Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Новые требования к СКЗИ

Андрей Елистратов

Новые требования к СКЗИ

- **Требования к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не составляющей государственную тайну**

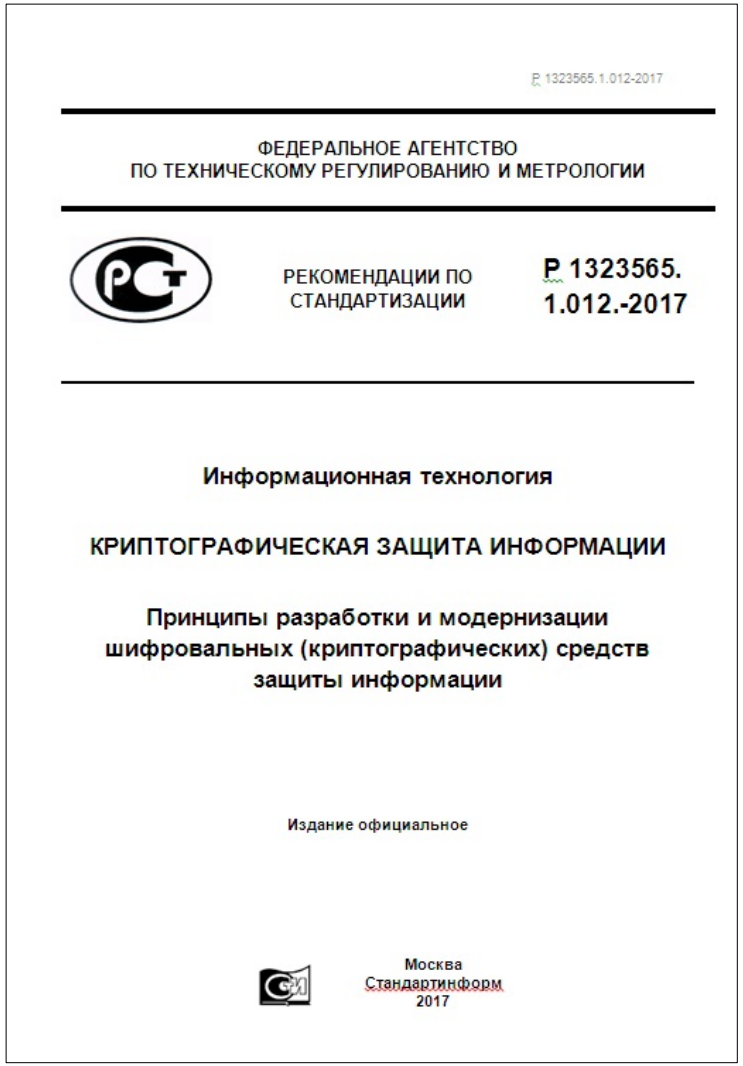
2021г.

Новая редакция Принципов

- **Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации**

Новая редакция Принципов

- **В техническом задании** на разработку (модернизацию) СКЗИ в дополнение к требованиям, определенным в «Положении о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», необходимо изложить следующее:



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

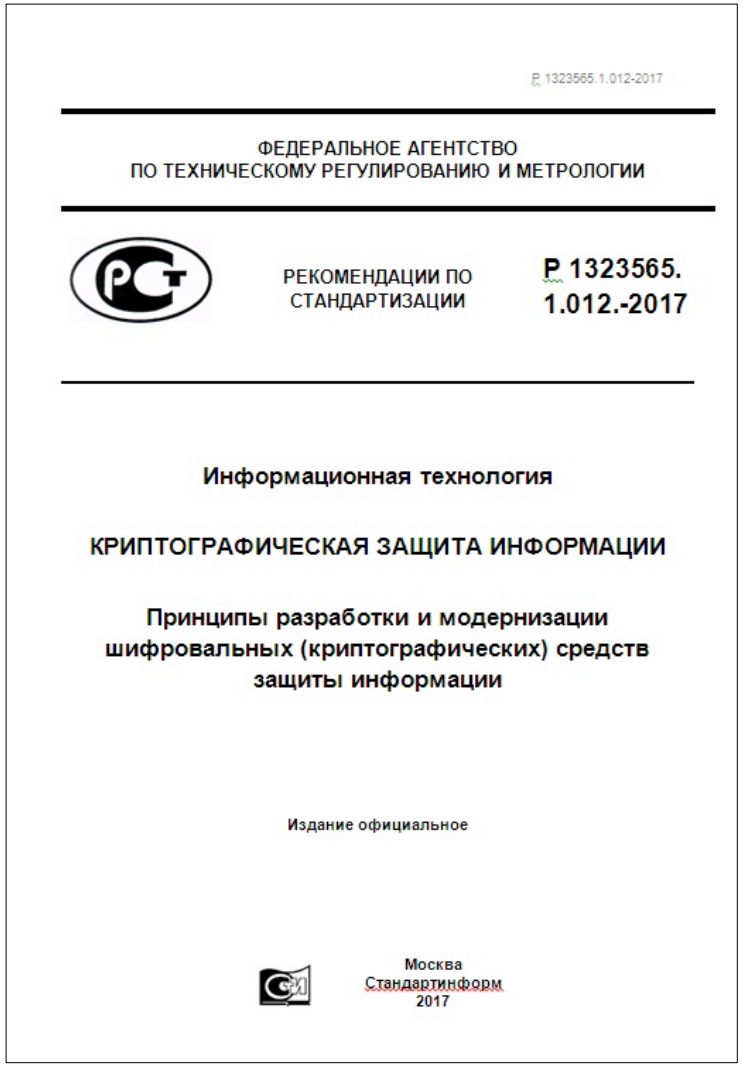
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- Класс разрабатываемого (модернизируемого) СКЗИ
- Условия эксплуатации СКЗИ
- Исходные положения для проведения тематических (контрольных тематических) исследований разрабатываемого (модернизируемого) СКЗИ



