Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС

сборник учебно-методических материалов для направления подготовки

10.03.01 Информационная безопасность

Благовещенск, 2019

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
Университета

Составитель: Соловцова Л.А.

Комплексное обеспечение информационной безопасности АС: сборник учебно-методических материалов для направления подготовки 10.03.01 Информационная безопасность – Благовещенск: Амурский гос. ун-т, 2019.

Содержание

Краткое изложение лекционного материала.

Тема 1. Стадии и этапы проектирования Комплексной системы обеспечения информационной безопасности..

Цель лекции. Рассмотреть основные стадии и этапы проектирования комплексной системы обеспечения информационной безопасности.

План

1. Разработка технико-экономического обоснования создания комплексной системы обеспечения информационной безопасности автоматизированных систем.
2. Формирование требований по обеспечению безопасности конфиденциальной информации.
3. Разработка и утверждение технического задания на создание комплексной системы ОИБ. Разработка технического проекта.
4. Разработка и адаптация организационно-распорядительных документов по вопросам обеспечения информационной безопасности.
5. Ввод в действие систему.
6. Этап сопровождения системы защиты

Краткое содержание

1. Разработка технико-экономического обоснования создания комплексной системы обеспечения информационной безопасности автоматизированных систем. На данном этапе обосновывается необходимость и актуальность задачи обеспечения защиты информации в автоматизированных системах (АС), приводятся цели построения системы, производится ориентировочная оценка затрат, этапы и сроки проведения работ.

2. Формирование требований по обеспечению безопасности конфиденциальной информации. Для формирования требований используются руководящие документы Гостехкомиссии при президенте Российской Федерации, в том числе "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий" (ГОСТ Р ИСО/МЭК 15408-2002, "Common Critera") реализующего более современный подход к обеспечению информационной безопасности.

3. Разработка и утверждение технического задания на создание комплексной системы ОИБ. На этом этапе проводят разработку, оформление, согласование и утверждение технического задания на систему.

4. Разработка технического проекта. Разработка проектных решений по созданию комплексной системы по обеспечению информационной безопасности АС включает в себя обоснование и выбор решений по защите информации в АС, выбор состава средств защиты информации, определение мест размещения средств защиты, определение режимов функционирования и настроек средств защиты, определение необходимости доработки существующих средств защиты, либо разработки дополнительных, разработка порядка и этапов внедрения системы информационной безопасности, сметную стоимость работ.

5. Разработка и адаптация организационно-распорядительных документов по вопросам обеспечения информационной безопасности. Разработку организационно-распорядительных документов по вопросам обеспечения информационной безопасности АС предполагается производить путем адаптации разработанных типовых организационно-распорядительных документов, регламентирующих защиту АС в соответствии с разработанной технологией управления безопасностью.

6. Ввод в действие систему. На этом этапе осуществляется установка и настройка внедряемой системы защиты на площадке пользователя, а также проведение обучения персонала.

7. Этап сопровождения системы защиты, на котором проводятся консультации Заказчика по вопросам, связанным с эксплуатацией комплекса защиты.

В общем случае этапы и стадии создания АС приведены в ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания». Конкретный состав работ по каждому из вышеперечисленных этапов формируется исходя из характеристик автоматизированной системы Заказчика, а также состава проектируемой системы обеспечения информационной безопасности.

Тема 2. Типовая структура Комплексной системы обеспечения информационной безопасности от несанкционированного доступа

Цель лекции. Познакомиться с типовой структурой комплексной системы обеспечения информационной безопасности

План

Характеристика элементов Комплексной системы обеспечения информационной безопасности от несанкционированного доступа : организационный, правовой, инженерно-технический, программно-аппаратный и криптографический.

Краткое содержание

Основной характеристикой системы является ее **комплексность**, т.е. наличие в ней обязательных элементов, охватывающих все направления защиты информации. Элементами системы являются: организационный, правовой, инженерно-технический, программно-аппаратный и криптографический.

Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы. Эти меры связаны с установлением режима конфиденциальности в фирме.

Элемент включает в себя регламентацию:

- Формирования и организации деятельности службы безопасности и службы конфиденциальной документации (или менеджера по безопасности, или референта первого руководителя), обеспечения деятельности этих служб (сотрудника) нормативно-методическими документами по организации и технологии защиты информации;
- Составления и регулярного обновления состава (перечня, списка, матрицы) защищаемой информации фирмы, составления и ведения перечня (описи) защищаемых бумажных, машиночитаемых и электронных документов фирмы;
- Разрешительной системы (иерархической системы) разграничения доступа персонала к защищаемой информации;
- Методов отбора персонала для работ с защищаемой информацией, методики обучения и инструктирования сотрудников;
- Направлений и методов воспитательной работы с персоналом, контроля соблюдения сотрудниками порядка защиты информации;
- Технологии защиты, обработки и хранения бумажных, машиночитаемых и электронных документов фирмы (делопроизводственной, автоматизированиий и смешанной технологии); внемашинной технологии защиты электронных документов;
- Порядка защиты ценной информации фирмы от случайных или умышленных несанкционированных действий персонала;
- Ведения всех видов аналитической работы;

