Стандартизация информационной безопасности в ТК27 ISO/IEC JTC1

Москва, 17 апреля 2019

Дмитрий Ларюшин, к.ф.-м.н

Структура Подкомитета ТК27 по Управлению ИБ

Широкий круг вопросов информационной безопасности распределен между 5 рабочими группами:

- РГ1 разрабатывает стандарты и методические рекомендации в области Систем Управления ИБ (ISMS);
- РГ2 – Криптография и Механизмы Безопасности для сферы информационных технологий;
- РГ3 – Оценка Критериев Безопасности, разработка стандартов и сертификационных требований для информационных систем и компонентов;
- РГ4 – Контроль Безопасности и Сервисов, сопутствующие стандарты для обеспечения мер защиты информации, определенных ISO/IEC 27001, 27002;
- РГ5 - Управление Индентификацией, разработка стандартов для управления идентификационными данными, биометрией и защиты персональных данных.

Организация работ Подкомитета

Рабочие группы руководствуются принципами и методическими указаниями, принятыми в ISO и IEC. В частности, они разрабатывают дорожные карты и проводят ревизию каждые 6 месяцев. Цели разработки ДК:

- Точная идентификация стандартов, относящихся к сфере ответственности РГ, как уже принятых, так и подготовленных к принятию стандартизующими организациями;
- Определение и описание логических связей между стандартами, разработанными РГ;
- Формулирование ключевых принципов для координации работ по разработке стандартов в целях исключения дублирования;
- Определение и уточнение расписания работ по разработке стандартов в сфере ответственности РГ;
- Обеспечение эффективной координации с работами других технических комитетов ISO/IEC

Типы стандартов РГ1

Дорожная карта РГ1 придерживается 4-уровневой модели для разработки стандартов:

- Тип A – Терминологические стандарты определяют базовую информацию и терминологию, относящуюся ко всем стандартам РГ;
- Тип B – Стандарты, определяющие требования к ИБ, например, стандарты:
  - B1: ISO/IEC 27001:2005. Information security management systems — Requirements
  - B2: ISO/IEC 27006:2007. Requirements for bodies providing audit and certification of information security management systems.
- Тип C – Стандарты, которые включают определенные методические указания, в частности, (C1) по удовлетворению требованиям к ISMS;
- Тип D – Смежные стандарты


intel
experience
what's inside™