Тема: Безопасность информации

Безопасность информации – это состояние защищенности информации от внутренних или внешних угроз, т.е. такое состояние, когда несанкционированное получение информации субъектами доступа, не имеющими соответствующих полномочий, невозможно, существенно затруднено или сведено к уровню не выше допустимого.

Аспекты информационной безопасности

1. Доступность для установленного круга лиц
2. Целостность (актуальность и непротиворечивость)
3. Конфиденциальность

Цели защиты информации

4. Предотвращение утечки, утраты, хищения, искажения, подделки информации;
5. Предотвращение угроз безопасности личности, организации, государству;
6. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
7. Предотвращение любых форм незаконного вмешательства в информационные ресурсы

Защита экономической информации

Системы защиты информации представляют собой комплекс специальных мер законодательного и административного характера, организационных мероприятий, физических и технических средств обеспечения безопасности информации.

Под безопасностью информации понимается ***состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.***

Безопасность информации - это ***состояние устойчивости информации к случайным или преднамеренным внешним воздействиям, исключающее недопустимый риск ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации.***

Острота проблемы защиты информации и информационных систем определяется следующими факторами:

- высокими темпами роста парка средств вычислительной техники и связи;
- вовлечением в процесс информационного взаимодействия большего числа людей и организаций;
- повышением уровня доверия к АИС;
- отношением к информации, как к товару с присущим ему стремлением к конкуренции и, как следствие промышленному шпионажу в области создания и сбыта информации услуг;
- концентрацией больших объемов информации различного назначения и принадлежности в определенных местах и на электронных носителях;
- наличием интенсивного обмена между участниками информационного процесса;
- количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;
- обострением противоречий между объективно существующими потребностями общества и расширением свободного обмена информацией и чрезмерными или недостаточными ограничениями на ее распространение и использование;
- дифференциацией уровня потерь от уничтожения, фальсификации, разглашения или незаконного тиражирования информации;
- многообразием видов угроз и возможных каналов несанкционированного доступа (НСД) к информации;
- ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими программно-математических воздействий на систему;
- развитием рыночных отношений в области разработки и обслуживания вычислительной техники и программных средств.