– Порядка защиты информации при проведении совещаний, заседаний, переговоров, приеме посетителей, работе с представителями рекламных агентств, средств массовой информации;

– Оборудования и аттестации помещений и рабочих зон, выделенных для работы с конфиденциальной информацией, лицензирования технических систем и средств защиты информации и охраны, сертификация информационных систем, предназначенных для обработки защищаемой информации;

– Пропускного режима на территории, в здании и помещениях фирмы, предназначенных для обработки защищаемой информации;

– Системы охраны территории, здания, помещений, оборудования, транспорта и персонала фирмы;

– Действий персонала в экстремальных ситуациях;

– Организационных вопросов приобретения, установки и эксплуатации технических средств зашиты информации и охраны;

– 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.

Правовой элемент системы защиты информации основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные собственником информации ограничительные и технологические меры защитного характера, а так же ответственности персонала за нарушение порядка защиты информации.

Этот элемент включает:

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

– формулирование и доведение до всех сотрудников фирмы (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.

Инженерно-технический элемент системы защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств. При защите информационных систем этот элемент имеет весьма важное значение, хотя стоимость средств технической защиты и охраны велика.

Элемент включает в себя:

– Сооружения физической (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.;

– Средств защиты помещений от визуальных способов технической разведки;

– Средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализации, информирования и идентификации);

– Средства противопожарной охраны;

– Средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т.п.);

– Технические средства контроля, предотвращающие вынос персоналом из помещений специально маркированных предметов, документов, дискет, книг и т.п.

Программно-аппаратный элемент системы защиты информации предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей и различных информационных системах. Однако фрагменты этой защиты могут применяться как сопутствующие средства в инженерно-технической и организационной защите.

Элемент включает в себя:

– 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 системы защиты информации предназначен для защиты конфиденциальной информации методами криптографии.

Элемент включает:

– 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 помещения с помощью идентифицирующих кодов, шифров

Тема 3. Последовательность работ при проектировании Комплексной системы обеспечения информационной безопасности от несанкционированного доступа.

Цель лекции. Изучить последовательность работ при проектировании комплексной системы обеспечения информационной безопасности

План

1. Анализ исходных данных о предмете защиты;
2. Классификация видов угроз,
3. Модель поведения нарушителя (способы и методы реализации угроз);
4. Анализ состояния защищенности информации в организации
5. Выбор средств защиты

Краткое содержание

Анализ исходных данных о предмете защиты;

Установить источники угроз, которые смогут воздействовать на предмет защиты;

Классифицировать виды угроз, которые при их реализации приведут к изменению качественных характеристик информационной безопасности (конфиденциальности, целостности, доступности);

Разработать вероятностную модель поведения нарушителя (способы и методы реализации угроз);

Провести анализ состояния защищенности информации в организации, выявить возможные каналы утечки, несанкционированного доступа к информации;

Выбрать средства защиты;

Обосновать критерии выбора оптимального варианта системы защиты информации (СЗИ);

Разработать комплекс рекомендаций по обеспечению информационной безопасности;

Внедрение и организация использования выбранных мер, способов и средств защиты;

Осуществление контроля целостности и управление системой защиты.

Тема 4. Предпроектное исследование системы безопасности

Цель лекции. Рассмотреть основные работы на этапе предпроектного исследованиясистемы безопасности.

План

1. Системный анализа соответствующих угроз безопасности
2. Кибернетический подход
3. Информационный подход

Краткое содержание

Классификация угроз безопасности информации

Следующий этап является решение проблемы организационного управления защитой информации в АСУ. Так, применение в АСУ современных вычислит. средств и новых технологий обработки информации могут не только повышать эффективность, но и снижать ее за счет появления новых угроз. Очевидно, что необходимо внедрять в такие АСУ соответствующие СЗИ, но при этом использование отдельных средств и механизмов защиты часто оказывается неэффективным без разработки соответствующего организационного управления ими. Суть такого управления заключается в принятии решений на выработку стратегий защиты на всех этапах обнаружения, анализа и компенсации деструктивного воздействия противника. Однако возрастающие требования по разработке и внедрению технологий управления СЗИ при проектировании новых и эксплуатации имеющихся АСУ противоречат существующему к настоящему времени состоянию комплексных научных исследований по организационному управлению защитой информации, которые бы позволяли адекватно решать задачи анализа и синтеза как самих СЗИ, так и процессов их функционирования. Наиболее практический интерес представляют задачи синтеза организационного управления защитой информации в следующей формулировке. При заданной структуре, характеристиках информационных потоков и решаемых в АСУ задач, характеристиках средств защиты информации, характеристиках множества угроз информации, определить значение структурных и функциональных показателей эффективности организационного управления СЗИ, при которых обеспечивается достижение максималь-

ной защищенности информации в АСУ на множестве заданных временных, технических, технологических ограничений.

