МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ ТАТАРСТАН

Государственное бюджетное образовательное учреждение
высшего образования
«Альметьевский государственный нефтяной институт»

УТВЕРЖДАЮ
И.о. ректора АГНИ
_____ А.Ф.Иванов
(подпись) (ФИО)
«22» 06 2020 г.

Рабочая программа дисциплины Б1.В.ДВ.03.02
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки: 15.04.04 – «Автоматизация технологических процессов и производств»
Направленность (профиль) программы: Автоматизация технологических процессов и производств
Квалификация выпускника: магистр
Форма обучения: очная, очно-заочная
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

Статус	ФИО	Подпись	Дата
Автор	Ю.Б.Томус А.И.Каюмова		19.06.2020. 19.06.2020г.
Рецензент	И.П.Ситдикова		19.06.2020г.
И.о. заведующего обеспечивающей (выпускающей) кафедрой автоматизации и информационных технологий	Р.Р. Ахметзянов		19.06.2020г.

Альметьевск, 2020 г.

Содержание

Рабочая программа дисциплины «**Информационная безопасность**» разработана доцентом кафедры автоматизации и информационных технологий **Томус Ю.Б.** и старшим преподавателем кафедры автоматизации и информационных технологий **Каюмовой А.И.**

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Компетенции обучающегося формируемые в результате освоения дисциплины «Информационная безопасность»:

Оцениваемые компетенции (код, наименование)	**Результаты освоения компетенции**	**Оценочные средства текущего контроля и промежуточной аттестации**
ПК-1 способностью разрабатывать технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, управления, контроля, диагностики и испытаний, новые виды продукции, автоматизированные и автоматические технологии ее производства, средства и системы автоматизации, управления процессами, жизненным циклом продукции и ее качеством	**знать**: - технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний, методы расчета надежности автоматизированных систем; **уметь**: - анализировать технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний; **владеть:** - навыками работы в электронных библиотечных системах, справочных, справочно-поисковых и иных системах, связанных техническими средствами и системами автоматизации, диагностики и испытаний, оценки показателей надежности автоматизированных систем.	**Текущий контроль:** Компьютерное тестирование по темам 1-6 Практические задачи по темам 1-6 Лабораторные работы по темам 1-6 **Промежуточная аттестация:** Зачет с оценкой
ПК-3 способностью: составлять описание принципов действия и конструкции устройств, проектируемых технических средств и систем автоматизации, управления,	**знать**: - функциональные и числовые показатели надежности, программные комплексы обеспечения надежности;	**Текущий контроль:** Компьютерное тестирование по темам 1-6 Практические задачи по темам 1-6

контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, проектировать их архитектурно-программные комплексы	- методы анализа и диагностирования автоматизированных систем; **уметь:** - синтезировать и диагностировать системы с заданным уровнем надежности; - диагностировать показатели надежности систем; **владеть:** - навыками составлять описание принципов действия и конструкции устройств, проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, основами построения надежных автоматизированных систем управления.	Лабораторные работы по темам 1-6 **Промежуточная аттестация:** Зачет с оценкой

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Дисциплина «Информационная безопасность» является дисциплиной по выбору, входит в состав Блока 1 «Дисциплины (модули)» и относится к вариативной части ОПОП по направлению подготовки 15.04.04 – Автоматизация технологических процессов и производств, направленность (профиль) – Автоматизация технологических процессов и производств – Б1.В.ДВ.03.02

Дисциплина изучается на 2 курсе в 4 семестре[1]/на 3 курсе в 5 семестре[2].

3. Объем дисциплины в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

Контактная работа обучающихся с преподавателем:

лекции – 14 ч.[1]/6 ч.[2],

лабораторные работы – 28 ч.[1]/12 ч.[2],

практические занятия – 28ч.[1]/12 ч.[2],

КСР – 2 ч.[1]/2 ч.[2]

Самостоятельная работа – 72 ч.[1]/122 ч.[2]

[1] Очная форма обучения

[2] Очно-заочная форма обучения

Форма промежуточной аттестации дисциплины: зачет с оценкой в 4 семестре[1]/зачет с оценкой в 5 семестре[2].

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине

Тематический план дисциплины

Очная форма обучения

№	Тема дисциплины	Семестр	Виды и часы контактной работы, их трудоемкость (в ч.)				Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	КСР	
1.	Тема 1. Введение. Основные понятия.	4	2	6	4	1	10
2.	Тема 2. Проблемы информационной безопасности.	4	2	2	4		12
3.	Тема 3. Методы и средства обеспечения информационной безопасности.	4	4	6	4	1	15
4.	Тема 4. Протоколы защиты.	4	2	4	6		10
5.	Тема 5. Защита от вредоносных программ. Основные программно-технические меры.	4	2	6	6		15
6.	Тема 6. Стандарты и спецификации в области информационной безопасности.	4	2	4	4		10
	Итого по дисциплине		**14**	**28**	**28**	**2**	**72**

Очно-заочная форма обучения

№	Тема дисциплины	Семестр	Виды и часы контактной работы, их трудоемкость (в ч.)				Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	КСР	
1.	Тема 1. Введение. Основные понятия.	5	1	2	2	1	22
2.	Тема 2. Проблемы информационной безопасности.	5	1	2	2		18
3.	Тема 3. Методы и средства обеспечения информационной безопасности.	5	1	2	2	1	24

[1] Очная форма обучения
[2] Очно-заочная форма обучения

4.	Тема 4. Протоколы защиты.	5	1	2	2		18
5.	Тема 5. Защита от вредоносных программ. Основные программно-технические меры.	5	1	2	2		22
6.	Тема 6. Стандарты и спецификации в области информационной безопасности.	5	1	2	2		18
	Итого по дисциплине		**6**	**12**	**12**	**2**	**122**