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

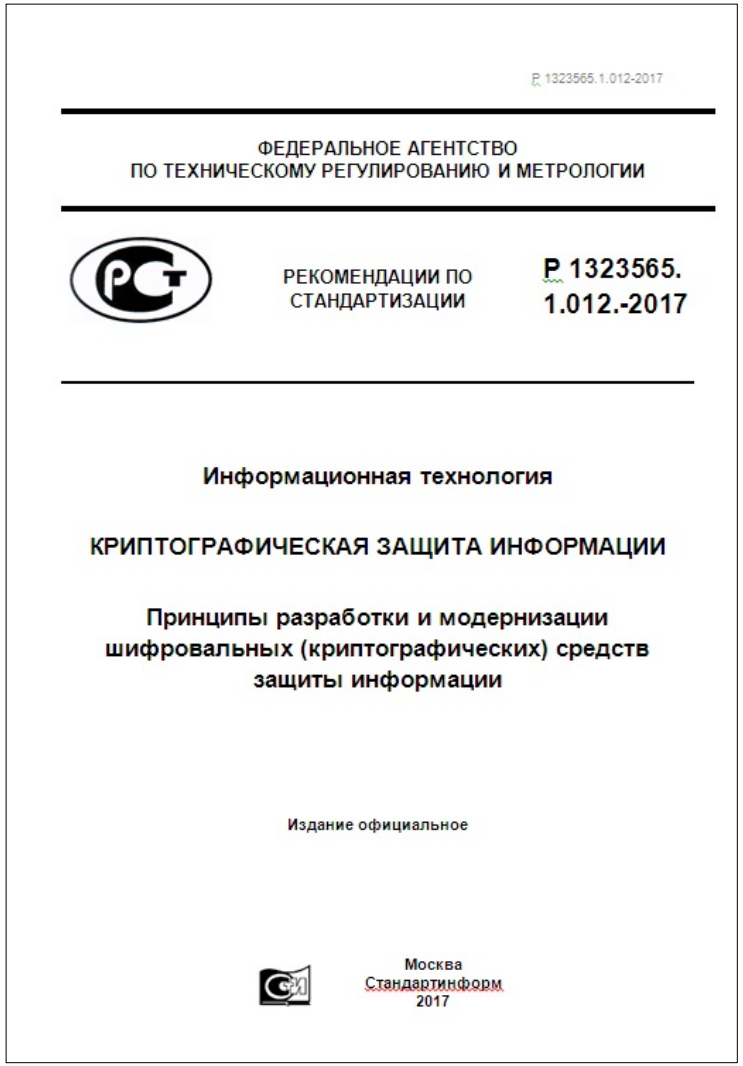
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- Срок действия криптоключей СКЗИ
- Верхний и нижний пределы изменения напряжения питания АС СКЗИ, а также температуры
- Необходимость и порядок использования криптографических механизмов контроля целостности СКЗИ (для СКЗИ классов КС1, КС2 и КС3)



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

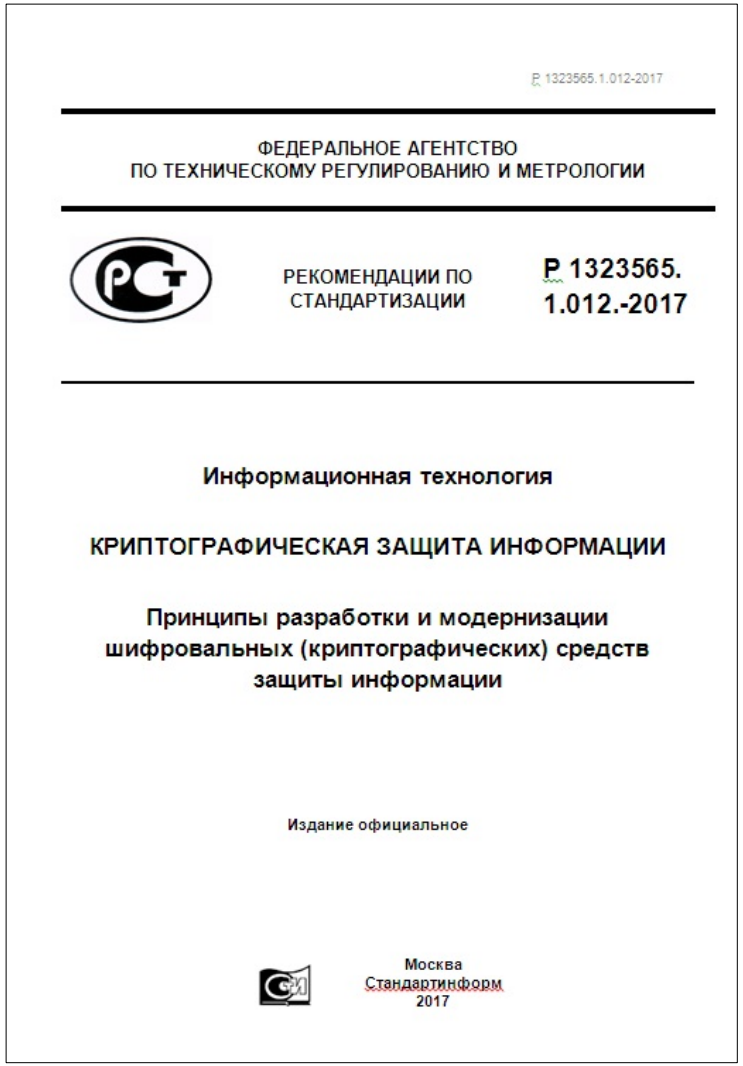
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- Необходимость и порядок использования криптографических механизмов контроля целостности СКЗИ (для СКЗИ классов КС1, КС2 и КС3)
- Необходимость наличия механизма динамического контроля целостности СКЗИ



