МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени В.Я.ГОРИНА

«УТВЕРЖДАЮ»
Декан инженерного факультета,
_____ С.В. Стребков
«05» 07 2018 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине **«Информационная безопасность»**

Направление 09.03.03 Прикладная информатика

Направленность (профиль) - Прикладная информатика в АПК

Квалификация – бакалавр

Майский, 2018

2

Рабочая программа составлена с учетом требований:

- федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки РФ от 12 марта 2015 г. № 207;
- порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства образования и науки РФ от 05.04.2017 г. № 301;
- основной профессиональной образовательной программы ФГБОУ ВО Белгородский ГАУ по направлению подготовки 09.03.03 «Прикладная информатика»

Составители: к.т.н., доцент Миронов А.Л.

Рассмотрена на заседании кафедры информатики и информационных технологий от 21.06. 2018 г., протокол № 13

и.о. зав. кафедрой _____ Игнатенко В.А.

Одобрена методической комиссией инженерного факультета

от 05.07. 2018 г., протокол № 9 - 17/18

Председатель методической комиссии _____Слободюк А.П.

I. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Информационная безопасность – дисциплина, изучающая теоретические вопросы и практические аспекты обеспечения информационной безопасности.

1.1. Цель дисциплины – ознакомление студентов с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации при проектировании информационных систем.

1.2. Задачи:

Задачи дисциплины заключаются в приобретение студентами прочных знаний и практических навыков в области, определяемой основной целью курса. В процессе изучения дисциплины студент должен получить представление о: международных стандартах информационного обмена; понятии угрозы; информационной безопасности в условиях функционирования в России глобальных сетей; видах противников или «нарушителей»; понятия о видах вирусов; видах возможных нарушений информационной системы; основных нормативных руководящих документах, касающиеся государственной тайны, нормативно-справочных документах; назначении и задачах в сфере обеспечения информационной безопасности на уровне государства; основных положениях теории информационной безопасности информационных систем; моделях безопасности и их применении; таксономии нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование; анализе способов нарушений информационной безопасности; использовании защищенных компьютерных систем; методах криптографии; основных технологиях построения защищенных ЭИС; месте информационной безопасности экономических систем в национальной безопасности страны; концепции информационной безопасности.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ (ОПОП)

2.1. Цикл (раздел) ОПОП, к которому относится дисциплина

Информационная безопасность относится к вариативной части (Б1.В.09) основной профессиональной образовательной программы.

2.2. Логическая взаимосвязь с другими частями ОПОП

Наименование предшествующих дисциплин, практик, на которых базируется данная дисциплина (модуль)	1. Математика
	2. Дискретная математика
	3. Информатика и программирование
Требования к предварительной подготовке обучающихся	***знать:*** ➢ основные понятия, используемые в информатике и программировании; ➢ элементарные методы математики, экономико-статистические методы исследования; ➢ понятия системы и системного анализа;

	уметь: ➢ применять средства компьютерной техники, пакеты прикладных программ для решения прикладных задач; ➢ пользоваться сетевыми информационными ресурсами, работать с сетевыми службами и сервисами; ***владеть:*** ➢ навыками использования офисных прикладных программ и информационных ресурсов сети Интернет

Освоение дисциплины «Информационная безопасность» необходимо для изучения дисциплин: «Разработка мобильных приложений», «Прикладное программирование», «Автоматические системы управления в агропромышленном комплексе», а так же для выполнения дипломных работ.

III. ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, СООТВЕТСТВУЮЩИЕ ФОРМИРУЕМЫМ КОМПЕТЕНЦИЯМ

Коды компетенций	**Формулировка компетенции**	**Планируемые результаты обучения по дисциплине**
ОПК-4	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** основные требования информационной безопасности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации
		Уметь: выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.
		Владеть: навыками обеспечения безопасного использования информационно-коммуникационных технологий, применения способов и средств защиты информации
ПК-8	способность программировать приложения и создавать программные прототипы решения прикладных задач	**Знать:** алгоритмы решения прикладных задач информационной безопасности, криптографические алгоритмы, инструменты программирования приложений и создания программных прототипов решения прикладных задач.
		Уметь: разрабатывать и реализовывать программно алгоритмы решения прикладных задач информационной безопасности, использовать инструменты программирования приложений и создания программных прототипов решения прикладных задач.
		Владеть: навыками программирования приложений и создания программных прототипов решения прикладных задач информационной

		безопасности

IV. ОБЪЕМ, СТРУКТУРА, СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, ВИДЫ УЧЕБНОЙ РАБОТЫ И ФОРМЫ КОНТРОЛЯ ЗНАНИЙ

4.1. Распределение объема учебной работы по формам обучения

Вид работы	**Объем учебной работы, час**	
Формы обучения (вносятся данные по реализуемым формам)	**Очная**	**Заочная**
Семестр (курс) изучения дисциплины	**6 семестр 3курс**	**5 курс**
Общая трудоемкость, всего, час *зачетные единицы*	216 *6*	216 *6*
Контактная работа обучающихся с преподавателем		
Аудиторные занятия *(всего)*	**80**	**22**
В том числе:		
Лекции	16	8
Лабораторные занятия	32	14
Практические занятия	32	-
Иные виды работ в соответствии с учебным планом (учебная практика)	-	-
Внеаудиторная работа *(всего)*	**16**	**6**
В том числе:		
Контроль самостоятельной работы (на 1 подгруппу в форме компьютерного тестирования)	-*	-
Консультации согласно графику кафедры	16	6
Иные виды работ в соответствии с учебным планом (курсовая работа, РГЗ и др.)	-	-
Промежуточная аттестация	**10**	**10**
В том числе:		
Зачет	-	-
Экзамен (на 1 группу)	8	8
Консультация предэкзаменационная (на 1 группу)	2	2
Самостоятельная работа обучающихся	**110**	**178**
Самостоятельная работа обучающихся *(всего)*	**110**	**178**
в том числе:		
Самостоятельная работа по проработке лекционного материала (до 60% от объема лекций)	9	4
Самостоятельная работа по подготовке к лабораторно-практическим занятиям (до 60% от объема аудиторных занятий)	48	13
Работа над темами (вопросами), вынесенными на самостоятельное изучение	27	125
Самостоятельная работа по видам индивидуальных заданий: подготовка реферата (контрольной работы)	10	20
Подготовка к экзамену	16	16

Примечание:*осуществляется на аудиторных занятиях

4.2 Общая структура дисциплины и виды учебной работы

Наименование модулей и разделов дисциплины	Объемы видов учебной работы по формам обучения, час									
	Очная форма обучения					Заочная форма обучения				
	Всего	Лекции	Лабораторно-практ. занятия	Внеаудиторная работа и пр. атт.	Самостоятельная работа	Всего	Лекции	Лабораторно-практ. занятия	Внеаудиторная работа и пр. атт.	Самостоятельная работа
1	2	3	4	5	6	7	8	9	10	11
Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»	**60**	**4**	**22**	**6**	**28**	**56**	**2**	**2**	**2**	**50**
1.Введение в ИБ и составляющие ИБ.	12	1	4	*Консультации*	7	13	0,5	-	*Консультации*	12,5
2.Формирование режима ИБ	14	1	6		7	13	0,5	-		12,5
3.Нормативно правовые основы ИБ в РФ. Стандарты ИБ.	14	1	6		7	13	0,5	-		12,5
4.Административный уровень обеспечения информационной безопасности. Классификация угроз ИБ.	12	1	5		6	15	0,5	2		12,5
Итоговое занятие по модулю 1	*2*	-	*1*		*1*	-	-	-		-
Модуль 2 «Вирусы и удаленные угрозы в сетях»	**60**	**6**	**20**	**6**	**28**	**57**	**2**	**6**	**2**	**47**
1.Вирусы как угроза ИБ. Классификация компьютерных вирусов.	12	1	4	*Консультации*	7	12,5	0,5	1	*Консультации*	11
2.Характеристика «вирусоподобных» программ. Антивирусные программные средства. Обнаружение и профилактика вирусных атак.	12	1	4		7	13,5	0,5	1		12
3.Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных.	15	2	6		7	14,5	0,5	2		12
4.Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях	13	2	5		6	14,5	0,5	2		12

