Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Астраханский государственный технический университет»
Система менеджмента качества в области образования, воспитания, науки и инноваций сертифицирована DQS по международному стандартуISO 9001:2015

Институт информационных технологий и коммуникаций

УТВЕРЖДАЮ:
Директор Института информационных технологий и коммуникаций
д.т.н., проф. Квятковская И.Ю. _____
Рассмотрено на Учебно-методическом совете,

протокол № 7 от «18» 06 2018 г.

Рабочая программа дисциплины

Защита информации

Направление подготовки
09.03.01 «Информатика и вычислительная техника»

Профиль подготовки
«Автоматизированные системы обработки информации и управления»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Согласовано:
к.т.н., доц., зав. кафедрой «Автоматизированные системы обработки информации и управления»
_____ Белов С.В.
«15» 06 2018 г.

Автор: к.т.н., доц.Давидюк Н.В. _____
Программа рекомендована кафедрой "Информационная безопасность"
протокол № 14 от « 14 » июня 2018 г.
Зав. кафедрой "Информационная безопасность",
д.т.н., проф. Попов Г.А. _____

Астрахань – 2018

Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Астраханский государственный технический университет»
Система менеджмента качества в области образования, воспитания, науки и инноваций сертифицирована DQS по международному стандартуISO 9001:2015

Институт информационных технологий и коммуникаций

УТВЕРЖДАЮ:
Директор Института информационных технологий и коммуникаций
д.т.н., проф. Квятковская И.Ю. _____
Рассмотрено на Учебно-методическом совете,
протокол № _7_ от «_18_»_июня__2018 г.

Рабочая программа дисциплины

Защита информации

Направление подготовки
09.03.01 «Информатика и вычислительная техника»

Профиль подготовки
«Автоматизированные системы обработки информации и управления»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Согласовано:
к.т.н., доц., зав. кафедрой «Автоматизированные системы обработки информации и управления»,
_____ Белов С.В.
«__» _____ 2018 г.

Автор: к.т.н., доц.Давидюк Н.В._____
Программа рекомендована кафедрой "Информационная безопасность"
протокол № _14 от «_14_» июня__ 2018 г.
Зав. кафедрой "Информационная безопасность",
д.т.н., проф. Попов Г.А. _____

Астрахань – 2018

1.Планируемые результаты обучения по дисциплине

Код	Определение	Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы		
		Знать	**Уметь**	**Владеть навыками и (или) иметь опыт**
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	основные нормативно-правовые акты в области информационной безопасности	применять на практике нормативные и правовые документы,регламентирующие деятельность в сфере информационной безопасности, классифицировать защищаемую информацию по видам тайн в соответствии с законодательством РФ и определять меры по ее защите	использования положений нормативно-правовых актов для обеспечения защиты информации ограниченного доступа
ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	основы государственной информационной политики, стратегию развития информационного общества в России; понятие государственной тайны и иных охраняемых законом тайн, сведений, составляющих государственную тайну, и сведений конфиденциального характера; организационно-правовые основы режима секретности; цели и задачи обеспечения информационной безопасности; основные термины по проблематике информационной	пользоваться законодательными и нормативными документами в профессиональной деятельности; пользоваться современными источниками информации по исследуемым проблемам и задачам; осуществлять сбор, обработку, анализ и систематизацию информации по обеспечению информационной безопасности; составлять аналитические обзоры по вопросам обеспечения информационной	анализа организаций и защищенности их информационных ресурсов с точки зрения информационной безопасности, состава комплекса мер для обеспечения защиты информации

		безопасности; методы обеспечения защиты информации; классификацию угроз; классификацию каналов утечки информации; модель потенциального злоумышленника	безопасности; пользоваться нормативно-правовой, организационно-распорядительной и методической документацией по вопросам обеспечения информационной безопасности; составлять перечень конфиденциальных информационных ресурсов; определять состав угроз безопасности информации и возможные каналы утечки информации; составить представление о потенциальном злоумышленнике	

2.Место дисциплиныв структуре ОП

Цикл (раздел) ОП, к которому относится данная дисциплина:	Б1.Б.22
Описание логической и содержательно-методической взаимосвязи с другими частям ОП (дисциплинами, практиками):	Организационные методы защиты информации Правовые аспекты защиты информации Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты Информатика
Компетенции, сформированные у обучающихся до начала изучения дисциплины:	-
Требования к «входным» знаниям, умениям и готовностям обучающегося, необходимым при освоении данной дисциплины:	Интеллектуальная зрелость, овладение своими познавательными процессами, аргументация и доказательство истинности суждений, критичность мышления, научное мировоззрение, творческая активность, профессиональные интересы, самоопределение, умение организовывать свою познавательную

	деятельность; умение найти нужную информацию по заданной теме в источниках различного типа, критически оценивать достоверность информации; владение основными видами публичных высказываний

3. Структура, содержание, объем (трудоёмкость) дисциплины

Общая трудоемкость дисциплины составляет 4 зачетныхединицы, 144 часа; в том числе на контактную работу обучающихся с преподавателем (далее - аудиторная работа по видам) - 54 часа (лекции -18 часов, лабораторные работы – 36 часов), на внеаудиторную самостоятельную работу обучающегося (далее внеаудиторная СРС) -90 часов.
По итогам освоения дисциплины –зачет с оценкой.

3.1.Для очной формы обучения:

№ п/п	Содержание дисциплины, структурированное по темам (разделам)	Семестр	Неделя	Аудиторная работа по видам			Внеаудиторная СРС	Образовательные технологии	Формы текущего контроля успеваемости
				Лек.	Лаб.	Пр.			
1	Основные термины и определения в области информационной безопасности. Понятие государственной тайны и иных охраняемых законом тайн, сведений конфиденциального характера.	7	1-2	2	4		8	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос
2	Базовые свойства защищаемой информации и систем ее обработки. Свойства информации как предмета защиты. Способы нанесения ущерба субъектам информационных		3-4	2	4		8	Информационная лекция, лабораторная работа с применением IT-технологи	Собеседование и отчет по лабораторной работе, устный опрос

