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
Р.Ю. Демина
«08» июня 2023 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой
информационной безопасности ИБ
Р.Ю. Демина
от «08» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Нормативные документы и стандарты по информационной безопасности

наименование

Составитель(-и)	**Гурская Т.Г., к.т.н., доцент кафедры ИБ**
Направление подготовки	**10.03.01 Информационная безопасность**
Направленность (профиль) ОПОП	**Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий)**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приема	**2023**
Курс	**4**
Семестр	**7**

Астрахань, 2023 г.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели освоения дисциплины: раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ.

1.2. Задачи освоения дисциплины (модуля): «Нормативные документы и стандарты по информационной безопасности» дать основы:

- информационного законодательства Российской Федерации;
- международного законодательства в области защиты информации;
- изучить международные стандарты в информационной сфере;
- изучить руководящие документы Гостехкомиссии, приказы ФСТЭК и ФСБ по вопросам ИБ.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина Б1.В.Д.03.02 «Нормативные документы и стандарты по информационной безопасности» в элективную часть, рассчитана на один семестр (7 семестр) и предусматривает сдачу студентами экзамена на основе балльно-рейтинговой системы оценивания.

Общая трудоемкость дисциплины – 3 кредита (ЗЕ).

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

1. Документоведение.
2. Организационное и правовое обеспечение информационной безопасности.
3. Основы информационной безопасности.

знания:

- структуры систем документационного обеспечения;
- основных групп организационно-распорядительной документации;

умения:

- пользоваться нормативными документами по защите информации;
- использовать программные и аппаратные средства персонального компьютера;

навыки:

- навыки поиска информации в глобальной информационной сети Интернет;
- навыки работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов и т.п.).

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

- Аттестация объектов информатизации.

Также дисциплина «Нормативные документы и стандарты по информационной безопасности» поможет студентам при написании 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):

профессиональных (ПК): ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать	Уметь	Владеть
ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях	ИПК 4.1. Знать: источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; принципы функционирования программных средств криптографической защиты информации; виды политик управления доступом и информационными потоками в компьютерных сетях; требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации	ИПК 4.2. Уметь: анализировать угрозы безопасности информации в компьютерных системах и сетях; настраивать правила обработки пакетов в компьютерных сетях; настраивать политики безопасности операционных систем, оценивать угрозы безопасности информации в компьютерных системах и сетях, противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем, настраивать антивирусные средства защиты информации в операционных системах,	ИПК 4.3. Владеть: навыками управления средствами межсетевого экранирования в компьютерных сетях методикой оценки оптимальности выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) 3 з.е., 108 часов, 52 часа выделено на контактную работу обучающихся с преподавателем (лекции – 18, лабораторные работы – 36), 54 часа – 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.	Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский	7	1-2	2		4		7	Контрольная работа №1 Отчет по лабораторной работе №1

№ 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	
	стандарт BSI. Виды угроз								
2.	Британский стандарт BS 7799. Аспекты информационной безопасности	7	3-4	2		4		7	Контрольная работа №1 Отчет по лабораторной работе №2
3.	Международный стандарт ISO 17799. Практические правила. Ключевые средства контроля	7	5-6	2		4		7	Контрольная работа №2 Отчет по лабораторной работе №2
4.	Международный стандарт ISO 15408 «Общие критерии». Типы уязвимостей	7	7-8	2		4		7	Контрольная работа №3 Отчет по лабораторной работе №3
5.	Стандарт COBIT. Аудит информационной безопасности. Этапы проведения аудита. Стадии жизненного цикла	7	9-10	2		4		7	Контрольная работа №3 Отчет по лабораторной работе №3
6.	Перечень сведений конфиденциального характера. ГОСТы по информационным технологиям. ГОСТ Р	7	11-12	2		4		7	Контрольная работа №4 Отчет по лабораторной работе №4
7.	ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1-3	7	13-14	2		4		7	Контрольная работа №4 Отчет по лабораторной работе №4
8.	ГОСТы по защите информации. Руководящие документы Гостехкомиссии, приказы ФСТЭК и ФСБ по вопросам ИБ	7	15-18	4		8		5	Контрольная работа №4 Отчет по лабораторной работе №4 Отчет

№ 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	
									реферата
	Итог за 7 семестр	108		18		36		54	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	
Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Виды угроз	13	+	**1**
Британский стандарт BS 7799. Аспекты информационной безопасности	13	+	**1**
Международный стандарт ISO 17799. Практические правила. Ключевые средства контроля	13	+	**1**
Международный стандарт ISO 15408 «Общие критерии». Типы уязвимостей	13	+	**1**
Стандарт COBIT. Аудит информационной безопасности. Этапы проведения аудита. Стадии жизненного цикла	13	+	**1**
Перечень сведений конфиденциального характера. ГОСТы по информационным технологиям.	13	+	**1**
ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1-3	13	+	**1**
ГОСТы по защите	17	+	**1**

информации. Руководящие документы Гостехкомиссии, приказы ФСТЭК и ФСБ по вопросам ИБ			

Содержание дисциплины

Тема 1. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Виды угроз.

«Оранжевая книга» поясняет понятие безопасной системы, которая «управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию».