В свою очередь обеспечение повышенной защищенности информации в сложных АСУ возможно только при комплексном решении научных задач организационного управления процессами защиты с позиции системного, кибернетического и информационного подходов. Основным содержанием системного подхода является разработка методов повышения защищенности информации с учетом исследования всех составляющих элементов обеспечения требуемой эффективности функционирования СЗИ как единой системы. Такая система в свою очередь является подсистемой общей системы автоматизированнонго управления. Основными методами системного подхода является системный, структурный и функциональный анализ. Системный анализ предполагает учет и классификацию всех аспектов и совокупности целей, связанных с назначением организ. управления системой защиты. Структурный анализ служит целям выявления организационных, топологических и информационных структур, связей в системе ЗИ.. Элементы структур представляются точками, узлами, массивами методами математических теорий графов, массового обслуживания, сетей и систем. Функциональный анализ используют для выявления функций системы защиты и и связей между ними. Функциональный анализ необходим для выработки гибких алгоритмов функционирования СЗИ.

Кибернетический подход распространяет методологию системных исследований на кибернетические подсистемы. С позиции данного подхода система защиты информации представляет собой совокупность органа управления (системы принятия рещения на защиту), объекта управления (механизмов защиты информации) и подсистемы информационного обеспечения (системы сбора информации о противнике). Основными принципами являются принцип единства управления и связи и принцип дуальности. Принцип единства и связи предполагает поиск связей, достаточных для реализации требуемых функций управления. Принцип дуальности утверждает, что информация, необходимая для управления объектами, добывается в ходе наблюдения в процессе управления.

Информационный подход определяет количественную меру неопределенности информации, благодаря чему оказывается возможным в разных организациях использовать одинаковый качественно-количественный аппарат теории информации. Информационный подход базируется на принципах отражения и неопределенности. Принцип отражения предполагает отображение структурно-функциональных свойств объектов информационного противоборства в соответствующей информационной модели.

Тема 5. Аттестация по требованиям безопасности

Цель лекции. Рассмотреть порядок аттестации объектов информатизации по требованиям безопасности.

План

1. Порядок организации и проведения аттестации объектов информатизации.
2. Работы, которые проводятся ходе аттестации объекта.
3. Обобщенная схема по проведению аттестационных испытаний объектов информатизации
4. Проверка организационно-распорядительной документации по защите информации.

Краткое содержание

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной

технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров [6.1].

Аттестация объектов информатизации (далее аттестация) - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России). Наличие аттестата соответствия в организации дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в аттестате.

Аттестация производится в порядке, установленном "Положением по аттестации объектов информатизации по требованиям безопасности информации" от 25 ноября 1994 года. Аттестация должна проводится до начала обработки информации, подлежащей защите. Это необходимо в целях официального подтверждения эффективности используемых мер и средств по защите этой информации на конкретном объекте информатизации.

Аттестация является обязательной в следующих случаях:

- государственная тайна;
- при защите государственного информационного ресурса;
- управление экологически опасными объектами;
- ведение секретных переговоров.

Во всех остальных случаях аттестация носит добровольный характер, то есть может осуществляться по желанию заказчика или владельца объекта информатизации.

Аттестация предполагает комплексную проверку (аттестационные испытания) объекта информатизации в реальных условиях эксплуатации. Целью является проверка соответствия применяемых средств и мер защиты требуемому уровню безопасности. К проверяемым требованиям относится:

- защита от НСД, в том числе компьютерных вирусов;
- защита от утечки через ПЭМИН;
- защита от утечки или воздействия информацию за счет специальных устройств, встроенных в объект информатизации.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом, и состоит из следующего перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Органы по аттестации должны проходить аккредитацию ФСТЭК в соответствии с "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".

Все расходы по проведению аттестации возлагаются на заказчика, как в случае добровольной, так и обязательной аттестации.

Органы по аттестации несут ответственность за выполнение своих функций, за сохранение в секрете информации, полученной в ходе аттестации, а также за соблюдение авторских прав заказчика.

В структуру системы аттестации входят:

– федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации – ФСТЭК России;

– органы по аттестации объектов информатизации по требованиям безопасности информации;

– испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;

– заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

В качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов информатизации.

В качестве органов по аттестации могут выступать отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию.

Органы по аттестации:

– аттестуют объекты информатизации и выдают "Аттестаты соответствия";

– осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;

– отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";

– формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

– ведут информационную базу аттестованных этим органом объектов информатизации;

– осуществляют взаимодействие с ФСТЭК России и ежеквартально информируют его о своей деятельности в области аттестации.