	отношений. Определение требований к защищаемой информации. Особенности автоматизированной системы обработки информации как объекта защиты.							й	
3	Понятие угрозы безопасности информации, коррелирующие с этим понятием термины. Основные виды угроз безопасности субъектов информационных отношений. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.		5-6	2	4		8	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос
4	Классификация каналов проникновения в систему и технических каналов утечки информации. Модель нарушителя.		7-8	2	4		8	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос
5	Основные меры противодействия угрозам безопасности (методы защиты информации) и их классификация. Основные механизмы защиты информации. Построение систем защиты от угроз нарушения конфиденциальности		9-10	2	4		8	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос

	информации. Модель системы защиты. Идентификация и аутентификация. Особенности парольных систем аутентификации. Протоколирование и аудит. Методы разграничения доступа. Понятие модели управления доступом.Типы моделей управления доступом. Системы обнаружения вторжений.								
6	Криптографические методы обеспечения конфиденциальности информации. Симметричные и ассиметричные криптосистемы. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов.		11-12	2	4		8	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос
7	Построение систем защиты от угроз нарушения целостности.		13-14	2	4		8	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос
8	Схема системы защиты от угроз нарушения доступности.		15-16	2	4		8	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос

9	Организационные меры защиты информации в автоматизированных системах.		17-18	2	4		26	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос, контрольная работа
	Итого:			18	36		90		
	Форма промежуточной аттестации	Зачет с оценкой							

3.2.Для заочной формы обучения:

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа; в том числе на контактную работу обучающихся с преподавателем (далее - аудиторная работа по видам) 12часов (лекционные занятия - 4 часа, лабораторные работы – 8 часов), на внеаудиторную самостоятельную работу обучающегося (далее внеаудиторная СРС) -128 часов, контроль – 4 часа. По итогам изучения дисциплины – зачет с оценкой.

№ п/п	Содержание дисциплины, структурированное по темам (разделам)	Курс	Аудиторная работа по видам			Внеаудиторная СРС	Образовательные технологии	Формы текущего контроля успеваемости
			Лек.	Лаб.	Пр.			
1	Основные термины и определения в области информационной безопасности. Понятие государственной тайны и иных охраняемых законом тайн, сведений конфиденциального характера. Базовые свойства защищаемой информации и систем ее обработки. Свойства информации как предмета защиты. Способы нанесения ущерба субъектам информационных отношений. Определение требований к защищаемой	5	1	2		26	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос

	информации. Особенности автоматизированной системы обработки информации как объекта защиты.Понятие угрозы безопасности информации, коррелирующие с этим понятием термины. Основные виды угроз безопасности субъектов информационных отношений. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация каналов проникновения в систему и технических каналов утечки информации. Модель нарушителя.							
2	Основные меры противодействия угрозам безопасности (методы защиты информации) и их классификация. Основные механизмы защиты информации. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Идентификация и		1	2		25	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос

	аутентификация. Особенности парольных систем аутентификации. Протоколирование и аудит. Методы разграничения доступа. Понятие модели управления доступом.Типы моделей управления доступом. Системы обнаружения вторжений.							
3	Криптографические методы обеспечения конфиденциальности информации. Симметричные и ассиметричные криптосистемы. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов.		1	2		25	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос
4	Построение систем защиты от угроз нарушения целостности. Схема системы защиты от угроз нарушения доступности. Организационные меры защиты информации в автоматизированных системах.		1	2		52	Информационная лекция, лабораторная работа с применением IT-технологий	Собеседование и отчет по лабораторной работе, устный опрос, контрольная работа
	Итого:		4	8		128		
	Форма промежуточной аттестации	Зачет с оценкой						

4. Программа и учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

4.1.Для очной формы обучения:

№ п/п	Содержание дисциплины, структурированное по темам (разделам), осваиваемое обучающимся в ходе самостоятельной работы	Семестр	Неделя	Виды СРС и учебно-методическое обеспечение самостоятельной работы		
				Учебные задания для самостоятельной работы		Учебно-методическое обеспечение СРС
				Аудиторная СРС	Внеаудиторная СРС	
1	Основные термины и определения в области информационной безопасности. Понятие государственной тайны и иных охраняемых законом тайн, сведений конфиденциального характера.	7	1-2	Лабораторная работа №1 «Расчет вероятности проникновения злоумышленника на объект хранения информации»	Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	1-2, 4-13
2	Базовые свойства защищаемой информации и систем ее обработки. Свойства информации как предмета защиты. Способы нанесения ущерба субъектам информационных отношений. Определение требований к защищаемой информации. Особенности автоматизированной системы обработки информации как объекта защиты.		3-4	Лабораторная работа №2 «Преобразование аналоговых телефонных сообщений (скремблеры)»	Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	1-2, 4-13
3	Понятие угрозы безопасности информации, коррелирующие с этим понятием термины. Основные виды угроз безопасности субъектов		5-6	Лабораторная работа №3 «Модели дискреционного управления доступом	Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	1-2, 4-13

	информационных отношений. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.			Харрисона-Руззо-Ульмана»		
4	Классификация каналов проникновения в систему и технических каналов утечки информации. Модель нарушителя.		7-8	Лабораторная работа №4 «Модель доступа Белла-ЛаПадула»	Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	1-2, 4-13
5	Основные меры противодействия угрозам безопасности (методы защиты информации) и их классификация. Основные механизмы защиты информации. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Идентификация и аутентификация. Особенности парольных систем аутентификации. Протоколирование и аудит. Методы разграничения доступа. Понятие модели управления доступом. Типы моделей управления доступом. Системы обнаружения вторжений.		9-10	Лабораторная работа №5 «Шифры перестановки»	Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	1-13
6	Криптографические методы обеспечения		11-12	Лабораторная работа №6	Подготовка к лабораторной	1-13

	конфиденциальности информации. Симметричные и ассиметричные криптосистемы. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов.			«Шифры простой замены»	работе, опросу, собеседованию и отчету по работе	
7	Построение систем защиты от угроз нарушения целостности.		13-14	Лабораторная работа №7 «Шифры сложной замены»	Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	1-13
8	Схема системы защиты от угроз нарушения доступности.		15-16	Лабораторная работа №8 «Шифрование методом гаммирования»	Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	1-13
9	Организационные меры защиты информации в автоматизированных системах.		17-18	Лабораторная работа №9 «Одноразовая система шифрования», контрольная работа	Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе. Подготовка к контрольной работе	1-13