Гармонизированные критерии европейских стран включают следующие основные составляющие информационной безопасности:

- конфиденциальность, то есть защиту от несанкционированного получения информации;
- целостность, то есть защиту от несанкционированного изменения информации;
- доступность, то есть защиту от несанкционированного удержания информации и ресурсов.

В основе германского стандарта BSI лежит общая методология и компоненты управления информационной безопасностью:

- Общий метод управления информационной безопасностью (организация менеджмента в области ИБ, методология использования руководства).
- Описания компонентов современных информационных технологий и др.

Тема 2. Британский стандарт BS 7799. Аспекты информационной безопасности.

В соответствии с этим стандартом любая служба безопасности, IT -отдел, руководство компании должны начинать работать согласно общему регламенту. Неважно, идет речь о защите бумажного документооборота или электронных данных. В настоящее время Британский стандарт BS 7799 поддерживается в 27 странах мира, в числе которых страны Британского Содружества, а также, например, Швеция и Нидерланды. В 2000 г. международный институт стандартов ISO на базе британского BS 7799 разработал и выпустил международный стандарт менеджмента безопасности ISO / IEC 17799. Поэтому сегодня можно утверждать, что BS 7799 и ISO 17799 это один и тот же стандарт, имеющий на сегодняшний день мировое признание и статус международного стандарта ISO.

Тема 3. Международный стандарт ISO 17799. Практические правила. Ключевые средства контроля.

Code of Practice for Information Security Management (Практические рекомендации по управлению безопасностью информации), принятом в 2000 году. ISO 17799 был разработан на основе британского стандарта BS 7799.

ISO 17799 может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Тема 4. Международный стандарт ISO 15408 «Общие критерии». Типы уязвимостей.

Международный стандарт ИСО/МЭК 15408-99 (исторически сложившееся название – «Общие критерии») представляет собой результат обобщения опыта различных государств по разработке и практическому использованию критериев оценки безопасности

информационных технологий (ИТ). Базовые документы, которые легли в основу «Общих критериев», и связи между ними.

Анализ развития нормативной базы оценки безопасности ИТ позволяет понять те мотивационные посылки, которые привели к созданию «Общих критериев».

Тема 5. Стандарт COBIT. Аудит информационной безопасности. Этапы проведения аудита. Стадии жизненного цикла.

Наиболее известной международной организацией занимающейся аудитом информационных систем является ISACA, по инициативе которой была разработана концепция по управлению информационными технологиями в соответствии с требованиями ИБ.

На основе этой концепции описываются элементы информационной технологии, даются рекомендации по организации управления и обеспечению режима информационной безопасности. Концепция изложена в документе под названием COBIT 3rd Edition (Control Objectives for Information and Related Technology - Контрольные объекты информационной технологии), который состоит из четырех частей:

- часть 1 – краткое описание концепции (Executive Summary);
- часть 2 – определения и основные понятия (Framework). Помимо требований и основных понятий, в этой части сформулированы требования к ним;
- часть 3 – спецификации управляющих процессов и возможный инструментарий (Control Objectives);
- часть 4 – рекомендации по выполнению аудита компьютерных информационных систем (Audit Guidelines).

Тема 6. Перечень сведений конфиденциального характера. ГОСТы по информационным технологиям. ГОСТ Р.

ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» и др.

ГОСТ Р 51725.6-2002 «Каталогизация продукции для федеральных государственных нужд. Сети телекоммуникационные и базы данных. Требования информационной безопасности»

Тема 7. ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1-3.

8 июня 1999 года был утвержден Международный стандарт ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий» (ОК).

Общие критерии обобщили содержание и опыт использования «Оранжевой книги», развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США. В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК – полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

Тема 8. ГОСТы по защите информации. Руководящие документы Гостехкомиссии, приказы ФСТЭК и ФСБ по вопросам ИБ.

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения» и др.

ПРИКАЗ 11 февраля 2013 г. № 17 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

Приказ ФСТЭК России № 21 от 18 февраля 2013 г. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

Приказ ФСТЭК России от «14» марта 2014 г. n 31 "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами ..." и др;

Приказ ФСБ РФ от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных..";

Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005) и др.

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. Лекции необходимо проводить с использованием презентаций, созданных в Microsoft PowerPont.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой, а также пользоваться ресурсами сети Интернет.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер раздела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
Тема 1.	Виды угроз	7	Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов
Тема 2.	Аспекты информационной безопасности	7	Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов
Тема 3.	Ключевые средства контроля	7	Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов
Тема 4.	Типы уязвимостей	7	Внеаудиторная, изучение учебных пособий, изучение

			нормативно-правовых документов
Тема 5.	Этапы проведения аудита.	7	Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов
Тема 6.	ГОСТ Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» и др. составление терминологического словаря	7	Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов
Тема 7.	Классификация набора требований безопасности ИТ	7	Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов
Тема 8.	ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», составление терминологического словаря	5	Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно - реферат.

Правила оформления текста пояснительной записки реферата

На титульном листе прописываются: название университета, факультета, кафедры, название дисциплины, темы реферата, Ф.И.О. студента, номер группы, Ф.И.О. преподавателя и оставляется место для проставления оценки и подписи преподавателя . Внизу пишется город и год написания.

