

Тема лекции

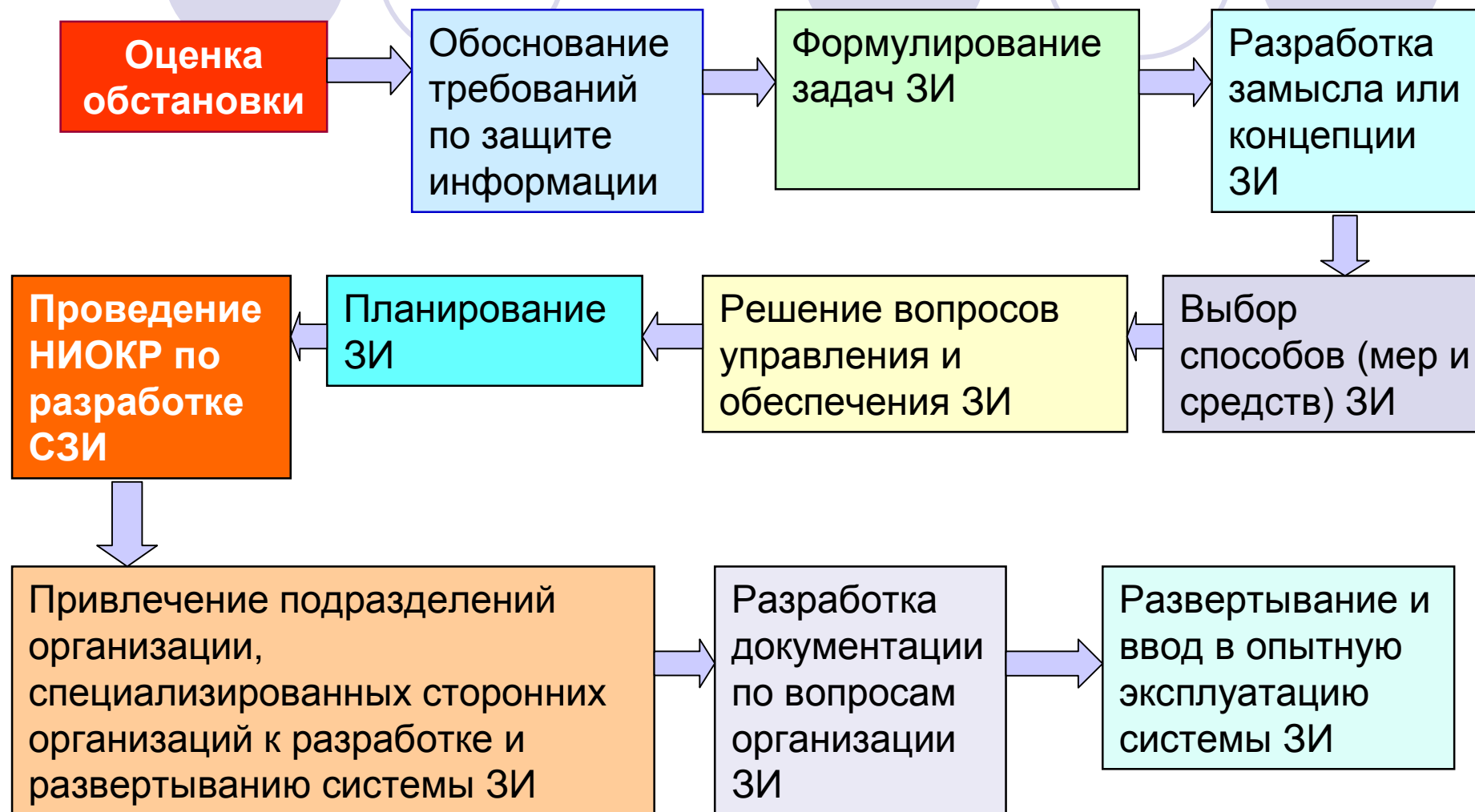
«Средства защиты компьютерной информации»

Цель лекции: ознакомление студентов с ролью физических и аппаратных средств защиты компьютерной информации

Принципы организации ЗИ

- **Принцип системности** предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ИТКС.
- **Принцип комплексности** предполагает согласованное применение разнородных средств при построении целостной системы защиты.
- **Принцип непрерывности** предполагает, что защита информации - это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер в ходе всего рассматриваемого периода защиты информации.
- **Разумная достаточность** предполагает то, что важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.
- **Принцип гибкости** системы защиты направлен на обеспечение возможности варьирования уровнем защищенности.
- **Принцип открытости алгоритмов и механизмов защиты** предполагает, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. При этом знание алгоритмов работы системы защиты не должно давать возможности ее преодоления.