4.2.Для заочной формы обучения:

№ п/п	Содержание дисциплины, структурированное по темам (разделам), осваиваемое обучающимся в ходе самостоятельной работы	Курс	Виды СРС и учебно-методическое обеспечение самостоятельной работы		
			Учебные задания для самостоятельной работы		Учебно-методическое обеспечение СРС
			Аудиторная СРС	Внеаудиторная СРС	
1	Основные термины и определения в области информационной	5	Лабораторная работа №1 «Расчет	Работа №2 «Преобразование аналоговых	1-2, 4-13

	безопасности. Понятие государственной тайны и иных охраняемых законом тайн, сведений конфиденциального характера. Базовые свойства защищаемой информации и систем ее обработки. Свойства информации как предмета защиты. Способы нанесения ущерба субъектам информационных отношений. Определение требований к защищаемой информации. Особенности автоматизированной системы обработки информации как объекта защиты. Понятие угрозы безопасности информации, коррелирующие с этим понятием термины. Основные виды угроз безопасности субъектов информационных отношений. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация каналов проникновения в систему и технических каналов утечки информации. Модель нарушителя.		вероятности проникновения злоумышленника на объект хранения информации», устный опрос, решение задач	телефонных сообщений (скремблеры)». Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	
2	Основные меры противодействия угрозам безопасности (методы защиты		Лабораторная работа №3 «Модели дискреционн	Лабораторная работа №4 «Модель доступа Белла-	1-2, 4-13

	информации) и их классификация. Основные механизмы защиты информации. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Идентификация и аутентификация. Особенности парольных систем аутентификации. Протоколирование и аудит. Методы разграничения доступа. Понятие модели управления доступом. Типы моделей управления доступом. Системы обнаружения вторжений.		ого управления доступом Харрисона-Руззо-Ульмана»	ЛаПадула». Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	
3	Криптографические методы обеспечения конфиденциальности информации. Симметричные и ассиметричные криптосистемы. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов.		Лабораторная работа №5 «Шифры перестановки»	Лабораторная работа №6-7 «Шифры простой замены. Шифры сложной замены». Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	1-13
4	Построение систем защиты от угроз нарушения целостности. Схема системы защиты от угроз нарушения доступности. Организационные меры защиты информации в автоматизированных		Лабораторная работа №8 «Шифрование методом гаммирования», контрольная работа	Лабораторная работа №9 «Одноразовая система шифрования». Подготовка к лабораторной работе, опросу, собеседовани	1-13

	системах.			ю и отчету по работе. Подготовка к контрольной работе	

5. Рекомендации по реализации дисциплины для обучающихся с ограниченными возможностями здоровья

5.1. Наличие соответствующих условий реализации дисциплины

Для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья на основании письменного заявления дисциплина реализуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья (далее - индивидуальных особенностей); обеспечивается соблюдение следующих общих требований: использование специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего такому обучающемуся необходимую техническую помощь, обеспечение доступа в здания и помещения, где проходит учебный процесс, другие условия, без которых невозможно или затруднено обучение по дисциплине.

5.2. Обеспечение соблюдения общих требований.

При реализации дисциплины на основании письменного заявления обучающегосяобеспечивается соблюдение следующих общих требований: проведение занятий для студентов-инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся; присутствие в аудитории ассистента (ассистентов), оказывающего(их) обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей на основании письменного заявления; пользование необходимыми обучающимся техническими средствами с учетом их индивидуальных особенностей.

5.3. Доведение до сведения обучающихся с ограниченными возможностями здоровья в доступной для них форме.

Все локальные нормативные акты АГТУ по вопросам реализации дисциплины (модуля) по данной доводятся до сведения обучающихся с ограниченными возможностями здоровья в доступной для них форме.

5.4. Реализация увеличения продолжительности прохождения промежуточной аттестации по отношению к установленной продолжительности для обучающегося с ограниченными возможностями здоровья.

Продолжительность прохождения промежуточной аттестации по отношению к установленной продолжительности увеличивается по письменному заявлению обучающегося с ограниченными возможностями здоровья; продолжительность экзамена и (или) зачета, проводимого в письменной форме увеличивается не менее чем на 0,5 часа; продолжительность подготовки обучающегося к ответу на экзамене и (или) зачете, проводимом в устной форме, – не менее чем на 0,5 часа; продолжительность ответа обучающегося при устном ответе увеличивается не более чем на 0,5 часа.

6. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств представлен в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие. - Москва, Берлин:Директ-Медиа, 2015, 253 с.: [Электронный ресурс].- URL:http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1

2. Аверченков А.И. Аудит информационной безопасности: учебное пособие для вузов -Москва:Флинта, 2016, 269 с.: [Электронный ресурс].- URL:http://biblioclub.ru/index.php?page=book_red&id=93245&sr=1

б) дополнительная литература:

3. Лапонина О.Р. Криптографические основы безопасности. - Москва:Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. - ISBN:5-9556-00020; [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book_red&id=429092&sr=1

4. Анализ состояния защиты данных в информационных системах: учебно-методическое пособие / сост. В.В. Денисов. - Новосибирск: НГТУ, 2012. - 52 с.: ил.,табл., схем. – ISBN 978-5-7782-1969-4; [Электронный ресурс]. – URL:http://biblioclub.ru/index.php?page=book_red&id=228844&sr=1

5. Журнал Вопросы кибербезопасности. [Электронный ресурс]. - URL:http://cyberrus.com/

в) ресурсы информационно-телекоммуникационной сети «Интернет»:

6. Образовательный портал ФГБОУ ВО «АГТУ» Moodle, portal.astu.org
7. ЭБС «Университетская библиотека on-line» http://www.biblioclub.ru.
8. ЭБС издательства «Лань» (коллекция «Инженерные науки») https://e.lanbook.com
9. ЭБС Юрайтhttps://www.biblio-online.ru.
10. ЭБС elibrary (периодические издания) http://elibrary.ru (елайбрери.ру) ООО "РУНЭБ" (г. Москва).
11. ЭБС Национальный цифровой ресурс «Руконт» (коллекция изданий Астраханского государственного технического университета).