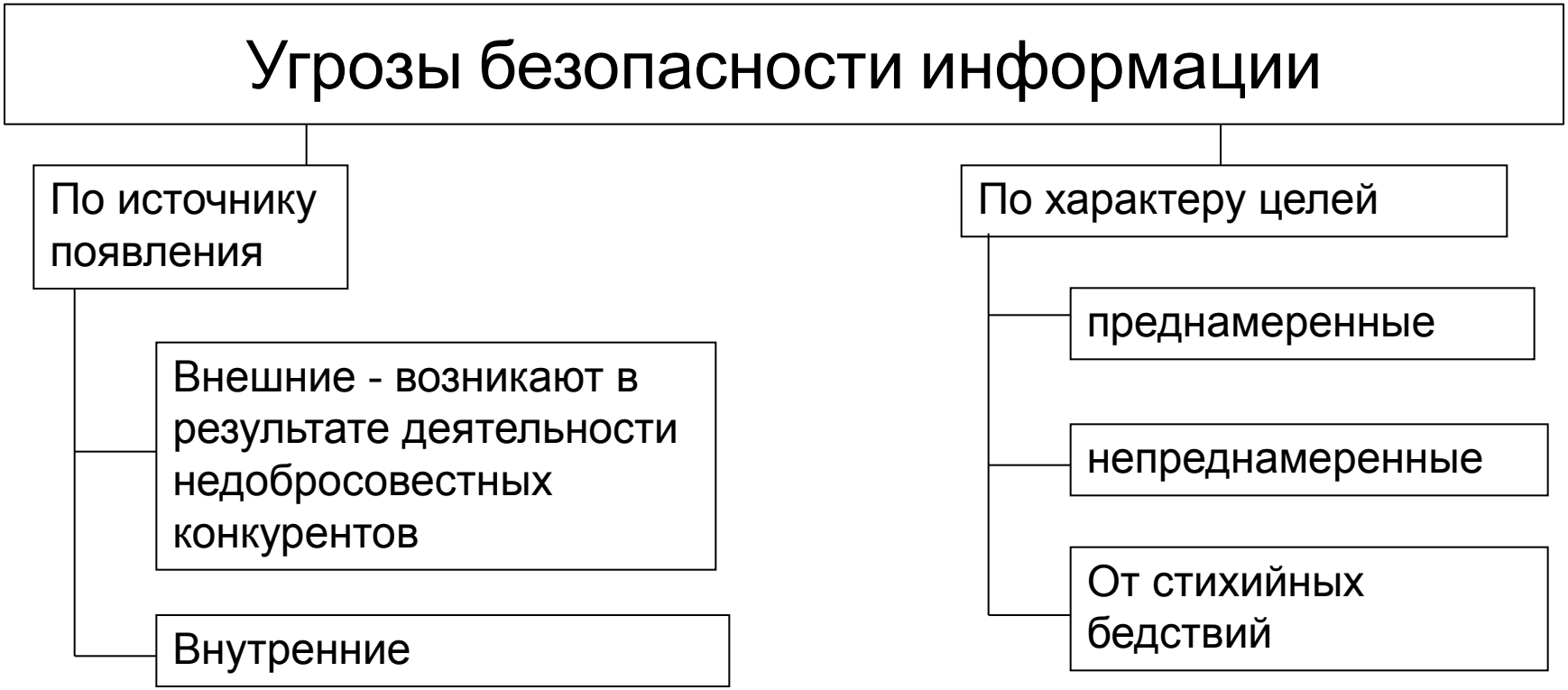
Компоненты системы защиты

- область физической безопасности, к средствам которой можно отнести механические и электронные замки, охрану и охранную сигнализацию и т.п.;
- безопасность персонала, где рассматривается защита сотрудников и защита от воздействия самих сотрудников. Это, в первую очередь, шпионаж, воздействие криминальных структур;
- правовая безопасность, аккумулирующая все проблемы законодательного регулирования вопросов защиты информации и вычислительных систем;
- безопасность оборудования, связанная с надежностью работы устройств, изучением возможностей несанкционированного перехвата информации и другими техническими аспектами;
- безопасность программного обеспечения, исключающая воздействие различного рода программных вирусов или непредусмотренных действий разработчиков;
- безопасность телекоммуникационной среды, связанная с проблемами распределения вычислительных систем. Это могут быть и физические повреждения каналов связи и просто утеря, подмена или неправомочная имитация законного пользователя.

Дестабилизирующие факторы

- количественная недостаточность
  - физическая нехватка одного или нескольких компонентов АИС для обеспечения требуемой защищенности информации по рассматриваемым показателям;
- качественная недостаточность
  - несовершенство конструкции или организации одного или нескольких компонентов АИС, в силу чего не обеспечивается требуемая защищенность информации;
- отказ
  - нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им своих функций;
- сбой
  - временное нарушение работоспособности какого-либо элемента АИС, следствием чего может быть неправильное выполнение им в этот момент своих функций;
- ошибка
  - неправильное (одноразовое или систематическое) выполнение элементом системы одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;
- стихийное бедствие
  - спонтанно возникающее неконтролируемое явление, проявляющееся как разрушительная сила;
- злоумышленные действия
  - действия людей, специально направленные на нарушение защищенности информации;
- побочное явление
  - явление, сопутствующее выполнению элементом своих основных функций, следствием которого может быть нарушение защищенности информации.

Угрозы безопасности информации



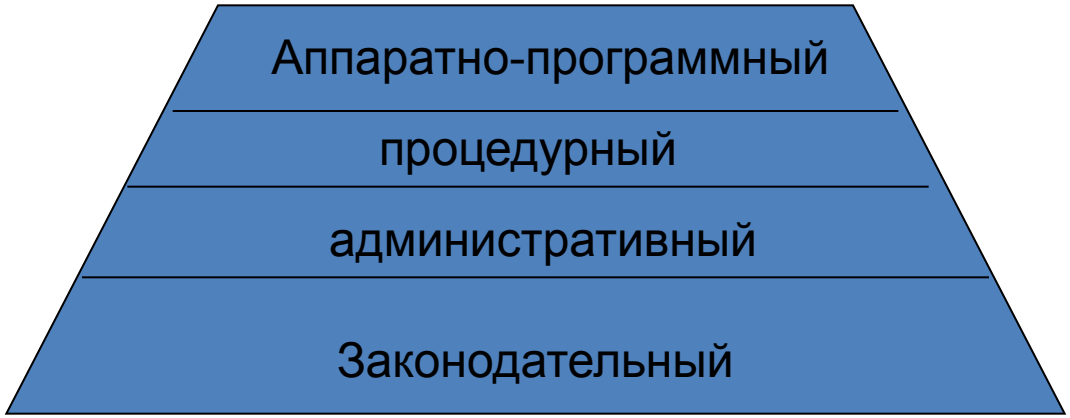
Способы реализации угроз

- Хищение носителей
- Применение программных ловушек
- Ошибки в программах обработки данных
- Неисправность аппаратуры
- Компьютерные вирусы
- Электромагнитное излучение

