МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
_____ И.М. Ажмухамедов
«06» июня 2024 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой ИБ
_____ Т.Г. Гурская
от «06» июня 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Комплексное обеспечение защиты информации объекта информатизации

Составитель(-и)	**Гурская Т.Г., доцент, к.т.н., доцент кафедры ИБ**
Направление подготовки	**09.03.02 Информационные системы и технологии**
Направленность (профиль) ОПОП	**Безопасность информационных систем**
Квалификация (степень)	**бакалавр**
Форма обучения	**очно-заочная**
Год приема	**2021**
Курс	**5**
Семестр	**9**

Астрахань, 2024

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины (модуля) – изучение методологических и законодательных основ организации комплексной системы защиты информации на предприятии, а также основных аспектов практической деятельности по ее созданию, обеспечению функционирования и контролю эффективности.

1.2. Задачи освоения дисциплины (модуля): предусматривают предоставление знаний по следующим вопросам:

изучить основы:

системного подхода к организации защиты информации, передаваемой, обрабатываемой и хранимой техническими средствами на основе применения криптографических методов;

принципов проектирования и анализа шифров;

математических методов, которые используются при проектировании и анализе шифров.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) Б1.В.10 «Комплексное обеспечение защиты информации объекта информатизации» относится к части, формируемая участниами образовательных отношений и осваивается в 9 семестре.

Изучение курса «Комплексное обеспечение защиты информации объекта информатизации» рассчитано на 1 семестр (9 семестр) и предусматривает сдачу студентами экзамена на основе балльно-рейтинговой системы оценивания.

Общая трудоемкость дисциплины – 3 ЗЕ.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами (модулями):

- Техническая защита информации.
- Организационное и правовое обеспечение информационной безопасности.
- Программно-аппаратные средства защиты информации.
- Методы и средства криптографической защиты информации.

В результате освоения этих дисциплин, студент должен:

знать:

− правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

− правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;

− принципы и методы организационной защиты информации;

- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.

– место и роль информационной безопасности в системе национальной безопасности Российской Федерации.

уметь:

− анализировать и оценивать угрозы информационной безопасности объекта;

− применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

− пользоваться нормативными документами по защите информации;

владеть:

− навыками работы с нормативными правовыми актами;

− методами технической защиты информации;

− методами расчета и инструментального контроля показателей технической защиты информации;

− методами организации и управления деятельностью − служб защиты информации на предприятии.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

Знания, полученные в результате изучения дисциплины, используются студентами при прохождении преддипломной практики и написанию бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

ПК-4. Способность проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения с учетом требований информационной безопасности.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать	Уметь	Владеть
ПК-4. Способность проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения с учетом требований информационной безопасности	ИПК-4.1. Знать методы проведения анализа и разработки требований к программному обеспечению.	ИПК- 4.2. Уметь выполнять работы по проектированию программного обеспечения	ИПК-4.3. Владеть методами проведения анализа требований к программному обеспечению, выполнять работы по проектированию программного обеспечения

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) 3 з.е., 108 часов, 21 часов выделено на контактную работу обучающихся с преподавателем (из них 7 часов – лекции, 14 часов – лабораторные работы), 87 часов – на самостоятельную работу обучающихся.

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
1	Раздел 1. Методология комплексной защиты информации на предприятии	9	1-2	2		4		17	Опрос по теме. Деловая игра. Отчет по лабораторной работе 1.

									Контрольная работа 1.
2	Раздел 2. Построение комплексной системы защиты информации		3-4	2		4		17	Опрос по теме. Отчет по лабораторной работе 2. Контрольная работа 2.
3	Раздел 3. Обеспечение комплексной системы защиты информации		5-6	1		2		17	Опрос по теме. Промежуточное тестирование. Отчет по лабораторной работе 3. Контрольная работа 3.
4	Раздел 4. Управление комплексной системой защиты информации		7-8	1		2		17	Опрос по теме. Проект. Контрольная работа 4
5	Раздел 5. Оценка эффективности комплексной системы защиты информации		9	1		2		19	Опрос по теме. Отчет по лабораторной работе 4. Контрольная работа 5. Итоговый тест
ИТОГО				**7**		**14**		**87**	**ЭКЗАМЕН**

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Темы, разделы дисциплины	Кол-во часов	Компетенции	общее количество компетенций
		ПК 4	
Раздел 1. Методология комплексной защиты информации на предприятии	23	+	1
Раздел 2. Построение комплексной системы защиты информации	23	+	1
Раздел 3. Обеспечение комплексной системы защиты информации	20	+	1
Раздел 4. Управление комплексной системой защиты информации	20	+	1
Раздел 5. Оценка эффективности комплексной	22	+	1

системы защиты информации			

Содержание дисциплины

Раздел 1. Методология комплексной защиты информации на предприятии

Тема 1.1. Сущность и задачи комплексной защиты информации на предприятии

Понятийный аппарат в области обеспечения информационной безопасности на предприятии. Цели, задачи и принципы построения комплексной системы защиты информации. О понятиях безопасности и защищенности. Разумная достаточность и экономическая эффективность. Управление безопасностью предприятия. Международные стандарты. Цели и задачи защиты информации в автоматизированных системах. Современное понимание методологии защиты информации: особенности национального технического регулирования, современная трактовка понятия безопасности информационных технологий, современные требования к средствам обеспечения безопасности. Доктрина информационной безопасности РФ. Утверждена Указом Президента. Российской Федерации от 5 декабря 2016 г. № 646. Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ. Закон РФ «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 4673. Закон РФ «О безопасности» // ВСНД и ВС РФ. 1992. № 15. Ст. 769. Закон РФ «О персональных данных» от 27.07.2006 №152-ФЗ. Закон РФ «О коммерческой тайне» от 29 июля 2004 г. N 98-ФЗ.

Тема 1.2. Принципы организации и этапы разработки комплексной системы защиты информации

Принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ. Методологические основы организации комплексной системы защиты информации. Разработка политики безопасности и регламента безопасности предприятия. Основные положения теории сложных систем. Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями. Требования, предъявляемые к комплексной системы защиты информации: требования к организационной и технической составляющим комплексной системы защиты информации; требования по безопасности, предъявляемые к изделиям ИТ. Этапы разработки комплексной системы защиты информации. Закон РФ «Об электронной цифровой подписи» от 6 апреля 2011 г. № 63-ФЗ.

Тема 1.3. Факторы, влияющие на организацию комплексной системы защиты информации

Влияние формы собственности на особенности защиты информации ограниченного доступа. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа. Характер основной деятельности предприятия. Состав, объекты и степень конфиденциальности защищаемой информации. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Конструктивные особенности предприятия. Количественные и качественные показатели ресурсообеспечения. Степень автоматизации основных процедур обработки защищаемой информации. Постановление Правительства РФ от 05.12.91 г, № 35 «Перечень сведений, которые не могут составлять коммерческую тайну» // Собрание постановление Правительства РФ. 1992. № 1-2. Ст. 7.

Раздел 2. Построение комплексной системы защиты информации

Тема 2.1. Определение и нормативное закрепление состава защищаемой информации

Классификация информации по видам тайны и степеням конфиденциальности. Нормативно-правовые аспекты определения состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия. Методика определения состава защищаемой информации. Порядок внедрения Перечня сведений, составляющих КТ, внесение в него изменений и дополнений. Постановление Правительства РФ от 04.09.1995 г. № 870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности» // СЗ РФ. 1995. № 37. Ст. 3619.

Тема 2.2. Определение объектов защиты

Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации. Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Транспортные средства и особенности транспортировки. Состав средств обеспечения, подлежащих защите. Постановление Правительства РФ от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти // СЗ РФ. 1995. № 17. Ст. 1455.

Тема 2.3. Определение компонентов комплексной системы защиты информации

Особенности синтеза СЗИ АС от НСД. Методика синтеза СЗИ: общее описание архитектуры АС, системы защиты информации и политики безопасности; формализация описания архитектуры исследуемой АС; формулирование требований к системе защиты информации; выбор механизмов и средств защиты информации; определение важности параметров средств защиты информации; оптимальное построение системы защиты для АС. Выбор структуры СЗИ АС. Проектирование системы защиты информации для существующей АС. 11. Указ Президента РФ от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10. Ст. 1127.

Тема 2.4. Определение условий функционирования комплексной системы защиты информации

Содержание концепции построения комплексной системы защиты информации. Объекты защиты. Цели и задачи обеспечения безопасности информации. Основные угрозы безопасности информации АС организации. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Определение потенциальных каналов и методов несанкционированного доступа к информации. Определение возможностей несанкционированного доступа к защищаемой информации. Основные положения технической политики в области обеспечения безопасности информации АС организации. Основные принципы построения комплексной системы защиты информации. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Первоочередные мероприятия по обеспечению безопасности информации АС организации. 12. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ, 1997, № 10, ст. 1127.

Тема 2.5. Разработка модели комплексной системы защиты информации

Общая характеристика задач моделирования комплексной системы защиты информации. Формальные модели безопасности и их анализ: классификация формальных моделей безопасности; модели обеспечения конфиденциальности; модели обеспечения

целостности; субъектно-ориентированная модель. Прикладные модели защиты информации в АС. Формальное построение модели защиты: описание объекта защиты; декомпозиция АС на субъекты и объекты; модель безопасности: неформальное описание; декомпозиция системы защиты информации; противостояние угрозам; реализация системы защиты информации субъекта АС субъектно-объектной модели. Формализация модели безопасности: процедура создания пары субъект – объект, наделение их атрибутами безопасности; осуществление доступа субъекта к объекту; взаимодействие с внешними сетями; удаление субъекта – объекта. 13. Указ Президента Российской Федерации от 24 января 1998 г. № 64 «О перечне сведений, отнесенных к государственной тайне» (с изменениями от 24 января 1998 г.) // СЗ РФ. 1995. № 49. ст. 4775; 1998, № 5, ст. 561.

Тема 2.6. Технологическое и организационное построение комплексной системы защиты информации

Общее содержание работ по организации комплексной системы защиты информации. Характеристика основных стадий создания комплексной системы защиты информации. Назначение и структура технического задания (общие требования к содержанию). Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию. 14. Указ Президента Российской Федерации от 12.05.2009 №537 «О стратегии национальной безопасности Российской Федерации до 2020 года».

Раздел 3. Обеспечение комплексной системы защиты информации

Тема 3.1. Кадровое обеспечение функционирования комплексной системы защиты информации

Специфика персонала предприятия как объекта защиты. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа. Подбор и обучение персонала. Указ Президента Российской Федерации от 12.05.2004 № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» (в редакции от 03.03. 2006).

Тема 3.2. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации

Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации. Перечень вопросов ЗИ, требующих документационного закрепления. 16. Положение о сертификации средств защиты информации по требованиям безопасности информации (введено в действие приказом Председателя Гостехкомиссии России от 05.01.1996 № 3. Зарегистрировано Госстандартом России в Государственном реестре 20.03.1995. (Свидетельство №РОСС RU.OOO1.O1БИОО).

Раздел 4. Управление комплексной системой защиты информации

Тема 4.1. Назначение, структура и содержание управления комплексной системы защиты информации

Понятие, сущность и цели управления комплексной системы защиты информации. Принципы управления комплексной системы защиты информации. Структура процессов управления. Основные процессы, функции и задачи управления комплексной системы защиты информации. Основные стили управления. Структура и содержание общей

технологии управления комплексной системы защиты информации. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения».

Тема 4.2. Принципы и методы планирования функционирования комплексной системы защиты информации

Понятие и задачи планирования функционирования комплексной системы защиты информации. Способы и стадии планирования. Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании. Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов. ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

Тема 4.3. Сущность и содержание контроля функционирования комплексной системы защиты информации

Виды контроля функционирования комплексной системы защиты информации. Цель проведения контрольных мероприятий в комплексной системы защиты информации. Анализ и использование результатов проведения контрольных мероприятий. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

Тема 4.4. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций

Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС. ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Раздел 5. Оценка эффективности комплексной системы защиты информации

Тема 5.1. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации

Вероятностный подход. Оценочный подход. Требования РД СВТ и РД АС. Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408□2002. Экспериментальный подход. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

Тема 5.2. Состав методов и моделей оценки эффективности комплексной системы защиты информации

Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности комплексной системы защиты информации. 22. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования». ГОСТ/ИСО МЭК 15408-2002 "Общие критерии оценки безопасности информационных технологий".

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным занятиям необходимо воспользоваться учебно-методической литературой из п.8 (основной). Лекции необходимо проводить с использованием презентаций, созданных в Microsoft PowerPoint.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8 (дополнительной).

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8 (основной), (дополнительной), источниками, Интернет-источниками.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
1	Подготовка к опросу по теме. Подготовка к деловой игре. Подготовка отчета по лабораторной работе 1. Подготовка к контрольной работе 1.	17	Внеаудиторная, изучение учебных пособий
2	Подготовка к опросу по теме. Подготовка отчета по лабораторной работе 2. Подготовка к контрольной работе 2.	17	Внеаудиторная, изучение учебных пособий
3	Подготовка к опросу по теме. Подготовка к промежуточному тестированию. Подготовка отчета по лабораторной работе 3. Подготовка к контрольной работе 3.	17	Внеаудиторная, изучение учебных пособий
4	Подготовка к опросу по теме. Проект. Подготовка к контрольной работе 4	17	Внеаудиторная, изучение учебных пособий
5	Подготовка к опросу по теме. Подготовка отчета по лабораторной работе 4. Подготовка к контрольной работе 5. Подготовка к итоговому тесту	19	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно – предусмотрено выполнение проекта.

Объем и оформление проекта, требования к оформлению

Содержание проекта определяется заданием. Проект состоит из пояснительной записки и графической части. Суммарный объем пояснительной записки с приложениями 30 – 40 листов формата А4 (297х210). Требования к пояснительной записке регламентированы ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Общие требования и правила оформления», а графического материала – Единой системе конструкторской документации (ГОСТ 2.104-68, ГОСТ 2.301-68 и др.). Правила оформления схем алгоритмов и программных продуктов по ГОСТ 19.002-80.

Общие требования к пояснительной записке (ПЗ). Все текстовые документы подшивают в одну папку.

ПЗ распечатывается на белой писчей бумаге форматом А4.

