможности обновления средства защиты информации и предоставляет возможность его получения по доверенному каналу.

Пользователь, при получении указанной информации, принимает решение о необходимости применения обновления.

Пользователь, в случае применения обновления, делает соответствующую отметку в эксплуатационной документации (формуляр или паспорт) с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.

10. Срок представления заявителем обновлений 2, 3 и 4 типа в испытательную лабораторию может уточняться в соответствии с требованиями к определенному средству защиты информации, утвержденными ФСТЭК России.