ТЕМА №6. СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИБ

ВЫПОЛНИЛ КИТАЕВ Д. И. ИВТ-192

ВИДЫ СТАНДАРТОВ И СПЕЦИФИКАЦИЙ

- Оценочные стандарты – направленные на классификацию информационных систем и средств защиты по требованиям безопасности.
- Технические спецификации, регламентирующие различные аспекты реализации средств защиты

Между этими видами нормативных документов нет “Глухой стены”. Оценочные стандарты выделяют важнейшие, с точки зрения информационной безопасности, аспекты информационной системы, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

СТЕПЕНЬ ДОВЕРИЯ

Существует такое понятие как “Степень доверия”, и оно разбивается по двум основным критериям:

1. Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности.
2. Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов.

ДОВЕРЕННАЯ ВЫЧИСЛИТЕЛЬНАЯ БАЗА

Важным средством обеспечения безопасности является механизм подотчетности. Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом.

Основное назначение доверенной вычислительной базы – выполнять функции монитора обращений, т.е. контролировать допустимость выполнения субъектами определенных операций над объектами.

КАЧЕСТВО МОНИТОРА ОБРАЩЕНИЯ

Монитор обращений должен обладать тремя качествами:

- *Изолированность*. Необходимо предупредить возможность отслеживания работы монитора.
- *Полнота*. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.
- *Верифицируемость*. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования

ЭЛЕМЕНТЫ ПОЛИТИКИ БЕЗОПАСНОСТИ

Реализация монитора обращений называется ядром безопасности. Ядро безопасности – это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Политика безопасности должна обязательно включаться в себя следующие элементы:

- Произвольное управление доступом
- Безопасность повторного использования объектов
- Метки безопасности
- Принудительное управление доступом

ЭЛЕМЕНТЫ ПОЛИТИКИ БЕЗОПАСНОСТИ

- *Произвольное управление доступом* – это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит.
- *Безопасность повторного использования объектов* – важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из “мусора”.
- *Принудительное управление* доступом основано на сопоставлении метод безопасности субъекта и объекта.