Итоговое занятие по модулю 2	*2*	*-*	*1*		*1*	*-*	*-*	*-*		*-*
Модуль 3 «Принципы и методы защиты в вычислительных сетях»	**60**	**6**	**22**	**4**	**28**	**57**	**4**	**6**	**2**	**45**
1.Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях	11	1	4	*Консультации*	6	13	1	-	*Консультации*	12
2.Принципы защиты распределенных вычислительных сетей. Идентификация и аутентификация.	12	1	4		7	14	1	2		11
3.Криптография и шифрование. Методы разграничения доступа.	17	2	8		7	14	1	2		11
4.Регистрация и аудит. Межсетевое экранирование.	14	2	5		7	14	1	2		11
Итоговое занятие по модулю 2	*2*	*-*	*1*		*1*	*-*	*-*	*-*		*-*
Подготовка реферата в форме презентации (контрольной работы)	***10***	***-***	***-***	***-***	***10***	***20***	***-***	***-***	***-***	***20***
Экзамен	***26***	***-***	***-***	***10***	***16***	***26***	***-***	***-***	***10***	***16***

4.3 Структура и содержание дисциплины по формам обучения

Наименование модулей и разделов дисциплины	**Объемы видов учебной работы по формам обучения, час**									
	Очная форма обучения					**Заочная форма обучения**				
	Всего	**Лекции**	**Лабор.практ. зан.**	**Внеаудит. работа**	**Самост. работа**	**Всего**	**Лекции**	**Лабор.практ. зан**	**Внеаудит. работа**	**Самост. работа**
1	2	3	4	5	6	7	8	9	10	11
Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»	**60**	**4**	**22**	**6**	**28**	**56**	**2**	**2**	**2**	**50**
1. Введение в ИБ и составляющие ИБ.	***12***	***1***	***4***	*Консультации*	***7***	***13***	***0,5***	***-***	*Консультации*	***12,5***
1.1 Предмет, задачи и структура дисциплины	6	0,5	2		3,5	6,5	0,25	-		6,25
1.2 Понятие и составляющие ИБ	6	0,5	2		3,5	6,5	0,25	-		6,25
2. . Формирование режима ИБ	***14***	***1***	***6***		***7***	***13***	***0,5***	***-***		***12,5***
2.1 Уровни формирования режимов ИБ и их взаимосвязь	6	0,5	2		3,5	6,5	0,25	-		6,25
2.2 Требования формирования режимов ИБ на различных уровняъ	8	0,5	4		3,5	6,5	0,25	-		6,25
3. Нормативно правовые основы ИБ в РФ. Стандарты ИБ.	***14***	***1***	***6***		***7***	***13***	***0,5***	***-***		***12,5***
3.1 Нормативно-правовые основы ИБ в РФ.	6	0,5	2		3,5	6,5	0,25	-		6,25
3.2 Стандарты ИБ.	8	0,5	4		3,5	6,5	0,25	-		6,25
4. Административный уровень обес-	***12***	***1***	***5***		***6***	***15***	***0,5***	***2***		***12,5***

печения информационной безопасности. Классификация угроз ИБ.										
4.1 Административный уровень обеспечения ИБ	***5,5***	***0,5***	***2***		***3***	***7,5***	***0,25***	***1***		6,25
4.2 Классификация угроз ИБ	***6,5***	***0,5***	***3***		***3***	***7,5***	***0,25***	***1***		6,25
Итоговое занятие по модулю 1	*2*	-	*1*		*1*	-	-	-		-
Модуль 2 «Вирусы и удаленные угрозы в сетях»	**60**	**6**	**22**	**6**	**26**	**57**	**2**	**6**	**2**	**47**
1. Вирусы как угроза ИБ. Классификация компьютерных вирусов.	12	1	4		*7*	***12,5***	***0,5***	***1***		***11***
1.1 Вирусы как угроза ИБ	6	0,5	2		3,5	6,25	0,25	0,5		5,5
1.2 Классификация компьютерных вирусов	6	0,5	2		3,5	6,25	0,25	0,5		5,5
2. Характеристика «вирусоподобных» программ. Антивирусные программные средства. Обнаружение и профилактика вирусных атак.	12	1	4		*7*	***13,5***	***0,5***	***1***		***12***
2.1 Характеристика «вирусоподобных» программ	6	0,5	2		3,5	6,75	0,25	0,5		6
2.2 Антивирусные программные средства. Борьба с вирусами.	6	0,5	2		3,5	6,75	0,25	0,5		6
3. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных.	15	2	6	***Консультации***	*7*	***14,5***	***0,5***	***2***	***Консультации***	***12***
3.1 Информационная безопасность в компьютерных сетях	6,5	1	2		3,5	7,25	0,25	1		
3.2 Сетевые модели передачи данных и безопасность	8,5	1	4		3,5	7,25	0,25	1		6
4. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях	***13***	***2***	***5***		***6***	***14,5***	***0,5***	***2***		***12***
4.1 Аспекты безопасности в модели взаимодействия открытых систем	***6,5***	***1***	***2***		***3***	***7,25***	***0,25***	***1***		***6***
4.2 Классификация удаленных угроз в вычислительных сетях	***6,5***	***1***	***3***		***3***	***7,25***	***0,25***	***1***		***6***
Итоговое занятие по модулю 2	***2***	-	***1***		***1***	-	-	-		-
Модуль 3 «Принципы и методы защиты в вычислительных сетях	**60**	**6**	**22**	**6**	**26**	**57**	**4**	**6**	**2**	**45**
1.Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях	11	1	4		6	13	1	-		12
2. Принципы защиты распределенных вычислительных сетей. Идентификация и аутентификация.	12	1	4	***Консультации***	7	14	1	2	***Консультации***	11
3. Криптография и шифрование. Методы разграничения доступа.	17	2	8		7	14	1	2		11
4. Регистрация и аудит. Межсетевое экранирование.	12	2	5		5	14	1	2		11
Итоговое занятие по модулю 3	***2***	-	***1***		***1***	-	-	-		-
Подготовка реферата в форме презентации (контрольной работы)	***10***	-	-	-	***10***	***20***	-	-	-	***20***
Экзамен	***26***	-	-	***10***	***16***	***26***	-	-	***10***	***16***

V. ОЦЕНКА ЗНАНИЙ И ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1. Формы контроля знаний, рейтинговая оценка и формируемые компетенции (дневная форма обучения)

№ п/п	Наименование рейтингов, модулей и блоков	Формируемые компетенции	Объем учебной работы					Форма контроля знаний	Количество баллов (max)
			Общая трудоемкос	Лекции	Лабор.-практ.заня	Внеаудиторн. раб.	Самост. работа		
Всего по дисциплине		***ОПК-4, ПК-8***	**216**	**16**	**64**	**26**	**110**	**Экзамен**	**100**
I. Входной рейтинг								Устный опрос	***5***
II. Рубежный рейтинг								Сумма баллов за модули	***60***
Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»		***ОПК-4, ПК-8***	**60**	**4**	**22**	**6**	**28**		***20***
1.	Введение в ИБ и составляющие ИБ.		12	1	4		7	Устный опрос	
2.	Формирование режима ИБ		14	1	6		7	Устный опрос, решение задач	
3.	Нормативно правовые основы ИБ в РФ. Стандарты ИБ.		14	1	6		7	Устный опрос, решение задач	
4.	Административный уровень обеспечения информационной безопасности. Классификация угроз ИБ.		12	1	5		6	Устный опрос, решение задач	
Итоговый контроль знаний по темам модуля 1.			2	*2*	-		1	*1*	
Модуль 2 «Информационные системы и технологии. Интеграция и классификация информационных систем»		***ОПК-4, ПК-8***	**60**	**6**	**20**	**6**	**28**		***20***
1.	Вирусы как угроза ИБ. Классификация компьютерных вирусов.		12	1	4		7	Устный опрос, решение задач	

2.	Характеристика «вирусоподобных» программ. Антивирусные программные средства. Обнаружение и профилактика вирусных атак.		12	1	4		7	Устный опрос, решение задач	
3.	Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных.		15	2	6		7	Устный опрос, решение задач	
4.	Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях		13	2	5		6	Устный опрос, решение задач	
Итоговый контроль знаний по темам модуля 2.			2		*1*		1	Тестирование, ситуационные задачи	
Модуль 3 «Современные информационные системы. Автоматизация документооборота и организация совместной работы»		***ОПК-4, ПК-8***	**60**	**6**	**20**	**6**	**28**		***20***
1.	Системы автоматизации документооборота (системы управления документооборотом)		12	1	4		7	Устный опрос, решение задач	
2.	Системы автоматизации делопроизводства и документооборота отечественных производителей		12	1	4		7	Устный опрос, решение задач	
3.	Системы групповой работы над документами (groupware)		15	2	6		7	Устный опрос, решение задач	
4.	Системы управления деловыми процессами (workflow management)		13	2	5		6	Устный опрос, решение задач	
Итоговый контроль знаний по темам модуля 2.			2		*1*		1	Тестирование, ситуационные задачи	
III. Творческий рейтинг			***10***	-	-	-	***10***		***5***
IV. Выходной рейтинг			***26***	-	-	***10***	***16***	***Экзамен***	***30***

5.2. Оценка знаний студента

5.2.1. Основные принципы рейтинговой оценки знаний

Уровень развития компетенций оценивается с помощью рейтинговых баллов.