Текстовая часть

Изложение текста и оформление работы следует выполнять в соответствии с требованиями.

Текст ПЗ оформляется на одной стороне листа формата А4.

Основной текст набирается шрифтом *Times New Roman 12,* с выравниванием *по ширине*, абзацный отступ должен быть одинаковым по всему тексту и равен *1,25 см*; строки разделяются *полуторным интервалом*.

Поля страницы: верхнее -2,5см, нижнее – 2,5 см, левое – 3,5 см, правое – 1,0 см.

Структурные элементы пояснительной записки **СОДЕРЖАНИЕ, ВВЕДЕНИЕ, ЗАКЛЮЧЕНИЕ, СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ, ПРИЛОЖЕНИЕ** должны начинаться с нового листа.

Их заголовки оформляются ***прописными буквами, шрифтом 14 Ж***, располагаются *в середине строки без точки в конце*. Дополнительный *интервал после* заголовка - 12 *пт*.

Основную часть работы разделяют на разделы, подразделы и, при необходимости, на пункты.

Каждый раздел необходимо начинать с нового листа. Разделы нумеруют арабскими цифрами в пределах всего текста. После номера и в конце заголовка раздела *точка не ставится*.

Если заголовок состоит из двух предложений, их разделяют точкой. *Переносы слов в заголовках не допускаются.*

Заголовки разделов оформляются ***с прописной буквы, шрифтом 14 Ж,*** с абзацного отступа *1,25* см. Дополнительный *интервал после заголовка - 6 пт.*

(Если заголовок раздела занимает две и большее число строк, то интервал между этими строками – *полуторным*).

Подразделы нумеруются в пределах каждого раздела. Номер подраздела состоит из номера раздела и порядкового номера подраздела, разделенных точкой. После номера подраздела точку не ставят.

Заголовки подразделов печатаются с абзацного отступа, ***с прописной буквы шрифтом 12 Ж,*** без точки в конце заголовка.

Дополнительный *интервал перед* заголовком подраздела – *6 пт*, *после* заголовка - 6 *пт*.

Пункты нумеруются в пределах каждого подраздела. Номер пункта состоит из номеров раздела, подраздела и пункта, разделенных точкой. После номера пункта точку не ставят.

Нельзя писать заголовок в конце страницы, если на ней не умещаются, по крайней мере, две строки текста, идущего за заголовком.

Пример оформления заголовков текста:

1 Разработка аппаратных средств

1.1
1.2 } **Нумерация пунктов первого раздела отчета**
1.3

2 Технические характеристики

2.1
2.2 } **Нумерация пунктов второго раздела отчета**
2.3

В пояснительной записке после титульного листа помещается лист **СОДЕРЖАНИЕ**, в котором указываются номера и наименования разделов, подразделов и приложений ТД с указанием номеров страниц, где они начинаются.

Разделы, подразделы записываются в содержании в точном соответствии с их наименованиями без сокращений *строчными буквами кроме первой прописной.*

Перечисления

В тексте пояснительной записки перечисления производятся с абзацного отступа, каждое с новой строки с *дефисом***.**

Примеры написания:

- текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
- приложения;
- перечень терминов;
- перечень сокращений;
- перечень литературы.

При необходимости ссылки в тексте отчета на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

При необходимости дальнейшей детализации перечислений используются арабские цифры и строчные буквы русского алфавита, после которых ставятся скобки:

а)…;

б)…;

1)…;

2)…;

в).

Примеры написания:

1) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
2) приложения;
3) перечень терминов;
4) перечень сокращений;
5) перечень литературы.

Примеры написания:

а) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
б) приложения;
в) перечень терминов;
г) перечень сокращений;
д) перечень литературы.

Сокращения слов

Сокращение слов в тексте, как правило, не допускается. Исключение составляют сокращения, общепринятые в русском языке: т. е. (то есть), и т. п. (и тому подобное), и т. д. (и так далее), и др. (и другие).

При необходимости применения специфических терминов или сокращений нужно дать их разъяснение при первом упоминании. Например «…создание систем автоматического проектирования (САПР)». В последующем тексте принятые сокращения пишутся без скобок.

Формулы

Составной частью текста пояснительной записки являются математические формулы и соотношения. Формулы создаются в редакторе формул.

Формулы располагают в середине строки и выделяют из текста свободными строками.

Пример оформления расчетов:

Количество населения в заданном пункте и подчиненных окрестностях с учетом среднего прироста населения определяется по формуле (3.1):

$$H_t = H_0\left(1 + \frac{\Delta H}{100}\right)^t, \qquad (3.1)$$

где H_0 – число жителей на время проведения переписи населения, тыс. чел.;

ΔH – средний годовой прирост населения в данной местности, % (принимается 2…3%);

t – период, определяемый как разность между назначенным годом перспективного проектирования и годом проведения переписи населения, год.

$$H_t = 32{,}6\left(1 + \frac{2}{100}\right)^8 = 38{,}2 \text{ тыс.чел.}$$

Расшифровка формулы, при необходимости, приводится непосредственно под формулой. В конце формулы ставится запятая, пояснение значений символов дают с новой строки в той последовательности, в какой они приведены в формуле.