г) методические указания для обучающихся по освоению дисциплины:

12. Методические указания для самостоятельной работы студентов по дисциплине «Защита информации» / Сост.: Н.В.Давидюк. – АГТУ,2018. -[Электронный ресурс].- Режим доступа: www. portal.astu.org.

13. Методические указания для выполнениялабораторных работпо дисциплине «Защита информации» / Сост.: Н.В. Давидюк, С.В.Белов – АГТУ,2018. - [Электронный ресурс].- Режим доступа: www. portal.astu.org.

д) перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем:

Перечень информационных технологий:

№	Наименование программного обеспечения	Назначение
1.	ЭБС издательства Лань (книги коллекции «Инженерные науки»)	Обеспечивает доступ к электронно-библиотечным системам издательств, например, ЭБС издательства «Лань»; доступ к электронному каталогу книг, трудам преподавателей, учебно-методическим разработкам АГТУ, периодическим изданиям. Позволяет принимать участие в виртуальных выставках.

2.	Образовательный портал Moodle	Образовательный портал ФГБОУ ВО «АГТУ»
3.	ЭБС «Университетская библиотека on-line»	Полнотекстовая база данных ScienceDirect; Реферативная и наукометрическая база данных Scopus; База данных российских стандартов «Технорма»; Межрегиональная аналитическая роспись статей (МАРС); Национальный цифровой ресурс «Руконт».
4.	ЭБС Юрайт	В электронной библиотеке представлены все книги издательства Юрайт. Первые 10% текста (но не более 50 страниц) каждого издания доступны для ознакомления всем пользователям сети Интернет.
5.	ЭБСeLibrary (периодические издания)	Научная электронная библиотека eLibrary – это крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 22 млн научных статей и публикаций, в том числе электронные версии более 4800 российских научно-технических журналов, из которых более 3800 журналов в открытом доступе.

Перечень лицензионногопрограммного обеспечения:

№	**Наименование программного обеспечения**	**Назначение**
1.	7-zip	Архиватор
2.	Foxit Reader	Программа для просмотра электронных документов.
3.	Google Chrome, Mozilla FireFox, Opera	Браузер
4.	MicrosoftOffice 2016	Офисный пакет приложений для работы с различными типами документов: текстами, электронными таблицами, базами данных и др.
5.	Visualstudio 2008/2010/2012/2015	Среда разработки для программирования
6.	LibreOffice	Свободный пакет офисных приложений для работы с электронными документами
7.	OpenOffice	Программное обеспечение для работы с электронными документами
8.	AdobeReader	Программа для просмотра электронных документов.
9.	MicrosoftOpenLicenseAcademic	Операционные системы.
10.	SQL Server 2008 R2 Standard on Windows Server 2008 R2 SP1 Standard (x64)	Система управления реляционными базами данных (РСУБД), разработанная корпорацией Microsoft.
11.	KasperskyEdpoinSecurity 10	Средство антивирусной защиты

Перечень информационно-справочных систем:

№	Наименование программного обеспечения	Назначение
1	Гарант	Предоставляет доступ к федеральному и региональному законодательству, комментариям и разъяснениям из ведущих профессиональных СМИ, книгам и обновляемым энциклопедиям, типовым формам документов, судебной практике, международным договорам и другой нормативной информации. Всего в нее включено более 2,5 млн документов. В программе представлены документы более 13 000 федеральных, региональных и местных эмитентов
2	Консультант+	Содержит российское и региональное законодательство, судебная практика, финансовые и кадровые консультации, консультации для бюджетных организаций, комментарии законодательства, формы документов, проекты нормативных правовых актов, международные правовые акты, правовые акты по здравоохранению, технические нормы и правила.
3	Правовая система ИПС "Кодекс"	Содержит российское и региональное законодательство, судебную практику, комментарии, консультации, справочные материалы, юридическую и бухгалтерскую прессу, образцы и формы документов и др.

8. Материально-техническое обеспечение дисциплины

Аудитория для занятий лекционного вида – аудитория, оснащенная набором демонстрационного оборудования (экран, компьютер, проектор) и оборудованная специализированной учебной мебелью (столы, стулья для обучающихся, стол, стул для преподавателя, доска).

Аудитория для проведения семинарских занятий и лабораторных работ - компьютерный класс, оснащенный компьютерами с выходом в сеть Интернет и оборудованный специализированной учебной мебелью (компьютерные столы и стулья для обучающихся, стол и стул для преподавателя, доска); проведение семинарских занятий возможно в аудитории, оборудованной специализированной учебной мебелью (столы, стулья для обучающихся, стол, стул для преподавателя, доска).

Аудитория для текущего контроля успеваемости и промежуточной аттестации – компьютерный класс, оснащенный компьютерами с выходом в сеть Интернет и оборудованный специализированной учебной мебелью (компьютерные столы и стулья для обучающихся, стол и стул для преподавателя, доска); проведение семинарских занятий возможно в аудитории, оборудованной специализированной учебной мебелью (столы, стулья для обучающихся, стол, стул для преподавателя, доска).

Аудитория для групповых и индивидуальных консультаций – компьютерный класс, оснащенный компьютерами с выходом в сеть Интернет и оборудованный специализированной учебной мебелью (компьютерные столы и стулья для обучающихся, стол и стул для преподавателя, доска).

Аудитория для самостоятельной работы студентов – аудитория, оснащенная компьютерами с выходом в сеть Интернет, обеспечивающими доступ к электронно-

библиотечным системам издательств, электронному каталогу книг, трудам преподавателей, учебно-методическим разработкам АГТУ, периодическим изданиям, Образовательному порталу ФГБОУ ВО «АГТУ».

Реализация программы бакалавриата поддерживается наличием в организации библиотеки, в том числе электронной, обеспечивающей обучающимся доступ к профессиональным базам данных, информационным справочным и поисковым системам, а также иным информационным ресурсам:

- залы научной библиотеки ФГБОУ ВО «АГТУ» - 4 корп., 2 корп., гл. корп. (читальный зал научной литературы и электронный читальный зал), 6 корп., 8 корп. Залы обеспечены компьютерами с доступом к сети Интернет, электронно-библиотечным системам и к электронной информационно-образовательной среде Университета.

