Національна академія СБ України

Козюра В.Д.

Лекція 24. Основні поняття і положення захисту інформації в комп'ютерних системах

МОДУЛЬ 7. ***Програмні засоби захисту інформації в комп'ютерних системах***

ТЕМА 20. ***Принципи захисту інформації в комп'ютерних системах***

Київ – 2011

Зміст

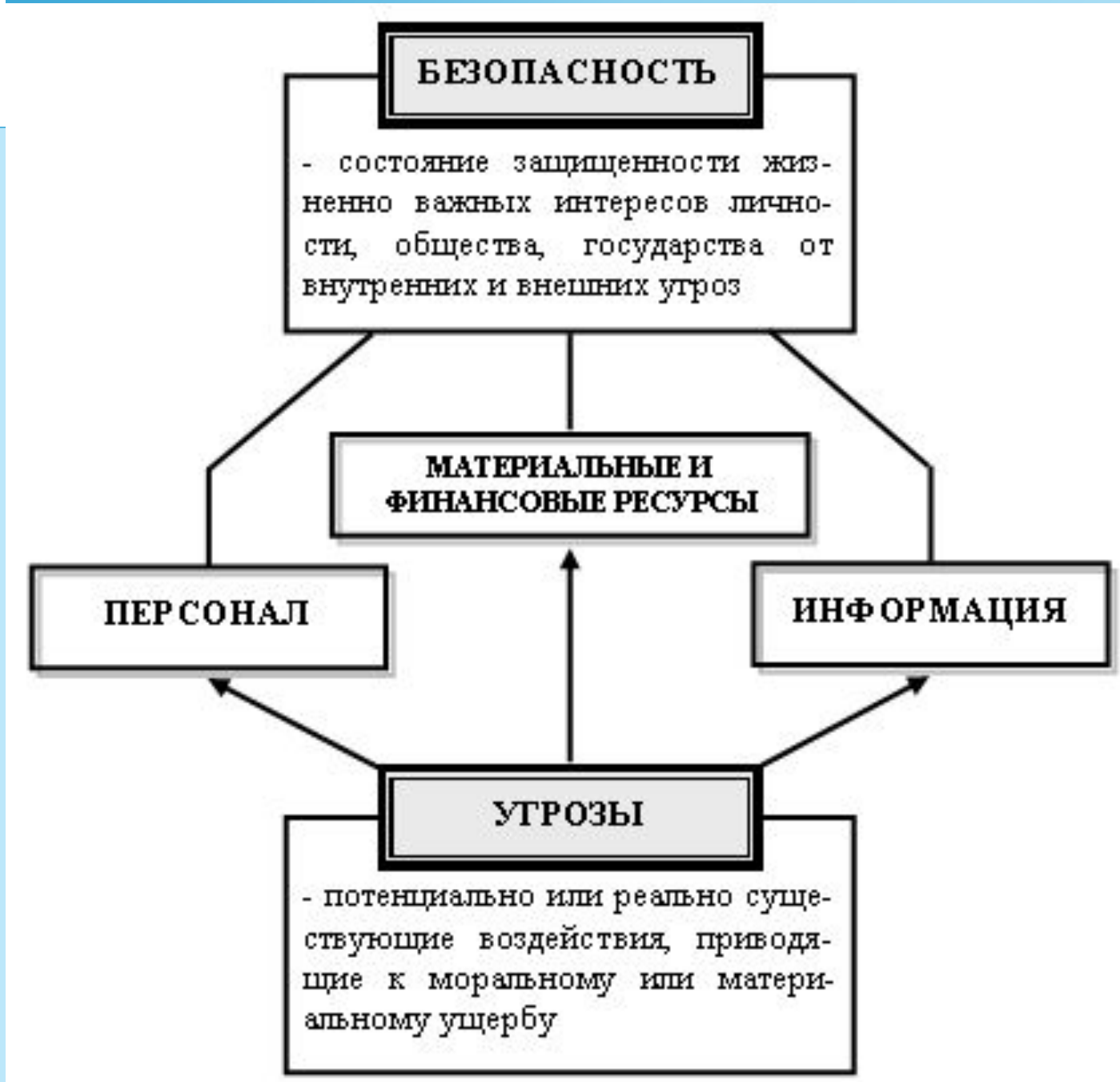
1. Основні концептуальні положення побудови системи захисту інформації в комп'ютерних системах
2. Загрози захисту інформації
3. Напрямки забезпечення інформаційної безпеки в комп'ютерних системах

ЛІТЕРАТУРА

1. *Ярочкин В.И.* Информационная безопасность: Учебник для студентов вузов. – М.: Академический проект; Фонд «Мир», 2003. с. 6-97.
2. *Завгородний В.И.* Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001. с. 8-37.

