НАЦИОНАЛЬНЫЙ СТАНДАРТ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Маалыматтык технологиялар
Коопсуздукту камсыз кылуу методдору
МААЛЫМАТТЫК КООПСУЗДУГУНУН МЕНЕДЖМЕНТ СИСТЕМАСЫ

Информационные технологии
Методы обеспечения безопасности
СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(СТБ ISO/IEC 27001-2016, IDT)

Издание официальное

ЦСМ

Бишкек

Предисловие

Цели, принципы и основные положения стандартизации в Кыргызской Республике установлены Законом Кыргызской Республики «Об основах технического регулирования в Кыргызской Республике» и КМС 1.0

Сведения о стандарте

1 ПОДГОТОВЛЕН И ВНЕСЕН Центром по стандартизации и метрологии при Министерстве экономики Кыргызской Республики

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Центра по стандартизации и метрологии при Министерстве экономики Кыргызской Республики от 15 января 2020г. №2–СТ

3 Настоящий стандарт идентичен СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности

4 ВЗАМЕН ГОСТ Р ИСО/МЭК 27001-2006

Содержание

0 Введение

0.1 Общие положения

Настоящий стандарт подготовлен для реализации требований по созданию, внедрению, поддержанию и постоянному улучшению системы менеджмента информационной безопасности. Внедрение системы менеджмента информационной безопасности является стратегическим решением для организации. Разработка и внедрение системы менеджмента информационной безопасности организации зависит от потребностей и целей организации, требований по безопасности, существующих процессов организации, размера и структуры организации. Предполагается, что все эти факторы влияния с течением времени меняются.

Система менеджмента информационной безопасности обеспечивает конфиденциальность, целостность и доступность информации за счет применения процесса менеджмента рисков и обеспечивает заинтересованным сторонам уверенность в том, что риски адекватно управляются.

Важно, чтобы система менеджмента информационной безопасности являлась частью процессов организации и была интегрирована с процессами организации и общей структурой менеджмента, а требования информационной безопасности были учтены при разработке процессов, информационных систем и элементов управления. Предполагается, что масштаб внедрения системы менеджмента информационной безопасности будет соответствовать потребностям организации.

Настоящий стандарт может использоваться внутренними и внешними сторонами для оценки способности организации выполнять требования по обеспечению информационной безопасности, установленные организацией.

Порядок представления требований в настоящем стандарте не подразумевает их важность и необходимость реализации в таком порядке. Элементы стандарта нумеруются только в справочных целях.

ISO/IEC 27000 представляет собой общие положения и словарь для систем менеджмента информационной безопасности, дает ссылки на соответствующие термины и определения, данные в серии стандартов на системы менеджмента информационной безопасности (включая ISO/IEC 27003 [1], ISO/IEC 27004 [2] и ISO/IEC 27005 [3]).

0.2 Взаимосвязь с другими стандартами на системы менеджмента

Настоящий стандарт применяет высокоуровневую структуру, идентичные наименования разделов, идентичный текст, общие термины и базовые определения, установленные в Директиве ISO/IEC (часть 1, консолидированное дополнение ISO, приложение SL) [4], и, следовательно, поддерживает совместимость с другими стандартами на системы менеджмента, которые соответствуют приложению SL.

Общий подход, определенный в приложении SL, будет полезен для тех организаций, которые предпочитают управлять единой системой менеджмента, отвечающей требованиям двух или более стандартов на системы менеджмента.