Цели злоумышленников

Нарушение конфиденциальности передаваемой информации

Нарушение целостности и достоверности передаваемой информации

Нарушение работоспособности всей системы или отдельных её частей

Классификация информационных сфер в соответствии с видами деятельности

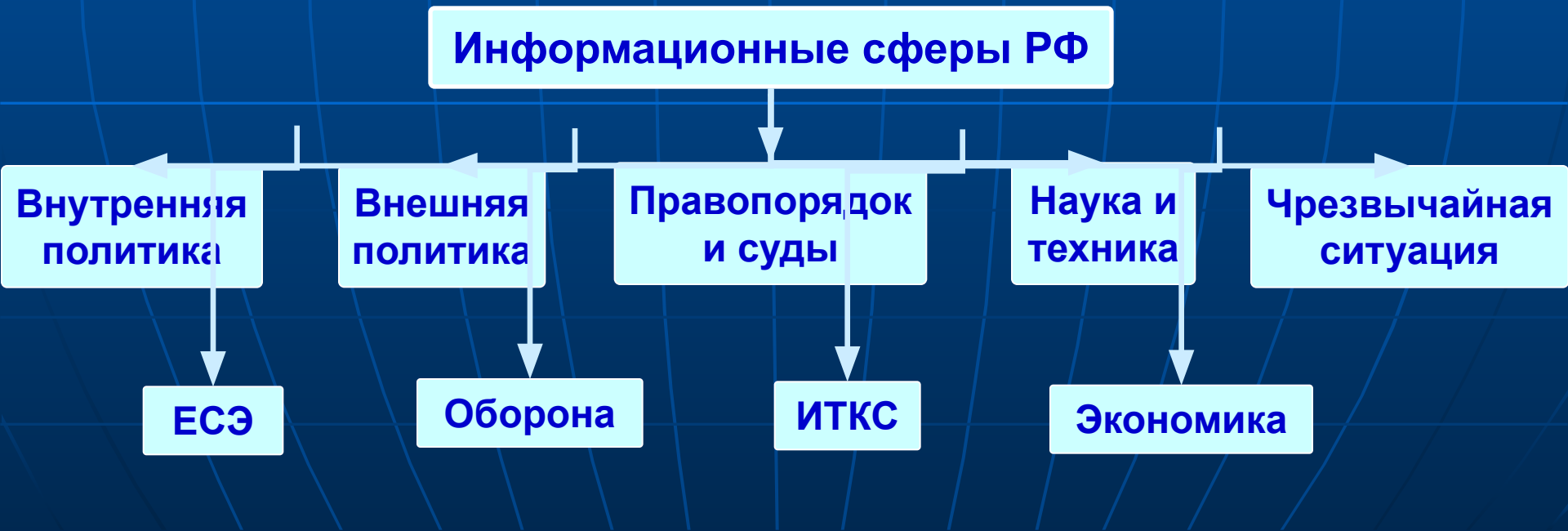
Угроза – потенциальная возможность нарушения защиты.

Угроза безопасности - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на неё.

Виды угроз ИБ РФ

- угрозы конституционным правам и свободам человека и гражданина;
- угрозы информационному обеспечению государственной политики РФ;
- угрозы развитию отечественной индустрии информации;
- угрозы безопасности ИТКС.



умышленное воздействие на защищаемую информацию с целью ее искажения, блокирования доступа к информации собственника (законного пользователя), а также с целью её уничтожения.

воздействия на информацию в результате ошибочных действий пользователя, сбоя технических и программных средств и воздействия природных явлений, приводящих к искажению, уничтожению, копированию и блокированию информации.