Угрозы безопасности информации

Способы нанесения ущерба	Объекты воздействий			
	оборудование	программы	данные	персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование, перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спец. вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	

Уровни защиты информации



Основные законы

1. Закон “Об информации, информатизации и защите информации” (1995)
2. Закон “О связи” (1995)
3. Закон “О банках и банковской деятельности”
4. Закон “О правовой охране программ для вычислительных машин и баз данных”
5. Закон “Об авторском праве и смежных правах”

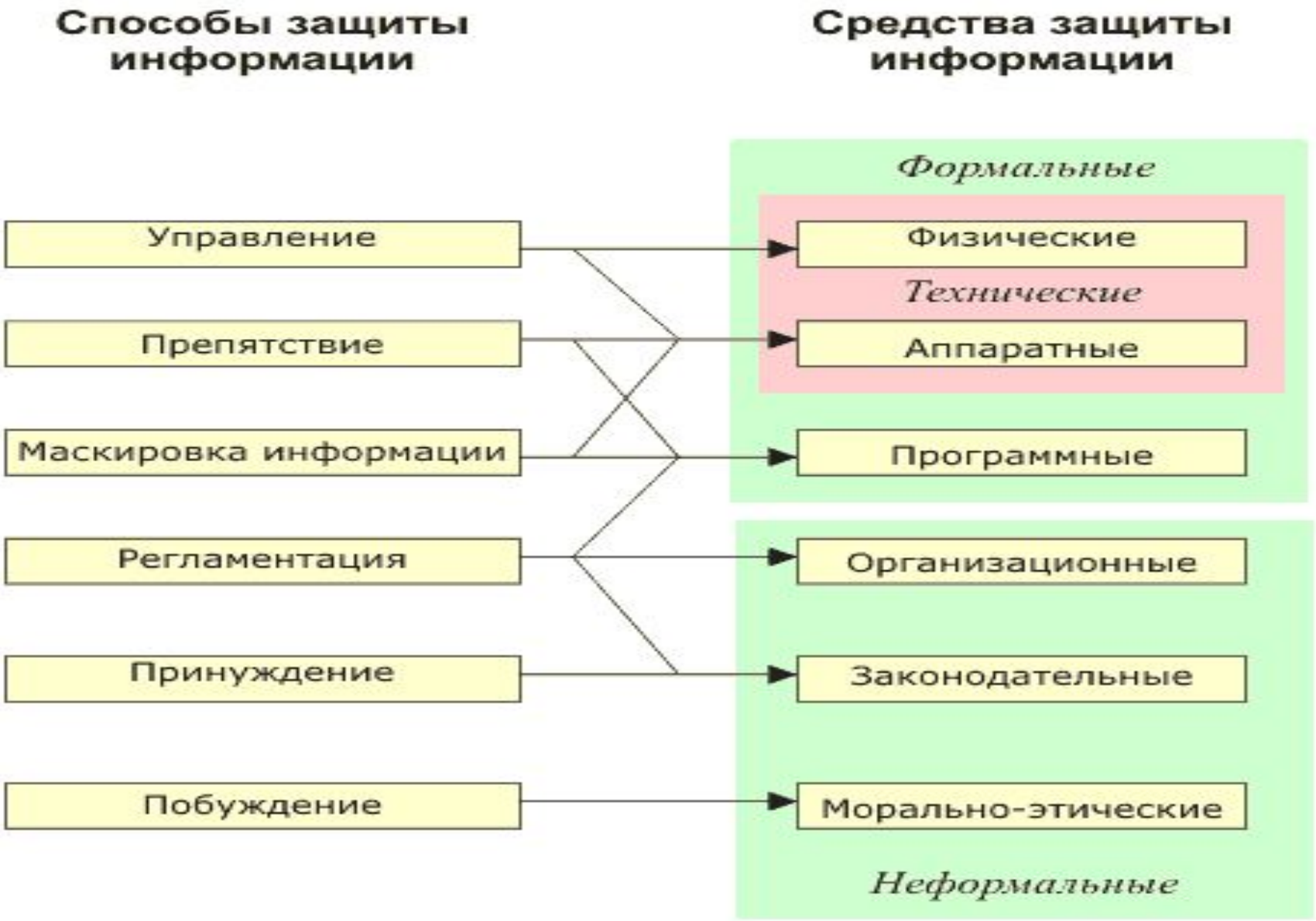
Формы защиты информации

- Признание коммерческой тайной
- Патентование
- Применение норм обязательного права