Библиотечный фонд укомплектован изданиями учебной, учебно-методической, научной и иной литературы, включая периодические издания, соответствующими рабочим программам дисциплин и практик (издания представлены в электронно-библиотечной системе организации с обеспечением каждому обучающемуся индивидуального неограниченного доступа к указанной системе посредством сети «Интернет»).

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль подготовки «Автоматизированные системы обработки информации и управления».

ПРИЛОЖЕНИЕ
к рабочей программе дисциплины
«Защита информации»
Рассмотрено на Учебно-методическом совете,
протокол № _7_ от «_18_»_июня__2018 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1. Перечень компетенций, формируемых в ходе освоения данной дисциплины с указанием этапов их формирования в процессе освоения образовательной

Перечень компетенций, формируемых в ходе освоения данной дисциплины с указанием этапов их формирования в процессе освоения образовательной программы-*ОК-4, ОПК-5*. Этапы формирования данных компетенций в процессе освоения ОП представлены в Паспорте компетенций.

2. Показатели и критерии оценивания компетенций, формируемых в ходе освоения данной дисциплины, описание шкал оценивания

<u>ОК-4</u>

Шкала оценивания уровня сформированности результата обучения (зачет с оценкой)	**Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы**			
	«Знать»	**«Уметь»**	**«Владеть навыками и/или иметь опыт»**	**«Компетенция»**
	Показатели			
	основные нормативно-правовые акты в области информационной безопасности	применять на практике нормативные и правовые документы, регламентирующие деятельность в сфере информационной безопасности, классифицировать защищаемую информацию по видам тайн в соответствии с законодательством РФ и определять меры по ее защите	использования положений нормативно-правовых актов для обеспечения защиты информации ограниченного доступа	способность использовать основы правовых знаний в различных сферах деятельности (ОК-4)
	Критерии			
Продвинутый уровень («отлично») 100-85 % (или баллов)	четко и правильно дает определения, полно раскрывает содержание понятий, верно использует терминологию, при этом ответ самостоятельный, использованы ранее приобретенные знания	выполняет все задания, последовательность их выполнения достаточно хорошо продумана, действие в целом осознанно	владеет всеми необходимыми навыками и/или имеет опыт	обучающийся способен проявить (реализовать) компетенцию в типовых ситуациях и в ситуациях повышенной сложности, а также в нестандартных и непредвиденных ситуациях, создавая при этом новые правила и пути применения нормативно-правовых актов
Углубленный	определения понятий дает	выполняет все задания,	в целом владеет	обучающийся способен проявить

уровень («хорошо») 84-71 % (или баллов)	неполные, допускает незначительные нарушения в последовательности изложения, небольшие неточности при использовании научных категорий, формулировки выводов	последовательность их выполнения соответствует требованиям, но действие выполняется недостаточно осознанно	необходимыми навыками и/или имеет опыт	(реализовать) компетенцию в типовых ситуациях и в ситуациях повышенной сложности
Базовый уровень («удовлетворительно») 70-60 % (или баллов)	усвоено основное содержание, но излагается фрагментарно, не всегда последовательно, определения понятий недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в использовании предметной терминологии	выполняет не все задания, допускает ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	владеет не всеми необходимыми навыками, имеющийся опыт фрагментарен	обучающийся способен проявить (реализовать) данную компетенцию в типовых ситуациях
Нулевой уровень («неудовлетворительно») менее 60% (или баллов)	основное содержание не раскрыто, не дает ответы на вспомогательные вопросы, допускает грубые ошибки в использовании терминологии	выполняет лишь отдельные задания, последовательность их хаотична, действие в целом неосознанно	не владеет всеми необходимыми навыками и/или не имеет опыт	обучающийся не способен проявлять (реализовать) данную компетенцию

ОПК-5

Шкала оценивания уровня сформированности результата	**Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы**			
	«Знать»	**«Уметь»**	**«Владеть навыками и/или иметь опыт»**	**«Компетенция»**
	Показатели			
	основы государственной информационной политики, стратегию развития	пользоваться законодательными и нормативными документами в профессиональной деятельности;	анализа организаций и защищенности их информационных ресурсов	способность решать стандартные задачи профессиональной деятельности на основе

обучения (зачет с оценкой)	информационного общества в России; понятие государственной тайны и иных охраняемых законом тайн, сведений, составляющих государственную тайну, и сведений конфиденциального характера; организационно-правовые основы режима секретности; цели и задачи обеспечения информационной безопасности; основные термины по проблематике информационной безопасности; методы обеспечения защиты информации; классификацию угроз; классификацию каналов утечки информации; модель потенциального злоумышленника	пользоваться современными источниками информации по исследуемым проблемам и задачам; осуществлять сбор, обработку, анализ и систематизацию информации по обеспечению информационной безопасности; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; пользоваться нормативно-правовой, организационно-распорядительной и методической документацией по вопросам обеспечения информационной безопасности; составлять перечень конфиденциальных информационных ресурсов; определять состав угроз безопасности информации и возможные каналы утечки информации; составить представление о потенциальном злоумышленнике	с точки зрения информационной безопасности, состава комплекса мер для обеспечения защиты информации	информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-5)
	Критерии			
Продвинутый уровень («отлично») 100-85 % (или баллов)	четко и правильно дает определения, полно раскрывает содержание понятий, верно использует терминологию, при этом ответ самостоятельный, использованы ранее приобретенные знания	выполняет все задания, последовательность их выполнения достаточно хорошо продумана, действие в целом осознанно	владеет всеми необходимыми навыками и/или имеет опыт	обучающийся способен проявить (реализовать) компетенцию в типовых ситуациях и в ситуациях повышенной сложности, а также в нестандартных и непредвиденных ситуациях, создавая при этом новые правила и пути применения нормативно-правовых актов
Углубленный	определения понятий дает	выполняет все задания,	в целом владеет	обучающийся способен проявить