Рейтинги	**Характеристика рейтингов**	**Максимум баллов**
Входной	Отражает степень подготовленности студента к изучению дисциплины. Определяется по итогам входного контроля знаний на первом практическом занятии.	5
Рубежный	Отражает работу студента на протяжении всего периода изучения дисциплины. Определяется суммой баллов, которые студент получит по результатам изучения каждого модуля.	60
Творческий	Результат выполнения студентом индивидуального творческого задания различных уровней сложности, в том числе, участие в различных конференциях и конкурсах на протяжении всего курса изучения дисциплины.	5
Выходной	Является результатом аттестации на окончательном этапе изучения дисциплины по итогам сдачи экзамена. Отражает уровень освоения информационно-теоретического компо-нента в целом и основ практической деятельности в частности.	30
Общий рейтинг	Определяется путём суммирования всех рейтингов	100

Итоговая оценка компетенций студента осуществляется путём автоматического перевода баллов общего рейтинга в стандартные оценки.

Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
менее 51 балла	51-67 баллов	68-85 баллов	86-100 баллов

5.2.2. Критерии оценки знаний студента на экзамене

На экзамене студент отвечает в письменно-устной форме на вопросы экзаменационного билета (вопрос, тест и задача).

Количественная оценка на экзамене определяется на основании следующих критериев:

- оценку «отлично» заслуживает студент, показавший всестороннее систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой; как правило, оценка «отлично» выставляется студентам,

усвоившим взаимосвязь основных понятий дисциплины и их значение для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

- оценку «хорошо» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе; как правило, оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности;
- оценку «удовлетворительно» заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой; как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя;
- оценка «неудовлетворительно» выставляется студенту, обнаружившему проблемы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий; как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжать обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

5.3. Фонд оценочных средств. Типовые контрольные задания или иные материалы, необходимые для оценки формируемых компетенций по дисциплине (приложение 2)

VI. УЧЕБНО - МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Основная учебная литература

1. Партыка, Т.Л. Информационная безопасность: Учебное пособие

[Электронный ресурс]/ Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. Режим доступа: http://znanium.com/bookread2.php?book=167284

2. Шаньгин , В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие [Электронный ресурс]/ В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. Режим доступа: http://znanium.com/bookread2.php?book=408107

6.2 Дополнительная литература

1. Миронов, А.Л. Информационная безопасность: Учебное пособие[электронный ресурс]/ А.Л. Миронов // Изд. Белгородского ГАУ, 2014. – 46 с. Режим доступа: https://clck.ru/FDtZ7

2. Миронов, А.Л. Методические указания для выполнения лабораторно-практических работ и самостоятельной работы по дисциплине «Информационная безопасность» для студентов направления подготовки «Прикладная информатика» [электронный ресурс]/ А.Л. Миронов, Д.А. Петросов // Изд. Белгородского ГАУ, 2014. – 38 с.

6.3. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов заключается в инициативном поиске информации о наиболее актуальных проблемах, которые имеют большое практическое значение и являются предметом научных дискуссий в рамках изучаемой дисциплины.

Самостоятельная работа планируется в соответствии с календарными планами рабочей программы по дисциплине и в методическом единстве с тематикой учебных аудиторных занятий.

Самостоятельную работу студента поддерживает электронная информационная среда ВУЗа, доступ к которой http:// do.belgau.edu.ru (логин, пароль студента)

6.3.1. Методические указания по освоению дисциплины

Игнатенко, В.А. Методические указания по самостоятельной работе студентов [Электронный ресурс]/ В.А. Игнатенко, В.Л. Михайлова// Изд. Белгородский ГАУ. 2015. - 42 с.

6.3.2. Видеоматериалы

1. https://www.youtube.com/watch?v=l_R3mpZ5qpY&list=PLC4B9227D19196ED9
2. https://www.youtube.com/watch?v=Wtr9FTWYIl4&list=PLceCi2zuMVQYTshyoko-aIv5pA7VjUF_q
3. https://www.youtube.com/watch?v=zsTay5MZz4U&list=PLDuhffxIYEDlQ9TggSrXD7nZ17_toHQXS
4. https://www.youtube.com/watch?v=OYj7fQjFBRE&list=PL7DC2D34B1

4С1936С

6.3.3 Печатные периодические издания

1. Журнал «Информационные технологии»
2. Журнал «Моделирование и анализ информационных систем»
3. Журнал «Information Security. Информационная безопасность»
4. Журнал «Вестник российской сельскохозяйственной науки»
5. Журнал «Достижения науки и техники АПК»
6. Журнал «Экономика, статистика и информатика»

6.4. Ресурсы информационно-телекоммуникационной сети «Интернет», современные профессиональные базы данных, информационные справочные системы.

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел. Информатика и информационные технологии» - http://window.edu.ru/catalog/
2. Новые информационные технологии и программы - Сайт о свободном программном обеспечении и новых информационных технологиях - http://pro-spo.ru/
3. CITForum.ru - on-line библиотека свободно доступных материалов по информационным технологиям на русском языке - http://citforum.ru/
4. Справочно - правовая система «Гарант».
5. Справочно - правовая система КонсультантПлюс.

6.5. Перечень программного обеспечения, информационных технологий

1. Операционная система Windows.
2. Пакет программ Microsoft Office.
3. SunRav – программа для тестирования.
4. ПО Anti-virus Kaspersky Security.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для преподавания дисциплины используются:

1. учебная аудитория лекционного типа, оборудованная мультимедийным оборудованием для демонстрации презентаций;
2. компьютерный класс для проведения лабораторно – практических занятий.

3. помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с подключением к сети Интернет и электронной информационно-образовательной среде ВУЗа.

VIII. ПРИЛОЖЕНИЯ

Приложение 1

СВЕДЕНИЯ О ДОПОЛНЕНИИ И ИЗМЕНЕНИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ НА 20__ / 20__ УЧЕБНЫЙ ГОД

Информационная безопасность

дисциплина (модуль)

09.03.03 Прикладная информатика

направление подготовки/специальность

ДОПОЛНЕНО (с указанием раздела РПД)
ИЗМЕНЕНО (с указанием раздела РПД)
УДАЛЕНО (с указанием раздела РПД)

Реквизиты протоколов заседаний кафедр, на которых пересматривалась программа

Кафедра информатики и информационных технологий № от _____ _____ Дата	Кафедра информатики и информационных технологий от № _____ _____ дата

Методическая комиссия инженерного факультета

«___» _____ 20 года, протокол № _____

Председатель методической комиссии Слободюк А.П.

Декан инженерного факультета Стребков С.В..

«___» _____ 20 г.

Приложение 2

Согласовано:
Генеральный директор
ООО «Центр Программных Систем»
«28» сентября 2018 г.
Конюхов В.М.
подпись

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся

по дисциплине Информационная безопасность
Направление подготовки 09.03.03 Прикладная информатика
Профиль «Прикладная информатика в АПК»

Майский, 2018

1.Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код контролируемой компетенции	Формулировка контролируемой компетенции	Этап (уровень) освоения компетенции	Планируемые результаты обучения	Наименование модулей и (или) разделов дисциплины	Наименование оценочного средства	
					Текущий контроль	Промежуточная аттестация
ОПК-4	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Первый этап (пороговой уровень)	**Знать:** основные требования информационной безопасности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации	**Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»**	Устный опрос Тестирование Решение ситуационных задач Подготовка рефератов	Итоговое тестирование, вопросы к экзамену
				Модуль 2 «Вирусы и удаленные угрозы в сетях»	Устный опрос Тестирование Решение ситуационных задач Подготовка рефератов	Итоговое тестирование, вопросы к экзамену
				Модуль 3 «Принципы и методы защиты в вычислительных сетях»	Устный опрос Тестирование Решение ситуационных задач Подготовка рефератов	Итоговое тестирование, вопросы к экзамену
		Второй этап (продвинутый	**Уметь:** выявлять угрозы ин-	**Модуль 1 «Составляющие, уровни**	Устный опрос	Итоговое тестирование, вопро-

		уровень)	формационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.	**обеспечения и угрозы ИБ»**	Тестирование	сы к экзамену
					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 2 «Вирусы и удаленные угрозы в сетях»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 3 «Принципы и методы защиты в вычислительных сетях»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
		Третий этап (высокий уровень)	**Владеть:** навыками обеспечения безопасного использования информационно-коммуникационных технологий, примене-	**Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»**	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	

