

Стандарты безопасности информационных технологий

В современном мире, где киберугрозы становятся всё более изощренными, обеспечение безопасности информационных систем является первостепенной задачей. Стандарты безопасности информационных технологий играют ключевую роль в защите данных, предотвращении кибератак и обеспечении доверия к информационным системам.

Морозова Камилла 21П-1

Введение: роль стандартов в области ИБ

Необходимость стандартизации

Стандарты устанавливают единые требования к процессам, технологиям и продуктам в области информационной безопасности. Это позволяет обеспечить совместимость и взаимодействие между различными системами и организациями.



Преимущества стандартов

Стандарты обеспечивают:

- Согласованность
- Снижение рисков
- Повышение эффективности
- Улучшение взаимодействия
- Увеличение доверия

"Оранжевая книга" - документ основного руководства безопасности ИС:

1 Происхождение

Разработана
Министерством обороны
США в 1985 году для
классификации и оценки
безопасности
операционных систем.

2 Цели

Обеспечение
конфиденциальности,
целостности и доступности
информации,
обрабатываемой на
защищаемых компьютерах.

3 Содержание

Определяет уровни безопасности (D, C, B, A), описывает
требования к архитектуре, реализации и тестированию
операционных систем.



Описание уровней

- **D (Minimal Protection):** Системы не имеют значительных мер безопасности. Необходимо минимальное управление доступом.

- **C1 (Discretionary Security Protection):** Системы обеспечивают базовые механизмы контроля доступа на основе прав пользователей.

- **C2 (Controlled Access Protection):** Уровень C2 включает более строгие меры контроля доступа, а также ведение журналов аудита.

- **B1 (Structured Protection):** Системы требуют четкой структуры управления доступом и выполнения строгих процедур по контролю безопасности.

- **B2 (Security Domains):** Системы должны иметь четко определенные домены безопасности с более высокими требованиями к архитектуре и управлению.

- **B3 (Security Domains with Formal Methods):** Наивысший уровень, требующий формальных методов в проектировании системы и обеспечении безопасности.

- **A1 (Verified Design):** Системы, прошедшие полное формальное доказательство безопасности.

ISO/IEC 15408

Также известный как Common Criteria (CC), является международным стандартом для оценки безопасности информационных технологий. Он был разработан для обеспечения совместимости и сопоставимости результатов оценок безопасности различных продуктов и систем.

Стандарт включает три основные части:

- **Часть 1:** Общие принципы.
- **Часть 2:** Классификация требований к безопасности.
- **Часть 3:** Методология оценки.

Преимущества

Обеспечивает независимую и объективную оценку безопасности, что повышает уровень доверия к продуктам и системам.

ISO/IEC 15408

Common Criteria предлагает семь уровней оценки (EAL - Evaluation Assurance Level), от EAL1 (базовый уровень) до EAL7 (наивысший уровень). Каждый уровень представляет собой набор требований к процессу разработки, тестированию и документированию продукта.

ISO/IEC 15408

✕

поиск

нейро

картинки

видео

карты

товары

переводчик

все

Скачать ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная...

docs.guap.ru › regdocs\stands\gost-r-iso-mec_15408-...

Часть 1. Введение и общая модель» (ISO/IEC 15408-1:2009 «Information technology — Security techniques — Evaluation criteria for IT security — Part 1...