Требования по оформлению пояснительной записки: верхнее поле страницы – 15 мм, нижнее – 20 мм, левое поле – 20 мм, правое – 10 мм; выравнивание по ширине страницы; интервал – одинарный; размер шрифта – 14; шрифт – Times New Roman; отступ – 1.27 см; нумерация страниц – справа в верху.

ПЗ должна содержать:

1. Титульный лист;
2. Задание для проекта;
3. Аннотация;
4. Содержание;
5. Введение;
6. Общая часть ПЗ;
7. Список используемой литературы;
8. Приложения.

В ПЗ содержится обоснования принятых решений: необходимые вычисления, назначения компонентов в структурных схемах и обоснования их применения, обоснования выбора необходимой технических средств и т.д. Объемные материалы (тексты инструкций, прайс-листы и т.п.) целесообразно выносить в приложения.

В аннотации в краткой форме приводят сведения о выполненной работе и каждая фраза должна нести информацию о том, что сделано, какими средствами и какой получен результат. Аннотация должна начинаться одноименным заголовком, выполняться на листах формата А4 и не должна повторять формулировку темы проекта, которая указана в задании.

Содержание общей части ПЗ делят на разделы, подразделы и пункты в соответствии с общепринятой рубрикацией. Каждая часть должна иметь заголовок. Разделы должны иметь порядковые номера, обозначенных арабскими цифрами с точкой.

Подразделы порядковые номер в пределах каждого раздела. Номера подразделов состоят из номера раздела и подраздела, разделенных точкой. В конце номера пункта должна ставиться точка. Например, пункты раздела 1, входящего в него подраздела 1.1, обозначают так: 1.1.1., 1.1.2., 1.1.3. и т.д.

Наименование разделов должны быть краткими, соответствовать содержанию и записываться в виде заголовков прописными буквами. Наименование подразделов записывают в виде заголовков строчными буквами (кроме первой прописной). Переносы слов в заголовках не допускаются, точку в конце не ставят. Если заголовок состоит из двух предложений, их разделяют точкой. Расстояние между заголовком и последующим текстом должно составлять 1 строку или быть не менее 10 мм. Для разделов, текст которых записывается на одном листе с текстом предыдущего раздела (подраздела) расстояние

между последней строкой текста и последующим заголовком должно быть не менее 3 строк или 20 мм.

В основной текст ПЗ включают введение и общая часть.

Объём введения – не более 2-х страниц. Во введении формулируются задачи, решаемые при выполнении проекта, дается краткая характеристика всей работы, а так же перечисляются и кратко характеризуются все главы.

Объём общей части ПЗ – 15-20 страниц. Содержание общей части описано ниже. Пояснения ведут в безличной форме или от первого лица множественного числа. Перечеркивания и сокращения в ПЗ не допускаются, за исключением общепринятых: т.д., т.п., т.к. и др.

Список используемой литературы оформляют в соответствии с ГОСТ Р 7.0.5-2008. В списке литературы должны быть указаны все информационные источники, использованные для подготовки проекта: книги, учебники, журнальные статьи, статьи из Internet. Всего от 5 до 20 источников. Нумерация источников в списке должна быть сквозная.

Для книг необходимо указывать фамилию и инициалы автора, название книги, место (город) издания, издательство, год издания и общее число страниц. Для журнальных статей – автора, название статьи, название журнала, год его издания, номер и страницы, на которых напечатана статья. Для источников, взятых из Internet - название статьи, автора, название Internet-портала, его точный web-адрес.

Иностранную литературу необходимо писать в латинской транскрипции. Ссылки на соответствующий литературный источник, помещенный в списке, дают в следующем виде [4], [3,6].

Список литературы, рекомендуемой при выполнении проекта и оформленный в соответствии с требованиями ГОСТа приведен ниже.

В **приложении** выносят объемные материалы: копии использованных документов, тексты инструкций, спецификации и т.п.

Имеющиеся в записке **иллюстрации** (рисунки, эскизы, схемы, диаграммы, графики) нумеруют арабскими цифрами в пределах всей записки, например: рис.1, рис.2 и т.д. Ссылки на ранее упомянутые иллюстрации дают в скобках, по типу: (рис.3). Графики функций снабжают координатными шкалами с равномерным шагом, выбранным из стандартного ряда чисел: 1, 2, 2.5, 4, 5... Каждое построение сопровождают надписью с указанием масштабного коэффициента этого построения.

В **графической части** проекта необходимо представить 2 листа (формат А1) и электронно-графическую презентацию 10-15 слайдов.

На листах представляется план объекта защиты и план системы информационной безопасности. Все чертежи, схемы, таблицы и т.п. выполняются только чёрным цветом. Запрещается использование стилизованных изображений. Плакаты должны быть выполнены в соответствии с требованиями ЕСКД. На каждом листе должна выполняться основная надпись.

Презентация, должна содержать наглядный графический материал, поясняющий выступление студента во время защиты проекта. Все чертежи, схемы, таблицы должны удовлетворять требованиям ЕСКД. Для более наглядного представления динамики процессов, взаимодействия отдельных узлов в составе устройства рекомендуется использовать различную раскраску или заливку, а так же стилизованные изображения. Анимацию графики и другие средства мультимедиа использовать не рекомендуется. Презентацию рекомендуется разрабатывать в среде Microsoft PowerPoint.

Содержание основной части пояснительной записки

Основная часть пояснительной записки должна содержать материал, на основании которого проводится проектирование. Её рекомендуется разбить на следующие разделы:

1. Анализ исходных данных.
2. Оценка угроз безопасности предприятия.
3. Разработка организационно-технических мероприятий.
4. Основные положения политики информационной безопасности.

В разделе анализ исходных данных должно быть представлено:

1. Характеристика предприятия.
2. Анализ информации, циркулирующий на предприятии.
3. Анализ технической оснащенности предприятия.

Рассматривая предприятие необходимо дать краткую характеристику деятельности предприятия и представить её организационно-штатную структуру. Организационно-штатная структура выполняется в виде схемы с необходимыми пояснения. Так же необходимо указать причину защиты информации от НСД, если она есть, и охарактеризовать её правовую основу. Например, банк должен сохранять “тайну вклада” на основании Закона РФ “О банковской деятельности…” и т.п. Здесь же необходимо охарактеризовать правовую сторону защиты информации на данном предприятии.

Анализ информации циркулирующей на предприятии состоит из структуры документооборота, существующей структуры конфиденциальности и сводной таблицы. Структура документооборота должна быть представлена в виде схемы, отражающей реально существующую технологию обработки документов.

Структура конфиденциальности представляется только в том случае, когда на предприятии таковая уже есть и закреплена во внутренних нормативных документах. Она представляется в виде таблицы, форма которой представлена в таблице 1:

Таблица 1

Структура конфиденциальности информации на предприятии

№ п.п.	Наименование грифа конфиденциальности	Степень защиты	Перечень информации, относящийся к данному грифу
1	2	3	4

Поскольку проект выполняется в открытом виде, то данная структура *не должна* учитывать документы, имеющие гриф государственной тайны.

В графе “Наименование грифа конфиденциальности” необходимо указать наименование грифа, как оно дано в нормативных документах предприятия. В графе “Степень защиты” необходимо указать уровень, на котором необходимо защищать информацию. Его можно указать качественно, например: “высший”, “высокий”, “нормальный” и “не конфиденциально”. Или – количественно, в условных единицах, с пояснением значения каждой единицы.

Сводная таблица анализа информации отражает результаты, проведённого студентом анализа. В ней даются реальные оценки. Её форма представлена в таблице 2:

Таблица 2

Анализ информации на предприятии

№ п.п.	Вид документа	Степень защиты	Количество	Срок хранения
1	2	3	4	5

В графе 2 “Вид документа” указывается документ. В виду того, что документы одного типа имеют разную степень конфиденциальности, то их наименования могут

повторяться. Например, бухгалтерские документы, относящиеся к конфиденциальному договору, относятся к конфиденциальным документам. А открытые – к не конфиденциальным.

В графе 3 указывается степень, с которой требуется защищать документ. Она должна отражать реальную необходимость, получается экспертным путём. Форма представления должна совпадать с соответствующей графой таблицы 1. Рекомендуется упорядочить информацию во всей таблице по этой графе.

В графе 4 указывается количество документов за тот период, пока они сохраняют свою актуальность. Т.е. пока не поменяется степень защиты.

В графе 5 должен быть указан срок актуальности документов. Этот срок так же получается экспертным путём и должен отражать необходимую реальность.

Анализ технической оснащённости включает план предприятия и технический паспорт объекта. План предприятия выполняется с указанием размещения АРМ, серверов, коммутационного оборудования, линий связи, электроснабжения, заземления, сигнализации, оргтехники и других элементов информационной системы предприятия. Технический паспорт представляет собой таблицу, форма которой представлена в таблице 3:

Таблица 3

Технический паспорт объекта

Наименование объекта	
Этаж (этажей в многоэтажном здании)	
Наличие хранилищ бумажных док-ов	Сколько? Какие комнаты?
Наличие комнат с неконтролируемым доступом	Сколько? Какие?
Порядок доступа в помещения	Какие комнаты и как сдаются по охрану?
Наличие других предприятий	Да/нет?
Состав технических средств	
Количество и тех. характеристики серверов	Тип процессора/мат. платы/объём ОЗУ/объём жесткого диска/ОС
Количество и характеристики АРМ	Тип процессора/мат. платы/объём ОЗУ/объём жесткого диска/монитор/ОС
Количество и характеристики терминалов	Тип процессора/мат. платы/объём ОЗУ/объём жесткого диска/монитор/ОС
Количество коммутаторов ЛВС	производитель/модель/пропускная способность/количество портов
Выход в Internet	
Тип подключения	(Dial-Up/ADSL/коммутированный канал)/скорость передачи
Коммуникационное оборудование	производитель/модель
Коммуникационное ПО	Шлюз, сетевой экран

Характеристика ПО	
Информационное ПО	
Тип ПО	Сетевое? (да/нет)/количество мест
Структура ПО (Клиент-сервер/Файл-сервер)	Производитель/версия
Объем базы данных	
Дополнительное ПО	
Наименование	Назначение/версия/сетевое? (да/нет)
Дополнительное оборудование	
Факсы	Производитель/модель/количество
Факс-модемы (не используемые для Internet)	Производитель/модель/количество
Внутренняя АТС	Производитель/модель/количество
Телефоны	Производитель/модель/количество

Графы, которые являются неактуальными для данного предприятия, разрешается не заполнять. Графы для описания различных моделей устройств или программного обеспечения должны повторятся.

Оценка угроз безопасности предприятия представляется в виде таблицы, форма которой представлена в таблице 4.

Таблица 4.

Оценка угроз безопасности информации предприятия

№ п.п.	Узел информационной системы	Выявленная угроза БИ		Оценка риска	
		Угроза	Уязвимость	P_s = P_t = P_p =	Итоговая оценка, Р
1.	2.	3.	4.	5.	6.

В графе 1, “№ п.п.”, должны быть пронумерованы узлы информационной системы и уязвимости, соответствующие им. При этом, номер уязвимости должен формироваться исходя из номера узла и уязвимости по порядку. Например, номер 1.2 соответствует второй по порядку уязвимости для первого узла.

Узлы информационной системы – это такие узлы, в которых информация меняет носитель или форму. К ним необходимо относить:

– рабочие места работников предприятия (АРМ);

– коммуникационную аппаратуру (концентраторы, коммутаторы, телефоны, АТС и т.д.);

– сервера;

– места хранения бумажных документов и электронных носителей и т.п.

Угроза, в общем случае, – это потенциально опасное событие или явление, которое может снизить защищённость информации. Угрозы рекомендуется группировать по трём признакам: угроза конфиденциальности, доступности и целостности информации.

В свою очередь, *уязвимость* представляет собой сочетание обстоятельств, позволяющее реализовать угрозу. Таким образом, в графе 4 должны быть указаны конкретные причины, позволяющие реализовать угрозу. Например: "…малое время наработки на отказ…", "возможность перехвата информации в следствии…", "несовершенство программного обеспечения…" и т.д.

В графе 5 должна быть дана оценка реальности реализации угрозы. Она вычисляется, исходя из трех параметров – прямых факторов:

P_s – пространственный фактор, т.е. вероятность того, что уязвимость реализуется в том месте, где находится информация;

P_t – временной фактор, т.е. вероятность того, что уязвимость реализуется в тот момент, когда информация существует;

P_p – энергетический фактор, вероятность того, что энергии, для выполнения уязвимости будет достаточно.

Итоговая оценка (графа 6, P) вычисляется прямым произведением величины вероятности каждого фактора, т.е.

$P = P_s \bullet P_t \bullet P_p$

Таким образом, при невыполнении хотя бы одного из прямых факторов, т.е. вероятность его равна 0, уязвимость можно считать устранённой.

Величина вероятности выполнения прямых факторов зависит от косвенных. К ним можно отнести: надёжность работы аппаратуры и программного обеспечения, квалификацию персонала, влияние внешней среды и т.д.

В качестве примера можно привести следующую оценку. Менеджер за рабочий день (8 ч.) вносит в базу данных примерно 40 документов. На обработку каждого документа требуется, в среднем, 5 мин. Сбой в системе электропитания происходит до 3 раз в день. Из этого следует, что: сбой в системе электропитания происходит раз в 160 мин (2 ч 40 мин). За это время менеджер обработает ≈ 14 документов. Совокупное время обработки составит 70 мин. Вероятность выполнения временного фактора равна 0.4375. Вероятности выполнения двух других факторов, объективно, можно считать равными 1. Таким образом, итоговая оценка равна 0.4375.

Если существуют уязвимости аналогичные уже рассмотренным случаям, разрешается не рассматривать их подробно. При этом необходимо сделать ссылку на номер той уязвимости, которая была рассмотрена выше, например: "аналогично п. № 3.4…"

В пояснениях к таблице необходимо привести косвенные факторы, их количественные показатели и методы расчета величин прямых факторов уязвимости. В случае отсутствия количественных показателей, допускается качественная оценка факторов, с использованием методов неформального оценивания.

Для разработки организационно-технических мероприятий необходимо провести совокупную оценку всех уязвимостей системы. Результаты оценки должны быть представлены в таблице (таблица 5).

