

Проблемные вопросы сертификации средств защиты информации



ШЕВЦОВ Дмитрий Николаевич
начальник управления ФСТЭК России

Проблемные вопросы и направления их решения

Проблемы

Низкий уровень внедрения требований доверия, в том числе процессов разработки безопасного программного обеспечения, большие сроки устранения уязвимостей средств защиты информации

Значительные сроки проведения сертификации средств защиты информации

Необходимость повышения квалификации специалистов, участвующих в разработке и испытаниях средств защиты информации

Отсутствие требований по безопасности информации к отдельным типам средств защиты информации

Необходимость регламентации порядка аттестации информационных систем и контроля за проведением работ по аттестации



Направления решения проблем

Совершенствование требований доверия и национальных стандартов по разработке безопасного программного обеспечения, большие сроки устранения уязвимостей средств защиты информации

Совершенствование порядка сертификации средств защиты информации

Организация деятельности по повышению квалификации специалистов испытательных лабораторий и изготовителей

Разработка и совершенствование требований по безопасности информации к средствам защиты информации

Разработка порядка аттестации информационных систем, требований к форме и содержанию материалов аттестационных испытаний

Реализация требований 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 14 ноября 2018 г.,
применяется при проведении сертификационных
испытаний с 1 июня 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 июня 2019 г.

Уровень доверия, уровень контроля	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

Информационное сообщение ФСТЭК России «О Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»
№ 240/24/1525 от 29 марта 2019 г.

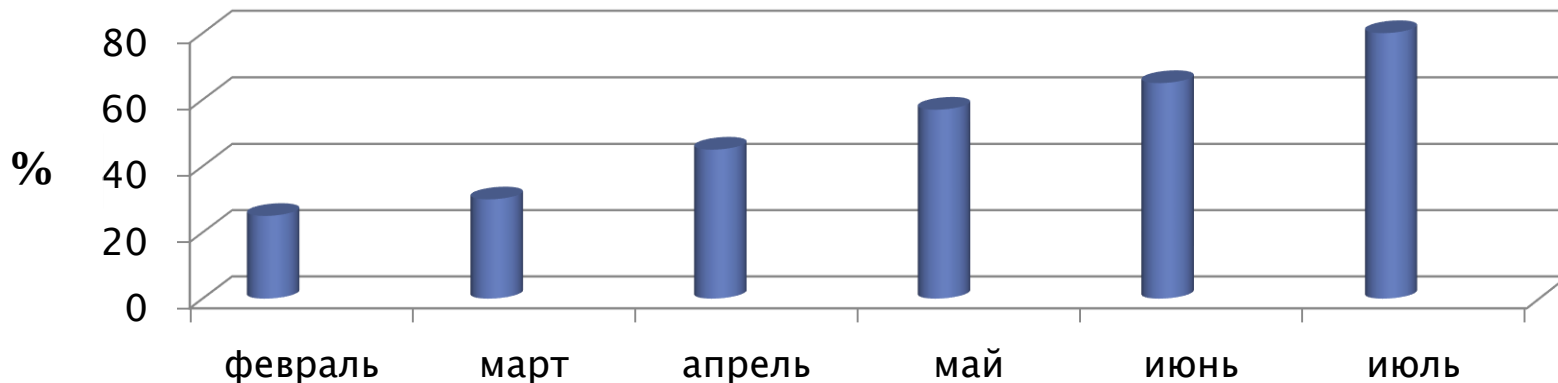


Реализация требований доверия

148 сертификатов соответствия на средства защиты информации от несанкционированного доступа должны быть переоформлены на соответствие Требованиям доверия

16 сертификатов соответствия (**10%**) переоформлено на соответствие Требованиям доверия

Динамика переоформления сертификатов соответствия в 2020 году



С 1 июня 2020 г. средства защиты информации, устанавливаемые при создании (модернизации) государственных информационных систем, должны соответствовать Требованиям доверия



Совершенствование требований доверия

Поручение Правительства Российской Федерации (ноябрь 2019 г.)

ФСТЭК России поручено до 1 марта 2020 г. обеспечить усиление требований по безопасности информации к оборудованию, применяемому на объектах критической информационной инфраструктуры в государственных информационных системах, взаимоувязанных с реализуемыми Минпромторгом России мерами по импортозамещению иностранного оборудования



Изменения в Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденные приказом ФСТЭК России от 30 июля 2018 г. № 131

Изменения подготовлены, проведено обсуждение с изготовителями СЗИ и СВТ, в феврале 2020 г. планируется согласовать изменения с Минпромторгом России и направить приказ об утверждении изменений на государственную регистрацию в Минюст России



