ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИСПРУДЕНЦИИ

Пургина Марина Владимировна,
к.т.н, доцент каф.ИТ
pur-LL@yandex.ru

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

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

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

КЛАССЫ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

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

КЛАССИФИКАЦИЯ УГРОЗ

1. **По цели воздействия**: нарушение конфиденциальности, целостности, доступности).
2. **По характеру источника угрозы**: субъективные и объективные.
3. **По характеру/природе происхождения**: случайные и преднамеренные (внутренние и внешние)
4. **По характеру воздействия**: активные, пассивные.

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 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.

ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Внешние:

- политика иностранных государств; действия разведок и спецслужб;
- экспансия информационных систем в другие государства;
- действия преступных групп;
- стихийные бедствия.

Внутренние:

- противозаконная деятельность различных структур, лиц, групп в области распространения и употребления информации;
- неэффективное регулирование правовых отношений в информационной среде;
- нарушение установленных регламентом сбора, обработки и передачи информации;
- ошибки персонала и пользователей, непреднамеренные и преднамеренные ошибки разработчиков, пользователей; отставание отечественной промышленности;
- отказы и сбои технических систем;неправомерное действие государственных структур.

КОНТРОЛЬНЫЕ ВОПРОСЫ ЛЕКЦИИ

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