Таблица 5

Совокупная оценка уязвимости информационной системы

№ п.п.	Уязвимость	№№ узлов	Метод предотвращения	Снижаемый показатель (P_s, P_t, P_p)
1	2	3	4	5

В графе 2 таблицы, "Уязвимость", необходимо указать уязвимость так, как она указана в таблице 4. В графе 3 указываются номера тех узлов, которым соответствует данная уязвимость. В графе 4 описывается метод предотвращения (или снижения до

приемлемого уровня) уязвимости. Поскольку уязвимость предотвращается (снижается) уменьшением одного из основных факторов уязвимости, то в графе 5 необходимо указать этот фактор.

После проведения анализа уязвимостей проводится подбор технических средств. Его можно произвести любым из известных методов, а именно:

– методом главного показателя;

– методом результирующего (аддитивного, мультипликативного или максиминного) показателя качества;

– лексикографическим методом.

Рекомендуется использовать метод нормализации и свертки критериев, изученный на лабораторных работах.

Результатом выполнения работы должен стать проект политики информационной безопасности (ПИБ) на предприятии.

При разработке ПИБ должны быть решены следующие вопросы:

1. Определён перечень информации подлежащей защите.

2. Определён тип ПИБ (избирательный или мандатный).

3. Определены категории пользователей, доступные им ресурсы ИС и порядок доступа к этим ресурсам.

4. Разработан порядок применения ТС.

Перечни информации подлежащей защиты формируются на основании законодательства РФ и реальной необходимости. Основой для них должен послужить анализ информации циркулирующей в ИС, представленный в таблице 2. Количество грифов конфиденциальности должно соответствовать графе 3 этой таблицы, но не более 4-х (рекомендуется 2 – “конфиденциально” и “не конфиденциально”). Состав информации должен соответствовать содержанию соответствующих документов.

Категории пользователей и тип ПИБ определяются исходя из структуры предприятия, должностных обязанностей работников, порядка доступа к ресурсам и методов защиты информации, представленных в таблице 5. Порядок применения ТС разрабатывается на основе методов защиты информации (таблица 5), назначения и функциональных возможностей выбранных ТС. Необходимо, так же, представить план их размещения.

На плане размещения ТС защиты информации необходимо обозначить размещение датчиков охранно-пожарной сигнализации, места расположения элементов системы видеонаблюдения и т.д. В тексте ПЗ необходимо пояснить выбор и размещение этих средств. В тексте основной части ПЗ необходимо отразить только основные положения ПИБ, указанные выше. Полнотекстовый вариант документа, отражающего ПИБ, рекомендуется приводить в приложении.

Содержание графической части

На листах графической части проекта представляется план объекта защиты и план защиты информации на нём.

План объекта защиты представляет собой план помещений объекта, с указанием размещения на нём ТС обработки информации, рабочих мест сотрудников предприятия, линий электроснабжения, связи и т.п. При необходимости, показывается план прилегающей территории. Если предприятие занимает несколько зданий, то на плане они показываются отдельными чертежами.

Дополнительно, на этом же плане, необходимо указать направления воздействия угроз безопасности информации. А так же представить технический паспорт объекта, и пояснения для каждой угрозы.

На втором плакате представляется план размещения ТС защиты информации вместе с пожарной и охранной сигнализацией и системой видеонаблюдения. Дополнительно, на плане размещается таблица с техническими характеристиками используемых средств.

Общий заголовок плаката указывается в основной надписи и не дублируется. При необходимости, озаглавливаются отдельные элементы плаката. На нём так же необходимо представить легенду.

Презентация должна содержать:

1. Титульный лист (копия титульного листа ПЗ).
2. Основную часть презентации.
3. Содержание.

В основной части презентации необходимо разместить слайды, содержащие основные сведенья о предприятии, схемы, примеры расчетов и другую информацию, иллюстрирующую доклад студента во время защиты. Рекомендуется избегать текстовых слайдов. Схемы и чертежи, представленные в пояснительной записке и презентации могут повторяться. Рекомендуется оформлять слайды презентации в едином стиле.

Каждый лист, за исключением титульного, должен быть пронумерован и озаглавлен. В содержании должны быть указаны заголовки слайдов и их номер. Рекомендуется создать ссылку из содержания на каждый слайд. Титульный лист в содержании не указывается.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Учебные занятия по дисциплине могут проводиться с применением информационно-телеком-муникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Раздел 1. Методология комплексной защиты информации на предприятии	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы, выполнение контрольной работы
Раздел 2. Построение комплексной системы защиты информации	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы, выполнение

			контрольной работы
Раздел 3. Обеспечение комплексной системы защиты информации	Лекция	Не предусмотрено	выполнение лабораторной работы, выполнение контрольной работы, тест
Раздел 4. Управление комплексной системой защиты информации	Лекция	Не предусмотрено	выполнение лабораторной работы, выполнение контрольной работы
Раздел 5. Оценка эффективности комплексной системы защиты информации	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы, выполнение контрольной работы, тест

6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

- использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));

-использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;

-использование возможностей электронной почты преподавателя;

-использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т.д.);

-использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

-использование виртуальной обучающей среды (или системы управления обучением LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров.

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение:

Наименование программного обеспечения	Назначение

Adobe Reader	Программа для просмотра электронных документов
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда

6.3.2. Современные профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Комплексное обеспечение защиты информации объекта информатизации» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Раздел 1. Методология комплексной защиты информации на предприятии	ПК 4	Вопросы для обсуждения. Деловая игра. Лабораторная работа 1. Контрольная работа 1.
2.	Раздел 2. Построение комплексной системы защиты информации	ПК 4	Вопросы для обсуждения. Вопросы для обсуждения. 2. Контрольная работа 2.
3.	Раздел 3. Обеспечение комплексной системы защиты информации	ПК 4	Вопросы для обсуждения. Промежуточное тестирование. Вопросы для обсуждения. 3. Контрольная работа 3.
4.	Раздел 4. Управление комплексной системой защиты информации	ПК 4	Вопросы для обсуждения. Проект. Контрольная работа 4
5.	Раздел 5. Оценка эффективности комплексной системы защиты информации	ПК 4	Вопросы для обсуждения. Вопросы для обсуждения. 4. Контрольная работа 5. Итоговый тест

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

При решении комплексной ситуационной задачи можно использовать следующие критерии оценки:

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры

4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетво рительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетво рительно»	не способен правильно выполнить задание

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Раздел 1. Методология комплексной защиты информации на предприятии

1. Вопросы для обсуждения.

1) Понятийный аппарат в области обеспечения информационной безопасности на предприятии.

2) Цели, задачи и принципы построения комплексной системы защиты информации.

3) Разумная достаточность и экономическая эффективность.

4) Управление безопасностью предприятия.

5) Международные стандарты.

6) Цели и задачи защиты информации в автоматизированных системах.

7) Современное понимание методологии защиты информации.

8) Принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ.

9) Методологические основы организации комплексной системы защиты информации.

10) Разработка политики безопасности и регламента безопасности предприятия.

11) Основные положения теории сложных систем.

12) Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями.

13) Требования, предъявляемые к комплексной системы защиты информации.

14) Этапы разработки комплексной системы защиты информации.

15) Влияние формы собственности на особенности защиты информации ограниченного доступа.

16) Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа.

17) Характер основной деятельности предприятия. Состав, объекты и степень конфиденциальности защищаемой информации.

18) Структура и территориальное расположение предприятия. Режим функционирования предприятия.

19) Конструктивные особенности предприятия. Количественные и качественные показатели ресурсообеспечения.

20) Степень автоматизации основных процедур обработки защищаемой информации.

2. Лабораторная работа 1.

Тема: Выявление источников и носителей информации на промышленном предприятии.

Цель:

1. Получить навыки анализа трудноформализуемой информации.
2. Отработать на практике методику анализа информации, циркулирующей на промышленном предприятии.
3. Закрепить теоретические знания, полученные на лекциях.

Введение

Анализ информации циркулирующей на предприятии является первым этапом в проектировании комплексной системе защиты информации (СЗИ) на предприятии. Этот этап практически позволяет определить, что необходимо защищать и на каком уровне. Но определение источников и носителей информации относится к, так называемым, трудноформализуемым задачам. Такая задача во многом зависит как от опыта специалиста, так и от условий функционирования предприятия.

Теоретическая часть

Основная задача анализа информации циркулирующей на предприятии является выявление полного перечня источников информации, носителей информации и выработка структуры конфиденциальности. Источниками информации являются:

- люди;
- документы;
- продукция;
- измерительные датчики;
- материалы и технологическое оборудование;
- черновики и отходы производства;
- интеллектуальные средства обработки информации.

Носителями информации являются:

- люди;
- материальные тела;
- поля;
- элементарные частицы.

При анализе информации, необходимо построить граф, узлами которого будут источники информации, а носителями станут связи между узлами. В узлах графа необходимо расположить, прежде всего, должностных лиц предприятия. Поскольку люди – это основной источник информации. Затем необходимо выявить связи между этими людьми.

После этого, к графу необходимо добавить другие источники информации, характерные для этого предприятия. Ими могут стать архивы. Например, архив документов предприятия, документы, хранящиеся у директора (архив директора), в бухгалтерии (архив бухгалтера), у других должностных лиц. Так же необходимо проанализировать документооборот предприятия, выявив другие узлы, в которых могут находиться документы, подлежащие защите. К узлам графа необходимо отнести измерительную аппаратуру, если таковая есть, места скопления (вывоза) отходов или мусора и т.п.

После выявления “внутренних”, т.е. характерных для предприятия источников, необходимо выявить “внешние”, которые образуются в результате внешних связей предприятия. Это могут быть клиенты, поставщики, посетители и т.д.

Средства вычислительной техники (СВТ) могут быть источниками информации, только в тех случаях, когда в алгоритмах их работы используются методы искусственного интеллекта. Однако, компьютерная система является очень важным информационным звеном в работе любого предприятия. По ней рекомендуется строить отдельный граф. В узлах этого графа располагаются непосредственно компьютеры, рабочие станции, сервера и т.д. – Хосты. Помимо этого, в узлах графа можно расположить коммуникационную аппаратуру (сетевые коммутаторы, концентратору, факс-модемы и т.д.), если эта аппаратура существенно влияет на работу ЛВС.

Выявление связей между узлами графа позволит выявить носители информации. Поскольку, информация доступна только тогда, когда она находится на носителе, то и защищать необходимо носитель.

При внимательном рассмотрении связей между вершинами графа, не трудно выяснить, что, по крайней мере, внутренние связи образуются “все со всеми”. Поэтому все носители рекомендуется разделить по их типам:

- люди;
- документы (традиционный документооборот);
- средства связи, без учёта ЛВС;
- компьютеры и ЛВС.

Конечно, на реальном предприятии может быть гораздо больше носителей, но, учитывая, что в ходе лабораторной работы студенты анализируют информацию на условном предприятии, данного перечня вполне достаточно. Поскольку общий граф, с учетом всех носителей слишком сложен и нагляден, необходимо построить четыре графа, в соответствии с каждым из носителей.

При выявлении связей, необходимо учитывать то, что документы, хранящиеся в архивах, сами являются носителями. Поэтому в каждом из архивов будет возникать связь “с собой”. Люди, как носитель информации, будут передавать её через устный разговор. Такую связь необходимо отразить в отдельном графе.

Порядок проведения

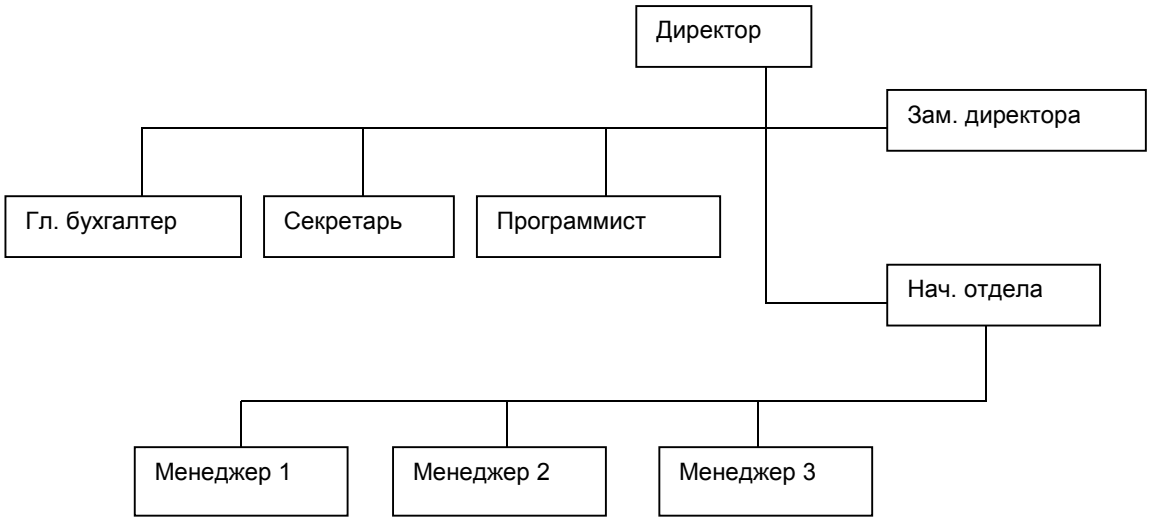

Рис. 1 Пример структурной схемы предприятия

1. На первом этапе выполнения работы необходимо построить структурную схему предприятия, в соответствии с заданием

2. На втором этапе разрабатываются графа для каждого из носителей информации. Если граф получается слишком сложным, то его можно упростить. Для этого можно объединить несколько вершин в одну. Можно объединять только те вершины, которые соответствуют должностным лицам, выделенным в логическую группу, например отдел. Эти вершины должны та же иметь одинаковые связи. В этом случае необходимо построить отдельный граф, отражающий связи внутри такой группы.

3. На третьем этапе необходимо заполнить таблицы связанности для каждого графа. В таблицах по столбцам и строкам располагаются вершины соответствующего графа, а пересечения заполняются 1, если связь между вершинами существует, и 0, если связь не существует.

Содержание отчета

Отчет оформляется на листах белой писчей бумаги и должен содержать титульный лист, тему, цель, а так же все схемы, графы и таблицы.

Контрольные вопросы по лабораторной работе 1

1. Что понимается под информацией?
2. Какие виды информации Вам известны?
3. Перечислите и охарактеризуйте источники информации.
4. Перечислите и охарактеризуйте носители информации.
5. Какие методы решения трудноформализуемых задач Вам известны? В чём их суть?