4.2 Содержание дисциплины

Тема	Кол-во часов	Используемый метод	Формируемые компетенции
Дисциплинарный модуль 4.1			
Тема 1. Введение. Основные понятия. (12ч.)			
Лекция 1. Понятие информационной безопасности. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности.	2	-	ПК-1, ПК-3
Практическое занятие № 1. Разработка политики безопасности предприятия.	2	*Ситуационный анализ*	ПК-1, ПК-3
Практическое занятие № 2. Анализ и оценка рисков предприятия.	2	*Ситуационный анализ*	ПК-1, ПК-3
Практическое занятие № 3. Шифрование данных.	2	*Ситуационный анализ*	ПК-1, ПК-3
Лабораторная работа № 1. Виды информации и основные методы ее защиты.	2	*Работа в малых группах*	ПК-1, ПК-3
Лабораторная работа № 2. Виды угроз информационной безопасности Российской Федерации.	2	-	ПК-1, ПК-3
Тема 2. Проблемы информационной безопасности. (8ч.)			
Лекция 2. Наиболее распространенные угрозы. Основные определения и критерии классификации угроз. Наиболее распространенные угрозы доступности.	2	*Лекция-визуализация*	ПК-1, ПК-3
Практическое занятие № 4. Парольная защита. Количественная оценка стойкости парольной защиты.	2	*Ситуационный анализ*	ПК-1, ПК-3
Лабораторная работа № 3. Источники угроз информационной безопасности Российской Федерации.	2	*Ситуационный анализ*	ПК-1, ПК-3
Лабораторная работа № 4. Анализ информационной инфраструктуры государства.	2	*Работа в малых группах*	ПК-1, ПК-3
Тема 3. Методы и средства обеспечения информационной безопасности. (14ч.)			
Лекция 3,4. Информационная безопасность автоматизированных систем. Криптография. Аутентификация.	4	-	ПК-1, ПК-3
Практическое занятие № 5. Настройка параметров безопасности браузера Internet Explorer.	2	*Ситуационный анализ*	ПК-1, ПК-3
Практическое занятие № 6. Анализ рисков информационной безопасности.	2	*Ситуационный анализ*	ПК-1, ПК-3

Практическое занятие № 7. Пакеты антивирусных программ.	2	*Ситуационный анализ*	ПК-1, ПК-3
Лабораторная работа № 5. Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.	2	*Работа в малых группах*	ПК-1, ПК-3
Лабораторная работа № 6. Причины, виды, каналы утечки и искажения информации.	2	-	ПК-1, ПК-3
Дисциплинарный модуль 4.2			
Тема 4. Протоколы защиты. (12ч.)			
Лекция 5. Канальный, сеансовый, сетевой, прикладной протокол защиты.	2	*Лекция-визуализация* -	ПК-1, ПК-3
Практическое занятие № 8. Программная реализация криптографических алгоритмов.	2	*Ситуационный анализ*	ПК-1, ПК-3
Практическое занятие № 9. Механизмы контроля целостности данных.	2	-	ПК-1, ПК-3
Лабораторная работа № 7. Тестовые испытания программных средств защиты.	2	*Работа в малых группах*	ПК-1, ПК-3
Лабораторная работа № 8. Защита от утечек по каналу ПЭМИН, по акустическим и виброакустическим каналам.	2	-	ПК-1, ПК-3
Лабораторная работа № 9. Анализ сетевой топологии и установленных сервисов.	2	-	ПК-1, ПК-3
Тема 5. Защита от вредоносных программ. Основные программно-технические меры. (14ч.)			
Лекция 6. Антивирусы. Основные программно-технические меры. Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.	2	-	ПК-1, ПК-3
Практическое занятие № 10. Обеспечение информационной безопасности в ведущих зарубежных странах.	2	*Ситуационный анализ*	ПК-1, ПК-3
Практическое занятие № 11. Обнаружение уязвимостей по сигнатурам.	2	-	ПК-1, ПК-3
Практическое занятие № 12. Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор».	2	*Ситуационный анализ*	ПК-1, ПК-3
Лабораторная работа № 10. Сетевое сканирование.	2	-	ПК-1, ПК-3
Лабораторная работа № 11. Анализ трафика и сбор критичной информации программами пассивного анализа.	2	-	ПК-1, ПК-3
Лабораторная работа № 12. Оценка уязвимости коммутируемого доступа.	2	-	ПК-1, ПК-3
Тема 6. Стандарты и спецификации в области информационной безопасности. (10ч.)			

Лекция 7. Оценочные стандарты и технические спецификации. Основные понятия. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".	2	-	ПК-1, ПК-3
Практическое занятие № 13. Метод минимального риска.	2	*Ситуационный анализ*	ПК-1, ПК-3
Практическое занятие № 14. Тестирование программ.	2	*Ситуационный анализ*	ПК-1, ПК-3
Лабораторная работа № 13. Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф».	2	*Работа в малых группах*	ПК-1, ПК-3
Лабораторная работа № 14. Аудит комплексной защиты информации предприятия.	2	-	ПК-1, ПК-3

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа обучающихся выполняется по заданию преподавателя, без его непосредственного участия и направлена на самостоятельное изучение отдельных аспектов тем дисциплины.

Цель самостоятельной работы – подготовка современного компетентного специалиста и формирования способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Самостоятельная работа способствует формированию аналитического и творческого мышления, совершенствует способы организации исследовательской деятельности, воспитывает целеустремленность, систематичность и последовательность в работе студентов, обеспечивает подготовку студента к текущим контактным занятиям и контрольным мероприятиям по дисциплине. Результаты этой подготовки проявляются в активности студента на занятиях и в качестве выполненных тестовых заданий, и других форм текущего контроля.

Самостоятельная работа может включать следующие виды работ:

- изучение понятийного аппарата дисциплины;
- проработка тем дисциплины, поиск информации в электронных библиотечных системах;
- подготовка к лабораторным работам, практическим занятиям;
- работа с основной и дополнительной литературой, представленной в рабочей программе;
- подготовка к промежуточной аттестации;
- изучение материала, вынесенного на самостоятельную проработку;
- работа в электронных библиотечных системах, справочных, справочно-поисковых и иных системах.

Темы для самостоятельной работы обучающегося, порядок их контроля по дисциплине «Информационная безопасность» приведены в методических указаниях:

А.И. Каюмова, Р.Р. Ахметзянов, Р.Н. Зарипова. Информационная безопасность: методические указания по выполнению лабораторных работ и организации самостоятельной работы по дисциплине «Информационная безопасность» для магистров направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» очной формы обучения. – Альметьевск: АГНИ, 2016. – 44с.

6. Фонд оценочных средств по дисциплине

Основной целью формирования ФОС по дисциплине «Информационная безопасность» является создание материалов для оценки качества подготовки обучающихся и установления уровня освоения компетенций.

Полный перечень оценочных средств текущего контроля и промежуточной аттестации по дисциплине приведен в Фонде оценочных средств (приложение 3 к данной рабочей программе).

Текущий контроль освоения компетенций по дисциплине проводится при изучении теоретического материала, решении задач на практических занятиях, сдаче отчетов по лабораторным работам.