PDF

Посмотреть

Содержание

1	Область применения	1
2	Нормативные ссылки	1
3	Термины и определения	2
3.1	Термины и определения, общие для всех частей ИСО/МЭК 15408	2
3.2	Термины и определения, относящиеся к классу ADV	6
3.3	Термины и определения, относящиеся к классу AGD	9
3.4	Термины и определения, относящиеся к классу ALC	9
3.5	Термины и определения, относящиеся к классу AVA	13
3.6	Термины и определения, относящиеся к классу ACO	13
4	Сокращения	13
5	Краткий обзор	14
5.1	Общая информация	14
5.2	Объект оценки	14
5.3	Пользователи ИСО/МЭК 15408	15
5.4	Части ИСО/МЭК 15408	16
5.5	Контекст оценки	17
6	Общая модель	17
6.1	Введение к общей модели	17
6.2	Активы и контрмеры	18
6.3	Оценка	21
7	Доработка требований безопасности для конкретного применения	21
7.1	Операции	21
7.2	Зависимости между компонентами	23
7.3	Расширенные компоненты	24
8	Профили защиты и пакеты	24
8.1	Введение	24
8.2	Пакеты	24
8.3	Профили защиты	25
8.4	Использование ПЗ и пакетов	26
8.5	Многократное использование профилей защиты	26
9	Результаты оценки	27
9.1	Введение	27
9.2	Результаты оценки ПЗ	28
9.3	Результаты оценки ЗБ/ОО	28
9.4	Утверждение о соответствии	28
9.5	Использование результатов оценки ЗБ/ОО	29
	Приложение А (справочное) Спецификация заданий по безопасности	30
	Приложение В (справочное) Спецификация профилей защиты	41
	Приложение С (справочное) Руководство по выполнению операций	45
	Приложение D (справочное) Соответствие ПЗ	47
	Приложение ДА (справочное) Сведения о соответствии ссылочных м...	48
	Библиография	49



Другие ключевые стандарты и спецификации: ФСТЭК, ГОСТ Р ИСО/МЭК 27000 и др.



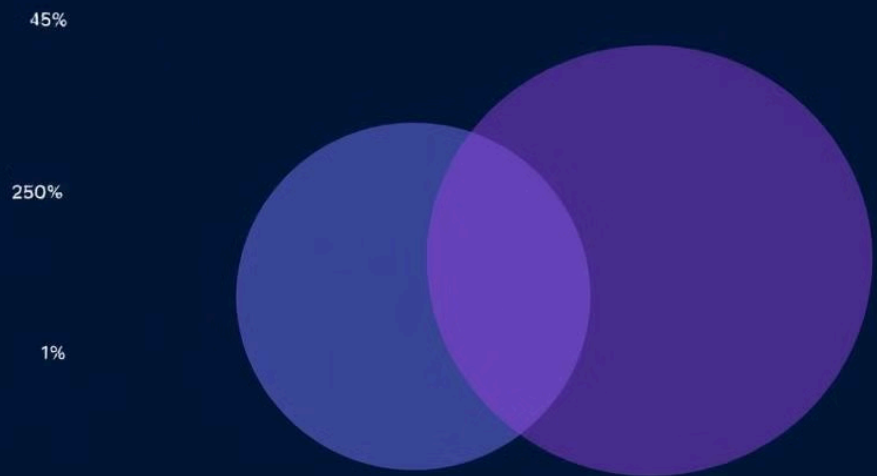
ФСТЭК

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) разрабатывает и утверждает стандарты безопасности для государственных информационных систем.



ГОСТ Р ИСО/МЭК 27000

Серия стандартов, устанавливающих требования к системам менеджмента информационной безопасности (ИБ).



Сравнение и взаимосвязь различных стандартов

- 1 Оранжевая книга фокусируется на защите операционных систем и конфиденциальности информации.
- 2 ИСО/МЭК 15408 имеет более широкий охват, включая оценку безопасности различных продуктов и систем.
- 3 ФСТЭК разрабатывает стандарты для государственных систем, а ГОСТ Р ИСО/МЭК 27000 устанавливает требования к системам менеджмента ИБ.

Практика внедрения стандартов безопасности: проблемы и решения

1

Сложность стандартов, требующая глубокой экспертизы.

2

Необходимость инвестиций в обучение, инструменты и ресурсы.

3

Совместимость с существующими системами и процессами.

4

Проведение регулярных аудитов и проверок соответствия.

Ключевые выводы и рекомендации