Угроза ИБ КС – возможность реализации воздействия на информацию, обрабатываемую в КС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты КС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

Угрозы ИБ КС

По природе возникновения

- Естественные угрозы
- Искусственные угрозы

По степени преднамеренности проявления

- Несанкционированного воздействия
- Непреднамеренного воздействия

По виду источника угроз

- Природные явления
- Человек
- Программно-аппаратные средства

По местоположению источника угроз

- Контролируемая зона
- В автоматизированных системах
- В периферийных устройствах

По степени активности КС

- Не работающая
- Работающая

По степени воздействия на КС

- Пассивные
- Активные

По этапам доступа к информационным ресурсам КС

- Получения доступа
- После разрешения доступа

По способу доступа

- Стандартный
- Не стандартный

По месту расположения информации

- Внешние ЗУ
- Оперативная память
- Линии связи
- Оконечное уст-во

Классификация угроз информационной безопасности КС

Уровни градации доступа к информации

- **уровень носителей информации**
- **уровень средств взаимодействия с носителем информации**
- **уровень представления информации**
- **уровень содержания информации**

Основные направления реализации угроз информации

1. **Непосредственное обращение к объектам доступа.**

2. Создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты.

3. Модификация средств защиты, позволяющая реализовать угрозы информационной безопасности.

4. Внедрение в технические средства КС программных или технических механизмов, нарушающих предполагаемую структуру и функции КС.

Основные методы реализации угроз информации

1. Определение злоумышленником типа и параметров носителей информации.
2. Получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения.
3. Получение злоумышленником детальной информации о функциях, выполняемых КС.
4. Получение злоумышленником данных о применяемых системах защиты.
5. Определение способа представления информации.
6. Определение злоумышленником содержания данных, обрабатываемых в КС, на качественном уровне (применяется для мониторинга КС и для дешифрования сообщений).
7. Использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок.
8. Уничтожение средств вычислительной техники и носителей информации.
9. Хищение носителей информации.
10. Несанкционированный доступ пользователя к ресурсам КС в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов.
11. Несанкционированное превышение пользователем своих полномочий.
12. Несанкционированное копирование программного обеспечения.
13. Перехват данных, передаваемых по каналам связи.
14. Визуальное наблюдение.
15. Раскрытие представления информации (дешифрование данных).

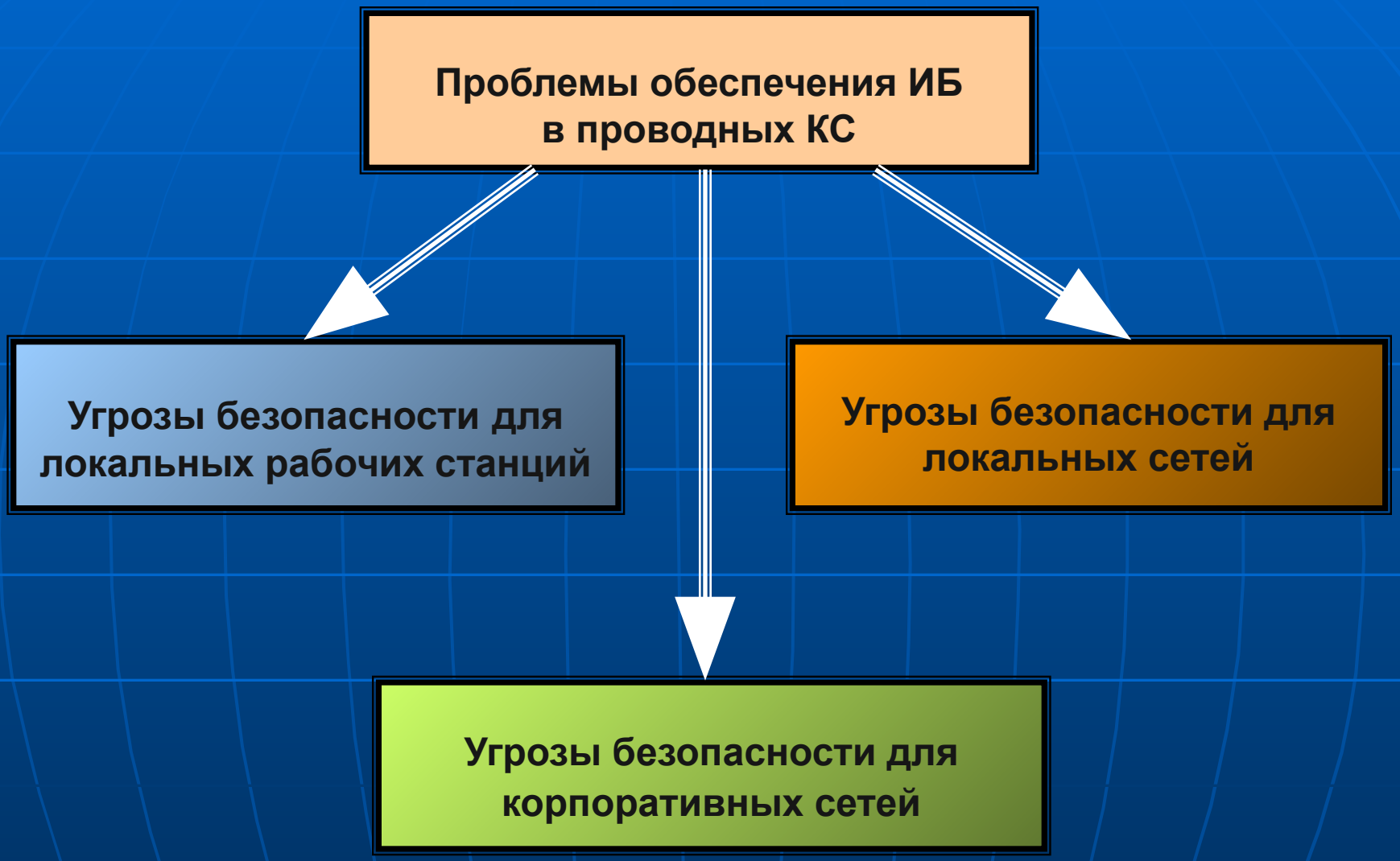
Основные методы реализации угроз информации