Общий алгоритм организации ЗИ на объекте информатизации



Порядок организации ЗИ на этапе оценки обстановки



Понятия цели и задачи защиты информации

ЦЕЛЬ – предмет стремления, то, что надо, желательно осуществить.
(С.И. Ожегов. Толковый словарь.)

ЦЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ – желаемый ожидаемый результат защиты

ЗАДАЧА ЗАЩИТЫ ИНФОРМАЦИИ - ожидаемый результат проведения мероприятий по устранению, ослаблению, искажению и созданию ложных технических и демаскирующих признаков объекта защиты. ОСТ. (Некорректное определение, соответствует понятию «цель защиты»).

ЗАДАЧА ЗАЩИТЫ ИНФОРМАЦИИ – связанная по смыслу совокупность, по крайней мере, четырех характеристик:
<цели защиты>, <наименования объекта защиты>,
<времени защиты> и <требуемой эффективности защиты>

ЭФФЕКТИВНОСТЬ ЗАЩИТЫ – это степень достижения ожидаемого результата защиты

Порядок организации ЗИ на этапе определения задач защиты



Содержание замысла защиты информации

- Цель защиты;
- Основные требования по ЗИ, которые необходимо выполнить;
- Направления, на которых должны быть сосредоточены усилия по ЗИ (элементы объекта информатизации, блоки защищаемой информации, угрозы, которые должны быть парированы в первую очередь);
- Целесообразные стратегии, основные способы защиты информации на объекте информатизации и контроля ее эффективности;
- Предложения по распределению задач ЗИ между подразделениями организации, должностными лицами;
- Перечень программных и программно-аппаратных средств защиты и контроля, подлежащих применению, разработке (закупке);
- Основные вопросы управления, взаимодействия и обеспечения решения задач ЗИ.

Порядок организации ЗИ на этапе определения замысла защиты

Определение замысла защиты информации



Понятия стратегии защиты информации

СТРАТЕГИЯ - ученье о лучшем расположении и употреблении всех военных сил и средств (Словарь В.И. Даля).

СТРАТЕГИЯ – искусство планирования руководства, основанного на правильных и далеко идущих прогнозах (Словарь С.И. Ожегова)

СТРАТЕГИЯ ЗАЩИТЫ ИНФОРМАЦИИ- кратко выраженная основополагающая идея, определяющая характер проводимых мероприятий по защите информации и применения мер и средств защиты

Признаки разных стратегий защиты информации

1. Признак характера ожидаемого результата защиты. По этому признаку формируются стратегии защиты от преднамеренных угроз. При этом могут быть стратегии, направленные на обман нарушителя, на силовое его подавление, на маскировку защищаемого ресурса и др.
2. Признак превентивности защиты. По этому признаку могут быть сформированы стратегии, направленные на предупреждение возникновения и реализации той или иной угрозы безопасности информации, на игнорирование угроз с восстановлением целостности или доступности информации (для угроз целостности и доступности), на своевременное выявление и отслеживание факта реализации угрозы.
3. Признак активности защиты. По этому признаку стратегии разделяют на те, которые предполагают применение активных средств и мер защиты, которые основаны на пассивных мерах и средствах (в том числе организационных мерах), и те, которые основаны на сочетании активных и пассивных мер и средств защиты.
4. Признак адаптивности. По этому признаку стратегии защиты разделяют на адаптивные, то есть позволяющие варьировать состав мер и средств защиты в зависимости от складывающейся обстановки, и неадаптивные, когда все возможные изменения условий функционирования должны быть предусмотрены заранее.
5. Признак охвата. По этому признаку могут быть тотальные и выборочные стратегии.