Итоговой оценкой освоения компетенций является промежуточная аттестация в форме зачета с оценкой, проводимая с учетом результатов текущего контроля.

6.1. Перечень оценочных средств

Этапы формирования компетенций	Вид оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Текущий контроль			
1	Лабораторная работа	Может выполняться в индивидуальном порядке или группой обучающихся. Задания в лабораторных работах должны включать элемент командной работы. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и оценить уровень сформированности аналитических, исследовательских навыков, а также навыков практического мышления. Позволяет оценить способность к профессиональным трудовым действиям	Темы, задания для выполнения лабораторных работ, вопросы к их защите
2	Тестирование компьютерное	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося по соответствующим компетенциям.	Банк тестовых заданий

		Обработка результатов тестирования на компьютере обеспечивается специальными программами. Позволяет проводить самоконтроль (репетиционное тестирование), может выступать в роли тренажера при подготовке к зачету или экзамену	
3	Практическая задача	Средство оценки умения применять полученные теоретические знания в практической ситуации. Задача должна быть направлена на оценивание тех компетенций, которые подлежат освоению в данной дисциплине, должна содержать четкую инструкцию по выполнению или алгоритм действий	Комплект задач
Промежуточная аттестация			
4	Зачет с оценкой	Итоговая форма определения степени достижения запланированных результатов обучения (оценивания уровня освоения компетенций). Зачет выставляется по результатам текущей работы в семестре без дополнительного опроса.	

6.2. Уровень освоения компетенций и критерии оценивания результатов обучения

№ п/п	Оцениваемые компетенции (код, наименование)	Планируемые результаты обучения	Уровень освоения компетенций			
			Продвинутый уровень	Средний уровень	Базовый уровень	Компетенции не освоены
			Критерии оценивания результатов обучения			
			«отлично» (от 86 до 100 баллов)	«хорошо» (от 71 до 85 баллов)	«удовлетворительно» (от 55 до 70 баллов)	«неудовлетв.» (менее 55 баллов)
1	**ПК-1** способностью разрабатывать технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, управления, контроля, диагностики и испытаний, новые виды продукции, автоматизированные и автоматические технологии ее производства, средства и системы автоматизации, управления	**знать**: - технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний, методы расчета надежности автоматизированных систем;	Сформированные систематические представления об технических заданиях на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний, методы расчета надежности автоматизированных систем;	Сформированные, но содержащие отдельные пробелы представления об технических заданиях на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний, методы расчета надежности автоматизированных систем;	Неполные представления об технических заданиях на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний, методы расчета надежности автоматизированных систем;	Фрагментарные представления об технических заданиях на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний, методы расчета надежности автоматизированных систем;
		уметь: - анализировать технические задания на модернизацию и	Сформированное умение анализировать технические задания	В целом успешное, но содержащее отдельные пробелы в умение	В целом успешное, но не систематическое умение анализировать технические задания	Фрагментарное умение анализировать технические задания

	процессами, жизненным циклом продукции и ее качеством	автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний;	на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний;	анализировать технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний;	на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний;	на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний;
		владеть: - навыками работы в электронных библиотечных системах, справочных, справочно-поисковых и иных системах, связанных техническими средствами и системами автоматизации, диагностики и испытаний, оценки показателей надежности автоматизированных систем.	Успешное и систематическое владение навыками работы в электронных библиотечных системах, справочных, справочно-поисковых и иных системах, связанных техническими средствами и системами автоматизации, диагностики и испытаний, оценки показателей надежности	В целом успешное, но содержащее отдельные пробелы владения навыками работы в электронных библиотечных системах, справочных, справочно-поисковых и иных системах, связанных техническими средствами и системами автоматизации, диагностики и испытаний, оценки показателей надежности	В целом успешное, но не систематическое владение навыками работы в электронных библиотечных системах, справочных, справочно-поисковых и иных системах, связанных техническими средствами и системами автоматизации, диагностики и испытаний, оценки показателей надежности автоматизированных систем.	Фрагментарное владение навыками работы в электронных библиотечных системах, справочных, справочно-поисковых и иных системах, связанных техническими средствами и системами автоматизации, диагностики и испытаний, оценки показателей надежности автоматизированных систем.

			автоматизированных систем.	автоматизированных систем.		
1	**ПК-3** способностью: составлять описание принципов действия и конструкции устройств, проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, проектировать их архитектурно-программные комплексы	**знать**: - функциональные и числовые показатели надежности, программные комплексы обеспечения надежности; - методы анализа и диагностирования автоматизированных систем;	Сформированные систематические представления о функциональных и числовых показателях надежности, программных комплексах обеспечения надежности; методах анализа и диагностирования автоматизированных систем;	Сформированные, но содержащие отдельные пробелы представления о функциональных и числовых показателях надежности, программных комплексах обеспечения надежности; методах анализа и диагностирования автоматизированных систем;	Неполные представления о функциональных и числовых показателях надежности, программных комплексах обеспечения надежности; методах анализа и диагностирования автоматизированных систем;	Фрагментарные представления о функциональных и числовых показателях надежности, программных комплексах обеспечения надежности; методах анализа и диагностирования автоматизированных систем;
		уметь: - синтезировать и диагностировать системы с заданным уровнем надежности; - диагностировать показатели надежности систем;	Сформированное умение синтезировать и диагностировать системы с заданным уровнем надежности; диагностировать показатели надежности систем;	В целом успешное, но содержащее отдельные пробелы в умение синтезировать и диагностировать системы с заданным уровнем надежности; диагностировать показатели надежности систем;	В целом успешное, но не систематическое умение синтезировать и диагностировать системы с заданным уровнем надежности; диагностировать показатели надежности систем;	Фрагментарное умение синтезировать и диагностировать системы с заданным уровнем надежности; диагностировать показатели надежности систем;
		владеть: - навыками составлять описание принципов действия	Успешное и систематическое владение навыками составлять описание	В целом успешное, но содержащее отдельные пробелы владения навыками	В целом успешное, но не систематическое владение навыками составлять описание	Фрагментарное владение навыками составлять описание принципов действия

		и конструкции устройств, проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, основами построения надежных автоматизированных систем управления.	принципов действия и конструкции устройств, проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, основами построения надежных автоматизированных систем управления.	составлять описание принципов действия и конструкции устройств, проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, основами построения надежных автоматизированных систем управления.	принципов действия и конструкции устройств, проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, основами построения надежных автоматизированных систем управления.	и конструкции устройств, проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, основами построения надежных автоматизированных систем управления.