Формулы нумеруются в пределах раздела. Номер формулы состоит из номера раздела и порядкового номера формулы в этом разделе. Номер формулы в круглых скобках помещается в крайнем правом положении на строке.

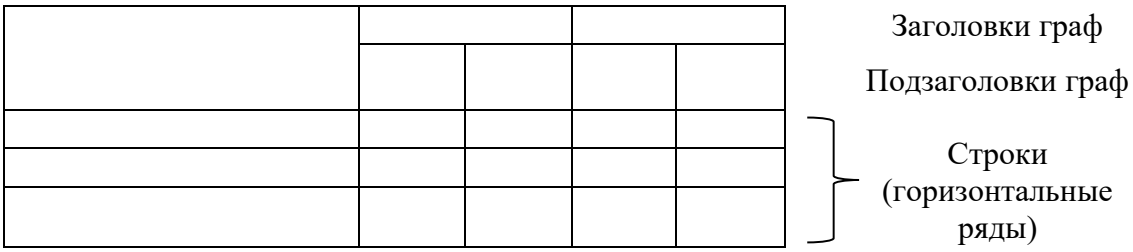
Ссылка в тексте на формулу: «…в формуле (3.1)».

Таблицы

Цифровой материал оформляется в виде таблиц. Таблицу следует располагать непосредственно после ссылки на нее.

Размеры таблиц выбираются произвольно, в зависимости от представляемого материала. Высота строк таблицы должна быть не менее 8 мм

Таблица 2.1 – Наименование таблицы



Заголовки граф и строк таблицы должны начинаться с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком. Если подзаголовки граф имеют самостоятельное значение, то их начинают с прописной буквы.

Заголовки указывают в единственном числе. В конце заголовков и подзаголовков таблицы точки не ставят.

Разделять заголовки боковика и граф диагональными линиями не допускается. Графу

«Номер по порядку» в таблицу включать не допускается.

Таблицы нумеруются в пределах раздела. Номер таблицы состоит из номера раздела и порядкового номера таблицы в этом разделе. Номер и наименование таблицы следует помещать над таблицей слева через тире.

Пример оформления таблицы:

Таблица 3.1– Длина участков трассы

Протяженность участка проектируемой трассы, км	Тип кабеля
0,084	ДПС-04-24А06-7,0
0,167	ДПС-04-24А06-7,0
0,301	ДПС-04-24А06-7,0

0,779	ДПС-04-24А06-7,0
Общая длина кабеля: 1,331 км	ДПС-04-24А06-7,0

Примечание – Толщину линий таблицы задайте 1 пт.

Таблицу с большим числом строк допускается переносить на другой лист. При этом в первой части таблицы нижнюю горизонтальную линию не проводят. Над второй частью слева пишут: «Продолжение Таблицы 2.1».

Продолжение Таблицы 2.1

Дата	Наименование	Стоимость

Рисунки

Графический материал располагают, возможно, ближе к тексту, в котором о нём упоминается.

Все рисунки нумеруются в пределах раздела и должны иметь наименование, Номер рисунка и его наименование располагают под рисунком следующим образом:

Рисунок 2.12 – Кривая коэффициента восприятия речи

Ссылка в тексте на рисунок: «…в соответствии с рисунком 4.3».

Если в разделе ВВЕДЕНИЕ есть рисунки, то они нумеруются как :

Рисунок В.1 – Название рисунка

Список использованных источников

Список использованных источников приводится в конце пояснительной записки. Список использованных учебников, справочников, статей, стандартов и др. следует располагать в порядке появления ссылок на источники в тексте работы и нумеровать арабскими цифрами без точки, печатать с абзацного отступа.

Список литературы должен быть составлен в алфавитном порядке. Список адресов серверов Internet указывается после литературных источников. При указании веб-адреса рекомендуется давать заголовок данного ресурса (заголовок веб-страницы).

При составлении списка литературы в алфавитном порядке следует придерживаться следующих правил:

1) законодательные акты и постановления правительства РФ;

2) специальная научная литература;

3) методические, справочные и нормативные материалы, статьи периодической печати.

Для многотиражной литературы при составлении списка указываются: полное название источника, фамилия и инициалы автора, издательство и год выпуска (для статьи – название издания и его номер). Полное название литературного источника приводится в начале книги на 2-3 странице.

Для законодательных актов необходимо указывать их полное название, принявший орган и дату принятия.

При указании адресов серверов Internet сначала указывается название организации, которой принадлежит сервер, а затем его полный адрес.

Примеры записей:

1 Глухов В. А. Исследование, разработка и построение системы электронной доставки документов в библиотеке: Автореф. дис. канд. техн. наук. – Новосибирск, 2000. – 18 с.

2 Экономика и политика России и государств ближнего зарубежья : аналит. обзор, апр. 2007, Рос. акад. наук, Ин-т мировой экономики и муждунар. отношений. – М. : ИМЭМО, 2007. – 39 с.

3 Фенухин В. И. Этнополитические конфликты в современной России: на примере Северо-Кавказкого региона : дис. … канд. полит. наук. – М., 2002. – с. 54–55.

