

**Маалымат технологияласы
КООПСУЗДУКТУ КАМСЫЗ КЫЛУУНУН МЕТОДДОРУ
ЖАНА КАРАЖАТТАРЫ МААЛЫМАТТЫК
ТЕХНОЛОГИЯЛАРДЫН КООПСУЗДУГУН БААЛОО
КРИТЕРИЙЛЕРИ**

2-бөлүк

Коопсуздуктун функционалдык талаптары

**Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ
БЕЗОПАСНОСТИ КРИТЕРИИ ОЦЕНКИ
БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ**

Часть 2

Функциональные требования безопасности

(ISO/IEC 15408-1:2005, 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 Государственного комитета 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 15408-2:2005, Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 2 Функциональные требования безопасности

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 15408-2-2008

© 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, определения, обозначения и сокращения	1
4	Краткий обзор	1
4.1	Структура данной части ИСО/МЭК 15408	1
5	Парадигма функциональных требований	2
6	Функциональные компоненты безопасности	6
6.1	Краткий обзор	6
6.2	Каталог компонентов	10
7	Класс FAU. Аудит безопасности	11
7.1	Автоматическая реакция аудита безопасности (FAU_ARP)	11
7.2	Генерация данных аудита безопасности (FAU_GEN)	12
7.3	Анализ аудита безопасности (FAU_SAA)	13
7.4	Просмотр аудита безопасности (FAU_SAR)	15
7.5	Выбор событий аудита безопасности (FAU_SEL)	16
7.6	Хранение данных аудита безопасности (FAU_STG)	17
8	Класс FCO. Связь	18
8.1	Неотказуемость отправления (FCO_NRO)	18
8.2	Неотказуемость получения (FCO_NRR)	20
9	Класс FCS. Криптографическая поддержка	21
9.1	Управление криптографическими ключами (FCS_CKM)	21
9.2	Криптографические операции (FCS_COP)	23
10	Класс FDP. Защита данных пользователя	23
10.1	Политика управления доступом (FDP_ACC)	25
10.2	Функции управления доступом (FDP_ACF)	26
10.3	Аутентификация данных (FDP_DAU)	27
10.4	Экспорт данных за пределы действия ФБО (FDP_ETC)	28
10.5	Политика управления информационными потоками (FDP_IFC)	29
10.6	Функции управления информационными потоками (FDP_IFF)	30
10.7	Импорт данных из-за пределов действия ФБО (FDP_ITC)	33
10.8	Передача в пределах ОО (FDP_ITT)	35
10.9	Защита остаточной информации (FDP_RIP)	36
10.10	Откат (FDP_ROL)	37
10.11	Целостность хранимых данных (FDP_SDI)	38
10.12	Защита конфиденциальности данных пользователя при передаче между ФБО (FDP_UCT)	39
10.13	Защита целостности данных пользователя при передаче между ФБО (FDP_UIT)	40
11	Класс FIA. Идентификация и аутентификация	41
11.1	Отказы аутентификации (FIA_AFL)	42
11.2	Определение атрибутов пользователя (FIA_ATD)	43
11.3	Спецификация секретов (FIA_SOS)	43
11.4	Аутентификация пользователя (FIA_UAU)	44
11.5	Идентификация пользователя (FIA_UID)	47
11.6	Связывание пользователь-субъект (FIA_USB)	48
12	Класс FMT. Управление безопасностью	48
12.1	Управление отдельными функциями ФБО (FMT_MOF)	49
12.2	Управление атрибутами безопасности (FMT_MSA)	50
12.3	Управление данными ФБО (FMT_MTD)	51
12.4	Отмена (FMT_REV)	52
12.5	Срок действия атрибута безопасности (FMT_SAE)	53
12.6	Спецификация функций управления (FMT_SMF)	54
12.7	Роли управления безопасностью (FMT_SMR)	54
13	Класс FPR. Приватность	56
13.1	Анонимность (FPR_ANO)	56
13.2	Псевдонимность (FPR_PSE)	57
13.3	Невозможность ассоциации (FPR_UNL)	58

