Практическое занятие №1 Общие требования безопасности

Подготовил: Ковалев М.А.

Цель презентации:

- Рассмотреть общие требования безопасности

Задачи:

- Разобрать стандарты и спецификации в области информационной безопасности.
- Определить термин доверенная система
- Указать классификация по требованиям безопасности.

Стандарты и спецификации в области информационной безопасности.

Специалистам в области *информационной безопасности* (ИБ) сегодня почти невозможно обойтись без знаний соответствующих*стандартов* и *спецификаций*. На то имеется несколько причин.

стандарты и *спецификации* - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами.

стандарты и *спецификации* - основное средство обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в *Internet*-сообществе это средство действительно работает, и весьма эффективно.

Стандарт и спецификация

- ***стандарт*** - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. *Стандарт* также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;

- ***стандартизация*** - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Стандартизация осуществляется в соответствии с принципами:

- добровольного применения стандартов;
- максимального учета при разработке стандартов законных интересов заинтересованных лиц;
- применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям либо Российская Федерация в соответствии с установленными процедурами выступала против принятия международного стандарта или отдельного его положения;
- недопустимости создания препятствий производству и обращению продукции, выполнению работ и оказанию услуг в большей степени, чем это минимально необходимо для выполнения целей, указанных в статье 11 настоящего Федерального закона;
- недопустимости установления таких стандартов, которые противоречат техническим регламентам;
- обеспечения условий для единообразного применения стандартов.

Доверенная система

Под доверенной системой в стандарте понимается система, использующая аппаратные и программные средства для обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа.

Уровень гарантированности - мера доверия, которая может быть оказана архитектуре и реализации ИС.

Сервис безопасности

- механизм защиты перечень и содержание для общего случая которого могут быть представлены следующим образом:

идентификация/аутентификация.

Современные средства идентификации / аутентификации должны удовлетворять двум условиям:

- *быть устойчивыми к сетевым угрозам (пассивному и активному прослушиванию сети);*
- *поддерживать концепцию единого входа в сеть.*

Классификация по требованиям безопасности.

Часть 2 "Общих критериев", представляющая собой весьма обширную *библиотеку функциональных требований безопасности*, описывает 11 *классов*, 66 *семейств*, 135 *компонентов* и содержит сведения о том, какие *цели безопасности* могут быть достигнуты при современном уровне информационных технологий и каким образом.

Безопасность повторного использования

Технологии обеспечения безопасности повторного использования объектов направлены на предотвращение угроз безопасности от случайного или преднамеренного извлечения интересующей злоумышленника информации по следам предшествующей деятельности или из технологического «мусора» Данные технологии условно можно разделить на три группы:

- *изоляция процессов;*
- *очистка памяти после завершения процессов;*
- *перекрытие косвенных каналов утечки информации.*

Выводы:

- Разобрали стандарты и спецификации в области информационной безопасности.
- Определили термин доверенная система
- Указали классификация по требованиям безопасности.