ФСТЭК осуществляет следующие функции в рамках системы аттестации:

– организует обязательную аттестацию объектов информатизации;

– создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;

– устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;

– организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;

– аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;

– осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;

– рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации;

– организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

Испытательные лаборатории проводят испытания несертифицированной продукции, используемой на аттестуемом объекте информатизации.

Со списком органов по аттестации и испытательных лабораторий, прошедших аккредитацию, можно ознакомиться на официальном сайте ФСТЭК России в разделе "Сведения о Системе сертификации средств защиты информации по требованиям безопасности информации".

Заявители:

– проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

– привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;

– предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;

– привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

– осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";

– извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");

– предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

Для проведения испытаний заявитель предоставляет органу по аттестации следующие документы и данные:

– приемо-сдаточную документацию на объект информатизации;

– акты категорирования выделенных помещений и объектов информатизации;

– инструкции по эксплуатации средств защиты информации;

– технический паспорт на аттестуемый объект;

– документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;

– сертификаты соответствия требованиям безопасности информации на ВТСС;

– сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;

– акты на проведенные скрытые работы;

– протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);

– протоколы измерения величины сопротивления заземления;

– протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;

– данные по уровню подготовки кадров, обеспечивающих защиту информации;

– данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;

– нормативную и методическую документацию по защите информации и контролю эффективности защиты.

Приведенный общий объем исходных данных и документации может уточняться заявителем в зависимости от особенностей аттестуемого объекта информатизации по согласованию с аттестационной комиссией.

– пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;

– перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;

– перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;

– перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;

– перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;

– перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;

– схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;

– технологические поэтажные планы здания с указанием мест расположения объектов информатизации и выделенных помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;

– планы объектов информатизации с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;

– план-схему инженерных коммуникаций всего здания, включая систему вентиляции;

– план-схему системы заземления объекта с указанием места расположения заземлителя;

– план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;

– план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;

– план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;

– схемы систем активной защиты (если они предусмотрены)[6.3].

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

– подача и рассмотрение заявки на аттестацию. Заявка имеет установленную форму, с которой можно ознакомиться в "Положении об аттестации объектов информатизации по требованиям безопасности". Заявитель направляет заявку в орган по аттестации, который в месячный срок рассматривает заявку, выбирает схему аттестации и согласовывает ее с заявителем.

– предварительное ознакомление с аттестуемым объектом – производится в случае недостаточности предоставленных заявителем данных до начала аттестационных испытаний;

– испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

– разработка программы и методики аттестационных испытаний. Этот шаг является результатом рассмотрения исходных данных и предварительного ознакомления с аттестуемым объектом. Орган по аттестации определяет перечень работ и их продолжительность, методику испытаний, состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или участия испытательных лабораторий. Программа аттестационных испытаний согласовывается с заявителем.

– заключение договоров на аттестацию. Результатом предыдущих четырех этапов становится заключение договора между заявителем и органом по аттестации, заключением договоров между органом по аттестации и привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

– проведение аттестационных испытаний объекта информатизации. В ходе аттестационных испытаний выполняется следующее:

– анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

– определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

– проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

– проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

– проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

– оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации[6.2]

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протокол аттестационных испытаний должен влючать:

– вид испытаний;

– объект испытаний;

– дату и время проведения испытаний;

– место проведения испытаний;

– перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);

– перечень нормативно-методических документов, в соответствии с которыми проводились испытания;

– методику проведения испытания (краткое описание);

– результаты измерений;

– результаты расчетов;

– выводы по результатам испытаний

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов.

Заключение по результатам аттестации подписывается членами аттестационной комиссии, утверждается руководителем органа аттестации и представляется заявителю . Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

– оформление, регистрация и выдача "Аттестата соответствия" (если заключение по результатам аттестации утверждено).

– осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;

– рассмотрение апелляций. В случае, если заявитель не согласен с отказом в выдаче "Аттестата соответствия", он может подать апелляцию в вышестоящий орган по аттестации или в ФСТЭК. Апелляция рассматривается в срок, не превышающий один месяц с привлечением заинтересованных сторон.

Аттестат соответствия должен содержать:

– регистрационный номер;

– дату выдачи;

– срок действия;

– наименование, адрес и местоположение объекта информатизации;

– категорию объекта информатизации;

– класс защищенности автоматизированной системы;

– гриф секретности (конфиденциальности) информации, обрабатываемой на объекте информатизации;

– организационную структуру объекта информатизации и вывод об уровне подготовки специалистов по защите информации;

– номера и даты утверждения программы и методики, в соответствии с которыми проводились аттестационные испытания;

– перечень руководящих документов, в соответствии с которыми проводилась аттестация;

– номер и дата утверждения заключения по результатам аттестационных испытаний;

– состав комплекса технических средств обработки информации ограниченного доступа, перечень вспомогательных технических средств и систем, перечень технических средств защиты информации, а также схемы их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств;

– организационные мероприятия, при проведении которых разрешается обработка информации ограниченного доступа;

– перечень действий, которые запрещаются при эксплуатации объекта информатизации;

– список лиц, на которых возлагается обеспечение требований по защите информации и контроль за эффективностью реализованных мер и средств защиты информации.