			ния способов и средств защиты информации		Подготовка рефератов	
				Модуль 2 «Вирусы и удаленные угрозы в сетях»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 3 «Принципы и методы защиты в вычислительных сетях»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
ПК-8	способность программировать приложения и создавать программные прототипы решения прикладных задач	Первый этап (пороговой уровень)	**Знать:** алгоритмы решения прикладных задач информационной безопасности, криптографические алгоритмы, инструменты программирования приложений и создания программных прототипов решения прикладных задач.	**Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»**	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 2 «Вирусы и удаленные угрозы в сетях»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	

				Модуль 3 «Принципы и методы защиты в вычислительных сетях»»	Устный опрос Тестирование Решение ситуационных задач Подготовка рефератов	Итоговое тестирование, вопросы к экзамену
		Второй этап (продвинутый уровень)	**Уметь:** разрабатывать и реализовывать программно алгоритмы решения прикладных задач информационной безопасности, использовать инструменты программирования приложений и создания программных прототипов решения прикладных задач.	**Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»**	Устный опрос Тестирование Решение ситуационных задач Подготовка рефератов	Итоговое тестирование, вопросы к экзамену
				Модуль 2 «Вирусы и удаленные угрозы в сетях»	Устный опрос Тестирование Решение ситуационных задач Подготовка рефератов	Итоговое тестирование, вопросы к экзамену
				Модуль 3 «Принципы и методы защиты в вычислительных сетях»»	Устный опрос Тестирование Решение ситуационных задач Подготовка рефератов	Итоговое тестирование, вопросы к экзамену
		Третий этап (высокий уровень)	**Владеть:** навыками программирования приложений и создания программ-	**Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»**	Устный опрос Тестирование Решение ситуационных за-	Итоговое тестирование, вопросы к экзамену

			ных прототипов решения прикладных задач информационной безопасности		дач	
					Подготовка рефератов	
				Модуль 2 «Вирусы и удаленные угрозы в сетях»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 3 «Принципы и методы защиты в вычислительных сетях»»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
					Подготовка рефератов	
		Второй этап (продвинутый уровень)	*Уметь:* выполнять работы на всех стадиях жизненного цикла проекта ИС	**Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»**	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 2 «Вирусы и удаленные угрозы в сетях»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	

					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 3 «Принципы и методы защиты в вычислительных сетях»»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
		Третий этап (высокий уровень)	*Владеть:* инструментальными средствами проектирования баз данных и знаний	**Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»**	Устный опрос	Итоговое тестирование, выполнение курсовой работы, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 2 «Вирусы и удаленные угрозы в сетях»	Устный опрос	Итоговое тестирование, вопросы к экзамену
					Тестирование	
					Решение ситуационных задач	
					Подготовка рефератов	
				Модуль 3	Устный опрос	Итоговое тести-

				«Принципы и методы защиты в вычислительных сетях»»	Тестирование	рование, вопросы к экзамену
					Решение ситуационных задач	
					Подготовка рефератов	

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

Компетенция	**Планируемые результаты обучения (показатели достижения заданного уровня компетенции)**	**Уровни и критерии оценивания результатов обучения, шкалы оценивания**			
		Компетентность не сформирована	*Пороговый уровень компетентности*	*Продвинутый уровень компетентности*	*Высокий уровень*
		не зачтено (неудовлетворительно)	*зачтено (удовлетворительно)*	*зачтено (хорошо)*	*зачтено (отлично)*
ОПК-4	***Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности***	***Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информаци-***	***Частично владеет способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с уче-***	***Владеет способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных тре-***	***Свободно владеет способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с***

		онной безопасности не сформирована	***том основных требований информационной безопасности***	***бований информационной безопасности***	***учетом основных требований информационной безопасности***
	Знать: основные требования информационной безопасности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации	Не знает основные требования информационной безопасности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации	Частично знает основные требования информационной безопасности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации	Знает основные требования информационной безопасности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации	Знает и аргументировано оценивает основные требования информационной безопасности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации
	Уметь: выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.	Не умеет выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.	Частично умеет выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.	Умеет выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.	Свободно умеет выявлять угрозы выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.
	Владеть: навыками обеспечения безопасного использования информационно-коммуникационных технологий, применения способов и	Не владеет навыками обеспечения безопасного использования информационно-коммуникационных технологий, применения	Частично владеет навыками обеспечения безопасного использования информационно-коммуникационных технологий, примене-	Владеет навыками обеспечения безопасного использования информационно-коммуникационных технологий, примене-	Свободно владеет навыками обеспечения безопасного использования информационно- коммуникационных технологий, при-

	средств защиты информации	способов и средств защиты информации	ния способов и средств защиты информации	ния способов и средств защиты информации	менения способов и средств защиты информации
ПК-8	***Способность программировать приложения и создавать программные прототипы решения прикладных задач***	***Способность программировать приложения и создавать программные прототипы решения прикладных задач не сформирована***	***Частично владеет способностью программировать приложения и создавать программные прототипы решения прикладных задач***	***Владеет способностью программировать приложения и создавать программные прототипы решения прикладных задач***	***Свободно владеет способностью программировать приложения и создавать программные прототипы решения прикладных задач***
	Знать: алгоритмы решения прикладных задач информационной безопасности, криптографические алгоритмы, инструменты программирования приложений и создания программных прототипов решения прикладных задач.	Не знает алгоритмы решения прикладных задач информационной безопасности, криптографические алгоритмы, инструменты программирования приложений и создания программных прототипов решения прикладных задач.	Частично знает алгоритмы решения прикладных задач информационной безопасности, криптографические алгоритмы, инструменты программирования приложений и создания программных прототипов решения прикладных задач.	Знает алгоритмы решения прикладных задач информационной безопасности, криптографические алгоритмы, инструменты программирования приложений и создания программных прототипов решения прикладных задач.	Знает и способен аргументировано оценить алгоритмы решения прикладных задач информационной безопасности, криптографические алгоритмы, инструменты программирования приложений и создания программных прототипов решения прикладных задач.
	Уметь: разрабатывать и реализовывать программно алгоритмы решения прикладных задач информационной безопасности, использовать инструменты программирования приложений и создания программных прототипов решения прикладных задач.	Не умеет разрабатывать и реализовывать программно алгоритмы решения прикладных задач информационной безопасности, использовать инструменты программирования приложений и создания про-	Частично умеет разрабатывать и реализовывать программно алгоритмы решения прикладных задач информационной безопасности, использовать инструменты программирования приложений и	Умеет разрабатывать и реализовывать программно алгоритмы решения прикладных задач информационной безопасности, использовать инструменты программирования приложений и создания	Способен свободно разрабатывать и реализовывать программно алгоритмы решения прикладных задач информационной безопасности, аргументировано использовать инструменты про-

		граммных прототипов решения прикладных задач.	создания программных прототипов решения прикладных задач.	программных прототипов решения прикладных задач.	граммирования приложений и создания программных прототипов решения прикладных задач.
	Владеть: навыками программирования приложений и создания программных прототипов решения прикладных задач информационной безопасности	Не владеет навыками программирования приложений и создания программных прототипов решения прикладных задач информационной безопасности	Частично владеет навыками программирования приложений и создания программных прототипов решения прикладных задач информационной безопасности	Владеет навыками программирования приложений и создания программных прототипов решения прикладных задач информационной безопасности	Свободно владеет навыками программирования приложений и создания программных прототипов решения прикладных задач информационной безопасности

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1. Первый этап (пороговой уровень)

ЗНАТЬ (помнить и понимать): студент помнит, понимает и может продемонстрировать широкий спектр фактических, концептуальных, процедурных знаний.

3.1.1. Перечень вопросов для определения входного рейтинга

1. Средства вычислительной техники.
2. Средства организационной техники.
3. Средства коммуникационной техники.
4. Классификация средств компьютерной техники.
5. Системное программное обеспечение.
6. Принципы графической операционной системы.
7. Прикладное программное обеспечение.
8. Системы обработки текстовой информации.
9. Текстовые редакторы и процессоры.
10. Офисные пакеты прикладных программ.
11. Электронные таблицы.
12. Графические редакторы.
13. Средства работы с мультимедиа.
14. Базы данных. Понятие и типы.
15. Системы управления базами данных.
16. Понятие базы знаний и интеллектуальной системы.
17. Экспертные системы. Понятие и структура.
18. Правила безопасной работы на компьютере и в сети.
19. Компьютерные вирусы и борьба с ними.
20. Справочно-правовые системы в профессиональной деятельности.
21. Навигация в сети Интернет.
22. Информационные ресурсы сети Интернет.
23. Настройки браузера.