14	Класс FPT. Защита ФБО	60
14.1	Тестирование базовой абстрактной машины (FPT_AMT)	62
14.2	Безопасность при сбое (FPT_FLS)	62
14.3	Доступность экспортируемых данных ФБО (FPT_ITA)	63
14.4	Конфиденциальность экспортируемых данных ФБО (FPT_ITC)	63
14.5	Целостность экспортируемых данных ФБО (FPT_ITI)	64
14.6	Передача данных ФБО в пределах ОО (FPT_ITT)	65
14.7	Физическая защита ФБО (FPT_PHP)	66
14.8	Надежное восстановление (FPT_RCV)	68
14.9	Обнаружение повторного использования (FPT_RPL)	69
14.10	Посредничество при обращениях (FPT_RVM)	70
14.11	Разделение домена (FPT_SEP)	71
14.12	Протокол синхронизации состояний (FPT_SSP)	72
14.13	Метки времени (FPT_STM)	73
14.14	Согласованность данных ФБО между ФБО (FPT_TDC)	73
14.15	Согласованность данных ФБО при дублировании в пределах ОО (FPT_TRC)	74
14.16	Самотестирование ФБО (FPT_TST)	74
15	Класс FRU. Использование ресурсов	75
15.1	Отказоустойчивость (FRU_FLT)	76
15.2	Приоритет обслуживания (FRU_PRS)	76
15.3	Распределение ресурсов (FRU_RSA)	77
16	Класс FTA. Доступ к ОО	78
16.1	Ограничение области выбираемых атрибутов (FTA_LSA)	79
16.2	Ограничение на параллельные сеансы (FTA_MCS)	79
16.3	Блокирование сеанса (FTA_SSL)	80
16.4	Предупреждения перед предоставлением доступа к ОО (FTA_TAB)	81
16.5	История доступа к ОО (FTA_TAH)	82
16.6	Открытие сеанса с ОО (FTA_TSE)	82
17	Класс FTP. Доверенный маршрут/канал	83
17.1	Доверенный канал передачи между ФБО (FTP_ITC)	83
17.2	Доверенный маршрут (FTP_TRP)	84
	Приложение А (обязательное) Замечания по применению функциональных требований безопасности	86
	А.1 Структура замечаний	86
	А.2 Таблицы зависимостей	87
	Приложение В (обязательное) Функциональные классы, семейства и компоненты	92
	Приложение С (обязательное) Аудит безопасности (FAU)	93
	С.1 Требования аудита в распределенной среде	93
	С.2 Автоматическая реакция аудита безопасности (FAU_ARP)	93
	С.3 Генерация данных аудита безопасности (FAU_GEN)	93
	С.4 Анализ аудита безопасности (FAU_SAA)	96
	С.5 Просмотр аудита безопасности (FAU_SAR)	98
	С.6 Выбор событий аудита безопасности (FAU_SEL)	99
	С.7 Хранение данных аудита безопасности (FAU_STG)	100
	Приложение D (обязательное) Связь (FCO)	102
	D.1 Неотказуемость отправления (FCO_NRO)	102
	D.2 Неотказуемость получения (FCO_NRR)	103
	Приложение E (обязательное) Криптографическая поддержка (FCS)	105
	E.1 Управление криптографическими ключами (FCS_CKM)	105
	E.2 Криптографические операции (FCS_COP)	107
	Приложение F (обязательное) Защита данных пользователя (FDP)	108
	F.1 Политика управления доступом (FDP_ACC)	109
	F.2 Функции управления доступом (FDP_ACF)	111
	F.3 Аутентификация данных (FDP_DAU)	113
	F.4 Экспорт данных за пределы действия ФБО (FDP_ETC)	113
	F.5 Политика управления информационными потоками (FDP_IFC)	114
	F.6 Функции управления информационными потоками (FDP_IFF)	115
	F.7 Импорт данных из-за пределов действия ФБО (FDP_ITC)	118
	F.8 Передача в пределах ОО (FDP_ITT)	120