Понятия концепции и доктрины обеспечения безопасности информации

КОНЦЕПЦИЯ (от латинского conceptio - понимание, система) - это определенный способ понимания, трактовки каких-либо явлений, основная точка зрения, руководящая идея для их освещения; ведущий замысел, конструктивный принцип различных видов деятельности.

КОНЦЕПЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ система взглядов на защиту информации, определяющая состав и характеристик возможных угроз безопасности информации, оценку состояния защищенности информации, совокупность возможных целей, стратегий защиты и условия их реализации, основные задачи и возможные (целесообразные) способы защиты информации, основные вопросы организации и обеспечения защиты информации.

ДОКТРИНА – это учение, научная концепция (С.И. Ожегов. Толковый словарь русского языка).

ДОКТРИНА представляет собой совокупность научно обоснованных официальных взглядов на цели, задачи, принципы и основные направления обеспечения защиты информации.

Содержание концепции защиты информации

- Краткая оценка состояния и обоснование необходимости защиты информации;
- Характеристика объектов защиты и актуальных угроз безопасности информации;
- Цель или цели защиты информации;
- Основные стратегии или принципы защиты информации;
- Замысел защиты или основные направления деятельности по защите информации (способы реализации выбранных стратегий);
- Основные (концептуальные) вопросы организации управления, связи и взаимодействия при выполнении мероприятий по защите информации;
- Систему взглядов на правовое, материальное, техническое, финансовое, научное, программное, кадровое и другие виды обеспечения и пути их развития в интересах достижения целей защиты информации;
- Достигаемые эффекты от реализации концепции

Определение способа защиты информации

Способ – действие или система действий, применяемые при выполнении какой-либо работы, при осуществлении чего-либо (С.И. Ожегов. Толковый словарь русского языка).

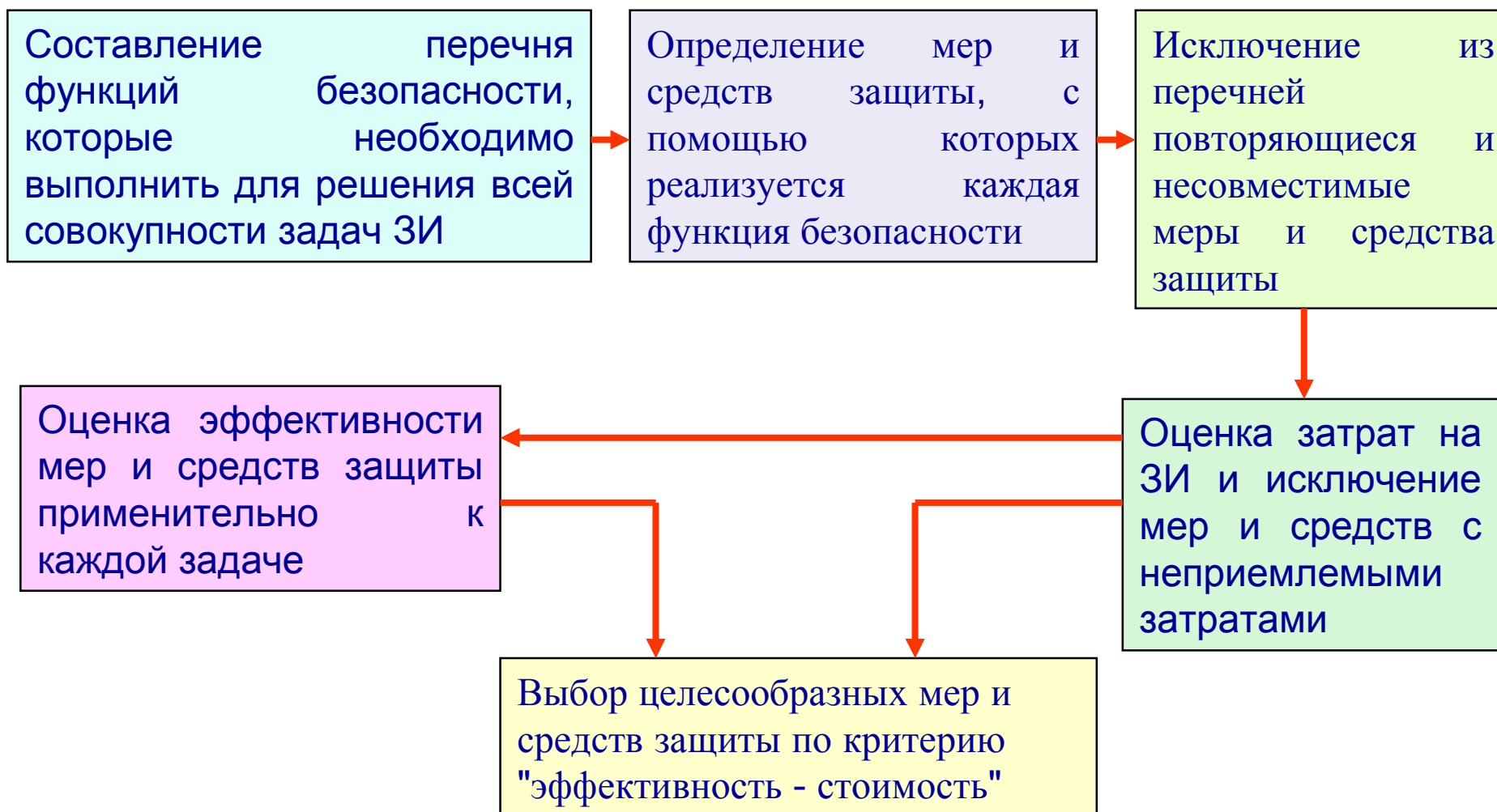
Способ защиты – совокупность мер и средств защиты и порядок их применения.