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

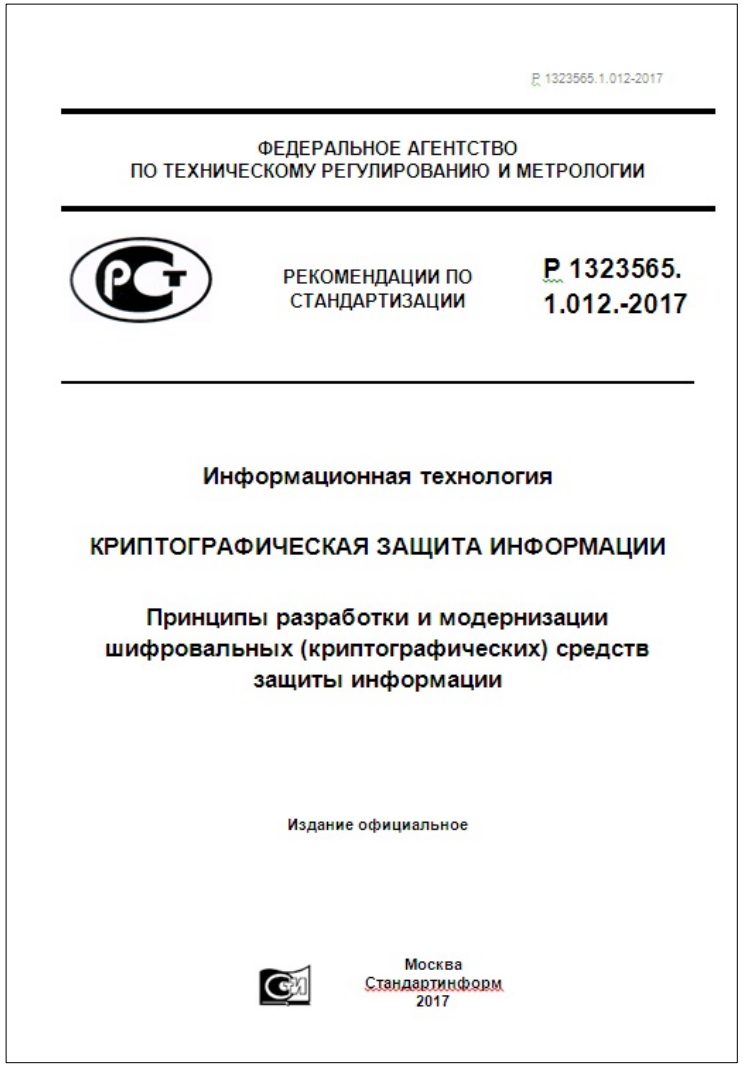
Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- Требования к разрабатываемому (модернизируемому) СКЗИ определяются:

- условиями эксплуатации СКЗИ (автономное/периодически контролируемое и располагаемое вне пределов контролируемой зоны,
- автономное/периодически контролируемое и располагаемое в контролируемой зоне,
- постоянно контролируемое и располагаемое в контролируемой зоне)



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

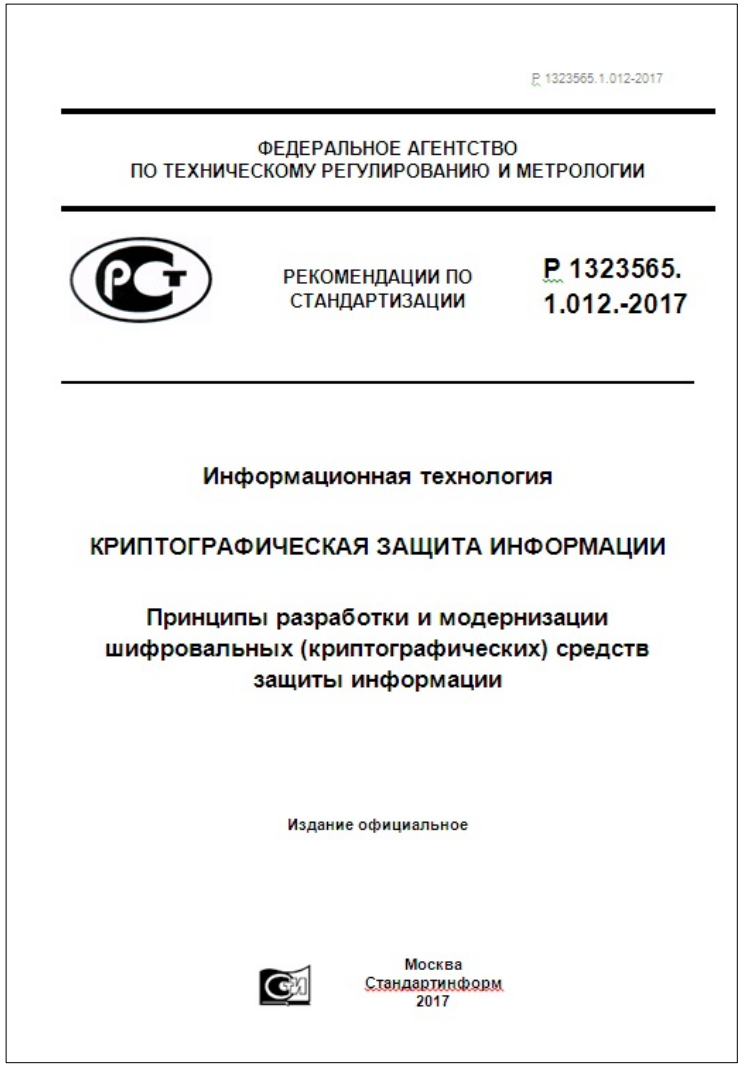
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- Работы по техническому заданию, всем дополнениям к нему и извещениям по изменениям должны быть завершены не позднее чем через 5 лет после утверждения первого/основного технического задания.



