Совершенствование порядка сертификации и требований по безопасности информации к средствам защиты информации

ШЕВЦОВ Дмитрий Николаевич
начальник управления ФСТЭК России

Новые документы по сертификации СЗИ

Положение о системе сертификации средств защиты информации

утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55

приказ прошел публичное обсуждение и антикоррупционную экспертизу, оценку регулирующего воздействия в Минэкономразвития России, зарегистрирован Минюстом России 11 мая 2018 г. № 51063, вступил в силу с 1 августа 2018 г.

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131

приказ зарегистрирован Минюстом России 14 ноября 2018 г. № 52686, вступил в силу с 1 августа 2018 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

утверждена ФСТЭК России 11 февраля 2019 г.

методика применяется при проведении сертификационных испытаний с 1 мая 2019 г.

Старые документы по сертификации СЗИ

Положение о сертификации средств защиты информации по требованиям безопасности информации

утверждено приказом Гостехкомиссии России от 27 октября 1995 г. № 199

не применяется с 1 августа 2018 г.

Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей

утвержден приказом Гостехкомиссии России от 4 июня 1999 г. № 114

Положение о системе сертификации СЗИ

Положение о системе сертификации средств защиты информации

утверждено приказом ФСТЭК России
от 3 апреля 2018 г. № 55

приказ прошел публичное обсуждение и антикоррупционную экспертизу, оценку регулирующего воздействия в Минэкономразвития России, зарегистрирован Минюстом России 11 мая 2018 г. № 51063, вступил в силу с 1 августа 2018 г.

Увеличение срока действия сертификата соответствия до 5 лет

Возможность применения средств защиты информации по окончанию срока действия сертификата соответствия

Детализация процедур сертификации, установление сроков осуществления процедур сертификации

Определение порядка внесения изменений в сертифицированные СЗИ

Повышение требований, предъявляемых к заявителю на сертификацию и изготовителю СЗИ

Уточнение схем сертификации, введение процедуры проверки технической поддержки

Установление критериев отказа в принятии решения о проведении сертификации, приостановления и прекращения сроков действия сертификатов

Возможность контроля за проведением сертификации

Заявитель на сертификацию, схемы сертификации

Организация, эксплуатирующая СЗИ

Изготовитель СЗИ

Схемы сертификации:

для единичного образца СЗИ - **проведение испытаний образца СЗИ** и **проверка организации его технической поддержки**

для партии СЗИ - **проведение испытаний выборки образцов СЗИ** и **проверка организации их технической поддержки**

для серийного производства СЗИ - **проведение испытаний выборки образцов СЗИ** и **проверка организации производства и технической поддержки**

*Сертификация единичного образца или партии СЗИ организуется заявителем, планирующим применять СЗИ защиты информации, в случае, **если отсутствуют идентичные серийно производимые сертифицированные СЗИ**.*

***Техническая поддержка СЗИ (поддержка безопасности) -** обеспечение соответствия сертифицированных СЗИ требованиям по безопасности информации, устранение недостатков и дефектов СЗИ, в том числе устранение уязвимостей и недекларированных возможностей программного обеспечения СЗИ, информирование потребителей об обновлении программного обеспечения СЗИ, доведение до потребителей обновлений программного обеспечения СЗИ, а также изменений в эксплуатационную документацию.*

Новые документы по сертификации СЗИ

Положение о системе сертификации средств защиты информации

утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55

приказ прошел публичное обсуждение и антикоррупционную экспертизу, оценку регулирующего воздействия в Минэкономразвития России, зарегистрирован Минюстом России 11 мая 2018 г. № 51063, вступил в силу с 1 августа 2018 г.

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131

приказ зарегистрирован Минюстом России 14 ноября 2018 г. № 52686, вступил в силу с 1 августа 2018 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

утверждена ФСТЭК России 11 февраля 2019 г.

методика применяется при проведении сертификационных испытаний с 1 мая 2019 г.