Совершенствование требований доверия

Повышение требований по безопасности информации к аппаратным платформам

Предъявление требований по применению в СЗИ отечественных аппаратных платформ

Уровень доверия, класс защиты СЗИ	Дополнительные требования к аппаратным платформам средств защиты информации
4	Сведения о процессорах или микросхемах, выполняющих функции процессоров (микроконтроллеры), элементах памяти, сетевых картах, графических адаптерах аппаратной платформы средства должны быть включены в единый реестр российской радиоэлектронной продукции (требование вступает в силу с 1 января 2028 г.).
5	Сведения об аппаратной платформе средства должны быть включены в единый реестр российской радиоэлектронной продукции (требование вступает в силу с 1 января 2022 г.).
6	Требования по применению отечественных аппаратных платформ не предъявляются



Сов

Осно

Задачи на 2020 год

ции

ции

- низкий уровень знан
- низкое качество п
- информации;
- умышленные дейст
- проведения сертифик

на средство защиты

о увеличению сроков

Провести совещания рабочей группы по совершенствованию порядка сертификации (изготовители, ИЛ, ОС)

Разработать и утвердить Изменения в Положение о системе сертификации СЗИ

Пройти общественное обсуждение, оценку регулирующего воздействия и государственную регистрацию приказа ФСТЭК России об утверждении Изменений в Положение

Внедрить изменения в Положение в деятельность системы сертификации

Процедуры	Принятие прове сертиф
Сроки	
Действующие сроки	1 ме
Планируемые сроки	20 календа

Проведение экспертизы	Рассмотрение материалов в ФСТЭК России
45 календарных дней	45 календарных дней
30 календарных дней	30 календарных дней

Повышение квалификации специалистов испытательных лабораторий и органов по сертификации

НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТР ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ»
(НОУ ДПО «ЦПК ТЗИ»)

СОГЛАСОВАНО

Заместитель директора
ФСТЭК России

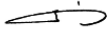


А. Куц

«26» апреля 2019 г.

СОГЛАСОВАНО

Начальник ФАУ «ГНИИИПТЗИ
ФСТЭК России»



А. Анищенко

«24» мая 2019 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА № 27
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ

«Техническая защита информации.

Инструментальная и технологическая поддержка методики
выявления уязвимостей и недеklarированных возможностей
в программном обеспечении»

УТВЕРЖДАЮ

Директор
НОУ ДПО «ЦПК ТЗИ»

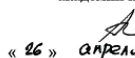


А. Акименко

«26» апреля 2019 г.

СОГЛАСОВАНО

Директор ФГБУН «Институт
системного программирования
им. В.П.Иванникова Российской
академии наук»



А. Аветисян

«26» апреля 2019 г.

ФЕДЕРАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«ГОСУДАРСТВЕННЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ ПРОБЛЕМ ТЕХНИЧЕСКОЙ
ЗАЩИТЫ ИНФОРМАЦИИ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО
ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ»



УДОСТОВЕРЕНИЕ

о повышении квалификации

Регистрационный номер 2626

НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ
ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ»

Настоящее удостоверение выдано Пужиче
Ольге Александровне

в том, что он (она)

с «20» мая 2019 г. по «1» июня 2019 г.

прошел (прошла) обучение

по программе повышения квалификации № 27

«Техническая защита информации.
Инструментальная и технологичес-
кая поддержка методики выявле-
ния уязвимостей и недеklarиро-
ванных возможностей в программном
обеспечении»

в объеме 122 часов

Приказ директора НОУ ДПО «ЦПК ТЗИ» о выпуске

июня 2019 года № 35

Директор

Секретарь

МП



А. Х. Анищенко

В. В. Федоров

г. Воронеж

54 специалиста
прошли повышение квалификации в 2019 году

Совершенствование порядка аттестации

Поручение Правительства Российской Федерации



ФСТЭК России до 1 сентября 2020 г. принять меры по установлению порядка аттестации объектов информатизации, информационных и автоматизированных систем на соответствие требованиям по защите информации, а также требований к форме и содержанию материалов аттестационных испытаний

детализация процедур аттестации,
установление сроков их проведения

требования к форме и содержанию
материалов аттестационных испытаний,
эксплуатационной документации

контроль ФСТЭК России за соблюдением
порядка аттестации

особенности аттестации сложных,
распределенных информационных систем



Совершенствование требований к средствам защиты информации

Задачи 2020 года

Требования к средствам антивирусной защиты (новая редакция)

Требования к системам управления базами данных

Требования к средствам управления потоками информации



- ▶ Вопросы по сертификации средств защиты информации
- ▶ Телефоны: (495) 693-6872
(495) 632-1449
- ▶ Почта: otd24@fstec.ru



Проблемные вопросы сертификации средств защиты информации



ШЕВЦОВ Дмитрий Николаевич
начальник управления ФСТЭК России