Информационная безопасность – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Целью лекции *является раскрытие основных положений построения комплексной системы защиты информации в компьютерных системах.*


БЕЗОПАСНОСТЬ
- состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз
МАТЕРИАЛЬНЫЕ И ФИНАНСОВЫЕ РЕСУРСЫ
ПЕРСОНАЛ
ИНФОРМАЦИЯ
УГРОЗЫ
- потенциально или реально существующие воздействия, приводящие к моральному или материальному ущербу

1. ОСНОВНЫЕ КОНЦЕПТУАЛЬНЫЕ ПОЛОЖЕНИЯ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Система защиты информации (СЗИ) – **организованная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.**

Объект защиты - компьютерная система, представляющая собой организационно-техническую систему, объединяющую:

- *сведения* на любом носителе, которые отнесены к информации с ограниченным доступом;
- *информационные ресурсы* (информационные массивы и базы данных);
- *оборудование компьютерной системы* (рабочие станции, коммуникационные каналы и оборудование, серверы, средства печати, накопители информации и т.д.);
- *программное обеспечение*, процессы и технологии обработки информации и ее защиты;
- *средства и системы физической охраны* материальных и информационных ресурсов;
- *владельцев* информации и КС, *обслуживающий персонал*, *пользователей*, а также их *права*.

Защита информации должна быть:

- ***непрерывной***;
- ***плановой***;
- ***целенаправленной*** (защищается то, что ценно);
- ***конкретной*** (защите подлежат конкретные данные);
- ***активной***;
- ***надежной*** (методы, формы и средства защиты должны надежно перекрывать возможные каналы несанкционированного доступа и утечки информации);
- ***универсальной***;
- ***комплексной*** - для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме.

Виды обеспечения СЗИ

- Правовое
- Организационное
- Аппаратное
- Информационное
- Программное
- Математическое
- Лингвистическое
- Нормативно-методическое

Правовое обеспечение - нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия.

Организационное обеспечение - реализация защиты информации осуществляется определенными структурными единицами (режимно-секретная служба, служба режима, служба охраны, служба ТЗИ и др.)

Аппаратное обеспечение - использование технических средств как для защиты информации, так и для обеспечения деятельности собственно СЗИ.

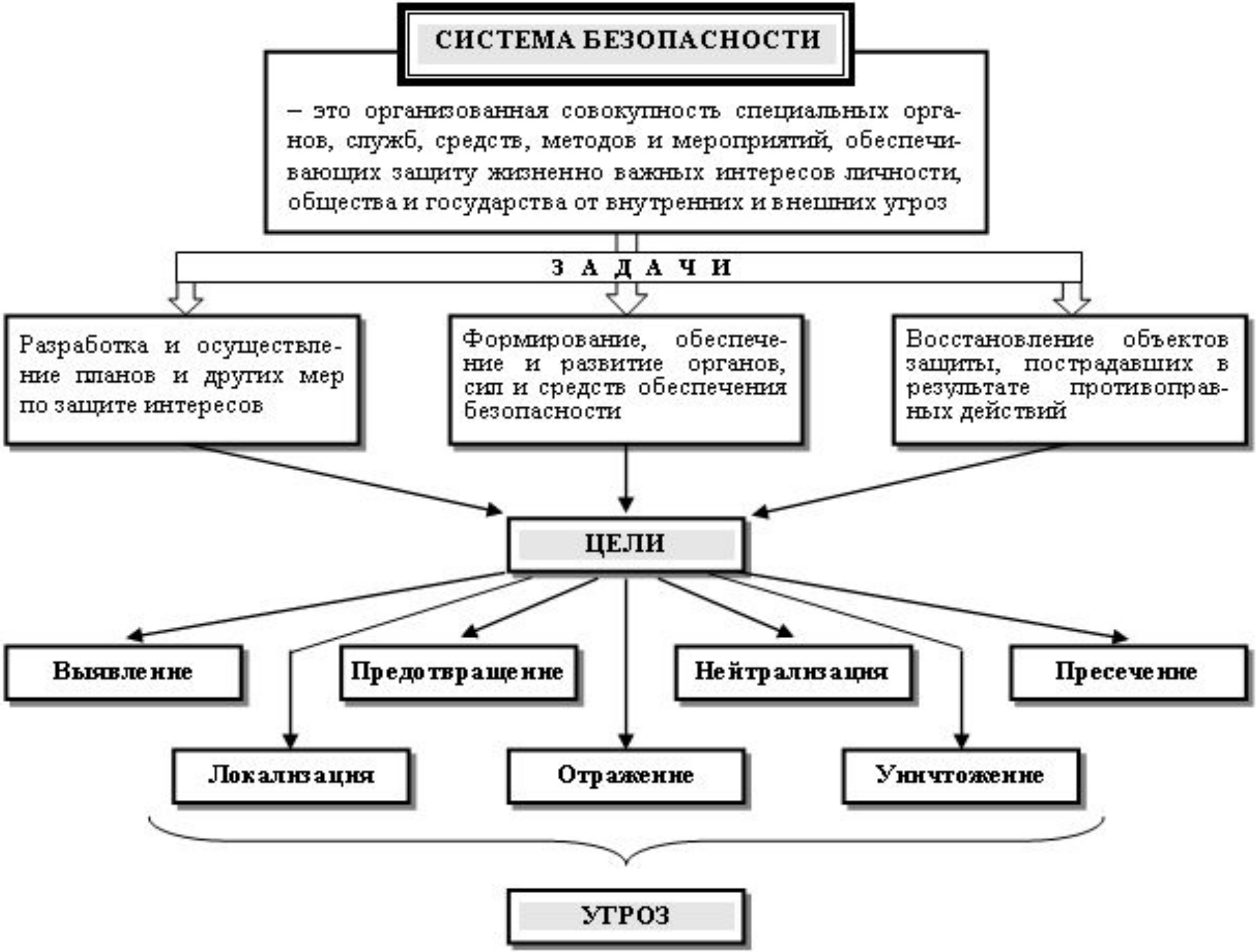
Информационное обеспечение - сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование СЗИ (показатели доступа, учета, хранения, системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности).