3.1.2. Перечень вопросов к экзамену

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.
2. Основные составляющие и аспекты информационной безопасности.
3. Классификация угроз информационной безопасности: для личности, для общества, для государства.
4. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.

5. Концепция «информационной войны» по оценкам российских спецслужб.

6. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?

7. Сфера применения информационного оружия.

8. Особенности информационного оружия. Организация защиты.

9. Основные задачи в сфере обеспечения информационной безопасности.

10. Отечественные стандарты в области информационной безопасности

11. Зарубежные стандарты в области информационной безопасности

12. Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?

13. Основные критерии оценки надежности: политика безопасности и гарантированность.

14. Понятие государственной тайны. Понятие профессиональной тайны.

15. Понятие коммерческой тайны. Понятие служебной тайны. Понятие банковской тайны.

16. Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере.

17. Понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.

18. Уязвимость информации в автоматизированных системах обработки данных.

19. Элементы и объекты защиты в автоматизированных системах обработки данных.

20. Методы защиты информации от преднамеренного доступа.

21. Защита информации от исследования и копирования.

22. Опознавание с использованием простого пароля. Метод обратимого шифрования.

23. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.

24. Использование динамически изменяющегося пароля. Метод «запрос-ответ»

25. Использование динамически изменяющегося пароля. Функциональные методы

26. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.

27. Электронная (цифровая) подпись. Цели применения электронной подписи.

28. Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.

29. Классификация методов криптографического закрытия.

30. Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.

31. Угрозы информации в персональных ЭВМ.

32. Обеспечение целостности информации в ПК. Физическая зашита ПК и носителей информации.

33. Защита ПК от несанкционированного доступа.

34. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации. Дать краткую характеристику.

35. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки.

36. Программные закладки. Классификация критериев вредоносного воздействия закладок.

37. Общие характеристики закладок.

38. Методы и средства защиты от закладок.

39. Компьютерный вирус. Какая программа считается зараженной.

40. По каким признакам классифицируются вирусы?

41. Способы заражения программ. Стандартные методы заражения.

42. Как работает вирус?

43. Методы защиты от вирусов.

44. Антивирусные программы. Программы-детекторы. Программы-доктора.

45. Антивирусы-полифаги. Эвристические анализаторы.

46. Программы-ревизоры. Программы-фильтры.

47. Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.

48. В чём заключаются задачи защиты в сетях передачи данных?

49. Проблемы защиты информации в вычислительных сетях.

50. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.

51. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.

52. Архитектура механизмов защиты информации в сетях ЭВМ.

3.2. Второй этап (продвинутый уровень)

УМЕТЬ (применять, анализировать, оценивать, синтезировать)**:** уметь использовать изученный материал в конкретных условиях и в новых ситуациях; осуществлять декомпозицию объекта на отдельные элементы и описывать то, как они соотносятся с целым, выявлять структуру объекта изучения; оценивать значение того или иного материала – научно-технической информации, исследовательских данных и т. д.; комбинировать элементы так, чтобы получить целое, обладающее новизной

3. 2.1. Тестовые задания

1. Составляющие информационной безопасности:

1) доступность информации
2) целостность информации
3) конфиденциальность информации
4) актуальность информации
5) 1-3

2. Понятие "информационная безопасность"...

1) значительно шире понятия компьютерной безопасности
2) совпадает с понятием компьютерной безопасности
3) уже понятия компьютерной безопасности

3. Глоссарий международных стандартов системы менеджмента информационной безопасности:

1) ISO/IEC 27000
2) ISO/IEC 27001
3) ISO/IEC 27002
4) ISO/IEC 27003
5) ISO/IEC 27004

4. Стандарт, по которому организация может быть сертифицирована по вопросам информационной безопасности:

1) ISO/IEC 27000
2) ISO/IEC 27001
3) ISO/IEC 27002
4) ISO/IEC 27003
5) ISO/IEC 27004

5. Год утверждения Доктрины информационной безопасности РФ:

1) 1995
2) 2000
3) 2003
4) 2015
5) 2016

6. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ закрепляет:

1) Концепция информационной безопасности РФ
2) Доктрина информационной безопасности РФ
3) Положение об информационной безопасности РФ

7. Орган, который является организатором деятельности государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам:

1) Гостехкомиссия России
2) Роскомнадзор
3) ФСТЭК

8. В настоящее время действует Федеральный закон от 27.07.2006 N 149-ФЗ...

1) «Об информации, информатизации и защите информации»
2) «Об информациии защите информации»

3) «Об информации, информационных технологиях и о защите информации»

4) «Об информации, информационных технологиях и защите информации»

#3

9. В настоящее время действует Федеральный закон от 06.04.2011 N 63-ФЗ...

1) "Об электронной цифровой подписи"

2) "Об электронно-цифровой подписи"

3) "Об электронной подписи"

10. Функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи осуществляет:

1) Гостехкомиссия России

2) Роскомнадзор

3) ФСТЭК

11 Уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных является

1) Гостехкомиссия России

2) Роскомнадзор

3) ФСТЭК

12. Гарантия получения требуемой информации или информационной услуги пользователем за определенное время:

1) доступность

2) целостность

3) конфиденциальность

4) актуальность

13. Гарантия того, что информация сейчас существует в ее исходном виде, т.е. не было произведено несанкционированных изменений:

1) доступность

2) целостность

3) конфиденциальность

4) актуальность

14. Гарантия доступности конкретной информации только тому кругу лиц, для которого она предназначена:

1) доступность

2) целостность

3) конфиденциальность

4) актуальность

15. Правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их статус регламентирует:

1) законодательно-правовой уровень формирования режима ИБ

2) административный уровень формирования режима ИБ

3) программно-технический уровень формирования режима ИБ

16. Комплекс мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации включает:

1) законодательно-правовой уровень формирования режима ИБ

2) административный уровень формирования режима ИБ

3) программно-технический уровень формирования режима ИБ

17. Программно-технический уровень формирования режима ИБ включает подуровни:

1) физический

2) технический (аппаратный)

3) программный

4) 2 и 3

5) 1,2 и 3

18. За нарушения в сфере информационной безопасности предусмотрена ответственность...

1) административная

2) гражданско-правовая

3) уголовная

4) 1 и 2

5) 1,2 и 3

19. Оценочный стандарт "Критерии оценки безопасности информационных технологий" ISO/IEC 15408 вводит иерархию:

1) класс–семейство–компонент–элемент

2) группа-подгруппа-компонент-элемент

3) семейство-группа-компонент-элемент

20. Типовой набор требований, которым с точки зрения ИБ должны удовлетворять продукты и/или системы определенного класса:

1) формуляр защиты;

2) стек защиты;

3) стандарт защиты

4) профиль защиты

21. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования

1) принцип системности

2) принцип комплексности

3) принцип непрерывной защиты

4) принцип разумной достаточности

5) принцип гибкости системы

22. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов:

1) компаньон - вирусы

2) черви

3) призраки

4) стелс - вирусы

5) макровирусы

23. Секретное слово или набор символов, предназначенный для подтверждения личности или полномочий, известное только пользователю и парольной системе:

1) идентификатор пользователя
2) пароль пользователя
3) учетная запись пользователя

24. К механическим системам защиты относятся:

1) проволока
2) забор
3) стена
4) сигнализация
5) 1-3

25. Какие компоненты входят в комплекс защиты охраняемых объектов:

1) сигнализация
2) охрана
3) датчики
4) телевизионная система
5) 1-4

26. Принцип определения Уровеня защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:

1) принцип системности
2) принцип комплексности
3) принцип непрерывности
4) принцип разумной достаточности
5) принцип гибкости системы

27.Совокупность норм и правил, регламентирующих процесс обработки информации, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз:

1) комплекс информационной безопасности
2) инструкции информационной безопасности
3) регламент информационной безопасности
4) политика информационной безопасности

28. К типам угроз безопасности парольных систем относятся:

1) словарная атака
2) тотальный перебор
3) атака на основе психологии
4) разглашение параметров учетной записи
5) 1-4

29. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов:

1) ревизор
2) иммунизатор

3) сканер
4) доктор

30.Наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа:

1) криптология
2) криптоанализ
3) криптография

31. Защищенность от негативных информационно-психологических и информационно- технических воздействий:

1) компьютерная безопасность
2) защищенность информации
3) защищенность потребителей информации

32. Гарантия того, что что авторизованные субъекты, осуществляя доступ к ресурсам, получат именно те ресурсы, доступ к которым запросили:

1) конфиденциальность
2) целостность
3) доступность
4) аутентичность
5) апеллируемость

3.2.2.Темы рефератов

1. Основные составляющие информационной безопасности.
2. Уровни режима информационной безопасности.
3. Административный уровень обеспечения информационной безопасности.
4. Классификация угроз ИБ.
5. Вирусы как угроза ИБ. Классификация компьютерных вирусов.
6. Характеристика «вирусоподобных» программ.
7. Антивирусные программные средства.
8. Обнаружение и профилактика вирусных атак.
9. Особенности обеспечения информационной безопасности в компьютерных сетях.
10. Сетевые модели передачи данных и безопасность.
11. Модель взаимодействия открытых систем OSI/ISO и проблемы ИБ.
12. Адресация в глобальных сетях и проблемы ИБ.
13. Классификация удаленных угроз в вычислительных сетях.
14. Типовые удаленные атаки и их характеристика.
15. Примеры и причины успешной реализации удаленных угроз в вычислительных сетях.
16. Принципы защиты распределенных вычислительных сетей.
17. Идентификация и аутентификация.
18. Криптография и шифрование. Методы разграничения доступа.
19. Регистрация и аудит. Межсетевое экранирование.
20. Технология виртуальных частных сетей VPN.

