

Маалымат технологиялары

Коопсуздукту камсыз кылуунун методдору жана каражаттары. Маалыматтык технологиялардын коопсуздугун баалоо критерийлери

3-бөлүк

Коопсуздук талаптарын коргоо

Информационные технологии

Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий

Часть 3

Требования к обеспечению защиты

(ISO/IEC 15408-3-2008, IDT)

Издание официальное

Кыргызстандарт

Бишкек

Предисловие

Цели, принципы и основные положения стандартизации в Кыргызской Республике установлены законом Кыргызской Республики «О техническом регулировании в Кыргызской Республике» и КМС 1.0

Сведения о стандарте

1 ПОДГОТОВЛЕН Центром по стандартизации и метрологии при Министерстве экономики и коммерции Кыргызской Республики (Кыргызстандарт)

2 ВНЕСЕН Государственным комитетом национальной безопасности Кыргызской Республики

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Центра по стандартизации и метрологии при Министерстве экономики и коммерции Кыргызской Республики (Кыргызстандарт) от 4 июня 2024 г. № 25-СТ.

4 Настоящий стандарт идентичен ISO/IEC 15408-3-2008, Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3 Требования к обеспечению защиты

5 Официальной версией является текст на государственном и официальном языках. Международный стандарт разработан техническим комитетом ISO/IEC JTC 1 Информационные технологии, SC 31, Технологии автоматической идентификации и сбора данных.

Перевод с английского языка (en).

Сведения о соответствии стандартов (межгосударственных) ссылочным международным стандартам приведены в дополнительном приложении В.А.

Степень соответствия - идентичная (IDT).

6 ВВЕДЕН впервые

© Кыргызстандарт, 2024

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Центра по стандартизации и метрологии при Министерстве экономики и коммерции Кыргызской Республики (Кыргызстандарт)

Содержание

1	Область применения	1
2	Нормативные ссылки	1
3	Термины и определения	1
4	Обзор	2
5	Парадигма доверия	2
6	Компоненты обеспечения безопасности	4
7	Уровни обеспечения оценки (УОО)	13
8	Составные пакеты обеспечения	22
9	Класс ОЗП: оценка профиля защиты	27
10	Класс ООБ: оценка безопасности	35
11	Класс ОРА: разработка	45
12	Класс ОРД: Руководящие документы	82
13	ОЖЦ класса: поддержка жизненного цикла	86
14	Класс ОТЕ: Тесты	114
15	Класс ООУ: оценка уязвимости	127
16	Класс ОКО: Состав	133
Приложение А	<i>(информационное)</i> Разработка (ОРА)	149
Приложение В	<i>(информационное)</i> Состав (ОКО)	170
Приложение С	<i>(информационное)</i> Перекрестная ссылка на зависимости компонента обеспечения	179
Приложение D	<i>(информационное)</i> Перекрестная ссылка на ПЗ и компоненты обеспечения	182
Приложение E	<i>(информационное)</i> Перекрестные ссылки ОУД и компонентов доверия	183
Приложение F	<i>(информационное)</i> Перекрестные ссылки между СоПД и компонентами доверия	184
Приложение В.А.	<i>(информационное)</i> Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств	185

Введение

ISO/IEC 15408 под общим названием Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности в ИТ состоит из следующих частей:

- Часть 1: Введение и общая модель
- Часть 2: Функциональные компоненты обеспечения безопасности
- Часть 3: Компоненты обеспечения гарантии безопасности

Функциональные компоненты безопасности, определенные в данной части ISO/IEC 15408, являются основой для выражения функциональных требований безопасности в профиле защиты (далее - ПЗ) или задании по безопасности (далее - ЗБ). Данные требования содержат описание безопасного режима функционирования объекта оценки (далее - ОО) или ИТ-среды ОО и предназначены для достижения целей безопасности, установленных в ПЗ или ЗБ. Данные требования содержат свойства безопасности, которые пользователи могут обнаружить при непосредственном взаимодействии с ИТ (то есть при входе и выходе) или при реакции ИТ на запросы.

Функциональные компоненты безопасности выражают требования безопасности, направленные на противостояние угрозам в предполагаемой среде эксплуатации ОО и/или охватывающие любую идентифицированную политику безопасности организации и предположения.

Пользователи для данной части ISO/IEC 15408 включает в себя потребителей, разработчиков и оценщиков безопасных ИТ-систем и продуктов. Дополнительная информация о потенциальных пользователях ISO/IEC 15408 и использовании ISO/IEC 15408 группами, которые включают в себя потенциальных пользователей, представлена в Разделе 5, ISO/IEC 15408-1. Эти группы могут использовать данную часть ISO/IEC 15408 следующим образом:

а) пользователи, которые используют эту часть ISO/IEC 15408 при выборе компонентов для выражения уверенности требования для удовлетворения целей безопасности, выраженных в ПП или СТ, определения требуемых уровней обеспечения безопасности ОО.

б) разработчики, которые отвечают на фактические или предполагаемые требования безопасности потребителей при построении ОО, должны ссылаться на эту часть ISO/IEC 15408 при интерпретации заявлений о требованиях к определению подходов к оценке достоверности ОО.

с) оценщики, которые используют требования к достоверности, определенные в этой части ISO/IEC 15408, в качестве обязательного утверждения критериев оценки при определении гарантий ОО и при оценке ПП и СЦ.