Программное обеспечение - информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей НСД к источникам защищаемой информации).

Математическое обеспечение - использование мат. методов для различных расчетов, связанных с оценкой опасности действий нарушителей, зон и норм необходимой защиты.

Лингвистическое обеспечение - специальные языковые средства общения специалистов и пользователей в сфере защиты информации.

Нормативно-методическое обеспечение **-** нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации


СИСТЕМА БЕЗОПАСНОСТИ
– это организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
З А Д А Ч И
Разработка и осуществление планов и других мер по защите интересов
Формирование, обеспечение и развитие органов, сил и средств обеспечения безопасности
Восстановление объектов защиты, пострадавших в результате противоправных действий
ЦЕЛИ
Выявление
Предотвращение
Нейтрализация
Пресечение
Локализация
Отражение
Уничтожение
УГРОЗ

Удовлетворить современные требования по обеспечению безопасности информационных ресурсов организации может только комплексная система защиты информации!!!

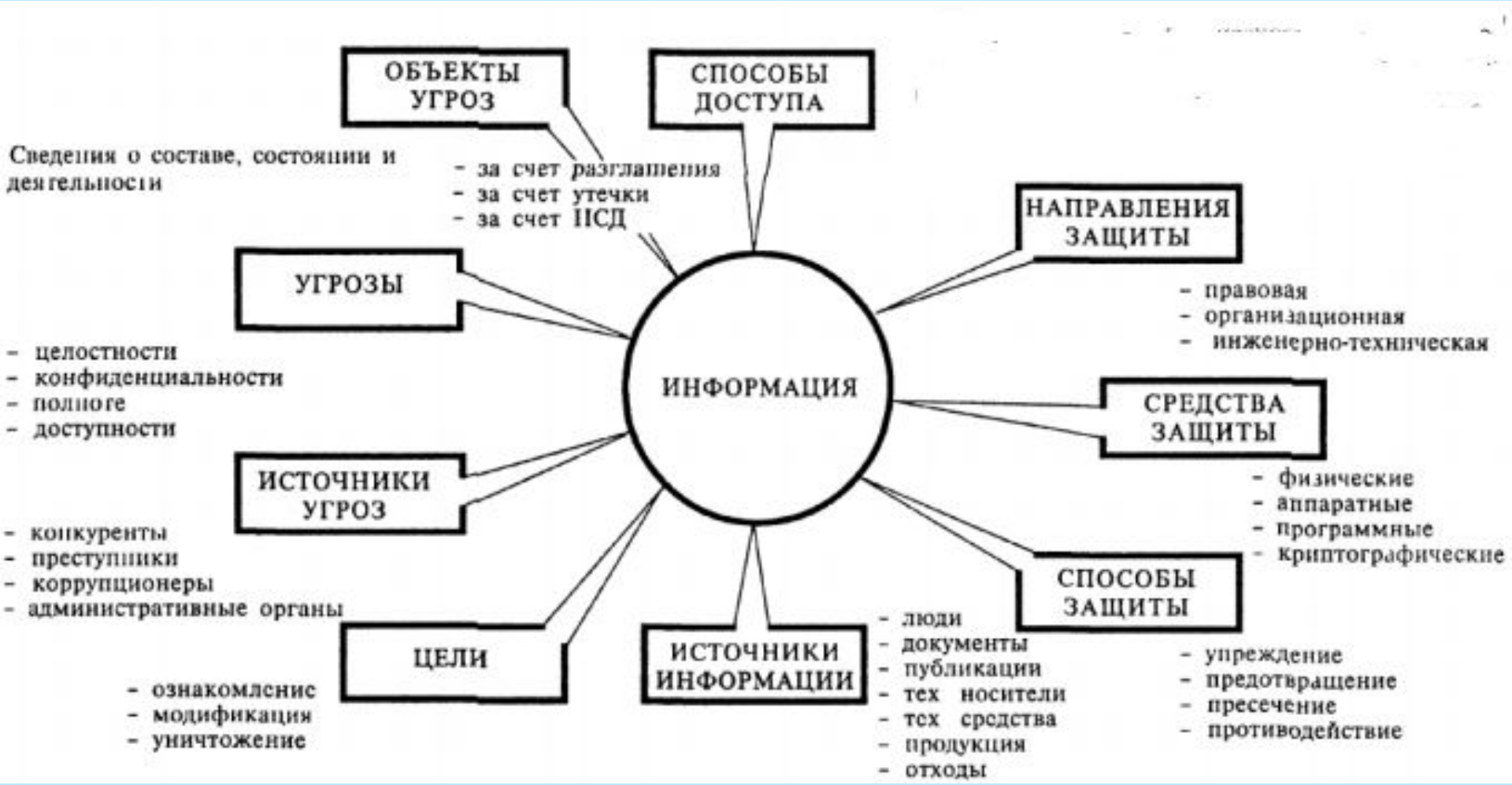
Комплексная система защиты информации в компьютерной системе (КСЗИ) - единый комплекс правовых норм, организационных и инженерных мероприятий, технических (аппаратных), программных и криптографических средств, обеспечивающий защищенность информации в соответствии с принятой политикой безопасности.