уровень («хорошо») 84-71 % (или баллов)	неполные, допускает незначительные нарушения в последовательности изложения, небольшие неточности при использовании научных категорий, формулировки выводов	последовательность их выполнения соответствует требованиям, но действие выполняется недостаточно осознанно	необходимыми навыками и/или имеет опыт	(реализовать) компетенцию в типовых ситуациях и в ситуациях повышенной сложности
Базовый уровень («удовлетворительно») 70-60 % (или баллов)	усвоено основное содержание, но излагается фрагментарно, не всегда последовательно, определения понятий недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в использовании предметной терминологии	выполняет не все задания, допускает ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	владеет не всеми необходимыми навыками, имеющийся опыт фрагментарен	обучающийся способен проявить (реализовать) данную компетенцию в типовых ситуациях
Нулевой уровень («неудовлетворительно») менее 60% (или баллов)	основное содержание не раскрыто, не дает ответы на вспомогательные вопросы, допускает грубые ошибки в использовании терминологии	выполняет лишь отдельные задания, последовательность их хаотична, действие в целом неосознанно	не владеет всеми необходимыми навыками и/или не имеет опыт	обучающийся не способен проявлять (реализовать) данную компетенцию

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1. Типовые контрольные задания для оценки уровня сформированности каждого результата обучения по дисциплине, в том числе уровня освоения компетенции

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы			
Знать	**Уметь**	**Владеть навыками и (или) иметь опыт**	**Компетенция**
основные нормативно-правовые акты в	применять на практике	использования положений	способность использовать основы

области информационной безопасности	нормативные и правовые документы, регламентирующие деятельность в сфере информационной безопасности, классифицировать защищаемую информацию по видам тайн в соответствии с законодательством РФ и определять меры по ее защите	нормативно-правовых актов для обеспечения защиты информации ограниченного доступа	правовых знаний в различных сферах деятельности (ОК-4)
основы государственной информационной политики, стратегию развития информационного общества в России; понятие государственной тайны и иных охраняемых законом тайн, сведений, составляющих государственную тайну, и сведений конфиденциального характера; организационно-правовые основы режима секретности; цели и задачи обеспечения информационной безопасности; основные термины по проблематике информационной безопасности; методы обеспечения защиты информации; классификацию угроз; классификацию каналов утечки информации; модель потенциального злоумышленника	пользоваться законодательными и нормативными документами в профессиональной деятельности; пользоваться современными источниками информации по исследуемым проблемам и задачам; осуществлять сбор, обработку, анализ и систематизацию информации по обеспечению информационной безопасности; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; пользоваться нормативно-правовой, организационно-распорядительной и методической документацией по вопросам обеспечения информационной безопасности; составлять перечень конфиденциальных информационных ресурсов; определять состав угроз безопасности информации и возможные каналы утечки информации; составить представление о потенциальном злоумышленнике	анализа организаций и защищенности их информационных ресурсов с точки зрения информационной безопасности, состава комплекса мер для обеспечения защиты информации	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и сучетом основных требований информационной безопасности (ОПК-5)

Процедура оценивания			
Опрос	Контрольная работа	Собеседование и отчет по лабораторной работе	Зачет с оценкой
Типовые контрольные задания			
Повторить материал лекционных занятий (п.3 РП), при необходимости обращаясь к указанным источникам, и ответить на вопрос преподавателя по тематике лекции.Примерный список вопросов представлен в п.3.2 Приложения к РП	Подготовиться к контрольной работе. Примеры типовых заданий представлены в Приложении к РП вп.3.2	Выполнить лабораторную работу, подготовиться к собеседованию и отчету по работе, оформить отчет в соответствии с типовой структурой: 1. Тема лабораторной работы 2. Цель и задачи работы 3. Ход и пошаговое описание выполнения заданий работы 7. Вывод по работе. Тематика лабораторных работ представлена в п.3.2 Приложения к РП.	Подготовиться к зачету. Зачетные вопросы представлены в п.3.2 Приложения к РП.

3.2. Типовые контрольные задания для проведения промежуточной аттестации (зачет с оценкой*)*

Содержание лабораторных работ:
Задание:
Изучить теоретический материал.
Реализовать изученный метод или решить поставленную задачу (согласно теме работы).
Оформить отчет по результатам выполнения работы.
Оформленные отчеты представлять по стандартному плану:
1. Тема лабораторной работы
2. Цель и задачи работы
3. Ход и пошаговое описание выполнения заданий работы
7. Вывод по работе.

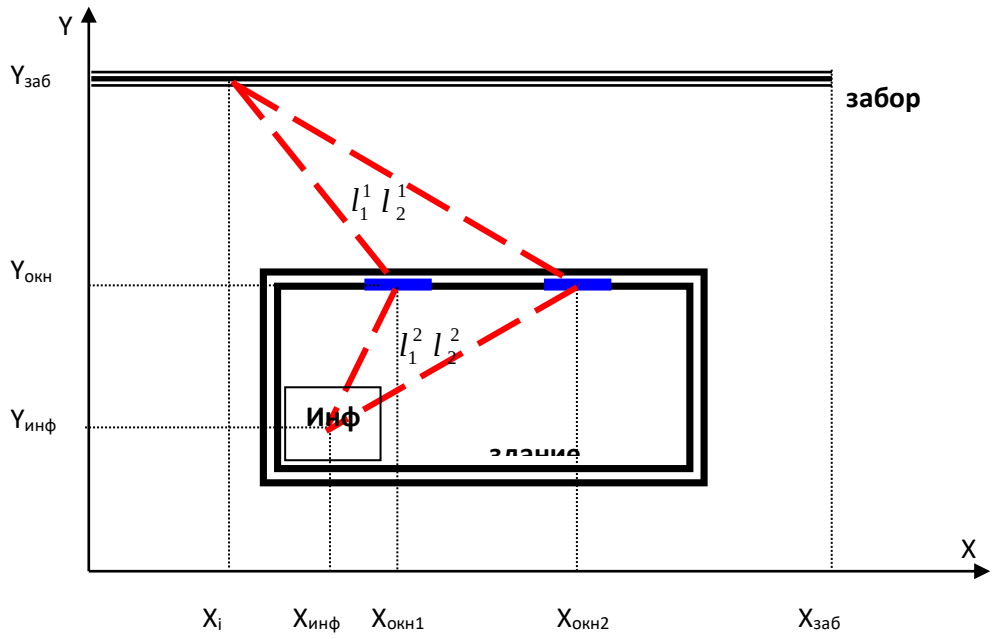
Темы лабораторных работ:

Лабораторная работа №1 «Расчет вероятности проникновения злоумышленника на объект хранения информации»
Лабораторная работа №2 «Преобразование аналоговых телефонных сообщений (скремблеры)»
Лабораторная работа №3 «Модели дискреционного управления доступом Харрисона-Руззо-Ульмана»
Лабораторная работа №4 «Модель доступа Белла-ЛаПадула»
Лабораторная работа №5 «Шифры перестановки»
Лабораторная работа №6 «Шифры простой замены»
Лабораторная работа №7 «Шифры сложной замены»
Лабораторная работа №8 «Шифрование методом гаммирования»
Лабораторная работа №9 «Одноразовая система шифрования»

Типовые вопросы для подготовки к опросу:
1. Что такое система физической защиты объекта?
2. Какие требования предъявляются к комплексной системе безопасности объекта?
3. Аналоговый, дискретный сигнал.
4. Спектр. Спектр аналогового и дискретного сигнала.
5. Скремблер. Принцип действия скремблера.
6. Условие для выбора n (число мелких интервалов в пределах T).
7. Виды скремблирования. Достоинства и недостатки.
8. Полосовой фильтр. Как он используется при скремблировании, в каком из видов скремблирования.
9. Инверсия частотного спектра сообщения. Для чего применяется?
10. Какие модели доступа Вам известны? Раскройте их сущность.
11. К каким криптосистемам относится данный шифр?
12. Алгоритм шифрования по данному методу.
13. Достоинства и недостатки указанного шифра.
14. Криптостойкость указанного шифра.

Примеры типовых заданий контрольной работы:
В качестве теоретического вопроса – вопросы из списка вопросов к зачету.
Типовые задачи:

1. Дан объект хранения информации, состоящий из заграждения и здания с двумя окнами. Необходимо определить траекторию, по которой вероятность проникновения злоумышленника на объект будет минимальной.



Исходные данные:
План расположения объекта:
Yзаб= 50,
Xзаб= 50,
Yок = 30,
Xокн1 = 20,
Xокн2 = 30,
Yин = 15,
Xин = 25,
Xi= 45
Вероятность проникновения через окна:
Рок1 = 0,2,
Рок2 = 0,4
3. Коэффициенты защищенности:
k1 = 1,
k2 = 0,5

2. Методом вертикальной перестановки зашифруйте словосочетание КОНТРОЛЬНАЯ_РАБОТА. Ключ: 531462.

3. С помощью магического квадрата 4x4 зашифруйте словосочетание ЗАЩИТАИНФОРМАЦИИ-НАША_ДИСЦИПЛИНА.

4. Методом двойной перестановки зашифруйте словосочетание ЖИЗНЬ_ПРЕКРАСНА!. Ключи (столбцы, строки): 3142, 1432.

5. К заданной шифрограмме слова ПЕРЕСТАНОВКА подберите все возможные ключи и объясните полученный результат. ЕАВПРОТАЕНКС.

6. Самостоятельно составьте шифрующую таблицу Трисемуса (размерность 8x4; й=и, ё=е, +_; ключевое слово: ОТЛИЧНО) и зашифруйте с ее помощью слово КОНФИДЕНЦИАЛЬНОСТЬ.

7. Методом аффинной подстановки Цезаря зашифруйте слово ИМПЕРАТОР. При этом учтите следующее: m=32 (й=и, ё=е, +_), константыA и B выбрать самостоятельно согласно существующим требованиям.

8. Методом аффинной подстановки Цезаря зашифруйте слово ПОДСТАНОВКА. При этом учтите следующее: m=32 (й=и, ё=е, +_), константыA и B выбрать самостоятельно согласно существующим требованиям.

9. Зашифруйте слово КРИПТОГРАФИЯ, используя для генерации гаммы шифра линейный конгруэнтный генератор. При этом считайте b=7, a=5, Y0=2, m=4 (почему выбраны такие константы?) или выберите константы самостоятельно, длина алфавита – 31 (и=й, е=ё).

Список вопросов к зачету:

1. Основные термины и определения: информация, информационные отношения, субъекты информационных отношений, автоматизированная система обработки информации, информационная безопасность автоматизированной системы.
2. Базовые свойства защищаемой информации и систем ее обработки. Свойства информации как предмета защиты. Способы нанесения ущерба субъектам информационных отношений.
3. Определение требований к защищаемой информации. Информационные пакеты.
4. Особенности автоматизированной системы (АС) как объекта защиты. Уязвимость основных структурно-функциональных элементов распределенных АС. Понятие угрозы безопасности. Основные виды угроз безопасности субъектов информационных отношений.
5. Классификация угроз безопасности информации, автоматизированных систем и субъектов информационных отношений по различным признакам. Методы перечисления угроз.
6. Основные искусственные угрозы информационной безопасности: преднамеренные и случайные.
7. Классификация каналов проникновения в систему и утечки информации.
8. Неформальная модель нарушителя в автоматизированных системах обработки информации.
9. Основные меры противодействия угрозам безопасности (методы защиты информации) и их классификация.
10. Взаимосвязь различных методов обеспечения информационной безопасности, их достоинства и недостатки. Задачи системы информационной безопасности.
11. Основные принципы обеспечения безопасности автоматизированных систем обработки информации.
12. Основные механизмы защиты автоматизированных систем. Термины и определения, касающиеся данного вопроса.
13. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Идентификация и аутентификация.
14. Особенности парольных систем аутентификации.
15. Рекомендации по практической реализации парольных систем аутентификации.
16. Оценка стойкости парольных систем аутентификации. Методы хранения паролей. Передача паролей по сети.
17. Два основных метода разграничения доступа. Понятие модели управления доступом.
18. Типы моделей управления доступом.
19. Криптографические методы обеспечения конфиденциальности информации. Симметричные и ассиметричные криптосистемы. Примеры.

20. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов.
21. Шифры перестановки: маршрутной перестановки, «Сцитала», «Поворотная решетка».
22. Шифры перестановки: вертикальной перестановки, применение магических квадратов, перестановка бит. Криптостойкость шифров перестановки.
23. Шифры замены. Определение. Шифры простой замены: система шифрования Цезаря, афинная система подстановок, лозунговый шифр.
24. Шифры простой замены: полибианский квадрат, шифрующая таблица Трисемуса, биграммный шифр Плейфера.
25. Шифры сложной замены: система омофонов, шифр Гронсфельда, система шифрования Вижинера, «двойной квадрат» Уитстона.
26. Шифрование методом гаммирования. Достоинства и недостатки метода. Методы генерации псевдослучайных последовательностей чисел. Система шифрования «Одноразовый блокнот».
27. Методы обеспечения сетевой безопасности. Системы обнаружения вторжений.
28. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Протоколирование и аудит.
29. Построение систем защиты от угроз нарушения целостности. Принципы обеспечения целостности (Кларка-Вилсона).
30. Криптографические методы обеспечения целостности информации. Цифровые подписи и порядок их использования.
31. Криптографические методы обеспечения целостности информации. Криптографические хэш-функции. Коды проверки подлинности.
32. Схема системы защиты от угроз нарушения доступности. Дублирование каналов передачи, шлюзов, межсетевых экранов. Методы резервного копирования информации.
33. Схема системы защиты от угроз нарушения доступности. Применение RAID-массивов. Дублирование и зеркалирование серверов. Использование кластеров, избыточной маршрутизации.
34. Механизмы защиты информации в операционных системах.
35. Организационные меры защиты информации в автоматизированных системах. Перечень основных нормативных и организационно-распорядительных документов, необходимых для организации комплексной системы безопасности информации.
36. Основные организационные и организационно-технические мероприятия по созданию и эксплуатации комплексной системы защиты: разовые, периодически проводимые, проводимые по необходимости, постоянные.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, формируемых в ходе освоения данной дисциплины

4.1. Формы контроля (процедуры оценивания)

Опрос - фронтальная форма контроля, представляющая собой ответы на вопросы преподавателя в устной форме
Собеседование и отчет по лабораторной работе - форма контроля, предусматривающая изложение и анализ знаниевых компонентов, методик исследования, этапов и результатов осуществления действий и операций по теме работе, представление и обоснование выводов по работе, факторный анализ результатов, формулирование предложений, ответы на вопросы преподавателя по теме работы. Отчет по лабораторной работе осуществляется ведущему преподавателю, предоставляется оформленная по установленному плану работа
Контрольная работа - письменная работа студента, направленная на решение задач или заданий, требующих поиска обоснованного ответа.

4.2. Шкалы оценивания

Шкала оценки устного ответа (опрос)

Уровень /оценка	Описание
Продвинутый уровень («отлично»)	правильно, всесторонне в полном объеме излагает знания: дает определения, раскрывает содержание понятий, верно использует терминологию; знает организацию и методику реализации профессиональной деятельности; демонстрирует всестороннее и полное понимание смысла изученного материала
Углубленный уровень («хорошо»)	правильно, в полном объеме излагает знания: дает определения, раскрывает содержание понятий, верно использует терминологию; знает организацию и методику реализации профессиональной деятельности; демонстрирует понимание смысла изученного материала; допускает малозначительные ошибки
Базовый уровень («удовлетворительно»)	правильно излагает базовые знания: дает определения, раскрывает содержание понятий, верно использует терминологию;демонстрирует понимание основного смысла изученного материала
Нулевой уровень («неудовлетворительно»)	содержание знаниевого компонента не раскрыто; допускает значительные ошибки в изложении теоретического основ, организации и методологии профессиональной деятельности; не дает ответы на вопросы, в том числе вспомогательные

Шкала оценки выполнения лабораторной работы (собеседования и отчета по лабораторной работе)

Уровень /оценка	Описание
Продвинутый уровень («отлично»)	понимает цель действия; *всесторонне* и в полном объеме использует информацию для *постановки* и выполнения задач; *планирует* и выполняет *последовательно* действия и операции; интерпретирует полученные результаты; грамотно формулирует выводы *и предложения*
Углубленный уровень («хорошо»)	понимает цель действия; использует полном объеме информацию для выполнения поставленных задач; выполняет действия и операции; интерпретирует полученные результаты; формулирует выводы; оформляет документацию; *допускает малозначительные ошибки*
Базовый уровень («удовлетворительно»)	понимает цель действия; использует *базовую* информацию для выполнения поставленных задач; выполняет *базовые* действия и операции; интерпретирует *основные* полученные результаты; формулирует *основные* выводы; допускает ошибки
Нулевой уровень («неудовлетворительно»)	не понимает цель действия; не выполняет действия и операции; не интерпретирует полученные результаты; не формулирует выводы; допускает *значительные ошибки*

Шкала оценки выполнения контрольной работы

Уровень /оценка	Описание
Продвинутый уровень («отлично»)	Демонстрирует полное понимание поставленных вопросов. Представленный ответ по вопросам контрольной работы отличается оригинальностью и логичностью изложения. Точно решены поставленные задачи.
Углубленный уровень («хорошо»)	Демонстрирует значительное понимание сути поставленных вопросов. Поставленные контрольные вопросы раскрыты в достаточном объеме, но присутствуют несущественные неточности. Поставленные задачи решены точно, либо с незначительными неточностями. Допускается незначительная ошибка в вычислениях при корректном алгоритме решения.
Базовый уровень («удовлетворительно»)	Демонстрирует частичное понимание сути поставленных вопросов. Поставленные контрольные вопросы в целом раскрыты, но присутствуют значительные неточности в формулировке требуемых определений. Поставленные задачи решены неточно, присутствуют ошибки в вычислениях при корректном алгоритме решения
Нулевой уровень («неудовлетворительно»)	Ответы на поставленные вопросы не получены. Задачи не решены.

Шкала оценки устного ответа на дифференцированном зачете по данной дисциплине

Уровень /оценка	Описание
Продвинутый уровень («отлично»)	Обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал дополнительной литературы, правильно обосновывает принятое решение
Углубленный уровень («хорошо»)	Обучающийся твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов, владеет необходимыми навыками выполнения, но затрудняется с ответом при видоизменении заданий, при обосновании принятого решения возникают незначительные затруднения в использовании изученного материала
Базовый уровень («удовлетворительно»)	Обучающийся имеет фрагментарные знания основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала
Нулевой уровень («неудовлетворительно»)	Ответы на поставленные вопросы не получены