3. Деловая игра

Тема (проблема) Принципы организации и этапы разработки комплексной системы защиты информации на предприятии

Концепция игры

Цели:

1. Закрепить и углубить изучаемый материал студентами.

2. Определить проблемные вопросы комплексной защиты в органах управления, в организациях и на предприятиях различной формы собственности и изложить свою позицию по совершенствованию мероприятий комплексной защиты информации.

Задание:

1. Выбрать предприятие, описать его организационную структуру.

2.Определить, какие принципы организации КСЗИ будут использоваться на данном предприятии.

3. Разработать основной круг вопросов, решаемых руководством предприятия по обеспечению комплексной безопасности предприятия.

4. Определить, факторы, влияющие на организацию КСЗИ на данном предприятии.

5. Описать этапы разработки КСЗИ на данном предприятии

6.Разработать политику безопасности и регламент безопасности предприятия.

7. В роли руководителя предприятия разработать систему управления информационной безопасностью предприятия.

8. Быть в готовности в роли руководителя, начальника службы безопасности решать управленческие задачи, связанные с обеспечением комплексной безопасности предприятия (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).

9. Студентам письменно выполнить задание (объем 5-7 листов) и быть в готовности к его защите на практическом занятии.

Порядок проведения практического занятия

1. Организация занятия (проверка присутствующих и готовности к занятиям, объявление темы и цели занятия, доведение порядка проведения занятия).

2. Распределение на подгруппы и озвучивается ситуация. Студентами выбирается одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.

Пример ситуации:

Промышленное предприятие (условно ОАО «Маяк») специализирующееся на производстве пластмассовых труб, которые по своим качествам пользуются большим спросом. Охрана и защита коммерческих секретов, связанных с технологией производства труб, находятся в центре внимания руководства и службы безопасности предприятия. Предприятие имеет административную зону, где расположены управленческие структуры, производственную и складскую зоны. Все эти зоны разделены заборами. Предприятие имеет широкий круг партнеров, клиентов (в том числе и за рубежом). В сфере деятельности предприятия часто возникают конфликтные ситуации с конкурентами и спорные вопросы с органами местной власти по земельным и финансовым вопросам. В отношении предприятия недобросовестные конкуренты постоянно используют методы коммерческого шпионажа. Имеются случаи подкупа сотрудников, грабежи и разбои криминальных структур в отношении ведущих специалистов предприятия.

3. Присвоение подгруппам первоначальных ролей (начальники службы безопасности предприятия, руководители предприятия, эксперты).

4. Обсуждение студентами каждой подгруппы вопросов, вынесенных на практическое занятие с целью выработки общих позиций.

4.1. Вопросы со стороны подгруппы выступающих в роли руководителей предприятия.

4.2. Вопросы со стороны подгруппы экспертов.

4.3. Ответы и дискуссии.

4.4. Выработка общей позиции и общего подхода к вопросам обеспечения комплексной безопасности предприятия.

5. Обсуждение преподавателем и старшими групп оценок участников занятия.

7. Подведение итогов занятия с объявлением окончательных оценок участников практического занятия.

Роли:

Студенты распределены на 3 подгруппы:

1-я подгруппа – сотрудники технической группы службы безопасности;

2-я подгруппа – руководители коммерческой организации;

3-я подгруппа – экспертная группа.

Ожидаемый (е) результат (ы)…

Формирование следующих компетенций:

ОК 5, ОК 6, ОК 8, ОПК 5, ОПК 6, ОПК 7, ПК 4, ПК 7, ПК 8, ПК 10, ПК 13, ПСК 1, ПСК 2.

4. ***Контрольная работа 1.***

Вопросы к контрольной работе № 1

1. Цели, задачи и принципы построения комплексной системы защиты информации.
2. Разумная достаточность и экономическая эффективность.
3. Управление безопасностью предприятия.
4. Международные стандарты.
5. Цели и задачи защиты информации в автоматизированных системах.
6. Современное понимание методологии защиты информации: особенности национального технического регулирования, современная трактовка понятия безопасности информационных технологий, современные требования к средствам обеспечения безопасности.
7. Принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ.
8. Методологические основы организации комплексной системы защиты информации.
9. Разработка политики безопасности и регламента безопасности предприятия.
10. Основные положения теории сложных систем.
11. Система управления информационной безопасностью предприятия.
12. Принципы построения и взаимодействие с другими подразделениями.
13. Требования, предъявляемые к комплексной системы защиты информации: требования к организационной и технической составляющим комплексной системы защиты информации; требования по безопасности, предъявляемые к изделиям ИТ.
14. Этапы разработки комплексной системы защиты информации.
15. Влияние формы собственности на особенности защиты информации ограниченного доступа.
16. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа.
17. Состав, объекты и степень конфиденциальности защищаемой информации.
18. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Конструктивные особенности предприятия.

Раздел 2. Построение комплексной системы защиты информации

1. ***Вопросы для обсуждения.***

1) Классификация информации по видам тайны и степеням конфиденциальности.

2) Нормативно-правовые аспекты определения состава защищаемой информации.

3) Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия. Методика определения состава защищаемой информации.

4) Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации.

5) Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа. Факторы, определяющие необходимость защиты периметра и здания предприятия.

6) Особенности помещений как объектов защиты для работы по защите информации.

7) Транспортные средства и особенности транспортировки. Состав средств обеспечения, подлежащих защите.

8) Особенности синтеза СЗИ АС от НСД. Методика синтеза СЗИ.

9) Выбор структуры СЗИ АС.

10) Проектирование системы защиты информации для существующей АС.

11) Содержание концепции построения комплексной системы защиты информации. Объекты защиты.

12) Цели и задачи обеспечения безопасности информации.

13) Основные угрозы безопасности информации АС организации. Анализ и оценка угроз безопасности информации.

14) Определение потенциальных каналов и методов несанкционированного доступа к информации.

15) Определение возможностей несанкционированного доступа к защищаемой информации.

16) Основные положения технической политики в области обеспечения безопасности информации АС организации.

17) Основные принципы построения комплексной системы защиты информации. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.

18) Первоочередные мероприятия по обеспечению безопасности информации АС организации.

19) Общая характеристика задач моделирования комплексной системы защиты информации.

20) Формальные модели безопасности и их анализ.

21) Прикладные модели защиты информации в АС. Формальное построение модели защиты. Формализация модели безопасности.

22) Общее содержание работ по организации комплексной системы защиты информации.

23) Характеристика основных стадий создания комплексной системы защиты информации.

24) Назначение и структура технического задания. Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию.

2. Лабораторная работа 2.

Тема: Выявление и анализ угроз безопасности информации в документообороте предприятия.

Цель:

1. Получить практические навыки в выявлении угроз безопасности информации
2. Закрепить навыки анализа рисков безопасности
3. Закрепить знания, полученные на лекциях

Введение

Выявление и анализ угроз безопасности информации является основным этапом в процессе проектирования комплексных СЗИ. Только опираясь на результаты количественных оценок возможно проектирование адекватных и эффективных систем

защиты. Поэтому умение обосновать критерии, а затем провести объективную оценку является неотъемлемой чертой специалиста по защите информации.

Поскольку механизмы защиты информации должны предусматриваться ещё на стадии проектирования любой информационной системы, то специалисту в области защиты информации необходимо иметь навыки не только в области построения защиты информации, но и собственно информационных систем.

Теоретическая часть

В ходе выполнения лабораторной работы студентам необходимо решить две задачи: во-первых, разработать порядок обработки документов, во-вторых, выявить и оценить угрозы безопасности информации.

Первая задача решается путём построения графа, в узлах которого располагаются люди, осуществляющие производственную деятельность. Связи между узлами проявят состав документов необходимый для работы предприятия. По этому графу можно качественно оценить состав и порядок обработки документов. При разработке документооборота необходимо придерживаться следующих принципов:

1) Количество документов должно быть минимальным.

2) Содержание каждого документа должно быть актуальным. Т.е. документ должен содержать минимальное количество полей. Информация в документе должна быть полной и объективной. Документ должен быть наглядным, ясным и не допускать двоякого толкования.

3) Каждый документ должен содержать реквизиты, позволяющие определить авторство документа и исключить отказ автора от документа.

4) Порядок обработки документов должен содержать минимальное количество операций. Сами операции должны быть интуитивно понятными и не требовать особой подготовки.

5) Должны быть предусмотрены механизмы контроля целостности и правильности документооборота.

Выявление угроз безопасности информации производится на каждом этапе обработки информации. Это соответствует каждому плечу графа. Поэтому при решении этой задачи граф будет являться основой для качественной оценки. Количественной оценкой будет риск реализации угрозы. В общем случае величина риска P будет вычисляться следующим образом:

$$P = P_t \cdot P_s \cdot P_p \quad (1)$$

где P_t – вероятность того, что злоумышленник попытается добыть информацию тогда, когда она уже будет существовать;

P_s – вероятность того, что злоумышленник попадёт в ту область пространства, где будет находится информация;

P_p – вероятность того, что злоумышленник сможет разобрать информацию.

Оценка каждой из вероятностей производится исходя из булевой функции:

$$P_i = \begin{cases} 1, \textit{если условие соблюдается} \\ 0, \textit{в противном случае} \end{cases} \quad (2)$$

где P_i – это одна из вероятностей P_t, P_s, P_p.

Пример расчета

Задано производственное предприятие, осуществляющее производство и продажу определённого вида товаров. Существует необходимость скрыть факт сделки с клиентами, например, в том случае, когда разные клиенты являются конкурентами друг по отношению к другу.

Среди работников предприятия нас будут интересовать следующие лица: менеджер (3), бухгалтер (4), работник планового отдела (5), начальники цехов (или мастера участков)

(6-8), рабочие (9-11), кладовщик (12). С учетом клиентов (1-2), граф обработки информации будет иметь вид, представленный на рис. 1. В скобках указаны соответствующие номера узлов графа, а стрелки указывают направление “движения” информации.

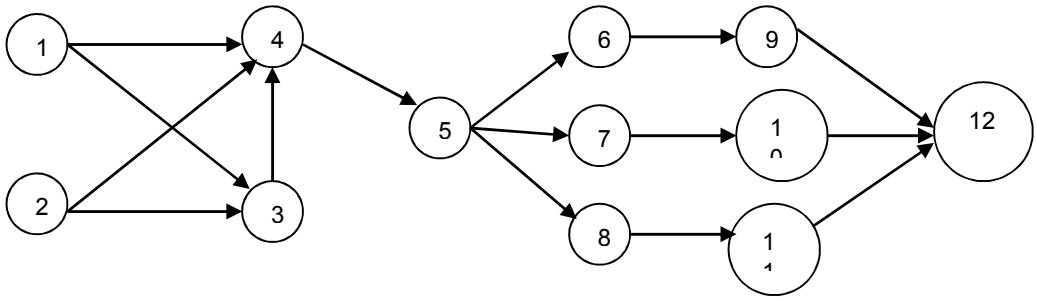

Рис. 1 Общий вид графа

Рассматривая решение первой задачи, становится очевидно, что порядок обработки по каждому клиенту идентичен. Идентичен, так же, и порядок обработки информации между рабочими и мастерами. Поэтому граф можно упростить (рис. 2).

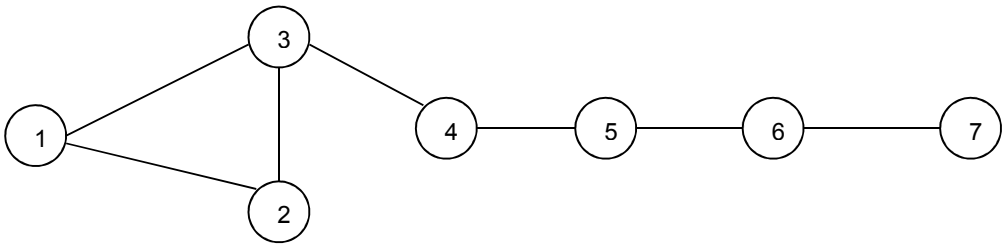

Рис. 2 Упрощенный вид графа

Номерами здесь обозначены следующие узлы:

1 – клиент;
2 – менеджер;
3 – бухгалтер;
4 – работник планового отдела;
5 – начальник цеха (мастер);
6 – рабочий;
7 – кладовщик.

К тому же граф перестал быть направленным. Это произошло потому, что информация будет “двигаться” в обоих направлениях. Рассмотрим этот процесс подробней.

Предположим, что клиент хочет сделать заказ на производство продукции данного предприятия. Его переговоры с менеджером закончились успешно. В этом случае заключается договор, по одной копии которого остаются у каждой стороны. Этот этап будет соответствовать плечу 1 – 2. Менеджер сообщает бухгалтеру о состоявшейся сделке, что будет соответствовать плечу 2 – 3. Для данной процедуры необходимо предусмотреть внутренний документ предприятия. Таким документом может быть, например, “Отчет менеджера”.

Далее клиент направляется к бухгалтеру, который выписывает “Счет на предоплату” – плечо 3 – 1. Клиент оплачивает заказ наличными или, скорей всего, через банк и предоставляет документы бухгалтеру предприятия, плечо 1 – 3. Получив подтверждение заказа, бухгалтер передаёт информацию о заказе в плановый отдел в виде внутреннего документа, например, “Заявки на выполнение заказа”. Плечо 3 – 4.

Работник планового отдела, получив сведения о всех заказах, рассчитает сколько каких деталей необходимо сделать в каком цеху. После чего передаст “Требование на выполнение работ” (внутренний документ) каждому начальнику цеха. Плечо 4 – 5.

Начальник цеха поставит задачу рабочему устно или в виде “Наряда”. Плечо 5 – 6. Рабочий выполнит задание и передаст готовую продукцию на склад по внутренней накладной. Плечо 6 – 7, 7 – 6. Копию накладной рабочий также отдаст мастеру в виде отчета о проделанной работе. Плечо 6 – 5. В свою очередь, мастер (начальник цеха) передаст “Отчет о выполнении заказов” (внутренний документ) в плановый отдел. Плечо 5 – 4.

Плановый отдел соберёт сведенья о выполненных заказах или о ходе их выполнения и передаст в бухгалтерию в виде “Отчета о работе предприятия” (внутренний документ). Плечо 4 – 3. Бухгалтер передаст эти сведенья менеджерам. Причем, если на предприятии несколько менеджеров, то каждый получит отчет о “своих” заказах. Информация поступит в виде “Отчёта о выполненных заказах” (внутренний документ). Плечо 3 – 2.

