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)

Теория информационной безопасности и методология защиты информации

наименование

Составитель(-и)	**Гурская Т.Г., к.т.н, доцент кафедры ИБ** **Демина Р.Ю., к.т.н., доцент кафедры ИБ** **Выборнова О.Н., к.т.н, доцент кафедры ИБ**
Направление подготовки / специальность	**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направленность (профиль) ОПОП	**Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий)**
Квалификация (степень)	**бакалавр**
Форма обучения	**Очно-заочная**
Год приема	**2023**
Курс	**4**
Семестр	**7**

Астрахань – 2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины «Теория информационной безопасности и методология защиты информации» является раскрытие значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.

1**.2. Задачи освоения дисциплины (модуля):**

- определить цели и принципы защиты информации;
- раскрыть методы определения состава защищаемой информации, классификация ее по видам тайны, материальным носителям, собственникам и владельцам; установить структуры угроз защищаемой информации;
- раскрыть направления, виды методов и особенностей деятельности разведывательных органов по добыванию конфиденциальной информации;
- раскрыть назначения, сущности и структуры систем защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина Б1.В.Д.06.01 «Теория информационной безопасности и методология защиты информации» относится к вариативной части (элективные дисциплины) учебного плана направления подготовки 10.03.01 Информационная безопасность 2023 года набора.

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

- Основы информационной безопасности.
- Документоведение.
- Организационное и правовое обеспечение информационной безопасности

Знания: правовых основ организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны; правовых норм и стандартов по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; принципов и методов организационной защиты информации; технических каналов утечки информации, возможностей технических разведок, способов и средств защиты информации от утечки по техническим каналам, методов и средств контроля эффективности технической защиты информации; места и роли информационной безопасности в системе национальной безопасности Российской Федерации.

Умения: 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.

Навыки: работы с нормативными правовыми актами; применения методов технической защиты информации; методов расчета и инструментального контроля показателей технической защиты информации; методов 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 «Теория информационной безопасности и методология защиты информации», используются студентами при прохождении преддипломной практики и 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) в зачетных единицах **3 зачетные единицы** (1 ЗЕ выделена на подготовку к экзамену). Всего 108 часов: 54 часов выделено на контактную работу обучающихся с преподавателем (лекции – 18, лабораторные работы – 36), 54 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)*
				Л	ПЗ	ЛР	КР	СР	

									Форма промежуточной аттестации *(по семестрам)*
1	Введение в курс. Информационная безопасность. Проблемы развития теории и практики обеспечения информационной безопасности.	7	1-4	4		8		5	Входное тестирование, опрос на экзамене
2	Значение информационной безопасности для субъектов информационных отношений. Составляющие национальных интересов РФ в информационной сфере.		5-6	2		4		7	отчет по лабораторной работе, опрос на экзамене
3	Общее содержание защиты информации. Концепция информационной безопасности		7-8	2		4		7	контрольная работа 1, опрос на экзамене
4	Предмет и объект защиты информации. Информация как объект права собственности.		9-10	2		4		7	отчет по лабораторной работе, опрос на экзамене
5	Теоретические и концептуальные основы защиты информации. Современные факторы, влияющие на защиту информации.		11-12	2		4		7	отчет по лабораторной работе, опрос на экзамене
6	Угрозы защищаемой информации. Уязвимость информации. Модель гипотетического нарушителя информационной безопасности		13-14	2		4		7	отчет по лабораторной работе, опрос на экзамене
7	Системное обеспечение защиты информации. Основные принципы построения системы защиты.		15-16	2		4		7	контрольная работа 2, опрос на экзамене
8	Методы защиты информации. Модели защиты информации. Конфиденциальность при работе с зарубежными партнерами. Аудит информационной безопасности		17-18	2		4		7	отчет по лабораторной работе, опрос на экзамене
	ИТОГО			**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	
Введение в курс. Информационная безопасность. Проблемы развития теории и практики обеспечения информационной безопасности.	17	+	1
Значение информационной безопасности для субъектов информационных отношений. Составляющие национальных интересов РФ в информационной сфере.	13	+	1
Общее содержание защиты информации. Концепция информационной безопасности	13	+	1
Предмет и объект защиты информации. Информация как объект права собственности.	13	+	1
Теоретические и концептуальные основы защиты информации. Современные факторы, влияющие на защиту информации.	13	+	1
Угрозы защищаемой информации. Уязвимость информации. Модель гипотетического нарушителя информационной безопасности	13	+	1
Системное обеспечение защиты информации. Основные принципы построения системы защиты.	13	+	1
Методы защиты информации. Модели защиты информации. Конфиденциальность при работе с зарубежными партнерами. Аудит информационной безопасности	13	+	1

Краткое содержание дисциплины

Тема 1

Введение в курс. Информационная безопасность. Проблемы развития теории и практики обеспечения информационной безопасности. Основные понятия и определения в области информационной безопасности. Основные составляющие информационной безопасности.

Тема 2

Значение информационной безопасности для субъектов информационных отношений. Составляющие национальных интересов РФ в информационной сфере. Международное сотрудничество в области информационной безопасности: проблемы и перспективы

Тема 3
Общее содержание защиты информации. Понятие и сущность защиты информации. Цели защиты информации. Концепция информационной безопасности

Тема 4
Предмет и объект защиты информации. Информация как объект права собственности. Классификация конфиденциальной информации по видам тайн и степеням конфиденциальности.

Тема 5
Теоретические и концептуальные основы защиты информации. Современные факторы, влияющие на защиту информации. Направления обеспечения информационной безопасности. Способы защиты информации.

Тема 6
Угрозы защищаемой информации. Уязвимость информации. Модель гипотетического нарушителя информационной безопасности

Тема 7
Системное обеспечение защиты информации. Основные принципы построения системы защиты. Пресечение разглашения конфиденциальной информации. Защита от утечки по техническим каналам. Противодействие несанкционированному доступу к источникам конфиденциальной информации

Тема 8
Методы защиты информации. Модели защиты информации. Конфиденциальность при работе с зарубежными партнерами. Аудит информационной безопасности.

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 и лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8. Лекции необходимо проводить с использованием презентаций, созданных в Microsoft PowerPont.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

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

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер радела (темы)	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
1	1. Дайте определение понятию защита информации. 2. Дайте определение понятию информационная безопасность 3. Какое место занимает защита информации в информационной безопасности?	5	Внеаудиторная, изучение учебных пособий
2	1. Преимущества и недостатки методов экспертной оценки. 2. Строгое и нестрогое ранжирование. Процедура оценки. Отличия.	7	Внеаудиторная, изучение учебных пособий
3	1. Что представляет собой политика безопасности организации?	7	Внеаудиторная, изучение учебных пособий

	2. Перечислите основные методы обеспечения информационной безопасности РФ 3. Перечислите основные документы в области международной информационной безопасности.		
4	1. Опишите классификацию информации, обрабатываемой (хранимой) в организации. 2. Опишите вид информационных ресурсов, средства их хранения и обеспечения к ним доступа	7	Внеаудиторная, изучение учебных пособий
5	1. Дайте определение понятию угроза. 2. Понятия дискреционной и мандатной моделей управления доступом.	7	Внеаудиторная, изучение учебных пособий
6	1. Составляющие модели нарушителя. 2. На основании чего строится модель нарушителя? 3. Типы нарушителей.	7	Внеаудиторная, изучение учебных пособий
7	1. Сформулируйте основные принципы построения системы защиты информации 2. Дайте определение понятиям идентификации и аутентификации 3. Перечислите основные виды аутентификации. 4. Какую роль играет подготовленность персонала в построении системы защиты?	7	Внеаудиторная, изучение учебных пособий
8	1. методы проведения аудита (анализ документации, инструментальный контроль, опрос сотрудников); 2. состав аудиторов (требования); 3. этапы и периодичность аудита.	7	Внеаудиторная, изучение учебных пособий

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

Отчет по лабораторной работе

Оформляется и отчитывается в электронном виде: формат листа А4, книжная ориентация страницы. Отчеты по всем лабораторным работам имеют единый титульный лист, на котором указывается наименование дисциплины, ФИО и группа исполнителя, ФИО преподавателя, принимающего отчеты. В отчете по каждой лабораторной работе должно быть представлено наименование работы, цель, ход выполнения работы (скриншоты, краткое текстовое описание), выводы по результатам работы.

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

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Введение в курс. Информационная безопасность. Проблемы развития теории и практики обеспечения информационной безопасности.	Обзорная лекция	Не предусмотрено	выполнение теста
Значение информационной безопасности для субъектов информационных отношений. Составляющие национальных интересов РФ в информационной сфере.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы, фронтальный опрос
Общее содержание защиты информации. Концепция информационной безопасности	Лекция	Не предусмотрено	выполнение контрольной работы
Предмет и объект защиты информации. Информация как объект права собственности.	Лекция	Не предусмотрено	выполнение лабораторной работы
Теоретические и концептуальные основы защиты информации. Современные факторы, влияющие на защиту информации.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Угрозы защищаемой информации. Уязвимость информации. Модель гипотетического нарушителя информационной безопасности	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Системное обеспечение защиты информации. Основные принципы построения системы защиты.	Лекция	Не предусмотрено	выполнение контрольной работы
Методы защиты информации. Модели защиты информации. Конфиденциальность при работе с зарубежными партнерами. Аудит информационной безопасности	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных 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%.

6.2. Информационные технологии

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 электронных учебников и различных сайтов как источник информации	1 - 8	Подготовка к защите отчетов по лабораторным работам
Использование возможностей электронной почты преподавателя	1 - 8	Подготовка к защите отчетов по лабораторным работам
Использование средств представления учебной информации	1 - 8	Использование мультимедийной презентации

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. Перечень программного обеспечения и информационных справочных систем

6.3.1. Программное обеспечение:

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
Kaspersky Endpoint Security	Средство антивирусной защиты

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) «Теория информационной безопасности и методология защиты информации» 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.	Введение в курс. Информационная безопасность. Проблемы развития теории и практики обеспечения информационной безопасности.	ПК 4	Тест, вопросы к экзамену
2.	Значение информационной безопасности для субъектов информационных отношений. Составляющие национальных интересов РФ в информационной сфере.	ПК 4	Вопросы к экзамену, задание и вопросы по лабораторной работе
3.	Общее содержание защиты информации. Концепция информационной безопасности	ПК 4	Вопросы к экзамену, контрольная работа 1
4.	Предмет и объект защиты информации. Информация как объект права собственности.	ПК 4	Вопросы к экзамену, задание и вопросы по лабораторной работе
5.	Теоретические и концептуальные основы защиты информации. Современные факторы, влияющие на защиту информации.	ПК 4	Вопросы к экзамену, задание и вопросы по лабораторной работе
6.	Угрозы защищаемой информации. Уязвимость информации. Модель гипотетического нарушителя информационной безопасности	ПК 4	Вопросы к экзамену, задание и вопросы по лабораторной работе
7.	Системное обеспечение защиты информации. Основные принципы построения системы защиты.	ПК 4	Вопросы к экзамену, контрольная работа 2
8.	Методы защиты информации. Модели защиты информации. Конфиденциальность при работе с зарубежными партнерами. Аудит информационной безопасности	ПК 4	Вопросы к экзамену, задание и вопросы по лабораторной работе

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

Для оценки результатов обучения применяются следующие критерии:

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 «Введение в курс. Информационная безопасность. Проблемы развития теории и практики обеспечения информационной безопасности.»

1. Входное тестирование

Пробные тесты:

1. Подберите слово к данному определению: _____ - сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают ИС (живые организмы, управляющие машины и др.) в процессе жизнедеятельности и работы.

а) информация;

б) сведения;

в) данные.

2. Подберите слово к данному определению: _____ - возможность за приемлемое время получить требуемую информационную.

а) доступность;

б) целостность;

в) конфиденциальность.

3. Какой из перечисленных уровней не относится к уровням формирования режима информационной безопасности?

а) правовой;

б) инженерно-технический;

в) информационный;

г) организационный.

4. Доступность информации гарантирует:

а) неизменность информации в любое время;

б) получение требуемой информации за определение время;

в) получение требуемой информации за неопределенное время;

г) защищенность информации от возможных угроз.

5. Конфиденциальность информации гарантирует:

а) доступность информации кругу лиц, для кого она предназначена;

б) защищенность информации от потери;

в) защищенность информации от фальсификации;

г) доступность информации только автору.

6. Подберите словосочетание к данному определению: _____ - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

а) информационная безопасность;

б) защита информации;

в) безопасность информации.

7. Что из перечисленного является составляющей информационной безопасности?

а) проверка прав доступа к информации;

б) доступность информации;

в) выявление нарушений.

8. Что из перечисленного является задачей информационной безопасности?

а) устранение неисправностей аппаратных средств;

б) устранений последствий стихийных бедствий;

в) защита технических и программных средств информатизации от ошибочных действий персонала;

г) восстановление линий связи.

9. Подберите словосочетание к данному определению: _____ - существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

а) доступность информации;

б) целостность информации;

в) конфиденциальность информации.

10. Что из перечисленного не относится к числу основных аспектов информационной безопасности?

а) доступность;

б) конфиденциальность;

в) целостность;

г) правдивое отражение действительности.

11. Подберите слово к данному определению: _____ - получение одних информационных объектов из других информационных объектов путем выполнения некоторых алгоритмов.

а) обработка информации;

б) конфиденциальность информации;

в) защита информации.

12. Подберите словосочетание к данному определению: _____ - организованный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления организаций, общественных объединений на основе формирования и использования информационных ресурсов.

а) информатизация общества;

б) информатика;

в) безопасность информации;

г) социометрия.

13. Подберите словосочетание к данному определению: _____ - состояние информации, ИР и ИС, при котором с требуемой вероятностью обеспечивается ЗИ (данных) от утечки, хищения, утраты, НС уничтожения, искажения, модификации (подделки), копирования, блокировки и т.п.

а) безопасность информации;

б) защита информации;

в) защита от НСД.

14. Подберите слово к данному определению: _____ - субъективно определяемая характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий доступа к ней.

а) доступность;

б) целостность;

в) конфиденциальность.

15. Основными задачами обеспечения информационной безопасности является ...?

а) создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения безопасности информации;

б) обеспечить производство средств защиты информации;

в) создать систему органов, ответственных за безопасность информации.

Тема «Значение информационной безопасности для субъектов информационных отношений. Составляющие национальных интересов РФ в информационной сфере.»

1. ***Лабораторная работа «Изучение методов экспертной оценки»***

Задание:

- Выбрать объекты (6-10 шт.) для проведения экспертной оценки и критерий оценки (например, объекты – компоненты компьютера, критерий – критичность выхода из строя).
- Выполнить оценку объектов с применением метода строгого ранжирования (с привлечением 5 экспертов). Проверить согласованность мнений экспертов.
- Выполнить оценку объектов с применением метода нестрогого ранжирования (с привлечением 5 экспертов). Проверить согласованность мнений экспертов.

Контрольные вопросы:

- Преимущества и недостатки методов экспертной оценки.
- Строгое и нестрогое ранжирование. Процедура оценки. Отличия.

Тема «Общее содержание защиты информации. Концепция информационной безопасности»

1. ***Контрольная работа 1***

Вопросы:

1. Дайте определение понятию защита информации.
2. Дайте определение понятию информационная безопасность
3. Какое место занимает защита информации в информационной безопасности?
4. Что представляет собой политика безопасности организации?
5. Перечислите основные методы обеспечения информационной безопасности РФ
6. Перечислите основные документы в области международной информационной безопасности.

Тема «Предмет и объект защиты информации. Информация как объект права собственности.»

1. ***Лабораторная работа «Классификация информационных ресурсов»***

Выберите сферу деятельности организации и непосредственного представителя (реального или вымышленного) из этой сферы. Проведите классификацию информации, обрабатываемой (хранимой) в организации: опишите вид информационных ресурсов, средства их хранения и обеспечения к ним доступа.

Оцените уровни защищенность информационных ресурсов в этой организации.

Результаты представьте в виде таблицы «виды ресурсов – горизонтальные строки»; вертикальные колонки – уровни защищенности информации в отношении возможностей повреждения по техническим причинам; из-за ошибок операторов; из-за несанкционированных корректировки, удаления, добавления информации, несанкционированного ознакомления с ней. В клетках таблицы оценки могут быть представлены в количественной форме или качественной (отличная защищенность, хорошая, удовлетворительная, неудовлетворительная, практически отсутствует). В столбце «примечания» дать ссылку на нормативный документ, связанный с видом информации.

Оцените, в каких направлениях могут быть приняты меры для повышения информационной безопасности различных видов информационных ресурсов.

Тема «Теоретические и концептуальные основы защиты информации. Современные факторы, влияющие на защиту информации.»

1. ***Лабораторная работа «Разграничение доступа пользователей к информационным ресурсам»***

   На основе данных из предыдущей лабораторной работы разработать систему доступа пользователей к информационным ресурсам на основе дискреционной и мандатной моделей.

   Оценить достоинства и недостатки рассматриваемых моделей.

Тема «Угрозы защищаемой информации. Уязвимость информации. Модель гипотетического нарушителя информационной безопасности»

1. ***Лабораторная работа «Модель нарушителя»***

   На основе данных из предыдущих лабораторных работ составить модель нарушителя. Оценить потенциал, мотив, оснащенность, опасность нарушителя в соответствии с перечнем и ценностью информационных ресурсов.

Тема «Системное обеспечение защиты информации. Основные принципы построения системы защиты.»

1. ***Контрольная работа 2***

Вопросы:

1. Дайте определение понятию угроза.
2. На основании чего строится модель нарушителя?
3. Сформулируйте основные принципы построения системы защиты информации
4. Дайте определение понятиям адентификации и аутентификации
5. Перечислите основные виды аутентификации.

6. Какую роль играет подготовленность персонала в построении системы защиты?

Тема «Методы защиты информации. Модели защиты информации. Конфиденциальность при работе с зарубежными партнерами. Аудит информационной безопасности»

1. ***Лабораторная работа «Аудит информационной безопасности»***

Составить план проведения аудита, включающий:

- перечень аудируемых ресурсов;
- методы проведения аудита (анализ документации, инструментальный контроль, опрос сотрудников);
- состав аудиторов (требования);
- этапы и периодичность аудита.

Перечень экзаменационных вопросов

1. Понятия: безопасность, информационная безопасность, защита информации.
2. Понятие национальной безопасности. Роль и место информационной безопасности в системе национальной безопасности.
3. Основные составляющие аспекты информационной безопасности.
4. Основные направления информационной безопасности.
5. Основные понятия защиты информации, безопасности информации.
6. Состояние проблемы защиты информации.
7. Основные принципы построения систем защиты.
8. Критерии, условия и принципы отнесения информации к защищаемой.
9. Становление и современное определение понятия “государственная тайна”. Перечень сведений, являющихся государственной тайной, их назначение и структура.
10. Степени секретности сведений, отнесенных к государственной тайне. Грифы секретности носителей информации.
11. Становление и современное определение коммерческой тайны. Степени конфиденциальности сведений, составляющих коммерческую тайну.
12. Понятие служебной тайны, границы и области ее действия.
13. Понятия “личная тайна”, “защищаемая информация и гражданах (персональные данные)”.
14. Категории информации, отнесенной к персональным данным. Разновидности личной тайны.
15. Понятие и особенности профессиональной тайны.
16. Действия, приводящие к неправомерному овладению конфиденциальной информацией
17. Понятие угрозы информационной безопасности.
18. Классификация угроз информационной безопасности.
19. Основные методы реализации угроз информационной безопасности.
20. Основные действия по определению конфиденциальности информации.
21. Каналы утечки информации. Классификация технических каналов утечки информации.
22. Источники образования ТКУИ и их основные характеристики.
23. Модель вероятного нарушителя и оценка его возможностей.
24. Алгоритм проведения специальных проверок помещений.
25. Правовое обеспечение ИБ.
26. Организационное обеспечения ИБ.
27. Инженерно-техническое обеспечение ИБ.
28. Требования руководящих документов по обеспечению информационной безопасности и НСД.
29. Защита информации от утечки по визуально-оптическим каналам.

30. Защита информации от утечки по акустическим каналам. Акустическая защита.
31. Защита информации от утечки по электромагнитным каналам.
32. Защита от утечки за счет микрофонного эффекта.
33. Защита от утечки за счет электромагнитного излучения.
34. Защита от утечки за счет паразитной генерации. Защита от утечки по цепям питания.
35. Защита от утечки по цепям заземления. Защита от утечки за счет высокочастотного навязывания.
36. Защита от утечки в волокно-оптических линиях и системах.
37. Защита информации от утечки по материально-вещественным каналам.
38. Состав и характеристика каналов несанкционированного доступа к конфиденциальной информации.
39. Методы несанкционированного доступа к конфиденциальной информации, применяемые при использовании каждого канала. Существующая классификация каналов.
40. Направления взаимодействия с зарубежными партнерами. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами.
41. Направления деятельности в области аудита информационной безопасности.
42. Этапы проведения аудита. Отчетные документы по проведению специальной проверки.

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	Основными источниками угроз информационной безопасности являются: а. Хищение жестких дисков, подключение к сети, инсайдерство б. Перехват данных, хищение данных, изменение архитектуры системы в. Хищение данных, подкуп системных администраторов, нарушение регламента работы	б	2
2.		Порядок и правила применения определенных принципов и средств защиты информации 1) Способ защиты информации 2) Система защиты информации 3) Метод защиты информации 4) Элемент защиты информации	1	3
3.		Условно технические средства защиты коммерческой информации можно разделить на: 1. Средства обнаружения угроз. 2. Средства отражения угроз. 3. Средства ликвидации угроз. 4. Средства защиты компьютерных систем и баз данных от несанкционированного доступа. 5. Средства регулирования доступа	1, 2, 3	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		6. Средства контроля вероятных каналов утечки информации		
4.		Система физической защиты (средства физической защиты) материальных и финансовых ресурсов должна предусматривать: 1. систему инженерно-технических средств защиты 2. систему регулирования доступа 3. систему контроля вероятных каналов утечки информации 4. систему программно-аппаратных средств защиты 5. систему регулирования допуска	1, 2, 3	3
5.		На сколько уровней с практической точки зрения целесообразно разделить политику безопасности? 1. 1 2. 2 3. 3 4. 4	3	3
6.	Задание открытого типа	Примерная структура концепции безопасности коммерческого предприятия	Примерная структура концепции безопасности коммерческого предприятия может выглядеть следующим образом: 1. Описание проблемной ситуации в сфере безопасности предприятия: • перечень потенциальных и реальных угроз безопасности, их классификация и ранжирование; • причины и факторы зарождения угроз; • негативные последствия угроз для предприятия. 2. Механизм обеспечения безопасности: • определение объекта и предмета безопасности предприятия; • формулирование политики и стратегии безопасности; • принципы обеспечения безопасности; • цели обеспечения безопасности;	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			• задачи обеспечения безопасности; • критерии и показатели безопасности предприятия; • создание оргструктуры по управлению системой безопасности предприятия. 3. Мероприятия по реализации мер безопасности: • формирование подсистем общей системы безопасности предприятия; • определение субъектов безопасности предприятия и их роли; • расчет средств и определение методов обеспечения безопасности. 4. Контроль и оценка процесса реализации концепции.	
7.		Аналитическая работа с источником угрозы конфиденциальной информации	Аналитическая работа с источником угрозы конфиденциальной информации предусматривает: • выявление и классификацию максимального состава источников угрозы конфиденциальной информации; • учет и изучение каждого отдельного субъективного внутреннего и внешнего источника, степени его опасности (анализ риска) при реализации угрозы; • разработку превентивных мероприятий по локализации и ликвидации объективных угроз.	6
8.		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	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			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.	
9.		При выполнении каких условий обеспечивается эффективная защита предприятия?	Эффективная защита предприятия обеспечивается при выполнении следующих условий: • единство в решении производственных, коммерческих, финансовых и режимных вопросов; • координация мер безопасности между заинтересованными подразделениями фирмы; • разработка режимных мер на основе оценки информации и объектов, подлежащих защите (классификации); • персональная ответственность на всех исполнительских уровнях за обеспечение сохранности конфиденциальной информации; • организация специального делопроизводства, введение соответствующей маркировки документов; • разработка и утверждение списка с перечнем лиц, допущенным к такого рода информации; • наличие охраны, а также пропускного и внутриобъектового режимов.	8
10.		Класс, которые присваивается типовой информационной системе по результатам анализа исходных данных	По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			• класс 1 (К1) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных; • класс 2 (К2) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к средним негативным последствиям для субъектов персональных данных; • класс 3 (К3) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных; • класс 4 (К4) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.	

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 результатов обучения по дисциплине (модулю)

Фонды оценочных средств по дисциплине

Фонд оценочных средств позволяет оценить знания, умения и уровень приобретенных компетенций.

Фонд оценочных средств по дисциплине включает:

- вопросы к экзамену;
- лабораторные работы;
- набор вариантов контрольных работ;
- набор тестов.

Оценка качества освоения программы дисциплины включает текущий контроль успеваемости, промежуточную аттестацию, итоговую аттестацию.

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.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных и тематических контрольных работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На экзамене осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины и с проверкой практических навыков и умений по разработке документов различных видов. Теоретические знания оцениваются путем компьютерного тестирования или на основании письменных ответов студентов по нескольким теоретическим вопросам.

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*	5/5	25	В соответствии с таблицей 2
2.	*Выполнение контрольной работы*	2/5	10	
3.	*Тест*	1/5	5	
Всего			**40**	-
Блок бонусов				
4.	*Посещение занятий без пропусков*		3	
5.	*Своевременное выполнение всех заданий*		3	
6.	*Активность студента на занятии*		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. Методологические основы построения защищенных автоматизированных систем : учеб. пособие / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий, А.П. Данилкин, А.А. Малышев - Воронеж : ВГУИТ, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785894489810.html (ЭБС «Консультант студента»).
2. Системы безопасности и устройства кодового доступа: просто о сложном / Кашкаров А.П. - М. : ДМК Пресс, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785940747697.html (ЭБС «Консультант студента»).
3. Защита персональных данных в организации / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин - М.: ФЛИНТА, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785976512733.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература:

1. Теория защиты информации / Малюк А.А. - М. : Горячая линия - Телеком, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785991202466.html (ЭБС «Консультант студента»).
2. Безопасность информации в автоматизированных системах / В.В. Мельников. - М. : Финансы и статистика, 2003. - URL: http://www.studentlibrary.ru/book/ISBN5279025607.html (ЭБС «Консультант студента»).
3. Мельников, В.П. Информационная безопасность и защита информации : доп. УМО по ун-тскому политех. образованию в качестве учеб. пособия для студентов вузов, обучающихся по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова. - 4-изд. ;

стер. - М. : Академия, 2009. - 336 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-6150-4 : 306-46. (19 экз.)
4. Концептуальные основы создания и применения системы защиты объектов / 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»).

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).