Требования к изготовителю СЗИ

Изготовители средств защиты информации, составляющей государственную тайну, должны иметь лицензию ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну.

Изготовители средств защиты информации ограниченного доступа, не составляющей государственную тайну, должны иметь лицензию ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации

Срок действия сертификата соответствия

Срок действия *сертификата соответствия не может превышать* ***5 лет.***

Сертификат соответствия выдается на срок, указанный в заявке на сертификацию.

Средство защиты информации может применяться по окончании срока действия сертификата соответствия *при условии соблюдения требований по безопасности информации и осуществления заявителем его технической поддержки.*

Назначение СЗИ

В заявке на сертификацию указывается ***назначение СЗИ*** *(степень секретности защищаемой информации, категория объекта информатизации, тип и класс защищенности информационной (автоматизированной) системы).*

Области применения СЗИ, сертифицированных в системе сертификации ФСТЭК России:

объекты информатизации;

государственные информационные системы;

значимые объекты критической информационной инфраструктуры;

информационные системы общего пользования;

информационные системы персональных данных;

автоматизированные системы управления производственными и технологическими процессами.

Направления совершенствования сертификации СЗИ

Утверждение Перечня типов средств защиты информации, подлежащей сертификации в системе сертификации ФСТЭК России

Совершенствование Государственного реестра сертифицированных средств защиты информации (уточнение состояния поддержки по каждому сертификату, повышение информативности, предоставление аналитических инструментов)

Разработка новых редакций Требований к средствам антивирусной защиты, системам обнаружения вторжений, средствам доверенной загрузки, средствам контроля съемных машинных носителей информации, межсетевым экранам и операционным системам

Разработка и утверждение Требований к средствам управления потоками информации, средствам виртуализации, системам управления базами данных и к иной продукции, подлежащей сертификации

Требования доверия

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131

приказ зарегистрирован Минюстом России 14 ноября 2018 г. № 52686, вступил в силу с 1 августа 2018 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

утверждена ФСТЭК России 11 февраля 2019 г.

методика применяется при проведении сертификационных испытаний с 1 мая 2019 г.

Порядок применения Требований доверия

Информационное сообщение ФСТЭК России «О порядке применения Требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий и Методики выявления уязвимостей и недекларированных возможностей в программном обеспечении при проведении сертификации средств защиты информации»

(ПРОЕКТ)

Требования доверия и Методика выявления уязвимостей и НДВ применяются при проведении сертификации с 1 мая 2019 г.

С 1 мая 2019 г. подать заявку на сертификацию СЗИ возможно только на соответствие Требованиям доверия.

Сертификация по решениям о проведении сертификации, выданным до 1 мая 2019 г. может быть завершена на соответствие требованиям РД НДВ.

Требования к средствам антивирусной защиты, системам обнаружения вторжений, средствам доверенной загрузки, средствам контроля съемных машинных носителей информации, межсетевым экранам и операционным системам, а также Профили защиты данных СЗИ применяются только в части общих требований и требований к функциям безопасности и не применяются в части требований доверия.

Требования доверия

Требования доверия являются *обязательными требованиями в области технического регулирования к продукции (работам, услугам), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа.*

Требования доверия применяются *к программным и программно-техническим средствам технической защиты информации, средствам обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.*

Требования доверия устанавливают *уровни, характеризующие безопасность применения средств для обработки и защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа.*

Уровни доверия

Устанавливается **6** уровней доверия. Самый низкий уровень – 6, самый высокий – 1.