Способ защиты – прием или совокупность приемов защиты, отличающиеся характерным составом применяемых мер или средств или характерной последовательностью действий по защите.

Способ защиты – это прием или совокупность приемов решения задачи защиты.

Способ защиты – это способ решения задачи защиты.

Порядок выбора целесообразных мер и средств защиты



Документы по организации ЗИ на объекте информатизации

Утвержденный перечень сведений конфиденциального характера по каждому виду тайны

Акт и журнал инвентаризации информационных ресурсов

Акт категорирования защищаемой информации

Концепция ЗИ на предприятии

Положение о порядке организации и проведения работ по защите конфиденциальной информации

Модель угроз безопасности информации на объекте информатизации

План проведения мероприятий по ЗИ на объекте информатизации

План обеспечения ЗИ и взаимодействия

План или график проведения контрольных мероприятий

Понятие системы защиты информации на объекте информатизации

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА -

комплекс организационных мер и программных, физических, аппаратных, программно-аппаратных средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Понятие системы защиты информации на объекте информатизации (продолжение)

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ - совокупность физических, аппаратных, программных, и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ - совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно - распорядительными и нормативными документами в области защиты информации. ГОСТ Р 50922-96. Защита информации. Основные термины и определения



Подсистема защиты информации от НСД

Подсистема защиты от угроз физического доступа (контроля физического доступа)

Подсистема контроля доступа на территорию объекта и в помещения

Подсистема охранной сигнализации и наблюдения

Автоматизированные контрольно - пропускные пункты

Комплекс средств контроля и защиты от физического доступа к аппаратуре

Комплекс средств контроля вскрытия аппаратуры

Комплекс средств блокирования аппаратуры

Средства учета и уничтожения носителей

Комплекс средств физической аутентификации пользователей

Подсистема защиты от НСД к программной среде

Комплекс программных и программно-аппаратных средств разграничения доступа (в том числе криптозащиты, межсетевого экранирования, построения VPN-сетей и др.)

