Глава 2
Концепция построения системы безопасности предприятия

1. Общая характеристика организационных методов защиты информации
2. Требования к построению систем безопасности предприятия
3. Концептуальная модель информационной безопасности
4. Виды объектов защиты
5. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии
6. Основные направления организационной защиты информации на предприятии

1. Общая характеристика организационных методов защиты информации

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе работы с информацией для обеспечения заданного уровня её безопасности.

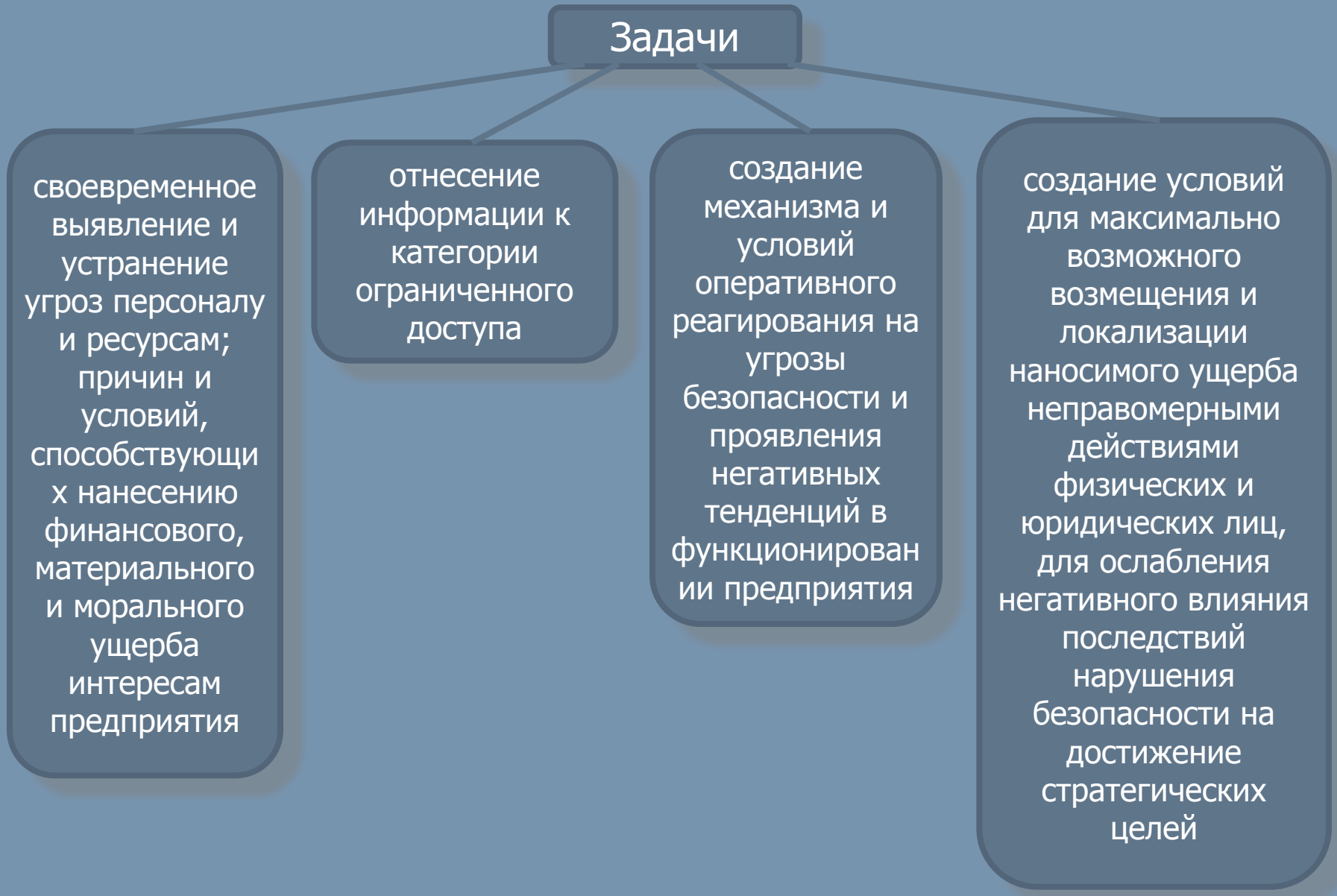
Организационная защита информации – это комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание системы защиты, побуждающих персонал соблюдать правила защиты конфиденциальной информации.