Аттестат соответствия подписывается руководителем аттестационной комиссии и утверждается руководителем органа по аттестации.

Аттестат соответствия выдается на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Тема 6. Концепция Комплексной системы обеспечения информационной безопасности.

Цель лекции. Рассмотреть концепцию комплексной системы обеспечения информационной безопасности..

План

1. Основные принципы построения.
2. Многоуровневая Комплексная система обеспечения информационной безопасности.
3. Блочная архитектура комплексной система обеспечения

Краткое содержание

Тема 7. Требования к эксплуатационной документации Комплексной системы обеспечения информационной безопасности.

Цель лекции. Рассмотреть Требования к эксплуатационной документации комплексной системы обеспечения информационной безопасности.

План

1. Инструкции эксплуатации КСЗИ и ее элементов;
2. Процедуры регламентного обслуживания КСЗИ;
3. Правила и положения по проведению тестирования и анализа работы КСЗИ

Краткое содержание

Тема 8. Организационное управление защитой информации. Организационно-функциональные задачи службы безопасности.

Цель лекции. Рассмотреть проблемы организационное управление защитой информации

План

1. Организационно-технические и организационно-правовые мероприятия.
2. Мероприятия, осуществляемые при создании системы обработки, накопления, хранения и передачи данных заключающиеся в учете требований защиты

Краткое содержание

Тема 9. Моделирование угроз информационной безопасности и защиты.

Цель лекции. Рассмотреть процессы моделирования угроз информационной безопасности и защиты..

План

1. Моделирование технических каналов утечки информации.

2. Моделирование способов физического проникновения злоумышленника к источникам информации.

Краткое содержание

Создание модели технических каналов утечки предполагает выявление и структурирование всех угроз безопасности защищаемой информации, возникающих при применении злоумышленником различных технических средств съема информации, с целью определения наиболее вероятных путей утечки и прогнозирования значений ущерба при различных сценариях развития информационных угроз.

Необходимо рассмотреть как можно более полный спектр технических каналов утечки защищаемой информации. Для этого нужно рассмотреть функционирование всех технических средств обработки информации, оконечные устройства, являющиеся источниками защищаемой информации, линии передачи конфиденциальной информации. Также необходимо проанализировать и работу вспомогательных технических систем - распределительных и коммутационных устройств, систем электропитания, заземления, технических средств открытой телефонной, факсимильной, громкоговорящей связи, систем охранной и пожарной сигнализации и т. д. В качестве каналов утечки интерес представляют металлические трубы систем отопления, водоснабжения, другие токопроводящие металлоконструкции, находящиеся в эффективной области действия ПЭМИН, несущих интересующую злоумышленника информацию. Особое внимание необходимо уделять линиям коммуникаций, выходящим за пределы охраняемой территории.

Также необходимо изучить возможности получения злоумышленником конфиденциальной информации из разговоров сотрудников, служебных документов, паров лабораторных образцов путем акустического, визуального или химического контроля соответствующих помещений.

При моделировании технических каналов утечки, для каждого канала указывается источник (передатчик) сигнала, путь утечки, а также производится оценка реальности канала, величины и ранга информационной угрозы, возникающей при использовании данного канала.

Методические указания к лабораторным занятиям

Лабораторная работа №1

Разработка технико-экономического обоснования на создания комплексной системы обеспечения информационной безопасности автоматизированных систем.

Цель работы: Получить навыки разработки технико-экономического обоснования на создания комплексной системы обеспечения информационной безопасности автоматизированных систем.

.

Задание

1. Выполнить анализ деятельность предложенного объекта (система защиты конфиденциальной информации вуза, детского образовательного центра, медицинского учреждения, страховой компании, промышленного предприятия).
2. Подготовить исходные данные для технико-экономического обоснования
3. Определить объемы и состав работ, подготовить сметы и сроков их выполнения.

Контрольные вопросы

1. Что такое технико-экономическое обоснование?
2. Какие действия выполняются на этапе анализа деятельности?
3. Какие расчеты должны быть выполнены на этапе технико-экономического обоснования.
4. Привести примеры уязвимости информационной безопасности.
5. Что такое комплексная система обеспечения информационной безопасности автоматизированных систем?
6. По каким признакам выполняется классификация уязвимостей безопасностей?
7. Какие уязвимости относятся к субъективным уязвимостям?
8. Как выполняется идентификация уязвимостей?
9. Какой математический аппарат используется для описания и расчета уязвимостей?
10. Что такое уровень уязвимости и как он оценивается?