4 Официальные периодические издания : электронный путеводитель / Рос. нац. б-ка, Центр правовой информации. [СПб], 200520076. URL: http://www.nlr.ru/lawcrnter/izd/index.html (дата обращения: 18.01.2007).

5 Логинова Л. Г. Сущность результата дополнительного образования детей // Образование: исследовано в мире: междунар. науч. пед. интернет-журн. 21.10.03. URL: http://www.oim.ru/reader.asp?nomer=366 (дата обращения: 17.04.07).

6 Рынок тренингов Новосибирска: своя игра [Электронный ресурс]. – Режим доступа: http://nsk.adme.ru/news/2006/07/03/2121.html (дата обращения: 17.10.08).

Оформление приложений

Нумерация приложений осуществляется русскими буквами, кроме букв Ё, Й, Ъ, Ь, Ы, О.

В разделе СОДЕРЖАНИЕ название приложения оформляется следующим образом:

ПРИЛОЖЕНИЕ А – Диаграмма классов

В самом приложении, слово **ПРИЛОЖЕНИЕ А** пишется жирным шрифтом по центру, на следующей строке пишется название приложения, по центру жирным шрифтом, например,

ПРИЛОЖЕНИЕ А
Диаграмма классов

Если приложение продолжается на следующей странице, то необходимо сверху по центру, нежирным шрифтом написать слова:

Продолжение Приложения А

Если в приложении, например, в приложении А есть таблицы, то они нумеруются как:

Таблица А.1– Название таблицы

Если в приложении есть рисунки, например, в приложении А, то они нумеруются как:

Рисунок А.1 – Название рисунка

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-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line и/или off-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
Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Виды угроз	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Британский стандарт BS 7799. Аспекты информационной безопасности	Лекция-диалог	Не предусмотрено	выполнение контрольной работы, выполнение лабораторной работы
Международный стандарт ISO 17799. Практические правила. Ключевые средства контроля	Лекция	Не предусмотрено	выполнение контрольной работы выполнение лабораторной работы
Международный стандарт ISO 15408 «Общие критерии». Типы уязвимостей	Лекция	Не предусмотрено	выполнение лабораторной работы
Стандарт COBIT. Аудит информационной безопасности. Этапы проведения аудита. Стадии	Обзорная лекция	Не предусмотрено	выполнение контрольной

жизненного цикла			работы выполнение лабораторной работы
Перечень сведений конфиденциального характера. ГОСТы по информационным технологиям. ГОСТ Р	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1-3	Лекция	Не предусмотрено	выполнение лабораторной работы
ГОСТы по защите информации. Руководящие документы Гостехкомиссии, приказы ФСТЭК и ФСБ по вопросам ИБ	Лекция-диалог	Не предусмотрено	выполнение контрольной работы выполнение лабораторной работы

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.

Название информационной технологии	Темы, разделы дисциплины	Краткое описание применяемой технологии
Использование возможностей Интернета в учебном процессе	1 –8	Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах дистанционного обучения)
Использование возможностей электронной почты преподавателя	1 – 8	Подготовка к защите отчетов по лабораторным работам
Использование средств представления учебной информации	1 – 8	Использование мультимедийной презентации

6.3. Перечень программного обеспечения и информационных справочных систем

6.3.1. Программное обеспечение:

В соответствии с ОПОП дисциплина должна быть поддержана соответствующими лицензионными программными продуктами.

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
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

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. Справочная правовая система КонсультантПлюс: http://www.consultant.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) «Нормативные документы и стандарты по информационной безопасности» 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 дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1	Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Виды угроз	ПК 4	Контрольная работа №1 Отчет по лабораторной работе №1
2	Британский стандарт BS 7799. Аспекты информационной безопасности	ПК 4	Контрольная работа №1 Отчет по лабораторной работе №2
3	Международный стандарт ISO 17799. Практические правила. Ключевые средства контроля	ПК 4	Контрольная работа №2 Отчет по лабораторной работе №2
4	Международный стандарт ISO 15408 «Общие критерии». Типы уязвимостей	ПК 4	Контрольная работа №3 Отчет по лабораторной работе №3
5	Стандарт COBIT. Аудит информационной безопасности. Этапы проведения аудита. Стадии жизненного цикла	ПК 4	Контрольная работа №3 Отчет по лабораторной работе №3
6	Перечень сведений конфиденциального характера. ГОСТы по информационным технологиям. ГОСТ Р	ПК 4	Контрольная работа №4 Отчет по лабораторной работе №4
7	ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1-3	ПК 4	Контрольная работа №4 Отчет по лабораторной работе №4
8	ГОСТы по защите информации. Руководящие документы Гостехкомиссии, приказы ФСТЭК и ФСБ по вопросам ИБ	ПК 4	Контрольная работа №4 Отчет по лабораторной работе №4 Отчет реферата

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 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	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 «удовлетворительно»	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 «неудовлетворительно»	не способен правильно выполнить задание

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

Тема 1. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Виды угроз

Лабораторная работа №1. Стандарты и спецификации в области информационной безопасности.

Цели:

Изучить международные и национальные стандарты и специфи-кации в области ИБ — «Оранжевая книга», Гармонизированные критерии европейских стран, Германский стандарт BSI. Получить навыки определения сильных и слабых стороны этих документов.