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

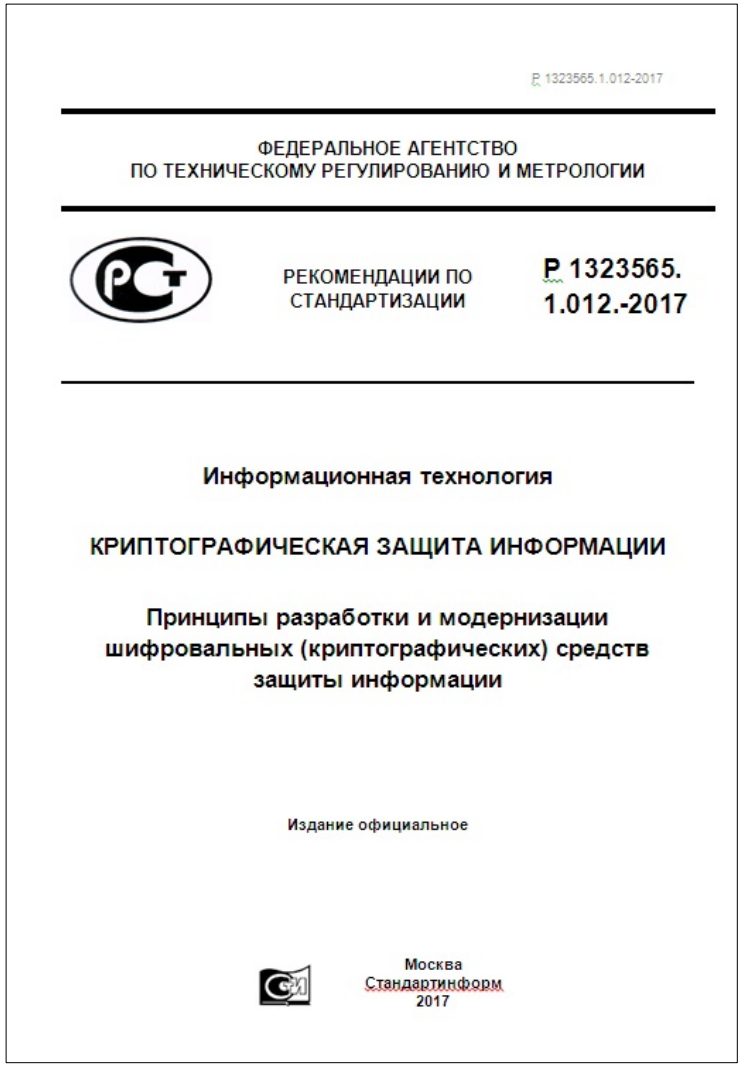
Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- **Новые функции СКЗИ**

- функция формирования кодов маркировки (реализуется техническими средствами формирования кода проверки);
- функция проверки кодов маркировки (реализуется техническим средствами проверки кода проверки, в том числе фискальным накопителем)



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

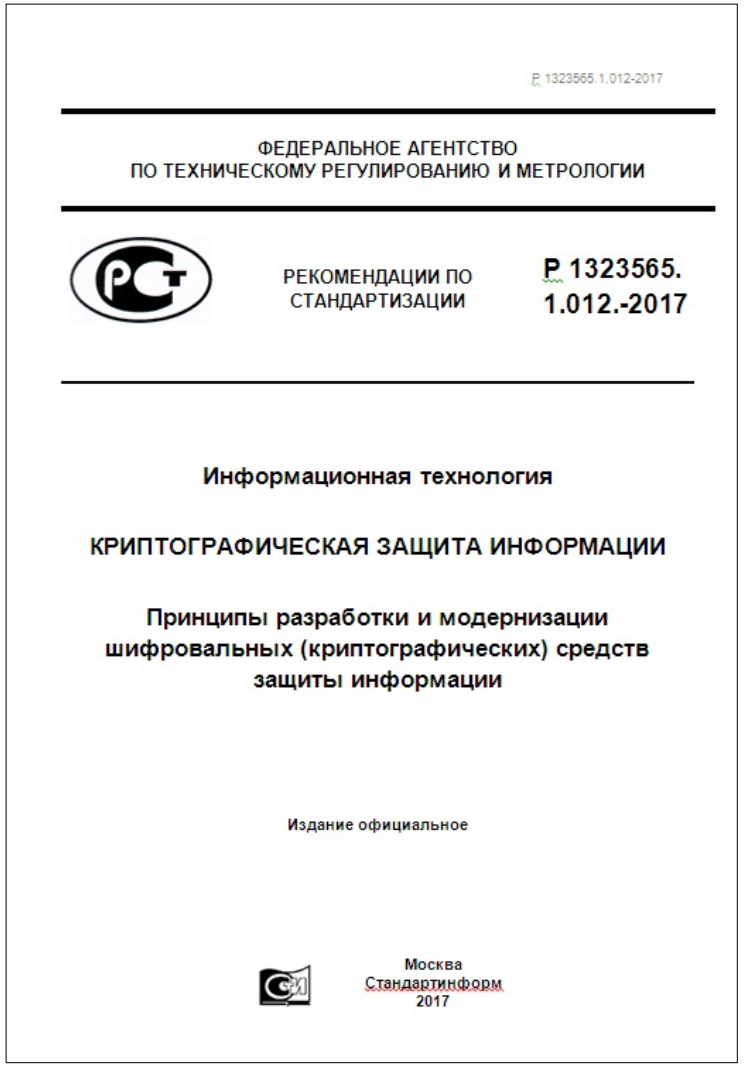
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- **Новый тип СКЗИ**
- Средство изготовления ключевых документов (СИКД) – средство предназначенное для изготовления ключевых документов (КД) для СКЗИ и использующее для изготовления ключевых документов, либо собственные датчики случайных чисел, либо исходную случайную двоичную последовательность, содержащуюся в ключевых документах, изготавливаемых ФСБ России