К коммерческой тайне не могут быть отнесены

- Учредительные документы
- Документы, дающие право заниматься предпринимательской деятельностью
- Сведения по установленным формам отчетности о финансово – хозяйственной деятельности
- Документы о платежеспособности
- Сведения о численности и составе работающих, заработной плате, условиях труда
- Документы об уплате налогов и других обязательных платежах
- Сведения о загрязнении окружающей среды, нарушениях антимонопольного законодательства
- Сведения об участии должностных лиц в кооперативах, малых предприятиях, товариществах, акционерных обществах и т.п.

Методы и средства защиты



Методы защиты

1. ***Управление доступом*** - метод защиты информации регулированием использования всех ресурсов системы, включающий следующие функции:
   - идентификация ресурсов системы;
   - установление подлинности (аутентификация) объектов или субъектов системы по идентификатору;
   - проверка полномочий в соответствии с установленным регламентом;
   - разрешение и создание условий работы в соответствии с регламентом;
   - регистрация обращений к защищаемым ресурсам;
   - реагирование при попытках несанкционированных действий.
2. ***Препятствие*** - метод физического преграждения пути нарушителю к защищаемым ресурсам системы.
3. ***Маскировка*** - метод защиты информации путем ее криптографического закрытия.
4. ***Регламентация*** - метод защиты информации, создающей такие условия автоматизированной обработки, хранения и передачи информации, при которых возможности несанкционированного доступа к ней минимизируются.
5. ***Принуждение*** - метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать регламент под угрозой ответственности.
6. ***Побуждение*** - метод защиты информации, который мотивирует пользователей и персонал системы соблюдать сложившиеся морально-этические нормы.

Организационные средства защиты

Организационные меры защиты определяют порядок:

- ведения системы защиты от несанкционированного доступа;
- ограничения доступа в помещения;
- назначения полномочий по доступу;
- контроля и учета событий;
- сопровождения ПО;
- контроля за системой защиты.

Программные средства защиты

- ***Программные средства защиты*** (ПСЗ) включают в себя:
- систему разграничения доступа к вычислительным и информационным ресурсам системы;
- средства криптографической защиты информации, хранящейся на магнитных носителях АРМ и файл-сервера системы;
- средства регистрации и учета попыток НСД, событий в системе, документов, выводимых на печать и т. д.;
- средства обеспечения и контроля целостности программных файлов, в том числе средства борьбы с программами-вирусами;
- средства контроля паузы неактивности пользователя системы.

Аппаратные и криптографические средства защиты

- ***Аппаратные средства защиты***, выбор которых определяется такими техническими характеристиками как:
- высокая надежность - с целью исключения искажения экономической информации и преодоления рубежей защиты нарушителем;
- высокая производительность шифрования информации, которая должна обеспечить время реакции системы на запрос пользователя не более 3 сек.
- ***Криптографические средства защиты*** информации автоматизированной системы, среди которых самым примитивным методом можно назвать обмен паролями со всеми присущими ему недостатками. Одно из последних достижений в области криптографии - цифровая сигнатура. Это способ обеспечения целостности с помощью дополнения сообщения специальным свойством, которое может быть проверено только тогда, когда известен открытый ключ, присвоенный автору сообщения. Криптографические средства предназначены для эффективной защиты информации:
- в случае кражи, утери компьютера или магнитного носителя;
- при выполнении ремонтных или сервисных работ посторонними лицами или обслуживающим персоналом, не допущенным к работе с конфиденциальной информацией;
- при передаче информации в виде зашифрованных файлов по незащищенным каналам связи;
- при использовании компьютера несколькими пользователями.

Этапы создания систем защиты

- инженерно-техническое обследование и описание информационных ресурсов системы;
- определение наиболее критичных, уязвимых мест системы;
- вероятностная оценка угроз безопасности информационным ресурсам;
- экономическая оценка возможного ущерба;
- стоимостной анализ возможных методов и средств защиты информации;
- определение рентабельности применения системы защиты информации.

Методы защиты информации

- Ограничение доступа
- Разграничение доступа
- Разделение привилегий
- Криптографическое преобразование
- Контроль и учет доступа