6.3. Варианты оценочных средств

6.3.1. Тестирование компьютерное

6.3.1.1. Порядок проведения

Тестирование компьютерное по дисциплине «Информационная безопасность» проводится два раза в течение семестра. Банк тестовых заданий содержит список вопросов и различные варианты ответов.

6.3.1.2. Критерии оценивания

Результат теста зависит от количества вопросов, на которые был дан правильный ответ.

6.3.1.3. Содержание оценочного средства

Тестовые задания для оценки уровня сформированности компетенций

Код компетенции	Тестовые вопросы	Варианты ответов			
		1	2	3	4
Дисциплинарный модуль 4.1.					
ПК-1	Информационная безопасность организации -	Это предмет определенного целевого назначения, рассматриваемый в процессах проектирования, производства, …	Это состояние защищенности информационной среды организации, обеспечивающее её формирование, использование и развитие	Свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки	Свойство объекта сохранять работоспособное состояние при установленной системе технического обслуживания и ремонта
	Объект - …	Это свойство объекта сохранять во времени в установленных пределах значения всех параметров …	Свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки	Это предмет определенного целевого назначения, рассматриваемый в процессах проектирования, производства, …	Свойство объекта сохранять работоспособное состояние при установленной системе технического обслуживания и ремонта
	Конфиденциальность -	Свойство объекта сохранять работоспособное состояние при установлен	Свойство объекта, заключающееся в приспособленности к поддержанию и	Свойство объекта сохранять в заданных пределах значения параметров, характеризу	Это состояние информации, при котором доступ к ней осуществляют только

		ной системе технического обслуживания и ремонта	восстановлению работоспособного состояния путем технического обслуживания и ремонта	ющих способность объекта выполнять требуемые функции, в течение и после хранения и / или транспортирования	субъекты, имеющие на него право
ПК-3	Доступность -	Свойство объекта сохранять работоспособное состояние при установленной системе технического обслуживания и ремонта	Свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки	Это избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа	Свойство объекта сохранять в заданных пределах значения параметров, характеризующих способность объекта выполнять требуемые функции, в течение и после хранения и / или транспортирования
	Целостность -	Свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки	Это избежание несанкционированной модификации информации	Свойство объекта, заключающееся в приспособленности к поддержанию и восстановлению работоспособного состояния путем технического обслуживания и ремонта	Свойство объекта сохранять в заданных пределах значения параметров, характеризующих способность объекта выполнять требуемые функции, в течение и после хранения и / или транспортирования

	Аппаратурное резервирование заключается в	Подключении резервной аппаратуры	Выполнении заданной функции различными способами	Введении избыточных символов при передаче, обработке	
	Функциональное резервирование заключается в	Подключении резервной аппаратуры	Выполнении заданной функции различными способами	Введении избыточных символов при передаче, обработке	Подключение аппаратуры
Дисциплинарный модуль 4.2.					
ПК-1	В АСУ применяют следующие виды резервирования:	Аппаратурное, неаппаратурное	Аппаратурное, функциональное, временное, информационное	Конструктивно- схемное и производственное	
	Аппаратурное резервирование заключается в	Подключении резервной аппаратуры	Выполнении заданной функции различными способами	Введении избыточных символов при передаче, обработке	
	Функциональное резервирование заключается в	Подключении резервной аппаратуры	Выполнении заданной функции различными способами	Введении избыточных символов при передаче, обработке	Подключение аппаратуры
ПК-3	Информационное резервирование заключается в	Подключении резервной аппаратуры	Выполнении заданной функции различными способами	Введении избыточных символов при передаче, обработке	Подключение аппаратуры
	Интернет -.	Всемирная информационная сеть развивается большими темпами, количество участников постоянно растет	Введении избыточных символов при передаче, обработке	Подключении резервной аппаратуры	Подключение аппаратуры
	В АСУ применяют следующие виды	Аппаратурное, неаппаратурное	Аппаратурное, функциональное, временное,	Конструктивно- схемное и	

	резервирования:		информационное	производственное	
	Информационное резервирование заключается в	Подключении резервной аппаратуры	Выполнении заданной функции различными способами	Введении избыточных символов при передаче, обработке	Подключение аппаратуры
	Интернет -.	Всемирная информационная сеть развивается большими темпами, количество участников постоянно растет	Введении избыточных символов при передаче, обработке	Подключении резервной аппаратуры	Подключение аппаратуры

6.3.2. Лабораторные работы

6.3.2.1. Порядок проведения

Лабораторные работы выполняются обучающимися самостоятельно во время аудиторных занятий, в учебной аудитории для проведения занятий лабораторного типа, оснащённой соответствующим оборудованием. Обучающиеся проводят учебные эксперименты и тренируются в применении практико-ориентированных технологий. По завершению лабораторных исследований проводится защита лабораторных работ. Оцениваются знание материала и умение применять его на практике, умения и навыки по работе с оборудованием в соответствующей предметной области. Ответ студента оценивается преподавателем в соответствии с установленными критериями.

6.3.2.2. Критерии оценивания

Баллы в интервале 86-100% от максимальных ставятся (максимальный балл по каждой лабораторной работе приведен в п. 6.4), если обучающимся:

- оборудование и методы использованы правильно, проявлена продвинутая теоретическая подготовка, необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует её целям.

Баллы в интервале 71-85% от максимальных ставятся, если обучающимся:

- оборудование и методы использованы в основном правильно, проявлена средняя теоретическая подготовка, необходимые навыки и умения в основном освоены, результат лабораторной работы в основном соответствует её целям.

Баллы в интервале 55-70% от максимальных ставятся, если обучающийся:

- оборудование и методы частично использованы правильно, проявлена базовая теоретическая подготовка, необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует её целям.

Баллы в интервале 0-54% от максимальных ставятся, если обучающимся:

- оборудование и методы использованы неправильно, проявлена неудовлетворительная теоретическая подготовка, необходимые навыки и умения не освоены, результат лабораторной работы не соответствует её целям.

6.3.2.3. Содержание оценочного средства

Задания и вопросы к защите лабораторных работ:

Лабораторная работа №3. Источники угроз информационной безопасности Российской Федерации (ПК-1, ПК-3).

Оборудование: Используемое оборудование и программное обеспечение - ПЭВМ IBM PC, операционная система WINDOWS –XP, программы архивации.

Задание.