Комплексная система защиты информации
Служба защиты информации
Комплекс средств криптографической защиты
Комплекс средств защиты от НСД
КСЗИ
Инженерно-технические мероприятия
Физическая охрана объектов
Комплекс средств блокирования технических каналов
Регламентация действий пользователей

Принципы создания КСЗИ

- концептуальное единство;
- адекватность требованиям;
- гибкость (адаптируемость);
- функциональная самостоятельность;
- удобство использования;
- минимизация предоставляемых прав;
- полнота контроля;
- адекватность реагирования на угрозы;
- экономическая целесообразность.

Концептуальная модель безопасности информации в КС



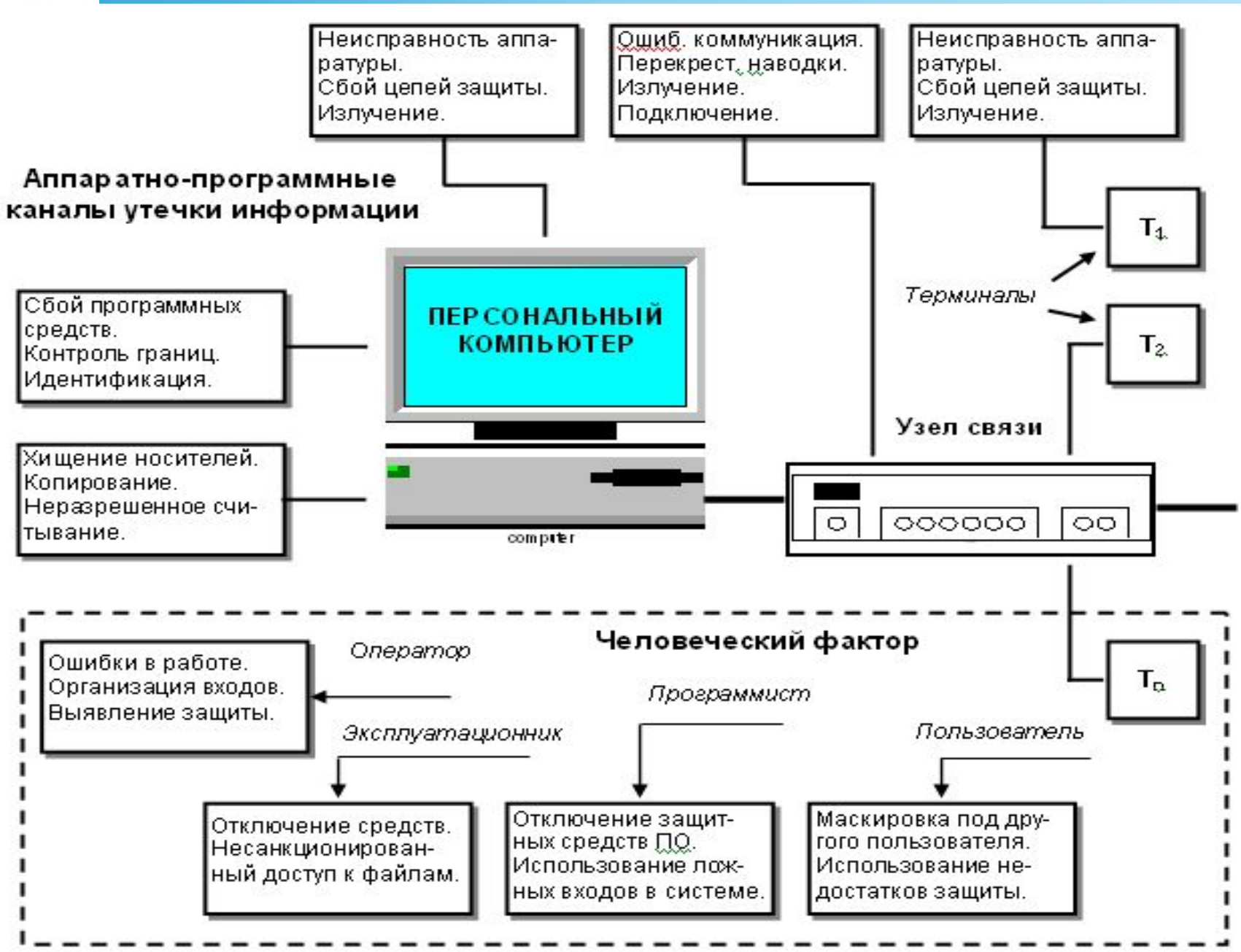
2. УГРОЗЫ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Безопасность (защищенность) информации в КС – такое состояние всех ее компонент, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.

