1. ГОСТ Р ИСО/МЭК 27001-2021

Стандарт про то, как в компании организовать управление информационной безопасностью: кто за что отвечает, как оценивать риски, какие правила вводить, как проверять, что всё работает, и как улучшать систему со временем. СУИБ (ISMS) это система управления информационной безопасностью.

2. ГОСТ Р ИСО/МЭК 27002-2021

Это справочник мер безопасности: что можно делать для защиты (например, управление доступами, резервное копирование, защита рабочих мест и т. п.). Помогает выбрать подходящие меры под риски и требования 27001.

3. ГОСТ Р ИСО/МЭК 20000-1-2021

Стандарт про управление ИТ-услугами (например, поддержка пользователей, работа сервис-деска, обработка инцидентов, изменения, качество сервиса). Показывает, как построить систему, чтобы ИТ-услуги были стабильными и улучшались.

4. ГОСТ Р ИСО/МЭК 12207-2010

Описывает, какие работы бывают в жизненном цикле ПО: от идеи и требований до разработки, тестирования, внедрения, поддержки и завершения использования.

5. ГОСТ Р ИСО/МЭК 25010-2015

Стандарт про качество программ и систем: какие свойства качества обычно оценивают (надёжность, безопасность, удобство, производительность, сопровождаемость). Полезен, чтобы формулировать требования к качеству и сравнивать продукты по понятным критериям.

6. ГОСТ Р ИСО/МЭК 38500-2017

Про управление ИТ на уровне руководства: как принимать решения об ИТ так, чтобы они были полезны организации, соответствовали правилам и реально контролировались.

7. ГОСТ Р 57580.1-2017

Стандарт для финансовых организаций (банки и т. п.): задаёт уровни защиты и минимальный набор мер, который нужен, чтобы защищать информацию и финансовые операции. Используется как основа при построении защиты и проверках соответствия требованиям регулятора.

8. ГОСТ Р 56939-2016

Стандарт про безопасную разработку ПО: какие работы и документы должны быть, чтобы программа получалась более защищённой (учёт уязвимостей, исправления, процессы разработки и поддержки). Secure SDLC — это безопасный жизненный цикл разработки: когда безопасность учитывают на всех этапах разработки.

9. ГОСТ Р 34.10-2012

Стандарт про то, как создаётся и проверяется электронная цифровая подпись (ЭЦП) по отечественным криптоалгоритмам (способы, по которым компьютер шифрует**,** проверяет подпись). Используется там, где нужна юридически значимая подпись и защита документов от подмены.

10. ГОСТ Р 34.11-2012

Стандарт про криптографическую хэш-функцию — способ получить цифровой отпечаток данных. Нужен для проверки целостности (чтобы понять, изменился файл или нет) и применяется внутри многих криптосхем.