Задание:

1.Ознакомиться со стандартами и спецификациями в области информационной безопасности:

- «Оранжевая книга»,
- Гармонизированные критерии европейских стран,
- Германский стандарт BSI

2. Проанализировать данные стандарты, выявить их сильные и слабые стороны.

3. Составить документ, содержащий исходную информацию о предприятии (выбирается студентом самостоятельно и согласуется с преподавателем). В документе должны быть отражены организационная структура предприятия, уровень его зрелости, задачи и функции предприятия, информационные потоки, реализованные на предприятии меры защиты информации

4. Провести анализ предприятия в соответствии с представленными стандартами.

Тема 2. Британский стандарт BS 7799. Аспекты информационной безопасности

Вопросы к контрольной работе 1

1. Какие критерии определяют степень доверия в стандарте «Оранжевая книга»?
2. Что такое монитор обращений? Основные качества монитора обращений?
3. Определите назначения и виды классов безопасности в «Оранжевой книге».
4. Какие элементы должна включать в себя политика безопасности согласно «Оранжевой книге»?
5. Как определяются составляющие ИБ в гармозированных критериях Европейских стран.
6. Какие три уровня детализации рассматриваются в европейских критериях относительно средств информационной безопасности?
7. Приведите составляющие германского стандарта BSI.
8. Какие классы угроз рассматриваются в германском стандарте BSI?
9. Почему Британский стандарт BS 7799 используется наиболее часто?
10. Какие аспекты ИБ рассматриваются в части «Практические рекомендации» стандарта BS 7799.

Тема 3. Международный стандарт ISO 17799. Практические правила. Ключевые средства контроля

Вопросы к контрольной работе 2

1. Назовите 10 разделов для управления ИБ по стандарту ISO 17799.
2. Приведите ключевые средства контроля ИБ предприятия.
3. Дайте определения понятия «Политика безопасности» и опишите особенности его разработки.
4. Какие организационные меры используются при управлении ИБ?
5. Приведите классификацию ресурсов и опишите уровни их защиты.
6. Перечислите правила безопасности при выборе и работе с персоналом.
7. Какие вопросы должны рассматриваться при обучении персонала?
8. Какие требования предъявляются при защите оборудования?
9. Что включает понятие «администрирование компьютерных систем и вычислительных сетей»?
10. Как регламентируется защита вредоносного программного обеспечения?
11. В каком разделе стандарта ISO 17799 рассматриваются вопросы шифрования данных?
12. Какие вопросы рассматриваются в разделе «Планирование бесперебойной работы организации»?
13. Что контролируется при выполнении правовых требований?

14. Какие условия должны выполняться при аудите ИБ

Лабораторная работа №2. Политика информационной безопасности.

Цели:

Изучить международные и национальные стандарты и специфи-кации в области ИБ — Британский стандарт BS 7799, Международный стандарт ISO 17799. Получить навыки определения сильных и слабых стороны этих документов.

Задание:

1.Ознакомиться со стандартами и спецификациями в области информационной безопасности:

- Британский стандарт BS 7799,
- Международный стандарт ISO 17799

2. Проанализировать данные стандарты, выявить их сильные и слабые стороны.

3. Провести анализ предприятия в соответствии с международным стандартом ISO 17799. Составить модель политики безопасности, которая будет включать в себя следующие пункты: термины и определения, цели и задачи, разделение полномочий и порядок внесения изменений в политику безопасности, определенные специально для вашего предприятия.

Тема 4. Международный стандарт ISO 15408 «Общие критерии». Типы уязвимостей

Тема 5. Стандарт COBIT. Аудит информационной безопасности. Этапы проведения аудита. Стадии жизненного цикла

Вопросы к контрольной работе 3

1. В чем отличие применения международных стандартов ISO 15408 и ISO 17799?
2. Опишите статус стандарта ISO 15408 в РФ
3. Что включает в себя понятие «доверие» в рамках стандарта ISO15408?
4. Изложите общую схему оценки безопасности ИТ на основе общих критериев.
5. Какие классы и семейства используются для оценки безопасности ПС?
6. Дайте определение понятиям «профиль защиты» и «Задание по безопасности».
7. Что определяет оценочный уровень доверия (ОУД)?
8. Какой оценочный уровень доверия является типовым (наиболее используемым) и почему?
9. Назовите основные этапы проведения аудита ИБ при использовании стандарта COBIT
10. Перечислите основные черты, отличающие стандарт COBIT.
11. Приведите общую последовательность проведения аудита в соответствии со стандартом COBIT.

Лабораторная работа №3. Аудит информационной безопасности.

Цели:

Изучить международные и национальные стандарты и специфи-кации в области ИБ — Международный стандарт ISO 15408 «Общие критерии», Стандарт COBIT. Получить навыки определения сильных и слабых стороны этих документов.

Задание:

1.Ознакомиться со стандартами и спецификациями в области информационной безопасности:

- Международный стандарт ISO 15408,
- Стандарт COBIT

2. Проанализировать данные стандарты, выявить их сильные и слабые стороны.

3. Провести аудит предприятие в соответствии со стандартом COBIT: провести сбор информации о предприятии, провести анализ исходных данных, выработать рекомендации

(организационные, технические и методологические).