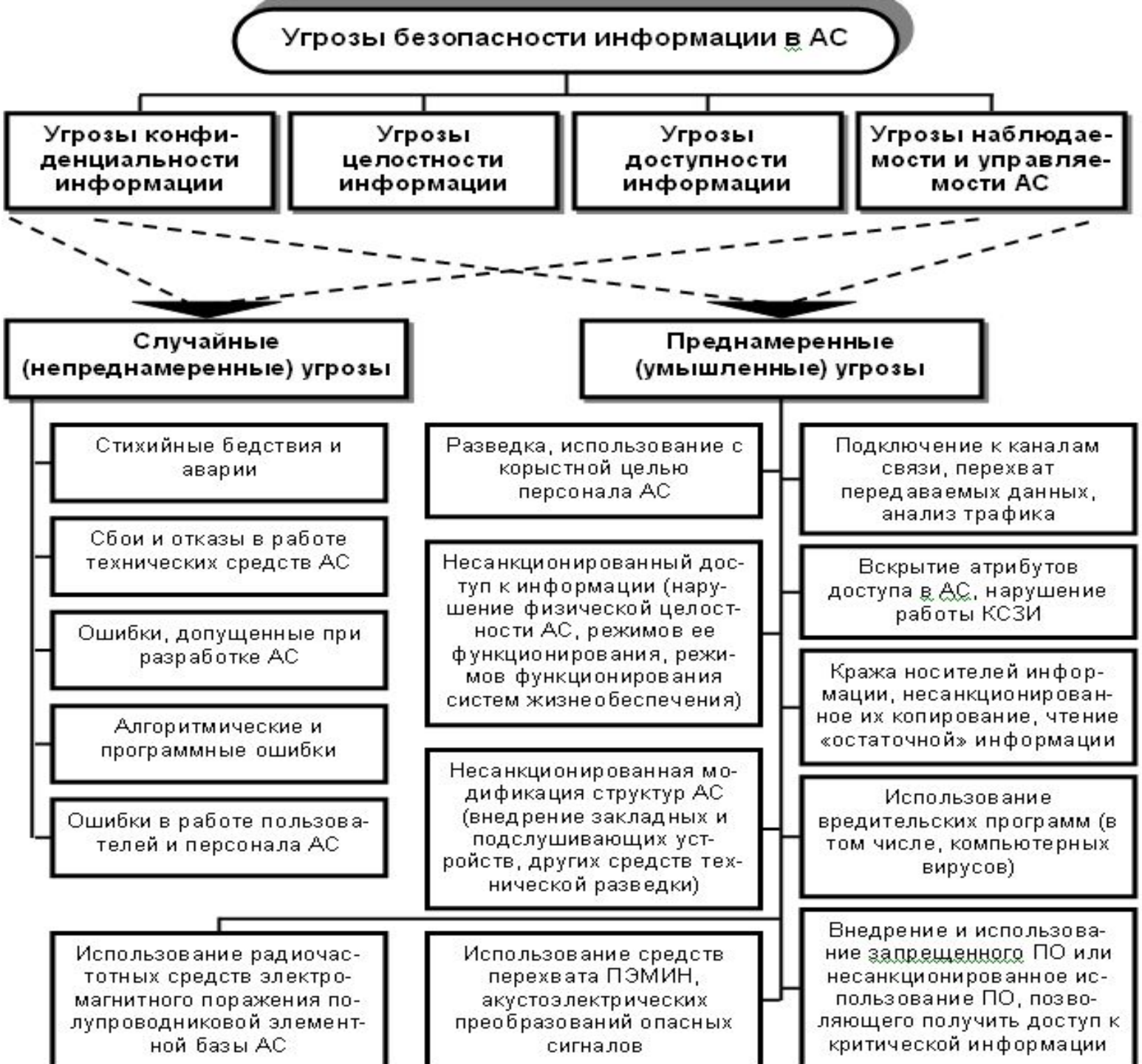
Угроза безопасности информации - потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации, а также нарушению наблюдаемости и управляемости КС.
Попытка реализации угрозы называется **атакой**.

Угрозы информации проявляются в нарушении

Пример потенциальных угроз в КС




КЛАССИФИКАЦИЯ УГРОЗ
Угроза – потенциально возможное или реальное действие злоумышленников, способное нанести моральный или материальный ущерб
По объектам
Персонал
Материальные и финансовые ценности
Информация
По величине ущерба
Предельный
Значительный
Незначительный
По вероятности возникновения
Весьма вероятные
Вероятные
Маловероятные
По причинам появления
Стихийные
Преднамеренные
По ущербу
Материальный
Моральный
По отношению к объекту
Внутренние
Внешние
По характеру воздействия
Активные
Пассивные


Угрозы безопасности информации в АС
Угрозы конфиденциальности информации
Угрозы целостности информации
Угрозы доступности информации
Угрозы наблюдаемости и управляемости АС
Случайные (непреднамеренные) угрозы
Преднамеренные (умышленные) угрозы
Стихийные бедствия и аварии
Сбои и отказы в работе технических средств АС
Ошибки, допущенные при разработке АС
Алгоритмические и программные ошибки
Ошибки в работе пользователей и персонала АС
Разведка, использование с корыстной целью персонала АС
Несанкционированный доступ к информации (нарушение физической целостности АС, режимов ее функционирования, режимов функционирования систем жизнеобеспечения)
Несанкционированная модификация структур АС (внедрение закладных и подслушивающих устройств, других средств технической разведки)
Использование радиочастотных средств электромагнитного поражения полупроводниковой элементной базы АС
Использование средств перехвата ПЭМИН, акустоэлектрических преобразований опасных сигналов
Подключение к каналам связи, перехват передаваемых данных, анализ трафика
Вскрытие атрибутов доступа в АС, нарушение работы КСЗИ
Кража носителей информации, несанкционированное их копирование, чтение «остаточной» информации
Использование вредительских программ (в том числе, компьютерных вирусов)
Внедрение и использование запрещенного ПО или несанкционированное использование ПО, позволяющего получить доступ к критической информации