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

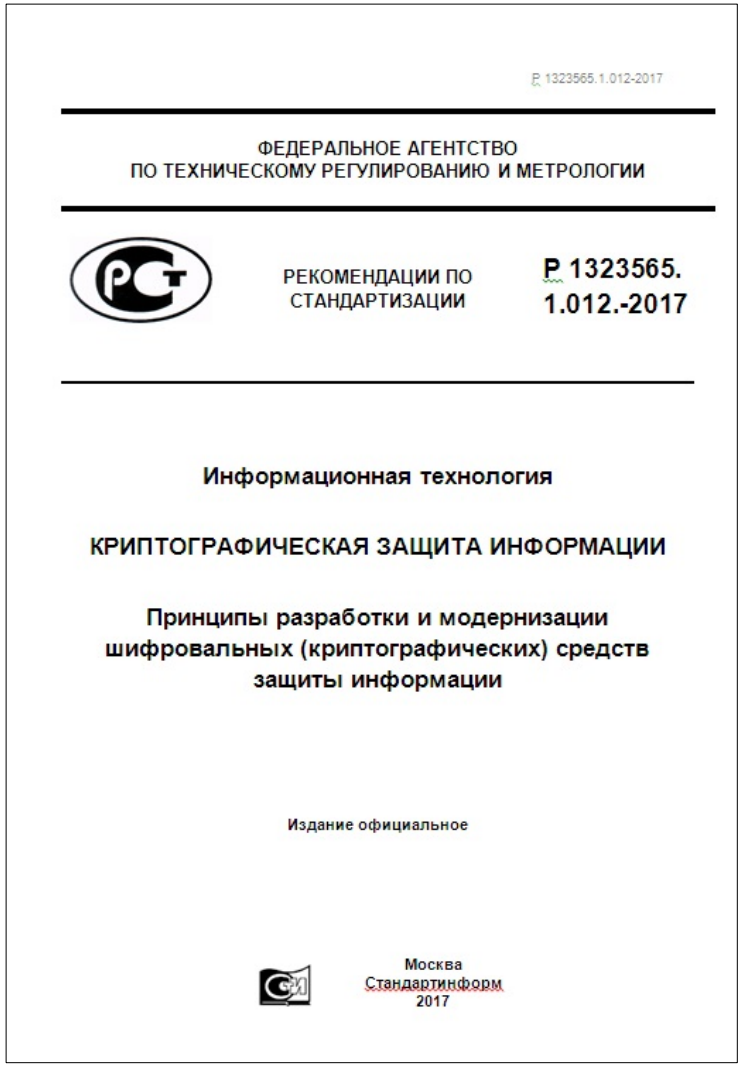
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- **Антивирусы**
- Совместно с СКЗИ должны применяться антивирусные средства (АВС) одобренные органом, ответственным за обеспечение технической защиты информации в создаваемой информационной системе, либо иные АВС по согласованию с органом, ответственным за обеспечение информационной безопасности в создаваемой информационной системе



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

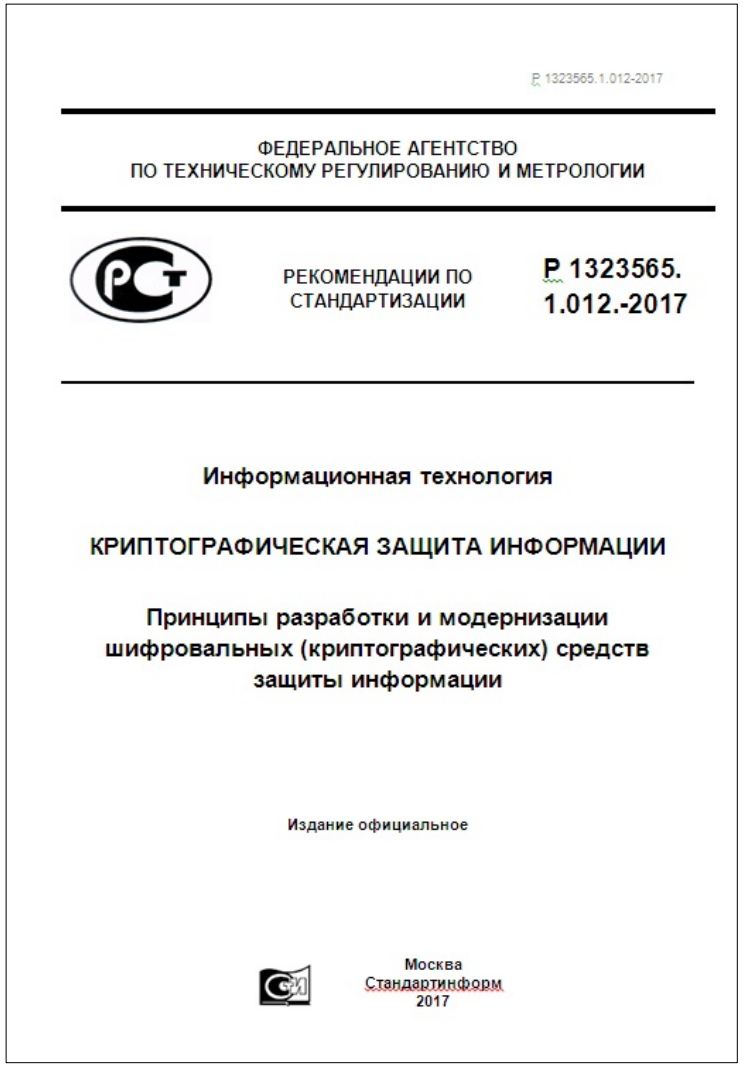
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- **Неявная компрометация**
- Последствия неявной компрометации ключа должны быть ограничены не более чем одним сроком действия ключа