2. Требования к построению систем безопасности предприятия

При построении системы безопасности следует учитывать следующие рекомендации:

- Обеспечение безопасности не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких мест и потенциальных угроз фирме.
- Безопасность может быть обеспечена лишь при комплексном использовании всего арсенала средств защиты и противодействия во всех структурных элементах производственной системы и на всех этапах технологического цикла. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм – ***систему безопасности предприятия (СБП)***.
- Никакая СБП не может обеспечить требуемый уровень безопасности без надлежащий подготовки персонала предприятия и пользователей, соблюдения ими всех установленных правил, направленных на обеспечение безопасности.

Основные задачи системы безопасности



Принципы организации и функционирования системы безопасности

1. *Комплексность*
2. *Своевременность*
3. *Непрерывность*
4. *Активность*
5. *Законность*
6. *Обоснованность*
7. *Экономическая целесообразность*
8. *Специализация*
9. *Взаимодействие и координация*
10. *Совершенствование*
11. *Централизация управления*

Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных

Совершенствование. Предусматривает совершенствование мери

Предполагает самостоятельное функционирование системы безопасности по единым организационным, функциональным и методологическим принципам с централизованным управлением деятельностью системы безопасности.

3. Концептуальная модель информационной безопасности И

Трехмерная модель комплексной безопасности

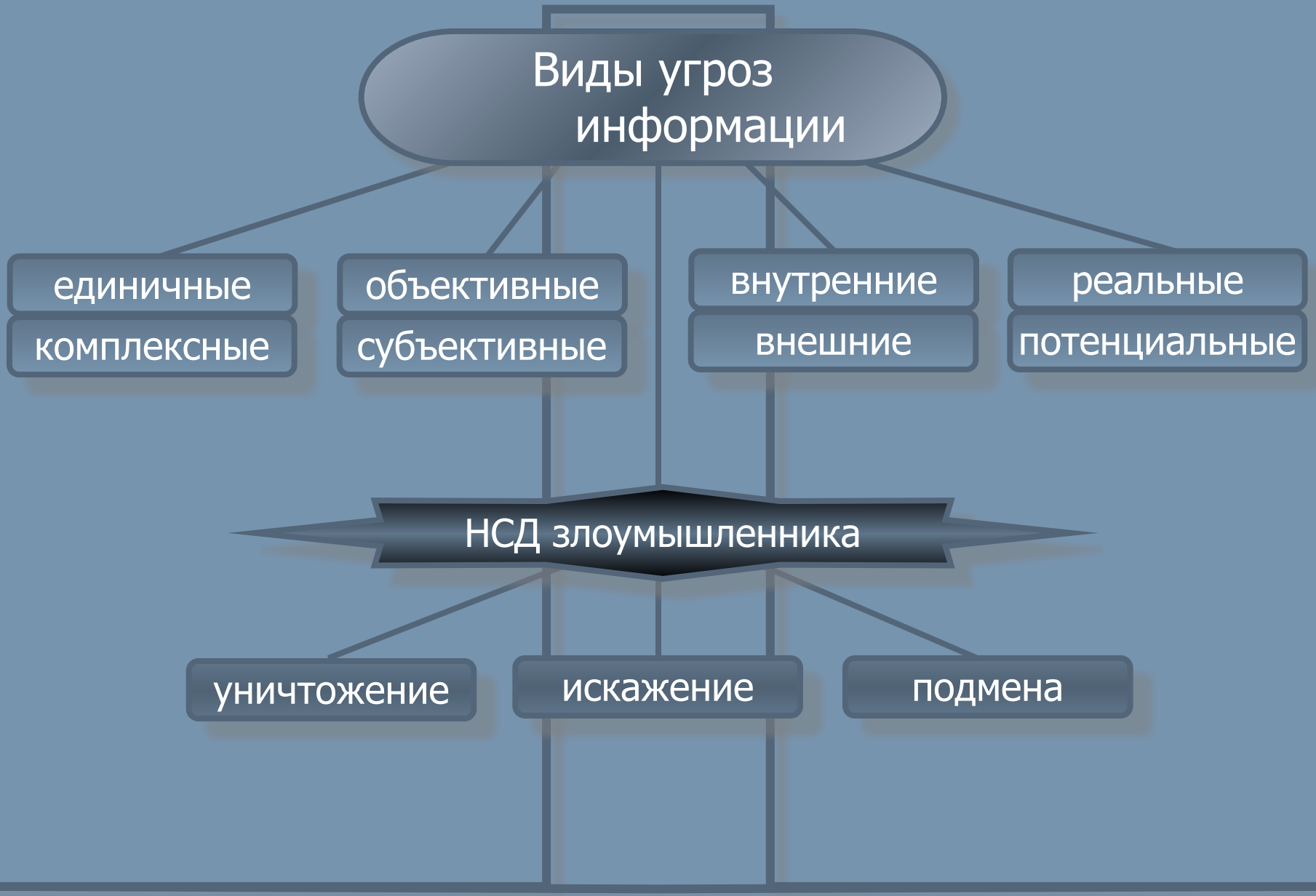
4. Виды объектов защиты

5. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии

Под **угрозой** или **опасностью утраты информации** понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемую информацию, документы и базы данных.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Виды угроз информации

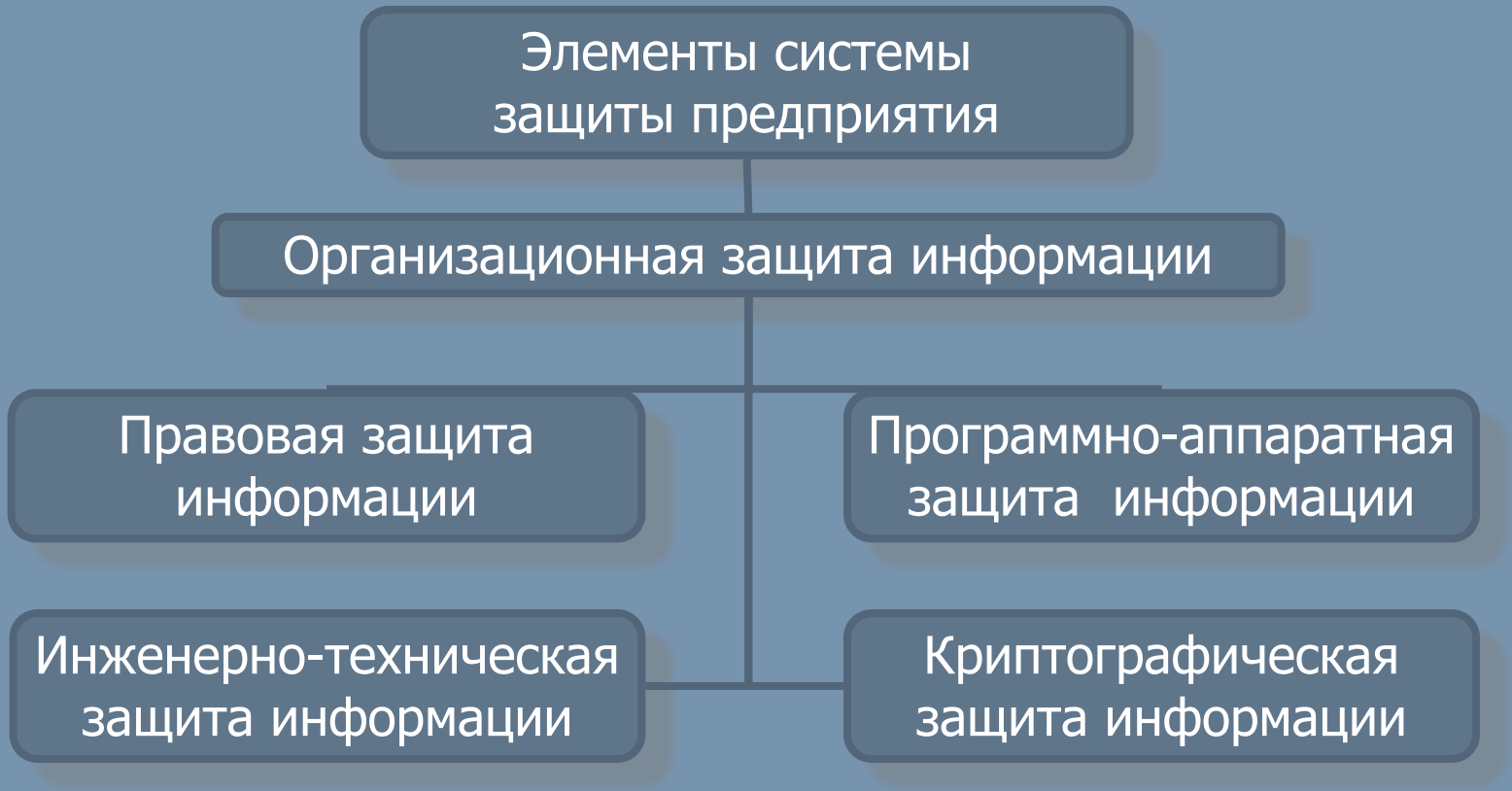


Возможные пути утраты информации

6. Основные направления организационной защиты информации на предприятии

Система защиты информации — это рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке.