3.3 Третий этап (высокий уровень)

ВЛАДЕТЬ навыками по применению теоретических и практических знаний и умений при решении ситуационных задач, практической направленности по дисциплине.

3.3.1. Ситуационные задачи

1. Оцените защищенность компьютера вашего рабочего места от вирусов, вирусоподобных программ и сетевых атак путем исследования наличия программных средств и настроек. Дайте оценку полученным результатам

2. Оцените защищенность данных на компьютерах вашего сетевого окружения и серверах сети. Дайте оценку полученным результатам.

3. Оцените эффективность и безопасность работы компьютера вашего рабочего места с точки зрения наличия ошибок, ненужных файлов на диске и его фрагментации. Дайте оценку полученным результатам.

4. Произведите оценку доступности компьютера вашего рабочего места для сетевых атак с точки зрения открытых для атак портов. Дайте оценку полученным результатам.

5. Произведите оценку открытости для сетевых атак заданного сайта. Узнайте его IP - адрес, владельца сайта, дату регистрацию домена, оплату домена, используемое ПО (CMS). Дайте оценку полученным результатам.

6. Произведите определение настроек браузера вашего компьютера, влияющих на безопасности работы в сети Интернет, а также актуальность браузера. Дайте оценку полученным результатам и рекомендации по улучшению настроек.

7 Вы обнаружили, что диск D не содержит информации, которая там была. Видимо, вирус сделал все объекты скрытыми. У вас нет прав администратора. Можно ли решить проблему без вызова инженера? Опишите ваши действия.

8. Пользователь заметил, что ПК стал выполнять операции, команды, которые им не отдавались, перезагружаться, «тормозить». Перечислите возможные причины. Составьте список действий, которые должен последовательно произвести пользователь.

9. Разрабатывается информационная система, которая, в том числе, должна обеспечить работу с персональными данными. Составьте список действий, которые необходимо выполнить на этапе проектирования системы, ее ввода в действие и при эксплуатации.

10. Разрабатывается информационная система, которая, в том числе, должна обеспечить работу с информацией ограниченного доступа (коммерческой тайной). Составьте список действий, которые необходимо выполнить на этапе проектирования системы, ее ввода в действие и при эксплуатации.

11. Зашифруйте пословицу методом Цезаря и методом Гронсфельда. Открытый текст: ВСЁ ТАЙНОЕ СТАНОВИТСЯ ЯВНЫМ. Ключи назначьте сами. Оцените достоинства и недостатки использованных методов. Охарактеризуйте практическую значимость и сферу применения этих методов в настоящее время.

12. Пользователь получил сообщение от партнеров, зашифрованное. как сообщалось в письме, алгоритмом BlowFish, хэш Haval. Ранее пользователю был сообщен ключ. Как расшифровать сообщение и послать ответное сообщение, зашифрованное таким же образом и с тем же ключем? Проиллюстрируйте действия на примере с ключем QWERTY. Зашифрованное сообщение:
bewdkbllvoJxe1laJmaqO1XMp5FvJeyrr5TV0OCzGvUNen6drkCOeiVeLbdstsUz
5Pa9DJwI8FEiqVUDWdNT21BBEv+b

13. Создайте папку Защищенная, а в ней несколько файлов. Средствами ОС зашифруйте созданную папку с файлами. выполните архивацию сертификата шифрования. Найдите способ снятия шифрования с папки и вложенных файлов. Оцените практическую пользу от такого шифрования.

4. На основе ГОСТ Р ИСО/МЭК 17799-2005, и с точки зрения начальника отдела по вопросам информационной безопасности в небольшой организации разработайте перечень мероприятий при привлечении сторонних организаций к обработке информации.

15. Приобретается новый компьютер с предустановленной проприетарной ОС. Составьте список последовательных мероприятий (действий) для обеспечения его эффективной и безопасной работы при введении в эксплуатацию.

3.4. Представления оценочного средства в фонде

3.4.1. Пример экзаменационного билета

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.

2. Тестирование.

1. Орган, который является организатором деятельности государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам:

1) Гостехкомиссия России
2) Роскомнадзор
3) ФСТЭК

2. В настоящее время действует Федеральный закон от 27.07.2006 N 149-ФЗ...

1) «Об информации, информатизации и защите информации»
2) «Об информациии защите информации»
3) «Об информации, информационных технологиях и о защите информации»
4) «Об информации, информационных технологиях и защите информации»

#3

6. В настоящее время действует Федеральный закон от 06.04.2011 N 63-ФЗ...

1) "Об электронной цифровой подписи"
2) "Об электронно-цифровой подписи"
3) "Об электронной подписи"

7. Гарантия доступности конкретной информации только тому кругу лиц, для которого она предназначена:

1) доступность
2) целостность
3) конфиденциальность
4) актуальность

3. Комплекс мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации включает:

1) законодательно-правовой уровень формирования режима ИБ
2) административный уровень формирования режима ИБ
3) программно-технический уровень формирования режима ИБ

4. Программно-технический уровень формирования режима ИБ включает подуровни:

1) физический
2) технический (аппаратный)
3) программный
4) 2 и 3
5) 1,2 и 3

5. Оценочный стандарт "Критерии оценки безопасности информационных технологий" ISO/IEC 15408 вводит иерархию:

1) класс–семейство–компонент–элемент
2) группа-подгруппа-компонент-элемент
3) семейство-группа-компонент-элемент

8. Типовой набор требований, которым с точки зрения ИБ должны удовлетворять продукты и/или системы определенного класса:

1) формуляр защиты;
2) стек защиты;
3) стандарт защиты
4) профиль защиты

9. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования

1) принцип системности
2) принцип комплексности
3) принцип непрерывной защиты
4) принцип разумной достаточности
5) принцип гибкости системы

10. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов:

1) компаньон - вирусы
2) черви
3) призраки
4) стелс - вирусы
5) макровирусы

3. Ситуационная задача.

Пользователь заметил, что ПК стал выполнять операции, команды, которые им не отдавались, перезагружаться, «тормозить». Перечислите возможные причины. Составьте список действий, которые должен последовательно произвести пользователь.

Критерии оценки:
Отлично
Хорошо
Удовлетворительно
Неудовлетворительно

3.4.2. Вопросы для устного опроса (собеседование)

Наименование раздела: «Модуль 1. «Составляющие, уровни обеспечения и угрозы ИБ»

1. Доступность информации. Понятие и характеристики.
2. Целостность информации. Понятие и характеристики.
3. Конфиденциальность информации. Понятие и характеристики.
4. Доступность информации. Основные угрозы.
5. Целостность информации. Основные угрозы.
6. Конфиденциальность информации. Основные угрозы.
7. Уровни формирования информационной безопасности.
8. Законодательно-правовой уровень информационной безопасности.
9. Административный уровень информационной безопасности.
10. Программно-технический уровень информационной безопасности.
11. Цели и задачи информационной безопасности.
12. Информационная безопасность личности.
13. Информационная безопасность общества.
14. Информационная безопасность государства.

Наименование раздела: «Модуль 2. «Вирусы и удаленные угрозы в сетях»

1. Понятие и классификация вирусов.
2. Как работает вирус?
3. Способы заражения программ. Стандартные методы заражения.
4. Троянские программы.
5. Программы-шпионы.
6. Методы защиты от вирусов.
7. Антивирусные программы. Программы-детекторы. Программы-доктора.
8. Антивирусы-полифаги. Эвристические анализаторы.
9. Программы-ревизоры. Программы-фильтры.
10. Классификация сетевых атак.