Тема 6. Перечень сведений конфиденциального характера. ГОСТы по информационным технологиям. ГОСТ Р

Тема 7. ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1-3

Тема 8. ГОСТы по защите информации. Руководящие документы Гостехкомиссии, приказы ФСТЭК и ФСБ по вопросам ИБ

Вопросы к контрольной работе 4

1. Какие стандарты, разработанные в России, используются при оценке защищенности информационных технологий?
2. Как связаны международные стандарты и стандарты РФ?
3. Какие основные стандарты РФ в области информационной безопасности существуют?
4. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
5. Что такое политика безопасности?
6. Классификация систем защиты АС согласно документам Федеральной службы по техническому и экспертному контролю России.
7. Место информационной безопасности в системе национальной безопасности России.
8. Важнейшие федеральные нормативные правовые акты, касающиеся информационной безопасности.
9. Законы, непосредственно касающиеся защиты компьютерной информации.

Лабораторная работа №4. Отечественное законодательство в области ИБ.

Цели:

Изучить отечественные стандарты и специфи-кации в области ИБ. Получить навыки определения сильных и слабых стороны этих документов.

Задание:

1.Ознакомиться со стандартами и спецификациями в области информационной безопасности:

- ГОСТы по информационным технологиям. ГОСТ Р,
- ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий…
- ГОСТы по защите информации. Руководящие документы Гостехкомиссии, приказы ФСТЭК и ФСБ по вопросам ИБ.

2. Проанализировать предприятие, определить виды и объемы обрабатываемой конфиденциальной информации. Определить нормативные документы, регламентирующие защиту данной информации. Разработать комплект документов для защиты конфиденциальной информации, обрабатываемой на предприятии.

Тематика рефератов

1. Практические подходы при проведении аудита ИБ.
2. Программные продукты для проведения аудита ИБ на предприятии.
3. Оценка безопасности информационных технологий на основе международных стандартов ИБ.
4. Организация информационной безопасности в коммерческом секторе.
5. Организация системы безопасности корпоративных информационных систем.
6. Инженерно-техническая безопасность предприятия. Международноправовые аспекты информационной безопасности.

7. Информационная собственность и ее защита.
8. Информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения и механизмов информационной безопасности.
9. Аудит информационной безопасности.
10. Роль информационной безопасности в сфере электронной торговли
11. Комплексный подход к созданию системы защиты информации на предприятии
12. Обеспечение безопасного доступа к информационным ресурсам организации.
13. Экономика информационной безопасности предприятия.
14. Комплексная информационная безопасность объекта.
15. Информационная безопасность организации и персонал.
16. Правовой статус и функции службы безопасности по обеспечению информационной безопасности бизнеса.
17. Методы оценки рисков информационной безопасности.
18. Принципы защиты информации и метрики ИБ.
19. Государственная система защиты информации.
20. Подготовка кадров в области ИБ
21. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.
22. Правовые основы сертификации и аттестации средств защиты информации. Основные понятия и принципы сертификации.
23. Требования к объектам информатизации и необходимость проведения их аттестации.
24. Политика безопасности предприятия и ее содержание.
25. Создание и функции службы безопасности на предприятии.

Критерии оценки реферата:

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

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

– оценка «удовлетворительно» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки;

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

Перечень вопросов к экзамену

1. Какие критерии определяют степень доверия в стандарте «Оранжевая книга»?
2. Определите назначения и виды классов безопасности в «Оранжевой книге».
3. Какие элементы должна включать в себя политика безопасности согласно «Оранжевой книге»?
4. Как определяются составляющие ИБ в гармозированных критериях Европейских

стран.

5. Какие три уровня детализации рассматриваются в европейских критериях относительно средств информационной безопасности?

6. Приведите составляющие германского стандарта BSI.

7. Какие классы угроз рассматриваются в германском стандарте BSI?

8. Какие аспекты ИБ рассматриваются в части «Практические рекомендации» стандарта BS 7799.

9. Назовите 10 разделов для управления ИБ по стандарту ISO 17799.

10. Приведите ключевые средства контроля ИБ предприятия.

11. Дайте определения понятия «Политика безопасности» и опишите особенности его разработки.

12. Какие организационные меры используются при управлении ИБ?

13. Что контролируется при выполнении правовых требований?

14. В чем отличие применения международных стандартов ISO 15408 и ISO 17799?

15. Опишите статус стандарта ISO 15408 в РФ

16. Что включает в себя понятие «доверие» в рамках стандарта ISO15408?

17. Изложите общую схему оценки безопасности ИТ на основе общих критериев.

18. Какие классы и семейства используются для оценки безопасности ПС?

19. Дайте определение понятиям «профиль защиты» и «Задание по безопасности».

20. Назовите основные этапы проведения аудита ИБ при использовании стандарта COBIT

21. Перечислите основные черты, отличающие стандарт COBIT.

22. Приведите общую последовательность проведения аудита в соответствии со стандартом COBIT.

23. Какие стандарты, разработанные в России, используются при оценке защищенности информационных технологий?

24. Как связаны международные стандарты и стандарты РФ?

25. Какие основные стандарты РФ в области информационной безопасности существуют?

26. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.

27. Классификация систем защиты АС согласно документам Федеральной службы по техническому и экспертному контролю России.

28. Важнейшие федеральные нормативные правовые акты, касающиеся информационной безопасности.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях				
1.	Задание закрытого типа	Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью	1	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		1. событие информационной безопасности 2. непредвиденная ситуация 3. чрезвычайная ситуация		
2.		Рисковое событие, связанное с неблагоприятными внешними событиями природного и техногенного характера, а также с действиями субъектов (групп субъектов), приводящими к невозможности функционирования организации или ее служб/подразделений в обычном, регламентируемом соответствующими стандартами режиме 1. событие информационной безопасности 2. непредвиденная ситуация 3. чрезвычайная ситуация	2	5
3.		Компонент информационно-телекоммуникационной системы, нарушение непрерывности функционирования которого может нанести значительный ущерб организации 1. критичный компонент (информационно-телекоммуникационной системы) 2. событие информационной безопасности (информационно-телекоммуникационной системы) 3. кризисный компонент (информационно-телекоммуникационной системы) 4. ущербный компонент (информационно-телекоммуникационной системы)	1	5
4.		Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию 1) Политика безопасности 2) Концепция безопасности 3) Устав 4) Регламент безопасности	1	5
5.		Политика информационной безопасности в общем случае является ...? 1. руководящим документом для администраторов безопасности и системных администраторов 2. руководящим документом для ограниченного использования 3. руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов 4. руководящим документом для всех сотрудников компании	4	5
6.	Задание	Категории обрабатываемых в информационной системе персональных	В информационной системе определяются следующие категории	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
	открытого типа	данных	обрабатываемых персональных данных: • категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни; • категория 2 – персональные данные, позволяющие идентифицировать субъекта этих данных и получить о нем дополнительную информацию, за исключение данных, относящихся к категории 1; • категория 3 – персональные данные, позволяющие идентифицировать субъекта этих данных; • категория 4 – обезличенные и (или) общедоступные персональные данные.	
7.		К режимным мерам комплексной безопасности предпринимательской деятельности относятся:	К режимным мерам комплексной безопасности предпринимательской деятельности относятся: порядок приема посетителей; порядок пропуска персонала и клиентов на охраняемые объекты; порядок пропуска транспортных средств и материальных ценностей на охраняемые объекты; порядок передачи информации с охраняемых объектов; порядок открытия-закрытия рабочих кабинетов, складов, хранилищ; порядок пропуска (допуска) служб экстренного вызова на охраняемые объекты.	8
8.		Организационная основа системы обеспечения информационной безопасности	Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.	
9.		От кого обладатель коммерческой тайны вправе требовать возмещения убытков в соответствии со статьей 139 ГК РФ	В статье 139 ГК РФ предусмотрено, что обладатель коммерческой тайны вправе требовать возмещения убытков: от лиц, незаконными методами получивших информацию, составляющую коммерческую тайну, например, путем похищения документов; от работника, разгласившего коммерческую тайну вопреки трудовому договору.	8
10.		От чего зависят информационные риски компании?	Информационные риски компании зависят: от показателей ценности информационных ресурсов; вероятности реализации угроз для ресурсов; эффективности существующих или планируемых средств обеспечения ИБ	8

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 основам делопроизводства.

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 теоретических 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.

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.
20-22 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.	*Выполнение лабораторной работы*	4/4	16	По расписанию
2.	*Выполнение контрольной работы*	4/4	16	
3.	*Реферат*	1/8	8	
Всего			**40**	-
Блок бонусов				
4.	*Посещение занятий без пропусков*	1	3	
5.	*Своевременное выполнение всех заданий*	1	3	
6.	*Активность студента на занятии*	1	4	
Всего			**10**	-
Дополнительный блок				
7.	*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. Галатенко В.А., Стандарты информационной безопасности / Галатенко В.А. - М.: Национальный Открытый Университет "ИНТУИТ", 2016. (Основы информационных технологий) - ISBN 5-9556-0053-1 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN5955600531.html.

2. Дронов В.Ю., Международные и отечественные стандарты по информационной безопасности : учеб.-метод. пособие / Дронов В.Ю. - Новосибирск : Изд-во НГТУ, 2016. - 34 с. - ISBN 978-5-7782-3112-2 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785778231122.html

8.2. Дополнительная литература

3. Анисимов А.А., Менеджмент в сфере информационной безопасности / Анисимов А.А. - М.: Национальный Открытый Университет "ИНТУИТ", 2016. (Основы информационных технологий) - ISBN 978-5-9963-0237-6 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785996302376.html

4. Бекетнова Ю.М., Международные основы и стандарты информационной безопасности финансово-экономических систем : Учебное пособие / Бекетнова Ю.М., Крылов Г.О., Ларионова С.Л. - М. : Прометей, 2018. - 174 с. - ISBN 978-5-907003-27-9 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785907003279.html

5. Костин В.Н., Методы и средства защиты компьютетной информации: законодательные и нормативные акты по защите информации : учеб. пособие / В.Н. Костин -

М. : МИСиС, 2017. - 26 с. - ISBN 978-5-906846-87-7 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785906846877.html

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, 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).