Уровень доверия	ГИС, ИСПДн, ЗО КИИ, АСУ ТП, ИСОП	Классы защиты СЗИ
4	ЗО КИИ 1 категории; ГИС 1 класса; АСУТП 1 класса; ИСПДн 1 уровня; ИСОП II класса	4
5	ЗО КИИ 2 категории; ГИС 2 класса; АСУТП 2 класса; ИСПДн 2 уровня	5
6	ЗО КИИ 3 категории; ГИС 3 класса; АСУТП 3 класса; ИСПДн 3 и 4 уровня	6

Содержание Требований доверия

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
1.	**Требования к разработке и производству средства:**			
1.1.	требования к разработке модели безопасности средства			+
1.2.	требования к проектированию архитектуры безопасности средства	+	=	=
1.3.	требования к разработке функциональной спецификации средства	+	+	+
1.4.	требования к проектированию средства	+	=	=
1.5.	требования к разработке представления реализации средства	+	+	+
1.6.	требования к средствам, применяемым для разработки средства	+	=	=
1.7.	требования к управлению конфигурацией средства	+	+	+
1.8.	требования к разработке документации по безопасной разработке средства	+	=	=
1.9.	требования к разработке руководства пользователя средства	+	=	=
1.10.	требования к разработке руководства администратора средства	+	=	=
2.	**Требования к проведению испытаний средства:**			
2.1.	требования к тестированию средства	+	+	+
2.2.	требования к испытаниям по выявлению уязвимостей и недекларированных возможностей средства	+	+	+
2.3.	требования к проведению анализа скрытых каналов в средстве		+	=
3.	**Требования к поддержке безопасности средства:**			
3.1.	требования к устранению недостатков средства	+	+	+
3.2.	требования к обновлению средства	+	+	+
3.3.	требования к документированию процедур устранения недостатков и обновления средства	+	=	=

Содержание Требований доверия

Требования к обновлению средства, соответствующего 6 уровню доверия

89. Обновление средства должно предусматривать:
информирование потребителей средства о выпуске обновлений;
обеспечение возможности получения обновления средства способами, обеспечивающими его целостность.

Требования к обновлению средства, соответствующего 5 уровню доверия

93. Наряду с требованиями к обновлению средства, установленными пунктом 89 настоящих Требований, дополнительно предъявляются следующие требования:
в случае получения обновления средства по сетям связи средство должно получать такие обновления с информационного ресурса заявителя;
при доведении обновлений средства до потребителей должны обеспечиваться подлинность и целостность обновлений за счет применения электронной цифровой подписи.

Требования к обновлению средства, соответствующего 4 уровню доверия

97. Наряду с требованиями к обновлению средства, установленными пунктом 93 настоящих Требований, доведение информации о выпуске обновлений средства должно осуществляться до каждого потребителя сертифицированного средства путем отправки сообщений на электронные адреса потребителей или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически.

Методика выявления уязвимостей и НДВ в ПО

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

утверждена ФСТЭК России 11 февраля 2019 г.

Методика определяет состав и содержание исследований по выявлению уязвимостей и НДВ в встраиваемом микропрограммном, общесистемном, прикладном программном обеспечении, в том числе программном обеспечении средств защиты информации, а также применяемые при этом методы исследований и инструментальные средства

В части встраиваемого микропрограммного (программного) обеспечения Методика применяется в случае, если такое программное обеспечение может быть извлечено из аппаратного обеспечения для проведения исследований

Методика применяется в полном объеме при проведении контроля отсутствия уязвимостей и НДВ, проводимого в соответствии с Требованиями доверия, утвержденными приказом ФСТЭК России от 30 июля 2018 г. № 131.

По решению заказчика или разработчика ПО Методика может применяться с целью обеспечения и поддержки процедур по разработке безопасного программного обеспечения, реализуемых в соответствии с ГОСТ Р 56939-2016 В этом случае объем исследований определяется заказчиком или разработчиком программного обеспечения

- Вопросы по сертификации средств защиты информации

- Телефоны: (495) 693-6872

(495) 632-1449

- Почта: **otd24@fstec.ru**

Совершенствование порядка сертификации и требований по безопасности информации к средствам защиты информации

ШЕВЦОВ Дмитрий Николаевич
начальник управления ФСТЭК России