Наименование раздела: «Модуль 3. «Принципы и методы защиты в вычислительных сетях»»

1. Методы защиты информации от несанкционированного доступа.
2. Способы опознавания (аутентификации) пользователей.
3. Опознавание с использованием простого пароля.
4. Использование динамически изменяющегося пароля.
5. Защита информации от исследования и копирования.
6. Криптографические методы защиты информации в автоматизированных

системах.

7. Симметричные криптосистемы. Системы с открытым ключом.

8. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации.

9. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.

10. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.

11. Архитектура механизмов защиты информации в сетях.

3.4.3. Пример ситуационной задачи (или задачи)

Задание:

Пользователь заметил, что ПК стал выполнять операции, команды, которые им не отдавались, перезагружаться, «тормозить». Перечислите возможные причины. Составьте список действий, которые должен последовательно произвести пользователь.

Перечень должен быть сохранен в файле с именем вида Фамилия, где Фамилия совпадает с фамилией студента, выполняющего работу.

Критерии оценки:

-оценка «зачтено/освоен» выставляется студенту, если студент продемонстрировал владение навыками решения ситуационной задачи, обладает теоретическими знаниями, умениями и владеет практическими навыками для решению данного класса задач;

- оценка «не зачтено/ не освоен» выставляется студенту, если студент не продемонстрировал владение навыками решения ситуационной задачи, не обладает теоретическими знаниями, умениями и не владеет практическими навыками для решению данного класса задач.

3.5. Критериев оценивания контрольных заданий для использования в ФОС дисциплины

3.5.1. Критерии оценивания на экзамене:

От 26 до 30 баллов и/или «отлично»: студент глубоко и полно владеет содержанием учебного материала и понятийным аппаратом; умеет связывать теорию с практикой, иллюстрировать примерами, фактами, данными научных исследований; осуществляет межпредметные связи, предложения, выводы; логично, показывает глубокие знания при ответах на поставленные вопросы; умеет обосновывать свои суждения и профессионально-личностную позицию по излагаемому вопросу; ответ носит самостоятельный характер.

От 16 до 25 баллов и/или «хорошо»: ответ студента соответствует указанным выше критериям, но в содержании имеют место отдельные неточности (несущественные ошибки) при изложении теоретического и практического материала; ответ отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой; однако допущенные ошибки исправляются самим студентом после дополнительных вопросов экзаменатора.

От 6 до 15 баллов и/или «удовлетворительно»: студент обнаруживает знание, умения и навыки основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности и существенные ошибки в определении понятий, формулировке положений; при аргументации ответа студент не опирается на основные положения исследовательских документов; не применяет теоретические знания, умения и навыки для объяснения эмпирических фактов и явлений, не обосновывает свои суждения; имеет место нарушение логики изложения; в целом ответ отличается низким уровнем самостоятельности, не содержит собственной профессионально-личностной позиции.

От 0 до 5 баллов и/или «неудовлетворительно»: студент имеет разрозненные, бессистемные знания, умения и навыки; не умеет выделять главное и второстепенное; в ответе допускаются ошибки в определении понятий, формулировке теоретических положений, искажающие их смысл; студент беспорядочно и неуверенно излагает материал; не умеет соединять теоретические положения с практикой; не владеет навыками и методами решения ситуационных задач.

3.5.2. Критерии оценивания тестового задания:

Тестовые задания оцениваются по шкале: 1 балл за правильный ответ, 0 баллов за неправильный ответ. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

Процент правильных ответов Оценка

90 – 100% *От 9 до 10 баллов и/или* «отлично»

70 –89 % *От 6 до 8 баллов и/или* «хорошо»

50 – 69 % *От 3 до 5 баллов и/или* «удовлетворительно»

менее 50 % *От 0 до 2 баллов и/или* «неудовлетворительно»

3.5.3. Критерии оценивания реферата (доклада):

От 4 до 5 баллов и/или «отлично»: глубокое и хорошо аргументированное обоснование темы; четкая формулировка и понимание изучаемой проблемы; широкое и правильное использование относящейся к теме литературы и примененных аналитических методов; содержание исследования и ход защиты указывают на наличие навыков работы студента в данной области; оформление работы хорошее с наличием расширенной библиографии; защита реферата (или выступление с докладом) показала высокий уровень профессиональной подготовленности студента;

От 2 до 3 баллов и/или «хорошо»: аргументированное обоснование темы; четкая формулировка и понимание изучаемой проблемы; использова-

ние ограниченного, но достаточного для проведения исследования количества источников; работа основана на среднем по глубине анализе изучаемой проблемы и при этом сделано незначительное число обобщений; содержание исследования и ход защиты (или выступление с докладом) указывают на наличие практических навыков работы студента в данной области; реферат (или доклад) хорошо оформлен с наличием необходимой библиографии; ход защиты реферата (или выступления с докладом) показал достаточную профессиональную подготовку студента;

От 1 до 2 баллов и/или «удовлетворительно»: достаточное обоснование выбранной темы, но отсутствует глубокое понимание рассматриваемой проблемы; в библиографии преобладают ссылки на стандартные литературные источники; труды, необходимые для всестороннего изучения проблемы, использованы в ограниченном объеме; заметна нехватка компетентности студента в данной области знаний; оформление реферата (или доклада) содержит небрежности; защита реферата (или выступление с докладом) показала удовлетворительную профессиональную подготовку студента;

0 баллов и/или «неудовлетворительно»: тема реферата (или доклада) представлена в общем виде; ограниченное число использованных литературных источников; шаблонное изложение материала; суждения по исследуемой проблеме не всегда компетентны; неточности и неверные выводы по рассматриваемой литературе; оформление реферата (или доклада) с элементами заметных отступлений от общих требований; во время защиты (или выступления с докладом) студентом проявлена ограниченная профессиональная эрудиция.

3.5.4. Критерии оценивания на ситуационную задачу:

От 9 до 10 баллов и/или «отлично»: студент глубоко и полно владеет методами решения задачи; решение выполнено оптимальным способом; полученное решение соответствует условиям задачи; решение ситуационной задачи носит самостоятельный характер.

От 6 до 8 баллов и/или «хорошо»: решение студента соответствует указанным выше критериям, но в ход решения имеет отдельные неточности (несущественные ошибки); однако допущенные при решении ошибки исправляются самим студентом после дополнительных вопросов.

От 3 до 5 баллов и/или «удовлетворительно»: студент обнаруживает отсутствие навыков и понимание основных методик решения ситуационной задачи, но решение является неполным, имеет неточности и существенные ошибки; допущенные при решении ошибки не исправляются самим студентом после дополнительных вопросов.

От 0 до 2 баллов и/или «неудовлетворительно»: студент имеет разрозненные, бессистемные знания в области решаемой задачи; не владеет методами и подходами для решения задачи.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура оценки знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, производится преподавателем в форме текущего контроля и промежуточной аттестации.

Для повышения эффективности текущего контроля и последующей промежуточной аттестации студентов осуществляется структурирование дисциплины на модули. Каждый модуль учебной дисциплины включает в себя изучение законченного раздела, части дисциплины.

Основными видами текущего контроля знаний, умений и навыков в течение каждого модуля учебной дисциплины являются устный опрос, тестирование, решение ситуационных задач, подготовка рефератов. Студент должен выполнить все контрольные мероприятия, предусмотренные в модуле учебной дисциплины к указанному сроку, после чего преподаватель проставляет балльные оценки, набранные студентом по результатам текущего контроля модуля учебной дисциплины.

Контрольное мероприятие считается выполненным, если за него студент получил оценку в баллах, не ниже минимальной оценки, установленной программой дисциплины по данному мероприятию.

Промежуточная аттестация обучающихся проводится в форме курсовой работы и экзамена.

Курсовая работа представляет собой завершенное исследование, в котором анализируются проблемы в исследуемой области, и раскрывается содержание и технологии разрешения этих проблем не только в теоретическом, но и в практическом плане на местном, региональном или федеральном уровнях. Работа должна носить творческий характер, отвечать требованиям логичного и четкого изложения материала, доказательности и достоверности фактов, отражать умения студента пользоваться рациональными приемами поиска, отбора, обработки и систематизации информации и содержать теоретические выводы и практические рекомендации.

Оценивание результатов курсового проектирования проводиться по следующим критериям:

1. Навыки самостоятельной работы с материалами, по их обработке, анализу и структурированию.
2. Умение правильно применять методы исследования.
3. Умение грамотно интерпретировать полученные результаты.
4. Способность осуществлять необходимые расчеты, получать результаты и грамотно излагать их в отчетной документации.
5. Умение выявить проблему, предложить способы ее разрешения, умение делать выводы.
6. Умение оформить итоговый отчет в соответствии со стандартными требованиями.