1. Изучить теоретический материал.
2. Написать на языке Си программу, реализующую модель монитора обращений, согласующуюся с мандатной моделью доступа.
3. Проанализировать проделанную работу и предложить свой метод противодействия угрозе раскрытия (нарушения конфиденциальности) в данной модели доступа.
4. Письменно ответить на контрольные вопросы.
5. Результат отразить в отчете.

Вопросы к защите:

1. Перечислите источники угроз безопасности информационного общества (ПК-1).
2. В чем заключается угроза раскрытия информации? Какие еще угрозы вы знаете, (ПК-1)?
3. Что положено в основу мандатной модели доступа (ПК-1)?
4. Раскройте понятие «деклассификация» в контексте защиты информации в вычислительной системе (ПК-1).
5. Какова роль принципалов и объектов в операционной системе (ПК-1)?
6. Какие средства позволяют реализовать мандатную модель доступа в ОС Novell Netware 4.12 (Windows 2000, XP) (ПК-1, ПК-3)?
7. Какие средства позволяют реализовать Z-модель в ММД в ОС Novell Netware 4.12 (Windows 2000, XP) (ПК-1)?
8. Расскажите о методах противодействия данной атаке (ПК-1).
9. Какие недостатки присущи мандатной модели помимо проблемы Z-Системы (ПК-1, ПК-3)?

Основные теоретические положения, последовательность выполнения

работы, методика, правила оформления и варианты индивидуальных заданий по лабораторным работам описаны в методическом указании:

А.И. Каюмова, Р.Р. Ахметзянов, Р.Н. Зарипова. Информационная безопасность: методические указания по выполнению лабораторных работ и организации самостоятельной работы по дисциплине «Информационная безопасность» для магистров направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» очной формы обучения. – Альметьевск: АГНИ, 2016. – 44с.

6.3.3. Практические задачи

6.3.3.1. Порядок проведения

Выполнение практических задач осуществляется студентами на практических занятиях и самостоятельно с использованием лекционного материала, а также материалов из списка рекомендованной основной и дополнительной литературы, учебно-методических изданий и нормативно-правовых источников. Ответ студента оценивается преподавателем в соответствии с установленными критериями.

6.3.3.2. Критерии оценивания

Баллы в интервале 86-100% от максимальных (максимальный балл приведен в п. 6.4) ставятся, если обучающийся:

- умеет разбирать альтернативные варианты решения практических задач, развиты навыки критического анализа проблем, предлагает новые решения в рамках поставленной задачи.

Баллы в интервале 71-85% от максимальных ставятся, если обучающийся:

- показал умение самостоятельно решать конкретные практические задачи, но допустил некритичные неточности и доказательства в ответе и решении.

Баллы в интервале 55-70% от максимальных ставятся, если обучающийся:

- в состоянии решать задачи в соответствии с заданным алгоритмом, однако допускает ряд ошибок при решение конкретной практической задачи из числа предусмотренных рабочей программой дисциплины.

Баллы в интервале 0-54% от максимальных ставятся, если обучающийся:

- допускает грубые ошибки в решении типовых практических задач (неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой дисциплины).

6.3.3.3. Содержание оценочного средства

Пример задачи 1 для оценки сформированности компетенции ПК-1, ПК-3:

1. Произвести оценку рисков существующей системы безопасности, результаты свести в таблицу 1.

2. Проставить в таблице коэффициент вероятности наступления и коэффициент ущерба от реализации угрозы по 3х бальной шкале. Произведение этих составляющих позволят определить риск. Рассчитать общую сумму рисков. На основе полученных данных выделить три типа риска: низкий (1,2), средний (3,4), высокий (6,9). Построить диаграмму оценки рисков по категориям. Сделать выводы.

3. Предложить средства улучшения системы информационной безопасности предприятия, охарактеризовать каждое из них. Провести сравнительный анализ этих средств с их аналогами (допускается использование данных социологических опросов; характеристики технических средств должны соответствовать реальным).

4. Провести оценку рисков разработанной системы безопасности и свести данные в таблицу 2 – Оценка рисков разработанной системы безопасности, аналогичную таблице 1. Построить диаграмму количества рисков после принятия разработанной политики безопасности. Сделать выводы.

5. Сделать общий вывод (можно ли считать разработанную систему безопасности эффективной, ответ аргументировать).

Пример задачи 2 для оценки сформированности компетенции ПК-1, ПК-3:

1. Изучить самостоятельно Шифр Виженера и зашифровать любое выбранное вами слово.

2. Зашифровать слово, связанное с ИБ 2-мя способами: шифром Цезаря и цифровым шифром.

3. Зашифровать словосочетание, связанное с ИБ шифром Гронсфельда и шифром Атбаш.

Примечание: при шифровании использовать слова с количеством букв не менее 7 и сложные словосочетания.

Сделать выводы.

Полный комплект практических задач по темам дисциплины представлен в ФОС и в методическом указании:

А.И. Каюмова, Р.Р. Ахметзянов, Р.Н. Зарипова. Информационная безопасность: методические указания по проведению практических занятий по дисциплине «Информационная безопасность» для магистров направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» очной формы обучения. – Альметьевск: АГНИ, 2016. – 44с.

6.3.4. Зачет с оценкой

6.3.4.1. Порядок проведения

Зачет с оценкой формируется по результатам текущего контроля, без дополнительного опроса, так как в течение семестра проводится

необходимое количество контрольных мероприятий, которые в своей совокупности проверяют уровень сформированности соответствующих компетенций.

6.3.4.2. Критерии оценивания

Для получения зачета с оценкой общая сумма баллов за контрольные мероприятия текущего контроля (с учетом поощрения обучающегося за участие в научной деятельности или особые успехи в изучении дисциплины) должна составлять от 55 до 100 баллов (шкала перевода рейтинговых баллов представлена в п.6.4).

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций.

В ГБОУ ВО АГНИ действует балльно-рейтинговая система оценки знаний обучающихся.

Общие положения:

- Для допуска к экзамену студенту необходимо набрать не менее **35 баллов** по результатам текущего контроля знаний.
- Если студент по результатам текущего контроля в учебном семестре набрал от **55** до **60** баллов и по данной дисциплине предусмотрен экзамен, то по желанию студента в экзаменационную ведомость и зачетную книжку экзаменатором без дополнительного опроса может быть проставлена оценка «удовлетворительно».
- Выполнение контрольных работ и тестов принимается в установленные сроки.
- Защита лабораторных работ принимается в установленные сроки.
- При наличии уважительных причин срок сдачи может быть продлен, но не более чем на две недели.
- Рейтинговая оценка регулярно доводится до студентов и передается в деканат в установленные сроки.