ДЕЙСТВИЯ,
приводящие к незаконному овладению конфиденциальной информацией
РАЗГЛАШЕНИЕ
Уменьшенные или неосторожные действия должностных лиц и граждан, которым соответствующие сведения были доверены в установленном порядке, приведшие к ознакомлению с ними лиц, не допущенных к ним
Выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и других иных способах и реализуется по каналам распространения и средствам массовой информации
УТЕЧКА
Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
Возможна по различным каналам утечки информации, в том числе визуально-оптическим, акустическим, электромагнитным и материально-вещественным
НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП
Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям
Реализуется различными способами, в том числе такими, как сотрудничество, выведывание, подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, перехват, фотографирование и др

Разглашение — умышленные или неосторожные действия с охраняемыми сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

Утечка — бесконтрольный выход охраняемой информации за пределы организации или круга лиц, которым она была доверена.

Несанкционированный доступ — противоправное преднамеренное овладение охраняемой информацией лицом, не имеющим права доступа к охраняемым секретам.

Технический канал утечки информации — физический путь от источника информации к нарушителю, посредством которого может быть осуществлен НСД к охраняемым сведениям.

Типы технических каналов утечки информации:

- ***радиоканалы*** (электромагнитные излучения радиодиапазона);
- ***акустические каналы*** (звуковые колебания в любой среде);
- ***электрические каналы*** (опасные напряжения и токи в токопроводящих коммуникациях);
- ***оптические каналы*** (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой части спектра);
- ***материально-вещественные каналы*** (бумага, фото, цифровые и магнитные носители, отходы и т.п.).

Какие условия способствуют неправомерному овладению конфиденциальной информацией?

- разглашение (излишняя болтливость) — **32%;**
- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок — **24%;**
- отсутствие в организации надлежащего контроля и жестких условий обеспечения информационной безопасности — **14%;**
- обмен производственным опытом — **12%;**
- бесконтрольное использование КС — **10%;**
- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций — **8%.**

3. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

1. Если не уверен в безопасности, считай, что опасность существует реально.
2. Безопасности бесплатной не бывает.
3. Безопасности не бывает много.
4. Безопасность должна быть только комплексной.
5. Комплексная безопасность может быть обеспечена только системой безопасности.
6. Никакая система безопасности не обеспечивает требуемого уровня без надлежащей подготовки руководителей, сотрудников и пользователей.
7. В безопасности должен быть заинтересован каждый.

Направления обеспечения информационной безопасности — нормативно-правовые категории, ориентированные на обеспечение комплексной защиты информации от внутренних и внешних угроз:

- **правовая защита** — законы, нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- **организационная защита** — регламентация служебной деятельности и взаимоотношений исполнителей на нормативно-правовой основе;
- **инженерно-техническая защита** — использование различных инженерных, аппаратных, программных, криптографических и других средств, препятствующих нанесению ущерба информационной деятельности.

Правовая защита

Право — совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Конституция Украины определяет, что «защита суверенитета и территориальной целостности Украины, обеспечение ее экономической и ***информационной безопасности*** являются важнейшими функциями государства, делом всего Украинского народа» (ст. 17).

Информационная безопасность государства – состояние защищенности его национальных интересов в информационной сфере:

- ***соблюдение конституционных прав и свобод человека*** в области получения информации и пользования ею;
- ***развитие современных информационных технологий, отечественной индустрии информации***, обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- ***защита информационных ресурсов*** от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

К основным угрозам национальным интересам и национальной безопасности Украины в информационной сфере относятся:

- ***компьютерная преступность и компьютерный терроризм***,
- ***разглашение информации***, составляющей государственную и другую, предусмотренную законом, тайну, а также конфиденциальной информации, являющейся собственностью государства.

(ст. 7 Закона Украины **«Об основах национальной безопасности Украины»** (19.06.2003 г.)).

«Об информации» (02.10.1992 г.) – базовый законом в области информационной деятельности, регламентирующий отношения, возникающие при формировании и использовании информационных ресурсов Украины;

«О государственной тайне» (21.01.1994 г.) – регулирует отношения, возникающие в связи с отнесением информации к государственной тайне, засекречиванием и рассекречиванием ее материальных носителей;

«О защите информации в информационно-телекоммуникационных системах» (31.05.2005 г.) - регулирует правовые отношения по защите информации в информационно-телекоммуникационных системах, устанавливает их юридический статус и систему защиты информации, обрабатываемой в них.

