МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

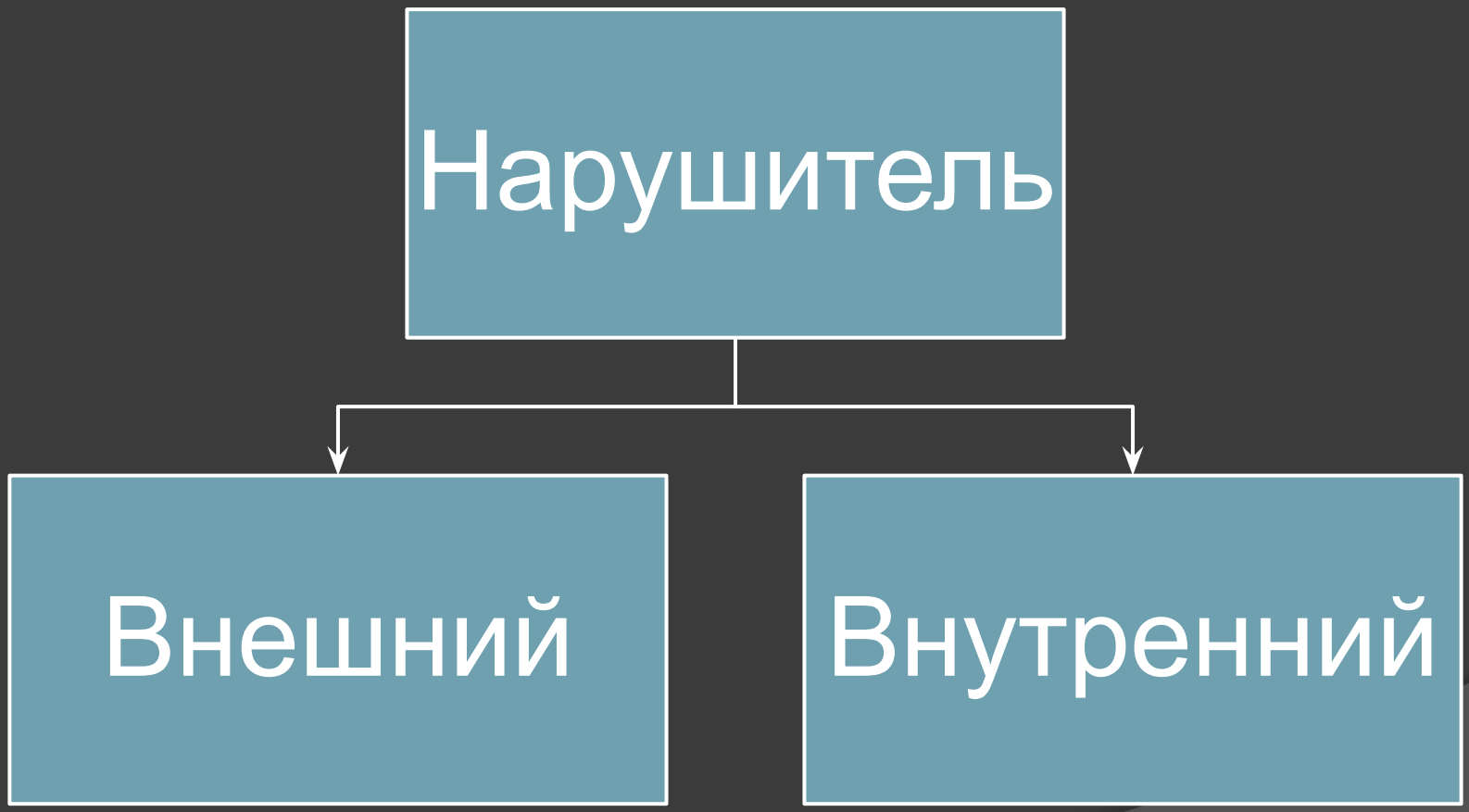
Презентация к РГР по дисциплине «Организационное и правовое обеспечение информационной безопасности»

Выполнила
студентка ФИиВТ
группы БИс-41
Девятилова Е.В.

Модель нарушителя информационной безопасности

это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д.

Классификации нарушителей



Виды внутренних нарушителей :

- непосредственных пользователей и операторов информационной системы, в том числе руководителей различных уровней
- администраторов вычислительных сетей и информационной безопасности
- прикладных и системных программистов;
- сотрудников службы безопасности
- технический персонал по обслуживанию зданий и вычислительной техники, от уборщицы до сервисного инженера
- вспомогательный персонал и временных работников

Причины, побуждающие сотрудников к неправомерным действиям

- безответственность;
- ошибки пользователей и администраторов
- демонстрацию своего превосходства (самоутверждение)
- «борьбу с системой»
- корыстные интересы пользователей системы
- недостатки используемых информационных технологий

Виды внешних нарушителей :

- клиенты
- приглашенные посетители
- представители конкурирующих организаций
- сотрудники органов ведомственного надзора и управления
- нарушители пропускного режима
- наблюдатели за пределами охраняемой территории

Используемые методы и средства

- сбор информации и данных
- пассивные средства перехвата
- использование средств, входящих в информационную систему или систему ее защиты, и их недостатков
- активное отслеживание модификаций существующих средств обработки информации, подключение новых средств, использование специализированных утилит, внедрение программных закладок и «черных ходов» в систему, подключение к каналам передачи данных

Уровень знаний нарушителя относительно организации информационной структуры:

- типовые знания о методах построения вычислительных систем, сетевых протоколов, использование стандартного набора программ
- высокий уровень знаний сетевых технологий, опыт работы со специализированными программными продуктами и утилитами
- высокие знания в области программирования, системного проектирования и эксплуатации вычислительных систем
- обладание сведениями о средствах и механизмах защиты атакуемой системы
- нарушитель являлся разработчиком или принимал участие в реализации системы обеспечения ИБ

Время информационного воздействия

- в момент обработки информации
- в момент передачи данных
- в процессе хранения данных (учитывая рабочее и нерабочее состояния системы)

По месту осуществления воздействия

- удаленно с использованием перехвата информации, передающейся по каналам передачи данных, или без ее использования
- доступ на охраняемую территорию
- непосредственный физический контакт с вычислительной техникой:
  - доступ к рабочим станциям,
  - доступ к серверам предприятия,
  - доступ к системам администрирования, контроля и управления информационной системой,
  - доступ к программам управления системы обеспечения информационной безопасности

Классификация нарушителей согласно методическим рекомендациям ФСБ

- В методических рекомендациях ФСБ выделено 6 классов нарушителей
- Они обозначены Н1-Н6
- Опасность нарушителя растет от Н1 к Н6

Сравнительная характеристика возможностей и целей основных типов нарушителей

Всех нарушителей можно условно разделить на 4 типа по их квалификации и возможностям:

- хакер-одиночка
- группа хакеров
- конкуренты
- госструктуры или спецподразделения