Порядок выставления рейтинговой оценки:

1. До начала семестра преподаватель формирует рейтинговую систему оценки знаний студентов по дисциплине, с разбивкой по текущим аттестациям.
2. Преподаватель обязан на первом занятии довести до сведения студентов условия рейтинговой системы оценивания знаний и умений по дисциплине.
3. После проведения контрольных испытаний преподаватель обязан ознакомить студентов с их результатами и по просьбе студентов объяснить объективность выставленной оценки.
4. В случае пропусков занятий по неуважительной причине студент имеет право добрать баллы после изучения всех модулей до начала экзаменационной сессии.

5. Студент имеет право добрать баллы во время консультаций, назначенных преподавателем.

6. Преподаватель несет ответственность за правильность подсчета итоговых баллов.

7. Преподаватель не имеет права аннулировать баллы, полученные студентом во время семестра, обязан учитывать их при выведении итоговой оценки.

Распределение рейтинговых баллов по дисциплинарным модулям

Дисциплинарный модуль	**ДМ 4.1**	**ДМ 4.2**
Текущий контроль (лабораторные работы, практические задачи)	12-25	12-25
Текущий контроль (тестирование)	15-25	16-25
Общее количество баллов по ДМ	**27-50**	**28-50**
Итоговый балл текущего контроля:		**55-100**

Дисциплинарный модуль 4.1.

№ п/п	**Виды работ**	**Максимальный балл**
Текущий контроль		
1	*Практическое занятие № 1.* Разработка политики безопасности предприятия.	2
2	*Практическое занятие № 2.* Анализ и оценка рисков предприятия.	2
3	*Практическое занятие № 3.* Шифрование данных.	2
4	*Лабораторная работа № 1.* Виды информации и основные методы ее защиты.	2
5	*Лабораторная работа № 2.* Виды угроз информационной безопасности Российской Федерации.	2
6	*Практическое занятие № 4.* Парольная защита. Количественная оценка стойкости парольной защиты.	2
7	*Лабораторная работа № 3.* Источники угроз информационной безопасности Российской Федерации.	2
8	*Лабораторная работа № 4.* Анализ информационной инфраструктуры государства.	2
9	*Практическое занятие № 5.* Настройка параметров безопасности браузера Internet Explorer.	2
10	*Практическое занятие № 6.* Анализ рисков информационной безопасности.	2
11	*Практическое занятие № 7.* Пакеты антивирусных программ.	2
12	*Лабораторная работа № 5.* Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.	2
13	*Лабораторная работа № 6.* Причины, виды, каналы утечки и искажения информации.	1
Итого:		**25**
Текущий контроль		
1	Тестирование	25

Итого по модулю 4.1:	**50**

Дисциплинарный модуль 4.2.

№ п/п	Виды работ	Максимальный балл
Текущий контроль		
1	*Практическое занятие № 8.* Программная реализация криптографических алгоритмов.	2
2	*Практическое занятие № 9.* Механизмы контроля целостности данных.	2
3	*Лабораторная работа № 7.* Тестовые испытания программных средств защиты.	2
4	*Лабораторная работа № 8.* Защита от утечек по каналу ПЭМИН, по акустическим и виброакустическим каналам.	2
5	*Лабораторная работа № 9.* Анализ сетевой топологии и установленных сервисов.	2
6	*Практическое занятие № 10.* Обеспечение информационной безопасности в ведущих зарубежных странах.	2
7	*Практическое занятие № 11.* Обнаружение уязвимостей по сигнатурам.	2
8	*Практическое занятие № 12.* Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор».	2
9	*Лабораторная работа № 10.* Сетевое сканирование.	2
10	*Лабораторная работа № 11.* Анализ трафика и сбор критичной информации программами пассивного анализа.	2
11	*Лабораторная работа № 12.* Оценка уязвимости коммутируемого доступа.	1
12	*Практическое занятие № 13.* Метод минимального риска.	1
13	*Практическое занятие № 14.* Тестирование программ.	1
14	*Лабораторная работа № 13.* Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф».	1
15	*Лабораторная работа № 14.* Аудит комплексной защиты информации предприятия.	1
Итого:		**25**
Текущий контроль		
1	Тестирование	25
Итого ДМ 4.2:		**50**

Студентам могут быть добавлены **дополнительные баллы** за следующие виды деятельности:

- участие в научно-исследовательской работе кафедры (до 7 баллов),
- выступление с докладами (по профилю дисциплины) на конференциях различного уровня (до 5 баллов),
- участие в написании статей с преподавателями кафедры (до 5 баллов),
- завоевание призового места (1-3) на олимпиаде, проводимой кафедрой автоматизации и информационных технологий (до 5 баллов), на олимпиадах по автоматизации в других вузах (до 10 баллов),

- разработка компьютерных программ в рамках автоматизации учебного процесса в Альметьевском государственном нефтяном институте (до 15 баллов).

При этом, если в течение семестра студент набирает более 100 баллов (по результатам дисциплинарных модулей и полученных дополнительных баллов), то итоговая сумма баллов округляется до 100 баллов.

В соответствии с Учебным планом направления подготовки 15.04.04– Автоматизация технологических процессов и производств по дисциплине «Информационная безопасность» предусмотрен **зачет с оценкой в 4 семестре**.

Для получения зачета с оценкой общая сумма баллов (за дисциплинарные модули и дополнительные баллы) должна составлять от 55 до 100 баллов.