Для того, что бы менеджер мог получить информацию о выполнении заказа и сообщить об этом клиенту, плановый отдел может передавать эту информацию непосредственно менеджеру. Но в это случае появится лишний документ, так как бухгалтер всё равно должен знать, кем и какой заказ выполнен, для того, чтобы рассчитать зарплату. Менеджер может сообщить клиенту о выполнении заказа устно. Плечо 2 – 1. Таким образом весь граф “замкнулся”. А все плечи оказались двунаправлены.

В документообороте участвуют следующие документы:

1. Договор – 2 экз.
2. “Счет на предоплату” – 1 экз.
3. Платежные документы (выписываются согласно требованиям бухгалтерского учета).
4. “Отчет менеджера” – 1 экз.
5. “Заявка на выполнение заказа” – по числу заказов или одна на все.
6. “Требование на выполнение работ” – по числу цехов.
7. “Наряд” – по числу рабочих, каждый день.
8. “Накладная” – 3 экз. на каждое изделие.
9. “Отчет о выполнении заказов” – по числу цехов.
10. “Отчет о работе предприятия” – один документ за период (возможно – каждый день)
11. “Отчет о выполненных заказах” – на каждого менеджера

Из одиннадцати документов – восемь внутренних. Название этих документов может быть и другим. Но смысл остаётся – документально закрепить факт передачи информации от одного исполнителя другому. Форму и содержание подобных документов необходимо разрабатывать исходя из особенностей производства.

С целью обеспечения категорий безопасности аутентичности и аппелируемости необходимо ввести такой внутренний документ, как “Журнал учета документов”. В “Журнале…” должны быть предусмотрены поля с информацией о виде передаваемых документов, реквизитах документа, авторе, а так же кому и когда документ передан. Пример записи в “Журнале…” показан в таблице 1.

Таблица 1

№ п.п.	Документ, номер, дата	Автор	Число	Кому передан, роспись
1.	*Отчет менеджера, № 000326, от 26.07.05*	*менеджер Иванов*	*27.07.05*	*бухгалтер Петрова*

Для обеспечения условия не распространения информации о состоявшейся сделке, необходимо защитить информацию на участке от узла 1 до узла 4. Именно здесь, в документах, будут содержаться сведенья о договоре с клиентом. На участке 4 – 7 будет информация обо всех или о нескольких заказах сразу. Это не позволит выяснить, для кого именно предназначена продукция, даже если эти документы будут разглашены. Другими словами для документов участка 4 – 7 отсутствует сама угроза НСД. Значит, угрозы безопасности информации на этом участке рассматривать нет необходимости.

Рассмотрим угрозы на других участках. Предположим, что на предприятии уже создана СЗИ для целей, не описанных в задании. Оценим угрозы для плеча 1 – 2. Переговоры проходят в кабинете менеджера. Этот кабинет защищён. Соответственно, вероятность утечки информации о сделке отсутствует, т.е. P = 0. Однако остаётся вероятность случайной встречи двух клиентов в офисе фирмы. Этот факт может косвенно указывать о готовящейся сделке. В этом случае все из трёх составляющих риска станут равны 1. Т.е. информация о факте сделке будет разглашена. Такая же опасность сохраняется и для плеча 1 – 3. На других участках, 2 – 3 и 3 – 4, информация передаётся внутри предприятия, где действует СЗИ. Значит вероятность разглашения P для этих участков равно 0. Сводная информация анализа представлена в таблице 2.

Таблица 2

Анализ выявленных угроз

№ п.п.	Описание		Канал, плечо	Значения условий	Значение риска
	угрозы	уязвимости			
1.	Раскрытие информации о сделке	Встреча клиентов в офисе	1 – 2	$P_t = 1$	P = 1
				$P_s = 1$	
				$P_p = 1$	
2.		Встреча клиентов в офисе	1 – 3	$P_t = 1$	P = 1
				$P_s = 1$	
				$P_p = 1$	

Если бы СЗИ на предприятии создана не была, то необходимо было бы рассматривать и другие угрозы и уязвимости их реализующие. Причем, наверняка, пришлось бы исследовать условия возникновения риска, и значения вероятностей P_t, P_s, P_p, и сам риск P могли бы отличатся от 0 или 1. В этом случае можно было бы сделать выводы о целесообразности устранения той или иной уязвимости.

Порядок выполнения работы

1. В качестве моделей предприятий использовать модели представленные в лабораторной работе № 1. Считать, что на предприятиях никакой СЗИ не создано.
2. Разработать традиционный (“бумажный”) документооборот, сопровождающий информацию по основной форме деятельности предприятия.
3. Разработать граф документооборота.
4. Упростить граф, при необходимости.
5. Описать содержание внутренних документов, в том числе и “Журналов учёта…”
6. Выявить и оценить угрозы безопасности информации.

Содержание отчета

Отчет представить на листах белой писчей бумаги форматом А4. Отчет должен содержать:

1. Титульный лист.
2. Полный граф документооборота.
3. Конечный упрощенный граф, промежуточные графы при необходимости.
4. Описание внутренних документов.
5. Таблицу анализа угроз безопасности информации.

Контрольные вопросы к лабораторной работе 2

1. Что подразумевается под понятием угрозы безопасности информации?
2. Что такое уязвимость? Как она может проявиться?
3. Какая количественная величина характеризует уязвимость?
4. Охарактеризуйте условия разведконтакта.
5. Какие меры можно предложить для устранения выявленных, в ходе лабораторной работы, уязвимостей.

3. Контрольная работа 2

Вопросы к контрольной работе № 2

1. Классификация информации по видам тайны и степеням конфиденциальности. Нормативно-правовые аспекты определения состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия.
2. Методика определения состава защищаемой информации. Порядок внедрения Перечня сведений, составляющих КТ, внесение в него изменений и дополнений.
3. Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации. Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа.
4. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации.
5. Транспортные средства и особенности транспортировки. Состав средств обеспечения, подлежащих защите.
6. Особенности синтеза СЗИ АС от НСД. Методика синтеза СЗИ: общее описание архитектуры АС, системы защиты информации и политики безопасности; формализация описания архитектуры, исследуемой АС; формулирование требований к системе защиты информации; выбор механизмов и средств защиты информации; определение важности параметров средств защиты информации; оптимальное построение системы защиты для АС.
7. Выбор структуры СЗИ АС. Проектирование системы защиты информации для существующей АС.
8. Содержание концепции построения комплексной системы защиты информации. Объекты защиты. Цели и задачи обеспечения безопасности информации.
9. Основные угрозы безопасности информации АС организации. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.
10. Определение потенциальных каналов и методов несанкционированного доступа к информации. Определение возможностей несанкционированного доступа к защищаемой информации.
11. Основные положения технической политики в области обеспечения безопасности информации АС организации. Основные принципы построения комплексной системы защиты информации.

12. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Первоочередные мероприятия по обеспечению безопасности информации АС организации.

13. Общая характеристика задач моделирования комплексной системы защиты информации.

14. Формальные модели безопасности и их анализ: классификация формальных моделей безопасности; модели обеспечения конфиденциальности; модели обеспечения целостности; субъектно-ориентированная модель. Прикладные модели защиты информации в АС.

15. Формальное построение модели защиты: описание объекта защиты; декомпозиция АС на субъекты и объекты; модель безопасности: неформальное описание; декомпозиция системы защиты информации; противостояние угрозам; реализация системы защиты информации субъекта АС субъектно-объектной модели.

16. Формализация модели безопасности: процедура создания пары субъект – объект, наделение их атрибутами безопасности; осуществление доступа субъекта к объекту; взаимодействие с внешними сетями; удаление субъекта – объекта.

17. Общее содержание работ по организации комплексной системы защиты информации. Характеристика основных стадий создания комплексной системы защиты информации.

18. Назначение и структура технического задания (общие требования к содержанию). Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию.

Раздел 3. Обеспечение комплексной системы защиты информации

1. ***Вопросы для обсуждения.***

1) Специфика персонала предприятия как объекта защиты.

2) Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации.

3) Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа.

4) Подбор и обучение персонала.

5) Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации.

6) Перечень вопросов ЗИ, требующих документационного закрепления.

2. ***Лабораторная работа № 3***

Тема: Подбор технических средств для обеспечения защиты информации

Цель:

1. Закрепить знания, полученные на лекциях.
2. Получить практические навыки в решении многокритериальных задач.
3. Получить опыт исследования слабоформализуемых проблем и методов их решения.

Введение

Технические средства (ТС), обеспечивающие защиту информации, являются одним из основных компонентом комплексной СЗИ. Поэтому подбор ТС является важной задачей при построении СЗИ. Основным критерием при этом будет оптимальное выполнение задач, стоящих перед всей системой в целом. Поскольку эти задачи противоречивы и зачастую даже антагонистичны, то выполнение всех условий оказывается труднодостижимым. Таким образом, подбор ТС является многокритериальной задачей.

Теоретическая часть

При подборе ТС для обеспечения работы любой, даже самой сложной, системы необходимо руководствоваться основным правилом – состав ТС определяется исключительно задачами, стоящими перед этой системой. А не наоборот. К сожалению, на практике можно часто наблюдать отход от этого правила. Зачастую техника подбирается исходя из престижа, моды, эстетических соображений и т.п. Как правило, это приводит к неоправданным расходам. Поэтому основными критериями для выбора ТС должны быть те, которые продиктованы выполнением основных задач системы.

При таком подходе, первым этапом является чёткое определение состава основных задач. Затем, необходимо определить сопутствующие задачи, т.е. такие задачи, без решения которых, выполнение основных задач не возможно. Это будет составлять второй этап. Для качественного анализа основных и сопутствующих задач необходимо хорошо представлять технологические процессы, происходящие на предприятии. Провести их декомпозицию, используя методы теории графов.

В данной работе, студентам предлагается подобрать ТС для обеспечения работы АСОД предприятия. Таким образом, основными задачами будут: ввод, хранение и обработка информации. По условиям работы, каждому из предприятий так же необходимо передавать часть данных из филиалов в центральный офис. Т.е. возникает задача обеспечения связи между компонентами АСОД разных офисов. Эта связь может осуществляться как через Internet, так и другими способами, например, передачей сведений на электронных носителях с посыльным.

Каждому предприятию необходимо сохранять часть информации в секрете, а значит, возникает первая из сопутствующих задач – защита от НСД к информации. Так же, любому предприятию необходимо оформлять “бумажные” документы. Следовательно, второй задачей будет обеспечение издания таких документов. Для обеспечения архива, необходимо производить резервное копирование. Возможно, возникнет необходимость обеспечения бесперебойного питания и т.д. Другие сопутствующие задачи будут зависеть от специфики предприятия.

Определение основных и сопутствующих задач необходимо для определения параметров ТС. Определение параметров ТС составляет третий этап. Из чего складываются параметры. Рассмотрим на примере.

Итак, на каждом предприятии, предлагаемом в данной работе, есть база данных, используемая для его управления. Основная задача состоит в том, что бы вносить в эту базу данных информацию, хранить и обрабатывать её. Соответственно, основные параметры ТС, выполняющих эту задачу должны касаться необходимого объёма памяти и быстродействия компьютеров (ПК).

Какой объём памяти ПК (дискового пространства) необходим для хранения базы. Это зависит от многих параметров: платформы, на которой реализована база, реализации каждого объекта базы и т.д. Такие величины являются чисто эмпирическими. Предположим, что вся информация базы данных логически разбита на объекты, условно называемые “документами”. Таким образом, база данных представляет собой, собственно, базу данных документов и комплекс программ, осуществляющих их обработку. Объём программной части, как правило, декларируется производителем, и является неизменным. База документов постоянно растёт.

Сколько занимает памяти один документ определить практически не возможно. Однако, из практики, известно, что каждый документ будет увеличивать объём базы на величину от 500 до 1000 байт. Будем считать, условно, объём документа равный в среднем примерно 0,5 kb. Проанализировав темпы работы предприятия, можно установить, сколько документов заносится в базу ежедневно. Предположим, что в день заносится 100 документов. Значит, база ежедневно вырастает на 50 kb. За год (в году ≈ 270 рабочих дней) на ≈ 15 Mb (13500 kb). Соответственно, необходим ПК с дисковым пространством,

позволяющим ежегодный прирост базы на 15-20 Mb. Исходя из возможностей современной техники, такой параметр сможет обеспечить любой компьютер.

Какие условия и как будут влиять на быстродействие ПК. Очевидно, что работу с базой данных можно условно разбить на внесение документов и их обработку, которая будет состоять из формирования статистических и аналитических отчетов. В свою очередь внесение каждого документа, так же условно, можно разбить на три этапа: формирование нового объекта "документ" – открытие документа, внесение пользователем в него информации – заполнение документа и запись содержимого документа в базу – закрытие документа.

Время работы на втором этапе – заполнение документа – зависит в основном от работы пользователя. На быстродействие ПК этот этап влияния оказывать не будет. Количество операций на первом и третьем этапе посчитать не возможно. Можно предположить, что при открытии совершается миллиарды операций (условно 1 мил.). Известно, что при закрытии – их в сотни раз больше (условно 100 мил.). При этом каждая операция происходит за один такт микропроцессора. Соответственно, любой современный ПК "откроет" документ менее чем за 1 с., а "закроет" документ за 0,5-1 мин. Такие показатели быстродействия нас так же устроят.

В связи со спецификой работы реляционной базы данных, время формирование отчетов в основном зависит от выполнения так называемых SQL-запросов. А точнее, от их числа, сложности и платформы, на которой реализована база. Время их работы даже условно определить не возможно. В этом случае мы можем полагаться только на производителя. Конечно, наиболее распространённые базы данных, например бухгалтерские, широко обсуждаются, в том числе и в Internet. В таком случае, возможно поинтересоваться мнением специалистов уже работавшим с продуктом. Но и в этом случае маловероятно, что оценка будет объективной.

На каждом предприятии используется ЛВС, и каждая база данных работает в сетевом варианте. Рассмотрим, как это будет влиять на быстродействие. С точки зрения места хранения и обработки информации все базы данных можно разделить на два типа: "файл-сервер" и "клиент-сервер". В первом случае на сервере база данных только хранится. А вся обработка происходит непосредственно на АРМ – "клиенте". Во втором – клиент только лишь формирует запрос базе данных. Всю обработку производит сервер, и на клиент попадает уже результат.