«**Доктрина информационной безопасности Украины**» (утверждена Указом Президента Украины от 8 июля 2009 г. № 514/2009) констатирует, что современные информационные технологии позволяют государствам реализовать собственные интересы без использования военной силы, поэтому информационная безопасность является неотъемлемой составной частью каждой из сфер национальной безопасности (внешнеполитической, государственной безопасности, военной, внутриполитической, экономической, социальной и гуманитарной, науко-технологической, экологической), а также важнейшей самостоятельной сферой обеспечения национальной безопасности.

«Положение о технической защите информации в Украине» (утверждено Указом Президента Украины от 27 сентября 1999 г. № 1229/99 с изменениями, внесенными в соответствии с Указом Президента № 1120/2000 от 06.10.2000 г.) определяет правовые и организационные основы технической защиты важной для государства, общества и человека информации, охрана которой обеспечивается государством.

«Положение о порядке осуществления криптографической защиты информации в Украине» (утверждено Указом Президента Украины от 22 мая 1998 г. № 505/98 с изменениями, внесенными в соответствии с Указами Президента № 1019/98 от 15.09.98 г. и № 1229/99 от 27.09.99 г.) определяет порядок осуществления криптографической защиты информации с ограниченным доступом, разглашение которой наносит (может нанести) ущерб государству, обществу и человеку.

Уголовный Кодекс Украины:

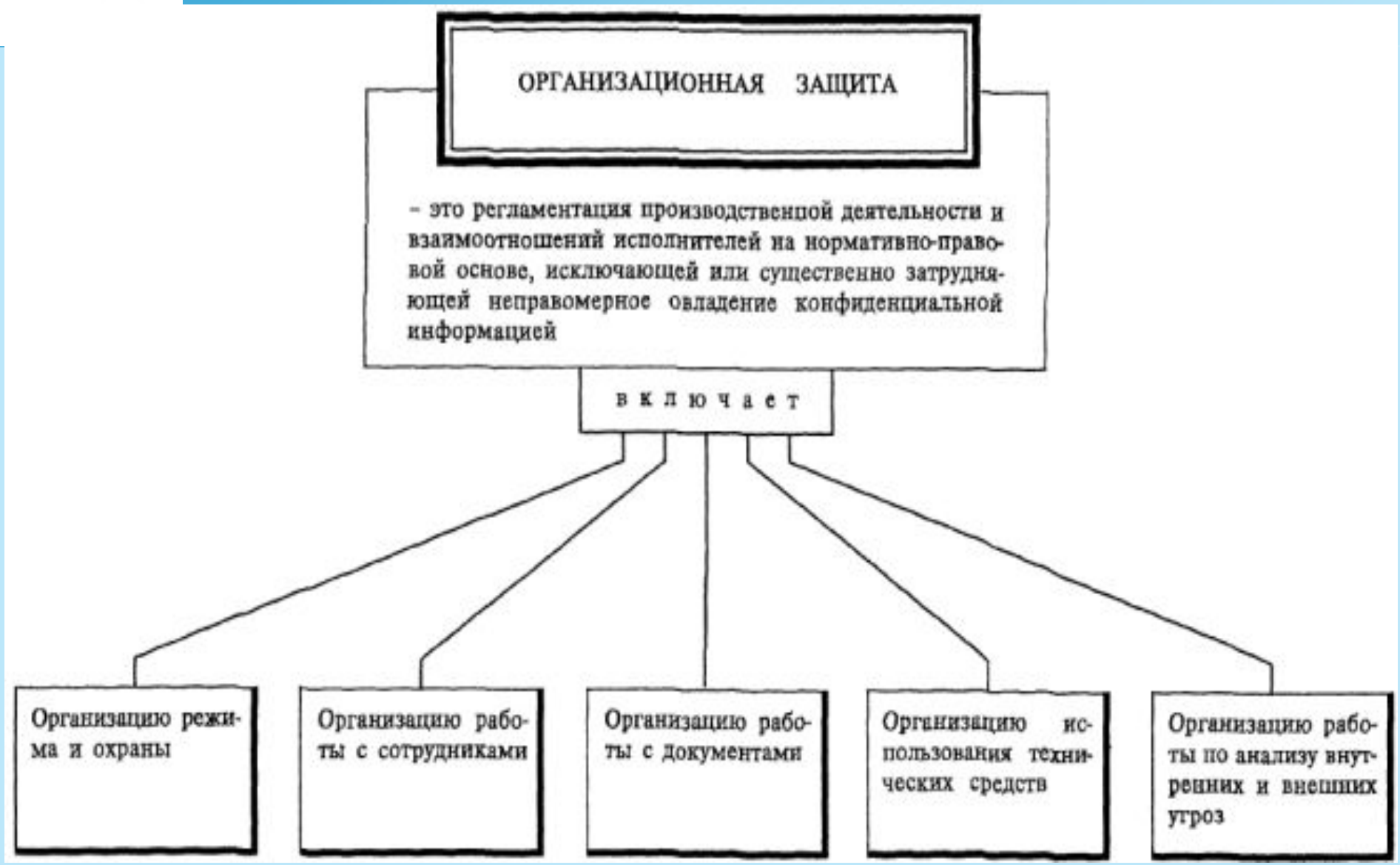
Ст. 361. Незаконное вмешательство в работу ЭВМ (компьютеров), АС, компьютерных сетей или сетей электросвязи.
Ст. 361-1. Создание с целью использования, распространения или сбыта вредных программ или технических средств, их распространение или сбыт.
Ст. 361-2. Несанкционированный сбыт или распространение информации с ограниченным доступом, которая хранится в ЭВМ (компьютерах), АС, компьютерных сетях или на носителях такой информации.
Ст. 362. Несанкционированные действия с информацией, которая обрабатывается в ЭВМ (компьютерах), АС, компьютерных сетях либо сохраняется на носителях такой информации, совершенные лицом, имеющем право доступа к ней.
Ст. 363. Нарушение правил эксплуатации ЭВМ (компьютеров), АС, компьютерных сетей и сетей электросвязи либо правил защиты информации, которая обрабатывается в них.
Ст. 363-1. Препятствование работе ЭВМ (компьютеров), АС, компьютерных сетей и сетей электросвязи путем массового распространения сообщений электросвязи.