Шкала перевода рейтинговых баллов

Общее количество набранных баллов	Оценка
55-70	3 (удовлетворительно)
71-85	4 (хорошо)
86-100	5 (отлично)

7. Перечень основной, дополнительной учебной литературы и учебно-методических изданий, необходимых для освоения дисциплины

№ п/п	Библиографическое описание	Количество печатных экземпляров или адрес электронного ресурса	Коэффициент обеспеченности
Основная литература			
1.	Басыня Е.А. Системное администрирование и информационная безопасность [Электронный ресурс]: учебное пособие/ Басыня Е.А.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2018.— 79 с.	Режим доступа: http://www.iprbookshop.ru/91423.html.	1

2.	Костин В.Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей [Электронный ресурс]: учебное пособие/ Костин В.Н.— Электрон. текстовые данные.— Москва: Издательский Дом МИСиС, 2018.— 31 с.	Режим доступа: http://www.iprbookshop.ru/98200.html.	1
3.	Суворова Г.М. Информационная безопасность [Электронный ресурс]: учебное пособие/ Суворова Г.М.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2019.— 214 с.	Режим доступа: http://www.iprbookshop.ru/86938.html.	1
4.	Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.	Режим доступа: http://www.iprbookshop.ru/29257.html.	1
Дополнительная литература			
1.	Сычев А.М. Безопасность электронного банкинга [Электронный ресурс]/ Сычев А.М., Ревенков П.В., Дудка А.Б.— Электрон. текстовые данные.— Москва, Саратов: ЦИПСиР, Ай Пи Эр Медиа, 2019.— 320 с.	Режим доступа: http://www.iprbookshop.ru/86159.html.	1
2.	Бахаров Л.Е. Информационная безопасность и защита информации (разделы криптография и стеганография) [Электронный ресурс]: практикум/ Бахаров Л.Е.— Электрон. текстовые данные.— Москва: Издательский Дом МИСиС, 2019.— 59 с.	Режим доступа: http://www.iprbookshop.ru/98171.html.	1
3	Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.	Режим доступа: http://www.iprbookshop.ru/10677.	1

4	Тюльпинова Н.В. Защита интеллектуальной собственности и компьютерной информации [Электронный ресурс]: учебное пособие для магистров/ Тюльпинова Н.В. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2020. — 341c.	Режим доступа: http://www.iprbookshop.ru/88755.html.	1
Учебно-методические издания			
1.	А.И. Каюмова, Р.Р. Ахметзянов, Р.Н. Зарипова. Информационная безопасность: методические указания по выполнению лабораторных работ и организации самостоятельной работы по дисциплине «Информационная безопасность» для магистров направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» очной формы обучения. – Альметьевск: АГНИ, 2016. – 44с.	http://elibrary.agni-rt.ru	1
2	А.И. Каюмова, Р.Р. Ахметзянов, Р.Н. Зарипова. Информационная безопасность: методические указания по проведению практических занятий по дисциплине «Информационная безопасность» для магистров направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» очной формы обучения. – Альметьевск: АГНИ, 2016. – 44с.	http://elibrary.agni-rt.ru	1

8. Перечень профессиональных баз данных, информационных справочных систем и информационных ресурсов, необходимых для освоения дисциплины

№ п/п	Наименование	Адрес в Интернете
1	Учебно-методическая литература для учащихся и студентов, размещенная на сайте «Studmed.ru»	http://www.studmed.ru
2	Единое окно доступа к информационным ресурсам	http://window.edu.ru
3	Российская государственная библиотека	http://www.rsl.ru
4	Электронная библиотека Elibrary	http://elibrary.ru
5	Электронно-библиотечная система IPRbooks	http://iprbookshop.ru

6	Электронная библиотека АГНИ	http://elibrary.agni-rt.ru.

9. Методические указания для обучающихся по освоению дисциплины

Цель методических указаний по освоению дисциплины – обеспечить обучающемуся оптимальную организацию процесса изучения дисциплины, а также выполнения различных форм самостоятельной работы.

Изучение дисциплины обучающимся требует систематического, упорного и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить как пропущенную тему, так и всю дисциплину в целом. Именно поэтому контроль над систематической работой студентов должен находиться в центре внимания преподавателя.

При подготовке к лекционным занятиям (теоретический курс) обучающимся необходимо:

- перед очередной лекцией необходимо изучить по конспекту материал предыдущей лекции, просмотреть рекомендуемую литературу;

- при затруднениях в восприятии материала следует обратиться к основным литературным источникам, рекомендованным рабочей программой дисциплины. Если разобраться в материале самостоятельно не удалось, то следует обратиться к лектору (по графику его консультаций) или к преподавателю на практических, лабораторных занятиях.

При подготовке к практическим и лабораторным занятиям, обучающимся необходимо:

- приносить с собой рекомендованную в рабочей программе литературу к конкретному занятию;

- до очередного лабораторного занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей теме;

- теоретический материал следует соотносить с нормативно-справочной литературой, так как в ней могут быть внесены последние научные и практические достижения, изменения, дополнения, которые не всегда отражены в учебной литературе;

- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов, в случае затруднений – обращаться к преподавателю.

Обучающимся, пропустившим занятия (независимо от причин), рекомендуется не позже, чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии.

Самостоятельная работа студентов имеет систематический характер и складывается из следующих видов деятельности:

- подготовка ко всем видам контрольных испытаний, в том числе к текущему контролю успеваемости (в течение семестра), промежуточной аттестации (по окончании семестра);

- самостоятельное изучение теоретического материала;

- оформление отчетов по лабораторным работам;

- подготовка к защите отчетов по лабораторным работам.

Для выполнения указанных видов работ необходимо изучить соответствующие темы теоретического материала, используя конспект лекций, учебники и учебно-методическую литературу, а также интернет-ресурсы.

Для изучения дисциплины также, используется система дистанционного обучения АГНИ «Цифровой университет» (СДО АГНИ), созданная на платформе MOODLE, которая позволяет организовать контактную работу обучающихся посредством сети «Интернет» в удаленном режиме доступа. При этом трудоемкость дисциплины и контактной работы, материалы, используемые для проведения занятий, соответствуют учебному плану, РПД и позволяют полностью освоить заданные компетенции. Вид и форма лекционного материала и материала для практических занятий определяется преподавателем и размещается в СДО АГНИ «Цифровой университет».

Перечень учебно-методических изданий, рекомендуемых студентам для подготовки к занятиям и выполнению самостоятельной работы, а также методические материалы на бумажных и/или электронных носителях, выпущенные кафедрой своими силами и предоставляемые студентам во время занятий, представлены в пункте 7 рабочей программы.

Учебно-методическая литература для данной дисциплины имеется в электронно-библиотечной системе «IPRbooks», доступ к которым предоставлен студентам.

10. Перечень программного обеспечения

№ п/п	Наименование программного обеспечения	Лицензия	Договор
1	Microsoft Office Professional Plus 2016 Rus Academic OLP (Word, Excel, PowerPoint, Access)	№67892163 от 26.12.2016г.	№0297/136 от 23.12.2016г.
2	Microsoft Office Standard 2016 Rus Academic OLP (Word, Excel, PowerPoint)	№67892163 от 26.12.2016г.	№0297/136 от 23.12.2016г.
3	Microsoft Windows Professional 10 Rus Upgrade Academic OLP	№67892163 от 26.12.2016г.	№0297/136 от 23.12.2016г.
4	ABBYY FineReader 12 Professional	№197059 от 26.12.2016г.	№0297/136 от 23.12.2016г.
5	Kaspersky Endpoint Security длябизнеса – Стандартный Russian Edition	№ 24C4191023143020830784	BP00347095-CT/582 от 10.10.2019г.