Пункты с 1 по 6 дают до 50% вклада в итоговую оценку студента.

7. Умение защищать результаты своей работы, грамотное построение речи, использование при выступлении специальных терминов.

8. Способность кратко и наглядно изложить результаты работы.

Пункты 7,8 дают до 35% вклада в итоговую оценку студента.

9. Уровень самостоятельности, творческой активности и оригинальности при выполнении работы.

10. Выступления на конференциях и подготовка к публикации тезисов для печати по итогам работы.

Пункты 9, 10 дают до 15 % вклада в итоговую оценку студента.

Оценка **«отлично»** ставится студенту, который в срок, в полном объеме и на высоком уровне выполнил курсовую работу (проект). Работа (проект) соответствует следующим требованиям:

1. Исследование выполнено самостоятельно, имеет научно-практический характер, содержит элементы новизны.

2. Студент показал знание теоретического материала по рассматриваемой проблеме, умение анализировать, аргументировать свою точку зрения, делать обобщение и выводы.

3. Материал излагается грамотно, логично, последовательно.

4. Отвечает требованиям написания курсовой работы.

5. Во время защиты студент показал умение кратко, доступно (ясно) представить результаты исследования, адекватно ответить на поставленные вопросы.

Оценка **«хорошо»** ставиться студенту, который выполнил курсовую работу (проект), но с незначительными замечаниями, был менее самостоятелен и инициативен.

1. Исследование выполнено самостоятельно, имеет научно-практический характер, содержит элементы новизны.

2. Студент показал знание теоретического материала по рассматриваемой проблеме, однако умение анализировать, аргументировать свою точку зрения, делать обобщения и выводы вызывают у него затруднения.

3. Материал не всегда излагается логично, последовательно.

4. Имеются недочеты в оформлении курсовой работы.

5. Во время защиты студент показал умение кратко, доступно (ясно) представить результаты исследования, однако затруднялся отвечать на поставленные вопросы.

Оценка **«удовлетворительно»** ставится студенту, если

1. Исследование не содержит элементы новизны.

2. Студент не в полной мере владеет теоретическим материалом по рассматриваемой проблеме, умение анализировать, аргументировать свою точку зрения, делать обобщение и выводы вызывают у него затруднения.

3. Материал не всегда излагается логично, последовательно.

4. Имеются недочеты в оформлении курсовой работы.

5. Во время защиты студент затрудняется в представлении результатов исследования и ответах на поставленные вопросы. Оценка **«неудовлетво-**

рительно» ставится студенту, который не выполнил курсовую работу, либо выполнил с грубыми нарушениями требований, не раскрыл заявленную тему, не выполнил практической части работы.

Экзамен проводится в устной или письменной форме по утвержденным билетам. Каждый билет содержит по два вопроса, и третьего, вопроса или задачи, или практического задания.

Первый вопрос в экзаменационном билете - вопрос для оценки уровня обученности «знать», в котором очевиден способ решения, усвоенный студентом при изучении дисциплины.

Второй вопрос для оценки уровня обученности «знать» и «уметь», который позволяет оценить не только знания по дисциплине, но и умения ими пользоваться при решении стандартных типовых задач.

Третий вопрос (задача/задание) для оценки уровня обученности «владеть», содержание которого предполагает использование комплекса умений и навыков, для того, чтобы обучающийся мог самостоятельно сконструировать способ решения, комбинируя известные ему способы и привлекая имеющиеся знания.

По итогам сдачи экзамена выставляется оценка.

Критерии оценки знаний обучающихся на экзамене:

- оценка «отлично» выставляется, если обучающийся обладает глубокими и прочными знаниями программного материала; при ответе на все вопросы билета продемонстрировал исчерпывающее, последовательное и логически стройное изложение; правильно сформулировал понятия и закономерности по вопросам; использовал примеры из дополнительной литературы и практики; сделал вывод по излагаемому материалу;
- оценка «хорошо» выставляется, если обучающийся обладает достаточно полным знанием программного материала; его ответ представляет грамотное изложение учебного материала по существу; отсутствуют существенные неточности в формулировании понятий; правильно применены теоретические положения, подтвержденные примерами; сделан вывод; два первых вопроса билета освещены полностью, а третий доводится до логического завершения после наводящих вопросов преподавателя;
- оценка «удовлетворительно» выставляется, если обучающийся имеет общие знания основного материала без усвоения некоторых существенных положений; формулирует основные понятия с некоторой неточностью; затрудняется в приведении примеров, подтверждающих теоретические положения; все вопросы билета начаты и при помощи наводящих вопросов преподавателя доводятся до конца;
- оценка «неудовлетворительно» выставляется, если обучающийся не знает значительную часть программного материала; допустил существенные ошибки в процессе изложения; не умеет выделить главное и сделать вывод; приводит ошибочные определения; ни один вопрос билета не рассмотрен до конца, даже при помощи наводящих вопросов преподавателя.

Основным методом оценки знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций является

балльно-рейтинговая система, которая регламентируется положением «О балльно-рейтинговой системе оценки качества освоения образовательных программ в ФГБОУ ВО Белгородский ГАУ».

Основными видами поэтапного контроля результатов обучения студентов являются: входной контроль, текущий контроль, рубежный (промежуточный) контроль, творческий контроль, выходной контроль (экзамен или вопросы к зачету).

Уровень развития компетенций оценивается с помощью рейтинговых баллов.

Рейтинги	**Характеристика рейтингов**	**Максимум баллов**
Входной	Отражает степень подготовленности студента к изучению дисциплины. Определяется по итогам входного контроля знаний на первом практическом занятии.	5
Рубежный	Отражает работу студента на протяжении всего периода изучения дисциплины. Определяется суммой баллов, которые студент получит по результатам изучения каждого модуля.	60
Творческий	Результат выполнения студентом индивидуального творческого задания различных уровней сложности, в том числе, участие в различных конференциях и конкурсах на протяжении всего курса изучения дисциплины.	5
Выходной	Является результатом аттестации на окончательном этапе изучения дисциплины по итогам сдачи экзамена. Отражает уровень освоения информационно-теоретического компонента в целом и основ практической деятельности в частности.	30
Общий рейтинг	Определяется путём суммирования всех рейтингов	100

Общий рейтинг по дисциплине складывается из входного, рубежного, выходного (экзамена или вопросы к зачету) и творческого рейтинга.

Входной (стартовый) рейтинг – результат входного контроля, проводимого с целью проверки исходного уровня подготовленности студента и оценки его соответствия предъявляемым требованиям для изучения данной дисциплины.

Он проводится на первом занятии при переходе к изучению дисциплины (курса, раздела). Оптимальные формы и методы входного контроля: тестирование, программированный опрос, в т.ч. с применением ПЭВМ и ТСО, решение комплексных и расчетно-графических задач и др.

Рубежный рейтинг – результат рубежного (промежуточного) контроля по каждому модулю дисциплины, проводимого с целью оценки уровня знаний, умений и навыков студента по результатам изучения модуля. Оптимальные формы и методы рубежного контроля: устные собеседования, письменные контрольные опросы, в т.ч. с использованием ПЭВМ и ТСО, результаты выполнения лабораторных и практических заданий. В качестве практических заданий могут выступать крупные части (этапы) курсовой работы или проекта, расчетно-графические задания, микропроекты и т.п.

Выходной рейтинг – результат аттестации на окончательном этапе изучения дисциплины по итогам сдачи экзамена, проводимого с целью проверки освоения информационно-теоретического компонента в целом и основ практической деятельности в частности. Оптимальные формы и методы выходного контроля: письменные экзаменационные или контрольные работы, индивидуальные собеседования.

Творческий рейтинг – составная часть общего рейтинга дисциплины, представляет собой результат выполнения студентом индивидуального творческого задания различных уровней сложности.

В рамках рейтинговой системы контроля успеваемости студентов, семестровая составляющая балльной оценки по дисциплине формируется при наборе заданной в программе дисциплины суммы баллов, получаемых студентом при текущем контроле в процессе освоения модулей учебной дисциплины в течение семестра.

Итоговая оценка /зачёта/ компетенций студента осуществляется путём автоматического перевода баллов общего рейтинга в стандартные оценки.

Максимальная сумма рейтинговых баллов по учебной дисциплине составляет 100 баллов.

По дисциплине с экзаменом необходимо использовать следующую шкалу пересчета суммарного количества набранных баллов в четырехбалльную систему:

Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
менее 51 балла	51-67 баллов	68-85 баллов	86-100 баллов