ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИСПРУДЕНЦИИ ЛЕКЦИЯ №3

ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации должна основываться на следующих **основных принципах:**

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости управления и применения;
- открытости алгоритмов и механизмов защиты;
- простоты применения защитных мер и средств.

ПОНЯТИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Система защиты информации (СЗИ) –это организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) в информационной системе (ИС) для решения в ней выбранных задач защиты.

ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДЫ (СПОСОБЫ) ЗАЩИТЫ ИНФОРМАЦИИ

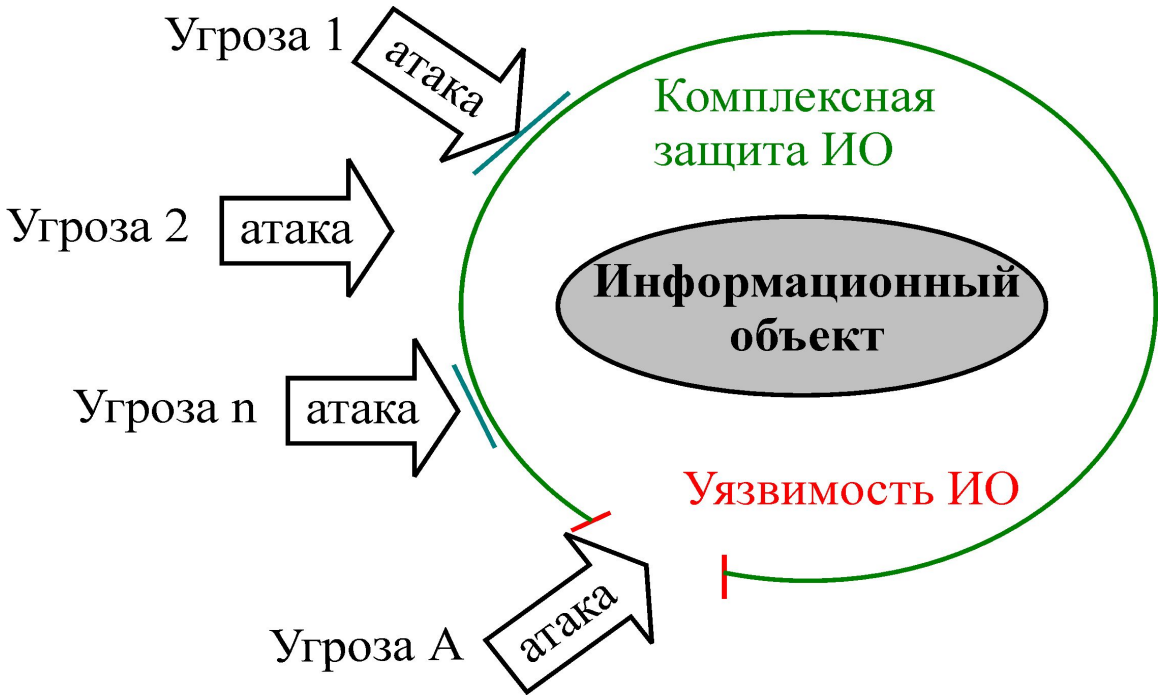
- препятствие;
- управление доступом;
- маскировка;
- регламентация;
- принуждение;
- побуждение.

КЛАССЫ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

- законодательные (правовые) СЗИ
- организационные СЗИ
- морально-этические СЗИ
- физические СЗИ
- программные СЗИ
- аппаратные СЗИ

УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- ***Угроза безопасности информации*** – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [ГОСТ Р 50922 – 2006 «Защита информации. Основные термины и определения»]
- ***Уязвимость*** – свойство объекта, делающее возможным возникновение и реализацию атаки
- ***Атака*** – действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости, попытка реализации угрозы.



ИНТЕРНЕТ-РЕСУРСЫ ОБ АКТУАЛЬНЫХ УГРОЗАХ И УЯЗВИМОСТЯХ

- Web Application Security Consortium (WASC) - международная некоммерческая организация, объединяющая экспертов-профессионалов в области безопасности веб-приложений. (WASC Threat Classification) – классификация уязвимостей и атак, которые могут причинить ущерб веб-сайту, обрабатываемой им информации или его пользователям.
- Open Web Application Security Project (OWASP) —открытый проект по безопасности веб-приложений.
- Common Vulnerabilities and Exposures (CVE) - каталог, содержащий список унфицированные стандартные названия для общеизвестных уязвимостей и обеспечивающий согласование сведений об уязвимостях, содержащихся в разных в разных базах данных.
- Банк данных угроз безопасности информации РФ (ФСТЭК России): http://bdu.fstec.ru.

ИДЕНТИФИКАЦИЯ ФАКТОРОВ В ПРОЦЕССЕ АНАЛИЗА УГРОЗ

Независимо от особенностей классификационных систем в процессе анализа угроз для каждой угрозы должны быть идентифицированы:

- возможные источники угрозы;
- уязвимости системы, позволяющие реализовать угрозу;
- способы, посредством которых может быть реализована угроза;
- объект воздействия угрозы;
- последствия для информации, ассоциированной с объектом угрозы.

КОНТРОЛЬНЫЕ ВОПРОСЫ ЛЕКЦИИ

1. Перечислите основные принципы защиты информации.
2. Дайте понятие систем защиты информации.
3. Приведите требования к системе защиты информации.
4. Опишите методы защиты информации.
5. Перечислите классы средств защиты информации.
6. Дайте определение понятиям атаки, угрозы и уязвимости информационной безопасности.
7. Приведите краткую идентификацию факторов в процессе анализа угроз.