Основные элементы системы защиты предприятия



Правовой элемент

- наличие в организационных документах предприятия, правилах внутреннего трудового распорядка, контрактах, заключаемых с сотрудниками, в должностных и рабочих инструкциях положений и обязательств по защите конфиденциальной информации;

- формулирование и доведение до сведения всех сотрудников предприятия (в том числе не связанных с конфиденциальной информацией) положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;

- разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

Организационный элемент

- порядка защиты информации при проведении совещаний, заседаний, переговоров, приеме посетителей, работе с представителями рекламных агентств, средств массовой информации;
- оборудования и аттестации помещений, рабочих мест, защищаемых для работы с конфиденциальной информацией;
- средств защиты информации и охраны, сертификации информационных систем, предназначенных для обработки защищаемой информации;
- пропускного режима на территории, в здании и помещениях предприятия, идентификации персонала и посетителей;
- системы охраны территории, здания, помещений, оборудования, транспорта и персонала предприятия;
- действий персонала в экстремальных ситуациях;
- организационных вопросов приобретения (установки и эксплуатации технических средств защиты информации);
- организационных вопросов защиты персональных компьютеров, информационных систем, локальных сетей;
- работы по управлению системой защиты информации;
- критериев и порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты информации.

- формирования и организации деятельности службы безопасности;
- составления и регулярного обновления перечня защищаемой информации и перечня лиц, допущенных к ней;
- ведения учета, составления и хранения перечня охраняемых бумажных, машиночитаемых и электронных документов предприятия;
- наличия разрешительной системы разграничения доступа персонала к защищаемой информации;
- использования методов отбора персонала для работы с защищаемой информацией, методики обучения и инструктирования сотрудников;
- формирования направлений и методов воспитательной работы с персоналом и контроля соблюдения сотрудниками порядка защиты информации;
- технологии защиты, обработки и хранения бумажных, машиночитаемых и электронных документов предприятия (автоматизированной и машинной технологии защиты электронных документов);
- порядка защиты сетей, информации предприятия от случайных или умышленных несанкционированных действий персонала;
- ведения всех видов аналитической работы;

Инженерно-технический элемент

- сооружения инженерной защиты от проникновения посторонних лиц на территорию, в здание и помещения (заборы, решетки, стальные двери, кодовые замки, идентификаторы, сейфы и др.);
- средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и других приборов и офисного оборудования, при проведении совещаний, заседаний, беседах с посетителями и сотрудниками, диктовке документов и т.п.;
- средства защиты помещений от визуальных способов технической разведки;
- средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, охранной и пожарной сигнализации);
- средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т.п.).

Программно-аппаратный элемент

- автономные программы, обеспечивающие защиту информации и контроль степени ее защищенности;
- программы защиты информации, работающие в комплексе с программами обработки информации;
- программы защиты информации, работающие в комплексе с техническими (аппаратными) устройствами защиты информации (прерывающими работу ЭВМ при нарушении системы доступа, стирающие данные при несанкционированном входе в базу данных и др.).

Криптографический элемент

- регламентацию использования различных криптографических методов в ЭВМ и локальных сетях;
- определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой, телеграфной, телетайпной, факсимильной и электронной связи;
- регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной и радио связи;
- регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами;
- регламентацию доступа персонала в выделенные помещение с помощью идентифицирующих кодов, шифров.

Контрольные вопросы

1. Что включают организационные методы защиты информации?
2. На что направлена деятельность по защите информации?
3. Какие задачи обеспечения информационной безопасности решаются на организационном уровне?
4. Что такое система безопасности предприятия?
5. На основе каких принципов осуществляется функционирование системы безопасности предприятия?
6. Каким требованиям должна удовлетворять система безопасности предприятия?
7. Что является компонентами комплексной модели информационной безопасности?
8. Перечислите виды объектов защиты.
9. Назовите возможные пути утраты информации.
10. Дайте характеристику основным элементы системы защиты предприятия.