Действия по защите информации от утечки по техническим каналам и несанкционированного доступа регламентируются документами: **«Временные рекомендации по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам побочных электромагнитных излучений и наводок. (ВР ЭВТ-95)»** и **«Временные рекомендации по технической защите информации от утечки по каналам побочных электромагнитных излучений и наводок. (ВР ЭВТ-95)»** (приказ ДСТСЗИ от 09.06.1995 г. № 25). **«НД ТЗИ 1.1-002-99 Общие положения по защите информации в компьютерных системах от несанкционированного доступа»** (приказ ДСТСЗИ от 28.04.1999 г. № 22) определяет методологические основы (концепцию) решения задач по защите информации в компьютерных системах и создания нормативных и методологических документов, регламентирующих вопросы определение требований относительно защиты компьютерных сетей от несанкционированного доступа; создание защищенных компьютерных систем и средств их защиты от НСД; оценки защищенности компьютерных систем и их пригодности для решения задач потребителя.

Организационная защита — регламентация служебной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение информацией ограниченного доступа и проявление внутренних и внешних угроз

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических и криптографических средств защиты и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз информационным ресурсам.


ОРГАНИЗАЦИОННАЯ ЗАЩИТА
– это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией
включает
Организацию режима и охраны
Организацию работы с сотрудниками
Организацию работы с документами
Организацию использования технических средств
Организацию работы по анализу внутренних и внешних угроз

Инженерно-техническая защита (ИТЗ) — совокупность технических средств и мероприятий по их использованию, направленных на предотвращение разглашения, утечки, несанкционированного доступа и других форм незаконного вмешательства в информационные ресурсы.


ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА
– совокупность специальных мер, персонала, технических средств, направленных на предотвращение разглашения, утечки, несанкционированного доступа и других форм незаконного вмешательства в информационные ресурсы
Классифицируется
По объектам воздействия
По характеру мероприятий
По способам реализации
По масштабу охвата
По классу технических средств защиты
По классу средств злоумышленника


КЛАССИФИКАЦИЯ
ИТЗ по используемым средствам
ФИЗИЧЕСКИЕ
Устройства, инженерные сооружения и организационные меры, затрудняющие или исключающие проникновение злоумышленников к источникам конфиденциальной информации
АППАРАТНЫЕ
Механические, электрические, электронные и др. устройства, предназначенные для защиты информации от утечки и разглашения и противодействия техническим средствам промышленного шпионажа
ПРОГРАММНЫЕ
Система специальных программ, включаемых в состав общего и специального обеспечения, реализующих функции защиты информации и сохранения целостности и конфиденциальности
КРИПТОГРАФИЧЕСКИЕ
Технические и программные средства шифрования
КОМБИНИРОВАННЫЕ
Совокупная реализация аппаратных и программных средств и криптографических методов защиты информации

Физические (инженерные) средства – включают различные устройства, инженерные сооружения и организационные меры, препятствующие физическому проникновению (или доступу) нарушителей на объекты защиты и к материальным носителям информации.

Аппаратные средства – механические, электрические, электронные и др. приборы, устройства, приспособления и иные технические решения, используемые в интересах защиты информации. Основная задача аппаратных средств — обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа, а также противодействие техническим средствам разведки.

Программные средства – специальные программы, программные комплексы и системы защиты информации, включаемые в состав общего и специального программного обеспечения информационных систем и средствах обработки данных, которые реализуют функции защиты информации, сохранение доступности, целостности, конфиденциальности и наблюдаемости.

Криптографические средства – специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Выводы

1. Информация — это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб.
2. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам.
3. Безопасность информационных ресурсов может быть обеспечена только комплексной системой защиты информации.

4. **Комплексная безопасность информационных ресурсов достигается использованием правовых актов государственного и ведомственного уровня, организационных мер и технических средств защиты.**
5. **Правовые меры обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников всех уровней и степени их ответственности за нарушения установленных норм и правил работы по обеспечению сохранности информации.**

6. **Организационные мероприятия являются решающим звеном в формировании и реализации комплексных мер защиты информации. Они, в первую очередь, выражаются в создании службы безопасности организации и обеспечении ее нормального функционирования.**
7. **Инженерно-техническая защита – это использование различных аппаратно-программных, криптографических и других средств в интересах обеспечения информационной безопасности.**

Дякую за увагу!