

Совершенствование требований по безопасности информации



ШЕВЦОВ Дмитрий Николаевич
начальник управления ФСТЭК России

Новые требования ФСТЭК России



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.



Уровни доверия

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

Уровень доверия	ОИ ,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

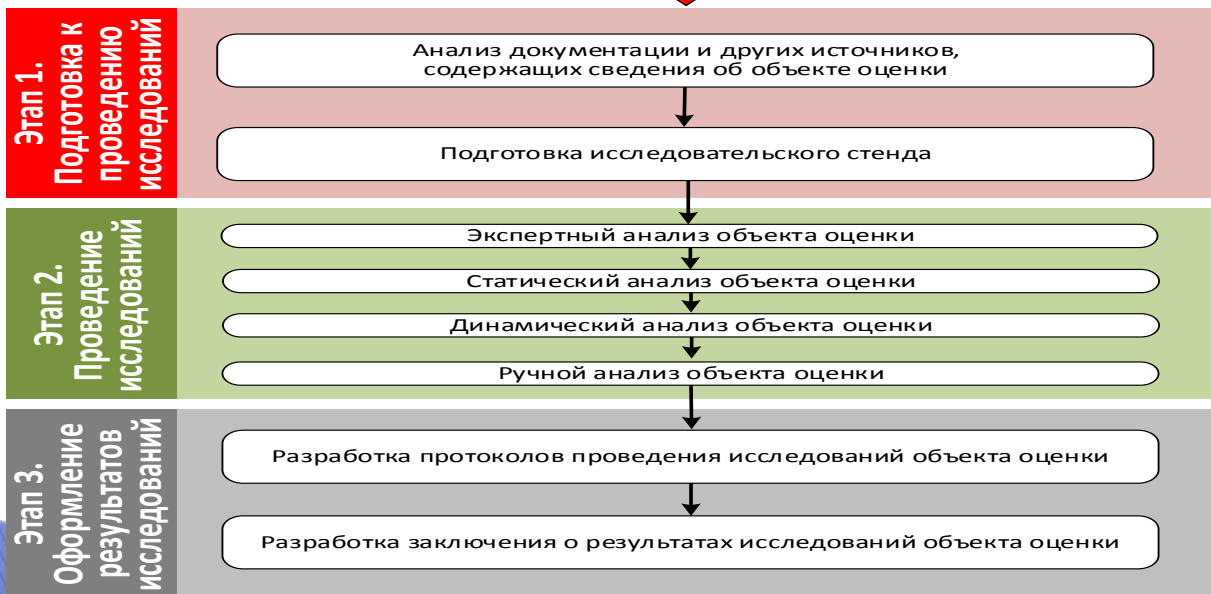


Содержание Требований доверия

№ 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 Методики выявления уязвимостей и НДВ в ПО



СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ ТК 362

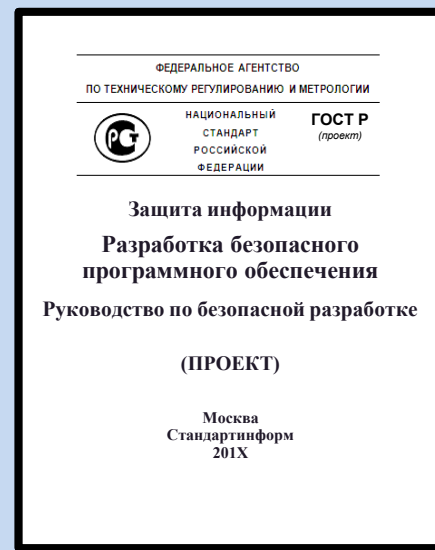
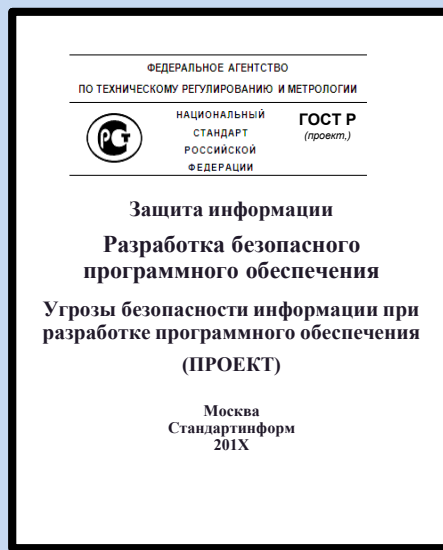
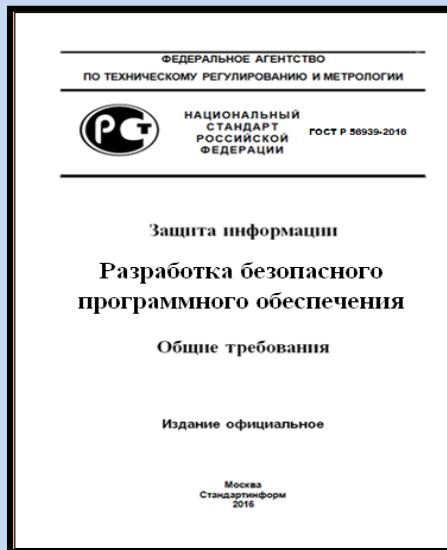
Структура технического комитета по стандартизации «Защита информации» (ТК 362)

ПК 1
Общеметодологический

ПК 2
Защита информации
на объектах информатизации
объектах
критической информационной
инфраструктуры

ПК 3
Средства и методы защиты
информации

ПК 4
Разработка безопасного
программного обеспечения



РАЗРАБОТКА НАЦИОНАЛЬНЫХ СТАНДАРТОВ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ ГОСТ Р 58256-2018
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

Защита информации

**Управление потоками информации в
информационной системе**

Формат классификационных меток

**Москва
Стандартинформ
2018**

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ ГОСТ Р *(проект)*
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

Защита информации

**Формальное моделирование
политики безопасности**

**Часть 1. Формальная модель
управления доступом**

(ПРОЕКТ)

**Москва
Стандартинформ
201X**

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ ГОСТ Р *(проект)*
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

Защита информации

**Формальное моделирование
политики безопасности**

**Часть 2. Верификация формальной
модели управления доступом**

(ПРОЕКТ)

**Москва
Стандартинформ
201X**

Совершенствование требований по безопасности информации



ШЕВЦОВ Дмитрий Николаевич
начальник управления ФСТЭК России