6	Электронно-библиотечная система IPRbooks		Лицензионный договор №494 от 01.10.2019г.
7	ПО «Автоматизированная тестирующая система	Свидетельство государственной регистрации программ для ЭВМ №2014614238 от 01.04.2014г.	
8	7-Zip File Manager	свободно распространяемое ПО	

11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Освоение дисциплины «Информационная безопасность» предполагает использование следующего материально-технического обеспечения.

№ п/п	Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Ул. Р. Фахретдина, 42. Учебный корпус В, аудитория В-206 (учебная аудитория для занятий лекционного и практического типа)	1.Компьютер в комплекте с монитором ITCorp 2.Проектор NEC 3.Экран проекционный 4.Принтер Pantum P2207
2.	Ул. Р. Фахретдина, 42. Учебный корпус В, аудитория В-214 компьютерный класс (Учебная аудитория для проведения занятий лабораторного типа, текущего контроля и промежуточной аттестации, самостоятельной работы)	1. Компьютер в комплекте с монитором IT Corp 3250 – 11 шт. с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду института. 2. Проектор NEC 3. Экран на штативе 4. Принтер HP LJ P3015d 5. Сканер Epson Perfection V33.

*Специальные помещения – учебные аудитории для проведения занятий лекционного типа, практических и лабораторных занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися лицам с ограниченными возможностями здоровья:

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем;
- применение дистанционных образовательных технологий для организации форм текущего контроля;
- увеличение продолжительности сдачи обучающимся лицам с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

Рабочая программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению подготовки 15.04.04 – Автоматизация технологических процессов и производств, направленность (профиль) программы «Автоматизация технологических процессов и производств».

Приложение 1

АННОТАЦИЯ
рабочей программы дисциплины

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки: 15.04.04 – Автоматизация технологических процессов и производств

Направленность (профиль) программы: «Автоматизация технологических процессов и производств»

Оцениваемые компетенции (код, наименование)	**Результаты освоения компетенции**	**Оценочные средства текущего контроля и промежуточной аттестации**
ПК-1 способностью разрабатывать технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, управления, контроля, диагностики и испытаний, новые виды продукции, автоматизированные и автоматические технологии ее производства, средства и системы автоматизации, управления процессами, жизненным циклом продукции и ее качеством	**знать**: - технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний, методы расчета надежности автоматизированных систем; **уметь**: - анализировать технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, диагностики и испытаний; **владеть:** - навыками работы в электронных библиотечных системах, справочных, справочно-поисковых и иных системах, связанных техническими средствами и системами автоматизации, диагностики и испытаний, оценки показателей надежности автоматизированных систем.	**Текущий контроль:** Компьютерное тестирование по темам 1-6 Практические задачи по темам 1-6 Лабораторные работы по темам 1-6 **Промежуточная аттестация:** Зачет с оценкой
ПК-3 способностью: составлять описание принципов действия и конструкции устройств,	**знать**: - функциональные и числовые показатели надежности,	**Текущий контроль:** Компьютерное тестирование

проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, проектировать их архитектурно-программные комплексы	программные комплексы обеспечения надежности; - методы анализа и диагностирования автоматизированных систем; **уметь:** - синтезировать и диагностировать системы с заданным уровнем надежности; - диагностировать показатели надежности систем; **владеть:** - навыками составлять описание принципов действия и конструкции устройств, проектируемых технических средств и систем автоматизации, управления, контроля, диагностики и испытаний технологических процессов и производств общепромышленного и специального назначения для различных отраслей национального хозяйства, основами построения надежных автоматизированных систем управления.	по темам 1-6 Практические задачи по темам 1-6 Лабораторные работы по темам 1-6 **Промежуточная аттестация:** Зачет с оценкой

Место дисциплины в структуре ОПОП ВО	**Б1.В.ДВ.03.02**. Дисциплина «Информационная безопасность» является дисциплиной по выбору, входит в состав Блока 1 «Дисциплины (модули)» и относится к вариативной части Дисциплина изучается на 2 курсе в 4 семестре[1]/на 3 курсе в 5 семестре[2].
Общая трудоемкость дисциплины (в зачетных единицах и часах)	Зачетных единиц по учебному плану: **4** ЗЕ. Часов по учебному плану:**144**ч.
Виды учебной работы	Контактная работа обучающихся с преподавателем: лекции – 14 ч.[1]/6 ч.[2], лабораторные работы – 28 ч.[1]/12 ч.[2], практические занятия – 28ч.[1]/12 ч.[2], КСР – 2 ч.[1]/2 ч.[2] Самостоятельная работа – 72 ч.[1]/122 ч.[2]
Изучаемые темы (разделы)	Тема 1. Введение. Основные понятия. Тема 2. Проблемы информационной безопасности. Тема 3. Методы и средства обеспечения информационной безопасности. Тема 4. Протоколы защиты.

[1] Очная форма обучения
[2] Очно-заочная форма обучения

	Тема 5. Защита от вредоносных программ. Основные программно-технические меры. Тема 6. Стандарты и спецификации в области информационной безопасности.
Форма промежуточной аттестации	**зачет с оценкой** в 4 семестре[1]/**зачет с оценкой** в 5 семестре[2].

[1] Очная форма обучения
[2] Очно-заочная форма обучения

ПРИЛОЖЕНИЕ 2

УТВЕРЖДАЮ
Первый проректор АГНИ

_____ _____
(подпись) *(И.О. Фамилия)*
«___» _____ 20___г.

ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ
к рабочей программе дисциплины Б1.В.ДВ.03.02

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки: 15.03.04 – Автоматизация технологических процессов и производств

Направленность (профиль) программы: Автоматизация технологических процессов и производств

на 20__/20__ учебный год

В рабочую программу вносятся следующие изменения:

_____
_____
_____
_____
_____
_____
_____

Изменения в рабочей программе рассмотрены и одобрены на заседании кафедры «Автоматизация и информационные технологии»
(наименование кафедры)

протокол № _____от "_____" _____ 20___г.

Заведующий кафедрой:

_____ _____ _____
(ученая степен, ученое звание) *(подпись)* *(И.О.Фамилия)*