Учреждение образования

Белорусский государственный технологический университет

Кафедра полиграфического оборудования и

системы обработки информации

**Отчет по лабораторной работе**

«Стандарты безопасности»

по дисциплине «Стандартизация и сертификация

информационных систем и технологий»

Выполнил студент

ФИТ ПОИТ 5-2 Валдайцев А. Д.

Проверил

кандидат технических наук

Сулим П.Е.

Отчет по лабораторной работе

защищен с отметкой баллов

Минск 2024

Найти отечественные стандарты в области безопасности информационных систем. Провести их сравнительный анализ.

Приведите выводы по содержанию работы.

## Стандарты безопасности

В сфере информационной безопасности главным зарубежным стандартом является **ISO/IEC 27001**, который был разработан совместно Международной организацией по стандартизации и Международной электротехнической комиссией. Он определяет основные понятия информационной безопасности, такие как конфиденциальность, целостность и доступность информации. Кроме того, этот стандарт включает и другие свойства, например, подлинность, невозможность отказа от авторства и достоверность.

ISO/IEC 27001 основан на британском стандарте **BS 7799-2** и описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) в организации. Эти механизмы определены на основе лучших примеров мирового опыта (best practices) в данной области.

В США существует **Радужная серия стандартов** информационной безопасности, разработанная и опубликованная в период с 1980 по 1990 гг. Эти стандарты были изначально опубликованы Министерством обороны США и затем получили широкое распространение через Центр национальной компьютерной безопасности США. Например, стандарт "Критерии определения безопасности компьютерных систем" неофициально известен как **Оранжевая Книга**. Его аналогом является международный стандарт ISO/IEC 15408, опубликованный в 2005 году. В отличие от распространенного заблуждения, ISO/IEC 15408 не заменил Оранжевую Книгу, так как они имеют разную юрисдикцию. Оранжевая Книга используется исключительно Министерством обороны США, в то время как ISO/IEC 15408 был ратифицирован множеством стран, включая Беларусь.

Одним из главных международных стандартов информационной безопасности является ISO/IEC 27001. Этот стандарт определяет требования к системе управления информационной безопасностью (СУИБ) в организации. ISO/IEC 27001 устанавливает процессный подход к управлению информационной безопасностью и включает в себя такие этапы, как оценка рисков, выбор и реализация контрмер, а также мониторинг и улучшение системы. Сертификация по ISO/IEC 27001 подтверждает соответствие организации международным стандартам в области информационной безопасности.

Еще одним важным международным стандартом является **NIST SP 800-53**, разработанный Национальным институтом стандартов и технологий (NIST) в США. Этот стандарт определяет набор контрольных мер, которые должны быть реализованы для обеспечения безопасности информационных систем в федеральных агентствах США. NIST SP 800-53 широко используется также в коммерческом секторе и за его пределами в качестве основы для разработки политик и практик информационной безопасности.

В Европейском союзе действует Общий регламент по защите данных (**GDPR**), который устанавливает правила по обработке персональных данных и требования к их защите. GDPR применим ко всем организациям, обрабатывающим персональные данные граждан ЕС, независимо от их местоположения. Регламент включает требования к безопасности обработки данных и предусматривает штрафы за нарушение правил.

В Беларуси стандарты информационной безопасности распространяются в виде документов СТБ. Например, СТБ 34.101.**73**-2017 устанавливает общие требования к программным и программно-аппаратным средствам межсетевого экранирования. Этот стандарт применяется при сертификационных испытаниях и государственной экспертизе для оценки соответствия требованиям.

Другой стандарт, СТБ 34.101.**74**-2017, устанавливает общие требования к программным и программно-аппаратным системам сбора и обработки данных событий информационной безопасности. Этот стандарт также применяется при сертификационных испытаниях и государственной экспертизе.

Стандарт СТБ 34.101.**78**-2019 определяет профиль инфраструктуры открытых ключей, рекомендуемый для использования в Беларуси. Он устанавливает стороны инфраструктуры, процессы их взаимодействия, протоколы взаимодействия и форматы объектов инфраструктуры.

Кроме того, существуют и другие национальные и отраслевые стандарты информационной безопасности, которые могут быть применимы в различных странах и отраслях. Эти стандарты могут определять конкретные требования и рекомендации по защите информации в соответствующих контекстах.

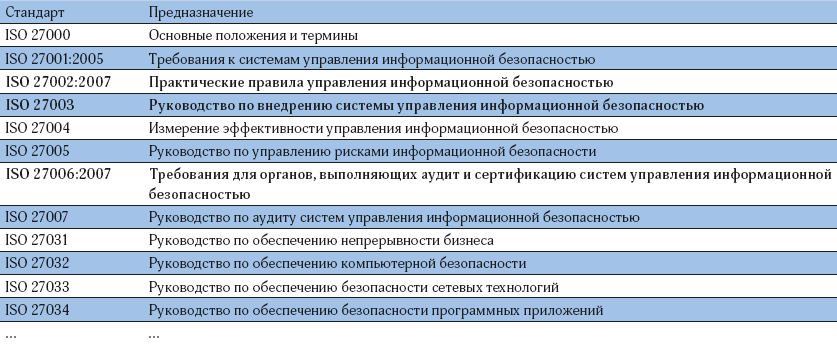


Рисунок 1.1 – Стандарты ISO 27000

## Источники

[Википедия. ISO/IEC 27001](https://ru.wikipedia.org/wiki/ISO/IEC_27001)

[BS 7799, ISO 27001, ISO 27002, ISO 27005, ГОСТ 17799 и ГОСТ 27001 (npo-echelon.ru)](https://npo-echelon.ru/news/562/)

["Оранжевая книга" (htmlweb.ru)](https://protect.htmlweb.ru/orange1.htm)

## Выводы

В ходе исследования были рассмотрены различные стандарты информационной безопасности, включая международные (например, ISO/IEC 27001 и NIST SP 800-53) и национальные (например, СТБ в Беларуси).

Национальные и отраслевые стандарты информационной безопасности также могут иметь значение в определенных контекстах. Они могут определять специфические требования и рекомендации, соответствующие особенностям конкретных стран и отраслей.

Изучение стандартов информационной безопасности является важным для организаций, стремящихся обеспечить защиту информации и соответствовать международным и национальным требованиям. Эти стандарты предоставляют ценные руководства и основы для разработки и внедрения мер безопасности информации.