Лабораторная работа №2

Формирование требований по обеспечению безопасности конфиденциальной информации

Цель работы: Получить практические умения формирования требований по обеспечению безопасности конфиденциальной безопасности.

Задание

1. Сформулировать угрозы безопасности для предложенного объекта (система защиты конфиденциальной информации вуза, детского образовательного центра, медицинского учреждения, страховой компании, промышленного предприятия).

2. Сформулировать требования по обеспечению безопасности конфиденциальной безопасности.

Контрольные вопросы

1. Какие основные виды политики безопасности известны?
2. В чем суть дискреционной политики безопасности?
3. Какими условиями определяется мандатная политика безопасности?
4. Чем отличается политика безопасности информационных потоков от политики ролевого разграничения доступа?
5. Какова цель реализации политики изолированной программной среды?
6. Перечислить классические угрозы безопасности?
7. Перечислить основные требования по обеспечению безопасности конфиденциальной безопасности.

Лабораторная работа №3

Разработка и утверждение технического задания на создание комплексной системы обеспечения информационной безопасности.

Цель работы: Получить навыки разработки и использования технического задания на создание комплексной системы обеспечения информационной безопасности..

Задание

1. Изучить нормативные документы, на основе которых выполняется построение технического задания.
2. Разработать техническое задание на создание комплексной системы обеспечения информационной безопасности для предложенного объекта (система защиты конфиденциальной информации вуза, детского образовательного центра, медицинского учреждения, страховой компании, промышленного предприятия)..
3. Оформить титульный лист с указанием лиц, утверждающих техническое задание

Контрольные вопросы

1. Что такое техническое задание.
2. Какие нормативные документы используются для разработки технического задания?
3. Кто подписывает техническое задание?
4. Из каких разделов состоит техническое задание?
5. Какие существуют виды конфиденциальности?

Лабораторная работа №4

Проектировании комплексной системы обеспечения информационной безопасности от несанкционированного доступа

Цель работы: Получить навыки проектировании комплексной системы обеспечения информационной безопасности от несанкционированного доступа

Задание

1. Построить диаграмму функционирования комплексной системы обеспечения информационной безопасности от несанкционированного доступа для предложенного объекта (система защиты конфиденциальной информации вуза, детского образовательного центра, медицинского учреждения, страховой компании, промышленного предприятия).
2. Построить диаграммы прецедентов, состояний, взаимодействия на языке UML для проекта комплексной системы обеспечения информационной безопасности от несанкционированного доступа.

Контрольные вопросы

1. Перечислить программные продукты для выполнения лабораторной работы.
2. Для построения каких диаграмм, используется языкUML?
3. Что представляют собой функциональные подсистемы комплексной системы обеспечения информационной безопасности?
4. Что представляют собой обеспечивающие подсистемы комплексной системы обеспечения информационной безопасности?
5. Для каких целей выполняется построения диаграммы прецедентов?
6. Какие диаграммы строятся для описания взаимодействия системы с пользователями?

Лабораторная работа №5

Разработка блочная архитектуры комплексной система обеспечения информационной безопасности

Цель работы: Получить навыки разработки блочная архитектуры комплексной система обеспечения информационной безопасности

Задание

1. Для комплексной системы обеспечения информационной безопасности для предложенного объекта (система защиты конфиденциальной информации вуза, детского образовательного центра, медицинского учреждения, страховой компании, промышленного предприятия) выполнить разработку блочной архитектуры.
2. Выполнить детализацию для каждого блока.

Контрольные вопросы

1. Перечислить виды архитектур комплексной системы обеспечения информационной безопасности.
2. Что представляет собой блочная архитектура?
3. Что такое разграничение доступа?
4. Что представляет собой многоуровневая архитектура?
5. Выполнить сравнение архитектур?
6. Что такое шифрование, криптография?
7. Какие существуют виды конфиденциальности?

Лабораторная работа №6

Моделирование угроз информационной безопасности и защиты

Цель работы: Получить навыки моделирования угроз информационной безопасности

Задание

1. Выполнить. разработку частной модели угроз и модели нарушителя информационной безопасности для предложенного объекта (система защиты конфиденциальной информации вуза, детского образовательного центра, медицинского учреждения, страховой компании, промышленного предприятия).
2. Выбрать и обосновать выбор методики построения модели угроз.
3. Построить модель угроз в соответствии с выбранной методикой.
4. Разработать алгоритм для реализации модели угроз.

Контрольные вопросы

1. Что такое модель угроз.
2. Какие существуют методики построения модели угроз?
3. Какая методика используется для моделирования угроз безопасности персональных данных ?
4. В чем суть методики идентификации угроз – «Дерево угроз»?
5. Из каких этапов состоит методика идентификации угроз «шаблоны типовых атак»?