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

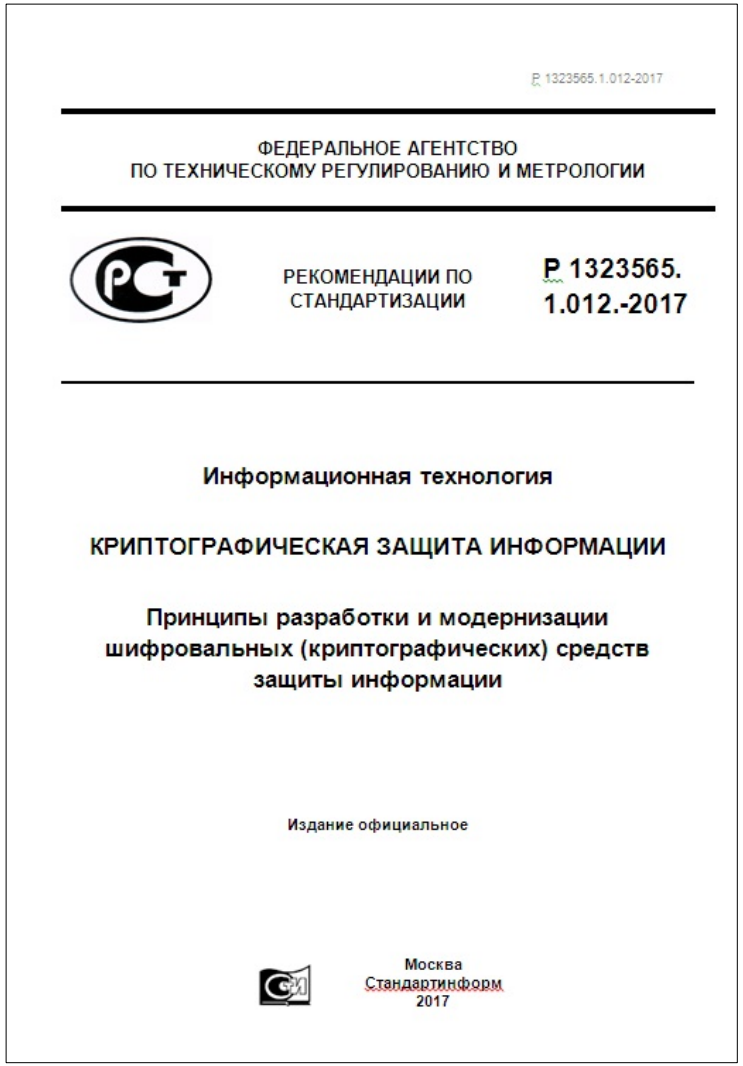
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- **Алгоритмическая защита**
- В ПО СКЗИ всех классов должно быть реализовано маскирование ключевой информации при ее вводе, пересылках и хранении, а также обязательное алгоритмическое выравнивание времени ввода и обработки ключевой информации по тактам вычислительной машины для любого обрабатываемого криптоключа.



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

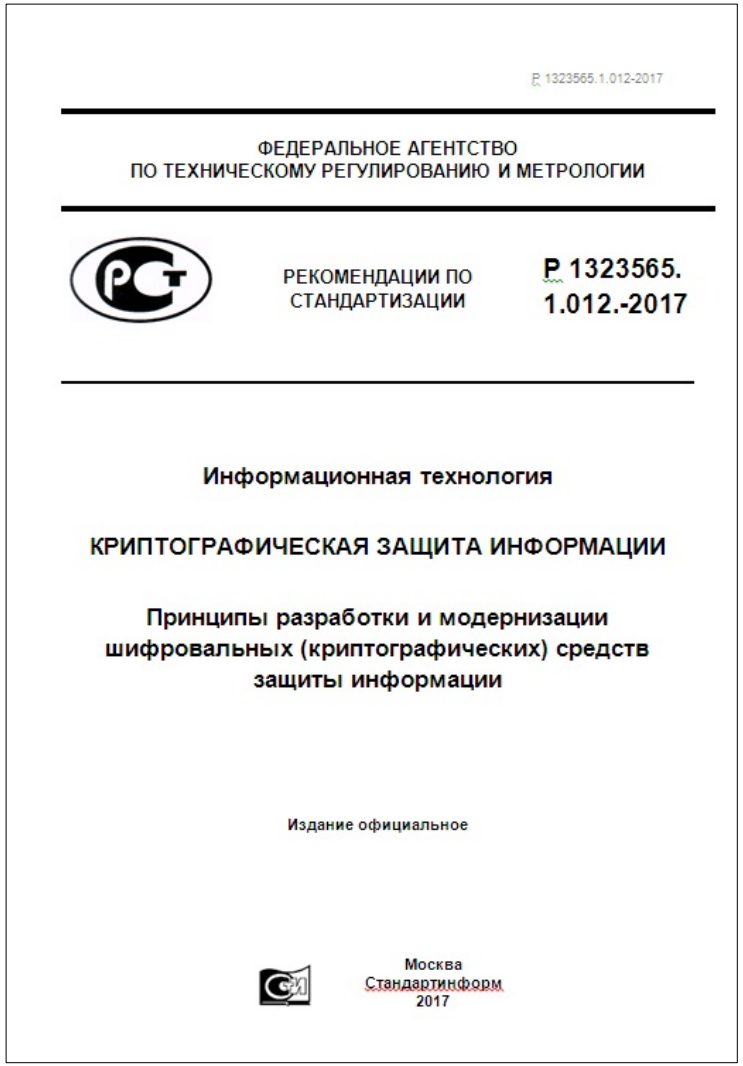
Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- **Требованиями по аутентификации процессов при сетевом взаимодействии**

- должна проводиться аутентификация лиц и процессов, осуществляющих удаленный (сетевой) доступ к СКЗИ. Доступ к криптографическим функциям СКЗИ по каналу связи возможен только после аутентификации.
- *Примечание: При дополнительном обосновании отсутствия возможности построения допустимых атак на СКЗИ возможно использование односторонней аутентификации процессов, осуществляющих удаленный (сетевой) доступ к СКЗИ.*