Таким образом, при использовании технологии "файл-сервер", на АРМ каждый раз будет необходимо "перебрасывать" всю базу данных. В настоящее время наиболее распространены ЛВС с пропускной способностью 100 Mbit/c, что позволяет пересылать примерно 12 Mb в течении 1 с. С учетом служебной информации, годовая база данных будет передаваться за 2-3 с. Таким образом, открытие и закрытие документа будет происходить за 3-4 с. Если в сети работает два ПК, один из которых выполняет роль файл-сервера, или если пользователи работают не одновременно, то такая характеристика нас вполне устроит.

В последнее время наибольшее распространение получили клиент-серверные базы данных. Из практики известно, что вариант клиент-сервер уменьшает нагрузку на сеть примерно в 300 раз. Соответственно, во столько же возрастает нагрузка на сервер. Что накладывает дополнительные требования по производительности и надёжности оборудования сервера.

Таким образом, мы выявили, что характеристиками, влияющими на выполнение основной задачи, будут: быстродействие микропроцессоров (МК) ПК рабочих станций и сервера, объём дискового пространства, пропускная способность ЛВС. Критичные значения этих характеристик и станут критериями подбора техники. Для качественного анализа, их необходимо свести в таблицу. Пример такой таблицы – табл. 1.

Таблица 1

№ п.п.	Задача	Критерий	Значение
1.	Работа с базой данных		

	– характеристики ПК	Тактовая частота МК	1000 kHz
		Объём жесткого диска (для базы данных)	> 20 Mb
	– характеристики ЛВС	Пропускная способность ЛВС	100 Mbit/c

Рынок предлагает большое количество ТС, имеющих различные свойства, так или иначе влияющих на выполнение задач. Выбор наиболее оптимального средства, в соответствии с выявленными критериями, составляет четвёртый этап. С учетом того, что каждое средство характеризует более чем 10 параметрами, задача выбора ТС становится достаточно сложной. Подобные задачи можно решать методами решения многокритериальных задач.

Существует несколько способов решения многокритериальных задач. В данной работе студентам предлагается “Метод свёртки и нормализации критериев”. Данный метод принятия технических решений применяется тогда, тогда все критерии имеют числовые значения, или их значения можно свести к таковым.

Суть метода состоит в следующем. Пусть имеется система S, характеризующаяся множеством критериев Q и состояний E. Каждый критерий $q_j \in Q$ не зависит от других критериев, имеет четкое числовое значение в каждом состоянии $e_i \in E$ (таб. 2). Необходимо выбрать такое e_i, при котором вектор q_j был бы оптимальным.

Таблица 2

	q_1	q_2	…	q_n
e_1	(r_{11})	(r_{12})	…	(r_{1n})
e_2	(r_{21})	(r_{22})	…	(r_{2n})
e_3	(r_{31})	(r_{32})	…	(r_{3n})
…	…	…	…	…
e_n	(r_{n1})	(r_{n2})	…	(r_{nn})

Каждая пара $(e_i q_j)$ представляет собой число r_{ij} из множества значений критериев R ($r_{ij} \in R = E \times Q$), причем для каждого q_k может быть свой оптимум, как правило, либо максимальное либо минимальное значение. Индексы i (i = 1, 2, 3…n) – номер ячейки (таб. 2) в столбце, j (j = 1, 2, 3,…n) – в строке.

Задача решается следующим образом. Сначала необходимо все значения r_{ij} привести к безразмерному виду. Для этого вводятся коэффициенты c_{ij}, такие что

$$\sum_i c_{ij} = 1,$$

для каждого q_j. Расчет каждого коэффициента производится исходя из следующего правила:

$$c_{ij} = \frac{(r_{ij})}{\max(r_{ij})}, \qquad (1)$$

т.е. каждое значение параметра в столбце разделить на максимальное значение из этого столбца. После этого, каждый критерий заменяется на коэффициент.

Далее необходимо выбрать по какому оптимуму будет производиться решение. Как отмечалось выше, для каждого критерия q существует свой оптимум. Причем, в рамках одной задачи, зачастую приходится одновременно выбирать максимум для одного критерия (например, тактовая частота) и минимум для другого (например, стоимость). Для того, что бы производить подбор по одному оптимуму, необходимо: во-первых, выбрать, производить подбор по минимуму или по максимуму; во-вторых, коэффициенты

критериев, обратных выбранному оптимуму, заменить на обратные, т.е. на значения, равные $\frac{1}{c_{ij}}$.

Для исключения влияния размерности шкал, вводятся нормировочные коэффициенты p_j (один на столбец). Каждый коэффициент p_j рассчитывается по следующему правилу:

$$p_j = \frac{1}{\sum_i c_{ij}}, \qquad (2)$$

После чего – умножить каждый c_{ij} на свой нормировочный коэффициент p_j.

Таким образом, мы получаем следующую таблицу (табл. 3)

Таблица 3

	q_1	q_2	…	q_n
e_1	$(p_1 \cdot c_{11})$	$(p_2 \cdot c_{12})$	…	$(p_n \cdot c_{1n})$
e_2	$(p_1 \cdot c_{12})$	$(p_2 \cdot c_{22})$	…	$(p_n \cdot c_{2n})$
e_3	$(p_1 \cdot c_{13})$	$(p_2 \cdot c_{23})$	…	$(p_n \cdot c_{3n})$
…	…	…	…	…
e_n	$(p_1 \cdot c_{1n})$	$(p_n \cdot c_{n2})$	…	$(p_n \cdot c_{nn})$

В этой таблице все значения – безразмерны и нормированы. Это значит, что их можно сравнивать между собой. Поэтому, для получения результата необходимо сложить значения критериев построчно и выбрать в образовавшемся векторе, оптимум, соответствующий решению задачи. Номер критерия (индекс i) будет соответствовать номеру оптимального состояния e_i, которое, в свою очередь, будет решением задачи.

Если в нормированной таблице некоторые значения, соответствующие важным критериям, которыми нельзя пренебрегать, оказываются заведомо малыми, то операцию сложения заменяют на операцию умножения. Т.е., при поиске максимума, перемножают построчно. При поиске минимума критичные значения перед умножением заменяют на обратные, т.е. на значения $1/(p_j \cdot c_{ij})$.

Порядок выполнения работы

Содержание работы:

Работа рассчитана на 6 часов. В ходе работы студенты должны определить перечень основных и сопутствующих задач для АСОД на предложенных моделях предприятий, а так же подобрать необходимые ТС для обеспечения работы АСОД и защиты информации в ней.

Условия выполнения:

В качестве моделей предприятия использовать модели, предложенные в лабораторной работе № 1. ТС предлагать на основе реально существующей техники. Быть готовым представить результаты расчетов.

Содержание отчета:

Отчет представить на листах белой писчей бумаги форматом А4. Отчет должен содержать:

1. Титульный лист.
2. Таблицу основных и сопутствующих задач (пример таб. 1)
3. Перечень выбранных ТС с их характеристиками и стоимостью.
4. Прайс-листы фирм-поставщиков.

Контрольные вопросы к лабораторной работе 3

1. Обоснуйте предложенные Вами основные и сопутствующие задачи, а так же выявленные критерии.
2. Какие угрозы безопасности информации в АСОД Вам известны? Дайте им характеристику.

3. Какие методы подбора ТС Вам известны? Охарактеризуйте их.
4. Обоснуйте, почему Вами были предложены именно такие ТС.
5. Какие требования к СЗИ Вам известны? Дайте им характеристику.
6. Какие средства защиты локальных ПК вам известны? От каких угроз они защищают.
7. Какие средства сетевой защиты Вам известны? Дайте характеристику этих средств.

3. Контрольная работа 3

Вопросы к контрольной работе № 3

1. Специфика персонала предприятия как объекта защиты.
2. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации.
3. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа.
4. Подбор и обучение персонала.
5. Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации.
6. Перечень вопросов ЗИ, требующих документационного закрепления.

4. Промежуточный тест

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

Тест 1. Моделирование ТКУИ поводится на основе пространственных моделей расположения источников и приемников информации
- С указанием конкретных расстояний между ними
- С указанием примерных расстояний между ними
- Без указания конкретных расстояний между ними
- Без указания примерных расстояний между ними

Тест 2. К техническим мероприятиям с использованием пассивных средств защиты относят
- пространственное зашумление
- экранирование ТСПИ и их соединительных линий
- линейное зашумление
- уничтожение закладных устройств

Тест 3. Одним из способов экранирования источников ПЭМИН является
- магнитодинамическое
- электродинамическое
- магнитостатическое
- стохастическое

Тест 4. На рис.1 представлена структурная схема

Рис. 1. Структурная схема канала утечки информации

- оптического канала утечки информации
- акустического канала утечки информации
- электронного канала утечки информации
- акустооптического канала утечки информации

Тест 5. К техническим мероприятиям с использованием активных средств защиты относят

- пространственное зашумление
- локализация излучений
- установка устройств гарантированного электропитания ТСПИ
- экранирование ТСПИ

Раздел 4. Управление комплексной системой защиты информации

1. Вопросы для обсуждения.

1) Понятие, сущность и цели управления комплексной системы защиты информации.

2) Принципы управления комплексной системы защиты информации. Структура процессов управления.

3) Основные процессы, функции и задачи управления комплексной системы защиты информации.

4) Основные стили управления. Структура и содержание общей технологии управления комплексной системы защиты информации.

5) Понятие и задачи планирования функционирования комплексной системы защиты информации. Способы и стадии планирования.

6) Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании.

7) Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов.

8) Виды контроля функционирования комплексной системы защиты информации.

9) Цель проведения контрольных мероприятий в комплексной системы защиты информации. Анализ и использование результатов проведения контрольных мероприятий.

10) Понятие и основные виды чрезвычайных ситуаций.

11) Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС.

12) Подготовка мероприятий на случай возникновения ЧС.

2. Проект

Задачами выполнения проекта являются: анализ каналов утечки информации; анализ угроз безопасности; выбор наиболее эффективных технических методов и средств защиты информации; принятие мер противодействия.

В проекте рассматривается организация, в которой перерабатывается (сбор, хранение, обработка и выдача) информация.

В проекте объектом защиты является информация, хранящаяся и обрабатываемая в организации, физическую основу которой представляет корпоративная сеть, состоящая из одной локально вычислительной сети и размещенная территориально в комплексе из одного здания. В такой сети организована специальная коммуникационная система обмена сообщениями (электронная почта, факс, совместная работа над документами).

Конфиденциальная информация в организации может передаваться по заданному подмножеству каналов передачи данных. Полное их множество содержит: акустический канал (для передачи информации между персоналом), аналоговый и стандартный цифровой

каналы (для передачи информации между основными техническими средствами). Конкретное подмножество каналов задается вариантом работы (Таблица 1).

Физическая среда передачи информации в проекте определяется заданным подмножеством линий связи. Полное их множество содержит: витую пару и коаксиальный кабель (реализующие среду передачи информации в ЛВС), телефонную линию связи (ТЛС), волоконно-оптическую линию связи (ВОЛС), мобильные телефонные системы (реализующие передачу информации между персоналом и техническими средствами). Конкретное подмножество линий связи задается вариантом задания (Таблица 2).

Каналы утечки информации в организации по физическим принципам можно классифицировать на следующие группы: прямой акустический канал; побочные электромагнитные излучения и наводки (ПЭМИН); наводки по цепям питания и заземления; в линиях связи; паразитная генерация; вибро-акустический канал; оптико-акустический канал; электроакустический канал. Предполагается, что незащищенными из этого списка является некоторое подмножество каналов утечки информации, задаваемое вариантом задания (Таблица 3).

Способы несанкционированного доступа к данным можно разделить на два вида: косвенные и прямые. Косвенные способы несанкционированного доступа к данным, в отличие от прямых, не требуют непосредственного доступа в хранилище информации. Прямые способы доступа могут быть без изменения и с изменением структуры системы Проектируемая система защиты должна оказывать эффективное противодействие заданному подмножеству (Таблица 4).

На основе исходных данных (Таблица 1 – 4) необходимо разработать систему защиты информации от утечки по техническим каналам.

Основные этапы построения оптимальной системы защиты информации от утечки по техническим каналам на предприятии:

1.Проводится анализ структурного построения, принципов функционирования объекта защиты, особенности технических каналов связи и выделяются на основе анализа уязвимые элементы, которые влияют на безопасность объекта.

2. Определяются и анализируются возможные угрозы для выделенных элементов и формируется перечень требований к системе защиты.

3. Обосновываются наиболее подходящий вариант средств и мер защиты, использование которых позволяет реализовать каждую из функций защиты, и для этих средств и мер приближенно определяются показатели эффективности.