Методические указания к практическим занятиям;

Практическое занятие №1
Разработка и утверждение технического задания на создание комплексной системы обеспечения информационной безопасности.

Цель занятия. Изучение основных понятий и определений, связанных с дисциплиной..

Задание

1. Сформулировать основные понятия и определения известные из других дисциплин.
2. Выполнить классификацию методов защиты информации.
3. Построить глоссарий по теме

Контрольные вопросы

1. Что такое информационная безопасность?
2. Перечислить виды угроз.
3. Назвать методы защиты информации?
4. Раскрыть понятие компьютерное преступление.
5. Что такое конфиденциальность информации?
6. Что такое целостность данных?
7. Что такое доступность данных?
8. В каком случае информация считается защищенной?
9. Назвать источники информации, требующие защиты?
10. Что относится к способам получения доступа к информации?

Практическое занятие №2
Разработка технического проекта для комплексной системы обеспечения информационной безопасности

Цель занятия. Изучение вопросов разработки технического проекта для комплексной системы обеспечения информационной безопасности.

Задание

Задание 1. В соответствии с функциями СФЗ и опираясь на результаты анализа угроз и каналов утечки информации на заданном объекте, необходимо построить структурные схемы:

– подсистемы обнаружения: датчики, извещатели;

– подсистемы задержки: ограждения, замки и т.д.;

– подсистемы реагирования: сигнализация, индикация, оповещения, организация сил охраны.

Затем разработать комплексную структурную схему системы физической защиты.

Задание 2.Разработать функциональную спецификацию системы физической защиты по образцу таблицы

Таблица - Функциональная спецификация системы физической защиты

№	Функция	Средство
1	Обнаружение нарушения периметра	Периметральный датчик
2	Обнаружение движущегося объекта	Датчик движения
3	Задержка прохода	Турникет

Задание 3.Осуществить выбор необходимых приборов и оборудования для обеспечения функций СФЗ. Составить спецификацию.

Построить модель защиты информации от утечки по техническим каналам по образцу таблицы.

Таблица - Модель защиты информации от утечки по техническим каналам

№ п\п	Место установки	Позиционное место установки устройств съема информации	Тип (индекс) устройства съема информации	Способ применения	Технический канал закрытия утечки информации
1.	Рабочий стол руководителя объекта защиты	С1:5	Генератор шума «Гром ЗИ – 4»	Постоянно	Радиоэлектронный
2.	ПЭВМ кабинета №3	V1:13	Генератор шума «ГШ-К-1000М»	Постоянно	Радиоэлектронный
3.	Помещение секретного отделения	Т6	Генератор шума «Купол-W-ДУ»	Постоянно	Радиоэлектронный
4.	Розетка 220 В. Кабинет руководителя объекта защиты	Х1:10	Генератор шума «SEL SP-41/C»	По решению руководства	Радиоэлектронный

Задание 4.Разработать план размещения приборов и оборудования на заданном объекте.

Контрольные вопросы

1. Дать определение и перечислить задачи системы контроля и управления доступом.
2. Назвать задачи и функции подсистемы обнаружения.
3. Дать определение и назвать средства контроля и управления доступом. Перечислить решаемые задачи.
4. Что такое периметральная защита, какие средства её реализуют?
5. Назовите основные классы периметральных датчиков. На чем основан их принцип работы.
6. Назовите средства реагирования и меры по их организации.

Практическое занятие №3

Разработка и адаптация организационно-распорядительных документов по вопросам обеспечения информационной безопасности

Цель занятия. Научиться выполнять разработку и адаптацию организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

Задание

Для выбранного объекта защиты составить структурную модель защищаемой информации. Структурирование производится путем классификации защищаемой информации в соответствии с функциями, задачами и дальнейшей привязкой элементов информации к их носителям. Пример структурной модели приведен на рисунке 2.1.

Провести классификацию и структурирование информации в соответствии с функциями, задачами и структурой организации, в результате чего защищаемая информация должна быть представлена в виде отдельных элементов информации.