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

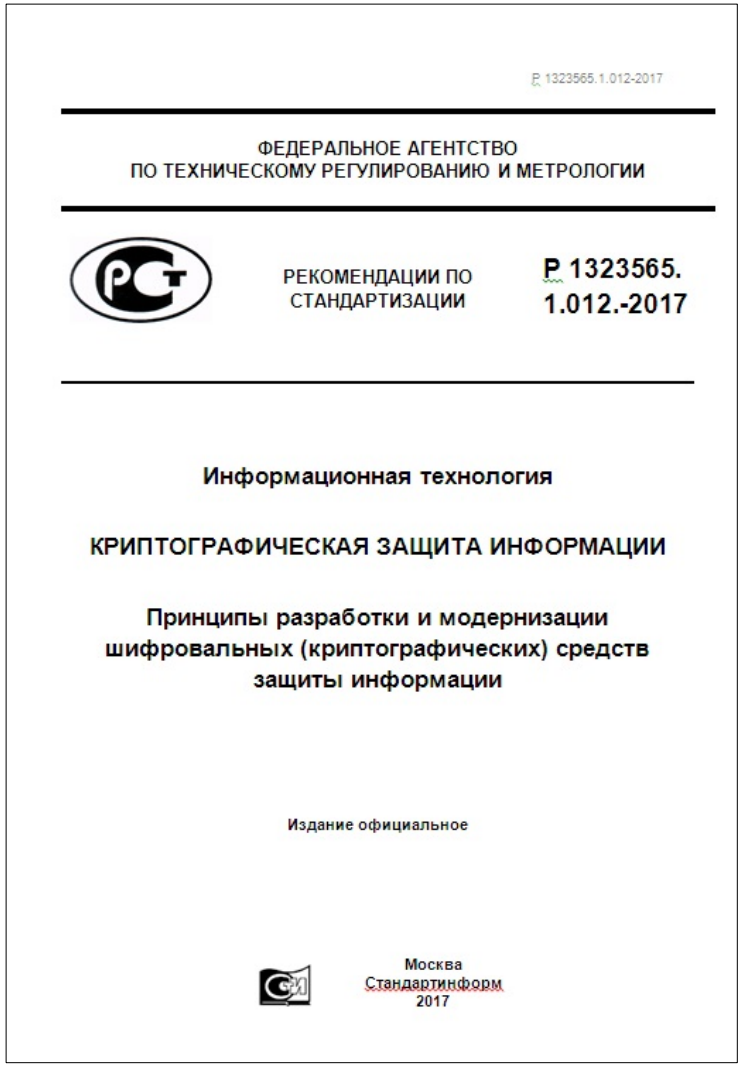
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- **Требованиями по НСД**
- Меры защиты СКЗИ от НСД могут быть обеспечены сторонними сертифицированными в системе сертификации ФСБ России средствами. В остальных случаях реализация мер защиты от НСД должна входить в состав СКЗИ



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

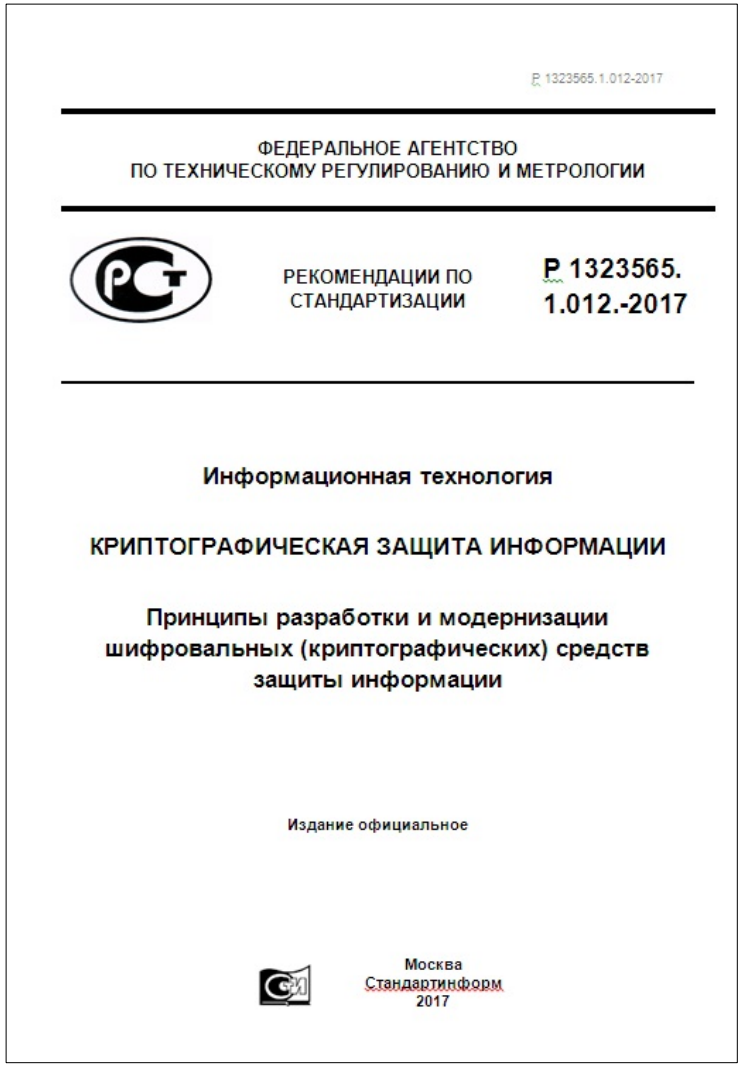
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- **Требования к документации**
- Правила пользования оформляются в соответствии с ТС 26.2.001-2020 «Состав и содержание правил пользования средств криптографической защиты информации» или, по согласованию с 8 Центром ФСБ России в другой форме