4. Определяется структура системы защиты и составляется ее описание и описание планируемых организационных мероприятий по защите информации

Таблица 1. Канал передачи информации

Вариант	Акустический канал	Аналоговый канал	Стандартный цифровой канал
1	•	•	
2	•		•
3	•	•	
4		•	•

5	•	•	
6	•		•
7	•	•	
8	•		•
9	•	•	
10	•		•
11	•	•	
12		•	•
13	•	•	
14	•		•
15	•	•	
16	•		•
17		•	•
18	•		•
19	•	•	
20		•	•
21	•	•	
22	•		•
23	•	•	
24	•		•
25	•	•	
26	•	•	
27	•	•	
28	•		•
29		•	•
30	•		•

Таблица 2. Среда передачи (линии связи)

Вариант	Телефонная линия связи	Витая пара	Коаксиальный кабель	Волоконно оптическая линия связи	Мобильные системы беспроводных
1		•			•
2	•		•		•
3	•			•	•
4	•	•			•
5			•	•	•
6	•			•	•
7	•	•			•
8	•		•		•

9	•			•	•
10	•	•			•
11	•		•		•
12	•			•	•
13		•		•	•
14	•		•		•
15	•			•	•
16	•	•			•
17		•	•		•
18	•			•	•
19	•	•			•
20	•		•		•
21	•			•	•
22	•	•			•
23	•		•		•
24	•			•	•
25		•		•	•
26	•			•	•
27		•	•		•
28	•	•			•
29	•		•		•
30	•			•	•

Таблица 3. Возможные каналы утечки информации

Вариант	Побочные Э/М наводки	Побочные Э/М излучения	По цепям питания	По цепям заземления	В линиях связи	Паразитная генерация	Вибро акустический канал	Оптико акустический канал	Электро акустический канал	Прямой акустический канал
1	•				•	•			•	
2		•			•	•		•		

3			•		•		•			•
4				•	•				•	•
5	•				•	•		•		•
6		•			•	•	•			
7			•		•				•	•
8				•	•			•		•
9	•				•		•			•
10		•			•	•			•	
11			•		•			•		•
12				•	•		•			•
13	•				•				•	•
14		•			•	•		•		
15			•		•		•			•
16				•	•				•	•
17	•				•	•		•		•
18		•			•	•	•			
19			•		•				•	•
20				•	•			•		•
21	•				•		•			•
22		•			•	•			•	
23			•		•			•		•
24				•	•		•			•
25	•				•				•	•
26		•			•	•				•
27			•		•	•			•	
28		•		•	•			•		
29	•				•		•		•	
30		•			•	•		•		

Таблица 4. Способы несанкционированного получения информации

Вариант	Применение подслушивающих устройств	Перехват электромагнитных излучений	Перехват электромагнитных наводок	Перехват информации по каналам передачи	Скрытая запись аудиоинформации	Скрытая запись видеоинформации	Высокочастотное навязывание	Преодоление программных средств защиты	Маскировка под зарегистрированного пользователя с помощью похищенных паролей и других реквизитов разграничения доступа	Маскировка несанкционированных запросов под запросы операционной системы	Использование программных закладок	Преднамеренное включение в библиотечные программы специальных блоков типа «троянских коней», регистрирующих обрабатываемые данные в интересах злоумышленников	Незаконное подключение к аппаратуре или линиям связи вычислительной системы	Вывод из строя механизма защиты.
1		•		•	•		•						•	•
2	•	•		•		•		•					•	
3	•	•		•	•				•				•	
4	•		•	•		•				•			•	
5	•		•	•	•						•		•	
6	•		•	•		•						•	•	
7		•		•	•				•				•	•
8	•	•		•		•				•			•	
9	•	•		•	•						•		•	
10	•		•	•		•						•	•	
11	•		•	•	•				•				•	
12	•		•	•		•				•			•	
13		•		•	•						•		•	•
14	•	•		•		•						•	•	
15	•	•		•	•				•				•	
16	•		•	•		•				•			•	
17	•		•	•	•						•		•	
18	•		•	•		•						•	•	
19		•		•	•				•				•	•
20	•	•		•		•				•			•	
21	•	•		•	•						•		•	
22	•		•	•		•						•	•	
23	•		•	•	•				•				•	
24	•		•	•		•				•			•	
25		•		•	•						•		•	•
26	•	•		•		•						•	•	
27	•	•		•	•				•				•	
28	•		•	•		•				•			•	
29	•		•	•	•						•		•	
30	•		•	•		•						•	•	

3. ***Контрольная работа 4.***

Вопросы к контрольной работе 4

1. Понятие, сущность и цели управления комплексной системы защиты информации.
2. Принципы управления комплексной системы защиты информации. Структура процессов управления.
3. Основные процессы, функции и задачи управления комплексной системы защиты информации. Основные стили управления.
4. Структура и содержание общей технологии управления комплексной системы защиты информации.
5. Принципы и методы планирования функционирования комплексной системы защиты информации
6. Понятие и задачи планирования функционирования комплексной системы защиты информации. Способы и стадии планирования.
7. Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании.
8. Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов.
9. Сущность и содержание контроля функционирования комплексной системы защиты информации
10. Виды контроля функционирования комплексной системы защиты информации.
11. Цель проведения контрольных мероприятий в комплексной системы защиты информации.
12. Анализ и использование результатов проведения контрольных мероприятий.
13. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций
14. Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях ЧС.
15. Факторы, влияющие на принятие решений в условиях ЧС.
16. Подготовка мероприятий на случай возникновения ЧС.

Раздел 5. Оценка эффективности комплексной системы защиты информации

1. ***Вопросы для обсуждения.***
   1) Вероятностный подход.
   2) Оценочный подход.
   3) Требования РД СВТ и РД АС.
   4) Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408□2002.
   5) Экспериментальный подход.
   6) Показатель уровня защищенности, основанный на экспертных оценках.
   7) Методы проведения экспертного опроса.
   8) Экономический подход к оценке эффективности комплексной системы защиты информации.
2. ***Лабораторная работа 4***

Тема: Анализ рисков безопасности информации

Цель:

1. Получить навыки оценки рисков безопасности информационной системы предприятия.

2. Получить практический опыт подбора критериев информационной безопасности системы

3. Закрепить теоретические навыки, полученные на лекциях

Введение

При построении комплексных систем защиты информации зачастую трудно определить уровень различных угроз безопасности. Это может привести к неадекватным мерам по их нейтрализации. Для избежания подобных ситуаций необходима количественная оценка степени влияния угроз безопасности информации на информационную систему.

Целью анализа рисков является количественная оценка угроз и уязвимостей, позволяющая определить комплекс контрмер, обеспечивающий достаточный уровень защищенности информационной системы.

Теоретическая часть

При проведении оценки рисков необходимо иметь чёткое представление таких понятий, *угроза* информационной безопасности и *уязвимость* информационной системы или системы защиты информации.

Угроза – совокупность условий и факторов, которые могут стать причиной снижения заданного уровня безопасности информации.

Уязвимость – слабость в системе защиты, которая делает возможным реализацию угрозы.

Риск нарушения ИБ – возможность реализации угрозы.

Величину риска можно определить, исходя из следующей формулы:

$$P = C \bullet P_y, \qquad (1)$$

где: P – величина риска,

C – стоимость информационного ресурса,

P_y – вероятность реализации угрозы.

Стоимость информационного ресурса – это количественная величина, характеризующая степень влияния данного ресурса на информационную систему. Его можно определить как уровень потерь, понесённых владельцами ресурса или информационной системой при его утрате или разглашении. В зависимости от реальных условий, стоимость может быть выражена либо в деньгах, либо условных единицах.

Вероятность реализации угрозы зависит от множества факторов. Основными из них будут:

– наличие самой угрозы;

– наличие и вероятность реализации уязвимостей системы;

– привлекательности уязвимости.

В рамках проведения данной лабораторной работы условимся не учитывать привлекательность той или иной уязвимости. Поскольку наличие угрозы может зависеть от субъективных факторов, например, желания злоумышленника реализовать угрозу, условимся не учитывать и этот фактор. Таким образом, примем вероятность реализации угрозы P_y равной вероятности реализации уязвимости.

Вероятность реализации уязвимости можно рассчитать, исходя из следующей формулы:

$$P_y = P_s \bullet P_t \bullet P_p, \qquad (2)$$

где: P_s – пространственное условие, т.е. вероятность того, что уязвимость реализуется в том месте, где находится информация;

P_t – временное условие т.е. вероятность того, что уязвимость реализуется в тот момент, когда информация существует;

$P_р$ – энергетическое условие реализации уязвимости, вероятность того, что энергии, для выполнения уязвимости будет достаточно.

Перечисленные условия являются *основными факторами* выполнения уязвимости. Т.е. при невыполнении хотя бы одного из них уязвимость реализовать не возможно. Однако эти условия сами зависят от множества факторов. Факторы, от которых зависит выполнимость основных называются *косвенными*. Состав косвенных факторов, характер их влияния на основные заранее определить не возможно. Поэтому значения вероятностей наступления основных факторов будут вычисляться из значений вероятности наступления косвенных для каждого конкретного случая отдельно.

При вычислении значений основных факторов необходимо помнить, что это вероятностные характеристики и вычисляются по правилам теории вероятности. Таким образом, если основной фактор зависит от одного показателя (косвенного фактора) – *расчет по одному критерию*, то находится он, как отношение величины критерия к его максимальному значению. Проще говоря, меньшее необходимо разделить на большее. О правильности выбора и расчёта вероятности можно судить исходя из простого правила – *значение вероятности всегда должно быть меньше 1.*

Если значение вероятности наступления основного фактора зависит от нескольких критериев, то расчет может производится либо по *суммовым*, либо по *критическим* критериям. Суммовыми будут критерии, которые вносят определенную долю в вероятность наступления фактора и не зависят друг от друга. При этом необходимо вычислить вероятность наступления каждого из косвенных факторов методом расчета по одному критерию, а затем сложить их, используя следующую формулу:

$$P_{оф} = \sum_{i}^{n} P_i - \prod_{i}^{n} P_i \,, \qquad (3)$$

где, $P_{оф}$ – вероятность наступления основного фактора;
P_i – вероятность наступления косвенного фактора;
i – индекс фактора, n – количество факторов.

Критические – это критерии, которые зависят друг от друга. Т.е. такие критерии, от значения каждого из которых зависит наступление события. Вероятностные показатели этих критериев необходимо перемножить.

$$P_{оф} = \prod_{i}^{n} P_i \,, \qquad (4)$$

Рассмотри теперь что же является, собственно, самими косвенными факторами и их критериями. *Косвенным фактором* может являться всё, что может привести к реализации угрозы через уязвимость. А критерием является количественный показатель, по которому можно вычислить вероятность наступления этого события.

Например, для бумажного документа, косвенным фактором будет время его хранения. Точнее вероятность утери документа за это время. А критериями этого события могут быть: объем документа (количество листов), температурно-влажностный режим в месте хранения, вероятность кражи и т.д. Для электронной информационной базы данных – объём “винчестера” (или томов), скорость передачи в ЛВС, мощность или быстродействие микропроцессора, объем оперативной памяти и т.д.

Все эти показатели могут быть 3-х типов: технические, статистические и приведённые. *Технические* – это показатели, имеющие свои единицы измерения. Такие показатели, как правило, относятся к характеристикам технических устройств. Они имеют четкое значение в каждый момент времени, область определения или максимальное значение. Определение вероятности наступления неблагоприятного события по этим показателям является наиболее простым. Например, что бы определить вероятность разрушения базы данных на “винчестере”, необходимо объём базы данных разделить на полный объём “винчестера”.

Статистические – это показатели, которые можно определить исходя из статистической информации. Ярким примером служит такой показатель, как время наработки на отказ. Этот показатель определяется в период эксплуатации технического устройства на основании статистики отказов данного устройства.

Приведённые показатели – это показатели, определяемые по качественным оценкам: мало, нормально, много, отлично, хорошо, удовлетворительно, неудовлетворительно и т.п. Оценка их производится методами неформального оценивания. Примером такого показателя может служить лояльность работника своим руководителям.

Рассмотрим, теперь, механизм оценки информационных рисков. На первом этапе необходимо выяснить, какие угрозы характеры для объекта защиты. Их принято делить на 3 больших группы: угрозы доступности, целостности и конфиденциальности информации. Каждая из угроз должна принадлежать к одной из групп. Последовательное рассмотрение каждого множества угроз позволит не “пропустить” какую-нибудь из них.

Далее следует рассмотреть уязвимости, через которые может реализоваться угроза. Любая уязвимость актуальна только тогда, когда выполняются три условия – основные факторы. Последовательное рассмотрение каждого основного фактора позволит составить полный перечень косвенных, и “не пропустить” ни одного из них. Оценка показателей косвенных факторов, в свою очередь, позволит принять адекватное решение по нейтрализации угрозы информационной безопасности.

Сложность механизма оценки угроз обусловлена тем, что он не всегда очевиден и может привести к неэффективным или неадекватным решениям. Приведём пример. При работе в электронной информационной базе данных происходит потеря документов из-за частых сбоев в системе электроснабжения (СЭС). Наиболее очевидным решением является установка устройств бесперебойного питания (УБП). Но помогает это не всегда. Допустим, что к одной линии СЭС подключены и компьютеры, и двигатель системы вентиляции помещения. При включении двигателя в линии происходит падение напряжения. Из-за чего и происходит сбой в работе компьютеров. Использование УБП не помогло, так как из-за частых “скачков” напряжения аккумуляторы УБП быстро разряжаются и УБП выходят из строя. Более эффективным будет замена проводов линии электроснабжения на провода с большим сечением или подключение двигателя и компьютеров к разным линиям.

Рассмотрим эту ситуацию в соответствии с изложенной выше методикой. Угрозой безопасности информации является нестабильное электроснабжение. Уязвимости здесь две:

1) недостаточная стабилизация напряжения в СЭС,

2) “слабые” характеристики стабилизации напряжения в блоках питания компьютеров.

Для обоих уязвимостей “на лицо” выполнение всех трёх условий - основных факторов:

1) пространственный фактор – двигатель и компьютеры подключены к одной линии СЭС;

2) временной – двигатель включается и выключается в то же время, когда работают компьютеры;

3) энергетический – в момент включения двигателя – энергии для работы компьютеров не хватает.

Выделим множество параметров:

по первому фактору: необходимость наличия ПК и двигателя на одной линии питания (приведённый показатель: да/нет);

по второму фактору: вероятность одновременной работы двигателя и ПК, рабочее время сотрудников, связанных с работой в базе данных;

по третьему фактору: минимальное напряжение стабильной работы ПК, максимально возможная нагрузка в линии СЭС, сечение проводов линии, вероятность сбоя при включении двигателя.

Рассматривая ситуацию в таком порядке, даже без проведения расчетов, становится очевидным нарушение энергетического фактора – подключение двигателя к другой линии СЭС. Нарушение временного фактора едва ли возможно. Для принятия решения по третьему фактору возможно после проведения расчетов.

Порядок выполнения работы

В ходе работы студенту необходимо решить три задачи:

1. Оценить информационные ресурсы.

2. Выявить косвенные факторы, влияющие на выполнение уязвимостей и составить перечень их параметров.

3. Оценить информационные риски.

Оценка информационных ресурсов производится следующим образом:

1) определяется состав параметров, влияющих на стоимость ресурса.

2) количественные значения приводятся в безразмерный вид. Для этого текущее значение параметра необходимо разделить на его максимальное значение.

3) значения параметров складываются.

Для выполнения второй задачи, студентам необходимо рассмотреть угрозы и уязвимости в информационной системе предприятий, выявленные на предыдущих лабораторных работах. При этом необходимо использовать то предприятие (модель предприятия), которая рассматривалась рабочей группой ранее. Методика выявления факторов и их показателей изложена выше.

Оценка рисков, производится в соответствии с формулами (1) и (2).

