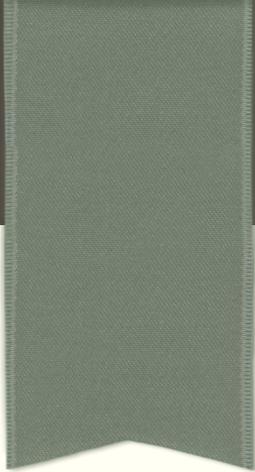


4.3 ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.





ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – СОСТОЯНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СРЕДЫ ОТ ВОЗДЕЙСТВИЯ ИСТОЧНИКОВ УГРОЗ, ОБЕСПЕЧИВАЮЩЕЕ ЕЕ ФОРМИРОВАНИЕ, ИСПОЛЬЗОВАНИЕ, РАЗВИТИЕ В ИНТЕРЕСАХ ГРАЖДАН, ОБЩЕСТВА, ГОСУДАРСТВА.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - МЕХАНИЗМ ЗАЩИТЫ, ОБЕСПЕЧИВАЮЩИЙ:

- **КОНФИДЕНЦИАЛЬНОСТЬ:** ДОСТУП К ИНФОРМАЦИИ ТОЛЬКО АВТОРИЗОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ;
- **ЦЕЛОСТНОСТЬ:** ДОСТОВЕРНОСТЬ И ПОЛНОТУ ИНФОРМАЦИИ И МЕТОДОВ ЕЕ ОБРАБОТКИ;
- **ДОСТУПНОСТЬ:** ДОСТУП К ИНФОРМАЦИИ И СВЯЗАННЫМ С НЕЙ АКТИВАМ АВТОРИЗОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ ПО МЕРЕ НЕОБХОДИМОСТИ.

Угроза информационной безопасности

- совокупность условий и факторов, создающих опасность нарушения информационной безопасности.
- Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.
- Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления, например, конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Информационные угрозы могут быть обусловлены:

естественными факторами

- стихийные бедствия — пожар, наводнение, ураган, молния и другие причины

человеческими факторами.

- угрозы, носящие случайный, неумышленный характер
- угрозы, обусловленные умышленными, преднамеренными действиями людей.

Неумышленные угрозы

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. п.);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная, порча носителей информации.

Умышленные угрозы

- Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.
- Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.
- Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы.

К основным угрозам безопасности относят:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование ресурсов;
- несанкционированный обмен информацией;
- отказ от информации;
- отказ от обслуживания

Классификация

- Устанавливается девять классов защищенности АС от НСД к информации

- Классы подразделяются на три группы:

-Третья группа(один пользователь, допущенный ко всей информации АС) содержит два класса: 3Б – КИ и 3-А – ГТ

-Вторая группа(пользователи имеют одинаковые права доступа полномочия ко всей информации АС) содержит два класса: 2Б – КИ и 2А – ГТ

-Первая группа(многопользовательская АС, в которой пользователи имеют разные права к АС) содержит пять классов защиты: 1Д, 1Г - КИ, 1В, 1Б, 1А – ГТ

Классы защиты: 3Б, 2Б, 1Д, 1Г предназначены для защиты конфиденциальной информации, классы защиты 3А, 2А, 1В, 1Б, 1А – для защиты государственной тайны

Требования к защите определяются в соответствии с руководящими документами ФСТЭК России после установления класса защищенности для АС

Литература:

- Презентация по предмету основы информационной безопасности.
- ГОСТ Р ИСО/МЭК 17799-2005 Практические правила управления информационной безопасностью
- [2.Inf.ugrozy-vred.programmykomp.prestupleniya.pdf \(unn.ru\)](#)