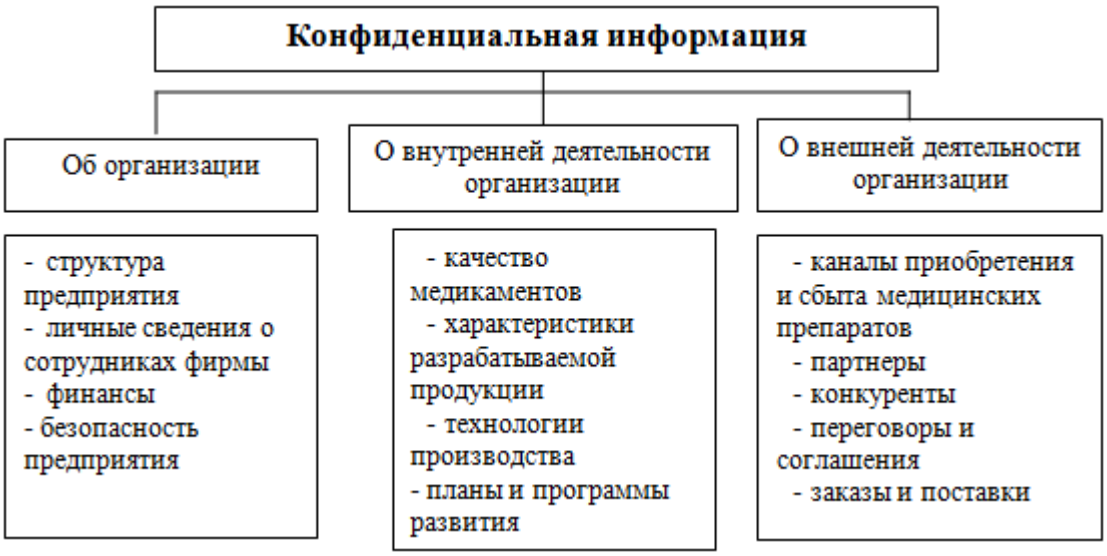

Рисунок 1 – Пример структурной модели конфиденциальной информации

Контрольные вопросы

1. Что такое уязвимость информации?
2. Какие злоумышленные действия характерны для СОД?
3. Назвать виды уязвимости информации.
4. Привести примеры уязвимости информационной безопасности.
5. Что такое уязвимость нулевого дня?
6. По каким признакам выполняется классификация уязвимостей безопасностей?
7. Какие уязвимости относятся к субъективным уязвимостям?
8. Как выполняется идентификация уязвимостей?
9. Какой математический аппарат используется для описания и расчета уязвимостей?
10. Что такое уровень уязвимости и как он оценивается?

Практическое занятие №4
Установка источников угроз, которые смогут воздействовать на предмет защиты

Цель занятия. Научиться выполнять установку источников угроз, которые смогут воздействовать на предмет защиты

Задание

1. Составить перечень угроз для заданного объекта по образцу таблицы 1.

Таблица 1 - Перечень угроз

№ угрозы	Источник угрозы	Среда распространения	Носитель информации

2. Провести анализ потенциальных каналов утечки на указанном объекте.Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу таблицы 2.

Таблица 2 - Перечень потенциальных каналов утечки информации

Каналы утечки информации с объекта защиты			Место расположения
1.	Оптический канал	Окно со стороны проспекта	каб. №1
		Окно со стороны проспекта	каб. №2
		Окно со стороны проспекта	каб. №3
2.	Радиоэлектронный канал	Стоянка автотранспорта на просп.	указать
		Система часофикации	указать
		Телефон	указать
		Розетки	указать
		ПЭВМ	указать
		Воздушная линия электропередачи	указать
		Система оповещения	указать
		Система пожарной сигнализации	указать
3.	Акустический канал	Теплопровод подземный	указать
		Водопровод подземный	указать
		Стены помещения	указать
		Батареи	указать
		Окна контролируемого помещения	указать
4.	Материально-вещественный канал	Документы на бумажных носителях	указать
		Персонал предприятия	указать
		Производственные отходы	указать

Контрольные вопросы

1. Назовите и кратко охарактеризуйте основные принципы построения системы защиты.
2. Что такое контролируемая зона, на какие типы подразделяются зоны, привести примеры.
3. Какие преимущества дает многозональность организации системы защиты?
4. Какие факторы определяют надежность системы безопасности?
5. Что такое адаптируемость системы безопасности?
6. В чем заключается принцип гибкости системы защиты объекта?
7. Дать определение и назвать средства контроль и управление доступом.

Практическое занятие №5
Разработка вероятностной модели поведения нарушителя (способы и методы реализации угроз)

Цель занятия. Изучить основные методы разработки вероятностной модели поведения нарушителя (способы и методы реализации угроз).

.

Задание

1. Провести анализ вероятных внешних и внутренних нарушителей.
2. Построить модель вероятного нарушителя (внешнего и внутреннего) на основе моделей угроз и утечки информации, а также граф-структуры защищаемой информации, разработанной в лабораторной работе

Контрольные вопросы

1. Что является исходными данными для проведения оценки и анализа угроз безопасности объектов?

2 Дать определение нарушителя, по каким критериям они классифицируются?

3 Дать определение технического канала утечки информации, назвать типы.

4 Дать определение носителя защищаемой информации, назвать типы.

5 Какие сведения включает пространственная модель каналов утечки?

6 Что такое формализованная и неформализованная модель нарушителя?

7 Перечислите цели и задачи вероятного нарушителя.

8 Какое оборудование относят к виброакустические каналам утечки информации?

9 Дать описание четырех категорий нарушителя.

10 Что представляет собой матрица угроз/средств защит и матрица вероятностей наступления угроз?

1.