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

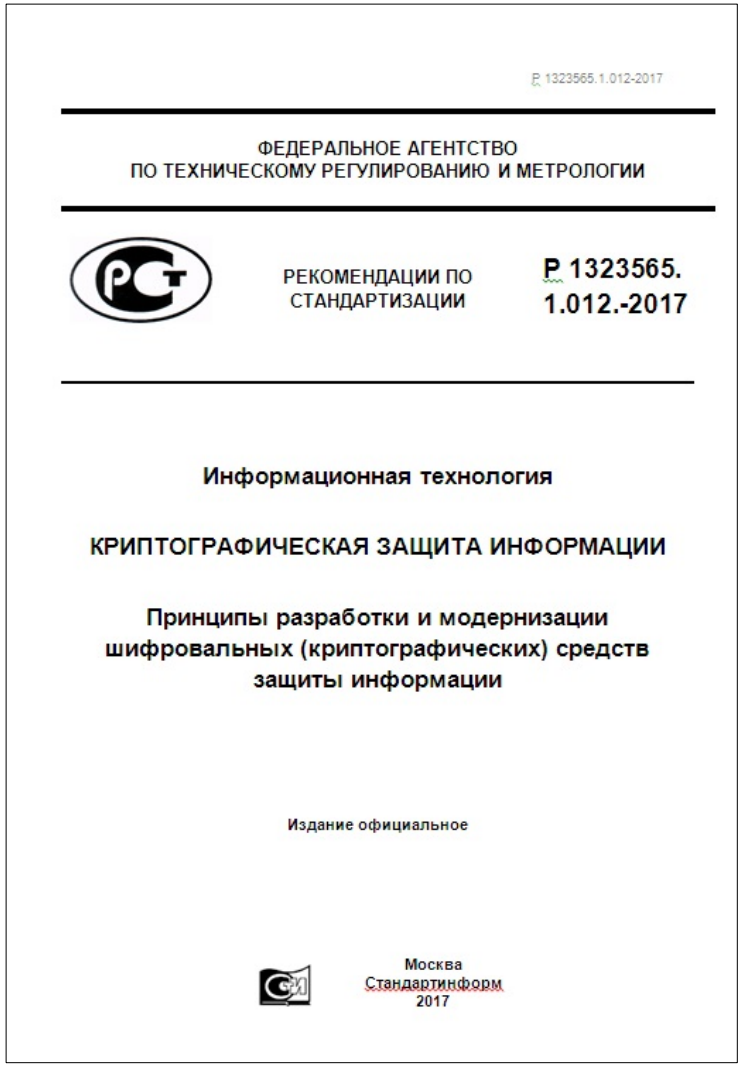
Москва
Стандартинформ
2017

Новая редакция Принципов

- **Требования к отчетным материалам**

По результатам тематических исследований готовятся следующие документы:

- - отчет по результатам тематических исследований;
- - оценка соответствия СКЗИ заданным требованиям.



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

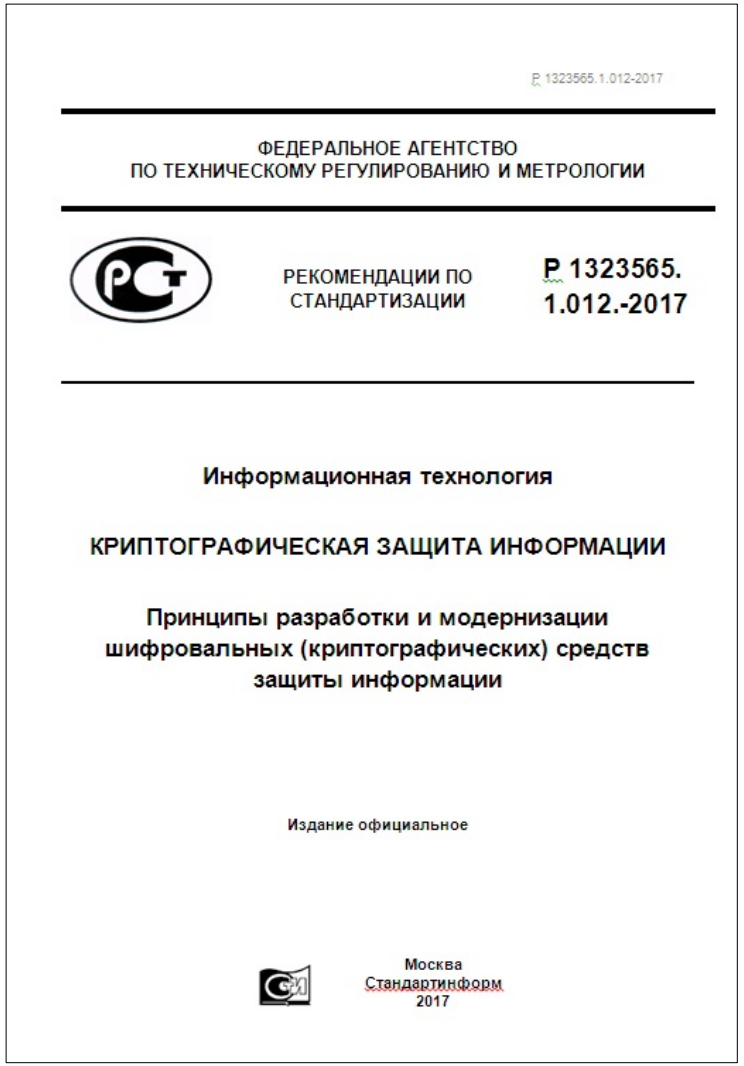
Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Новая редакция Принципов

- Экспертная организация, при необходимости, может запросить дополнительные обоснования соответствия предъявляемым требованиям, в том числе произвести контроль проведенных тематических исследований в организации, предоставившей результаты тематических исследований, а также может провести дополнительный встречный анализ некоторых результатов тематических исследований СКЗИ.



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

Вопросы