Содержание отчета

Отчет по лабораторной работе выполняется на листах белой писчей бумаги формата А4 в печатном виде и должен содержать:

1. Титульный лист;

2. Тему и цель занятия;

3. Оценку информационных ресурсов (таблица 1);

Таблица 1.

Оценка стоимости ресурса

№ п.п.	Наименование ресурса	Параметры	Значение	Приведённое значение

4. Перечень параметров уязвимостей системы (таблица 2);

Таблица 2.

Перечень параметров уязвимости системы

№ п.п.	Параметр	Уязвимости	Значение

5. Оценку информационных рисков (таблица 3)

Таблица 3.

Оценка рисков информационной безопасности

№ п.п.	Уязвимость	Риск

Контрольные вопросы к лабораторной работе 4

1. Что называется угрозой информационной безопасности?
2. Что называется уязвимостью информационной системы?
3. Что называется информационным риском?
4. Дайте понятие основным и косвенным факторам уязвимости информационной системы.
5. Как оценить опасность уязвимости?
6. Какие типы показателей косвенных факторов уязвимости Вы знаете? Для чего они нужны?
7. Что является целью оценки информационных рисков?

3. ***Контрольная работа 5***

Вопросы к контрольной работе 5

1. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации
2. Вероятностный подход.
3. Оценочный подход.
4. Требования РД СВТ и РД АС.
5. Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408-2002.
6. Экспериментальный подход.
7. Состав методов и моделей оценки эффективности комплексной системы защиты информации
8. Показатель уровня защищенности, основанный на экспертных оценках.
9. Методы проведения экспертного опроса.
10. Экономический подход к оценке эффективности комплексной системы защиты информации.

4. ***Итоговый тест***

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

Тест 1. Одним из способов экранирования источников ПЭМИН является
- магнитодинамическое
- электродинамическое
- электромагнитное
- стохастическое

Тест 2. Одним из методов энергетического скрытия информации является
- Маскировка сигнала
- Дезинформирование
- Усиление сигнала
- Зашумление сигнала

Тест 3. Одним из методов информационного скрытия информации является
- Зашумление
- Ослабление сигнала
- Усиление сигнала
- Дезинформирование

Тест 4. Потенциальными излучателями _____ в виде ПЭМИН могут быть сигнальный кабель, видеоусилитель, потенциальный рельеф на экране кинескопа
- видеосигнала
- электрического сигнала
- акустического сигнала
- электромагнитного сигнала

Тест 5. В _____ каналах утечки информации средой распространения речевых сигналов является воздух
- виброакустических
- акустоэлектрических
- акустических
- параметрических

Перечень вопросов к экзамену

1. Цели, задачи и принципы построения комплексной системы защиты информации.
1. Разумная достаточность и экономическая эффективность. Управление безопасностью предприятия.
2. Международные стандарты.
3. Цели и задачи защиты информации в автоматизированных системах.
4. Современное понимание методологии защиты информации: особенности национального технического регулирования, современная трактовка понятия безопасности информационных технологий, современные требования к средствам обеспечения безопасности.
5. Принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ.
6. Методологические основы организации комплексной системы защиты информации.
7. Разработка политики безопасности и регламента безопасности предприятия.
8. Основные положения теории сложных систем. Система управления информационной безопасностью предприятия.
9. Требования, предъявляемые к комплексной системы защиты информации: требования к организационной и технической составляющим комплексной системы защиты информации; требования по безопасности, предъявляемые к изделиям ИТ.
10. Этапы разработки комплексной системы защиты информации.
11. Влияние формы собственности на особенности защиты информации ограниченного доступа. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа.
12. Состав, объекты и степень конфиденциальности защищаемой информации. Классификация информации по видам тайны и степеням конфиденциальности.
13. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия. Порядок внедрения Перечня сведений, составляющих КТ, внесение в него изменений и дополнений.
14. Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации.
15. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации.
16. Особенности синтеза СЗИ АС от НСД. Методика синтеза СЗИ: общее описание архитектуры АС, системы защиты информации и политики безопасности; формализация описания архитектуры, исследуемой АС; формулирование требований к системе защиты информации; выбор механизмов и средств защиты информации; определение важности параметров средств защиты информации; оптимальное построение системы защиты для АС.
17. Выбор структуры СЗИ АС. Проектирование системы защиты информации для существующей АС.
18. Содержание концепции построения комплексной системы защиты информации. Объекты защиты. Цели и задачи обеспечения безопасности информации.
19. Основные угрозы безопасности информации АС организации. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.

20. Определение потенциальных каналов и методов несанкционированного доступа к информации. Определение возможностей несанкционированного доступа к защищаемой информации.

21. Основные положения технической политики в области обеспечения безопасности информации АС организации.

22. Основные принципы построения комплексной системы защиты информации. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.

23. Формальные модели безопасности и их анализ: классификация формальных моделей безопасности; модели обеспечения конфиденциальности; модели обеспечения целостности; субъектно-ориентированная модель.

24. Прикладные модели защиты информации в АС.

25. Формальное построение модели защиты: описание объекта защиты; декомпозиция АС на субъекты и объекты; модель безопасности: неформальное описание; декомпозиция системы защиты информации; противостояние угрозам; реализация системы защиты информации субъекта АС субъектно-объектной модели.

26. Формализация модели безопасности: процедура создания пары субъект – объект, наделение их атрибутами безопасности; осуществление доступа субъекта к объекту; взаимодействие с внешними сетями; удаление субъекта – объекта.

27. Характеристика основных стадий создания комплексной системы защиты информации.

28. Назначение и структура технического задания (общие требования к содержанию). Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию.

29. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации.

30. Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации. Перечень вопросов ЗИ, требующих документационного закрепления.

32. Понятие, сущность и цели управления комплексной системы защиты информации.

33. Принципы управления комплексной системы защиты информации. Структура процессов управления.

34. Основные процессы, функции и задачи управления комплексной системы защиты информации. Основные стили управления.

35. Структура и содержание общей технологии управления комплексной системы защиты информации.

36. Принципы и методы планирования функционирования комплексной системы защиты информации

37. Понятие и задачи планирования функционирования комплексной системы защиты информации.

38. Способы и стадии планирования. Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании.

39. Методы сбора, обработки и изучения информации, необходимой для планирования.

40. Сущность и содержание контроля функционирования комплексной системы защиты информации. Виды контроля функционирования комплексной системы защиты информации.

41. Цель проведения контрольных мероприятий в комплексной системы защиты информации. Анализ и использование результатов проведения контрольных мероприятий.

42. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций

43. Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях ЧС.

44. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС.

45. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации

46. Вероятностный подход. Оценочный подход.

47. Требования РД СВТ и РД АС. Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408-2002.

48. Экспериментальный подход.

49. Состав методов и моделей оценки эффективности комплексной системы защиты информации. Показатель уровня защищенности, основанный на экспертных оценках.

50. Методы проведения экспертного опроса. Экономический подход к оценке эффективности комплексной системы защиты информации.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-4. Способность проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения с учетом требований информационной безопасности				
1.	Задание закрытого типа	Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации: а. Источник информации б. Потребитель информации в. Уничтожитель информации г. Носитель информации д. Обладатель информации	д	3
2.		Возможность получения информации и ее использования это: а. Сохранение информации б. Распространение информации в. Предоставление информации г. Конфиденциальность информации д. Доступ к информации	д	3
3.		Порядок и правила применения определенных принципов и средств защиты информации 1) Способ защиты информации 2) Система защиты информации	1	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		3) Метод защиты информации 4) Элемент защиты информации		
4.		Какие цели могут преследовать источники угроз (конкуренты, преступники, административно-управленческие органы)? 1. Ознакомление (получение) информации 2. Искажение (модификация) информации 3. Разрушение (уничтожение) информации 4. Обеспечение конфиденциальности, целостности, доступности информации	1, 2, 3	3
5.		Компонентами концептуальной модели безопасности информации могут быть ...? 1. объекты угроз 2. источники угроз 3. источники информации 4. способы и средства защиты информации 5. недобросовестные конкуренты 6. преступные группировки и формирования	1, 2, 3	3
6.	Задание открытого типа	Элементы, которые должна обязательно включать в себя политика безопасности согласно «Оранжевой книге»	Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы: • произвольное управление доступом; • безопасность повторного использования объектов; • метки безопасности; • принудительное управление доступом.	8
7.		Согласно «Оранжевой книге» дать определение политики безопасности	Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности — это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.	8
8.		Принципы проектирования систем технической защиты	Принципы проектирования систем технической защиты:	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности; многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности; избирательность, заключающаяся в предотвращении угроз в первую очередь для наиболее важной информации; интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности; создание централизованной службы безопасности в интегрированных системах	
9.		Комплекс мероприятий по защите выделенных помещений (ВП) или защищенных помещений	В общем случае комплекс мероприятий по защите выделенных помещений (ВП) или защищенных помещений (ЗП) включает: защиту речевой информации, обрабатываемой техническими средствами, от утечки за счет электромагнитных излучений и наводок (ПЭМИН); защиту речевой информации от утечки за счет эффекта электроакустического преобразования вспомогательных технических средств и систем (ВТСС); защиту речевой информации от утечки за счет лазерного зондирования стекол или стетоскопического прослушивания ограждающих конструкций; защиту речевой информации от утечки за счет несанкционированного доступа в помещение и скрытой установки в нем подслушивающих приборов; акустическую защиту помещений.	8
10.		Источники речевого сигнала	Источники речевого сигнала могут быть следующих видов: источник первичного речевого сигнала (говорящий человек): а) локализованный в определенной области пространства, ограниченного	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			ограждающими конструкциями помещения или границами контролируемой зоны; б) неопределенный (нелокализованный) в области пространства, ограниченного ограждающими конструкциями помещения или границами контролируемой зоны; технические средства звукоусиления и звуковоспроизведения; технические средства передачи речевых сигналов по проводным линиям связи; технические средства передачи речевых сигналов по радиоканалу	

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению экзамена

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:

- тема лабораторной работы,
- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

Критерии оценки лабораторных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по предмету.

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретический заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Критерии оценки проекта:

– оценка «отлично» выставляется обучающемуся, если студент представил отчет в соответствии с методическими указаниями, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход;

– оценка «хорошо» выставляется обучающемуся, если студент представил отчет в соответствии с методическими указаниями, информация в отчете сформулирована обоснованно, формулировки конкретные, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент представил отчет в соответствии с методическими указаниями, информация в отчете

сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не представил отчет или выполнил задания неверно, без использования методических указаний, обоснования неверные, сделаны грубые ошибки.

Критерии оценки деловой игры:

– оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;
- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.
- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.
- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;
- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

Критерии оценок на экзамене:

40-50 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности.

35-39 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.

25-34 балла – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера.

20-24 балла – студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы.

15-19 баллов – студент отвечает в основном правильно, но чувствуется механическое заучивание материала.

11-14 баллов – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки.

10 баллов – ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

6-9 баллов – студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

1-5 баллов – студент имеет лишь частичное представление о теме. 0 баллов – нет ответа.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Ответ на занятии*	5/2	10	По расписанию
2.	*Выполнение лабораторной работы*	4/2	8	
3.	*Выполнение контрольной работы*	5/2	10	
4.	*Тест*	2/3	6	
5.	*Проект*	1/4	4	
6.	*Деловая игра*	1/2	2	
Всего			**40**	-
Блок бонусов				
7.	*Посещение занятий без пропусков*	1	3	
8.	*Своевременное выполнение всех заданий*	1	3	
9.	*Активность студента на занятии*	1	4	
Всего			**10**	-
Дополнительный блок				
10.	*Экзамен*		50	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Защита брендов: стратегии, системы, методы [Электронный ресурс] / Ворожевич А.С. - М. : Проспект, 2017. - URL: http://www.studentlibrary.ru/book/ISBN9785392235483.html (ЭБС «Консультант студента»).
2. Комплексные (интегрированные) системы обеспечения безопасности [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 7. - М. : Горячая линия - Телеком, 2013. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202381.html (ЭБС «Консультант студента»).
3. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М. : Горячая линия - Телеком, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html (ЭБС «Консультант студента»).
4. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202749.html (ЭБС «Консультант студента»).
5. Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202756.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература

1. Защита предпринимательства (экономическая и информационная безопасность) [Электронный ресурс]: учебное пособие / Одинцов А.А. - М. :

Международные отношения, 2003. - URL: http://www.studentlibrary.ru/book/ISBN5713311694.html

2. Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А.А. - М. : ДМК Пресс, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785940746478.html (ЭБС «Консультант студента»).

3. Концептуальные основы создания и применения системы защиты объектов [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 1. - М. : Горячая линия - Телеком, 2012. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202404.html (ЭБС «Консультант студента»).

4. Галатенко, В.А. Основы информационной безопасности : Курс лекций. Учебное пособие. Рек. для вузов ... по специальностям в области информационных технологий / В. А. Галатенко ; Под ред. В.Б. Бетелина. - Изд. 3-е. - М. : ИНТУИТ. РУ "Интернет-университет Информационных Технологий", 2004. - 264 с. (45 экз.)

5. Садердинов, А.А. Информационная безопасность предприятия: Учеб. пособ. - 2-е изд. - М.: Дашков и К, 2005. - 336 с. (45 экз.)

6. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах : рек. УМО вузов по университетскому политехническому образованию в качестве учеб.пособ. для студентов вузов ... "Информатика и вычислительная техника" / П. Б. Хорев. - 3-е изд. ; стереотип. - М. : Академия, 2005. - 256 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-4157-5. (69 экз.)

7. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745181.html

8. Девянин, П.Н. Модели безопасности компьютерных систем : Доп. УМО объединением вузов по образованию в области информационной безопасности в качестве учеб.пособ. для вузов... по специальности "Комплексное обеспечение информационной безопасности автоматизированных систем" / П. Н. Девянин. - М. : Академия, 2005. - 144 с. - (Высшее профессиональное образование). - ISBN 5-7695-2053-1 (50 экз.)

9. Основы организационного обеспечения информационной безопасности объектов информатизации : Доп. УМО по образованию в области ИБ качестве учеб. пособ. по специальностям в области ИБ / С.Н. Семкин [и др.].. : Гелиос АРВ, 2005. - 192 с. (55 экз.)

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории, библиотеки АГУ, центр мониторинга и аудита качества образования, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы

дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).