Программные средства блокирования несанкционированных действий, сигнализации и регистрации

Подсистема защиты от программно-математического воздействия

Средства повышения достоверности данных и надежности транзакций

Средства архивирования, резервного копирования

Программные средства обнаружения вторжений и сетевых атак

Подсистема защиты информации от утечки

Комплекс пассивных средств защиты

Средства локализации излучений

Экранирование
соединительных линий

Заземление экранов
соединительных линий

Меры и средства развязывания информационных сигналов

Спецсредства защиты от микрофонного
эффекта типа «Гранит»

Диэлектрические вставки

Автономные или стабилизированные
источники электропитания, устройства
гарантированного питания

Помехоподавляющие фильтры

Комплекс активных средств защиты

Пространственные средства зашумления

Генераторы шума и средства создания
прицельных по частоте помех

Генераторы акустического шума
(акустических и вибрационных помех)

Подавители диктофонов в режиме записи

Средства линейного зашумления

Для линий электропитания

Для посторонних проводников и
линий за пределами зоны

Специальные генераторы импульсов
для уничтожения закладных
устройств («выжигатели жучков»)

Подсистема управления защитой информации

Организационная подсистема

- Подсистема управления физическим доступом
- Служба безопасности и система администраторов
- Подсистема организационного контроля

Техническая подсистема

- Программные средства администрирования
- АРМ администратора
- Технические средства регистрации и учета
- Подсистемы обнаружения атак, вторжений и ликвидации их последствий

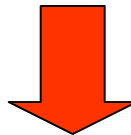
Подсистема технического контроля

Стадии создания системы ЗИ с проведением НИОКР

- **предпроектная стадия, включающую предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание;**
- **стадия проектирования (разработки проектов), включающая разработку СЗИ в составе объекта информатизации;**
- **стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации**

Предпроектная стадия - обследование объекта информатизации

- устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;
- определяется перечень сведений конфиденциального характера, подлежащих защите;
- определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта;
- определяются условия расположения объекта информатизации относительно границ КЗ;



Предпроектная стадия - обследование объекта информатизации (продолжение)

- **определяются конфигурация и топология АС и систем связи в целом и их отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;**
- **определяются технические средства и системы, предполагаемые к использованию в разрабатываемой АС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;**
- **определяются режимы обработки информации в АС в целом и в отдельных компонентах;**



Предпроектная стадия - обследование объекта информатизации (продолжение)

- **определяется класс защищенности АС;**
- **определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;**
- **определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации.**

Содержание аналитического обоснования необходимости создания СЗИ

- **информационная характеристика и организационная структура объекта информатизации;**
- **характеристика комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;**
- **возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;**
- **перечень предлагаемых к использованию сертифицированных средств защиты информации;**
- **обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;**
- **оценка материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;**
- **ориентировочные сроки разработки и внедрения СЗИ;**
- **перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.**

Содержание ТЗ на разработку СЗИ

- обоснование разработки;
- исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах;
- класс защищенности АС;
- ссылка на нормативно-методические документы, с учетом которых будет разрабатываться СЗИ и приниматься в эксплуатацию объект информатизации;
- требования к СЗИ на основе нормативно-методических документов и установленного класса защищенности АС;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения;
- перечень подрядных организаций-исполнителей видов работ;
- перечень предъявляемой заказчику научно-технической продукции и документации.

Состав оформляемых документов

На стадии ввода в действие объекта информатизации и СЗИ

- акты внедрения средств защиты информации по результатам их приемосдаточных испытаний;
- протоколы аттестационных испытаний и заключение по их результатам;
- аттестат соответствия объекта информатизации требованиям по безопасности информации.

Приказы, указания и решения:

- ☐ • на проектирование СЗИ и назначение ответственных исполнителей;
- ☐ • на проведение работ по защите информации;
- ☐ • о назначении лиц, ответственных за эксплуатацию объекта информатизации;
- ☐ • на обработку в АС (обсуждение в защищаемом помещении) конфиденциальной информации.

Содержание “Положения о порядке организации и проведения работ по защите конфиденциальной информации”

- порядок определения защищаемой информации;
- порядок привлечения подразделений организации, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и СЗИ, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;
- порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
- порядок разработки, ввода в действие и эксплуатацию объектов информатизации;
- ответственность должностных лиц за своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗИