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)

Основы управления информационной безопасностью

наименование

Составитель(-и)	**Гурская Т.Г., 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. Цели освоения дисциплины «Основы управления информационной безопасностью»: дать представление об управлении информационной безопасностью для обеспечения бесперебойной работы организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму.

1.2. Задачи освоения дисциплины (модуля):

- освоение основ теории управления информационной безопасностью: концепциями контроля и оптимизации стратегии и тактики защиты объектов информатизации с учетом специфики организации и видов угроз;
- изучение основных положений разработки методологии управления организацией и реализацией политик информационной безопасности на предприятиях, знакомство с базовыми методами и средствами управления комплексной защитой объектов информатизации;
- применение организационных, правовых, инженерно-технических и аппаратно-программных методов и средств управления информационной безопасностью в научно-исследовательских и практических разработках, а также при эксплуатации систем защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина Б1.Б.20 «Основы управления информационной безопасностью» относится к базовой части 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*:*

- Вероятностно-статистические методы в анализе данных.
- Информатика.
- Теория информации.
- Организационное и правовое обеспечение информационной безопасности.
- Защита информации от утечки по техническим каналам.

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; 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.

Умения: анализировать и оценивать угрозы информационной безопасности объекта; строить структурные и имитационные модели систем защиты объектов информатизации, алгоритмизировать и программировать порядок решения задач по оценке и исследованию уровней защищенности компьютерных систем; пользоваться нормативными документами по защите информации.

Навыки: работы с нормативными правовыми актами; работы с ЭВМ, офисными и специализированными пакетами программ, предназначенных для организации защиты объектов информатизации и подготовки технических решений; владения методами технической защиты информации; методами расчета и инструментального контроля

показателей технической защиты информации;

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 «Основы управления информационной безопасностью» поможет студентам при реализации задач 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):

общепрофессиональных (ОПК): ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба; ОПК-2.2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИОПК-10.1. Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности.	ИОПК-10.2. Уметь: в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	ИОПК-10.3. Владеть: методами формирования и выполнения комплекса мер по информационной безопасности.
ОПК-2.1. Способен проводить анализ	ИОПК-2.1.1. Знать: возможные источники	ИОПК-2.1.2. Уметь: проводить	ИОПК-2.1.3. Владеть: методами анализа

функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб.	анализ функционального процесса объекта защиты и его информационных составляющих.	функционального процесса объекта защиты и его информационных составляющих.
ОПК-2.2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК-2.2.1. Знать: структуру и функциональные процессы объекта защиты и его информационные составляющие	ОПК-2.2.2. Уметь: формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК-2.2.3. Владеть: методами повышения их устойчивости к деструктивным воздействиям на информационные ресурсы

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) в зачетных единицах **3 зачетные единицы**. Всего 108 часов: 36 часов выделено на контактную работу обучающихся с преподавателем (лекции – 18, лабораторные работы – 18), 72 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	Структура документа. Задание требований к информационной безопасности организации. Оценка рисков нарушения безопасности.	7	1-2	2		2		9	Входное тестирование, отчет по лабораторной работе, опрос на зачете

2	Политика безопасности. Организация защиты. Инфраструктура информационной безопасности.		3-4	2		2		9	отчет по лабораторной работе, опрос на зачете
3	Классификация ресурсов и их контроль. Безопасность персонала. Реагирование на события, таящие угрозу безопасности.		5-6	2		2		9	отчет по лабораторной работе, контрольная работа 1, опрос на зачете
4	Физическая безопасность и безопасность окружающей среды. Планирование систем и их приёмка. Защита от вредоносного ПО.		7-8	2		2		9	отчет по лабораторной работе, опрос на зачете
5	Обслуживание систем. Оперирование с носителями информации и их защита.		9-10	2		2		9	отчет по лабораторной работе, опрос на зачете
6	Управление доступом к системам. Управление доступом к сети.		11-12	2		2		9	отчет по лабораторной работе, опрос на зачете
7	Разработка и сопровождение информационных систем. Безопасность в прикладных системах.		13-14	2		2		9	отчет по лабораторной работе, контрольная работа 2, опрос на зачете
8	Планирование бесперебойной работы организации. Аудит систем.		15-18	4		4		9	отчет по лабораторной работе, итоговое тестирование, опрос на зачете
	ИТОГО		**108**	**18**		**18**		**72**	**ЗАЧЕТ**

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
		ОПК 10	ОПК 2.1	ОПК 2.2.	
Структура документа. Задание требований к информационной безопасности организации. Оценка	13	+	+	+	**3**

рисков нарушения безопасности.					
Политика безопасности. Организация защиты. Инфраструктура информационной безопасности.	13	+	+	+	**3**
Классификация ресурсов и их контроль. Безопасность персонала. Реагирование на события, таящие угрозу безопасности.	13	+	+	+	**3**
Физическая безопасность и безопасность окружающей среды. Планирование систем и их приёмка. Защита от вредоносного ПО.	13	+	+	+	**3**
Обслуживание систем. Оперирование с носителями информации и их защита.	13	+	+	+	**3**
Управление доступом к системам. Управление доступом к сети.	13	+	+	+	**3**
Разработка и сопровождение информационных систем. Безопасность в прикладных системах.	13	+	+	+	**3**
Планирование бесперебойной работы организации. Аудит систем.	17	+	+	+	**3**
Итого	***108***				

Краткое содержание дисциплины

Тема 1

Структура документа. Ключевые средства контроля. Задание требований к информационной безопасности организации. Оценка рисков нарушения безопасности. Разработка собственных рекомендаций. ГОСТ Р ИСО/МЭК 27001. ГОСТ Р ИСО/МЭК 27005.

Тема 2

Политика безопасности. Политика информационной безопасности. Организация защиты. Инфраструктура информационной безопасности. Безопасность доступа сторонних организаций. ГОСТ Р ИСО/МЭК 27002.

Тема 3

Классификация ресурсов и их контроль. Ответственность за ресурсы. Безопасность персонала. Безопасность в должностных инструкциях и при выделении ресурсов. Обучение пользователей. Реагирование на события, таящие угрозу безопасности.

Тема 4

Физическая безопасность и безопасность окружающей среды. Защищённые области. Защита оборудования. Администрирование компьютерных систем и вычислительный сетей. Операционные процедуры и обязанности. Планирование систем и их приёмка. Защита от вредоносного программного обеспечения. ГОСТ Р ИСО/МЭК 27003

Тема 5
Обслуживание систем. Сетевое администрирование. Оперирование с носителями информации и их защита. Обмен данными и программами.

Тема 6
Управление доступом к системам. Управление доступом к сети. Слежение за доступом к системам и их использованием.

Тема 7
Разработка и сопровождение информационных систем. Требования к безопасности систем. Безопасность в прикладных системах. Защита файлов прикладных систем. Безопасность в среде разработки и рабочей среде.

Тема 8
Планирование бесперебойной работы организации. Выполнение правовых требований. Проверка безопасности информационных систем. Аудит систем. ГОСТ Р ИСО/МЭК 27006. ГОСТ Р ИСО/МЭК 27007.

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 PowerPoint.

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	а) написать классификации предприятий по форме собственности и в соответствии с отраслевой принадлежностью, б) изучить Общероссийский классификатор видов экономической деятельности ОК 029-2014 (ОКВЭД) и определить каким видом деятельности занимается выбранное предприятие.	9	Внеаудиторная, изучение учебных пособий
2	а) опишите процесс информирования об инцидентах нарушения информационной безопасности	9	Внеаудиторная, изучение учебных пособий

	б) опишите порядок оценки угроз безопасности информации в соответствии с "Методическим документом. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021).		
3	в соответствии с "Методическим документом. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021): 1) опишите порядок оценки актуальности угроз безопасности информации, 2) опишите процесс формирования экспертной группы и проведения экспертной оценки при оценке угроз безопасности информации.	9	Внеаудиторная, изучение учебных пособий
4	в соответствии с "Методическим документом. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021): а) опишите процесс определения источников угроз безопасности информации. б) опишите виды нарушителей, актуальных для систем и сетей.	9	Внеаудиторная, изучение учебных пособий
5	1) определение корпоративной политики организации, 2) определение частной политики организации, 3) виды трастовых моделей.	9	Внеаудиторная, изучение учебных пособий
6	1. Опишите группы средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации. 2. Сущность метода экспертных оценок.	9	Внеаудиторная, изучение учебных пособий
7	1. Понятия социальной инженерии и обратной социальной инженерии. 2. Защита от социальной инженерии.	9	Внеаудиторная, изучение учебных пособий
8	1. Понятие уязвимости, угрозы, атаки. 2. Понятие риска, оценки риска. 3. Экономическая модель оценки риска: основное содержание, достоинства, недостатки.	9	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
Структура документа. Задание требований к информационной безопасности организации. Оценка рисков нарушения безопасности.	Обзорная лекция	Не предусмотрено	выполнение теста, выполнение лабораторной работы
Политика безопасности. Организация защиты. Инфраструктура информационной безопасности.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Классификация ресурсов и их контроль. Безопасность персонала. Реагирование на события, таящие угрозу безопасности.	Лекция	Не предусмотрено	выполнение лабораторной работы, выполнение контрольной работы
Физическая безопасность и безопасность окружающей среды. Планирование систем и их приёмка. Защита от вредоносного ПО.	Лекция	Не предусмотрено	выполнение лабораторной работы
Обслуживание систем. Оперирование с носителями информации и их защита.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Управление доступом к системам. Управление доступом к сети.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Разработка и сопровождение информационных систем. Безопасность в прикладных системах.	Лекция	Не предусмотрено	выполнение контрольной работы, выполнение лабораторной работы
Планирование бесперебойной работы организации. Аудит систем.	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, составление словаря, подготовка обзора методик оценки рисков
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
Google Chrome	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) «Основы управления информационной безопасностью» 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.	Структура документа. Задание требований к информационной безопасности организации. Оценка рисков нарушения безопасности.	ОПК 10, ОПК 2.1, ОПК 2.2.	Входное тестирование, лабораторная работа 1, вопросы к зачету
2.	Политика безопасности. Организация защиты. Инфраструктура информационной безопасности.	ОПК 10, ОПК 2.1, ОПК 2.2.	лабораторная работа 1 Вопросы к зачету
3.	Классификация ресурсов и их контроль. Безопасность персонала. Реагирование на события, таящие угрозу безопасности.	ОПК 10, ОПК 2.1, ОПК 2.2.	лабораторная работа 2 Вопросы к зачету, контрольная работа 1
4.	Физическая безопасность и безопасность окружающей среды. Планирование систем и их приёмка. Защита от вредоносного ПО.	ОПК 10, ОПК 2.1, ОПК 2.2.	лабораторная работа 2 Вопросы к зачету
5.	Обслуживание систем. Оперирование с носителями информации и их защита.	ОПК 10, ОПК 2.1, ОПК 2.2.	лабораторная работа 3 Вопросы к зачету
6.	Управление доступом к системам. Управление доступом к сети.	ОПК 10, ОПК 2.1, ОПК 2.2.	лабораторная работа 4 Вопросы к зачету
7.	Разработка и сопровождение информационных систем. Безопасность в прикладных системах.	ОПК 10, ОПК 2.1, ОПК 2.2.	лабораторная работа 5 Вопросы к зачету, контрольная работа 2
8.	Планирование бесперебойной работы организации. Аудит систем.	ОПК 10, ОПК 2.1, ОПК 2.2.	лабораторная работа 6 итоговое тестирование Вопросы к зачету

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 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетво рительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

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

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

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

Тема «Структура документа. Задание требований к информационной безопасности организации. Оценка рисков нарушения безопасности»

1. Входное тестирование

Пробные тесты:

1. По объекту воздействия угрозы бывают:

- воздействующие на информационную среду в целом
- воздействующие на отдельные элементы информационной среды
- активные
- пассивные

2. Выберите правильный вариант ответа. Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий (информационной безопасности), имеющих значительную вероятность компрометации бизнес-операции и создания угрозы
- инцидент
- нарушение
- сигнал

3. Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности называется
- событием (информационной безопасности)
- инцидентом (информационной безопасности)
- угрозой (информационной безопасности)

4. Первым шагом в управлении сетью является ее
- документирование
- ревизия
- оформление

5. Какова цель ревизии эффективности?
- Мониторинг и анализ работы сети.
- Определение того, работает ли сеть в соответствии со своим потенциалом.
- Идентификация типов оборудования и устройств, сети.
- Обеспечение информации о восстановлении после сбоя или катастрофического отказа.

2. ***Лабораторная работа №1 «Сбор исходной информации о предприятии»***

Выбрать реальную или вымышленную организацию, для которой будет разрабатываться система управления информационной безопасностью. Используя информацию в открытых источниках, собрать (придумать) сведения о деятельности организации, обрабатываемой информации.

Тема «Политика безопасности. Организация защиты. Инфраструктура информационной безопасности»

1. ***Лабораторная работа № 1 «Сбор исходной информации о предприятии» (продолжение)***

Составить документ, содержащий исходную информацию о предприятии, на котором вы должны будете внедрять СУИБ. В документе должны быть отражены организационная структура предприятия, уровень его зрелости, задачи и функции предприятия, информационные потоки, реализованные на предприятии меры защиты информации.

Тема «Классификация ресурсов и их контроль. Безопасность персонала. Реагирование на события, таящие угрозу безопасности»

1. ***Контрольная работа 1***

Вопросы к контрольной работе:

1. Задание требований к информационной безопасности организации
2. Оценка рисков нарушения безопасности
3. Политика информационной безопасности
4. Координация действий по защите информации
5. Распределение обязанностей по обеспечению информационной безопасности
6. Инвентаризация информационных ресурсов
7. Безопасность в должностных инструкциях
8. Соглашение о конфиденциальности
9. Уведомление об инцидентах в системе безопасности
10. Процедура наложения дисциплинарных взысканий

2. ***Лабораторная работа №2 «Методика составления модели угроз»***

Изучить «Базовую модель угроз» и «Методику определения актуальных угроз» ФСТЭК. Описать структуру информационной системы персональных данных (ИСПДн), имеющейся в рассматриваемой организации.

Тема «Физическая безопасность и безопасность окружающей среды. Планирование систем и их приёмка. Защита от вредоносного ПО.»

1. ***Лабораторная работа №2 «методика составления модели угроз» (продолжение)***

Составить документ, содержащий в себе модель угроз безопасности персональных данных, используя методику определения актуальных угроз ФСТЭК.

Тема «Обслуживание систем. Оперирование с носителями информации и их защита»

1. ***Лабораторная работа № 3 «Разработка политики безопасности»***

Составить модель политики безопасности, которая будет включать в себя следующие пункты: термины и определения, цели и задачи, содержание политики, разделение полномочий и порядок внесения изменений в политику безопасности, определенные специально для вашего предприятия.

Тема «Управление доступом к системам. Управление доступом к сети.»

1. ***Лабораторная работа №4 «Анализ рынка и подбор СЗИ»***

В соответствии с выявленными актуальными угрозами подберите несколько средств защиты информации для своего предприятия и обоснуйте свой выбор методом экспертных оценок.

Тема «Разработка и сопровождение информационных систем. Безопасность в прикладных системах»

1. ***Контрольная работа 2***

Вопросы к контрольной работе:

1. Контроль доступа в помещения
2. Защита оборудования
3. Процедуры реагирования на события
4. Резервное копирование данных
5. Средства управления безопасностью сетей
6. Управление доступом пользователей
7. Система управления паролями
8. Требования к безопасности систем
9. Вопросы планирования бесперебойной работы организации

10. Аудит систем информационной безопасности

2. *Лабораторная работа № 5 «Проведение семинаров и аттестация сотрудников»*

Подготовить семинар по одному из вопросов, связанных с информационной безопасностью (социальная инженерия, возможности конкурентной разведки, конфиденциальное делопроизводство и др.). Семинар должен сопровождаться презентацией. Подготовить список вопросов для аттестации сотрудников вашего предприятия.

Отчет проводится в виде деловой игры, где докладчик – сотрудник службы информационной безопасности предприятия, остальные студенты – сотрудники рассматриваемой докладчиком организации (в соответствии со спецификой деятельности организации между студентами преподавателем могут распределяться конкретные роли (должности сотрудников)).

Тема «Планирование бесперебойной работы организации. Аудит систем»

1. *Лабораторная работа № 6 «Экономическая модель оценки рисков»*

Написать программу, реализующую экономическую модель оценки рисков.

Оценить риски на основе результатов выполнения предыдущих лабораторных работ (риск до применения защитных мер, риск после применения защитных мер).

2. *Итоговое тестирование*

1. Какова цель ревизии установленного оборудования?
   - Идентификация типов оборудования и устройств, сети.
   - Идентификация местонахождения каждого элемента сети.
   - Мониторинг и анализ работы сети.
   - Перенос информации на чертежи здания для создания карты нарезки.

2. Действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов - это
   - Защитные меры
   - Комплексные меры
   - Превентивные меры
   - Организационные меры

3. Какова цель ревизии средств защиты сети?
   - Согласование требований по защите сети со строительными нормами и нормами секретности.
   - Оценка способностей клиентов пользоваться сетевым оборудованием и программным обеспечением.
   - Выяснение способности сети гарантировать целостность данных.
   - Определение состава аппаратно-программного комплекса, требующегося для обеспечения защиты сети.

4. Какие шаги следует предпринять для анализа и решения проблемы в сети после сбора данных о работе?
   - Определить, является ли проблема периодической или устойчивой; составить список возможных причин; расставить приоритеты причин.
   - Расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины; отследить тенденции с целью предвидения возникновения проблем в будущем.
   - Составить список возможных причин; расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины.

- Определить, можно ли воспроизвести проблему; расставить приоритеты возможных причин; используя средства управления сетью или метод замены, идентифицировать причины.

5. Что из приведенного ниже должно быть включено в отчет о проведении оценки?

- Состав сетевой аппаратуры и программного обеспечения, которые не удовлетворяют промышленным стандартам.
- Журналы, показывающие тенденцию к уменьшению скорости трафика в определенных сегментах сети.
- Описание случаев и мест несанкционированного доступа к файлам.
- Описание типов пользователей, наиболее часто сталкивающихся с проблемами при пользовании сетью.

Список вопросов к зачету

1. Концептуальный анализ понятия информационной безопасности
2. Основные понятия в области информационной безопасности
3. Онтологическая модель процесса обеспечения ИБ
4. Классификация угроз информационной безопасности
5. Модель нарушителя
6. Классификация уязвимостей безопасности
7. Основные типы атак на информационные ресурсы
8. Ущерб от реализации атак на информационные ресурсы
9. Методы обеспечения информационной безопасности
10. Модель реализации угроз информационной безопасности
11. Управление безопасностью информационных активов
12. Принципы комплексного обеспечения информационной безопасности
13. Функциональная модель процесса комплексного обеспечения ИБ
14. Когнитивная модель системы комплексного обеспечения ИБ
15. Оценка повреждений сервисов безопасности
16. Общий алгоритм управления уровнем информационной безопасности
17. Экономическая эффективность внедрения систем КОИБ
18. Современные угрозы информационной безопасности
19. Причина неэффективности применяемых мер защиты
20. Направления и меры обеспечения информационной безопасности
21. СУИБ, процессный подход.
22. Понятие системы менеджмента информационной безопасности. Шесть уровней зрелости организации
23. Меры контроля ISO 17799
24. Стандарты ISO 27001 и ISO 27002
25. Стандарт Банка России СТО БР ИББС 1.0.
26. Идентификация информационных активов и классификация ресурсов.
27. Особенности сертификации системы менеджмента информационной безопасности.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение				

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты				
1.	Задание закрытого типа	Детальный процесс оценки риска ИБ включает 1) тщательное определение 2) установление ценности активов 3) оценку угроз этим активам 4) оценку уязвимостей 5) оценку информационной безопасности 6) оценку риска информационной безопасности	1, 2, 3	2
2.		Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя 1) Конфиденциальность информации 2) Целостность информации 3) Доступность информации 4) Неотказуемость информации	1	3
3.		Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) 1) Конфиденциальность информации 2) Целостность информации 3) Доступность информации 4) Неотказуемость информации	2	3
4.		Состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно 1) Конфиденциальность информации 2) Целостность информации 3) Доступность информации 4) Неотказуемость информации	3	3
5.		Группы пользователей ИСПДн: 1) Администраторы 2) Разработчики 3) Операторы 4) Руководители 5) Менеджеры	1, 2, 3	3
6.	Задание открытого типа	Основные этапы менеджмента рисков в соответствии с ГОСТ Р ИСО/МЭК 27003-2012	Основными этапами менеджмента рисков в соответствии с ГОСТ Р ИСО/МЭК 27003-2012 являются: 1. Проведение оценки риска 2. Выбор целей и средств управления 3. Получение санкций руководства на внедрение СМИБ	5
7.		Выходные данные этапа оценки рисков	Выходные данные этапа оценки рисков следующие: а) описание методологий оценки риска;	6

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			b) результаты оценки риска.	
8.		Какие факторы оказывают влияние на вероятность возникновения конкретной угрозы?	На вероятность возникновения конкретной угрозы оказывают влияние следующие факторы: - привлекательность актива или возможное воздействие - применимо при рассмотрении умышленной угрозы со стороны персонала; - простота преобразования актива, использующего уязвимость за вознаграждение, - применимо при рассмотрении умышленной угрозы со стороны персонала; - технические возможности действующего фактора угрозы - применимо при рассмотрении умышленной угрозы со стороны персонала; - чувствительность уязвимости к использованию - применимо к техническим и нетехническим уязвимостям.	8
9.		Что должна обеспечивать деятельность, связанная с информационной безопасностью?	Деятельность, связанная с информационной безопасностью, должна: a) обеспечивать уверенность в том, что обеспечение безопасности осуществляется в соответствии с политикой информационной безопасности; b) определять способ устранения несоответствия; c) утверждать методики и процессы обеспечения информационной безопасности, например оценку риска, классификацию информации; d) выявлять значительные изменения угроз и подверженность информации и средств обработки информации угрозам; e) оценивать адекватность и координировать реализацию мер и средств контроля и управления информационной безопасности; f) эффективно способствовать осведомленности, обучению и тренингу в отношении информационной безопасности в рамках организации; g) оценивать информацию, полученную в результате мониторинга и анализа инцидентов информационной безопасности, и рекомендовать	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			соответствующие действия в ответ на выявленные инциденты информационной безопасности.	
10.		Круг обязанностей каждого руководителя должен быть четко определен в соответствии с ГОСТ Р ИСО/МЭК 27002-2012	Круг обязанностей каждого руководителя должен быть четко определен в соответствии с ГОСТ Р ИСО/МЭК 27002-2012: a) активы и процессы (процедуры) безопасности, связанные с каждой конкретной системой, должны быть четко определены; b) необходимо назначить ответственных за каждый актив или процедуру безопасности, и подробно описать их обязанности в соответствующих документах; c) уровни полномочий должны быть четко определены и документально оформлены.	8
ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба				
11.	Задание закрытого типа	Совокупность механизмов, процедур и других средств защиты информации, которая обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление атаки: 1) сервис информационной безопасности 2) угроза безопасности информации 3) свойства информационной безопасности 4) защита информации	1	2
12.		Сервис, гарантирующий, что к информации при ее хранении или передаче не был получен доступ нелегитимными пользователями: 1) Конфиденциальность 2) Целостность 3) Доступность 4) Аутентичность	1	2
13.		Сервис, гарантирующий, что отсутствует изменение информации либо изменение осуществляется только преднамеренно субъектами, имеющими на это право 1) Конфиденциальность 2) Целостность 3) Доступность 4) Аутентичность	2	2
14.		Сервис, гарантирующий, что субъекты, имеющие права доступа к информации, могут реализовать их беспрепятственно 1) Конфиденциальность 2) Целостность	3	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		3) Доступность 4) Аутентичность		
15.		Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации 1) сервис информационной безопасности 2) угроза безопасности информации 3) свойства информационной безопасности 4) защита информации	2	2
16.	Задание открытого типа	Факторы, которые необходимо принять во время действия «Определение области действия и границ для информационных и коммуникационных технологий (ИКТ)»	Факторы, которые необходимо принять во время действия «Определение области действия и границ для информационных и коммуникационных технологий (ИКТ)»: a) социально-культурная среда; b) законные, обязательные или контрактные требования, применяемые к организациям; c) подотчетность за ключевые сферы ответственности; d) технические ограничения (например, доступная ширина полосы частот, наличие сервиса и т.д.).	8
17.		Границы ИКТ для действия «Определение области действия и границ для информационных и коммуникационных технологий (ИКТ)»	Границы ИКТ для действия «Определение области действия и границ для информационных и коммуникационных технологий (ИКТ)» должны включать описание следующих элементов: a) инфраструктура связи, в которой ответственность за ее управление входит в компетенцию организации, располагающей различными технологиями (например, беспроводные и проводные сети или сети передачи данных и телефонной связи); b) программное обеспечение в рамках организационных границ, используемое и контролируемое организацией; c) аппаратное обеспечение ИКТ, требуемое для сети или сетей, приложений или производственных систем; d) роли и сферы ответственности, связанные с аппаратным обеспечением ИКТ, сетью и программным обеспечением.	8
18.		Выходные данные действия «Определение физической области действия и границ»	Выходные данные действия «Определение физической области действия и границ» следующие:	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			a) описание физических границ СМИБ с обоснованием для исключения каких-либо физических границ, находящихся под управлением организации, из области действия СМИБ; b) описание организации и ее географических характеристик, относящихся к области действия СМИБ.	
19.		Выходные данные действия «Объединение всех областей действия и границ для получения области действия и границ СМИБ»	Выходные данные действия «Объединение всех областей действия и границ для получения области действия и границ СМИБ» представляют собой документ, описывающий область действия и границы СМИБ и содержащий следующую информацию: a) ключевые характеристики организации (функция, структура, услуги, активы и область действия и границы ответственности для каждого актива); b) процессы в организации, находящиеся в области действия СМИБ; c) конфигурация оборудования и сетей, находящихся в области действия СМИБ; d) предварительный перечень информационных активов, находящихся в области действия СМИБ; e) перечень активов ИКТ, находящихся в области действия СМИБ (например, серверов); f) схемы объектов, находящихся в области действия СМИБ, определяющие физические границы СМИБ; g) описание ролей и сфер ответственности в рамках СМИБ и их связи со структурой организации; h) подробное описание и обоснование исключений каких-либо элементов из области действия СМИБ.	8
20.		Какие аспекты необходимо определить при определении политики СМИБ?	При определении политики СМИБ необходимо определить следующие аспекты: a) установить цели СМИБ на основе требований и приоритетов организации в области информационной безопасности;	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			b) установить общие фокусные точки и руководства к действию для достижения целей СМИБ; c) учесть законные обязательные требования организации и договорные обязательства, связанные с информационной безопасностью; d) контекст управления рисками в рамках организации; e) установить критерии для оценки рисков и определения структуры оценки рисков; f) определить сферы ответственности руководителей высшего уровня в отношении СМИБ; g) получить одобрение руководства.	
ОПК-2.2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы				
21.	Задание закрытого типа	Блок изменений для оперативного исправления или нейтрализации ошибки в исполняемой программе, чаще всего поставляемый (или размещаемый на сайте разработчика) в виде небольшой программы, вставляющей исправления в объектный код соответствующих модулей приложения. 1) Патч 2) Вирус 3) Оператор 4) Компилятор	1	5
22.		Привлечение внешних организаций (на договорной основе) для выполнения некоторых бизнес-функций или частей бизнес-процесса организации 1) Аутсорсинг 2) Клиринг 3) Сотрудничество 4) Договоренность	1	5
23.		К программным активам относятся: 1) прикладные программные средства, 2) системные программные средства, 3) средства разработки и утилиты 4) компьютерное оборудование, 5) средства связи, 6) съемные носители информации	1, 2, 3	5
24.		К физическим активам относятся: 1) прикладные программные средства, 2) системные программные средства, 3) средства разработки и утилиты 4) компьютерное оборудование, 5) средства связи, 6) съемные носители информации и другое оборудование	4, 5, 6	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
25.		Владелец актива в соответствии с ГОСТ Р ИСО/МЭК 27002-2012 должен нести ответственность за: 1) обеспечение уверенности в том, что информация и активы, связанные со средствами обработки информации, классифицированы соответствующим образом; 2) определение и периодический пересмотр ограничений и классификаций доступа, принимая в расчет применимые политики управления доступом 3) планирование мероприятий на случай непредвиденных ситуаций и тщательность проверок 4) сбор и управление информацией по инцидентам безопасности	1, 2	5
26.	Задание открытого типа	Меры и средства контроля и управления против вредоносной программы в соответствии с ГОСТ ИСО 27002	Меры и средства контроля и управления против вредоносной программы в соответствии с ГОСТ ИСО 27002: a) создать официальную политику, устанавливающую запрет на использование неавторизованного программного обеспечения; b) создать официальную политику защиты от рисков, связанных с получением файлов и программного обеспечения, либо из внешних сетей, либо через другие передающие среды, показывающую, какие защитные меры следует принять; c) проводить регулярный анализ программного обеспечения и содержания данных систем, поддерживающих критические процессы бизнеса; необходима формальная процедура расследования причин наличия любых неавторизованных или измененных файлов; d) осуществлять в качестве превентивной меры или обычным порядком инсталляцию и регулярное обновление программного обеспечения по обнаружению вредоносной программы и восстановлению для сканирования компьютеров и носителей информации	8
27.		Проводимые проверки ПО в соответствии с ГОСТ ИСО 27002	Проводимые проверки ПО в соответствии с ГОСТ ИСО 27002 должны включать:	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			1) проверку на наличие вредоносной программы любых файлов на электронных или оптических носителях и файлов, полученных из сетей перед их использованием; 2) проверку любых вложений электронной почты и скачиваемой информации до их использования на наличие вредоносной программы; эта проверка должна выполняться в разных точках, например на серверах электронной почты, настольных компьютерах или при входе в сеть организации; 3) проверку web-страниц на наличие вредоносной программы;	
28.		Какие меры необходимо предпринять для предотвращения выполнения мобильной программой неразрешенных действий в соответствии с ГОСТ ИСО 27002?	Для предотвращения выполнения мобильной программой неразрешенных действий в соответствии с ГОСТ ИСО 27002 необходимо принимать следующие меры: a) обеспечивать выполнение мобильной программы в логически изолированной среде; b) блокировать любое несанкционированное использование мобильной программы; c) блокировать прием мобильной программы; d) активизировать технические меры, доступные в отношении определенной системы, чтобы обеспечить уверенность в управляемости мобильной программы; e) контролировать ресурсы, доступные мобильной программе; f) применять криптографические меры и средства контроля и управления для однозначной аутентификации мобильной программы.	8
29.		Какие вопросы необходимо решить в отношении резервирования информации в соответствии с ГОСТ ИСО 27002?	В отношении резервирования информации в соответствии с ГОСТ ИСО 27002 необходимо рассматривать следующие вопросы: a) необходимо определить надлежащий уровень резервной информации; b) необходимо обеспечивать точные и полные записи резервных копий и документально оформленные процедуры восстановления;	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			c) объем (т.е. полное или выборочное резервирование) и частота резервирования должны отражать требования бизнеса организации, требования к безопасности затрагиваемой информации и критичность информации для непрерывной работы организации; d) резервные копии должны храниться в удаленном месте, на надежном расстоянии, достаточном, чтобы избежать любого повреждения вследствие аварийной ситуации в основном здании; e) в отношении резервной информации должен быть обеспечен соответствующий уровень физической защиты и защиты от воздействий окружающей среды (см. 9), в соответствии со стандартами, применяемыми в основном здании; меры и средства контроля и управления, применяемые к носителям информации в основном здании, должны также применяться и на резервной площадке; f) носители резервной информации должны регулярно тестироваться для обеспечения уверенности в том, что в случае чрезвычайных ситуаций они могут быть использованы; g) процедуры восстановления следует регулярно проверять и тестировать для обеспечения уверенности в их эффективности, а также в том, что для выполнения этих процедур потребуется не больше времени, чем это определено; h) в ситуациях, когда конфиденциальность играет важную роль, резервные копии необходимо защищать посредством шифрования.	
30.		Меры и средства контроля и управления сетями в соответствии с ГОСТ ИСО 27002	Меры и средства контроля и управления сетями в соответствии с ГОСТ ИСО 27002: a) следует разделить, где это необходимо, ответственность за поддержку сетевых ресурсов и за поддержку компьютерных операций;	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			b) следует определить обязанности и процедуры для управления удаленным оборудованием, включая оборудование, установленное у конечных пользователей; c) специальные меры и средства контроля и управления следует внедрить для обеспечения конфиденциальности и целостности данных, передаваемых по общедоступным сетям, или по беспроводным сетям, а также для защиты подключенных систем и прикладных программ; специальные меры и средства контроля и управления могут потребоваться для поддержки доступности сетевых сервисов и рабочих станций; d) соответствующая регистрация и мониторинг должны применяться с целью обеспечения возможности регистрации действий, имеющих значение для безопасности; e) действия руководства должны быть тщательно согласованы как для оптимизации получаемых организацией услуг, так и для обеспечения уверенности в том, что меры и средства контроля и управления единообразно применимы ко всей инфраструктуре обработки информации.	

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)

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:

- небрежное выполнение,
- отсутствие выводов,
- нарушение сроков предоставления отчета.

Отчет не может быть принят и подлежит доработке в случае:

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

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

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

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине отводится 100 баллов (90 баллов на текущие формы контроля и до 10 баллов отводится на бонусы), которые накапливаются студентом в течение всего семестра изучения дисциплины.

Оценивание студентов на зачете 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 зачета.

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 зачете 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*	6/10	60	По расписанию
2.	*Выполнение контрольной работы*	2/10	20	
3.	*Тест*	1/10	10	
Всего			**90**	-
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**	-
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)

<table>
<tr><td>Сумма баллов</td><td colspan="2">Оценка по 4-балльной шкале</td></tr>
<tr><td>90–100</td><td>5 (отлично)</td><td rowspan="5">Зачтено</td></tr>
<tr><td>85–89</td><td rowspan="3">4 (хорошо)</td></tr>
<tr><td>75–84</td></tr>
<tr><td>70–74</td></tr>
<tr><td>65–69</td><td rowspan="2">3 (удовлетворительно)</td></tr>
<tr><td>60–64</td></tr>
<tr><td>Ниже 60</td><td>2 (неудовлетворительно)</td><td>Не зачтено</td></tr>
</table>

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

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

8.1. Основная литература:

1. Защита 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»)

2. Современные системы управления информационной безопасностью: учебное пособие / Абденов А.Ж. - Новосибирск : Изд-во НГТУ, 2017. - URL: http://www.studentlibrary.ru/book/ISBN9785778232365.html (ЭБС «Консультант студента»).

3. Ажмухамедов, И. М., Князева, О. М.,Гурская, Т. Г., Управление информационной безопасностью :учебное пособие: Издательский дом «Астраханский университет», 2016. URL: https://biblio.asu.edu.ru/Reader/Book/2017110114480712600002064338 (ЭБС Электронный Читальный зал – БиблиоТех).

4. Ажмухамедов, И. М., Князева, О. М., Сафаров, И. В., Управление информационной безопасностью: учебно-методическое пособие: Издательский дом «Астраханский университет», 2016. URL: https://biblio.asu.edu.ru/Reader/Book/2017052313503027600002063243 ЭБС Электронный Читальный зал – БиблиоТех).

8.2. Дополнительная литература:

1. Основы управления информационной безопасностью: Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Вып. 1. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202718.html (ЭБС «Консультант студента»)
2. Технические, организационные и кадровые аспекты управления информационной безопасностью : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202749.html (ЭБС «Консультант студента»)
3. Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202756.html (ЭБС «Консультант студента»)

8.3. 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.
2. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu.edu.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).