(продолжение)

16. Внесение пользователем несанкционированных изменений в программно-аппаратные компоненты АС и обрабатываемые данные.
17. Установка и использование нештатного аппаратного и программного обеспечения.
18. Заражение программными вирусами.
19. Внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи.
20. Внедрение дезинформации.
21. Выведение из строя машинных носителей информации без уничтожения информации.
22. Проявление ошибок проектирования и разработки аппаратных и программных компонентов КС.
23. Обход (отключение) механизмов защиты.
24. Искажение соответствия синтаксических и семантических конструкций языка.
25. Запрет на использование информации.

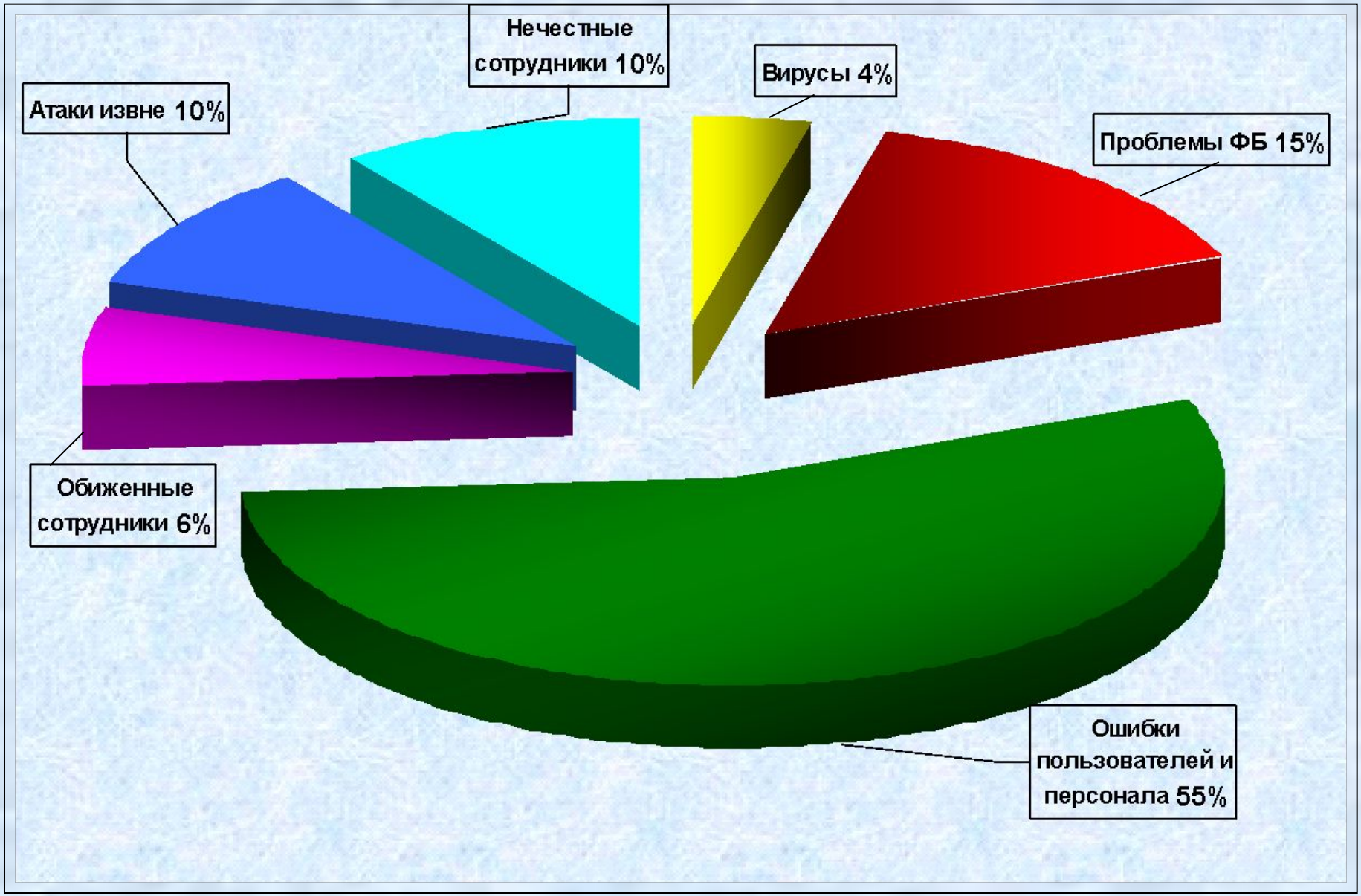
Распределение методов реализации угроз информации в соответствии с видом угроз и уровнем доступа к информации

