## Учреждение образования

## Белорусский государственный технологический университет

Кафедра полиграфического оборудования и

системы обработки информации

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №10**

по дисциплине «Стандартизация и сертификация

информационных систем и технологий»

Тема

«Стандарты безопасности»

Выполнил студент:

Трошко Валерия

ф-та ИТ 4 к. 5 гр.

Проверил

кандидат технических наук

Сулим П.Е.

Отчет по лабораторной работе

защищен с отметкой баллов

Минск 2023

СТАНДАРТЫ БЕЗОПАСНОСТИ

Главным зарубежным стандартом в сфере информационной безопасности является ISO/IEC 27001, разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией.

Основные понятия ISO/IEC 27001.

Информационная безопасность — сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность.

Конфиденциальность — обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи).

Целостность — обеспечение точности и полноты информации, а также методов её обработки.

Доступность — обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).

Стандарт основан на британском стандарте BS 7799-2. Этот документ описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области.

В США существует Радужная серия — серия стандартов информационной безопасности, разработанная и опубликованная в США в период с 1980 по 1990 гг. Изначально книги были опубликованы Министерством обороны США, а затем в Центре национальной компьютерной безопасности США.

Например, стандарт «Критерии определения безопасности компьютерных систем» неофициально называется Оранжевой Книгой. Аналогом Оранжевой книги является международный стандарт ISO/IEC 15408, опубликованный в 2005 году. Это более универсальный и совершенный стандарт, но вопреки распространённому заблуждению, он не заменял собой Оранжевую книгу в силу разной юрисдикции документов — Оранжевая книга используется исключительно Министерством Обороны США, в то время как ISO/IEC 15408 ратифицировали множество стран, включая Беларусь.

В Беларуси стандарты информационной безопасности распространяются как документы СТБ.

СТБ 34.101.73-2017, BY.

Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования. — Введ. 01.01.18. — Минск, 2017. — ІІ, 7 с. — Попр. (ИУ ТНПА № 9-2017). — Введен впервые.

Стандарт распространяется на программные и программно-аппаратные средства межсетевого экранирования. Стандарт устанавливает общие требования к межсетевым экранам (МЭ). Стандарт применяется при сертификационных испытаниях, проведении испытаний в рамках государственной экспертизы для оценки соответствия требованиям стандарта, а также может быть применен при разработке МЭ.

СТБ 34.101.74-2017, BY.

Информационные технологии. Система сбора и обработки данных событий информационной безопасности. Общие требования. — Введ. 01.10.17. — Минск, 2017. — II, 6 с. — Введен впервые.

Стандарт распространяется на программные и программно-аппаратные системы сбора и обработки данных событий информационной безопасности. Стандарт устанавливает классификацию и общие требования к системам сбора и обработки данных событий информационной безопасности. Стандарт применяется при сертификационных испытаниях, проведении испытаний в рамках государственной экспертизы для оценки соответствия требованиям стандарта, а также может быть применен при разработке систем сбора и обработки данных событий информационной безопасности.

СТБ 34.101.78-2019, BY.

Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей. — Введ. 01.10.19. — Минск, 2019. — IV, 43, [1] с. : ил., табл. — Введен впервые. — Попр. (ИУ ТНПА № 9-2020).

Стандарт устанавливает профиль инфраструктуры открытых ключей, рекомендуемый для использования в Республике Беларусь. В стандарте определяются стороны инфраструктуры, процессы их взаимодействия, протоколы взаимодействия, уточняются форматы объектов инфраструктуры. Стандарт применяется при разработке средств криптографической защиты информации и информационных систем, в которых используются открытые ключи.

СТБ ISO/IEC 27006-2018, BY.

Информационные технологии. Методы обеспечения безопасности. Требования к органам, проводящим аудит и сертификацию систем менеджмента информационной безопасности. — Взамен СТБ ISO/IEC 27006-2014; введ. 01.05.18. — Минск, 2018. — V, 35 с. — Попр. (ИУ ТНПА № 4-2018).

Стандарт конкретизирует требования и предоставляет руководство для органов, проводящих аудит и сертификацию системы менеджмента информационной безопасности (СМИБ), в дополнение к требованиям, содержащимся в ISO/IEC 17021-1 и ISO/IEC 27001. Стандарт, в первую очередь, предназначен для поддержки аккредитованных органов по сертификации, проводящих сертификацию СМИБ. Любому органу, проводящему сертификацию СМИБ, необходимо продемонстрировать соответствие требованиям, содержащимся в стандарте, с точки зрения компетентности и надежности, а содержащееся в стандарте руководство, предоставляет дополнительную интерпретацию этих требований для любого органа, проводящего сертификацию СМИБ. Стандарт может использоваться в качестве основополагающего документа при аккредитации, оценке равной стороной или других процессов аудита.

**Источники**

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

**Вывод**

В ходе выполнения лабораторной работы ознакомился с зарубежными и отечественными стандартами.