

Характеристики стандартов информационной безопасности

Лекция 1

Стандарты информационной безопасности

Обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам.

Функции стандартов ИБ

1. Выработка понятийного аппарата и терминологии в области информационной безопасности
2. Формирование шкалы измерений уровня информационной безопасности
3. Согласованная оценка продуктов, обеспечивающих информационную безопасность
4. Повышение технической и информационной совместимости продуктов, обеспечивающих ИБ
5. Накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории – производителям средств ИБ, экспертам, ИТ-директорам, администраторам и пользователям информационных систем
6. Функция нормотворчества – придание некоторым стандартам юридической силы и установление требования их обязательного выполнения.

Задачи стандартов ИБ

1. Определение целей обеспечения информационной безопасности компьютерных систем;
2. Создание эффективной системы управления информационной безопасностью;
3. Расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям;
4. Применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
5. Использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения разработчиков информационных систем, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Цели стандартов ИБ

1. Заранее намеченный результат защиты информации.

Основные области стандартизации ИБ

1. Аудит информационной безопасности
2. Модели информационной безопасности
3. Методы и механизмы обеспечения информационной безопасности
4. Криптография
5. Безопасность межсетевых взаимодействий
6. Управление информационной безопасностью.

Классификация стандартов ИБ

По области регламентации

- оценочные стандарты, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности (направлены больше на концепции и аспекты ИБ)
- спецификации (направлены больше на реализацию концепций ИБ и использование средств и методов защиты)

По территории распространения

- международные - ISO, IEC, Common Criteria for IT Security
- национальные - BSI, NIST, BS, ГОСТ Р ИСО/МЭК и др.

По обязательности выполнения

- обязательные
- рекомендуемые

По доступности

- общедоступные
- распространяемые по лицензии