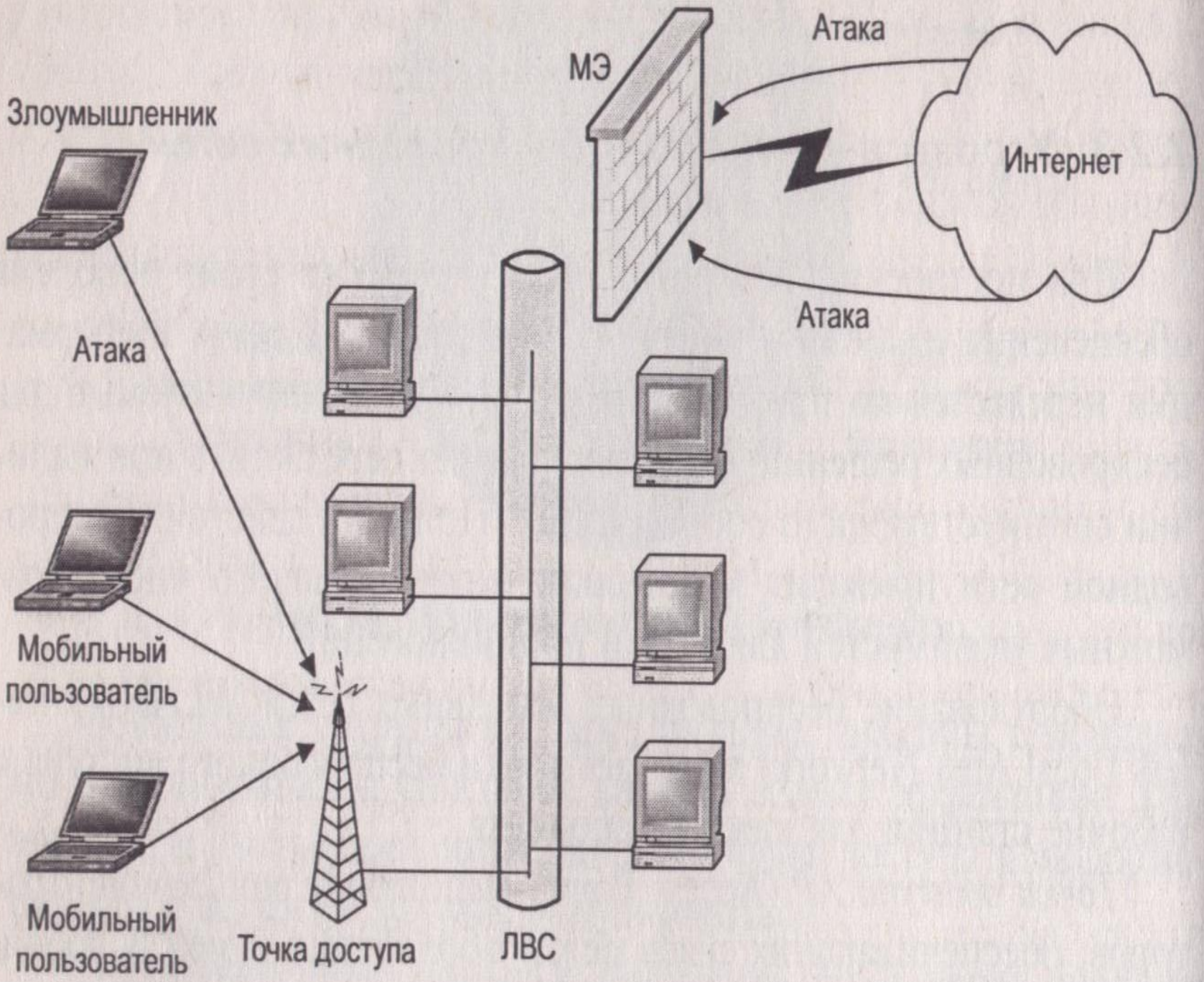
Уровень доступа к информации	Основные методы реализации угроз информации			
	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза нарушения доступа к информации	Угроза раскрытия параметров системы
Носителей информации	Хищение (копирование) носителей информации. Перехват ПЭМИН	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации	Определение типа и параметров носителей информации
Средств взаимодействия с носителем	НСД к ресурсам АС. Совершение пользователем несанкционированных действий. Несанкционированное копирование программного обеспечения. Перехват	Внесение пользователем несанкционированных изменений в программы и данные. Установка и использование нештатного программного обеспечения. Заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонентов АС. Обход механизмов защиты АС	Получение информации о программно-аппаратной среде. Получение детальной информации о функциях, выполняемых АС. Получение данных о применяемых системах защиты
Представления информации	Визуальное наблюдение. Раскрытие представления информации	Внесение искажения в представление данных; уничтожение данных	Искажение соответствия синтаксических и семантических конструкций языка	Определение способа представления информации
Содержания информации	Раскрытие содержания информации	Внедрение дезинформации	Запрет на использование информации	Определение содержания данных на качественном уровне


Проблемы обеспечения ИБ
в проводных КС
Угрозы безопасности для
локальных рабочих станций
Угрозы безопасности для
локальных сетей
Угрозы безопасности для
корпоративных сетей


Основные угрозы в проводных КС
Подслушивание (sniffing)
Изменение данных
Анализ сетевого трафика
Подмена доверенного субъекта (spoofing)
Посредничество
Перехват сеанса
Парольные атаки
Отказ в обслуживании
Атаки на уровне приложений
Компьютерные вирусы

Источники нарушения безопасности




Злоумышленник
Атака
МЭ
Атака
Интернет
Атака
Мобильный пользователь
Мобильный пользователь
Точка доступа
ЛВС


Основные угрозы в беспроводных КС
Подслушивание (sniffing)
Вещание радиомаяка
Обнаружение WLAN
Ложные точки доступа в сеть
Атаки типа «человек-в-середине»
Анонимный доступ в Интернет
Отказ в обслуживании